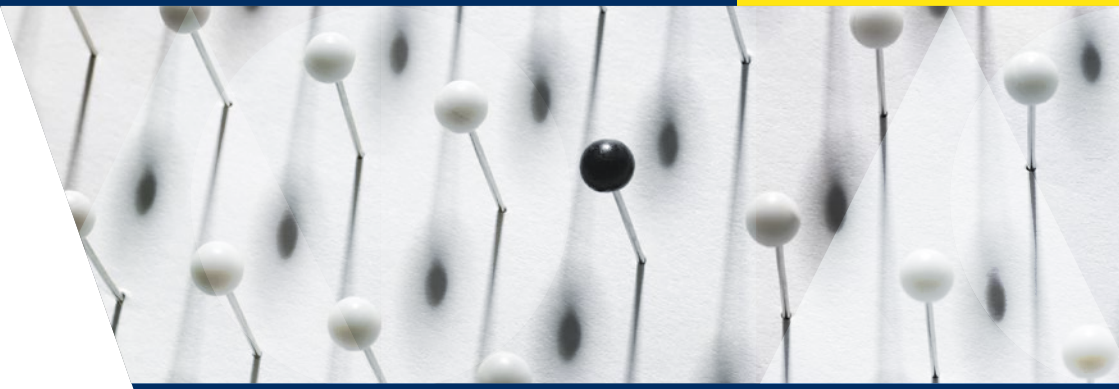
HANDBOEK



Handboek Europese gegevensbeschermings-wetgeving

Editie 2018

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Het manuscript van dit handboek is voltooid in april 2018.

Updates zullen in de toekomst beschikbaar worden gesteld op de website van FRA op fra.europa.eu, de website van de Raad van Europa op coe.int/dataprotection, de website van het Europees Hof voor de Rechten van de Mens onder het menu Rechtspraak (Case-law/Jurisprudence) op echr.coe.int, en op de website van de Europese Toezichthouder voor gegevensbescherming op edps.europa.eu.

Foto's (omslag en binnenin): © iStockphoto

Luxemburg: Bureau voor publicaties van de Europese Unie, 2021

RvE:	ISBN 978-92-871-9834-1		
FRA — print:	ISBN 978-92-9474-292-6	doi:10.2811/422118	TK-05-17-225-NL-C
FRA — pdf:	ISBN 978-92-9474-296-4	doi:10.2811/659087	TK-05-17-225-NL-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Handboek Europese gegevensbeschermings-wetgeving

Editie 2018

Voorwoord

Onze samenleving raakt in toenemende mate gedigitaliseerd. Het tempo waarin de technologie zich ontwikkelt en de manier waarop persoonsgegevens verwerkt worden, beïnvloeden het leven van iedereen elke dag en op allerlei manieren. Wettelijke kaders van de Europese Unie (EU) en de Raad van Europa, die de bescherming van persoonsgegevens en de persoonlijke levenssfeer waarborgen, zijn onlangs herzien.

Europa neemt wereldwijd het voortouw op het gebied van gegevensbescherming. De gegevensbeschermingsnormen van de EU zijn gebaseerd op Verdrag 108 van de Raad van Europa, EU-instrumenten — waaronder de algemene verordening gegevensbescherming en de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten — alsook op de respectievelijke jurisprudentie van het Europees Hof voor de Rechten van de Mens en het Hof van Justitie van de Europese Unie.

De door de EU en de Raad van Europa doorgevoerde gegevensbeschermingshervormingen zijn omvangrijk en bij tijd en wijle complex, met zeer uiteenlopende voordelen en gevolgen voor personen en ondernemingen. Met dit handboek wordt beoogd het bewustzijn en de kennis van gegevensbeschermingsregels te vergroten, in het bijzonder bij niet-gespecialiseerde juristen die in hun werk te maken hebben met gegevensbeschermingskwesties.

Het handboek is een gezamenlijke productie van het Bureau van de Europese Unie voor de grondrechten (FRA), de Raad van Europa (samen met de griffie van het Europees Hof voor de rechten van de mens) en de Europese Toezichthouder voor gegevensbescherming. Het is een nieuwe editie van het handboek van 2014 en onderdeel van een reeks juridische handboeken die geredigeerd zijn door FRA in samenwerking met de Raad van Europa.

Onze dank gaat uit naar de gegevensbeschermingsautoriteiten in België, Estland, Frankrijk, Georgië, Hongarije, Ierland, Italië, Monaco, Zwitserland en het Verenigd Koninkrijk voor hun nuttige feedback op de ontwerpversie van het handboek. Daarnaast willen wij de eenheden Gegevensbescherming en Internationale Datastromen

en -bescherming van de Europese Commissie onze waardering betuigen. Wij spreken onze dank uit aan het Hof van Justitie van de Europese Unie voor het beschikbaar stellen van relevante documenten tijdens de voorbereidende werkzaamheden voor dit handboek.

Christos Giakoumopoulos	**Giovanni Buttarelli**	**Michael O'Flaherty**
Directeur-generaal Mensenrechten en rechtsstaat van de Raad van Europa	Europese Toezichthouder voor gegevensbescherming	Directeur van het Bureau van de Europese Unie voor de grondrechten

Inhoudsopgave

Afkortingen en acroniemen

AVG	Algemene verordening gegevensbescherming
C.SIS	Centraal deel van het Schengeninformatiesysteem
CCTV	Gesloten televisiecircuit
CETS	Council of Europe Treaty Series
CRM	Customer relations management
DIS	Douane-informatiesysteem
DPA	Gegevensbeschermingsautoriteit
DPO	Functionaris voor gegevensbescherming
EDPB	Europees Comité voor gegevensbescherming
EDPS	Europese Toezichthouder voor gegevensbescherming
EER	Europese Economische Ruimte
EFSA	Europese Autoriteit voor Voedselveiligheid
EG	Europese Gemeenschap
EHRM	Europees Hof voor de Rechten van de Mens
Enisa	Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging
EOM	Europees Openbaar Ministerie
ESMA	Europese Autoriteit voor effecten en markten
eTEN	Trans-Europese telecommunicatienetwerken
EU	Europese Unie
eu-LISA	EU-agentschap voor grootschalige IT-systemen
EuroPriSe	European Privacy Seal
EVA	Europese Vrijhandelsassociatie
EVRM	Europees Verdrag voor de rechten van de mens
FRA	Bureau van de Europese Unie voor de grondrechten
GCO	Gemeenschappelijk controleorgaan
Gps	Global positioning system
Handvest	Handvest van de grondrechten van de Europese Unie
HvJ-EU	Hof van Justitie van de Europese Unie (tot december 2009 Hof van Justitie van de Europese Gemeenschappen (HvJ-EG) geheten)

ICT	Informatie- en communicatietechnologie
Isp	Internetserviceprovider
IVBPR	Internationaal Verdrag inzake burgerrechten en politieke rechten
N.SIS	Nationaal deel van het Schengeninformatiesysteem
NEE	Nationale Europol-eenheid
Ngo	Niet-gouvernementele organisatie
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
PB	Publicatieblad
Pin	Persoonlijk identificatienummer
PNR	Persoonsgegevens van passagiers
RvE	Raad van Europa
SCG	Coördinatiegroep voor toezicht
SEPA	Gemeenschappelijke betalingsruimte voor de euro
SIS	Schengeninformatiesysteem
Swift	Society for Worldwide Interbank Financial Telecommunication
UVRM	Universele Verklaring van de Rechten van de Mens
Verdrag 108	Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Raad van Europa) Het Wijzigingsprotocol (CETS nr. 223) bij Verdrag 108 ("Gemoderniseerd Verdrag 108") is door het Comité van Ministers van de Raad van Europa aangenomen ter gelegenheid van zijn 128ste zitting in Elsinore, Denemarken (17-18 mei 2018). Verwijzingen naar het "Gemoderniseerd Verdrag 108" verwijzen naar het Verdrag zoals gewijzigd door Protocol CETS nr. 223.
VEU	Verdrag betreffende de Europese Unie
VIS	Visuminformatiesysteem
VN	Verenigde Naties
VWEU	Verdrag betreffende de werking van de Europese Unie

Hoe dit handboek te gebruiken

Dit handboek biedt een overzicht van de rechtsnormen op het gebied van gegevensbescherming die door de Europese Unie (EU) en de Raad van Europa (RvE) zijn vastgesteld. Het is bedoeld voor niet in gegevensbescherming gespecialiseerde beroepsbeoefenaars, zoals advocaten, rechters en andere beoefenaars van juridische beroepen, evenals personen die werkzaam zijn voor andere organen, zoals niet-gouvernementele organisaties (ngo's), die in hun werk te maken kunnen krijgen met juridische vraagstukken die verband houden met gegevensbescherming.

Het handboek dient als eerste referentiepunt voor de toepasselijke EU-wetgeving en het Europees Verdrag voor de rechten van de mens (EVRM), het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108) en andere instrumenten van de RvE.

In elk hoofdstuk wordt eerst een tabel gegeven met de wettelijke bepalingen die relevant zijn voor de onderwerpen in dat hoofdstuk. In de tabellen wordt zowel wetgeving van de RvE als EU-wetgeving vermeld, evenals een selectie van jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en het Hof van Justitie van de Europese Unie (HvJ-EU). Vervolgens wordt voor elk behandeld onderwerp de toepasselijke wetgeving van de twee Europese rechtsstelsels gepresenteerd. Hierdoor kan de lezer zien op welke punten de twee rechtsstelsels overeenkomen en op welke punten ze van elkaar verschillen. Dit zou lezers tevens moeten helpen om de belangrijkste informatie met betrekking tot hun situatie te vinden, met name als ze alleen onder het RvE-recht vallen. In sommige hoofdstukken wijkt de volgorde van de onderwerpen in de tabellen enigszins af van die in de tekst, indien dit ertoe bijdraagt de inhoud beknopt te presenteren. Het handboek biedt bovendien een summier overzicht van het rechtskader van de Verenigde Naties.

Beoefenaars van juridische beroepen in niet-EU-lidstaten die zijn aangesloten bij de RvE en partij zijn bij het EVRM en Verdrag 108, kunnen de informatie die relevant is voor hun eigen land vinden door rechtstreeks naar de gedeelten over de RvE-wetgeving te gaan. Beroepsbeoefenaars in niet-EU-lidstaten moeten er ook rekening mee houden dat sinds de aanneming van de algemene verordening gegevensbescherming van de Europese Unie de EU-regels inzake gegevensbescherming ook van toepassing zijn op organisaties en andere entiteiten die niet in de EU zijn gevestigd, indien zij persoonsgegevens verwerken en goederen en diensten aanbieden aan betrokkenen in de Unie of het gedrag van die betrokkenen observeren.

Beoefenaars van juridische beroepen in EU-lidstaten zullen beide delen moeten gebruiken, omdat deze staten aan beide rechtsordes zijn gebonden. De hervormingen en de modernisering van de regelgeving aangaande gegevensbescherming in Europa zijn gelijktijdig doorgevoerd in het kader van de Raad van Europa (Gemoderniseerd Verdrag 108 zoals gewijzigd door Protocol CETS nr. 223) en de EU (vaststelling van de algemene verordening gegevensbescherming en Richtlijn (EU) 2016/680). Toezichthouders in beide rechtsstelsels hebben nauwlettend toegezien op de consistentie en de compatibiliteit tussen de twee rechtskaders. De hervormingen hebben aldus voor een betere harmonisatie gezorgd tussen de gegevensbeschermingswetgeving van de RvE en die van de EU. Voor wie behoefte heeft aan meer informatie over een bepaald onderwerp, is een lijst met meer gespecialiseerd materiaal opgenomen onder "Aanbevolen literatuur". Voor informatie over de bepalingen van Verdrag 108 en het aanvullende Protocol van 2001, die van toepassing blijven tot de inwerkingtreding van het Wijzigingsprotocol, dienen lezers de editie van 2014 van het handboek te raadplegen.

De RvE-wetgeving wordt gepresenteerd door middel van korte verwijzingen naar geselecteerde zaken van het EHRM. Deze zijn gekozen uit een groot aantal arresten en beslissingen van het EHRM over gegevensbeschermingsvraagstukken.

Het relevante EU-recht omvat vastgestelde wetgevingsmaatregelen, relevante bepalingen van de verdragen en het Handvest van de grondrechten van de Europese Unie, zoals uitgelegd in de jurisprudentie van het HvJ-EU. Voorts geeft het handboek adviezen en richtsnoeren die zijn vastgesteld door Groep artikel 29, het adviesorgaan dat in het kader van de richtlijn gegevensbescherming belast is met het verstrekken van deskundig advies aan de EU-lidstaten, en dat met ingang van 25 mei 2018 zal worden opgevolgd door het Europees Comité voor gegevensbescherming (EDPB). Ook adviezen van de Europese Toezichthouder voor gegevensbescherming bieden een belangrijk inzicht in de interpretatie van EU-wetgeving en zijn daarom in dit handboek opgenomen.

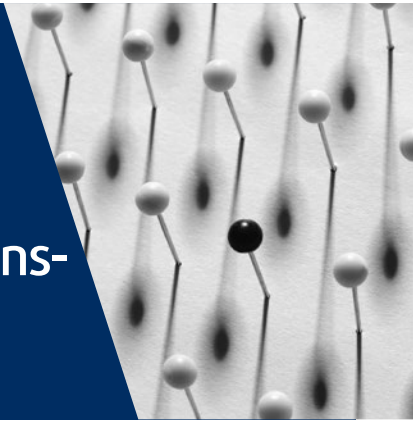
De in het handboek beschreven of geciteerde zaken dienen als voorbeeld van de uitgebreide jurisprudentie van zowel het EHRM als het HvJ-EU. De richtsnoeren aan het eind van dit handboek zijn bedoeld om de lezer te helpen bij het zoeken naar jurisprudentie op internet. De gepresenteerde rechtspraak van het HvJ-EU heeft betrekking op de voormalige richtlijn gegevensbescherming. De interpretaties van het HvJ-EU blijven echter van toepassing op de overeenkomstige rechten en verplichtingen die zijn vastgesteld in de algemene verordening gegevensbescherming.

Voorts worden, in tekstvakken met een blauwe achtergrond, met behulp van hypothetische scenario's praktische voorbeelden gegeven. Deze vormen een nadere illustratie van de toepassing van Europese gegevensbeschermingsregels in de praktijk, in het bijzonder wanneer er geen specifieke jurisprudentie van het EHRM of het HvJ-EU over het desbetreffende onderwerp bestaat. In andere tekstvakken, met een grijze achtergrond, worden voorbeelden gegeven uit andere bronnen dan het EHRM en het HvJ-EU, zoals wetgeving en de adviezen van Groep artikel 29.

Het handboek begint met een korte beschrijving van de rol van de twee rechtsstelsels als vastgesteld door het EVRM en het EU-recht (hoofdstuk 1). De hoofdstukken 2 tot en met 10 hebben betrekking op de volgende onderwerpen:

- gegevensbeschermingsterminologie;
- de belangrijkste beginselen van de Europese gegevensbeschermingswetgeving;
- de voorschriften van de Europese gegevensbeschermingswetgeving;
- het onafhankelijk toezicht;
- de rechten van betrokkenen en de handhaving van deze rechten;
- grensoverschrijdende doorgifte en grensoverschrijdend verkeer van persoonsgegevens;
- gegevensbescherming in het kader van politie en justitie;
- andere Europese gegevensbeschermingsregels op specifieke gebieden;
- actuele uitdagingen bij de bescherming van persoonsgegevens.

1 Context en achtergrond van de Europese gegevens-beschermingswetgeving



EU	Behandelde onderwerpen	RvE
Het recht op gegevensbescherming		
Verdrag betreffende de werking van de Europese Unie, artikel 16 Handvest van de grondrechten van de Europese Unie ("het Handvest"), artikel 8 (recht op bescherming van persoonsgegevens) Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (richtlijn gegevensbescherming), PB L 281 van 23.11.1995 (van kracht tot mei 2018) Kaderbesluit 2008/977/JBZ van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, PB L 350 van 30.12.2008 (van kracht tot mei 2018) Verordening (EU) 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), PB L 119 van 4.5.2016		EVRM, artikel 8 (recht op eerbiediging van het privéleven, het familie- en gezinsleven, de woning en de correspondentie) Gemoderniseerd Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Gemoderniseerd Verdrag 108)

EU	Behandelde onderwerpen	RvE
Richtlijn (EU) 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ (gegevensbescherming voor politiële en strafrechtelijke autoriteiten), PB L 119 van 4.5.2016 Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), PB L 201 van 31.7.2002 Verordening (EG) nr. 45/2001 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (verordening gegevensbescherming EU-instellingen), PB L 8 van 12.1.2001		
Beperkingen van het recht op bescherming van persoonsgegevens		
Handvest, artikel 52, lid 1 Algemene verordening gegevensbescherming, artikel 23 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert/Land Hessen* [Grote kamer], 2010		EVRM, artikel 8, lid 2 Gemoderniseerd Verdrag 108, artikel 11 EHRM, *S. en Marper/Verenigd Koninkrijk* [Grote kamer], nr. 30562/04 en 30566/04, 2008

EU	Behandelde onderwerpen	RvE
Afweging van rechten		
HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert/Land Hessen* [Grote kamer], 2010	**Algemeen**	
HvJ-EU, zaak C-73/07, *Tietosuojavaltuutettu/ Satakunnan Markkinapörssi Oy en Satamedia Oy* [Grote kamer], 2008 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 2014	**Vrijheid van meningsuiting**	EHRM, *Axel Springer AG/Duitsland* [Grote kamer], nr. 39954/08, 2012 EHRM, *Mosley/ Verenigd Koninkrijk*, nr. 48009/08, 2011 EHRM, *Bohlen/ Duitsland*, nr. 53495/09, 2015
HvJ-EU, zaak C-28/08 P, *Europese Commissie/The Bavarian Lager Co. Ltd* [Grote kamer], 2010 HvJ-EU, zaak C-615/13 P, *ClientEarth, PAN Europe/EFSA*, 2015	**Toegang tot documenten**	EHRM, *Magyar Helsinki Bizottság/Hongarije* [Grote kamer], nr. 18030/11, 2016
Algemene verordening gegevensbescherming, artikel 90	**Beroepsgeheim**	EHRM, *Pruteanu/ Roemenië*, nr. 30181/05, 2015
Algemene verordening gegevensbescherming, artikel 91	**Vrijheid van godsdienst en overtuiging**	
	Vrijheid van kunsten en wetenschappen	EHRM, *Vereinigung bildender Künstler/ Oostenrijk*, nr. 68354/01, 2007
HvJ-EU, zaak C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [Grote kamer], 2008	**Bescherming van eigendom**	
HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 2014 HvJ-EU, zaak C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 2017	**Economische rechten**	

1.1. Het recht op bescherming van persoonsgegevens

Belangrijkste punten

- Krachtens artikel 8 van het EVRM is het recht van een persoon op bescherming in verband met de verwerking van persoonsgegevens onderdeel van het recht op eerbiediging van het privéleven, het familie- en gezinsleven, de woning en de correspondentie.
- Verdrag 108 van de Raad van Europa is het eerste en tot nu toe enige internationale wettelijk bindende instrument dat betrekking heeft op gegevensbescherming. Het Verdrag heeft een moderniseringsproces ondergaan, dat werd voltooid met de aanname van het Wijzigingsprotocol CETS nr. 223.
- In het EU-recht is gegevensbescherming erkend als een afzonderlijk grondrecht. Het wordt bekrachtigd in artikel 16 van het Verdrag betreffende de werking van de Europese Unie en in artikel 8 van het EU-Handvest van de grondrechten.
- In het EU-recht werd gegevensbescherming voor het eerst gereguleerd in 1995 middels de richtlijn gegevensbescherming.
- Gezien de snelle technologische ontwikkelingen nam de EU in 2016 nieuwe wetgeving aan om de voorschriften op het gebied van gegevensbescherming aan te passen aan het digitale tijdperk. De algemene verordening gegevensbescherming is in mei 2018 in werking getreden, waarbij de richtlijn gegevensbescherming werd ingetrokken.
- De EU heeft naast de algemene verordening gegevensbescherming wetgeving aangenomen op het gebied van de verwerking van persoonsgegevens door autoriteiten van de lidstaten voor rechtshandhavingsdoeleinden. Richtlijn (EU) 2016/680 bepaalt de gegevensbeschermingsregels en de beginselen in verband met de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

1.1.1. Het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens: een korte introductie

Het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens zijn, hoewel nauw verwant, afzonderlijke rechten. Het recht op bescherming van de persoonlijke levenssfeer (in de Europese wetgeving: "recht op eerbiediging van het privéleven") verscheen voor het eerst in het internationale

recht inzake de mensenrechten in de in 1948 aangenomen Universele Verklaring van de Rechten van de Mens (UVRM), als één van de beschermde fundamentele mensenrechten. Kort na aanneming van de UVRM werd dit recht tevens erkend in het Europese recht door opneming in het in 1950 opgestelde Europees Verdrag voor de rechten van de mens (EVRM), dat juridisch bindend is voor de partijen bij het verdrag. In het EVRM is bepaald dat eenieder recht heeft op respect voor zijn of haar privéleven, familie- en gezinsleven, woning en correspondentie. Het is overheidsinstanties niet toegestaan aan dit recht voorbij te gaan, behalve wanneer dit gebeurt in overeenstemming met de wettelijke voorzieningen en in dienst van belangrijke en rechtmatige openbare belangen, en wanneer het noodzakelijk is in een democratische samenleving.

De aanneming van de UVRM en van het EVRM vond plaats ver vóór de ontwikkeling van computers en het internet en de opkomst van de informatiemaatschappij. Deze ontwikkelingen hebben zowel individuele personen als samenlevingen aanzienlijke voordelen gebracht, zoals een betere kwaliteit van leven, meer efficientie en een hogere productiviteit. Tegelijkertijd brengen ze nieuwe bedreigingen met zich mee voor het recht op eerbiediging van het privéleven. In antwoord op de noodzaak specifieke regels in te voeren voor de verzameling en het gebruik van persoonlijke informatie, ontstond een nieuwe opvatting van het begrip privacy dat in sommige rechtsgebieden wordt aangeduid als "informationele privacy" en in andere als het "recht op informationele zelfbeschikking"[1]. Deze opvatting heeft geleid tot de ontwikkeling van specifieke wettelijke voorschriften ter bescherming van persoonsgegevens.

Gegevensbescherming in Europa begon in de jaren zeventig, toen een aantal lidstaten wetgeving invoerden om de verwerking van persoonsgegevens door overheidsinstanties en grote ondernemingen te reguleren[2]. Instrumenten voor gege-

1 Het Duits Constitutioneel Gerechtshof erkende in 1983 het recht op informationele zelfbeschikking met de uitspraak in *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. Het Hof oordeelde dat informationele zelfbeschikking een afgeleide is van het door de Duitse grondwet beschermde fundamentele recht op eerbiediging van de persoonlijkheid. In 2017 erkende het EHRM in een uitspraak dat artikel 8 van het EVRM "voorziet in het recht op een vorm van informationele zelfbeschikking". Zie EHRM, *Satakunnan Markkinapörssi Oy en Satamedia Oy/Finland*, nr. 931/13, 27 juni 2017, punt 137.

2 De Duitse deelstaat Hessen nam in 1970 de eerste wet voor gegevensbescherming aan. Deze was slechts van toepassing in de deelstaat. In 1973 werd in Zweden de eerste nationale gegevensbeschermingswet aangenomen. Tegen het einde van de jaren 80 van de vorige eeuw hadden verschillende andere Europese landen (Frankrijk, Duitsland, Nederland en het Verenigd Koninkrijk) ook wetgeving voor gegevensbescherming aangenomen.

vensbescherming werden toen vastgesteld op Europees niveau[3], en door de jaren heen is gegevensbescherming geëvolueerd tot een afzonderlijke waarde die niet wordt ondergebracht onder het recht op eerbiediging van het privéleven. In de rechtsorde van de EU wordt de bescherming van gegevens erkend als een grondrecht, los van het fundamentele recht op eerbiediging van het privéleven. Dit onderscheid werpt de vraag op wat het verband is en wat de verschillen zijn tussen deze twee rechten.

Het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens zijn nauw met elkaar verbonden. Beide streven de bescherming na van vergelijkbare waarden: de autonomie en menselijke waardigheid van personen, door hun een persoonlijke levenssfeer toe te kennen waarin zij vrijelijk hun persoonlijkheid kunnen ontwikkelen en hun gedachten en opvattingen kunnen vormen. Zij zijn dan ook een noodzakelijke voorwaarde voor de uitoefening van andere fundamentele vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van vreedzame vergadering en vereniging, en de vrijheid van godsdienst.

De twee rechten verschillen in hun formulering en werkingssfeer. Het recht op eerbiediging van het privéleven behelst een algemeen verbod op inmenging, met inachtneming van een aantal criteria van algemeen belang die in bepaalde gevallen inmenging kunnen rechtvaardigen. De bescherming van persoonsgegevens wordt beschouwd als een modern, actief recht[4], waarbij een systeem van controlemechanismen wordt ingevoerd dat personen iedere keer dat hun persoonsgegevens worden verwerkt, bescherming biedt. Bij de verwerking moet worden voldaan aan de essentiële elementen van persoonsgegevensbescherming: onafhankelijk toezicht en eerbiediging van de rechten van de betrokkene[5].

Artikel 8 van het EU-Handvest van de grondrechten (hierna "het Handvest") bekrachtigt niet alleen het recht op bescherming van persoonsgegevens, maar

3 Het Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108) werd aangenomen in 1981. In 1995 nam de EU haar eerste alomvattende instrument voor gegevensbescherming aan: Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

4 Advocaat-generaal Sharpston heeft opgemerkt dat er in de betreffende kwestie sprake is van twee afzonderlijke rechten: het "klassieke" recht op bescherming van de persoonlijke levenssfeer en een meer "modern" recht: het recht op gegevensbescherming. Zie HvJ-EU, gevoegde zaken C-92/09 en C-93/02, *Volker und Markus Schecke GbR/Land Hessen, Conclusie van advocaat-generaal Sharpston* van 17 juni 2010, punt 71.

5 Hustinx, P., EDPS Speeches & Articles, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, juli 2013.

beschrijft tevens nauwkeurig de met dit recht verband houdende fundamentele waarden. Het bepaalt dat de verwerking van persoonsgegevens eerlijk dient te geschieden, voor bepaalde doeleinden, en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Betrokkenen moeten recht van inzage hebben in de over hen verzamelde gegevens en recht op rectificatie daarvan, en een onafhankelijke autoriteit dient erop toe te zien dat deze regels worden nageleefd.

Het recht op bescherming van persoonsgegevens is van toepassing in iedere situatie waarin persoonsgegevens worden verwerkt. Het is dan ook ruimer dan het recht op eerbiediging van het privéleven. Voor elke verrichting waarbij persoonsgegevens worden verwerkt, geldt een passende bescherming. Gegevensbescherming geldt voor alle mogelijke soorten persoonsgegevens en gegevensverwerking, ongeacht de relatie en het effect op de persoonlijke levenssfeer. De verwerking van persoonsgegevens kan daarnaast inbreuk maken op het recht op een privéleven, zoals met de onderstaande voorbeelden wordt geïllustreerd. De regels voor gegevensbescherming kunnen echter van toepassing zijn zonder dat een inbreuk op de persoonlijke levenssfeer wordt aangetoond.

Het recht op een privéleven is van toepassing in situaties waarin inbreuk is gemaakt op een persoonlijk belang, of de "persoonlijke levenssfeer" van een individu. Zoals uit vele voorbeelden in dit handboek blijkt, wordt in de jurisprudentie het begrip "persoonlijke levenssfeer" ruim geïnterpreteerd: als betrekking hebbend op intieme situaties, gevoelige of vertrouwelijke informatie, informatie die het imago van een persoon kan schaden, en zelfs aspecten van het beroepsleven en gedrag in het openbaar. Per geval moeten echter de omstandigheden en de feiten worden beoordeeld om te kunnen vaststellen of er sprake is of is geweest van inbreuk op de "persoonlijke levenssfeer".

Daarentegen kan elke handeling waarbij persoonsgegevens worden verwerkt binnen de werkingssfeer van de gegevensbeschermingsregels vallen en het recht op bescherming van persoonsgegevens activeren. Wanneer een werkgever bijvoorbeeld gegevens vastlegt met betrekking tot de naam van werknemers en het aan hen betaalde loon kan het vastleggen alleen van deze gegevens niet worden beschouwd als een inmenging in de persoonlijke levenssfeer. Een dergelijke inmenging zou echter wel kunnen worden aangevoerd als de werkgever de persoonlijke gegevens van werknemers bijvoorbeeld aan derden zou doorgeven. Werkgevers moeten hoe dan ook voldoen aan de voorschriften inzake gegevensbescherming, omdat de registratie van gegevens van werknemers een vorm van gegevensverwerking is.

Voorbeeld: In de zaak *Digital Rights Ireland*[6] werd het HvJ-EU verzocht om een prejudiciële beslissing over de geldigheid van Richtlijn 2006/24/EG in het licht van het fundamentele recht op bescherming van persoonsgegevens en eerbiediging van het privéleven, zoals neergelegd in het EU-Handvest van de grondrechten. Volgens deze richtlijn moesten aanbieders van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken telecommunicatiegegevens van burgers tot een periode van twee jaar bewaren, om te waarborgen dat die gegevens beschikbaar waren voor het onderzoeken, opsporen en vervolgen van zware criminaliteit. De maatregel had alleen betrekking op metagegevens, locatiegegevens en gegevens die nodig waren om de abonnee of gebruiker te identificeren. Hij was niet van toepassing op de inhoud van elektronische communicatie.

Het HvJ-EU oordeelde dat de richtlijn een inmenging vormde in het fundamentele recht op bescherming van persoonsgegevens "aangezien zij voorziet in de verwerking van persoonsgegevens"[7]. Daarbij kwam het tot de bevinding dat de richtlijn een inbreuk vormde op het recht op eerbiediging van het privéleven[8]. Uit de krachtens deze richtlijn bewaarde persoonsgegevens, waartoe bevoegde instanties toegang zouden hebben, zouden, in hun geheel beschouwd, "zeer precieze conclusies [kunnen] worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren"[9]. Er was sprake van een zeer ruime en bijzonder ernstige inmenging in de twee rechten.

Het HvJ-EU verklaarde dat Richtlijn 2006/24/EG ongeldig was en oordeelde dat het nagestreefde doel weliswaar legitiem was, maar de inmenging in de rechten op bescherming van persoonsgegevens en eerbiediging van het privéleven ernstig was en niet beperkt tot het strikt noodzakelijke.

6 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en Kärntner Landesregierung e.a. [Grote kamer], 8 april 2014.

7 *Ibid.*, punt 36.

8 *Ibid.*, punten 32-35.

9 *Ibid.*, punt 27.

1.1.2. Internationaal wettelijk kader: Verenigde Naties

Het wettelijk kader van de VN erkent de bescherming van persoonsgegevens niet als grondrecht, hoewel het recht op privacy een reeds lang gevestigd grondrecht is in het internationale recht. Artikel 12 van de UVRM betreffende de eerbiediging van het privé- en gezinsleven[10] markeerde de eerste keer dat een internationaal rechtsinstrument het recht van personen op bescherming tegen inbreuken op hun persoonlijke levenssfeer, met name door de staat, vastlegde. Hoewel een niet-bindende verklaring, geniet de UVRM toch aanmerkelijke erkenning als het grondleggend instrument van het internationale recht inzake de mensenrechten, en is ze van invloed geweest op de ontwikkeling van andere mensenrechteninstrumenten in Europa. Het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR) trad in 1976 in werking. Het verklaart dat niemand mag worden onderworpen aan willekeurige of onrechtmatige inmenging in het privéleven, de woning of de correspondentie, of aan onrechtmatige aantasting van zijn of haar eer en reputatie. Het IVBPR is een internationaal verdrag waarmee de 169 deelnemende partijen zich ertoe verplichten de uitoefening van burgerrechten voor natuurlijke personen, waaronder het recht op een privéleven, te eerbiedigen en te beschermen.

Sinds 2013 hebben de Verenigde Naties in antwoord op de ontwikkeling van nieuwe technologieën en onthullingen over in sommige landen plaatsvindende massasurveillance (de Snowden-onthullingen) twee resoluties over privacykwesties aangenomen onder de noemer "het recht op privacy in het digitale tijdperk"[11]. Hierin wordt grootschalige surveillance sterk veroordeeld en wordt benadrukt welke gevolgen dergelijke surveillance kan hebben voor het grondrecht op privacy en de vrijheid van meningsuiting, en voor het functioneren van een dynamische en democratische samenleving. Hoewel zij niet juridisch bindend zijn, hebben de resoluties een belangrijk internationaal politiek debat op hoog niveau op gang gebracht over privacy, nieuwe technologieën en surveillance. Zij hebben ook geleid tot de instelling van een speciale VN-rapporteur voor het recht op privacy, met het mandaat dit recht te bevorderen en te beschermen. De taken van de rapporteur zijn onder meer het verzamelen van informatie over nationale praktijken en ervaringen op het gebied van privacy en de uitdagingen die voortvloeien uit nieuwe technologieën, de uitwisseling en bevordering van beste praktijken, en het signaleren van mogelijke belemmeringen.

10 Verenigde Naties (VN), Universele Verklaring van de Rechten van de Mens (UVRM), 10 december 1948.

11 Zie VN, Algemene Vergadering, Resolution on the right to privacy in the digital age, A/RES/68/167, New York, 18 december 2013, en VN, Algemene Vergadering, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev.1, New York, 19 november 2014.

Terwijl in eerdere resoluties aandacht werd besteed aan de negatieve effecten van grootschalige surveillance en de verantwoordelijkheid van landen om de macht van inlichtingendiensten te beperken, zijn recentere resoluties een weerspiegeling van een cruciale ontwikkeling in het debat over privacy binnen de Verenigde Naties[12]. De in 2016 en 2017 vastgestelde verordeningen herbevestigen de nood om de bevoegdheden van inlichtingendiensten te beperken en grootschalige bewaking te veroordelen. Daarin wordt echter ook uitdrukkelijk gesteld dat "de toenemende mogelijkheden van ondernemingen voor het verzamelen, verwerken en gebruiken van persoonsgegevens een gevaar vormen voor de uitoefening van het recht op privacy in het digitale tijdperk". In de resoluties wordt dan ook gewezen op de verantwoordelijkheid van de particuliere sector, naast die van de overheden, voor het eerbiedigen van de mensenrechten, en ondernemingen worden opgeroepen gebruikers te informeren over de verzameling, het gebruik, de uitwisseling en de bewaring van persoonsgegevens en een transparant verwerkingsbeleid vast te stellen.

1.1.3. Het Europees Verdrag voor de rechten van de mens

De Raad van Europa (RvE) is opgericht in de nasleep van de Tweede Wereldoorlog om de staten van Europa te verenigen met het oog op de bevordering van de rechtsstaat, de democratie, de mensenrechten en de sociale ontwikkeling. Hiertoe heeft de RvE in 1950 het EVRM aangenomen, dat in 1953 in werking trad.

De partijen bij het verdrag hebben een internationale verplichting om het EVRM na te leven. Alle lidstaten van de RvE hebben het EVRM inmiddels in hun nationaal recht geïntegreerd of rechtskracht aan het EVRM gegeven, waardoor ze in overeenstemming met de bepalingen van het verdrag moeten handelen. De verdragsluitende partijen moeten de overeengekomen rechten eerbiedigen bij elke uitvoering van een activiteit of uitoefening van een bevoegdheid. Hier onder zijn begrepen activiteiten die worden ondernomen ten behoeve van de nationale veiligheid. Het Europees Hof voor de rechten van de mens (EHRM) heeft verschillende beginselarresten gewezen in zaken waarin sprake was van activiteiten door de staat op de gevoelige gebieden van het nationale veiligheidsrecht en de nationale

12 VN, Algemene Vergadering, Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/Rev.1, New York, 16 november 2016; VN, Raad voor de mensenrechten, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22 maart 2017.

veiligheidspraktijk[13]. Het Hof heeft niet geaarzeld te bevestigen dat surveillance-activiteiten een inbreuk op de eerbiediging van het privéleven inhouden[14].

Om ervoor te zorgen dat de verdragsluitende partijen hun verplichtingen uit hoofde van het EVRM nakomen, is in 1959 het EHRM opgericht, dat is gevestigd in Straatsburg, Frankrijk. Het EHRM zorgt ervoor dat staten hun verplichtingen uit hoofde van het EVRM nakomen door klachten van natuurlijke personen, groepen van natuurlijke personen, ngo's of rechtspersonen naar aanleiding van een vermeende inbreuk op het EVRM te beoordelen. Het EHRM kan ook geschillen tussen staten die door een of meer RvE-lidstaten tegen een andere lidstaat aanhangig zijn gemaakt, aan een onderzoek onderwerpen.

In 2018 telde de RvE 47 lidstaten, waarvan er 28 ook lidstaat van de EU zijn. Iemand hoeft geen onderdaan van een van de verdragsluitende partijen te zijn om een verzoek bij het EHRM te kunnen indienen, maar vermeende inbreuken moeten wel plaatshebben (of hebben gehad) binnen het rechtsgebied van een van de verdragsluitende partijen.

Het recht op bescherming van persoonsgegevens maakt deel uit van de rechten die worden beschermd door artikel 8 van het EVRM, dat het recht op eerbiediging van het privé-, familie- en gezinsleven, de woning en de correspondentie garandeert en waarin de voorwaarden zijn neergelegd waaronder beperkingen van dit recht zijn toegestaan[15].

Het EHRM heeft een groot aantal situaties beoordeeld waarin kwesties op het gebied van gegevensbescherming een rol speelden. Onder andere de onderscheppping van communicatie[16], verschillende vormen van surveillance door zowel de particuliere als de publieke sector[17], en bescherming tegen de opslag van persoonsge-

13 Zie bijvoorbeeld: EHRM, *Klass e.a./Duitsland*, nr. 5029/71, 6 september 1978; EHRM, *Rotaru/Roemenië* [Grote kamer], nr. 28341/95, 4 mei 2000 en EHRM, *Szabó en Vissy/Hongarije*, nr. 37138/14, 12 januari 2016.

14 *Ibid.*

15 Raad van Europa, Europees Verdrag voor de rechten van de mens, CETS nr. 005, 1950.

16 Zie bijvoorbeeld: EHRM, *Malone/Verenigd Koninkrijk*, nr. 8691/79, 2 augustus 1984; EHRM, *Copland/Verenigd Koninkrijk*, nr. 62617/00, 3 april 2007, en EHRM, *Mustafa Sezgin Tanrıkulu/Turkije*, nr. 27473/06, 18 juli 2017.

17 Zie bijvoorbeeld: EHRM, *Klass e.a./Duitsland*, nr. 5029/71, 6 september 1978; EHRM, *Uzun/Duitsland*, nr. 35623/05, 2 september 2010.

gevens door overheidsautoriteiten[18]. Het recht op eerbiediging van het privéleven is geen absoluut recht daar waar de uitoefening van het recht op privacy zou kunnen leiden tot inbreuk op andere rechten, zoals de vrijheid van meningsuiting of de toegang tot informatie, en vice versa. Vandaar dat het Hof ernaar streeft een evenwicht te vinden tussen de verschillende rechten die in het geding zijn. Het EHRM heeft verduidelijkt dat artikel 8 van het EVRM staten niet alleen verplicht om zich te onthouden van elke handeling die mogelijk een inbreuk op dit verdragsrecht vormt, maar dat ze in bepaalde omstandigheden ook een positieve verplichting hebben om de effectieve eerbiediging van het privé-, familie- en gezinsleven actief te waarborgen[19]. Op veel van deze zaken zal in de desbetreffende hoofdstukken nader worden ingegaan.

1.1.4. Verdrag 108 van de Raad van Europa

Met de opkomst van de informatietechnologie in de jaren zestig van de vorige eeuw was er een toenemende behoefte aan gedetailleerdere regels om natuurlijke personen bescherming te bieden door hun persoonsgegevens te beschermen. Medio jaren zeventig nam het Comité van Ministers van de RvE een aantal resoluties over de bescherming van persoonsgegevens aan, onder verwijzing naar artikel 8 van het EVRM[20]. In 1981 werd een Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108)[21] ter ondertekening opengesteld. Verdrag 108 was, en is nog steeds, het enige internationale wettelijk bindende instrument op het gebied van gegevensbescherming.

Verdrag 108 is van toepassing op alle gegevensverwerking die wordt uitgevoerd door zowel de particuliere als de publieke sector, met inbegrip van gegevensverwerking door de rechterlijke macht en wetshandhavingsinstanties. Het beschermt natuurlijke personen tegen misbruik dat kan plaatsvinden bij de verwerking van persoonsgegevens en beoogt tegelijkertijd het grensoverschrijdend verkeer van

18 Zie bijvoorbeeld: EHRM, *Roman Zakharov/Rusland*, nr. 47143/06, 4 december 2015; EHRM, *Szabó en Vissy/Hongarije*, nr. 37138/14, 12 januari 2016.

19 Zie bijvoorbeeld: EHRM, *I./Finland*, nr. 20511/03, 17 juli 2008; EHRM, *K.U./Finland*, nr. 2872/02, 2 december 2008.

20 Raad van Europa, Comité van Ministers (1973), Resolutie (73) 22 inzake de bescherming van de persoonlijke levenssfeer bij geautomatiseerde registratiesystemen in de particuliere sector, 26 september 1973; Raad van Europa, Comité van Ministers (1974), Resolutie (74) 29 inzake de bescherming van de persoonlijke levenssfeer bij geautomatiseerde registratiesystemen in de publieke sector, 20 september 1974.

21 Raad van Europa, Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, CETS nr. 108, 1981.

persoonsgegevens te reguleren. Wat betreft de verwerking van persoonsgegevens hebben de beginselen die in het verdrag zijn vastgelegd met name betrekking op een eerlijke en rechtmatige verzameling en automatische verwerking van gegevens, voor duidelijk omschreven en gerechtvaardigde doeleinden. Dit betekent dat de gegevens niet mogen worden gebruikt om redenen die onverenigbaar zijn met deze doeleinden, en dat ze niet langer mogen worden bewaard dan noodzakelijk is. Ook hebben ze betrekking op de kwaliteit van de gegevens, die in het bijzonder toereikend, ter zake dienend, nauwkeurig en niet overmatig (onevenredig) dienen te zijn.

Behalve dat Verdrag 108 garanties biedt ten aanzien van de verwerking van persoonsgegevens en verplichtingen met betrekking tot gegevensbeveiliging, verbiedt het, bij ontstentenis van passende wettelijke waarborgen, de verwerking van "gevoelige" gegevens, zoals gegevens betreffende ras, politieke overtuiging, gezondheid, seksuele geaardheid, godsdienst of andere levensbeschouwing en strafrechtelijk verleden.

Ook is in het verdrag het recht vervat van een natuurlijke persoon om te weten welke informatie over hem of haar is opgeslagen en indien nodig om deze te laten corrigeren. Beperkingen van de in het verdrag vastgelegde rechten zijn alleen mogelijk wanneer hogere belangen, zoals de staatsveiligheid of defensie, in het geding zijn. Bovendien voorziet het verdrag in vrij verkeer van persoonsgegevens tussen de partijen bij het verdrag en legt het enkele beperkingen op aan stromen naar staten waarvan de wettelijke bepalingen geen gelijkwaardige bescherming bieden.

Opgemerkt moet worden dat Verdrag 108 bindend is voor staten die het hebben geratificeerd. Het is niet onderworpen aan het rechterlijk toezicht van het EHRM, maar is in zaken in de context van artikel 8 van het EVRM wel betrokken in de overwegingen van het EHRM. In de loop der jaren heeft het Hof geoordeeld dat de bescherming van persoonsgegevens een belangrijk onderdeel is van het recht op eerbiediging van het privéleven (artikel 8), en heeft het zich door de beginselen van Verdrag 108 laten leiden wanneer het moest besluiten of er wel of niet sprake was van inbreuk op dit fundamentele recht[22].

Om de in Verdrag 108 neergelegde algemene beginselen en voorschriften verder te ontwikkelen, heeft het Comité van Ministers van de RvE diverse niet wettelijk

22 Zie bijvoorbeeld: EHRM, *Z./Finland*, nr. 22009/93, 25 februari 1997.

bindende aanbevelingen vastgesteld. Deze aanbevelingen zijn van invloed geweest op de ontwikkeling van de gegevensbeschermingswetgeving in Europa. Zo was er in Europa jarenlang maar één instrument dat richtsnoeren bood voor het gebruik van persoonsgegevens in de politiesector, te weten de Politieaanbeveling[23]. De in deze aanbeveling opgenomen beginselen, zoals de wijze van bewaren van gegevensbestanden en de noodzaak duidelijke regels in te voeren met betrekking tot de personen die toegang tot deze bestanden wordt verleend, werden verder uitgewerkt en zijn in de latere EU-wetgeving terug te vinden[24]. Recentere aanbevelingen zijn gericht op de uitdagingen van het digitale tijdperk, bijvoorbeeld in verband met gegevensverwerking in het kader van de arbeidsverhouding (zie hoofdstuk 9).

Alle EU-lidstaten hebben Verdrag 108 geratificeerd. In 1999 zijn er wijzigingen op Verdrag 108 voorgesteld om de EU als partij te laten toetreden, maar deze zijn nooit in werking getreden[25]. In 2001 is een aanvullend protocol bij Verdrag 108 aangenomen. Dit introduceerde bepalingen inzake grensoverschrijdende gegevensstromen naar niet-verdragspartijen, zogeheten derde landen, en de verplichte oprichting van nationale toezichthoudende autoriteiten op het gebied van gegevensbescherming[26].

Verdrag 108 staat open voor toetreding door niet bij de RvE aangesloten staten. Het potentieel van het verdrag als universele norm dient, samen met het open karakter ervan, als basis voor het bevorderen van gegevensbescherming op mondiaal niveau. Op het moment van verschijnen van dit handboek zijn 51 landen partij bij het Verdrag 108. Dit betreft alle lidstaten van de Raad van Europa (47 landen); Uruguay, het eerste niet-Europese land, dat toetrad in augustus 2013, en Mauritius, Senegal en Tunesië, die zijn toegetreden in 2016 en 2017.

Het verdrag heeft recentelijk een Modernisation of Convention 108 (coe.int) ondergaan. In 2011 werd een openbare raadpleging gehouden die de twee belangrijkste

23 Raad van Europa, Comité van Ministers (1987), Aanbeveling Rec(87)15 aan de lidstaten tot regeling van het gebruik van persoonsgegevens op politieel gebied, Straatsburg, 17 september 1987.

24 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, PB L 281 van 23.11.1995.

25 Raad van Europa, wijzigingen in het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108), aangenomen door het Comité van Ministers op 15 juni 1999 in Straatsburg.

26 Raad van Europa, Aanvullend Protocol bij het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, betreffende toezichthoudende instanties en grensoverschrijdende gegevensstromen, CETS nr. 181, 2001. Met de modernisering van Verdrag 108 wordt dit protocol niet langer toegepast, aangezien de bepalingen ervan zijn bijgewerkt en geïntegreerd in het Gemoderniseerd Verdrag 108.

doelstellingen van deze exercitie bekrachtigde: het verbeteren van de bescherming van de privacy in de digitale ruimte en het versterken van de follow-upmechanismen van het verdrag. Het moderniseringsproces was voornamelijk gericht op deze doelstellingen en werd voltooid met de aanname van het Wijzigingsprotocol CETS nr. 223. De modernisering werd tegelijkertijd met andere hervormingen van internationale instrumenten voor gegevensbescherming uitgevoerd, en gebeurde parallel aan de hervorming van de EU-regels betreffende gegevensbescherming, waarmee in 2012 werd aangevangen. Toezichthouders bij de Raad van Europa en op EU-niveau hebben nauwlettend toegezien op de consistentie en compatibiliteit tussen de twee rechtskaders. Bij de modernisering is het algemene en flexibele karakter van het verdrag behouden. De gemoderniseerde versie bekrachtigt bovendien het potentieel van het verdrag als universeel instrument op het gebied van gegevensbeschermingswetgeving. Het verdrag bevestigt en bestendigt belangrijke beginselen en verleent natuurlijke personen nieuwe rechten, terwijl tegelijkertijd aan entiteiten die persoonsgegevens verwerken meer verantwoordelijkheden worden toegewezen en er een betere verantwoording wordt verzekerd. Zo hebben personen wier persoonsgegevens worden verwerkt, het recht informatie te verkrijgen over de redenering voor deze gegevensverwerking en het recht bezwaar te maken tegen de verwerking. Als antwoord op de toename van profilering in de onlinewereld bepaalt het verdrag tevens dat personen het recht hebben niet te worden onderworpen aan besluiten die louter worden genomen op grond van geautomatiseerde gegevensverwerking, zonder dat hun eigen zienswijze in aanmerking wordt genomen. Voor de praktische uitvoering van het verdrag wordt een doeltreffende handhaving van de gegevensbeschermingsregels door onafhankelijke toezichthoudende instanties in de verdragsluitende partijen essentieel geacht. Daartoe benadrukt het Gemoderniseerd Verdrag dat toezichthoudende instanties moeten worden uitgerust met effectieve bevoegdheden en taken, en hun missie in daadwerkelijke onafhankelijkheid moeten kunnen uitvoeren.

1.1.5. Gegevensbeschermingswetgeving van de Europese Unie

Het EU-recht bestaat uit primair en secundair EU-recht. Het Verdrag betreffende de Europese Unie (VEU) en het Verdrag betreffende de werking van de Europese Unie (VWEU) zijn door alle EU-lidstaten geratificeerd en vormen het "primaire EU-recht". De verordeningen, richtlijnen en besluiten van de EU zijn vastgesteld door de EU-instellingen waaraan deze bevoegdheid is toegekend door de Verdragen; ze zijn het "secundaire EU-recht".

Gegevensbescherming in het primaire EU-recht

In de oorspronkelijke Verdragen van de Europese Gemeenschappen wordt niet naar de rechten van de mens of de bescherming daarvan verwezen, aangezien de Europese Economische Gemeenschap in eerste instantie was bedoeld als een regionale organisatie die zich richtte op economische integratie en de invoering van een gemeenschappelijke markt. Eén van de grondbeginselen waarop de oprichting en ontwikkeling van de Europese Gemeenschappen zijn gestoeld, en die ook nu nog evenzeer van kracht is, is het beginsel van bevoegdheidstoedeling. Volgens dit beginsel handelt de EU alleen binnen de grenzen van de haar door de lidstaten verleende bevoegdheden, zoals beschreven in de EU-Verdragen. In tegenstelling tot de oprichtingsakten van de Raad van Europa, is in de EU-Verdragen geen uitdrukkelijke bevoegdheid op het gebied van grondrechten opgenomen.

Aangezien er echter zaken voor het HvJ-EU werden gebracht waarin mensenrechtenschendingen op gebieden die binnen het toepassingsgebied van het EU-recht vielen aan de kaak werden gesteld, is door het Hof een belangrijke uitlegging gegeven aan de Verdragen. Om natuurlijke personen te beschermen, heeft het HvJ-EU grondrechten tot één van de zogeheten algemene beginselen van het Europees recht gemaakt. Volgens het Hof weerspiegelen deze algemene beginselen de inhoud van de mensenrechtenbescherming die wordt geboden door nationale grondwetten en mensenrechtenverdragen, met name het EVRM. Het HvJ-EU verklaarde te zullen waarborgen dat deze beginselen in het EU-recht zouden worden nageleefd.

Erkennend dat haar beleid consequenties voor de mensenrechten kon hebben en in een poging de EU "dichter bij" de burgers te brengen, kondigde de EU in 2000 plechtig het Handvest van de grondrechten van de Europese Unie af. Doordat de grondwettelijke tradities en internationale verplichtingen die gemeenschappelijk voor de lidstaten zijn tot één geheel zijn gemaakt, omvat dit Handvest het hele scala aan politieke, economische, sociale en burgerrechten van Europese burgers. De rechten die in het Handvest worden beschreven, zijn onderverdeeld in zes titels: waardigheid, vrijheden, gelijkheid, solidariteit, burgerschap en rechtspleging.

Hoewel het Handvest aanvankelijk slechts een politiek document was, werd het wettelijk bindend[27] als primair EU-recht (zie artikel 6, lid 1, van het VEU) toen het

27 EU (2012), Handvest van de grondrechten van de Europese Unie, PB C 326 van 26.10.2012.

Verdrag van Lissabon op 1 december 2009 in werking trad[28]. De bepalingen van het Handvest zijn gericht tot de EU-instellingen en -organen, waarmee deze worden verplicht de hierin opgenomen rechten te eerbiedigen bij de vervulling van hun taken. De lidstaten zijn eveneens gebonden aan de bepalingen van het Handvest bij het uitvoeren van EU-wetgeving.

Het Handvest garandeert niet alleen de eerbiediging van het privé-, familie- en gezinsleven (artikel 7), maar ook het recht op bescherming van persoonsgegevens (artikel 8). Het Handvest verhoogt daardoor expliciet de status van deze bescherming naar het niveau van een grondrecht in het EU-recht. De EU-instellingen en -organen moeten dit recht, dat ook van toepassing is op de lidstaten wanneer deze het EU-recht ten uitvoer brengen (artikel 51 van het Handvest), in acht nemen en waarborgen. Artikel 8 van het Handvest, dat jaren na de goedkeuring van de richtlijn gegevensbescherming is geformuleerd, moet worden begrepen als de belichaming van daarvóór reeds bestaand EU-gegevensbeschermingsrecht. In het Handvest wordt daarom niet alleen in artikel 8, lid 1, uitdrukkelijk het recht op gegevensbescherming genoemd, maar worden in artikel 8, lid 2, ook de belangrijkste beginselen van gegevensbescherming vermeld. Tot slot vereist artikel 8, lid 3, van het Handvest dat een onafhankelijke autoriteit erop toeziet dat deze beginselen worden nageleefd.

De aanneming van het Verdrag van Lissabon vormt een mijlpaal in de ontwikkeling van de wetgeving op het gebied van gegevensbescherming, niet alleen omdat het Handvest hiermee de status van bindend rechtsdocument op het niveau van het primaire recht verkreeg, maar tevens omdat het Verdrag bepalingen bevat inzake het recht op bescherming van persoonsgegevens. Dit recht wordt uitdrukkelijk vastgesteld in artikel 16 van het VWEU, in het deel van het Verdrag waarin de algemene beginselen van de EU zijn uiteengezet. Artikel 16 creëert tevens een nieuwe rechtsgrond, door de EU de bevoegdheid toe te kennen wetgeving vast te stellen op het gebied van gegevensbescherming. Dit is een belangrijke ontwikkeling, omdat de EU-regels betreffende gegevensbescherming, in het bijzonder de gegevensbeschermingsrichtlijn, van oorsprong hun basis hadden in de rechtsgrond van de interne markt en de noodzaak de nationale wetgevingen nader tot elkaar te brengen, zodat het vrije verkeer van gegevens binnen de EU niet werd belemmerd. Artikel 16 van het VWEU biedt nu een zelfstandige rechtsgrond voor een moderne, alomvattende benadering van gegevensbescherming die van toepassing is in alle

28 Zie de geconsolideerde versies van het Verdrag betreffende de Europese Unie, PB C 326 van 26.10.2012, en het Verdrag betreffende de werking van de Europese Unie, PB C 326 van 26.10.2012.

kwesties die onder de bevoegdheid van de EU vallen, met inbegrip van politiële en justitiële samenwerking in strafzaken. Artikel 16 van het VWEU bekrachtigt daarnaast dat naleving van de gegevensbeschermingsregels die in het kader van het Verdrag worden aangenomen, onderworpen moet zijn aan toezicht door een onafhankelijke autoriteit. Artikel 16 heeft als rechtsgrondslag gediend bij het vaststellen van de grondige hervorming van de gegevensbeschermingsregels in 2016, d.w.z. de algemene verordening gegevensbescherming en de richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten (zie hieronder).

De algemene verordening gegevensbescherming

Van 1995 tot mei 2018 was het belangrijkste wettelijke instrument van de EU op het gebied van gegevensbescherming Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (richtlijn gegevensbescherming)[29]. Ze werd vastgesteld in 1995, in een periode waarin verschillende lidstaten reeds nationale wetgevingen inzake gegevensbescherming hadden vastgesteld[30], en ontstond uit de noodzaak om deze wetgevingen op elkaar af te stellen teneinde een hoog beschermingsniveau en het vrije verkeer van persoonsgegevens tussen de verschillende lidstaten te waarborgen. Voor het vrije verkeer van goederen, kapitaal, diensten en personen binnen de interne markt was vrij verkeer van gegevens nodig, dat niet gerealiseerd kon worden totdat de lidstaten konden vertrouwen op een uniform hoog niveau van gegevensbescherming.

In de richtlijn gegevensbescherming kwamen de beginselen van gegevensbescherming die reeds waren vervat in nationale wetgeving en in Verdrag 108 tot uitdrukking en werden deze dikwijls uitgebreid. De richtlijn maakte gebruik van de mogelijkheid die artikel 11 van Verdrag 108 biedt om beschermingsinstrumenten toe te voegen. Met name de invoering van onafhankelijk toezicht als instrument voor het verbeteren van de naleving van gegevensbeschermingsvoorschriften is een belangrijke bijdrage tot de doeltreffende werking van de Europese

29 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, PB L 281 van 23.11.1995.

30 De Duitse deelstaat Hessen nam in 1970 's werelds eerste wet voor gegevensbescherming aan. Deze was slechts van toepassing in de deelstaat. Zweden nam in 1973 de *Datalagen* aan, Duitsland de *Bundesdatenschutzgesetz* in 1976, en Frankrijk de *Loi relative à l'informatique, aux fichiers et aux libertés* in 1977. In het Verenigd Koninkrijk werd in 1984 de Data Protection Act aangenomen. Ten slotte werd in 1989 in Nederland de *Wet Persoonsregistraties* aangenomen.

gegevensbeschermingswetgeving gebleken. Bijgevolg werd dit kenmerk in 2001 overgenomen in het RvE-recht, in het Aanvullend Protocol bij Verdrag 108. Dit illustreert de nauwe wisselwerking en de onderlinge positieve invloed van de twee instrumenten in de loop der jaren.

Met de richtlijn gegevensbescherming werd een gedetailleerd en uitvoerig systeem voor gegevensbescherming in de EU ingesteld. Volgens het rechtssysteem van de EU zijn richtlijnen echter niet rechtstreeks toepasbaar en moeten zij eerst worden omgezet in het nationale recht van de lidstaten. De lidstaten beschikken hierbij onvermijdelijk over enige beoordelingsruimte. Hoewel met de richtlijn complete harmonisatie werd beoogd[31] (en een uitputtend niveau van bescherming), is ze in de praktijk in de lidstaten verschillend omgezet. Dit leidde ertoe dat binnen de EU uiteenlopende gegevensbeschermingswetten van kracht waren, waarbij definities en regels in de nationale wetgevingen verschillend waren geïnterpreteerd. Ook bestond er tussen de lidstaten verschil in de mate van handhaving en de ernst van sancties. Tot slot hadden er sinds de opstelling van de richtlijn in het midden van de jaren negentig van de vorige eeuw belangrijke veranderingen plaatsgevonden op het gebied van informatietechnologie. Deze redenen tezamen vormden aanleiding de gegevensbeschermingswetgeving van de EU te hervormen.

Na jaren intensief overleg resulteerde de hervorming in april 2016 in de aanneming van de algemene verordening gegevensbescherming (AVG). De besprekingen over de noodzaak de Europese gegevensbeschermingsregels te moderniseren begonnen in 2009, toen de Commissie een openbare raadpleging initieerde over het toekomstige rechtskader voor het fundamentele recht op de bescherming van persoonsgegevens. Het voorstel voor de verordening werd in januari 2012 door de Commissie gepubliceerd, waarmee een langdurig wetgevingsproces met onderhandelingen tussen het Europees Parlement en de Raad van de Europese Unie van start ging. De algemene verordening gegevensbescherming voorzag in een overgangsperiode van twee jaar na aanneming. Sinds 25 mei 2018 is ze volledig van toepassing en is de richtlijn gegevensbescherming ingetrokken.

Met de aanneming van de algemene verordening gegevensbescherming in 2016 is de wetgeving van de EU op het gebied van gegevensbescherming gemoderniseerd en passend gemaakt voor de bescherming van grondrechten in de context van de economische en maatschappelijke uitdagingen van het digitale tijdperk. In

31 HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 november 2011, punt 29.

de AVG zijn de kernbeginselen en rechten van betrokkenen, zoals voorzien in de richtlijn gegevensbescherming, behouden en uitgebreid. Daarnaast gelden voor organisaties nieuwe verplichtingen. Zij moeten standaard ingebouwde gegevensbescherming invoeren in systemen, onder bepaalde omstandigheden een functionaris voor gegevensbescherming aanstellen, het nieuwe recht op overdraagbaarheid van gegevens naleven en voldoen aan het verantwoordingsbeginsel. In het EU-recht zijn verordeningen rechtstreeks toepasselijk; zij hoeven niet eerst in nationale wetgeving te worden omgezet. De algemene verordening gegevensbescherming voorziet derhalve in een reeks gegevensbeschermingsvoorschriften die in de gehele EU gelijkelijk van toepassing zijn. Doordat overal in de EU dezelfde regels gelden wordt een omgeving met rechtszekerheid gecreëerd waarvan economische actoren en personen als "betrokkenen" voordelen kunnen ondervinden.

Hoewel de algemene verordening gegevensbescherming rechtstreeks toepasselijk is, wordt echter wel van de lidstaten verwacht dat zij de bestaande nationale wetgeving op het gebied van gegevensbescherming actualiseren om deze volledig op één lijn te brengen met de verordening en tegelijkertijd invulling te geven aan de ruimte voor specifieke bepalingen zoals bedoeld in overweging 10. De voornaamste voorschriften en beginselen van de verordening en de sterke rechten die daarin aan personen worden toegekend, vormen een groot deel van dit handboek. Zij worden in de volgende hoofdstukken behandeld. De verordening bevat gedetailleerde bepalingen betreffende het territoriaal toepassingsgebied. Zij is van toepassing op ondernemingen die gevestigd zijn in de EU, alsook op verwerkingsverantwoordelijken en verwerkers die niet in de EU zijn gevestigd maar goederen of diensten aanbieden aan betrokkenen in de EU of hun gedrag monitoren. Gezien het belangrijke aandeel van een aantal technologiebedrijven van buiten de Unie in de Europese markt van miljoenen EU-klanten, is het van belang dat deze organisaties onderworpen zijn aan de EU-wetgeving inzake gegevensbescherming, zodat de bescherming van personen kan worden gewaarborgd en een gelijk speelveld wordt gerealiseerd.

Gegevensbescherming bij de rechtshandhaving — Richtlijn (EU) 2016/680

De ingetrokken richtlijn gegevensbescherming voorzag in gedetailleerde regelgeving op het gebied van gegevensbescherming. Met de aanneming van de algemene verordening gegevensbescherming is deze regelgeving nu verder uitgebreid. De ingetrokken richtlijn bevatte weliswaar gedetailleerde voorschriften, maar het toepassingsgebied was beperkt tot activiteiten binnen de interne markt en activiteiten van niet bij wetshandhaving betrokken overheidsdiensten. Het was dan

ook noodzakelijk specifieke instrumenten vast te stellen waarmee de vereiste duidelijkheid en het benodigde evenwicht tussen gegevensbescherming en andere gerechtvaardigde belangen kon worden bereikt en uitdagingen die in het bijzonder een rol spelen in bepaalde sectoren, het hoofd kon worden geboden. Dit geldt bijvoorbeeld voor regels betreffende de verwerking van persoonsgegevens door wetshandhavingsinstanties.

Het eerste rechtsinstrument van de EU waarin regels op dit gebied werden vastgelegd, was Kaderbesluit 2008/977/JBZ van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken. De regels hadden echter slechts betrekking op politiële en justitiële gegevens die tussen lidstaten werden uitgewisseld. De binnenlandse verwerking van persoonsgegevens door rechtshandhavingsautoriteiten viel buiten het toepassingsgebied.

Deze situatie is verholpen in Richtlijn (EU) 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens[32], ook algemene richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten genoemd. Met deze richtlijn, die parallel aan de algemene verordening gegevensbescherming werd aangenomen, is het Kaderbesluit 2008/977/JBZ ingetrokken en is een alomvattend stelsel voor de bescherming van persoonsgegevens in het kader van de wetshandhaving vastgesteld, waarbij rekening is gehouden met de bijzonderheden van gegevensverwerking in verband met kwesties betreffende de openbare veiligheid. Waar de algemene verordening gegevensbescherming algemene regels vaststelt ter bescherming van natuurlijke personen op het gebied van de verwerking van persoonlijke gegevens en het vrije verkeer van die gegevens binnen de EU, zijn in deze richtlijn specifieke regels neergelegd voor gegevensbescherming in het kader van justitiële samenwerking in strafzaken en politiële samenwerking. Wanneer een bevoegde autoriteit persoonsgegevens verwerkt met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten, is Richtlijn (EU) 2016/680 van toepassing. Wanneer bevoegde autoriteiten persoonsgegevens

32 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens, PB L 119 van 4.5.2016.

verwerken voor andere doeleinden dan de hierboven genoemde, gelden de algemene regels van de algemene verordening gegevensbescherming. Anders dan bij de voorganger ervan (Kaderbesluit 2008/977/JBZ van de Raad) is Richtlijn (EU) 2016/680 ook van toepassing op de verwerking van persoonsgegevens door nationale wetshandhavingsinstanties en geldt zij niet slechts voor de uitwisseling van dergelijke gegevens tussen lidstaten. In de richtlijn is tevens beoogd een evenwicht te bereiken tussen de rechten van personen en de legitieme doeleinden bij het verwerken van gegevens in verband met veiligheidsoverwegingen.

De richtlijn bekrachtigt hiertoe het recht op bescherming van persoonsgegevens en de kernbeginselen waaraan de verwerking van gegevens moet voldoen, hierbij nauw aansluitend op de regels en principes zoals vervat in de algemene verordening gegevensbescherming. De rechten van personen en de aan verwerkingsverantwoordelijken gestelde verplichtingen, bijvoorbeeld op het gebied van gegevensbeveiliging, gegevensbescherming door ontwerp en standaardinstellingen, en melding van inbreuken op de veiligheid van persoonsgegevens, zijn vergelijkbaar met die in de algemene verordening gegevensbescherming. In de richtlijn is ook oog voor belangrijke nieuwe technologische uitdagingen die een bijzonder bezwarend effect kunnen hebben op personen, zoals het gebruik van profileringsmethoden door wetshandhavingsautoriteiten. In het algemeen moeten uitsluitend op geautomatiseerde verwerking gebaseerde besluiten, met inbegrip van profilering, worden verboden[33]. Beslissingen mogen ook niet worden gebaseerd op gevoelige gegevens. In de richtlijn zijn een aantal uitzonderingen opgenomen die gelden voor dergelijke beginselen. Bovendien mag de bedoelde gegevensverwerking niet leiden tot discriminatie van personen[34].

De richtlijn bevat tevens regels voor het waarborgen van de verantwoording van verwerkingsverantwoordelijken. Zij moeten een functionaris voor gegevensbescherming aanwijzen die toeziet op naleving van de gegevensbeschermingsvoorschriften, die de instantie en de werknemers die de verwerking uitvoeren, informeert en adviseert over hun verplichtingen, en die samenwerkt met de toezichthoudende autoriteit. De verwerking van persoonsgegevens door politiële en strafrechtelijke autoriteiten is nu onderworpen aan het toezicht van onafhankelijke toezichthoudende instanties. Zowel de algemene gegevensbeschermingswetgeving als de specifieke voorschriften voor wetshandhaving en strafzaken moeten in

33 Richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten, artikel 11, lid 1.

34 *Ibid.*, artikel 11, leden 2 en 3.

overeenstemming zijn met de in het Handvest voor de grondrechten van de Europese Unie vastgelegde bepalingen.

De speciale voorschriften voor gegevensverwerking in het kader van politiële en justitiële samenwerking, zoals vastgesteld bij de richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten, worden in meer detail beschreven in hoofdstuk 8.

Richtlijn betreffende privacy en elektronische communicatie

Ook in de sector elektronische communicatie werd het noodzakelijk geacht aparte gegevensbeschermingsregels vast te stellen. Gezien de ontwikkeling van internet, telefonie via vaste lijnen en mobieletelefonienetwerken was het van belang het recht van gebruikers op privacy en vertrouwelijkheid veilig te stellen. Richtlijn 2002/58/EG[35] betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie of e-Privacy-richtlijn) bevat voorschriften in verband met de veiligheid van persoonsgegevens in deze netwerken, de melding van inbreuken op de veiligheid van persoonsgegevens en het vertrouwelijke karakter van de communicatie.

Wat veiligheid betreft moeten aanbieders van elektronische communicatiediensten onder meer garanderen dat slechts bevoegde personen toegang hebben tot persoonsgegevens en zij moeten maatregelen nemen om te voorkomen dat persoonsgegevens worden vernietigd, kwijtgeraakt of per ongeluk worden beschadigd[36]. Wanneer er een specifiek risico bestaat op inbreuk op de veiligheid van het openbare communicatienetwerk, moeten exploitanten de abonnees over dit risico informeren[37]. Als ondanks de toegepaste veiligheidsmaatregelen toch een inbreuk op de veiligheid plaatsvindt, moeten aanbieders de bevoegde nationale autoriteit die met de invoering en handhaving van de richtlijn is belast, van de inbreuk in kennis stellen. Soms moeten aanbieders inbreuken op de beveiliging van persoonsgegevens ook melden aan personen, namelijk wanneer de persoonsgegevens of de privacy

35 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie of e-Privacy-richtlijn), PB L 201.

36 Richtlijn betreffende privacy en elektronische communicatie, artikel 4, lid 1.

37 *Ibid.*, artikel 4, lid 2.

van deze personen door de inbreuk waarschijnlijk negatief worden beïnvloed[38]. Gezien het vertrouwelijke karakter van communicatieverkeer dient afluisteren, aftappen, opslaan of anderszins controleren of onderscheppen van de communicatie en metagegevens in beginsel verboden te zijn. De richtlijn verbiedt tevens ongevraagde communicatie (vaak aangeduid als "spam"), tenzij gebruikers daarvoor toestemming hebben gegeven, en bevat voorschriften voor de plaatsing van "cookies" op computers en andere apparaten. Deze negatieve kernverplichtingen geven duidelijk aan dat er een belangrijk verband is tussen het vertrouwelijke karakter van communicatieverkeer en de bescherming van het recht op eerbiediging van het privéleven zoals vervat in artikel 7 van het Handvest en het recht op bescherming van persoonsgegevens zoals vervat in artikel 8 van het Handvest.

In januari 2017 heeft de Commissie een voorstel voor een verordening met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie gepubliceerd, die is bedoeld ter vervanging van de e-Privacy-richtlijn. Met de hervorming wordt beoogd de voorschriften voor elektronische communicatie op één lijn te brengen met de nieuwe regelgeving zoals die is vastgesteld in de algemene verordening gegevensbescherming. De nieuwe verordening zal rechtstreeks van toepassing zijn in de hele EU. Voor de elektronische communicatie van alle natuurlijke personen geldt hetzelfde beschermingsniveau, terwijl telecommunicatieaanbieders en bedrijven voordeel zullen ondervinden van de duidelijkheid, rechtszekerheid en het feit dat overal in de EU dezelfde verzameling regels van toepassing is. De voorgestelde regels met betrekking tot het vertrouwelijke karakter van elektronische communicatie zullen ook gelden voor nieuwe spelers die elektronische communicatiediensten aanbieden die niet onder de e-Privacy-richtlijn vallen. Deze laatste betreft enkel de traditionele aanbieders van telecommunicatiediensten. Gezien de enorme toename van het gebruik van diensten zoals Skype, WhatsApp, Facebook Messenger en Viber voor het verzenden van berichten en het voeren van telefoongesprekken, zullen deze over-the-top-diensten (OTT-diensten) worden inbegrepen in het toepassingsgebied van de nieuwe verordening, en zullen ze moeten voldoen aan de vereisten die hierin worden gesteld op het gebied van gegevensbescherming, privacy en veiligheid. Ten tijde van de publicatie van dit handboek was het wetgevingsproces in verband met de e-Privacy-richtlijn nog gaande.

38 *Ibid.*, artikel 4, lid 3.

Verordening (EG) nr. 45/2001

Omdat de richtlijn gegevensbescherming alleen van toepassing kon zijn op EU-lidstaten, was een aanvullend rechtsinstrument nodig om gegevensbescherming in verband met de verwerking van persoonsgegevens door instellingen en organen van de EU te reguleren. Verordening (EG) nr. 45/2001 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (verordening gegevensbescherming EU-instellingen) vervult deze taak[39].

In Verordening (EG) nr. 45/2001 worden de beginselen van de algemene EU-wetgeving op het gebied van gegevensbescherming nauw gevolgd en worden deze toegepast op de verwerking van gegevens door EU-instellingen en -organen bij de uitoefening van hun taken. Daarnaast stelt de verordening een onafhankelijke toezichthoudende autoriteit in, de Europese Toezichthouder voor gegevensbescherming (EDPS), die toezicht houdt op de toepassing van de in de verordening opgenomen bepalingen. De EDPS heeft de bevoegdheid toezicht uit te oefenen en de taak de verwerking van persoonsgegevens binnen EU-instellingen en -organen te controleren, en klachten betreffende vermeende inbreuken op de gegevensbeschermingswetgeving aan te horen en te onderzoeken. Hij verstrekt EU-instellingen en -organen advies over alle zaken die verband houden met de bescherming van persoonsgegevens, variërend van voorstellen voor nieuwe wetgeving tot het opstellen van interne regels met betrekking tot gegevensverwerking.

In januari 2017 heeft de Europese Commissie een voorstel voor een nieuwe verordening betreffende de gegevensverwerking door EU-instellingen gepresenteerd, waarbij de huidige verordening zal worden ingetrokken. Evenals bij de hervorming van de e-Privacy-richtlijn zullen bij de hervorming van Verordening (EG) nr. 45/2001 de daarin opgenomen voorschriften worden gemoderniseerd en op één lijn gebracht met de nieuwe gegevensbeschermingsregels zoals vastgesteld in de algemene verordening gegevensbescherming.

39 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, PB L 8 van 12.1.2001.

De rol van het HvJ-EU

Het HvJ-EU is bevoegd te bepalen of een lidstaat al dan niet heeft voldaan aan zijn verplichtingen volgens het gegevensbeschermingsrecht van de EU, en de EU-wetgeving te duiden teneinde een doelmatige en eenduidige toepassing ervan in alle lidstaten te waarborgen. Sinds de aanneming van de richtlijn gegevensbescherming in 1995 is een aanzienlijke jurisprudentie opgebouwd, waarin het toepassingsgebied en de betekenis van de gegevensbeschermingsbeginselen, en het fundamentele recht op bescherming van persoonsgegevens zoals vervat in artikel 8 van het Handvest, worden verduidelijkt. Hoewel deze richtlijn inmiddels is ingetrokken en er een nieuw rechtsinstrument van kracht is (de algemene verordening gegevensbescherming), blijft de bestaande jurisprudentie relevant en geldig voor de uitlegging en toepassing van de gegevensbeschermingsbeginselen van de EU, voor zover het de kernbeginselen en -concepten van de richtlijn gegevensbescherming betreft die in de AVG zijn behouden.

1.2. Beperkingen van het recht op bescherming van persoonsgegevens

Belangrijkste punten

- Het recht op bescherming van persoonsgegevens is niet absoluut. Het kan worden beperkt indien dat noodzakelijk is voor een doel van algemeen belang of ter bescherming van de rechten en vrijheden van anderen.
- De voorwaarden voor het beperken van het recht op eerbiediging van het privéleven en op de bescherming van persoonsgegevens worden genoemd in artikel 8 van het EVRM en artikel 52, lid 1, van het Handvest. Zij zijn verder ontwikkeld en geïnterpreteerd in de jurisprudentie van het EHRM en het HvJ-EU.
- Volgens het RvE-recht inzake gegevensbescherming vormt de verwerking van persoonsgegevens slechts dan een rechtmatige inmenging in het recht op eerbiediging van het privéleven en kan uitsluitend worden uitgevoerd wanneer deze:
  - overeenkomstig de wet plaatsvindt;
  - een rechtmatig doel dient;
  - de wezenlijke inhoud van de grondrechten en fundamentele vrijheden eerbiedigt;
  - in een democratische samenleving noodzakelijk en evenredig is voor de verwezenlijking van een rechtmatig doel.

- De rechtsorde van de EU stelt vergelijkbare voorwaarden aan beperkingen van de uitoefening van in het Handvest erkende grondrechten. Beperkingen van een grondrecht, met inbegrip van de bescherming van persoonsgegevens, kunnen slechts dan rechtmatig zijn wanneer zij:
  - overeenkomstig de wet plaatsvinden;
  - de wezenlijke inhoud van dat recht eerbiedigen;
  - noodzakelijk zijn, met inachtneming van het evenredigheidsbeginsel, en
  - beantwoorden aan door de EU erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten van anderen.

Het grondrecht van bescherming van persoonsgegevens uit hoofde van artikel 8 van het Handvest is geen absoluut recht, "maar moet in relatie tot de functie ervan in de maatschappij worden beschouwd"[40]. Artikel 52, lid 1, van het Handvest erkent zo dat de uitvoering van rechten kan worden beperkt, zoals uiteengezet in de artikelen 7 en 8 van het Handvest, voor zover deze beperkingen zijn vastgesteld bij wet, de wezenlijke inhoud van de rechten en vrijheden geëerbiedigd wordt en de beperkingen overeenkomstig het evenredigheidsbeginsel noodzakelijk zijn en daadwerkelijk de door de Unie erkende doelstellingen van algemeen belang dienen of beantwoorden aan de noodzaak tot bescherming van rechten en vrijheden van anderen[41]. Op vergelijkbare wijze wordt in het EVRM-stelsel gegevensbescherming gegarandeerd door artikel 8, en uitoefening van dit recht kan worden beperkt indien dit noodzakelijk is voor de verwezenlijking van een rechtmatig doel. In deze paragraaf worden de voorwaarden voor inmenging als bedoeld in het EVRM en als uitgelegd in de jurisprudentie van het EHRM, en de voorwaarden voor wettelijke beperkingen in artikel 52 van het Handvest bekeken.

1.2.1. Vereisten voor gerechtvaardigde inmenging als bedoeld in het EVRM

De verwerking van persoonsgegevens kan een inmenging in het recht op eerbiediging van het privéleven van de betrokkene vormen, zoals die wordt beschermd

40 Zie bijvoorbeeld HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert/Land Hessen* [Grote kamer], 9 november 2010, punt 48.

41 *Ibid.*, punt 50.

krachtens artikel 8 van het EVRM[42]. Zoals hierboven uiteengezet (zie punt 1.1.1 en punt 1.1.4) en in tegenstelling tot de rechtsorde van de Unie bevestigt het EVRM de bescherming van persoonsgegevens niet als een afzonderlijk grondrecht. Of preciezer gezegd: de bescherming van persoonsgegevens behoort tot de rechten die worden beschermd onder het recht op eerbiediging van het privéleven. Niet elke verrichting waarbij persoonsgegevens worden verwerkt valt dan ook onder de werkingssfeer van artikel 8 van het EVRM. Artikel 8 is slechts dan van toepassing wanneer kan worden vastgesteld dat er sprake is van inbreuk op een particulier belang of iemands privéleven. Het EHRM heeft in zijn jurisprudentie het begrip "privéleven" breed geïnterpreteerd en zelfs aspecten van het beroepsleven en openbaar gedrag hier onder begrepen. Het EHRM heeft tevens geoordeeld dat de bescherming van persoonsgegevens een belangrijk onderdeel vormt van het recht op eerbiediging van het privéleven. Ondanks de brede interpretatie van het begrip privéleven vertegenwoordigen niet alle vormen van gegevensverwerking automatisch een inbreuk op de krachtens artikel 8 beschermde rechten.

Wanneer het EHRM van oordeel is dat de verwerkingshandeling het recht van de desbetreffende persoon op eerbiediging van het privéleven schaadt, onderzoekt het of de inmenging is gerechtvaardigd. Het recht op eerbiediging van het privéleven is geen absoluut recht, maar moet worden afgewogen tegen en worden verzoend met andere gerechtvaardigde belangen en rechten, hetzij van andere personen (particuliere belangen), hetzij van de samenleving als geheel (algemene belangen).

De cumulatieve voorwaarden waaronder inmenging zou kunnen worden gerechtvaardigd zijn:

In overeenstemming met de wet

Volgens de jurisprudentie van het EHRM is inmenging in overeenstemming met de wet indien deze is gebaseerd op een nationale wettelijke bepaling die bepaalde eigenschappen moet hebben. De wet "moet toegankelijk zijn voor de betrokkene en qua gevolgen voorzienbaar zijn"[43]. Een voorschrift is voorzienbaar indien het "voldoende nauwkeurig is om iedere persoon — zo nodig met deskundig advies — in

42 EHRM, *S. en Marper/Verenigd Koninkrijk* [Grote kamer], nr. 30562/04 en 30566/04, 4 december 2008, punt 67.

43 EHRM, *Amann/Zwitserland* [Grote kamer], nr. 27798/95, 16 februari 2000, punt 50; zie ook EHRM, *Kopp/Zwitserland*, nr. 23224/94, 25 maart 1998, punt 55 en EHRM, *Iordachi e.a./Moldavië*, nr. 25198/02, 10 februari 2009, punt 50.

staat te stellen zijn gedrag daarop af te stemmen"[44]. Bovendien zal "[de] vereiste mate van nauwkeurigheid van de wet in dit verband afhankelijk zijn van het specifieke onderwerp"[45].

Voorbeelden: In de zaak *Rotaru/Roemenië*[46] voerde de verzoeker aan dat zijn recht op eerbiediging van zijn privéleven was geschonden door de opslag en het gebruik van een bestand met zijn persoonlijke gegevens door de Roemeense inlichtingendienst. Het EHRM oordeelde dat de nationale wet weliswaar toestond informatie die van belang was voor de nationale veiligheid te verzamelen, vast te leggen en in geheime dossiers op te slaan, maar dat geen beperkingen aan de uitoefening van deze bevoegdheden werden gesteld en dit derhalve aan de autoriteiten werd overgelaten. Zo werd in de nationale wet geen definitie gegeven van het type informatie dat mocht worden verwerkt, de categorieën van personen tegen wie surveillancemaatregelen konden worden genomen, de omstandigheden waarin dergelijke maatregelen konden worden genomen en de te volgen procedure. Het Hof concludeerde derhalve dat het nationale recht niet voldeed aan de eisen van voorzienbaarheid als bedoeld in artikel 8 van het EVRM en dat het artikel was geschonden.

In *Taylor-Sabori/Verenigd Koninkrijk*[47] was de verzoeker het doelwit van surveillance door de politie. Door gebruik te maken van een "kloon" van de pieper van de verzoeker had de politie aan hem verzonden berichten weten te onderscheppen. Vervolgens werd de verzoeker aangehouden en samenzwering met het oogmerk om een gecontroleerde drug te leveren ten laste gelegd. De zaak van de openbaar aanklager was deels gebaseerd op de transcripties van de verstuurde berichten die de politie had gemaakt. Ten tijde van de rechtszaak tegen de verzoeker bevatte het Britse recht

44 EHRM, *Amann/Zwitserland* [Grote kamer], nr. 27798/95, 16 februari 2000, punt 56; zie ook EHRM, *Malone/Verenigd Koninkrijk*, nr. 8691/79, 2 augustus 1984, punt 66; EHRM, *Silver e.a./Verenigd Koninkrijk*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 maart 1983, punt 88.

45 EHRM, *The Sunday Times/Verenigd Koninkrijk*, nr. 6538/74, 26 april 1979, punt 49; zie ook EHRM, *Silver e.a./Verenigd Koninkrijk*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 maart 1983, punt 88.

46 EHRM, *Rotaru/Roemenië* [Grote kamer], nr. 28341/95, 4 mei 2000, punt 57; zie ook EHRM, *Association for European Integration and Human Rights en Ekimdzhiev/Bulgarije*, nr. 62540/00, 28 juni 2007, EHRM, *Shimovolos/Rusland*, nr. 30194/09, 21 juni 2011, en EHRM, *Vetter/Frankrijk*, nr. 59842/00, 31 mei 2005.

47 EHRM, *Taylor-Sabori/Verenigd Koninkrijk*, nr. 47114/99, 22 oktober 2002.

echter geen bepaling inzake de onderschepping van via een particulier telecommunicatiesysteem verzonden berichten. De inmenging in zijn rechten was daarom niet "in overeenstemming met de wet" geweest. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

In *Vukota-Bojić/Zwitserland*[48] was sprake van geheime surveillance van een ontvangster van sociale uitkeringen door privédetectives in opdracht van haar verzekeringsmaatschappij. Het EHRM verklaarde dat, hoewel een particuliere verzekeringsmaatschappij opdracht had gegeven tot de surveillancemaatregel in kwestie, deze maatschappij door de staat het recht was toegekend om uitkeringen te verstrekken uit hoofde van een verplichte ziektekostenverzekering en om verzekeringspremies te innen. Een staat kan zich niet van zijn verantwoordelijkheid krachtens het Verdrag ontheffen door zijn verplichtingen te delegeren aan particuliere lichamen of individuen. Het nationale recht moest voldoende waarborgen bieden tegen misbruik, wilde inmenging in rechten volgens artikel 8 van het EVRM "in overeenstemming met de wet" zijn. In het onderhavige geval concludeerde het EHRM dat artikel 8 van het EVRM was geschonden omdat in het nationale recht onvoldoende duidelijk was aangegeven in welke omstandigheden en op welke wijze verzekeringsmaatschappijen die in verzekeringsgeschillen optraden namens openbare instanties, bij de uitoefening van de hun toegekende discretionaire bevoegdheden in het geheim surveillance van een verzekerde mochten uitvoeren. Er waren, in het bijzonder, onvoldoende waarborgen opgenomen tegen misbruik.

Een rechtmatig doel dienen

Het rechtmatige doel kan ofwel één van de genoemde algemene belangen zijn, ofwel bescherming van de rechten en vrijheden van anderen. Inmenging zou volgens artikel 8, lid 2, van het EVRM gerechtvaardigd kunnen zijn wanneer zij geschiedt in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

48 EHRM, *Vukota-Bojić/Zwitserland*, nr. 61838/10, 18 oktober 2016, punt 77.

Voorbeeld: In *Peck/Verenigd Koninkrijk*[49] had de verzoeker geprobeerd zelfmoord te plegen door op straat zijn polsen door te snijden, zich er niet van bewust dat hij werd gefilmd door een bewakingscamera. De politie, die op de bewakingscamera meekeek, redde hem en droeg nadien het beeldmateriaal over aan de media, die het materiaal publiceerden zonder het gezicht van de verzoeker onherkenbaar te maken. Het EHRM oordeelde dat er geen toepasselijke of voldoende redenen waren voor de directe bekendmaking van het beeldmateriaal door de autoriteiten aan het publiek zonder eerst toestemming van de verzoeker te hebben verkregen of zijn identiteit te verhullen. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Noodzakelijk in een democratische samenleving

Het EHRM heeft bepaald dat "het begrip noodzakelijkheid [...] erop [duidt] dat de inmenging haar grond moet vinden in een dwingende maatschappelijke behoefte en in het bijzonder evenredig moet zijn aan het nagestreefde wettige doel"[50]. Wanneer het EHRM nagaat of een maatregel noodzakelijk is om in een nijpende sociale behoefte te voorzien, onderzoekt het de relevantie en geschiktheid ervan met betrekking tot het nagestreefde doel. Met het oog hierop kan het Hof in zijn overwegingen betrekken of met de inmenging wordt getracht een kwestie op te lossen die, als niet wordt ingegrepen, nadelige gevolgen zou kunnen hebben voor de maatschappij, of kan worden aangetoond dat de inmenging dergelijke nadelige gevolgen kan beperken, en hoe in de samenleving in het algemeen wordt geoordeeld over de desbetreffende kwestie[51]. Het verzamelen en bewaren door inlichtingendiensten van persoonsgegevens van bepaalde personen van wie is gebleken dat zij banden hebben met terroristische bewegingen, zou een inmenging inhouden in het recht van personen op eerbiediging van het privéleven, maar tegelijkertijd een dwingende maatschappelijke behoefte dienen, te weten bescherming van de nationale veiligheid en bestrijding van terrorisme. De inmenging moet bovendien evenredig zijn om te kunnen voldoen aan het vereiste van noodzakelijkheid. In de rechtspraak van het EHRM wordt evenredigheid benaderd binnen het kader van noodzakelijkheid. Het evenredigheidsbeginsel vereist dat een inmenging in de uit

49 EHRM, *Peck/Verenigd Koninkrijk*, nr. 44647/98, 28 januari 2003, punt 85.

50 EHRM, *Leander/Zweden*, nr. 9248/81, 26 maart 1987, punt 58.

51 Groep gegevensbescherming artikel 29 (Groep artikel 29) (2014), *Advies over de toepassing van de begrippen noodzakelijkheid en evenredigheid en over gegevensbescherming in de rechtshandhavingssector*, WP 211, Brussel, 27 februari 2014, blz. 7-8.

hoofde van het EVRM beschermde rechten niet verder gaat dan wat noodzakelijk is voor het bereiken van het rechtmatige doel. Bij de evenredigheidstoetsing dienen de volgende belangrijke factoren in aanmerking te worden genomen: de omvang van de inmenging, in het bijzonder het aantal getroffen personen, en de waarborgen of voorbehouden waarin is voorzien ter beperking van de omvang of de schadelijke gevolgen voor de rechten van personen[52].

Voorbeeld: In *Khelili/Zwitserland*[53] had de politie tijdens een controle bij de verzoekster visitekaartjes aangetroffen met de volgende tekst: "Aardige, mooie vrouw, achterin de dertig, wil een man leren kennen om soms mee uit te gaan en iets te drinken. Tel.: [...]". De verzoekster voerde aan dat de politie na deze ontdekking haar naam in de politieregisters had ingevoerd als prostituee, welk beroep zij consistent ontkende uit te oefenen. De verzoekster verzocht dat het woord "prostituee" werd verwijderd uit de geautomatiseerde registers van de politie. Het EHRM erkende in beginsel dat het bewaren van de persoonsgegevens van een natuurlijke persoon, op grond van het vermoeden dat hij of zij mogelijk opnieuw een strafbaar feit zou gaan plegen, in bepaalde omstandigheden evenredig kan zijn. In het geval van verzoekster leek het vermoeden van illegale prostitutie echter te vaag en te algemeen en werd dit vermoeden niet ondersteund door concrete feiten, aangezien zij nooit was veroordeeld voor illegale prostitutie, en was er derhalve geen "dwingende maatschappelijke behoefte" in de zin van artikel 8 van het EVRM. Het Hof was van mening dat het aan de autoriteiten was om de juistheid van de opgeslagen gegevens van verzoekster te bewijzen en oordeelde, ook gezien de ernst van de inmenging in de rechten van verzoekster, dat jarenlange bewaring van het woord "prostituee" in de politieregisters niet noodzakelijk was in een democratische samenleving. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Voorbeeld: In *S. en Marper/Verenigd Koninkrijk*[54] waren beide verzoekers gearresteerd en waren hun strafbare feiten ten laste gelegd. De politie nam vingerafdrukken en DNA-monsters af op basis van de Police and Criminal Evidence Act. De aanvragers werden nooit veroordeeld voor de strafbare feiten: een van hen werd door de rechtbank vrijgesproken en

52 *Ibid.*,blz. 9-11.

53 EHRM, *Khelili/Zwitserland*, nr. 16188/07, 18 oktober 2011.

54 EHRM, *S. en Marper/Verenigd Koninkrijk* [Grote kamer], nr. 30562/04 en 30566/04, 4 december 2008.

de strafvervolging van de ander werd beëindigd. Hun vingerafdrukken, DNA-profielen en celmonsters werden niettemin door de politie behouden en in een database opgeslagen, en de nationale wetgeving stond toe dat dergelijke gegevens voor onbepaalde tijd werden bewaard. Het Verenigd Koninkrijk voerde aan dat de bewaring bijdroeg aan de identificatie van toekomstige overtreders en derhalve het rechtmatige doel van misdaadpreventie en opsporing diende. Het EHRM oordeelde echter dat hier sprake was van ongerechtvaardigde inmenging in het recht op eerbiediging van het privéleven. Het Hof herinnerde eraan dat de kernbeginselen van gegevensbescherming vereisen dat de bewaring van persoonsgegevens in evenredigheid met het doel van de vergaring gebeurt en dat gegevens slechts gedurende een beperkte periode worden bewaard. Het Hof erkende dat de opname in de database van DNA-profielen van niet enkel veroordeelde personen, maar tevens van iedereen die was verdacht maar niet veroordeeld, mogelijk had bijgedragen tot de opsporing en voorkoming van criminaliteit in het Verenigd Koninkrijk. Het was echter "getroffen door de algemene en niet selectieve aard van de bevoegdheden tot opslag"[55].

Gezien de grote hoeveelheid genetische en gezondheidsinformatie in de celmonsters werd de inmenging in het recht op het privéleven van de verzoekers bijzonder inbreukmakend bevonden. Vingerafdrukken en monsters konden bij arrestanten worden afgenomen en voor onbepaalde tijd worden bewaard in de politiedatabase, ongeacht de aard of ernst van het strafbare feit, en zelfs in het geval van lichtere overtredingen waarop geen gevangenisstraf staat. Personen die waren vrijgesproken hadden bovendien maar beperkte mogelijkheden om hun gegevens uit de database te laten verwijderen. Ten slotte schonk het EHRM speciale aandacht aan het feit dat een van de verzoekers op het moment van arrestatie elf jaar oud was. Het bewaren van persoonsgegevens van een minderjarige die niet is veroordeeld, kan extra nadelig zijn gezien diens kwetsbaarheid en het belang van zijn ontwikkeling en integratie in de samenleving[56]. Het Hof oordeelde unaniem dat de bewaring een onevenredige inbreuk was op het recht op privéleven, die niet kon worden beschouwd als noodzakelijk in een democratische samenleving.

55 *Ibid.*, punt 119.

56 *Ibid.*, punt 124.

Voorbeeld: In *Leander/Zweden*[57] oordeelde het EHRM dat het in het geheim controleren van personen die solliciteren naar een functie die van belang is voor de nationale veiligheid op zichzelf niet in strijd was met de eis dat dit noodzakelijk moest zijn in een democratische samenleving. De bijzondere waarborgen in het nationale recht die de belangen van de betrokkene moesten beschermen — zoals door het nationale parlement of de minister van Justitie uitgevoerde controles — leidden tot de conclusie van het EHRM dat het Zweedse systeem om personeel te controleren voldeed aan de eisen van artikel 8, lid 2, van het EVRM. Gelet op de ruime beoordelingsmarge die hem ter beschikking stond, had de Zweedse staat het recht om in de zaak van de verzoekster het nationale belang te laten prevaleren boven de individuele belangen. Het Hof concludeerde dat artikel 8 van het EVRM niet was geschonden.

1.2.2. Voorwaarden voor rechtmatige beperkingen volgens het EU-Handvest van de grondrechten

De structuur en de bewoording van het Handvest wijken af van die van het EVRM. In het Handvest wordt niet gesproken van inmenging in gegarandeerde rechten, maar wel bevat het een bepaling inzake beperking(en) op de uitoefening van de in het Handvest erkende rechten en vrijheden.

Volgens artikel 52, lid 1, zijn beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden, en dientengevolge op het recht op persoonsgegevensbescherming alleen toegestaan indien deze:

- bij wet zijn gesteld, en
- het wezen van het recht op gegevensbescherming eerbiedigen, en
- met inachtneming van het evenredigheidsbeginsel noodzakelijk zijn[58], en
- beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

57 EHRM, *Leander/Zweden*, nr. 9248/81, 26 maart 1987, punten 59 en 67.

58 Zie voor de beoordeling van de noodzaak van maatregelen die het grondrecht op bescherming van persoonsgegevens beperken: EDPS (2017), *Necessity Toolkit*, Brussel, 11 april 2017.

Gezien het feit dat de bescherming van persoonsgegevens binnen de rechtsorde van de EU een afzonderlijk, op zichzelf staand grondrecht is dat is beschermd krachtens artikel 8 van het Handvest, is elke verwerking van persoonsgegevens op zichzelf al een inmenging waarmee dit recht wordt geschonden. Het is van geen belang of de persoonsgegevens in kwestie betrekking hebben op het privéleven van de persoon, van gevoelige aard zijn, of dat de betrokkenen op enige wijze hinder hebben ondervonden. De inmenging is alleen dan rechtmatig wanneer wordt voldaan aan alle voorwaarden die worden genoemd in artikel 52, lid 1, van het Handvest.

Bij wet zijn gesteld

Beperkingen van het recht op bescherming van persoonsgegevens moeten in wetgeving zijn voorzien. Dit vereiste houdt in dat beperkingen moeten zijn gestoeld op een wettelijke grond die voldoende toegankelijk en voorzienbaar is en die dusdanig nauwkeurig is geformuleerd dat personen begrijpen welke hun verplichtingen zijn en zij hun gedrag kunnen aanpassen. De rechtsgrondslag moet ook duidelijk de reikwijdte van de bevoegdheid van de aangewezen autoriteiten beschrijven en de wijze waarop de bevoegdheid moet worden uitgeoefend, om personen te beschermen tegen willekeurige inmenging. Deze interpretatie is vergelijkbaar met het vereiste van "rechtmatige inmenging" volgens de jurisprudentie van het EHRM[59], en er is gesuggereerd dat de betekenis van de in het Handvest gebruikte uitdrukking "bij wet zijn gesteld" hetzelfde zou moeten zijn als die welke eraan wordt gegeven in verband met het EVRM[60]. De rechtspraak van het EHRM, en met name het begrip "kwaliteit van de wet" dat het met de jaren heeft ontwikkeld, moet bij de uitlegging van artikel 52, lid 1, van het Handvest door het HvJ-EU in de overwegingen worden betrokken[61].

De wezenlijke inhoud van het recht eerbiedigen

Binnen de rechtsorde van de EU moet bij elke beperking van de uit hoofde van het Handvest beschermde grondrechten de wezenlijke inhoud van deze rechten worden geëerbiedigd. Dit betekent dat beperkingen die dusdanig omvangrijk en

59 EDPS (2017), *Necessity Toolkit*, Brussel, 11 april 2017, blz. 4; zie ook HvJ-EU, *Advies 1/15 van het Hof (Grote kamer)*, 26 juli 2017.

60 HvJ-EU, gevoegde zaken C-203/15 en C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen* en *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*, *Conclusie van advocaat-generaal Saugmandsgaard Øe* van 19 juli 2016, punt 140.

61 HvJ-EU, C-70/10, *Scarlet Extended SA/Société belge des auteurs compositeurs et éditeurs (SABAM)*, *Conclusie van advocaat-generaal Cruz Villalón* van 14 april 2011, punt 100.

inbreukmakend zijn dat een grondrecht van zijn wezenlijke inhoud wordt ontdaan, niet gerechtvaardigd zijn. Als het wezen van het recht geweld wordt aangedaan, moet de beperking als onwettig worden beschouwd, zonder dat verder hoeft te worden onderzocht of de beperking een doel van algemeen belang dient en voldoet aan de criteria voor noodzakelijkheid en evenredigheid.

Voorbeeld: De zaak *Schrems*[62] had betrekking op de bescherming van natuurlijke personen in verband met de doorgifte van hun persoonsgegevens naar een derde land, in dit geval de Verenigde Staten. Schrems, een Oostenrijks burger die al meerdere jaren gebruikmaakte van Facebook, diende een klacht in bij de Ierse toezichthouder voor gegevensbescherming en verzocht deze de doorgifte te veroordelen van zijn persoonlijke gegevens van de Ierse dochteronderneming van Facebook naar Facebook Inc. en diens servers die zich op het grondgebied van de Verenigde Staten bevonden, waar de gegevens werden verwerkt. Hij voerde aan dat, in het licht van de onthullingen in 2013 door de Amerikaanse klokkenluider Edward Snowden met betrekking tot de surveillanceactiviteiten van de inlichtingendiensten van de Verenigde Staten, het geldende recht en de praktijk in dat land geen afdoende bescherming boden van naar Amerikaans grondgebied doorgestuurde persoonsgegevens. Snowden had bekendgemaakt dat de National Security Agency rechtstreeks van de servers van bedrijven zoals Facebook gegevens aftapte en de inhoud van chatgesprekken en privéberichten kon lezen.

Bij de doorgifte van gegevens naar de VS werd uitgegaan van een in 2000 door de Commissie gegeven beschikking betreffende gepastheid, welke doorgifte toestond naar bedrijven in de VS die middels zelfcertificering verklaarden dat zij vanuit de EU doorgegeven persoonsgegevens zouden beschermen en dat zij de "veiligehavenbeginselen" zouden naleven. Toen de zaak voor het HvJ-EU werd gebracht, onderzocht het Hof de geldigheid van de beschikking van de Commissie in het licht van het Handvest. Het herinnerde eraan dat de EU-wetgeving ter bescherming van de grondrechten voorschrijft dat derogaties en beperkingen van die rechten alleen geldig zijn wanneer ze strikt noodzakelijk zijn. Het HvJ-EU oordeelde dat een regeling op grond waarvan autoriteiten algemeen toegang kunnen krijgen tot de inhoud van elektronische communicatie moest worden beschouwd als "een

62 HvJ-EU, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer], 6 oktober 2015.

aantasting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven zoals door artikel 7 van het Handvest gewaarborgd". Het recht zou elke gelding worden ontnomen indien overheden in de VS op aleatoire wijze toegang konden krijgen tot communicatieverkeer zonder dat hiervoor een objectieve rechtvaardiging hoefde te worden aangevoerd die berustte op concrete overwegingen van nationale veiligheid of misdaadpreventie die specifiek met de betrokken personen verband hielden, en zonder te worden omringd met passende waarborgen tegen misbruik van bevoegdheden.

Het Hof oordeelde bovendien dat "een regeling die niet in enige beroepsmogelijkheid voor de justitiabele voorziet om toegang tot de hem betreffende persoonsgegevens te verkrijgen, of rectificatie of verwijdering van die gegevens" strijdig is met het grondrecht op een effectieve voorziening in rechte (artikel 47 van het Handvest). De "veiligehavenbeschikking" kon dus niet waarborgen dat de VS een niveau van bescherming van de grondrechten bood dat in grote lijnen overeenkwam met het niveau dat binnen de Unie wordt gewaarborgd op grond van de richtlijn, gelezen in samenhang met het Handvest. Bijgevolg verklaarde het HvJ-EU de beschikking ongeldig[63].

Voorbeeld: In *Digital Rights Ireland*[64] onderzocht het HvJ-EU de verenigbaarheid van Richtlijn 2006/24/EG (richtlijn gegevensbewaring) met de artikelen 7 en 8 van het Handvest. De richtlijn verplichtte aanbieders van elektronische-communicatiediensten verkeers- en locatiegegevens gedurende ten minste zes maanden en ten hoogste twee jaar te bewaren, en bevoegde nationale autoriteiten toegang te bieden tot deze gegevens voor het voorkomen, onderzoeken, opsporen en vervolgen van ernstige criminaliteit. Bewaring van de inhoud van het elektronische communicatieverkeer was niet toegestaan. Het Hof merkte op dat de gegevens die exploitanten uit hoofde van de richtlijn moesten bewaren

63 Aan de beslissing van het HvJ-EU om Beschikking 2000/520/EG van de Commissie ongeldig te verklaren lagen nog andere overwegingen ten grondslag, welke in andere hoofdstukken van dit handboek nader zullen worden beschouwd. Het Hof oordeelde met name dat de beschikking de bevoegdheden van nationale toezichthoudende autoriteiten op het gebied van gegevensbescherming op onrechtmatige wijze beperkte. Bovendien waren er in het kader van de "veiligehavenregeling" geen rechtsmiddelen beschikbaar voor personen die toegang tot de hen betreffende gegevens wilden verkrijgen en/of rectificatie of verwijdering van die gegevens. De wezenlijke inhoud van het grondrecht op een effectieve voorziening in rechte, zoals neergelegd in artikel 47 van het Handvest, was derhalve ook aangetast.

64 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en Kärntner Landesregierung e.a. [Grote kamer], 8 april 2014.

ook gegevens omvatten die nodig waren om de bron en bestemming van een communicatie, de datum, het tijdstip en de duur van een communicatie, het oproepende en de opgeroepen nummers, en IP-adressen te traceren en te identificeren. "Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren."

De bewaring van persoonsgegevens in het kader van deze richtlijn vormde derhalve een bijzonder ernstige inbreuk op het recht op privacy en het recht op bescherming van persoonsgegevens. Het Hof was echter van oordeel dat geen inbreuk werd gemaakt op de wezenlijke inhoud van deze rechten. Wat het recht op privacy betreft, werd de inhoud niet aangetast omdat de richtlijn niet toestond kennis te verwerven over de inhoud van de elektronische communicatie als dusdanig. Evenmin werd het recht op bescherming van persoonsgegevens aangetast, aangezien de richtlijn van aanbieders van elektronische communicatie vereiste dat zij bepaalde beginselen van gegevensbescherming en gegevensveiligheid in acht namen en gepaste technische en organisatorische maatregelen hiertoe namen.

Noodzakelijkheid en evenredigheid

Artikel 52, lid 1, van het Handvest bepaalt dat, met inachtneming van het evenredigheidsbeginsel, beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden slechts kunnen worden gesteld indien deze noodzakelijk zijn.

Een beperking kan **noodzakelijk** zijn wanneer maatregelen moeten worden genomen in het kader van doelstellingen van algemeen belang, maar noodzakelijkheid, zoals uitgelegd door het HvJ-EU, impliceert tevens dat de genomen maatregelen minder ingrijpend zijn in vergelijking met alternatieve mogelijkheden om hetzelfde doel te bereiken. In het geval van de rechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens hanteert het HvJ-EU een strikte noodzakelijkheidstoets, en vereist het dat "derogaties […] en […] beperkingen […] binnen de grenzen van het strikt noodzakelijke blijven". Indien een beperking strikt noodzakelijk wordt geacht, moet tevens worden bepaald of ze evenredig is.

Er is sprake van **evenredigheid** wanneer de uit de beperking voortkomende voordelen groter zijn dan de nadelen waartoe de beperking leidt met betrekking tot de uitoefening van de desbetreffende grondrechten[65]. Het is van belang dat beperkingen vergezeld gaan van gepaste waarborgen om nadelen en risico's met betrekking tot het genot van het recht op privacy en gegevensbescherming te beperken.

Voorbeeld: In *Volker und Markus Schecke*[66] concludeerde het HvJ-EU dat de Raad en de Commissie, door het opleggen van een verplichting om persoonsgegevens van iedere natuurlijke persoon die de begunstigde was van steun uit bepaalde landbouwfondsen te publiceren, zonder dat daarbij een onderscheid werd gemaakt op basis van relevante criteria, zoals de tijdvakken waarin zij dergelijke steun hadden ontvangen, de frequentie, het type en de omvang van die steun, de door het evenredigheidsbeginsel gestelde grenzen hadden overschreden.

Om die reden achtte het HvJ-EU het noodzakelijk om bepaalde bepalingen van Verordening (EG) nr. 1290/2005 van de Raad, en Verordening (EG) nr. 259/2008 in haar geheel, nietig te verklaren[67].

Voorbeeld: In de zaak *Digital Rights Ireland*[68] oordeelde het HvJ-EU dat de uit de richtlijn gegevensbewaring voortvloeiende inbreuk op het recht op privacy het wezen van dat recht niet raakte, aangezien de richtlijn niet toestond dat de inhoud van elektronische communicatie werd bewaard. Het Hof concludeerde echter dat de richtlijn niet in overeenstemming was met de artikelen 7 en 8 van het Handvest en verklaarde de richtlijn ongeldig. Gezien het feit dat verkeers- en locatiegegevens, geaggregeerd en in hun geheel beschouwd, zouden kunnen worden geanalyseerd en een gedetailleerd beeld kunnen geven van het privéleven van personen, was hier sprake van een

65 EDPS (2017), *Necessity Toolkit*, blz. 5.

66 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert/Land Hessen* [Grote kamer], 9 november 2010, punten 89 en 86.

67 Verordening (EG) nr. 1290/2005 van de Raad van 21 juni 2005 betreffende de financiering van het gemeenschappelijk landbouwbeleid, PB L 209 van 11.8.2005; Verordening (EG) nr. 259/2008 van de Commissie van 18 maart 2008 tot vaststelling van uitvoeringsbepalingen van Verordening (EG) nr. 1290/2005 van de Raad met betrekking tot de bekendmaking van informatie over de begunstigden van financiële middelen uit het Europees Landbouwgarantiefonds (ELGF) en het Europees Landbouwfonds voor Plattelandsontwikkeling (ELFPO), PB L 76 van 19.3.2008.

68 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en Kärntner Landesregierung e.a., [Grote Kamer], 8 april 2014, punt 39.

ernstige inmenging in deze rechten. Het HvJ-EU nam in zijn overwegingen mee dat de richtlijn de bewaring vereiste van alle metagegevens met betrekking tot vaste telefonie, mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie, en van toepassing was op alle vormen van elektronische communicatie, waarvan in het dagelijks leven zeer veelvuldig gebruik wordt gemaakt. Het ging feitelijk om een inmenging die de gehele Europese bevolking raakte. Gezien de omvang en de ernst van deze inmenging kon de bewaring van verkeers- en locatiegegevens volgens het HvJ-EU enkel worden gerechtvaardigd wanneer dit gebeurde voor de bestrijding van zware criminaliteit. In de richtlijn ontbraken voorts objectieve criteria die waarborgden dat de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens beperkt zou blijven tot het strikt noodzakelijke. Bovendien bevatte ze geen materiële en procedurele voorwaarden betreffende de toegang tot en het gebruik van de bewaarde gegevens door nationale autoriteiten, en was hiervoor geen voorafgaande controle door een rechterlijke instantie of andere onafhankelijke instantie vereist.

Het Hof kwam tot een soortgelijke conclusie in de gevoegde zaken *Tele2 Sverige AB/Post- och telestyrelsen* en *Secretary of State for the Home Department/Tom Watson e.a*[69]. Deze betroffen de bewaring van verkeers- en locatiegegevens van "alle abonnees en geregistreerde gebruikers" en "alle elektronische communicatiemiddelen" evenals metagegevens, zonder "differentiatie, beperking of uitzondering naargelang van het nagestreefde doel"[70]. In het betreffende geval konden gegevens worden bewaard van alle personen, of deze nu, direct of indirect, in verband konden worden gebracht met ernstige strafbare feiten of niet, en of hun communicatieverkeer nu relevant was voor de nationale veiligheid of niet. Gezien het feit dat geen verband werd vereist tussen de bewaarde gegevens en een bedreiging van de openbare veiligheid, of beperkingen op grond van periode of geografisch gebied, concludeerde het HvJ-EU dat de nationale regeling verder ging dan strikt noodzakelijk was voor de bestrijding van zware criminaliteit[71].

69 HvJ-EU, gevoegde zaken C-203/15 en C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen* en *Secretary of State for the Home Department/Tom Watson e.a.* [Grote kamer], 21 december 2016, punten 105-106.

70 *Ibid.*, punt 105.

71 *Ibid.*, punt 107.

De Europese Toezichthouder voor gegevensbescherming volgt in diens *Necessity Toolkit*[72] een vergelijkbare benadering wat noodzakelijkheid betreft. De toolkit dient als hulpmiddel bij het beoordelen of voorgestelde maatregelen in overeenstemming zijn met het EU-recht op het gebied van gegevensbescherming. Hij werd ontwikkeld om EU-beleidsmakers en -wetgevers die verantwoordelijk zijn voor het voorbereiden of controleren van maatregelen waarbij de verwerking van persoonsgegevens een rol speelt, en die het recht op bescherming van persoonsgegevens en andere rechten en vrijheden zoals neergelegd in het Handvest beperken, beter toe te rusten.

Doelstellingen van algemeen belang

Elke beperking op de uitoefening van de in het Handvest erkende rechten moet, om gerechtvaardigd te zijn, tevens daadwerkelijk een door de Unie erkend doel van algemeen belang dienen, of beantwoorden aan de noodzaak tot bescherming van rechten en vrijheden van anderen. Wat de noodzaak tot bescherming van rechten en vrijheden van anderen betreft, hangt het recht op bescherming van persoonsgegevens vaak samen met andere grondrechten. Paragraaf 1.3 biedt een gedetailleerde analyse van dergelijke onderlinge verbanden. Wat de doeleinden van algemeen belang betreft, deze omvatten de algemene doeleinden van de EU zoals vastgelegd in artikel 3 van het Verdrag betreffende de Europese Unie (VEU), zoals de bevordering van de vrede en het welzijn van haar volkeren, sociale rechtvaardigheid en bescherming, en de totstandbrenging van een ruimte van vrijheid, veiligheid en rechtvaardigheid waarin het vrije verkeer van personen gewaarborgd is in combinatie met passende maatregelen ter voorkoming en bestrijding van criminaliteit, evenals andere doeleinden en belangen die door specifieke bepalingen in de Verdragen worden beschermd[73]. De algemene verordening gegevensbescherming geeft in dit verband een verdere specificatie van artikel 52, lid 1, van het Handvest: Artikel 23, lid 1, van de verordening bevat een reeks doeleinden van algemeen belang die worden beschouwd als rechtmatige redenen voor de beperking van de rechten van natuurlijke personen, vooropgesteld dat de beperking de wezenlijke inhoud van het recht op bescherming van persoonsgegevens onverlet laat en zij noodzakelijk en evenredig is. Enkele doeleinden van nationaal belang die worden genoemd zijn: de nationale veiligheid en landsverdediging, voorkoming van strafbare feiten,

72 EDPS (2017), *Necessity Toolkit*, Brussel, 11 april 2017.

73 Toelichtingen bij het Handvest van de grondrechten (2007/C 303/02), PB C 303 van 14.12.2007, blz. 17-35.

bescherming van belangrijke economische of financiële belangen van de EU of van lidstaten, volksgezondheid en sociale zekerheid.

Het is belangrijk het doeleinde van algemeen belang dat door de beperking wordt gediend voldoende gedetailleerd te omschrijven en uit te leggen, aangezien de noodzakelijkheid van de beperking tegen deze achtergrond zal worden beoordeeld. Er kan alleen een beoordeling worden gemaakt van de noodzakelijkheid van de beperking wanneer een duidelijke, gedetailleerde beschrijving van het doeleinde van de beperking en van de voorgestelde maatregelen wordt gegeven[74]. Het nagestreefde doel, en de noodzaak en evenredigheid van de beperking zijn nauw met elkaar verbonden.

Voorbeeld: De zaak *Michael Schwarz/Stadt Bochum*[75] had betrekking op beperkingen van het recht op een privéleven en het recht op bescherming van persoonsgegevens die voortvloeiden uit het afnemen en opslaan van vingerafdrukken door autoriteiten van lidstaten bij de afgifte van paspoorten[76]. De aanvrager had bij de gemeente Bochum om afgifte van een paspoort verzocht, waarbij hij zich verzette tegen de afname van zijn vingerafdrukken; dit resulteerde in de afwijzing door de gemeente Bochum van zijn paspoortaanvraag. Hij stelde vervolgens beroep in bij een Duitse rechtbank om de verstrekking van een paspoort zonder afname van zijn vingerafdrukken te vorderen. Het Duitse gerecht verwees de zaak naar het HvJ-EU en legde het de vraag voor of artikel 1, lid 2, van Verordening (EG) nr. 2252/2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten als geldig moet worden beschouwd.

Het HvJ-EU betoogde dat vingerafdrukken **vallen onder het begrip persoonsgegevens**, aangezien zij objectief gezien unieke informatie bevatten over natuurlijke personen, en het mogelijk maken deze personen precies te identificeren, terwijl het afnemen en bewaren van vingerafdrukken onder verwerking vallen. Deze laatste verwerking, zoals geregeld door artikel 1, lid 2, van Verordening (EG) nr. 2252/2004, vormt een aantasting van de rechten op eerbiediging van het privéleven en de bescherming van

74 EDPS (2017), *Necessity Toolkit*, Brussel, 11 april 2017, blz. 4.

75 HvJ-EU, zaak C-291/12, *Michael Schwarz/Stadt Bochum*, 17 oktober 2013.

76 *Ibid.*, punten 33–36.

persoonsgegevens[77]. Artikel 52, lid 1, van het Handvest voorziet echter in beperkingen op de uitoefening van die rechten, voor zover deze beperkingen zijn vastgesteld bij wet, de wezenlijke inhoud van de rechten eerbiedigen, en in overeenstemming met het evenredigheidsbeginsel noodzakelijk zijn en daadwerkelijk door de Unie erkende doelstellingen van algemeen belang dienen of beantwoorden aan de noodzaak tot bescherming van rechten en vrijheden van anderen.

In de onderhavige zaak merkte het HvJ-EU ten eerste op dat de beperking die voortvloeit uit de afneming en bewaring van vingerafdrukken in het kader van de afgifte van paspoorten, moet worden aangemerkt als een beperking waarin **bij wet is voorzien**, aangezien artikel 1, lid 2, van Verordening (EG) nr. 2252/2004 in deze handelingen voorziet. Ten tweede wordt met deze laatste bepaling beoogd paspoortvervalsing en frauduleus gebruik van paspoorten te voorkomen. Artikel 1, lid 2, is derhalve bedoeld ter voorkoming van, onder meer, de illegale binnenkomst van personen op het grondgebied van de Unie, en streeft dus een door de Unie erkende doelstelling van algemeen belang na. Ten derde bleek uit de gegevens waarover het Hof beschikte niet en werd overigens ook niet gesteld, dat de beperkingen die in casu waren gesteld aan de uitoefening van de door de artikelen 7 en 8 van het Handvest erkende rechten, de wezenlijke inhoud van deze rechten niet eerbiedigden. Ten vierde is voor de in deze bepaling voorziene bewaring van vingerafdrukken op een opslagmedium dat aan de hoogste veiligheidsnormen voldoet een zeer geavanceerde techniek vereist. Deze bewaring kan het risico van vervalsing van paspoorten verminderen en de taak van de autoriteiten die aan de EU-grenzen de authenticiteit van die documenten moeten onderzoeken, vergemakkelijken. Het feit dat bovengenoemde methode niet volledig betrouwbaar is, is niet doorslaggevend. Hoewel deze methode de acceptatie van niet-geautoriseerde personen niet volledig uitsluit, volstaat het dat ze leidt tot een aanzienlijke vermindering van het risico van dergelijke acceptaties. Het HvJ-EU stelde vast, gelet op het voorgaande, dat het afnemen en bewaren van vingerafdrukken, als bedoeld in artikel 1, lid 2, van Verordening (EG) nr. 2252/2004, geschikt is om de door die verordening nagestreefde doelstellingen en dus ook die van de voorkoming van de illegale binnenkomst van personen op het grondgebied van de Unie, te verwezenlijken[78].

77 *Ibid.*, punten 27–30.

78 *Ibid.*, punten 35–45.

Het Hof onderzocht vervolgens of een dergelijke verwerking **noodzakelijk** is, waarbij werd opgemerkt dat bij het afnemen slechts de afdruk wordt genomen van twee vingers. Deze zijn trouwens normaliter blootgesteld aan het zicht van anderen, zodat deze handeling geen intiem karakter heeft. Het veroorzaakt ook geen fysieke of psychische ongemakken voor de betrokkene, evenmin als het afnemen van zijn gezichtsopname dat doet. Tevens zij opgemerkt dat het enige reële alternatief voor de afneming van vingerafdrukken dat tijdens de procedure voor het Hof werd genoemd, bestond in het afnemen van een irisscan. Het aan het Hof voorgelegde dossier bevatte evenwel niets dat erop wees dat laatstgenoemde methode de in de artikelen 7 en 8 van het Handvest erkende rechten minder ingrijpend zou aantasten dan het afnemen van vingerafdrukken. Wat voorts de doeltreffendheid van deze twee laatste methoden betreft, staat vast dat het stadium van technische ontwikkeling van de methode die is gebaseerd op irisherkenning, niet het niveau heeft van de op vingerafdrukken gebaseerde methode, het procedé van irisherkenning op dit moment veel duurder is dan dat van het afnemen van vingerafdrukken, en het daardoor minder geschikt is voor algemeen gebruik. Het Hof was dan ook niet in kennis gesteld van het bestaan van maatregelen die voldoende doeltreffend kunnen bijdragen tot het doel van bescherming van paspoorten tegen frauduleus gebruik ervan en die een minder ingrijpende aantasting meebrengen van de in de artikelen 7 en 8 van het Handvest erkende rechten dan het afnemen van vingerafdrukken[79].

Het HvJ-EU merkte op dat artikel 4, lid 3, van Verordening (EG) nr. 2252/2004 uitdrukkelijk preciseert dat vingerafdrukken alleen mogen worden gebruikt voor het verifiëren van de authenticiteit van het paspoort en de identiteit van de houder ervan, terwijl artikel 1, lid 2, van dezelfde verordening bepaalt dat vingerafdrukken enkel mogen worden bewaard in het paspoort zelf, dat exclusief in het bezit blijft van de houder ervan. De verordening bood derhalve geen rechtsgrondslag voor een eventuele centralisatie van verzamelde gegevens, of voor het gebruik van deze gegevens voor andere doeleinden dan dat van voorkoming van de illegale binnenkomst van personen op het grondgebied van de Unie[80]. Het HvJ-EU concludeerde,

79 HvJ-EU, zaak C-291/12, *Michael Schwarz/Stadt Bochum*, 17 oktober 2013, punten 46–53.

80 *Ibid.*, punten 56–61.

gelet op het voorgaande, dat bij het onderzoek van de prejudiciële vraag niet was gebleken van feiten of omstandigheden die de geldigheid van artikel 1, lid 2, van Verordening (EG) nr. 2252/2004 konden aantasten.

Verhouding tussen het Handvest en het EVRM

Hoewel verschillend geformuleerd, zijn de voorwaarden voor rechtmatige beperkingen op de rechten in artikel 52, lid 1, van het Handvest vergelijkbaar met artikel 8, lid 2, van het EVRM betreffende het recht op eerbiediging van het privéleven. Het HvJ-EU en het EHRM verwijzen regelmatig in hun rechtspraak naar elkaars beslissingen in het kader van de permanente dialoog tussen de twee gerechtshoven ten behoeve van een geharmoniseerde uitlegging van de gegevensbeschermingsregels. Artikel 52, lid 3, van het Handvest bepaalt: "Voor zover dit Handvest rechten bevat die corresponderen met rechten welke zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend." Artikel 8 van het Handvest komt echter niet rechtstreeks overeen met een bepaald artikel in het EVRM[81]. Artikel 52, lid 3, van het Handvest betreft de inhoud en reikwijdte van de in beide rechtsordes beschermde rechten, niet de voorwaarden voor de beperking daarvan. Met het oog op het bredere kader van dialoog en samenwerking tussen de twee gerechtshoven kan het HvJ-EU echter in zijn onderzoeken de criteria voor beperking die worden genoemd in artikel 8 van het EVRM, en zoals uitgelegd door het EHRM, in aanmerking nemen. Ook de tegenovergestelde situatie, waarin het EHRM verwijst naar de rechtmatige voorwaarden voor beperking volgens het Handvest, is mogelijk. Tevens moet er hoe dan ook rekening mee worden gehouden dat geen enkele bepaling in het EVRM volledig overeenkomt met artikel 8 van het Handvest, dat betrekking heeft op de bescherming van persoonsgegevens, met name op de rechten van betrokkenen, gerechtvaardigde grondslagen voor verwerking en toezicht door een onafhankelijke autoriteit. Een aantal elementen van artikel 8 van het Handvest kunnen worden gegrond op de rechtspraak van het EHRM die zich heeft ontwikkeld op basis van artikel 8 van het EVRM en met betrekking tot Verdrag 108[82]. Deze koppeling garandeert dat het HvJ-EU en het EHRM elkaar wederzijds inspireren waar het gaat om kwesties die verband houden met de bescherming van persoonsgegevens.

81 EDPS (2017), *Necessity Toolkit*, Brussel, 11 april 2017, blz. 6.

82 Toelichtingen bij het Handvest van de grondrechten van de Europese Unie (2007/C 303/02), artikel 8.

1.3. Wisselwerking met andere rechten en gerechtvaardigde belangen

Belangrijkste punten

- Er bestaat vaak een wisselwerking tussen het recht op gegevensbescherming en andere rechten, zoals de vrijheid van meningsuiting en de vrijheid kennis te nemen en te geven van informatie.
- Deze wisselwerking is vaak ambivalent: aan de ene kant zijn er situaties waarin het recht op bescherming van persoonsgegevens op gespannen voet staat met een bepaald ander recht, maar er zijn ook omstandigheden waarin het recht op bescherming van persoonsgegevens juist garandeert dat datzelfde recht wordt geëerbiedigd. Dit geldt bijvoorbeeld voor de vrijheid van meningsuiting. Het beroepsgeheim valt immers onder het recht op eerbiediging van het privéleven.
- De noodzaak om de rechten en vrijheden van anderen te beschermen is een van de criteria die worden gehanteerd bij de beoordeling van de rechtmatigheid van een beperking van het recht op bescherming van persoonsgegevens.
- Wanneer verschillende rechten in het geding zijn, moeten rechterlijke instanties de verschillende belangen tegen elkaar afwegen.
- De algemene verordening gegevensbescherming vereist dat lidstaten een evenwicht bereiken tussen het recht op bescherming van persoonsgegevens en de vrijheid van meningsuiting.
- De lidstaten kunnen eveneens in de nationale wetgeving specifieke voorschriften vaststellen om het recht op bescherming van persoonsgegevens en de publieke toegang tot officiële documenten en verplichtingen in verband met het beroepsgeheim in overeenstemming te brengen.

Het recht op bescherming van persoonsgegevens is geen absoluut recht; de voorwaarden voor een rechtmatige beperking van dit recht zijn hierboven beschreven. Een van de criteria voor een rechtmatige beperking op rechten, die zowel in het RvE- als het EU-recht wordt toegepast, is dat de inbreuk op het recht op gegevensbescherming noodzakelijk is om de rechten en vrijheden van anderen te beschermen. Wanneer er een spanningsveld bestaat tussen gegevensbescherming en andere rechten, hebben het EHRM en het HvJ-EU herhaaldelijk gesteld dat er bij de toepassing en uitleg van artikel 8 van het EVRM en artikel 8 van het Handvest een

afweging met andere rechten moet plaatsvinden[83]. Hier onder zal met een aantal belangrijke voorbeelden worden geïllustreerd hoe deze afweging plaatsvindt.

In aanvulling op de afweging door deze gerechten kunnen lidstaten indien nodig wetgeving aannemen waarmee het recht op bescherming van persoonsgegevens in overeenstemming wordt gebracht met andere rechten. Met het oog hierop zijn in de algemene verordening gegevensbescherming een aantal gebieden opgenomen waarvoor op nationaal niveau afwijkende bepalingen kunnen gelden.

Wat de vrijheid van meningsuiting betreft, vereist de AVG dat lidstaten "het recht op bescherming van persoonsgegevens overeenkomstig deze verordening wettelijk in overeenstemming [brengen] met het recht op vrijheid van meningsuiting en van informatie, daar onder begrepen de verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen"[84]. De lidstaten kunnen eveneens wetgevingen vaststellen die de bescherming van gegevens in overeenstemming brengt met de publieke toegang tot officiële documenten en de verplichtingen in verband met het beroepsgeheim dat wordt beschermd als een soort recht op eerbiediging van het privéleven[85].

1.3.1. Vrijheid van meningsuiting

Een van de belangrijkste rechten die in wisselwerking staan met het recht op gegevensbescherming is het recht op vrijheid van meningsuiting.

De vrijheid van meningsuiting wordt beschermd door artikel 11 van het Handvest ("Vrijheid van meningsuiting en van informatie"). Dit recht omvat de "vrijheid een mening te hebben en de vrijheid kennis te nemen en te geven van informatie of ideeën, zonder inmenging van enig openbaar gezag en ongeacht grenzen". De vrijheid van informatie betreft volgens artikel 11 van het Handvest en artikel 10 van het EVRM niet alleen het recht om informatie te verstrekken, maar ook het recht om informatie te *ontvangen*.

83 EHRM, *Von Hannover/Duitsland* (nr. 2) [Grote kamer], nr. 40660/08 en 60641/08, 7 februari 2012; HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 november 2011, punt 48; HvJ-EU, zaak C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [Grote kamer], 29 januari 2008, punt 68.

84 Algemene verordening gegevensbescherming, artikel 85.

85 *Ibid.*, artikelen 86 en 90.

Beperkingen aan de vrijheid van meningsuiting moeten voldoen aan de in artikel 52, lid 1, van het Handvest vastgestelde criteria, zoals hierboven beschreven. Artikel 11 komt bovendien overeen met artikel 10 van het EVRM. Krachtens artikel 52, lid 3, van het Handvest, zijn, voor zover het Handvest rechten bevat die corresponderen met rechten die worden gegarandeerd door het EVRM, "de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend". De beperkingen die bij wet kunnen worden gesteld aan het door artikel 11 van het Handvest gegarandeerde recht kunnen derhalve niet verder gaan dan die waarin wordt voorzien in artikel 10, lid 2, van het EVRM, d.w.z. dat ze wettelijk moeten zijn voorgeschreven en in een democratische samenleving noodzakelijk moeten zijn voor "de bescherming van de goede naam of de rechten van anderen". Het gaat hierbij in het bijzonder om het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens.

De verhouding tussen de bescherming van persoonsgegevens en de vrijheid van meningsuiting wordt geregeld door artikel 85 van de algemene verordening gegevensbescherming, getiteld "Verwerking en vrijheid van meningsuiting en van informatie". Dit artikel schrijft voor dat de lidstaten een evenwicht bereiken tussen het recht op bescherming van persoonsgegevens en het recht op vrijheid van meningsuiting. In het bijzonder moeten uitzonderingen en derogaties van bepaalde hoofdstukken van de algemene verordening gegevensbescherming gelden voor verwerking voor journalistieke doeleinden of ten behoeve van academische, artistieke of literaire uitdrukkingsvormen, voor zover deze noodzakelijk zijn om het recht op bescherming van persoonsgegevens in overeenstemming te brengen met de vrijheid van meningsuiting en van informatie.

Voorbeeld: In *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy en Satamedia Oy*[86] werd het HvJ-EU verzocht de verhouding tussen gegevensbescherming en persvrijheid te preciseren[87]. Het Hof moest de publicatie door een bedrijf, via een sms-dienst, van belastinggegevens van circa 1,2 miljoen natuurlijke personen die zij rechtmatig van de Finse

86 HvJ-EU, zaak C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy en Satamedia Oy* [Grote kamer], 16 december 2008, punten 56, 61 en 62.

87 De zaak betrof de uitlegging van artikel 9 van de richtlijn gegevensbescherming, dat inmiddels is vervangen door artikel 85 van de algemene verordening gegevensbescherming, waarin het volgende werd bepaald: "De lidstaten voorzien voor de verwerking van persoonsgegevens voor uitsluitend journalistieke of voor artistieke of literaire doeleinden in uitzonderingen op en derogaties van de bepalingen van dit hoofdstuk en van de hoofdstukken IV en VI uitsluitend voor zover deze nodig blijken om het recht op persoonlijke levenssfeer te verzoenen met de regels betreffende de vrijheid van meningsuiting".

belastingautoriteiten had verkregen, aan een onderzoek onderwerpen. De Finse autoriteit voor toezicht op gegevensbescherming had het bedrijf gelast deze gegevens niet langer te publiceren. De onderneming stelde tegen deze beslissing beroep in bij een nationale rechtbank, die daarop het HvJ-EU om verduidelijking verzocht betreffende de uitlegging van de richtlijn gegevensbescherming. Met name moest het HvJ-EU verifiëren of de verwerking van persoonsgegevens — die de belastingdienst beschikbaar had gesteld — om gebruikers van mobiele telefoons de mogelijkheid te bieden belastinggegevens over andere natuurlijke personen te ontvangen, moest worden beschouwd als een activiteit die uitsluitend voor journalistieke doeleinden werd verricht. Na eerst te hebben geconcludeerd dat de activiteiten van de onderneming als "verwerking van persoonsgegevens" in de zin van artikel 3, lid 1, van de richtlijn gegevensbescherming moesten worden beschouwd, gaf het HvJ-EU een uitleg van artikel 9 van de richtlijn (betreffende de verwerking van persoonsgegevens en de vrijheid van meningsuiting). Daarbij wees het Hof in de eerste plaats op het belang van het recht op vrijheid van meningsuiting in elke democratische samenleving en stelde het dat met deze vrijheid samenhangende begrippen, waaronder het begrip journalistiek, ruim moeten worden geïnterpreteerd. Vervolgens merkte het HvJ-EU op dat om tot een evenwichtige afweging tussen de beide fundamentele rechten te komen, de derogaties en beperkingen van het recht op gegevensbescherming binnen de grenzen van het strikt noodzakelijke moeten blijven. In deze omstandigheden oordeelde het HvJ-EU dat activiteiten als die welke door de bedrijven in kwestie werden verricht met betrekking tot gegevens afkomstig uit documenten die volgens de nationale wetgeving openbaar zijn, kunnen worden aangemerkt als "journalistieke activiteiten" indien zij de bekendmaking aan het publiek van informatie, meningen of ideeën tot doel hebben, ongeacht het overdrachtsmedium. Ook bepaalde het Hof dat deze activiteiten niet zijn voorbehouden aan mediaondernemingen en een winstoogmerk kunnen hebben. Het HvJ-EU oordeelde echter dat het aan de nationale rechter was om te bepalen of dit in deze specifieke zaak het geval was.

Dezelfde zaak werd tevens onderzocht door het EHRM, nadat het nationale gerecht op grond van de toelichting van het HvJ-EU had geoordeeld dat het bevel van de toezichthoudende autoriteit om de publicatie van alle belastinggegevens te staken een gerechtvaardigde inbreuk op de vrijheid van meningsuiting van het bedrijf was. Deze opvatting werd door het EHRM

onderschreven[88]. Het oordeelde dat, hoewel er sprake was van inbreuk op het recht van het bedrijf op het kennisgeven van informatie, deze inbreuk in overeenstemming was met de wet, een rechtmatig doel diende en noodzakelijk was in een democratische samenleving.

Het Hof bracht de criteria uit de rechtspraak in herinnering die als leidraad zouden moeten dienen voor de nationale autoriteiten, en het EHRM zelf, bij het tegen elkaar afwegen van de vrijheid van meningsuiting en het recht op eerbiediging van het privéleven. In het geval van politieke uitspraken of discussies over zaken van algemeen belang is er weinig ruimte voor beperking van de vrijheid kennis te nemen en te geven van informatie, aangezien het publiek er recht op heeft geïnformeerd te worden, "en dit is een fundamenteel recht in een democratische samenleving"[89]. Artikelen in de pers echter, die uitsluitend ten doel hebben de nieuwsgierigheid van een bepaald lezerspubliek naar bijzonderheden van iemands privéleven te bevredigen, kunnen niet worden beschouwd als bijdrage aan een discussie van algemeen belang. Met de derogatie van gegevensbeschermingsregels voor journalistieke doeleinden wordt beoogd journalisten toegang tot gegevens te bieden en het hun mogelijk te maken deze te verzamelen en te verwerken in het kader van hun journalistieke activiteiten. Er was derhalve wel sprake van een algemeen belang voor zover het de toegangsverschaffing tot de grote hoeveelheid belastinggegevens betrof, en de verlening van toestemming aan de verzoekende bedrijven om deze gegevens te verzamelen en te verwerken. Het Hof oordeelde echter dat er geen sprake was van algemeen belang bij de publicatie van dergelijke onbewerkte gegevens door de kranten, in ongewijzigde vorm en zonder ze op enige manier te analyseren. De belastinginformatie zou nieuwsgierige lezers in staat hebben gesteld personen op grond van hun economische positie te klasseren en zou de nieuwsgierigheid van het publiek naar het privéleven van anderen bevredigen. Dit kon niet worden beschouwd als bijdrage aan een discussie van algemeen belang.

88 EHRM, *Satakunnan Markkinapörssi Oy en Satamedia Oy/Finland*, [Grote kamer], nr. 931/13, 27 juni 2017.

89 *Ibid.*, punt 169.

Voorbeeld: In de zaak *Google Spain*[90] onderzocht het HvJ-EU of Google verplicht was verouderde informatie over financiële problemen van de verzoeker uit de resultatenlijst te verwijderen. Wanneer in de zoekmachine van Google werd gezocht op de naam van de verzoeker verschenen in de resultatenlijst koppelingen naar oude krantenartikelen waarin de betrokkenheid van verzoeker bij een faillissementsprocedure werd genoemd. De verzoeker beschouwde dit als een inbreuk op zijn recht op eerbiediging van het privéleven en het recht op de bescherming van persoonsgegevens, aangezien de procedure jaren eerder al was afgerond, waardoor deze informatie niet langer relevant was.

Het HvJ-EU verduidelijkte ten eerste dat via internetzoekmachines en zoekresultaten die persoonsgegevens bevatten een gedetailleerd profiel van een natuurlijke persoon kan worden opgesteld. Het is, met het oog op de steeds sterker gedigitaliseerde samenleving, van fundamenteel belang dat persoonsgegevens correct zijn en dat niet meer wordt gepubliceerd dan wat noodzakelijk is voor informatieverschaffing aan het publiek, om voor natuurlijke personen een hoog niveau van gegevensbescherming te kunnen waarborgen. De "voor deze verwerking verantwoordelijke [moet], [...] binnen het kader van zijn verantwoordelijkheden, bevoegdheden en mogelijkheden verzekeren dat deze verwerking aan de vereisten [...] voldoet" van het EU-recht, zodat de daarin vervatte wettelijke waarborgen hun volle werking kunnen krijgen. Dit betekent dat het recht op verwijdering van persoonsgegevens wanneer de verwerking niet langer noodzakelijk is of de informatie is verouderd, tevens betrekking heeft op zoekmachines, die werden beschouwd als voor de verwerking verantwoordelijken en niet slechts als verwerkers (zie paragraaf 2.3.1).

Het onderzoek naar de vraag of Google verplicht moest worden de koppelingen met betrekking tot de verzoeker te verwijderen, bracht het HvJ-EU tot het oordeel dat natuurlijke personen onder bepaalde omstandigheden recht hebben op verwijdering van hun persoonsgegevens uit de zoekresultaten van een internetzoekmachine. Op dit recht kan een beroep worden gedaan wanneer informatie over een natuurlijke persoon niet correct, toereikend of ter zake dienend is, of bovenmatig is, uitgaande van de doeleinden van de gegevensverwerking. Het HvJ-EU erkende dat dit

90 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 13 mei 2014, punten 81–83.

recht geen absolute gelding heeft. Het dient te worden afgewogen tegen andere rechten, met name het belang van het algemene publiek bij en het recht op toegang tot de informatie. Verzoeken om uitwissing moeten van geval tot geval worden beoordeeld, zodat een evenwicht kan worden gevonden tussen enerzijds het fundamentele recht op bescherming van persoonsgegevens en eerbiediging van het privéleven van de betrokkene en anderzijds de gerechtvaardigde belangen van alle internetgebruikers. Het Hof verduidelijkte welke factoren in de afweging dienen te worden meegenomen. Met name de aard van de gegevens is een belangrijke factor. Wanneer het gaat om gevoelige gegevens uit het privéleven van een natuurlijke persoon en de beschikbaarheid van de informatie geen algemeen belang dient, krijgen gegevensbescherming en privacy voorrang op het recht van het publiek op toegang tot de informatie. Als daarentegen blijkt dat de betrokkene een bekend persoon is, of dat de informatie van dien aard is dat het gerechtvaardigd is dat het publiek hiervan kennisneemt, dan is de inbreuk op het fundamentele recht op gegevensbescherming en op privacy gerechtvaardigd.

Volgend op dit arrest heeft Groep artikel 29 richtsnoeren aangenomen voor de uitvoering van de uitspraak van het HvJ-EU. Deze richtsnoeren omvatten onder meer een lijst met door toezichthoudende autoriteiten te hanteren gemeenschappelijke criteria bij het afhandelen van klachten in verband met verwijderingsverzoeken van natuurlijke personen, als leidraad bij deze afweging[91].

Met betrekking tot de verzoening van het recht op gegevensbescherming met het recht op vrijheid van meningsuiting, heeft het EHRM verschillende beginselarresten gewezen.

Voorbeeld: In *Axel Springer AG/Duitsland*[92] oordeelde het EHRM dat een aan het verzoekende bedrijf opgelegd gerechtelijk verbod om een artikel te publiceren over de aanhouding en veroordeling van een bekende acteur, strijdig was met artikel 10 van het EVRM. Het EHRM herhaalde daarbij de

91 Groep artikel 29 (2014),*Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Brussel, 26 november 2014.

92 EHRM, *Axel Springer AG/Duitsland* [Grote kamer], nr. 39954/08, 7 februari 2012, punten 90 en 91.

criteria die moeten worden overwogen bij het tegen elkaar afwegen van het recht van vrijheid van meningsuiting en het recht op eerbiediging van het privéleven, zoals vastgesteld in zijn jurisprudentie:

- of de gebeurtenis waarop het gepubliceerde artikel betrekking had van algemeen belang was;
- of de betrokken persoon een publieke figuur was, en
- hoe de informatie was verkregen en of de informatie betrouwbaar was.

Het EHRM oordeelde dat de aanhouding en veroordeling van de acteur een openbaar rechtsfeit was en derhalve van publiek belang was; dat de acteur voldoende bekend was om als publiek figuur te kunnen worden aangemerkt, en dat de informatie was verstrekt door het bureau van de openbaar aanklager en de juistheid van de informatie die beide publicaties bevatten door geen van de partijen werd betwist. De beperkingen van de publicatie die aan het bedrijf waren opgelegd konden bijgevolg redelijkerwijs niet worden beschouwd als evenredig aan het rechtmatige doel om het privéleven van de verzoeker te beschermen. Het Hof concludeerde dat artikel 10 van het EVRM was geschonden.

Voorbeeld: *Couderc en Hachette Filipacchi Associés/Frankrijk*[93] betrof de publicatie door een Frans weekblad van een interview met mw. Coste, die stelde dat prins Albert van Monaco de vader was van haar zoontje. In het interview werd ook de relatie van mw. Coste met de prins beschreven en de manier waarop hij op de geboorte van het kind had gereageerd, vergezeld van foto's van prins Albert met het kind. Prins Albert dagvaardde de uitgever wegens schending van zijn recht op bescherming van het privéleven. De Franse gerechten oordeelden dat de publicatie van het artikel prins Albert onomkeerbare schade had toegebracht en veroordeelden de uitgever tot het betalen van een schadevergoeding en tot het publiceren van de gerechtelijke uitspraak op de voorpagina van het tijdschrift.

93 EHRM, *Couderc en Hachette Filipacchi Associés/Frankrijk* [Grote kamer], nr. 40454/07, 10 november 2015.

De uitgevers van het tijdschrift dienden een klacht in bij het EHRM en stelden dat de uitspraak van de Franse rechtbanken een ongerechtvaardigde inbreuk was op hun vrijheid van meningsuiting. Het EHRM moest het recht van prins Albert op eerbiediging van zijn privéleven afwegen tegen het recht van de uitgever op vrijheid van meningsuiting en het recht van het publiek op kennisneming van de informatie. Daarnaast vormden het recht van mw. Coste om het publiek deelgenoot te maken van haar verhaal en het belang van het kind bij het formeel vestigen van een vader-kindrelatie belangrijke overwegingen.

Het EHRM gaf aan dat de publicatie van het interview een inmenging was met het privéleven van de prins en onderzocht vervolgens of deze inmenging noodzakelijk was. Het stelde vast dat de publicatie betrekking had op een publieke figuur en van publiek belang was, omdat de inwoners van Monaco belang hadden bij kennis over het bestaan van een kind van de prins. De toekomst van een erfelijke monarchie is immers "onlosmakelijk verbonden aan het bestaan van afstammelingen" en is als zodanig een zaak van publiek belang[94]. Het Hof merkte tevens op dat mw. Coste met het artikel haar recht en dat van haar kind op vrijheid van meningsuiting had kunnen uitoefenen. De nationale gerechten hadden de beginselen en criteria voor het afwegen van het recht op privéleven en de vrijheid van meningsuiting, zoals neergelegd in de jurisprudentie van het EHRM, onvoldoende in acht genomen. Het Hof concludeerde dat Frankrijk artikel 10 van het EVRM betreffende de vrijheid van meningsuiting had geschonden.

In de jurisprudentie van het EHRM is een van de cruciale criteria met betrekking tot de afweging van rechten of de uiting in kwestie al dan niet bijdraagt tot een debat van algemeen publiek belang.

Voorbeeld: In *Mosley/Verenigd Koninkrijk*[95] had een nationaal weekblad intieme foto's gepubliceerd van de verzoeker, een algemeen bekend persoon. Hij stelde een civielrechtelijke vordering in tegen de uitgever en kreeg een schadevergoeding toegewezen. Ondanks de toegekende financiële vergoeding beklaagde de verzoeker zich erover dat hij nog altijd slachtoffer was van een inbreuk op zijn recht op privacy, omdat hij niet voorafgaand aan

94 *Ibid.*, punten 104–116.

95 EHRM, *Mosley/Verenigd Koninkrijk*, nr. 48009/08, 10 mei 2011, punten 129 en 130.

de publicatie van de desbetreffende foto's een publicatieverbod had kunnen eisen, aangezien het weekblad wettelijk niet verplicht was hem van tevoren van de publicatie in kennis te stellen.

Het EHRM merkte op dat, hoewel de verspreiding van dit materiaal in algemene zin meer voor amusements- dan voor educatieve doeleinden had plaatsgevonden, de publicatie zonder twijfel de bescherming genoot van artikel 10 van het EVRM, die mogelijk moest wijken voor de eisen van artikel 8 van het EVRM indien de informatie privé en intiem van aard was en er geen algemeen belang werd gediend met de publicatie ervan. Daarbij diende echter zeer zorgvuldig te worden gekeken naar beperkingen die zouden kunnen neerkomen op een vorm van censuur voorafgaand aan de publicatie. Gezien het afschrikwekkende effect ("chilling effect") waartoe een vereiste van voorafgaande kennisgeving mogelijk zou kunnen leiden, en gelet op de twijfels over de doeltreffendheid daarvan en de ruime beoordelingsmarge op dat gebied, concludeerde het EHRM echter dat artikel 8 het bestaan van een wettelijk bindende vereiste van voorafgaande kennisgeving niet verplicht stelde. Bijgevolg concludeerde het Hof dat er geen inbreuk op artikel 8 had plaatsgevonden.

Voorbeeld: In de zaak *Bohlen/Duitsland*[96] had de verzoeker, een bekende zanger en muziekproducent, een autobiografie gepubliceerd en werd hij vervolgens bij rechterlijke beslissing verplicht een aantal passages te verwijderen. Het verhaal kreeg veel aandacht in de nationale media en een tabaksfabrikant lanceerde een humoristische reclamecampagne waarin naar deze gebeurtenis werd verwezen. Hierin werd de voornaam van de verzoeker zonder zijn toestemming gebruikt. De verzoeker eiste een schadevergoeding van het reclamebureau wegens inbreuk op zijn rechten krachtens artikel 8 van het EVRM, zonder succes. Het EHRM benadrukte de criteria op basis waarvan het recht op eerbiediging van het privéleven en het recht op vrijheid van meningsuiting tegen elkaar worden afgewogen, en concludeerde dat artikel 8 niet was geschonden. De aanvrager is een algemeen bekend persoon en de reclame bevatte geen verwijzingen naar zijn privéleven, maar naar een publiekelijk bekende gebeurtenis die al in de media was beschreven en bij het publiek onderwerp van discussie was. Bovendien was de reclame humoristisch van aard en bevatte deze niets dat vernederend of negatief was ten opzichte van de verzoeker.

96 EHRM, *Bohlen/Duitsland*, nr. 53495/09, 19 februari 2015, punten 45–60.

Voorbeeld: In *Biriuk/Litouwen*[97] betoogde verzoekster voor het EHRM dat Litouwen had verzuimd het recht op eerbiediging van haar privéleven te waarborgen, omdat, hoewel een belangrijk nieuwsblad haar privacy ernstig had geschonden, haar door de nationale rechtbanken die haar zaak hadden onderzocht, een beledigend laag bedrag aan schadevergoeding was toegewezen. Bij het toekennen van de vergoeding voor immateriële schade hadden de nationale rechters zich gebaseerd op de bepalingen van de nationale wetgeving inzake de verstrekking van informatie aan het algemene publiek. Hierin wordt een lage bovengrens gesteld aan compensatie voor immateriële schade ten gevolge van onwettige publicatie door de media van informatie over iemands privéleven. De zaak volgde op de publicatie door het grootste dagblad van Litouwen van een artikel op de voorpagina waarin werd gemeld dat de verzoekster hiv-positief was. In het artikel werd tevens kritiek geuit op het gedrag van verzoekster en werden haar zedelijke normen in twijfel getrokken.

Het EHRM bracht in herinnering dat de bescherming van persoonsgegevens, en in het bijzonder medische gegevens, van fundamenteel belang was voor het recht op eerbiediging van het privéleven volgens het EVRM. Vooral de vertrouwelijkheid van gezondheidsgegevens is van belang, aangezien de bekendmaking van medische gegevens (de hiv-status van verzoekster in dit geval) ingrijpende gevolgen kan hebben voor het privéleven en familieleven van de desbetreffende persoon, zijn of haar werksituatie en maatschappelijke inclusie. Het Hof hechtte met name belang aan het feit dat, volgens het verslag in het nieuwsblad, medisch personeel van het ziekenhuis informatie had verstrekt over de hiv-status van verzoekster, hetgeen duidelijk in strijd was met hun medische beroepsgeheim. Er was dan ook sprake van een onrechtmatige inbreuk op het recht op een privéleven van de verzoekster.

Het artikel was gepubliceerd in de pers, en vrijheid van meningsuiting is ook een grondrecht krachtens het EVRM. Na te hebben onderzocht of met de publicatie van dergelijke informatie over verzoekster een openbaar belang was gediend, oordeelde het Hof dat het belangrijkste doel van de publicatie een toename van de verkoop van het nieuwsblad was door de nieuwsgierigheid van de lezers te bevredigen. Een dergelijke doelstelling kon niet worden geacht bij te dragen aan enig debat van algemeen belang. Aangezien hier sprake was van "onacceptabel misbruik van de

97 EHRM, *Biriuk/Litouwen*, nr. 23373/03, 25 november 2008.

persvrijheid" betekenden de ernstige beperkingen in de toekenning van een schadevergoeding en de lage vergoeding voor immateriële schade volgens het nationale recht, dat Litouwen zijn uitdrukkelijke verplichting om het recht op eerbiediging van het privéleven van de verzoekster te beschermen, niet was nagekomen. Het Hof concludeerde dat er een inbreuk op artikel 8 van het EVRM had plaatsgevonden.

Er is niet altijd een conflict tussen het recht op vrijheid van meningsuiting en het recht op bescherming van persoonsgegevens. Er zijn situaties waarin de doeltreffende bescherming van persoonsgegevens ook de vrijheid van meningsuiting waarborgt.

Voorbeeld: Het HvJ-EU verklaarde in *Tele2 Sverige* dat Richtlijn 2006/24/EG (richtlijn gegevensbewaring) een "zeer ruime en bijzonder ernstige inmenging" vormt in de door de artikelen 7 en 8 van het Handvest gewaarborgde fundamentele rechten. "Bovendien kan het feit dat de gegevens worden bewaard en later worden gebruikt zonder dat de abonnee of de geregistreerde gebruiker hierover wordt ingelicht, bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden." Het Hof oordeelde verder dat het veralgemeniseren van de bewaring van verkeers- en locatiegegevens invloed zou kunnen hebben op het gebruik van elektronische communicatiemiddelen en "dus op de wijze waarop de gebruikers van deze communicatiemiddelen van hun in artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting gebruikmaken"[98]. In die zin dragen gegevensbeschermingsregels, door strikte waarborgen te eisen dat gegevens niet als regel worden bewaard, uiteindelijk bij aan gebruikmaking van het recht op vrijheid van meningsuiting.

Wat het recht op het ontvangen van informatie betreft, wat evenzeer een onderdeel van de vrijheid van meningsuiting is, wordt het belang van transparant overheidshandelen voor de werking van een democratische samenleving in toenemende mate onderkend. Transparantie is een doelstelling van algemeen belang die een inbreuk op het recht van gegevensbescherming, mits noodzakelijk en evenredig,

98 HvJ-EU, gevoegde zaken C-203/15 en C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen* en *Secretary of State for the Home Department/Tom Watson e.a.* [Grote kamer], 21 december 2016, punten 37 en 101; HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en Kärntner Landesregierung e.a. [Grote kamer], 8 april 2014, punt 28.

zou kunnen rechtvaardigen, zoals beschreven in paragraaf 1.2. Dienovereenkomstig is in de afgelopen twee decennia het recht op toegang tot documenten die bij overheidsinstanties berusten erkend als een belangrijk recht van iedere EU-burger en elke natuurlijke of rechtspersoon die verblijft of zijn statutaire zetel heeft in een lidstaat.

In het RvE-recht kan worden verwezen naar de beginselen die zijn vervat in de Aanbeveling inzake de toegang tot officiële documenten, die als inspiratiebron heeft gediend voor de opstellers van het Verdrag betreffende de toegang tot officiële documenten (Verdrag 205)[99].

In het EU-recht wordt het recht op toegang tot documenten gegarandeerd door Verordening (EG) nr. 1049/2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie (Verordening inzake de toegang tot documenten)[100]. Artikel 42 van het Handvest en artikel 15, lid 3, van het VWEU hebben dit recht op toegang uitgebreid "tot documenten van de instellingen, organen en instanties van de Unie, ongeacht de informatiedrager waarop zij zijn vastgelegd".

Dit recht kan botsen met het recht op gegevensbescherming indien door het geven van inzage in een document persoonsgegevens van anderen bekend zouden worden. Artikel 86 van de algemene verordening gegevensbescherming bepaalt duidelijk dat persoonsgegevens in officiële documenten die in het bezit zijn van een overheidsinstantie of een orgaan, door de instantie of het orgaan in kwestie mogen worden bekendgemaakt in overeenstemming met het Unierecht[101] of het lidstatelijke recht, teneinde het recht van toegang van het publiek tot officiële documenten in overeenstemming te brengen met het recht op bescherming van persoonsgegevens uit hoofde van deze verordening.

Verzoeken om inzage in documenten of informatie die bij overheidsinstanties berusten moeten worden afgewogen tegen het recht op gegevensbescherming van personen van wie in de opgevraagde documenten persoonsgegevens zijn opgenomen.

99 Raad van Europa, Comité van Ministers (2002), Aanbeveling Rec(81)19 en Aanbeveling Rec(2002)2 van het Comité van Ministers aan de lidstaten inzake de toegang tot officiële documenten, 21 februari 2002; Raad van Europa, Verdrag betreffende de toegang tot officiële documenten, CETS nr. 205, 18 juni 2009. Het Verdrag is nog niet in werking getreden.

100 Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie, PB L 145 van 31.5.2001, blz. 43.

101 Artikel 42 van het Handvest, artikel 15, lid 3, van het VWEU en Verordening (EG) nr. 1049/2009.

Voorbeeld: In *Volker und Markus Schecke en Hartmut Eifert/Land Hessen*[102] moest het HvJ-EU de evenredigheid van de door de EU-wetgeving verplichte publicatie van de namen van de begunstigden van landbouwsubsidies van de EU en de door hen ontvangen bedragen beoordelen. Met de publicatie werd beoogd de transparantie te vergroten en bij te dragen aan de openbare controle van het doeltreffend gebruik van overheidsgelden door de administratie. De evenredigheid van deze publicatie werd door diverse begunstigden bestreden.

Het HvJ-EU, dat opmerkte dat het recht op gegevensbescherming niet absoluut is, argumenteerde dat de publicatie op een website van gegevens waarin de begunstigden van twee landbouwsteunfondsen van de EU en de precieze door hen ontvangen bedragen werden genoemd inmenging in hun privéleven in het algemeen en in de bescherming van hun persoonsgegevens in het bijzonder vormde.

Het HvJ-EU stelde dat deze aantasting van de in de artikelen 7 en 8 van het Handvest erkende rechten bij wet was bepaald en beantwoordde aan een door de Unie erkende doelstelling van algemeen belang, namelijk het vergroten van de transparantie wat het gebruik van communautaire middelen betreft. Het HvJ-EU oordeelde echter dat de publicatie van de namen van natuurlijke personen die begunstigden van EU-landbouwsteun uit deze twee fondsen waren en van de precieze door hen ontvangen bedragen een onevenredige maatregel was die gelet op artikel 52, lid 1, van het Handvest niet was gerechtvaardigd. Het erkende het belang in een democratische samenleving van het informeren van belastingplichtigen over het gebruik van overheidsmiddelen. "Het doel van openheid mag evenwel niet automatisch de voorrang krijgen op het recht op bescherming van persoonsgegevens"[103], en bijgevolg moesten de EU-instellingen een afweging maken tussen het belang van transparantie van de Unie en de beperking van de uitoefening van het recht op privacy en gegevensbescherming voor begunstigden ten gevolge van de publicatie.

102 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert/Land Hessen* [Grote kamer], 9 november 2010, punten 47–52, 58, 66–67, 75, 86 en 92.

103 *Ibid.*, punt 85.

Het HvJ-EU concludeerde dat de EU-instellingen geen evenwichtige afweging van deze belangen hadden gemaakt, aangezien maatregelen denkbaar zijn die voor de betrokken personen een minder ingrijpende aantasting van de grondrechten hadden meegebracht en tegelijkertijd doeltreffend hadden bijgedragen tot de verwezenlijking van de doelstelling van transparantie die met de publicatie werd nagestreefd. In plaats van een algemene publicatie waarin alle begunstigden werden genoemd, bij naam en met de precieze bedragen die zij hadden ontvangen, had onderscheid kunnen worden gemaakt naar gelang van de tijdvakken waarin zij steun hadden ontvangen, de frequentie van de steun, of het type en de omvang van die steun[104]. Bijgevolg verklaarde het Hof de EU-wetgeving inzake de publicatie van informatie over de begunstigden van Europese landbouwfondsen deels ongeldig.

Voorbeeld: In *Rechnungshof/Österreichischer Rundfunk e.a*[105]. onderzocht het HvJ-EU of bepaalde Oostenrijkse wetgeving verenigbaar was met het EU-recht op het gebied van gegevensbescherming. De betrokken regelgeving verplichtte een overheidsorgaan ertoe gegevens over inkomsten te verzamelen en door te geven met het oog op openbaarmaking van de namen en het inkomen van werknemers van verscheidene publiekrechtelijke lichamen in een jaarverslag dat ter beschikking werd gesteld van het grote publiek. Een aantal personen weigerde hun gegevens mee te delen op grond van gegevensbescherming.

Het HvJ-EU baseerde zich in zijn arrest op de bescherming van grondrechten als algemeen beginsel van het EU-recht en op artikel 8 van het EVRM, waarbij het in herinnering bracht dat het Handvest op dat moment niet bindend was. Het Hof oordeelde dat het verzamelen van gegevens over het inkomen uit arbeid van een persoon, en met name de mededeling ervan aan derden, in het toepassingsgebied van het recht op eerbiediging van het privéleven valt en een aantasting van dit recht vormt. De inmenging had gerechtvaardigd kunnen zijn indien deze in de wet was neergelegd, een legitieme doelstelling had nagestreefd en in een democratische samenleving noodzakelijk was geweest om dat doel te bereiken. Het HvJ-EU merkte op dat de Oostenrijkse wetgeving inderdaad een legitiem doel nastreefde, te weten het binnen

104 *Ibid.*, punt 89.

105 HvJ-EU, gevoegde zaken C-465/00, C-138/01 en C-139/09, *Rechnungshof/Österreichischer Rundfunk e.a.* en *Christa Neukomm en Joseph Lauermann/Österreichischer Rundfunk*, 20 mei 2003.

redelijke perken houden van de salarissen van overheidspersoneel, dat tevens verband hield met het economisch welzijn van de staat. Het belang van Oostenrijk, echter, bij een optimaal gebruik van de overheidsgelden, moest worden afgewogen tegen de zwaarwichtigheid van de aantasting van het recht op persoonlijke levenssfeer van de betrokken personen.

Terwijl het HvJ-EU het aan de nationale rechter overliet om te bepalen of de publicatie van de gegevens over het inkomen van personen noodzakelijk was en evenredig aan het middels de wetgeving nagestreefde doel, riep het de nationale rechter op na te gaan of een dergelijke doelstelling niet op even doeltreffende wijze had kunnen worden verwezenlijkt op een minder indringende manier. Zo hadden de persoonsgegevens alleen kunnen worden doorgegeven aan de toezichthoudende overheidsdiensten en niet aan het grote publiek.

In latere zaken werd duidelijk dat de afweging tussen gegevensbescherming en toegang tot documenten een gedetailleerd onderzoek van zaak tot zaak vereist. Noch het ene, noch het andere recht heeft automatisch voorrang op het andere. Het HvJ-EU heeft in twee zaken de gelegenheid gehad het recht op toegang tot documenten met persoonsgegevens te interpreteren.

Voorbeeld: In het arrest *Europese Commissie/Bavarian Lager*[106] heeft het HvJ-EU de reikwijdte van de bescherming van persoonsgegevens gedefinieerd in de context van de toegang tot documenten van EU-instellingen en de verhouding tussen Verordening (EG) nr. 1049/2001 (Verordening inzake de toegang tot documenten) en Verordening (EG) nr. 45/2001 (verordening gegevensbescherming EU-instellingen). Bavarian Lager, opgericht in 1992, importeert gebotteld Duits bier in het Verenigd Koninkrijk, voornamelijk voor verkoop in cafés en bars. Daarbij ondervond het bedrijf echter moeilijkheden omdat de Britse autoriteiten nationale producenten *de facto* een voorkeursbehandeling gaven. In reactie op de klacht van Bavarian Lager leidde de Europese Commissie een procedure in tegen het Verenigd Koninkrijk wegens niet-nakoming van zijn verplichtingen, wat ertoe leidde dat de betwiste bepalingen werden aangepast en in overeenstemming met het EU-recht werden gebracht. Vervolgens verzocht Bavarian Lager de Commissie, naast andere documenten, om een kopie van de notulen

106 HvJ-EU, zaak C-28/08 P, *Europese Commissie/The Bavarian Lager Co. Ltd* [Grote kamer], 29 juni 2010.

van een vergadering die was bijgewoond door vertegenwoordigers van de Commissie, de Britse autoriteiten en de *Confédération des Brasseurs du Marché Commun* (CBMC). De Commissie stemde ermee in om bepaalde documenten die verband hielden met de vergadering openbaar te maken, maar maakte vijf namen in de notulen onleesbaar, namelijk van twee personen die uitdrukkelijk bezwaar hadden gemaakt tegen de bekendmaking van hun identiteit en van drie personen die de Commissie niet had weten te bereiken. Bij een besluit van 18 maart 2004 verwierp de Commissie een nieuw verzoek van Bavarian Lager om verkrijging van de volledige notulen van de vergadering, waarbij ze in het bijzonder de bescherming van het privéleven van deze personen als gegarandeerd door de verordening gegevensbescherming EU-instellingen aanvoerde.

Bavarian Lager nam geen genoegen met dit standpunt en maakte een procedure aanhangig bij het Gerecht van eerste aanleg. Dit Gerecht verklaarde het besluit van de Commissie bij arrest van 8 november 2007 nietig (zaak T-194/04, *The Bavarian Lager Co. Ltd/Commissie van de Europese Gemeenschappen*), oordelend dat de loutere vermelding van de namen van de personen in kwestie op de lijst van personen die een vergadering hadden bijgewoond namens het orgaan dat ze vertegenwoordigden, geen aantasting van hun privéleven inhield en de privélevens van deze personen niet in gevaar bracht.

Nadat de Commissie hiertegen beroep had ingesteld, vernietigde het HvJ-EU het arrest van het Gerecht van eerste aanleg. Het HvJ-EU oordeelde dat de Verordening inzake de toegang tot documenten voorziet in "een specifieke en versterkte regeling van bescherming van personen wier persoonsgegevens, in voorkomend geval, openbaar kunnen worden gemaakt". Volgens het HvJ-EU worden, wanneer een verzoek op grond van de Verordening inzake de toegang tot documenten strekt tot het verkrijgen van toegang tot documenten die persoonsgegevens bevatten, de bepalingen van de verordening gegevensbescherming EU-instellingen in volle omvang van toepassing. Het HvJ-EU concludeerde dat de Commissie het verzoek om toegang tot de volledige notulen van de vergadering van oktober 1996 terecht had verworpen. Bij het ontbreken van toestemming van de vijf deelnemers aan die vergadering heeft de Commissie zich in voldoende mate aan haar transparantieverplichting gehouden door een versie van het document waarin hun namen onleesbaar waren gemaakt openbaar te maken.

Bovendien stelde het HvJ-EU dat "[a]angezien Bavarian Lager geen enkele uitdrukkelijke en legitieme rechtvaardigingsgrond en evenmin enig overtuigend argument tot staving van de noodzaak van de doorgifte van deze persoonsgegevens heeft aangevoerd, [...] de Commissie de verschillende belangen van de betrokken partijen niet tegen elkaar [heeft] kunnen afwegen. De Commissie heeft evenmin kunnen nagaan of er geen reden bestond om aan te nemen dat door deze doorgifte de gerechtvaardigde belangen van de betrokkenen worden geschaad", zoals vereist door de verordening gegevensbescherming EU-instellingen.

Voorbeeld: In de zaak *Client Earth en PAN Europe/EFSA*[107] onderzocht het HvJ-EU of de beslissing van de Europese Autoriteit voor voedselveiligheid (EFSA) om verzoekers geen volledige toegang tot documenten te verlenen, noodzakelijk was om het recht op bescherming van de persoonlijke levenssfeer en op gegevensbescherming van de personen op wie de documenten betrekking hadden, te beschermen. De documenten betroffen ontwerprichtsnoeren die door een werkgroep van de EFSA in samenwerking met externe deskundigen waren opgesteld, over het op de markt brengen van gewasbeschermingsmiddelen. In eerste instantie verleende de EFSA de verzoekers gedeeltelijk toegang. Ze weigerde toegang tot een aantal opeenvolgende versies van de ontwerprichtsnoeren. Later verleende ze toegang tot de ontwerpversie waarin de individuele opmerkingen van de externe deskundigen waren opgenomen. Zij had echter de namen van die deskundigen bewerkt, op grond van artikel 4, lid 1, onder b), van Verordening (EG) nr. 45/2001 betreffende de verwerking van persoonsgegevens door EU-instellingen en -organen en de noodzaak de persoonlijke levenssfeer van de deskundigen te beschermen. In eerste aanleg bevestigde het Gerecht het besluit van de EFSA.

Nadat verzoekers hiertegen beroep hadden ingesteld, werd door het HvJ-EU het in eerste aanleg gewezen vonnis herzien. Het Hof concludeerde dat de doorgifte van persoonsgegevens in dit geval noodzakelijk was om de onpartijdigheid van elke externe deskundige in de uitvoering van zijn wetenschappelijke taak na te kunnen gaan en om de transparantie van het besluitvormingsproces binnen de EFSA te waarborgen. Volgens het HvJ-EU had de EFSA niet gespecificeerd hoe bekendmaking van de namen van de

107 HvJ-EU, zaak C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Europese Autoriteit voor voedselveiligheid (EFSA), Europese Commissie*, 16 juli 2015.

externe deskundigen die specifieke opmerkingen hadden gemaakt over de ontwerprichtsnoeren, de gerechtvaardigde belangen van de deskundigen zou schaden. Het algemene argument dat openbaarmaking de persoonlijke levenssfeer kan schaden volstaat niet als het niet wordt gestaafd door concreet bewijs in de zaak in kwestie.

Volgens deze uitspraken is er voor inmenging in het recht op gegevensbescherming in verband met de toegang tot documenten een specifieke en gerechtvaardigde reden nodig. Het recht op toegang tot documenten mag niet automatisch voorrang krijgen boven het recht op gegevensbescherming[108].

Dit standpunt is vergelijkbaar met dat van het EHRM ten aanzien van privacy en toegang tot documenten, zoals het volgende arrest laat zien: In de zaak *Magyar Helsinki* stelde het EHRM dat artikel 10 een persoon niet het recht op toegang tot door een overheidsinstelling bewaarde informatie toekende of de overheid verplichtte tot het verstrekken van dergelijke informatie aan een persoon. Een recht of verplichting als deze zou echter kunnen ontstaan wanneer, ten eerste, bekendmaking van de informatie wordt opgelegd door een gerechtelijk bevel dat rechtsgeldigheid heeft gekregen; ten tweede, wanneer toegang tot de informatie noodzakelijk is voor de uitoefening van iemands recht op vrijheid van meningsuiting, met name de vrijheid kennis te nemen en te geven van informatie, en wanneer ontzegging van de toegang dit recht zou schenden[109]. Of, en in welke mate, de ontzegging van toegang tot informatie een inbreuk op de vrijheid van meningsuiting van een verzoeker inhoudt, moet per geval worden beoordeeld, met inachtneming van de voor dat geval geldende specifieke omstandigheden, zoals: (i) het doel van het verzoek om informatie; (ii) de aard van de gevraagde informatie; (iii) de functie van de aanvrager, en (iv) de vraag of de informatie al gereed en beschikbaar is.

Voorbeeld: In *Magyar Helsinki Bizottság/Hongarije*[110] had verzoekster, een ngo op het gebied van mensenrechten, bij de politie informatie opgevraagd over het werk van pro-Deoadvocaten, teneinde een studie te voltooien naar het functioneren van het systeem van pro-Deoadvocaten in Hongarije. De politie weigerde de informatie te verstrekken, met als argument dat het

108 Zie echter de gedetailleerde beraadslagingen in EDPS (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling*, Brussel, 24 maart 2011.

109 EHRM, *Magyar Helsinki Bizottság/Hongarije* [Grote kamer], nr. 18030/11, 8 november 2016, punt 148.

110 *Ibid.*, punten 181, 187–200.

ging om persoonsgegevens die niet konden worden geopenbaard. Na overweging van de hiervoor genoemde criteria concludeerde het EHRM dat er inbreuk was gemaakt op een bij artikel 10 beschermd recht. Preciezer gezegd: verzoekster wilde haar recht uitoefenen kennis te geven van informatie betreffende een zaak van openbaar belang; zij had met dit doel toegang gevraagd tot informatie, en de informatie was noodzakelijk voor de uitoefening van het recht van verzoekster op vrijheid van meningsuiting. De informatie over de benoeming van pro-Deoadvocaten was van publiek belang. Er was geen reden om eraan te twijfelen dat de desbetreffende studie informatie bevatte die verzoekster had verzameld om door te geven aan het publiek en op de kennisneming waarvan het publiek recht had. Het Hof was er derhalve van overtuigd dat toegang tot de gevraagde informatie voor de aanvraagster noodzakelijk was om haar taak te verrichten. De informatie was bovendien al gereed en beschikbaar.

Het EHRM concludeerde dat de weigering toegang te verlenen tot informatie in dit geval de wezenlijke inhoud van de vrijheid kennis te nemen van informatie had geschonden. Het kwam tot deze conclusie na onderzoek van met name het doel van het verzoek om informatie en de bijdrage ervan aan een belangrijk openbaar debat, de aard van de gevraagde informatie en of het publiek er belang bij had, en de rol van de aanvraagster in deze zaak in de samenleving.

Het Hof merkte in zijn motivering op dat de door de ngo uitgevoerde studie betrekking had op het functioneren van de rechtspraak en het recht op een eerlijk proces, een recht dat een belangrijke plaats inneemt in het EVRM. Aangezien de aangevraagde informatie geen gegevens bevatte van buiten het publieke domein, zouden de privacyrechten van de betrokkenen (de pro-Deoadvocaten) niet negatief zijn beïnvloed als de politie verzoekster toegang tot de informatie had verleend. De door verzoekster aangevraagde informatie was statistisch van aard en betrof het aantal keren dat pro-Deoadvocaten waren aangewezen voor de verdediging van verdachten in openbare strafzaken.

Het Hof oordeelde dat, gezien het feit dat de studie was bedoeld als bijdrage aan een belangrijk debat van publiek belang, elke beperking aan de door de ngo voorgestelde publicatie aan een grondige toetsing had moeten worden onderworpen. De desbetreffende informatie was van algemeen belang. Het algemeen belang omvat "zaken die aanleiding tot aanzienlijke

controverse kunnen geven, die betrekking hebben op een belangrijke maatschappelijke kwestie, of die een probleem betreffen waarbij het publiek er belang bij zou hebben erover geïnformeerd te worden"[111]. Een discussie over het functioneren van het rechtssysteem en eerlijke processen, wat het onderwerp was van de studie van verzoekster, zou dus zeker vallen onder het algemeen belang. Het EHRM oordeelde, na de verschillende rechten tegen elkaar te hebben afgewogen en het evenredigheidsbeginsel in aanmerking te hebben genomen, dat de rechten van verzoekster krachtens artikel 10 van het EVRM waren geschonden.

1.3.2. Beroepsgeheim

In nationale wetgeving kan zijn voorgeschreven dat bepaalde mededelingen zijn onderworpen aan het beroepsgeheim. Onder beroepsgeheim wordt een speciale morele plicht verstaan vanwege welke een wettelijke plicht ontstaat die inherent is aan bepaalde beroepen en functies die zijn gebaseerd op vertrouwen. Personen en instellingen die dergelijke functies vervullen zijn verplicht de vertrouwelijke informatie die tijdens de uitoefening van hun werk aan hen wordt verstrekt, geheim te houden. Het beroepsgeheim geldt in het bijzonder voor medische beroepen en de relatie tussen advocaat en cliënt, terwijl in veel rechtsgebieden tevens de financiële sector gehouden is tot beroepsgeheim. Het beroepsgeheim is geen fundamenteel recht, maar het geniet bescherming als een uitdrukking van het recht op eerbiediging van het privéleven. Het HvJ-EU heeft bijvoorbeeld gesteld dat het "in bepaalde zaken [...] noodzakelijk [kan] zijn te verbieden dat bepaalde als vertrouwelijk aangemerkte gegevens openbaar worden gemaakt, ter vrijwaring van het fundamentele recht van een onderneming op eerbiediging van het privéleven, neergelegd in artikel 8 van het [...] EVRM en in artikel 7 van het Handvest"[112]. Ook het EHRM is verzocht zich uit te spreken over de vraag of beperkingen aan het beroepsgeheim een schending van artikel 8 van het EVRM inhouden, zoals wordt toegelicht in de onderstaande voorbeelden.

111 *Ibid.*, punt 156.

112 HvJ-EU, zaak T-462/12 R, *Pilkington Group Ltd/Europese Commissie*, Beschikking van de president van het Gerecht, 11 maart 2013, punt 44.

Voorbeeld: In de zaak *Pruteanu/Roemenië*[113] trad de verzoeker op als advocaat van een commerciële onderneming die het wegens verdenkingen van fraude was verboden banktransacties uit te voeren. Tijdens het onderzoek van de zaak gaf de Roemeense rechtbank de vervolgingsautoriteiten de bevoegdheid gedurende bepaalde tijd de telefoongesprekken van een van de partners in het bedrijf te onderscheppen en vast te leggen. Een deel van deze opnamen en onderschepte gesprekken betroffen gesprekken met zijn advocaat.

De heer Pruteanu voerde aan dat dit inbreuk maakte op het recht op eerbiediging van zijn privéleven en zijn communicatie. Het EHRM benadrukte in zijn vonnis de status en het belang van de relatie tussen advocaat en zijn of haar cliënt. Het onderscheppen van de gesprekken van een advocaat met zijn cliënt vormde zonder twijfel een schending van het beroepsgeheim waarop de relatie tussen deze twee personen was gebaseerd. In dergelijke gevallen zou de advocaat zich ook kunnen beklagen over inbreuk op het recht op eerbiediging van zijn privéleven en zijn communicatie. Het Hof concludeerde dat artikel 8 van het EVRM was geschonden.

Voorbeeld: In *Brito Ferrinho Bexiga Villa-Nova/Portugal*[114] weigerde de klaagster, die advocaat is, haar persoonlijke bankafschriften aan de belastingdienst te overleggen op grond van het beroepsgeheim en het bankgeheim. Het openbaar ministerie opende een onderzoek naar belastingfraude en verzocht om toestemming om het beroepsgeheim tijdelijk op te heffen. Nationale rechters bevalen opschorting van het bank- en beroepsgeheim op de grond dat het algemene belang voorrang moest krijgen op de persoonlijke belangen van verzoekster.

Toen de zaak bij het EHRM terechtkwam oordeelde het Hof dat het toegang verkrijgen tot de bankafschriften van klaagster een inmenging inhield van haar recht op eerbiediging van het beroepsgeheim, dat valt onder de persoonlijke levenssfeer. De inmenging had weliswaar een rechtsgrondslag, omdat ze gebaseerd was op het wetboek van strafvordering en een rechtmatig doel diende. Na onderzoek van de noodzakelijkheid en evenredigheid van de inmenging wees het EHRM echter op het feit dat de procedure ter opheffing van het bank- en beroepsgeheim was uitgevoerd

113 EHRM, *Pruteanu/Roemenië*, nr. 30181/05, 3 februari 2015.

114 EHRM, *Brito Ferrinho Bexiga Villa-Nova/Portugal*, nr. 69436/10, 1 december 2015.

zonder medewerking of inkennisstelling van verzoekster. Zij was derhalve niet in de gelegenheid gesteld haar argumenten aan te voeren. Bovendien was de vereniging van advocaten, die volgens de nationale wet diende te worden geraadpleegd in het geval van dergelijke procedures, niet geraadpleegd. Tot slot werd de klaagster niet de mogelijkheid geboden op een effectieve manier beroep in te stellen tegen de opheffing van het bank- en beroepsgeheim, of op enige andere wijze de maatregel te opponeren. Wegens het ontbreken van procedurele waarborgen en doeltreffende rechterlijke toetsing van de maatregel tot opschorting van de geheimhoudingsplicht, concludeerde het EHRM dat er sprake was van een inbreuk op artikel 8 van het EVRM.

De wisselwerking tussen het beroepsgeheim en gegevensbescherming is vaak ambivalent. Enerzijds dragen de in de wetgeving vastgelegde regels en waarborgen voor gegevensbescherming bij aan het verzekeren van het beroepsgeheim. Zo is regelgeving waarin verwerkers en voor de verwerking verantwoordelijken worden verplicht robuuste maatregelen voor gegevensbeveiliging te nemen onder meer bedoeld om te garanderen dat door beroepsgeheim beschermde persoonsgegevens vertrouwelijk blijven. Tevens maakt de algemene verordening gegevensbescherming de verwerking van medische gegevens, een speciale categorie persoonsgegevens waarvoor extra bescherming aangewezen is, mogelijk, maar wordt hieraan de voorwaarde gesteld dat er passende en specifieke maatregelen zijn getroffen ter bescherming van de rechten van betrokkenen, in het bijzonder het beroepsgeheim[115].

Anderzijds kunnen de verplichtingen met betrekking tot het beroepsgeheim die aan verwerkers en voor de verwerking verantwoordelijken worden gesteld in verband met bepaalde persoonsgegevens de rechten van betrokkenen beperken, met name het recht op het kennisnemen van informatie. Hoewel de algemene verordening gegevensbescherming een uitgebreide lijst bevat met informatie die, in beginsel, aan een betrokkene moet worden verstrekt wanneer persoonsgegevens niet van hem of haar zijn verkregen, is dit vereiste van kennisgeving niet van toepassing wanneer de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Unierecht of lidstatelijk recht[116].

115 Algemene verordening gegevensbescherming, artikel 9, lid 2, onder h), en artikel 9, lid 3.

116 *Ibid.*, artikel 14, lid 5, onder d).

De algemene verordening gegevensbescherming (AVG) voorziet in de mogelijkheid dat lidstaten bij wet specifieke voorschriften invoeren om het beroepsgeheim of andere gelijkaardige geheimhoudingsverplichtingen te waarborgen en het recht op bescherming van persoonsgegevens in overeenstemming te brengen met het beroepsgeheim[117].

De AVG bepaalt dat lidstaten specifieke voorschriften mogen invoeren betreffende de bevoegdheden van toezichthoudende autoriteiten met betrekking tot verwerkers en verwerkingsverantwoordelijken die zijn onderworpen aan het beroepsgeheim. Het gaat om specifieke regels die verband houden met de bevoegdheid toegang te verkrijgen tot de bedrijfsruimte van een verwerkingsverantwoordelijke of een verwerker, diens gegevensverwerkingapparatuur en de opgeslagen persoonsgegevens, wanneer dergelijke persoonsgegevens zijn ontvangen gedurende de uitvoering van een activiteit die valt onder het beroepsgeheim. De toezichthoudende autoriteit die met gegevensbescherming is belast moet bijgevolg het beroepsgeheim waaraan verwerkingsverantwoordelijken en verwerkers zijn gehouden, eerbiedigen. Bovendien zijn de leden van toezichthoudende autoriteiten zelf ook gedurende en na afloop van hun ambtstermijn onderworpen aan het beroepsgeheim. Tijdens de uitoefening van hun taken nemen leden en medewerkers van toezichthoudende autoriteiten mogelijk kennis van vertrouwelijke informatie. In artikel 54, lid 2, van de verordening is duidelijk bepaald dat ze met betrekking tot dergelijke vertrouwelijke informatie gehouden zijn aan het beroepsgeheim.

De AVG schrijft voor dat lidstaten de Commissie in kennis stellen van de voorschriften die zij aannemen om de gegevensbescherming en de in de verordening neergelegde beginselen te verzoenen met het beroepsgeheim.

1.3.3. Vrijheid van godsdienst en overtuiging

De vrijheid van godsdienst en overtuiging wordt beschermd op grond van artikel 9 van het EVRM (vrijheid van gedachte, geweten en godsdienst) en artikel 10 van het EU-Handvest van de grondrechten. Persoonsgegevens waaruit iemands godsdienstige of levensbeschouwelijke overtuiging blijkt, worden zowel in het EU-recht als in het RvE-recht beschouwd als "gevoelige gegevens", en de verwerking en het gebruik ervan zijn onderworpen aan extra bescherming.

117 *Ibid.*, overweging 164 en artikel 90.

Voorbeeld: De verzoeker in de zaak *Sinan Işık/Turkije*[118] was lid van de alevitische geloofsgemeenschap. Het geloof van deze gemeenschap is beïnvloed door het soefisme en andere, pre-islamitische geloven en wordt door sommigen beschouwd als een afzonderlijke godsdienst. Volgens anderen behoort het tot de islam. De klacht van verzoeker betrof het feit dat zijn identiteitskaart tegen zijn wil een vakje bevatte waarin zijn godsdienst werd aangeduid als "islam" in plaats van "alevitisme". De nationale rechtbanken verworpen zijn verzoek de beschrijving op zijn identiteitskaart te wijzigen in "alevitisme" op de grond dat met dat woord een subgroep van de islam werd aangeduid en niet een afzonderlijke religie. Hij diende vervolgens een klacht in bij het EHRM over het feit dat hij was verplicht zijn geloof bekend te maken, zonder dat hij hiervoor toestemming had gegeven, vanwege de verplichting om de godsdienst van personen op hun identiteitskaart te vermelden, en dat dit een schending van zijn recht op vrijheid van godsdienst en geweten inhield, in het bijzonder gezien het feit dat de aanduiding "islam" op zijn identiteitskaart onjuist was.

Het EHRM herhaalde dat godsdienstvrijheid onder meer bestaat uit de vrijheid een godsdienst te belijden met anderen, in het openbaar of met een groep personen die hetzelfde geloof aanhangen, maar tevens alleen en in een privéomgeving. De nationale wetgeving die destijds van toepassing was schreef voor dat iedereen een identiteitskaart bij zich droeg waarop zijn of haar godsdienst was vermeld en dit document toonde als hierom door een overheidsinstelling of particuliere onderneming werd verzocht. Met deze verplichting werd over het hoofd gezien dat iemands recht op het tot uitdrukking brengen van zijn of haar geloof tevens het tegenovergestelde inhoudt, namelijk het recht niet verplicht te zijn persoonlijke overtuigingen bekend te maken. De regering voerde weliswaar aan dat de nationale wetgeving was gewijzigd en personen inmiddels konden verzoeken het vakje voor godsdienst op hun identiteitskaart leeg te laten, maar volgens het Hof kon louter het feit dat om verwijdering van de godsdienst moest worden verzocht, betekenen dat informatie over iemands houding ten opzichte van religie werd bekendgemaakt. Bovendien heeft het leeglaten van een godsdienstvakje op een identiteitskaart een bijzondere connotatie, aangezien houders van een identiteitskaart zonder informatie over godsdienst op

118 EHRM, *Sinan Işık/Turkije*, nr. 21924/05, 2 februari 2010.

zullen vallen ten opzichte van anderen van wie de kaart wel een godsdienst vermeldt. Het EHRM concludeerde dat de nationale wetgeving in strijd was met artikel 9 van het EVRM.

Het kan echter voor kerken en geloofsverenigingen en -gemeenschappen nodig zijn persoonsgegevens van hun leden te verwerken, zodat binnen de congregatie met elkaar kan worden gecommuniceerd en activiteiten kunnen worden georganiseerd. Veel kerken en religieuze verenigingen hebben derhalve regels ingevoerd voor de verwerking van persoonsgegevens. Artikel 91 van de algemene verordening gegevensbescherming bepaalt dat deze, wanneer het uitgebreide voorschriften betreft, kunnen blijven gelden, mits ze in overeenstemming worden gebracht met de bepalingen van de verordening. Kerken en religieuze verenigingen die dergelijke regels hanteren, moeten zijn onderworpen aan toezicht door een onafhankelijke toezichthoudende autoriteit. Dit kan een specifiek op hen gerichte autoriteit zijn, op voorwaarde dat ze voldoet aan de voorwaarden die voor dergelijke autoriteiten worden gesteld in de algemene verordening gegevensbescherming[119].

Religieuze verenigingen kunnen persoonsgegevens verwerken voor verschillende doeleinden: bijvoorbeeld om contact te houden met leden van de congregatie of informatie mee te delen over activiteiten, religieuze of liefdadigheidsevenementen en festiviteiten die ze organiseren. In bepaalde lidstaten moeten kerken een register van hun leden aanhouden om belastingredenen, omdat lidmaatschap van een religieuze organisatie daar invloed kan hebben op de hoeveelheid belasting die iemand verschuldigd is. Hoe dan ook zijn gegevens waaruit iemands geloofsovertuiging blijkt volgens het Europese recht gevoelige gegevens, en kerken moeten rekenschap afleggen over hun behandeling en verwerking van die gegevens, met name omdat de door religieuze organisaties verwerkte informatie vaak betrekking heeft op kinderen, ouderen of andere kwetsbare leden van de samenleving.

1.3.4. Vrijheid van kunsten en wetenschappen

Een ander recht waartegen het recht op eerbiediging van het privéleven en het recht op gegevensbescherming moeten worden afgewogen is het recht van vrijheid van kunsten en wetenschappen, dat uitdrukkelijk wordt beschermd door artikel 13 van het Handvest van de grondrechten van de EU. Dit recht is hoofdzakelijk afgeleid uit het recht van vrijheid van gedachte en meningsuiting en moet worden

119 Algemene verordening gegevensbescherming, artikel 91, lid 2.

uitgeoefend met inachtneming van artikel 1 van het Handvest (menselijke waardigheid). Het EHRM is van oordeel dat de vrijheid van kunsten wordt beschermd krachtens artikel 10 van het EVRM[120]. Ook aan het krachtens artikel 13 van het Handvest gegarandeerde recht kunnen beperkingen worden gesteld op grond van artikel 52, lid 1, van het Handvest, dat tevens kan worden geïnterpreteerd in het licht van artikel 10, lid 2, van het EVRM[121].

Voorbeeld: In *Vereinigung bildender Künstler/Oostenrijk*[122] hadden de Oostenrijkse rechtbanken de verzoekende vereniging verboden om een schilderij tentoon te stellen dat foto's bevatte van de hoofden van verschillende publieke figuren op lichamen in seksuele posities. Een Oostenrijkse parlementariër, van wie een foto was gebruikt in het schilderij, maakte een procedure aanhangig tegen de verzoekende vereniging waarin hij om een verbod op de tentoonstelling van het schilderij vroeg. De nationale rechtbank vaardigde een verbod uit. Het EHRM herhaalde dat artikel 10 van het EVRM ook van toepassing is op de communicatie van ideeën die de staat of een deel van de bevolking beledigen, schokken of verontrusten. Personen die kunstwerken creëren, uitvoeren, verspreiden of tentoonstellen, dragen bij tot de uitwisseling van ideeën en opinies, en de staat heeft de verplichting om hun vrijheid van meningsuiting niet te veel aan te tasten. Aangezien het schilderij een collage was waarin alleen gebruik werd gemaakt van foto's van de hoofden van personen, terwijl hun lichamen op onrealistische en overdreven wijze waren geschilderd, waarmee duidelijk niet werd beoogd de werkelijkheid weer te geven of zelfs maar te suggereren, bepaalde het EHRM voorts dat "het schilderij moeilijk kan worden gezien als een weergave van details van het privéleven [van de afgebeelde persoon], maar betrekking heeft op zijn publieke statuur als politicus" en dat de afgebeelde persoon "in deze hoedanigheid een grotere tolerantie tegenover kritiek tentoon dient te spreiden". Na een afweging van de verschillende belangen die in het geding waren oordeelde het EHRM dat het onbegrensde verbod op de verdere tentoonstelling van het schilderij onevenredig was. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 10 van het EVRM.

120 EHRM, *Müller e.a./Zwitserland*, nr. 10737/84, 24 mei 1988.

121 Toelichtingen bij het Handvest van de grondrechten, PB C 303 van 14.12.2007.

122 EHRM, *Vereinigung bildender Künstler/Oostenrijk*, nr. 68345/01, 25 januari 2007, punten 26 en 34.

De Europese gegevensbeschermingswetgeving erkent tevens de bijzondere waarde van de wetenschap voor de samenleving. De algemene verordening gegevensbescherming en het Gemoderniseerd Verdrag 108 staan toe dat gegevens langer worden bewaard zolang de persoonsgegevens enkel worden verwerkt voor wetenschappelijk of historisch onderzoek. Voorts moet, ongeacht het oorspronkelijke doel van een specifieke verwerkingsactiviteit, het verdere gebruik van persoonsgegevens voor wetenschappelijk onderzoek niet als een onverenigbaar doel worden beschouwd[123]. Tegelijkertijd moeten noodzakelijke waarborgen voor dergelijke verwerkingen worden ingevoerd om de rechten en vrijheden van betrokkenen te beschermen. In EU- of lidstatelijke wetgeving kunnen derogaties van de rechten van betrokkenen worden vastgesteld, zoals bijvoorbeeld het recht op toegang, rectificatie of beperking van de verwerking, en op bezwaarmaking tegen de verwerking van persoonsgegevens voor wetenschappelijk onderzoek of historische of statistische doeleinden (zie ook paragraaf 6.1 en paragraaf 9.4).

1.3.5. Bescherming van intellectuele eigendom

Het recht op bescherming van eigendom is vervat in artikel 1 van Protocol nr. 1 bij het EVRM en ook in artikel 17, lid 1, van het Handvest van de grondrechten van de EU. Een belangrijk aspect van het eigendomsrecht dat in het bijzonder van belang is in verband met gegevensbescherming is de bescherming van intellectuele eigendom, die uitdrukkelijk wordt genoemd in artikel 17, lid 2, van het Handvest. In de rechtsorde van de EU beogen diverse richtlijnen een doeltreffende bescherming van intellectuele eigendom, en met name van het auteursrecht. Intellectuele eigendom omvat niet alleen literaire en artistieke eigendom, maar ook octrooi-, merken- en aanverwante rechten.

Zoals de jurisprudentie van het HvJ-EU duidelijk heeft gemaakt, moet de bescherming van het grondrecht op eigendom worden afgewogen tegen de bescherming van andere grondrechten, in het bijzonder het recht op gegevensbescherming[124]. Er zijn gevallen geweest waar instellingen ter bescherming van het auteursrecht eisten dat aanbieders van internettoegang de identiteit van gebruikers van platforms die bestanden delen op het internet, bekendmaken. Dergelijke platforms maken het voor internetgebruikers vaak mogelijk om gratis muziek te downloaden, ook al berust er op deze werken auteursrecht.

123 Algemene verordening gegevensbescherming, artikel 5, lid 1, onder b), en Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder b).

124 HvJ-EU, zaak C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [Grote kamer], 29 januari 2008, punten 62-68.

Voorbeeld: De zaak *Promusicae/Telefónica de España*[125] had betrekking op de weigering van een Spaanse internetaanbieder, Telefónica, om Promusicae, een organisatie zonder winstoogmerk van muziekproducenten en uitgevers van muziek- en audiovisuele opnamen, de persoonsgegevens te verstrekken van bepaalde personen aan wie Telefónica internettoegangsdiensten leverde. Promusicae verzocht om bekendmaking van de informatie teneinde civiele procedures te kunnen aanspannen tegen deze personen, die volgens Promusicae gebruikmaakten van een programma voor de uitwisseling van bestanden dat toegang bood tot muzieknummers waarvan de exploitatierechten toebehoorden aan leden van Promusicae.

De Spaanse rechter had de zaak verwezen naar het HvJ-EU met de vraag of deze persoonsgegevens krachtens het communautaire recht, in het kader van een civiele procedure, moesten worden meegedeeld om een doeltreffende bescherming van het auteursrecht te verzekeren. Daarbij verwees de verwijzende rechter naar de Richtlijnen 2000/31/EG, 2001/29/EG en 2004/48/EG, mede gelezen in het licht van de artikelen 17 en 47 van het Handvest. Het HvJ-EU concludeerde dat deze drie richtlijnen, evenals de e-Privacy-richtlijn (Richtlijn 2002/58/EG), de lidstaten niet beletten om een verplichting op te leggen om in het kader van een civiele procedure persoonsgegevens mee te delen teneinde een doeltreffende bescherming van het auteursrecht te verzekeren.

Het HvJ-EU wees erop dat de zaak derhalve de vraag opwierp hoe de vereisten van de bescherming van verschillende grondrechten met elkaar moesten worden verzoend, namelijk het recht op eerbiediging van het privéleven, het recht op bescherming van eigendom en het recht op een doeltreffende voorziening in rechte.

Het Hof concludeerde dat "[b]ij de omzetting van bovengenoemde richtlijnen [...] de lidstaten niettemin erop [moeten] toezien dat zij zich baseren op een uitlegging daarvan die het mogelijk maakt een juist evenwicht tussen de verschillende door de communautaire rechtsorde beschermde grondrechten te verzekeren. Bij de tenuitvoerlegging van de maatregelen ter omzetting van deze richtlijnen moeten de autoriteiten en de rechterlijke instanties van de lidstaten vervolgens niet alleen hun nationale recht conform deze richtlijnen uitleggen, maar er ook op toezien dat zij zich niet baseren op

125 *Ibid.*, punten 54 en 60.

een uitlegging van deze richtlijnen die in conflict zou komen met deze grondrechten of de andere algemene beginselen van gemeenschapsrecht, zoals het evenredigheidsbeginsel"[126].

Voorbeeld: De zaak *Bonnier Audio AB e.a./Perfect Communication Sweden AB*[127] had betrekking op het evenwicht tussen intellectuele-eigendomsrechten en de bescherming van persoonsgegevens. De verzoekers, vijf uitgeverijen die de auteursrechten op 27 luisterboeken bezaten, hadden een rechtszaak aangespannen bij een Zweedse rechtbank, waarin zij stelden dat hun auteursrechten waren geschonden via een ftp-server (een bestandsoverdrachtprotocol dat de uitwisseling van bestanden en de overdracht van gegevens via internet mogelijk maakt). Verzoekers hadden de internetaanbieder (isp) verzocht om de mededeling van naam en adres van de gebruiker van het IP-adres vanwaar de bestanden waren verstuurd. De isp, ePhone, verweerde zich tegen de vordering door aan te voeren dat deze in strijd was met Richtlijn 2006/24/EG (de richtlijn gegevensbewaring, die in 2014 ongeldig is verklaard).

De Zweedse rechtbank verwees de zaak naar het HvJ-EU, met de vraag of Richtlijn 2006/24/EG in de weg stond aan de toepassing van een op artikel 8 van Richtlijn 2004/48/EG (richtlijn betreffende de handhaving van intellectuele-eigendomsrechten) gebaseerde nationale bepaling, volgens welke een isp kan worden gelast auteursrechthouders informatie te verstrekken over abonnees van wie het IP-adres gebruikt zou zijn om inbreuk te plegen. Bij deze vraag werd uitgegaan van de veronderstelling dat de verzoeker een duidelijk bewijs van de inbreuk op een bepaald auteursrecht had overgelegd en de maatregel in overeenstemming was met het evenredigheidsbeginsel.

Het Hof wees erop dat Richtlijn 2006/24/EG enkel van toepassing was op de verwerking en de bewaring van door aanbieders van elektronische communicatiediensten gegenereerde gegevens voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit en de verstrekking ervan aan de bevoegde nationale autoriteiten. Bijgevolg valt een nationale bepaling ter omzetting van de richtlijn betreffende de handhaving van

126 *Ibid.*, punten 65 en 68; zie ook HvJ-EU, zaak C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*, 16 februari 2012.

127 HvJ-EU, zaak C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB/Perfect Communication Sweden AB*, 19 april 2012.

intellectuele-eigendomsrechten buiten de werkingssfeer van Richtlijn 2006/24/EG en staat deze richtlijn niet in de weg aan een dergelijke bepaling[128].

Het HvJ-EU oordeelde dat de door verzoekers gevraagde mededeling van naam en adres een verwerking van persoonsgegevens vormt en valt binnen de werkingssfeer van Richtlijn 2002/58/EG (e-Privacy-richtlijn). Voorts merkte het Hof op dat om de mededeling van deze gegevens was gevraagd in een civielrechtelijke procedure, ten voordele van de auteursrechthouder en ter verzekering van de doeltreffende bescherming van auteursrechten, en dat de mededeling derhalve wegens het voorwerp ervan tevens binnen de werkingssfeer van Richtlijn 2004/48/EG viel[129].

Het Hof van Justitie concludeerde dat Richtlijnen 2002/58/EG en 2004/48/EG aldus moeten worden uitgelegd dat ze niet in de weg staan aan een nationale wettelijke regeling als die in het hoofdgeding, voor zover deze regeling de nationale rechterlijke instantie waarbij een verzoek om een bevel tot mededeling van persoonsgegevens is ingediend, in staat stelt om de in het geding zijnde tegengestelde belangen af te wegen op basis van de concrete omstandigheden van de zaak en daarbij terdege rekening te houden met de uit het evenredigheidsbeginsel voortvloeiende vereisten.

1.3.6. Gegevensbescherming en economische belangen

In het digitale tijdperk, of het tijdperk van big data, worden gegevens wel de "nieuwe olie" van de economie genoemd omdat innovatie en creativiteit erdoor worden gestimuleerd[130]. Vele bedrijven hebben stabiele businessmodellen opgesteld omtrent gegevensverwerking, en een dergelijke verwerking heeft vaak betrekking op persoonsgegevens. Er zijn mogelijk ondernemingen die geloven dat bepaalde regels in verband met de bescherming van persoonsgegevens in de praktijk kunnen leiden tot bovenmatig belastende verplichtingen die hun economische belangen zouden kunnen schaden. De vraag doet zich dan ook voor of beperkingen

128 *Ibid.*, punt 40-41.

129 *Ibid.*, punten 52-54. Zie ook HvJ-EU, zaak C-275/06, *Productores de Música de España (Promusicae)/ Telefónica de España SAU* [Grote kamer], 29 januari 2008, punt 58.

130 Zie bijvoorbeeld: *Financial Times* (2016), "Data is the new oil… who's going to own it?", 16 november 2016.

aan het recht op gegevensbescherming zouden kunnen worden gerechtvaardigd door de economische belangen van verwerkers en verwerkingsverantwoordelijken, of van het algemene publiek.

Voorbeeld: In *Google Spain*[131] oordeelde het HvJ-EU dat natuurlijke personen onder bepaalde omstandigheden het recht hebben van de exploitant van een zoekmachine te eisen dat zoekresultaten uit de resultatenlijst worden verwijderd. In zijn motivering wees het Hof op het feit dat middels het gebruik van zoekmachines en de vermelde zoekresultaten een gedetailleerd profiel van een persoon kan worden opgesteld. De gevonden informatie kan betrekking hebben op tal van aspecten van iemands privéleven en zou zonder zoekmachine niet eenvoudig zijn gevonden of met elkaar in verband zijn gebracht. Er was hier derhalve sprake van een potentieel ernstige inmenging in het recht van betrokkenen op eerbiediging van de persoonlijke levenssfeer en bescherming van persoonsgegevens.

Het Hof heeft vervolgens onderzocht of de inmenging kon worden gerechtvaardigd. Wat het economische belang van de zoekmachine-exploitant bij het uitvoeren van de verwerking betreft, stelde het HvJ-EU over de inmenging dat "moet worden vastgesteld dat zij niet kan worden gerechtvaardigd door louter het economisch belang dat de exploitant van een dergelijke zoekmachine bij deze verwerking heeft", en dat "in beginsel" de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten voorrang krijgen op een dergelijk economisch belang en het belang van het publiek om deze informatie te vinden wanneer op de naam van de betrokken persoon wordt gezocht[132].

Een van de belangrijkste overwegingen bij de Europese gegevensbeschermingswetgeving is om natuurlijke personen meer controle te geven over hun persoonsgegevens. Met name in het huidige digitale tijdperk is er een gebrek aan evenwicht tussen de macht van ondernemingen die toegang hebben tot grote hoeveelheden persoonsgegevens en deze verwerken, en de mogelijkheden van de personen op wie die gegevens betrekking hebben tot zeggenschap over deze informatie. Het HvJ-EU beoordeelt van geval tot geval het evenwicht tussen gegevensbescherming

131 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 13 mei 2014.

132 *Ibid.*, punten 81 en 97.

en economische belangen, zoals de belangen van derden ten aanzien van vennootschappen op aandelen en vennootschappen met beperkte aansprakelijkheid, wat wordt geïllustreerd door het arrest-*Manni*.

Voorbeeld: De zaak *Manni*[133] betrof de opname van de persoonsgegevens van een natuurlijke persoon in een openbaar handelsregister. De heer Manni had de Kamer van Koophandel van Lecce verzocht zijn persoonsgegevens uit het handelsregister te schrappen, nadat hij had ontdekt dat potentiële klanten die het register zouden raadplegen, zouden zien dat hij bestuurder was geweest van een bedrijf dat meer dan tien jaar eerder failliet was verklaard. Potentiële klanten werden door deze informatie beïnvloed en dit zou een negatief effect kunnen hebben op zijn zakelijke belangen.

Het HvJ-EU werd verzocht om na te gaan of een recht tot verwijdering in een dergelijk geval in het Unierecht is erkend. Het Hof maakte een afweging tussen enerzijds de EU-regels voor gegevensbescherming en het economische belang van de heer Manni bij het verwijderen van informatie over het faillissement van zijn eerdere onderneming en anderzijds het belang van het publiek bij toegang tot de informatie. Het nam nota van het feit dat opname in het openbaar handelsregister bij wet was voorgeschreven, in het bijzonder een EU-richtlijn waarmee wordt beoogd de toegang tot bedrijfsinformatie eenvoudiger te maken voor derden. De openbaarmaking was belangrijk met het oog op de bescherming van de belangen van derden die mogelijk zaken willen doen met een bepaalde onderneming, omdat vennootschappen op aandelen en vennootschappen met beperkte aansprakelijkheid aan derden geen andere waarborg bieden dan het vermogen van de vennootschap. "De openbaarmaking moet derden dan ook in de gelegenheid stellen kennis te nemen van de voornaamste akten van de vennootschap en van bepaalde gegevens die haar betreffen, met name de identiteit van de personen die de bevoegdheid hebben haar te verbinden"[134].

Gezien het belang van het gerechtvaardigde doeleinde van het register, oordeelde het HvJ-EU dat de heer Manni niet het recht had uitwissing van zijn persoonsgegevens te verkrijgen, daar de noodzaak de belangen van derden

133 HvJ-EU, zaak C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 maart 2017.

134 *Ibid.*, punt 49.

ten aanzien van vennootschappen op aandelen en vennootschappen met beperkte aansprakelijkheid te beschermen en rechtszekerheid te bieden, de eerlijkheid van handelstransacties en dus het goede functioneren van de interne markt prevaleerden boven zijn in de gegevensbeschermingswetgeving neergelegde rechten. Dit gold des te meer omdat natuurlijke personen die ervoor kiezen om aan het economisch verkeer deel te nemen met behulp van een vennootschap op aandelen of een vennootschap met beperkte aansprakelijkheid op de hoogte zijn van de verplichting de gegevens met betrekking tot hun identiteit en taken openbaar te maken.

Hoewel het HvJ-EU in dit geval geen gronden zag voor het verkrijgen van uitwissing, erkende het wel het bestaan van een recht van verzet tegen de verwerking. Het Hof merkte op dat: "niet valt uit te sluiten dat er uitzonderlijke situaties kunnen zijn waarin zwaarwegende en gerechtvaardigde redenen die verband houden met het specifieke geval van de betrokkene, bij wijze van uitzondering rechtvaardigen dat de toegang tot de hem betreffende persoonsgegevens in het register, na verloop van een voldoende lange termijn [...] wordt beperkt tot derden die een aantoonbaar belang hebben bij inzage in die gegevens"[135].

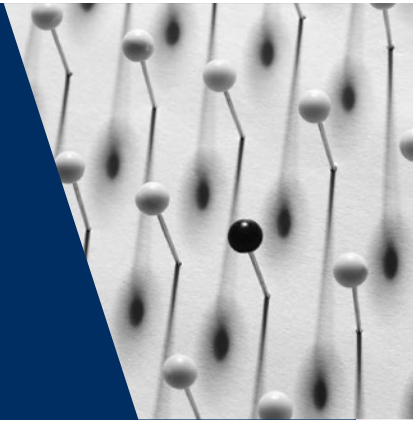
Het HvJ-EU verklaarde dat het aan de nationale rechterlijke instanties is om in elke zaak te beoordelen, rekening houdend met alle relevante omstandigheden van de betrokkene, of er rechtmatige en dwingende redenen bestaan die, bij wijze van uitzondering, beperking van de toegang van derden tot persoonsgegevens in handelsregisters kunnen rechtvaardigen. Het verduidelijkte evenwel dat in de zaak van de heer Manni het loutere feit dat de openbaarmaking van zijn persoonsgegevens in het register zijn klanten zou beïnvloeden, niet kon worden beschouwd als een rechtmatige en dwingende reden. Potentiële klanten van de heer Manni hebben er rechtmatig belang bij om toegang te krijgen tot de informatie over het faillissement van zijn eerdere vennootschap.

De inbreuk op het door de artikelen 7 en 8 van het Handvest gewaarborgde fundamentele recht van de heer Manni en anderen in het register op eerbiediging van het privéleven en bescherming van persoonsgegevens diende een algemeen belang en was noodzakelijk en evenredig.

135 *Ibid.*, punt 60.

In de zaak *Manni* concludeerde het HvJ-EU dan ook dat het recht op gegevensbescherming en op privacy niet prevaleerden boven het belang van derden bij toegang tot de informatie in het handelsregister met betrekking tot vennootschappen op aandelen en vennootschappen met beperkte aansprakelijkheid.

2 Gegevensbeschermings-terminologie



EU	Behandelde onderwerpen	RvE
Persoonsgegevens		
Algemene verordening gegevensbescherming, artikel 4, punt 1 Algemene verordening gegevensbescherming, artikel 4, punt 5 en artikel 5, lid 1, onder e) Algemene verordening gegevensbescherming, artikel 9 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert/Land Hessen* [Grote kamer], 2010 HvJ-EU, zaak C-275/06, *Productores de Música de España (Promusicae)/ Telefónica de España SAU* [Grote kamer], 2008 HvJ-EU, zaak C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 HvJ-EU, zaak C-582/14, *Patrick Breyer/ Bundesrepublik Deutschland*, 2016 HvJ-EU, gevoegde zaken C-141/12 en C/372/12, *Y.S./Minister voor Immigratie, Integratie en Asiel* en *Minister voor Immigratie, Integratie en Asiel/M. en S.*, 2014	**Wettelijke definitie van gegevens-bescherming**	Gemoderniseerd Verdrag 108, artikel 2, onder a) EHRM, *Bernh Larsen Holding AS e.a./ Noorwegen*, nr. 24117/08, 2013 EHRM, *Uzun/Duitsland*, nr. 35623/05, 2010 EHRM, *Amann/ Zwitserland* [Grote kamer], nr. 27798/95, 2000

EU	Behandelde onderwerpen	RvE
HvJ-EU, zaak C-101/01, *Strafzaak tegen Bodil Lindqvist*, 2003	**Bijzondere categorieën persoonsgegevens (gevoelige gegevens)**	Gemoderniseerd Verdrag 108, artikel 6, lid 1
HvJ-EU, zaak C-434/16, *Peter Nowak/Data Protection Commissioner*, 2017	**Geanonimiseerde en gepseudonimiseerde persoonsgegevens**	Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder e) Memorie van toelichting bij Gemoderniseerd Verdrag 108, paragraaf 50
Gegevensverwerking		
Algemene verordening gegevensbescherming, artikel 4, punt 2 HvJ-EU, zaak C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 2014 HvJ-EU, zaak C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 2017 HvJ-EU, zaak C-101/01, *Strafzaak tegen Bodil Lindqvist*, 2003 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 2014	**Definities**	Gemoderniseerd Verdrag 108, artikel 2, onder b) en c)
Gebruikers van gegevens		
Algemene verordening gegevensbescherming, artikel 4, punt 7 HvJ-EU, zaak C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 2014 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 2014	**Verwerkingsverantwoordelijke**	Gemoderniseerd Verdrag 108, artikel 2, onder d) Aanbeveling inzake profilering, artikel 1, onder g)*

EU	Behandelde onderwerpen	RvE
Algemene verordening gegevensbescherming, artikel 4, punt 8	Verwerker	Gemoderniseerd Verdrag 108, artikel 2, onder f) Aanbeveling inzake profilering, artikel 1, onder h)
Algemene verordening gegevensbescherming, artikel 4, punt 9	Ontvanger	Gemoderniseerd Verdrag 108, artikel 2, onder e)
Algemene verordening gegevensbescherming, artikel 4, punt 10	Derde	
Toestemming		
Algemene verordening gegevensbescherming, artikel 4, punt 11 en artikel 7 HvJ-EU, zaak C-543/09, *Deutsche Telekom AG/Bondsrepubliek Duitsland*, 2011 HvJ-EU, zaak C-536/15, *Tele2 (Netherlands) BV e.a./Autoriteit Consument en Markt (ACM)*, 2017	Definitie en vereisten voor geldige toestemming	Gemoderniseerd Verdrag 108, artikel 5, lid 2 Aanbeveling inzake medische gegevens, artikel 6, en verschillende daaropvolgende aanbevelingen EHRM, *Elberte/Letland*, nr. 61243/08, 2015

**Raad van Europa, Comité van Ministers (2010), Aanbeveling CM/Rec(2010)13 aan de lidstaten inzake de bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens in de context van profilering (aanbeveling inzake profilering), 23 november 2010.*

2.1. Persoonsgegevens

Belangrijkste punten

- Gegevens zijn persoonsgegevens indien ze betrekking hebben op een geïdentificeerde of identificeerbare persoon, de "betrokkene".
- Om te bepalen of een natuurlijke persoon identificeerbaar is, moet door een verwerkingsverantwoordelijke of een andere persoon rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.
- Onder authenticatie wordt verstaan: bewijzen dat een bepaalde persoon een bepaalde identiteit heeft en/of is gemachtigd om bepaalde activiteiten te verrichten.

- Er zijn bijzondere categorieën gegevens, de zogeheten gevoelige gegevens, die worden genoemd in het Gemoderniseerd Verdrag 108 en in de EU-wetgeving inzake gegevensbescherming, die een betere bescherming vereisen en daarom onder een speciale wettelijke regeling vallen.
- Gegevens zijn geanonimiseerd als ze niet langer in verband kunnen worden gebracht met een geïdentificeerde of identificeerbare persoon.
- Pseudonimisering is een maatregel waarmee ervoor wordt gezorgd dat persoonsgegevens niet kunnen worden gekoppeld aan de betrokkene zonder over extra gegevens te beschikken, die apart worden bewaard. De "sleutel" die de betrokkene weer identificeerbaar maakt moet apart en veilig worden bewaard. Gegevens die een pseudonimiseringsproces hebben ondergaan blijven persoonsgegevens. In het EU-recht komen "gepseudonimiseerde gegevens" niet voor als begrip.
- De beginselen en voorschriften op het gebied van gegevensbescherming zijn niet van toepassing op geanonimiseerde gegevens. Ze gelden echter wel voor gepseudonimiseerde gegevens.

2.1.1. Belangrijkste aspecten van het begrip persoonsgegevens

Zowel **in het EU-recht** als **in het RvE-recht** wordt het begrip "persoonsgegevens" gedefinieerd als informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon[136]. Het betreft informatie over een persoon van wie de identiteit ofwel volkomen duidelijk is, ofwel kan worden vastgesteld door aanvullende informatie te verkrijgen. Om te bepalen of iemand identificeerbaar is, moet door een verwerkingsverantwoordelijke of een andere persoon rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon direct of indirect te identificeren, zoals selectietechnieken, waarmee een verschillende behandeling voor afzonderlijke personen mogelijk wordt gemaakt[137].

Als gegevens over een dergelijke persoon worden verwerkt, wordt die persoon "de betrokkene" genoemd.

136 Algemene verordening gegevensbescherming, artikel 4, punt 1; Gemoderniseerd Verdrag 108, artikel 2, onder a).

137 Algemene verordening gegevensbescherming, overweging 26.

De betrokkene

De gegevensbeschermingsvoorschriften **in het EU-recht** gelden alleen voor natuurlijke personen[138] en alleen levende personen worden door het Europese gegevensbeschermingsrecht beschermd[139]. De algemene verordening gegevensbescherming (AVG) definieert "persoonsgegevens" als: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Het RvE-recht, in het bijzonder het Gemoderniseerd Verdrag 108, verwijst eveneens naar de bescherming van natuurlijke personen met betrekking tot de verwerking van hun persoonsgegevens. Ook daarin wordt onder persoonsgegevens verstaan: iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Deze natuurlijke persoon, waarop zowel de AVG als het Gemoderniseerd Verdrag 108 betrekking hebben, wordt in de gegevensbeschermingswetgeving aangeduid als "de betrokkene".

Daarnaast genieten ook rechtspersonen enige bescherming. Er bestaat jurisprudentie van het EHRM waarin het Hof een oordeel heeft gegeven over verzoeken van rechtspersonen die schending van hun recht op bescherming tegen het gebruik van hun gegevens krachtens artikel 8 van het EVRM aanvoeren. Artikel 8 van het EHRM heeft zowel betrekking op het recht op eerbiediging van privé- en gezinsleven als op eerbiediging van woning en correspondentie. Het Hof kan derhalve zaken onderzoeken op grond van dit laatste recht in plaats van het recht op privéleven.

> Voorbeeld: Het arrest *Bernh Larsen Holding AS e.a./Noorwegen*[140] had betrekking op een klacht van drie Noorse ondernemingen over een besluit van een belastingautoriteit dat hen verplichtte om de belastinginspecteurs een kopie te verstrekken van alle gegevens op een computerserver die zij gezamenlijk gebruikten.
>
> Het EHRM oordeelde dat een dergelijke verplichting voor de verzoekende ondernemingen inmenging in hun rechten op eerbiediging van de "woning" en de "correspondentie" als bedoeld in artikel 8 van het EVRM vormde.

138 *Ibid.*, artikel 1.

139 *Ibid.*, overweging 27. Zie ook Groep artikel 29 (2007), *Advies 4/2007 over het begrip persoonsgegeven*, WP 136, 20 juni 2007, blz. 22.

140 EHRM, *Bernh Larsen Holding AS e.a./Noorwegen*, nr. 24117/08, 14 maart 2013. Zie echter ook EHRM, *Liberty e.a./Verenigd Koninkrijk*, nr. 58243/00, 1 juli 2008.

Het Hof oordeelde echter ook dat de belastingautoriteiten doeltreffende en toereikende waarborgen tegen misbruik hadden toegepast: de verzoekende ondernemingen waren ruim van tevoren geïnformeerd; ze waren aanwezig bij de interventie ter plaatse en konden tijdens de interventie opmerkingen maken, en het materiaal zou worden vernietigd zodra de belastingcontrole was voltooid. In dergelijke omstandigheden was een redelijk evenwicht bereikt tussen het recht van de verzoekende ondernemingen op eerbiediging van de woning en de correspondentie en hun belang om de privacy van personen die voor hen werkten te beschermen, enerzijds, en het algemeen belang van een efficiënte inspectie voor belastingcontroledoeleinden anderzijds. Het Hof concludeerde dat er geen inbreuk op artikel 8 had plaatsgevonden.

Volgens het Gemoderniseerd Verdrag 108 heeft gegevensbescherming in de eerste plaats betrekking op de bescherming van natuurlijke personen; de verdragspartijen kunnen de gegevensbescherming krachtens hun nationale recht niettemin uitbreiden tot rechtspersonen, zoals ondernemingen en verenigingen. In de memorie van toelichting bij Gemoderniseerd Verdrag wordt gesteld dat de gerechtvaardigde belangen van rechtspersonen kunnen worden beschermd middels nationale regelingen door de werkingssfeer van het Verdrag tot dergelijke actoren uit te breiden[141]. De **EU-wetgeving inzake gegevensverwerking** heeft geen betrekking op de verwerking van gegevens over rechtspersonen en met name als rechtspersonen gevestigde ondernemingen, zoals de naam en de rechtsvorm van de rechtspersoon en de contactgegevens[142]. De e-Privacy-richtlijn beschermt echter wel het vertrouwelijke karakter van communicatie en de gerechtvaardigde belangen van rechtspersonen in verband met de toenemende mogelijkheden voor de geautomatiseerde opslag en verwerking van gegevens met betrekking tot de abonnees en de gebruikers[143]. Evenzo wordt in het voorstel voor de e-Privacy-verordening de bescherming uitgebreid tot rechtspersonen.

141 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 30.

142 Algemene verordening gegevensbescherming, overweging 14.

143 e-Privacy-richtlijn, overweging 7 en artikel 1, lid 2.

Voorbeeld: In *Volker und Markus Schecke en Hartmut Eifert/Land Hessen*[144] oordeelde het HvJ-EU, met betrekking tot de publicatie van persoonsgegevens van begunstigden van landbouwsteun, dat "rechtspersonen ter zake van een dergelijke vermelding evenwel slechts beroep [kunnen] doen op de door de artikelen 7 en 8 van het Handvest geboden bescherming voor zover uit de officiële naam van de rechtspersoon de identiteit van een of meer natuurlijke personen blijkt. [...D]e eerbiediging van het in de artikelen 7 en 8 van het Handvest erkende recht op persoonlijke levenssfeer bij de verwerking van persoonsgegevens betreft elke informatie aangaande een geïdentificeerde of identificeerbare natuurlijke persoon [...]"[145].

Na afweging van het belang van de EU bij het verzekeren van transparantie met betrekking tot de toekenning van steun enerzijds en de fundamentele rechten op het gebied van privacy en gegevensbescherming van de personen die de steun hadden ontvangen anderzijds, oordeelde het HvJ-EU dat de inbreuk op deze grondrechten onevenredig was. Het Hof stelde dat de doelstelling van transparantie doeltreffend had kunnen worden verwezenlijkt met maatregelen die voor de betrokken personen een minder ingrijpende aantasting van voormeld fundamenteel recht hadden meegebracht. Na onderzoek naar de evenredigheid van het publiceren van gegevens van rechtspersonen die steun ontvingen, concludeerde het HvJ-EU evenwel dat een dergelijke publicatie de grenzen van het evenredigheidsbeginsel niet overschreed. Het verklaarde: "De ernst van de aantasting van het recht op bescherming van de persoonsgegevens verschilt immers naar gelang het gaat om rechtspersonen dan wel om natuurlijke personen"[146]. Rechtspersonen waren onderworpen aan een ruimere verplichting om hen betreffende gegevens bekend te maken. Het HvJ-EU stelde dat de verplichting voor nationale autoriteiten om, voorafgaand aan de bekendmaking van de gegevens met betrekking tot iedere steun ontvangende rechtspersoon, te onderzoeken of uit die gegevens de identiteit van betrokken natuurlijke personen blijkt, deze autoriteiten een bovenmatig grote administratieve last zou opleggen. De wetgeving die de algemene bekendmaking van gegevens betreffende rechtspersonen voorschrijft, nam derhalve een rechtvaardig evenwicht in acht tussen de conflicterende belangen.

144 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert/Land Hessen* [Grote kamer], 9 november 2010, punt 53.

145 *Ibid.*, punten 52–53.

146 *Ibid.*, punt 87.

Aard van de gegevens

Elk type informatie kan persoonsgegevens omvatten, mits de informatie betrekking heeft op een geïdentificeerde of identificeerbare persoon.

Voorbeeld: Een beoordeling van het functioneren van een werknemer door een leidinggevende, opgeslagen in het personeelsdossier van de werknemer, is een persoonsgegeven van de werknemer. Dit geldt ook als de beoordeling slechts — geheel of gedeeltelijk — de persoonlijke mening van de leidinggevende weergeeft, zoals: "de werknemer is niet toegewijd aan zijn/haar werk", en het geen weergave van harde feiten betreft, zoals: "de werknemer is in de afgelopen zes maanden gedurende vijf weken niet op zijn/haar werk aanwezig geweest".

Het begrip "persoonsgegevens" heeft betrekking op informatie die behoort tot het privéleven van een persoon, waaronder begrepen beroepsactiviteiten, en op informatie over zijn of haar openbare leven.

In de zaak *Amann*[147] heeft het EHRM het begrip persoonsgegevens zodanig uitgelegd dat het zich niet strikt beperkt tot de persoonlijke levenssfeer van een natuurlijke persoon. Deze betekenis van het begrip persoonsgegevens is ook relevant voor de AVG.

Voorbeeld: In *Volker und Markus Schecke en Hartmut Eifert/Land Hessen*[148] heeft het HvJ-EU bepaald dat het "irrelevant [is] dat de bekendgemaakte gegevens verband houden met beroepsactiviteiten [...]. Het Europees Hof voor de Rechten van de Mens heeft in dat verband betreffende de interpretatie van artikel 8 van het EVRM geoordeeld dat de term "persoonlijke levenssfeer" niet eng moet worden uitgelegd en dat om geen enkele principiële reden de beroepsactiviteiten [...] van het begrip "persoonlijke levenssfeer" kunnen worden uitgesloten".

147 Zie EHRM, *Amann/Zwitserland*, nr. 27798/95, 16 februari 2000, punt 65.

148 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert/Land Hessen* [Grote kamer], 9 november 2010, punt 59.

Voorbeeld: In de gevoegde zaken *Y.S./Minister voor Immigratie, Integratie en Asiel* en *Minister voor Immigratie, Integratie en Asiel/M. en S*[149]. stelde het HvJ-EU dat de juridische analyse in het ontwerpbesluit van de Immigratie- en Naturalisatiedienst, waar aanvragen van verblijfstitels worden behandeld, niet als zodanig kan worden betiteld als persoonsgegevens, ondanks het feit dat er persoonsgegevens in kunnen zijn opgenomen.

De jurisprudentie van het EHRM over artikel 8 van het EVRM bevestigt dat het moeilijk kan zijn om privé- en beroepsleven volledig van elkaar te scheiden[150].

Voorbeeld: In *Bărbulescu/Roemenië*[151] was de verzoeker ontslagen omdat hij tijdens werkuren gebruik had gemaakt van het internet van zijn werkgever, wat in strijd was met de interne voorschriften. Zijn werkgever had zijn communicatie gemonitord en toonde gedurende het proces bij de nationale rechtbanken de afschriften hiervan, die berichten van louter persoonlijke aard lieten zien. Het EHRM oordeelde dat artikel 8 van toepassing was en liet daarmee de vraag open of de verzoeker gezien de beperkende voorschriften van de werkgever een redelijke mate van privacy had kunnen verwachten. Het oordeelde echter hoe dan ook dat de voorschriften van een werkgever het persoonlijke sociale leven van werknemers op de werkplek niet volledig konden uitsluiten. Wat de gegrondheid betreft, moest de verdragsluitende staten een ruime beoordelingsmarge worden verleend bij het bepalen van de noodzaak tot vaststelling van een rechtskader ter regulering van de voorwaarden onder welke een werkgever de niet-werkgerelateerde communicatie van werknemers — in elektronische of andere vorm — op de werkplek mag reglementeren. Niettemin moesten de nationale autoriteiten verzekeren dat de invoering door werkgevers van maatregelen ter monitoring van correspondentie en andere communicatie, ongeacht de omvang en duur van dergelijke maatregelen, vergezeld ging van passende en voldoende waarborgen tegen misbruik. Evenredigheid en procedurele waarborgen tegen willekeur zijn essentiële voorwaarden en het EHRM stelde een aantal factoren vast die in de gegeven omstandigheden van belang waren. Dit waren bijvoorbeeld: de omvang van de monitoring

149 HvJ-EU, gevoegde zaken C-141/12 en C/372/12, *Y.S./Minister voor Immigratie, Integratie en Asiel* en *Minister voor Immigratie, Integratie en Asiel/M. en S.*, 17 juli 2014, punt 39.

150 Zie bijvoorbeeld EHRM, *Rotaru/Roemenië* [Grote kamer], nr. 28341/95, 4 mei 2000, punt 43; EHRM, *Niemietz/Duitsland*, nr. 13710/88, 16 december 1992, punt 29.

151 EHRM, *Bărbulescu/Roemenië* [Grote kamer], nr. 61496/08, 5 september 2017, punt 121.

van werknemers door de werkgever en de mate waarin inbreuk wordt gepleegd op de privacy van de werknemer, de consequenties voor de werknemer en de vraag of in adequate waarborgen werd voorzien. Nationale autoriteiten moesten er bovendien voor zorgen dat een werknemer wiens communicatie was gemonitord toegang had tot een rechtsmiddel bij een rechterlijke instantie die bevoegd was te bepalen in hoeverre, in ieder geval in beginsel, de genoemde criteria in acht waren genomen en of de betwiste maatregelen rechtmatig waren. In deze zaak oordeelde het EVRM dat artikel 8 was geschonden omdat de nationale autoriteiten de verzoeker geen adequate bescherming hadden geboden van het recht op eerbiediging van zijn privéleven en zijn communicatie en daardoor geen rechtvaardig evenwicht tussen de verschillende belangen hadden verzekerd.

Zowel **krachtens het EU-recht** als **krachtens het RvE-recht** bevat informatie gegevens over een persoon indien:

- een natuurlijke persoon wordt geïdentificeerd of identificeerbaar is door deze informatie, of

- een natuurlijke persoon, hoewel niet geïdentificeerd, door deze informatie kan worden onderscheiden op een wijze die het mogelijk maakt om vast te stellen wie de betrokkene is door verder onderzoek te doen.

Deze beide typen informatie worden in de Europese gegevensbeschermingswetgeving op dezelfde wijze beschermd. Om de directe of indirecte identificeerbaarheid van personen te kunnen bepalen, is een voortdurende beoordeling nodig, "met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen"[152]. Het EHRM heeft herhaaldelijk opgemerkt dat het begrip "persoonsgegevens" als bedoeld in het EVRM identiek is aan dit begrip als bedoeld in Verdrag 108, met name wat betreft de voorwaarde dat de informatie betrekking moet hebben op geïdentificeerde of identificeerbare personen[153].

In de AVG is bepaald dat een natuurlijke persoon identificeerbaar is wanneer hij of zij "direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online

152 Algemene verordening gegevensbescherming, overweging 26.

153 Zie EHRM, *Amann/Zwitserland* [Grote kamer], nr. 27798/95, 16 februari 2000, punt 65.

identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon"[154]. Identificatie vereist daarom elementen die een persoon zo beschrijven dat hij/zij van alle andere personen kan worden onderscheiden en als een individu kan worden herkend. Een duidelijk voorbeeld van een dergelijk beschrijvend element is de naam van een persoon, waarmee een persoon direct geïdentificeerd kan worden. In sommige gevallen kunnen andere kenmerken een vergelijkbaar effect hebben als een naam en een persoon indirect identificeerbaar maken. Een telefoonnummer, socialezekerheidsnummer of voertuigregistratienummer zijn voorbeelden van informatie die ervoor kunnen zorgen dat een persoon identificeerbaar is. Het is ook mogelijk om personen te onderscheiden door met gebruikmaking van hulpmiddelen zoals computerbestanden, cookies en bewakingsinstrumenten voor het webverkeer hun gedrag en gewoonten te achterhalen. Zoals Groep artikel 29 in een advies heeft verduidelijkt: "[z]onder zelfs maar naar de naam en het adres van de persoon te vragen, kan de betrokkene worden ingedeeld aan de hand van sociaaleconomische, psychologische, filosofische of andere criteria en kunnen bepaalde beslissingen aan hem of haar worden toegeschreven, omdat het voor het contactpunt voor de persoon (de computer) niet langer nodig is zijn of haar identiteit in enge zin bekend te maken"[155]. De definitie van persoonsgegevens is zowel in het RvE-recht als het EU-recht dermate ruim dat het alle mogelijke manieren van identificatie (en derhalve elke mate van identificeerbaarheid) bestrijkt.

Voorbeeld: In de zaak *Promusicae/Telefónica de España*[156] stelde het HvJ-EU dat "niet [wordt] betwist dat de door Promusicae gevorderde mededeling van de naam en het adres van bepaalde gebruikers van [naam van het internetplatform voor het delen van bestanden] impliceert dat persoonsgegevens ter beschikking worden gesteld, dat wil zeggen — volgens de definitie van artikel 2, onder a), van Richtlijn 95/46/EG [thans: artikel 4, punt 1, van de algemene verordening gegevensbescherming] — informatie betreffende geïdentificeerde of identificeerbare natuurlijke

154 Algemene verordening gegevensbescherming, artikel 4, punt 1.

155 Groep gegevensbescherming artikel 29, *Advies 4/2007 over het begrip persoonsgegeven*, WP 136, 20 juni 2007, blz. 15.

156 HvJ-EU, zaak C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [Grote kamer], 29 januari 2008, punt 45.

personen [...]. Deze verstrekking van informatie die volgens Promusicae door Telefónica wordt opgeslagen — wat deze laatste niet betwist — vormt een verwerking van persoonsgegevens [...]"[157].

Voorbeeld: De zaak *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] had betrekking op de weigering van internetaanbieder Scarlet om een systeem in te voeren waarbij elektronische communicatie die via bestandsdelingssoftware werd verricht, werd gefilterd om te voorkomen dat bestanden werden uitgewisseld in strijd met door SABAM, een beheersmaatschappij die auteurs, componisten en uitgevers vertegenwoordigt, beschermde auteursrechten. Het HvJ-EU oordeelde: "[a]angezien die IP-adressen de precieze identificatie van die gebruikers mogelijk maken, vormen zij beschermde persoonsgegevens".

Omdat veel namen niet uniek zijn, kunnen voor de identificatie van een persoon aanvullende identificatiemiddelen nodig zijn om ervoor te zorgen dat een persoon niet wordt verward met iemand anders. Soms kan het nodig zijn directe en indirecte identificatiemiddelen te combineren om de persoon op wie de informatie betrekking heeft te kunnen identificeren. Vaak worden daarvoor de geboortedatum en -plaats gebruikt. Daarnaast zijn in enkele landen gepersonaliseerde nummers ingevoerd om beter onderscheid tussen burgers te kunnen maken. Overgedragen belastinggegevens[159], gegevens van een aanvrager van een verblijfstitel in een administratief document[160], en documenten betreffende bancaire en fiduciaire betrekkingen[161] kunnen persoonsgegevens zijn. Biometrische gegevens, zoals vingerafdrukken, digitale foto's of irisscans, locatiegegevens en online identificatiemiddelen worden in het technologische tijdperk steeds vaker gebruikt om personen te identificeren.

Voor de toepasselijkheid van de Europese gegevensbeschermingswetgeving is daadwerkelijke identificatie van de betrokkene evenwel niet noodzakelijk; het is voldoende dat de desbetreffende persoon identificeerbaar is. Een persoon wordt

157 Voormalige Richtlijn 95/46/EG, artikel 2, onder b), thans algemene verordening gegevensbescherming, artikel 4, punt 2.

158 HvJ-EU, zaak C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 november 2011, punt 51.

159 HvJ-EU, zaak C-201/14, *Smaranda Bara e.a./Casa Națională de Asigurări de Sănătate e.a.*, 1 oktober 2015.

160 HvJ-EU, *Y.S./Minister voor Immigratie, Integratie en Asiel* en *Minister voor Immigratie, Integratie en Asiel/M. en S.*, 17 juli 2014.

161 EHRM, *M.N. e.a./San Marino*, nr. 28005/12, 7 juli 2015.

identificeerbaar geacht als voldoende elementen aanwezig zijn aan de hand waarvan de persoon direct of indirect kan worden geïdentificeerd[162]. Volgens overweging 26 van de AVG bestaat de maatstaf hierin of middelen waarvan mag worden aangenomen dat zij redelijkerwijs kunnen worden ingezet om genoemde persoon te identificeren, beschikbaar zijn voor en zullen worden gebruikt door de voorziene gebruikers van de informatie; hier onder valt ook informatie waarover derde ontvangers beschikken (zie paragraaf 2.3.2).

Voorbeeld: Een lokale autoriteit besluit om gegevens te verzamelen over auto's die te snel rijden in lokale straten. De auto's worden gefotografeerd, waarbij automatisch de tijd en de locatie worden geregistreerd, om de gegevens vervolgens door te geven aan de bevoegde autoriteit, zodat deze boetes kan opleggen aan de snelheidsovertreders. Een betrokkene dient een klacht in en voert daarin aan dat de lokale autoriteit krachtens de gegevensbeschermingswetgeving niet beschikt over een rechtsgrondslag voor deze gegevensverzameling. De lokale autoriteit stelt dat zij geen persoonsgegevens verzamelt. Volgens de lokale autoriteit zijn kentekens van auto's anoniem. De lokale autoriteit is wettelijk niet bevoegd om het voertuigenregister in te zien om achter de identiteit van de eigenaar of bestuurder van de auto te komen.

Deze redenering is niet in overeenstemming met overweging 26 van de AVG. Aangezien het doel van de gegevensverzameling duidelijk is om snelheidsovertreders te identificeren en te beboeten, kan worden voorzien dat een poging tot identificatie zal worden gedaan. Hoewel de lokale autoriteiten niet beschikken over directe identificatiemiddelen, zullen zij de gegevens overdragen aan de bevoegde autoriteit, de politie, die die middelen wel heeft. Overweging 26 omvat uitdrukkelijk een scenario waarin kan worden voorzien dat een latere ontvanger van de gegevens, die niet de onmiddellijke gebruiker is, kan proberen de persoon te identificeren. In het licht van overweging 26 staat het handelen van de lokale autoriteit gelijk aan het verzamelen van gegevens over identificeerbare personen en is er daarom een rechtsgrondslag krachtens de gegevensbeschermingswetgeving nodig.

Om "uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden

162 Algemene verordening gegevensbescherming, artikel 4, punt 1.

gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen"[163].

Voorbeeld: In *Breyer/Bundesrepublik Deutschland*[164] onderzocht het HvJ-EU het begrip indirecte identificeerbaarheid van betrokkenen. Het ging in deze zaak om dynamische IP-adressen, die bij elke nieuwe verbinding met het internet worden gewijzigd. Bij bezoek aan door Duitse federale instellingen beheerde websites werden dynamische IP-adressen geregistreerd en bewaard teneinde cyberaanvallen af te weren en waar nodig strafvervolging mogelijk te maken. Alleen de heer Breyers internetprovider beschikte over de extra gegevens die nodig waren om hem te identificeren.

Het HvJ-EU oordeelde dat een dynamisch IP-adres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als een persoon een website bezoekt die door deze aanbieder toegankelijk is gemaakt voor het publiek, een persoonsgegeven vormt wanneer enkel een derde, in casu de internetprovider van die persoon, beschikt over de extra informatie die nodig is om die persoon te identificeren[165]. Het was van oordeel dat "het [...] immers niet vereist [is] dat alle informatie aan de hand waarvan de betrokkene kan worden geïdentificeerd bij een en dezelfde persoon berust" opdat informatie een persoonsgegeven vormt. Gebruikers van dynamische IP-adressen die door een internetaanbieder worden geregistreerd kunnen onder bepaalde omstandigheden met behulp van derden worden geïdentificeerd, bijvoorbeeld in het kader van strafvervolging in het geval van cyberaanvallen[166]. Het Hof stelde dat, wanneer de aanbieder "beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust", dit "een middel vormt waarvan mag worden aangenomen dat het redelijkerwijs kan worden ingezet om de betrokken persoon te identificeren". Dergelijke gegevens worden derhalve beschouwd als persoonsgegevens.

163 *Ibid.*, overweging 26.

164 HvJ-EU, zaak C-582/14, *Patrick Breyer/Bundesrepublik Deutschland*, 19 oktober 2016, punten 47-48.

165 Voormalige Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, artikel 2, onder a).

166 HvJ-EU, zaak C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 november 2011, punten 47-48.

In het RvE-recht wordt het begrip identificeerbaarheid op soortgelijke wijze begrepen. De memorie van toelichting bij het Gemoderniseerd Verdrag 108 bevat een vergelijkbare beschrijving: het begrip "identificeerbaar" verwijst niet alleen naar de burgerlijke of wettelijke identiteit als zodanig, maar tevens naar datgene waarmee een bepaalde persoon kan worden "geïndividualiseerd" of onderscheiden van anderen, en ten gevolge hiervan mogelijk afwijkend zal worden behandeld. Deze individualisering zou bijvoorbeeld kunnen plaatsvinden door specifiek naar hem of haar te verwijzen, of naar een apparaat of een aantal gerelateerde apparaten (computer, mobiele telefoon, camera, spelletjessystemen enz.), op basis van een identificatienummer, een pseudoniem, biometrische of genetische gegevens, locatiegegevens, een IP-adres of een ander identificatiemiddel[167]. Een natuurlijke persoon wordt niet identificeerbaar geacht indien voor zijn of haar identificatie een bovenmatige hoeveelheid tijd, moeite of middelen zou moeten worden aangewend. Hiervan is bijvoorbeeld sprake wanneer voor het identificeren van een betrokkene buitensporig gecompliceerde, langdurige en kostbare verrichtingen nodig zouden zijn. Er moet van geval tot geval worden beoordeeld of de benodigde tijd, moeite of middelen bovenmatig zijn, waarbij factoren zoals het doel van de verwerking, de kosten en het belang van de identificatie, het type verwerkingsverantwoordelijke en de gebruikte technologie in aanmerking worden genomen[168].

Het is belangrijk op te merken dat de vorm waarin de persoonsgegevens worden opgeslagen of gebruikt niet relevant is voor de toepasselijkheid van de gegevensbeschermingswetgeving. Schriftelijke of mondelinge mededelingen kunnen persoonsgegevens bevatten, evenals afbeeldingen[169], met inbegrip van beeldmateriaal van gesloten televisiecircuits[170] of geluid(en)[171]. Ook elektronisch vastgelegde informatie en informatie op papier kan persoonsgegevens bevatten. Zelfs celmonsters van menselijk weefsel — waarin het DNA van een persoon is vastgelegd — kunnen een bron zijn waaruit biometrische gegevens worden afgeleid[172], zolang de gege-

167 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 18.

168 *Ibid.*, punt 17.

169 EHRM, *Von Hannover/Duitsland*, nr. 59320/00, 24 juni 2004; EHRM, *Sciacca/Italië*, nr. 50774/99, 11 januari 2005; HvJ-EU, zaak C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 december 2014.

170 EHRM, *Peck/Verenigd Koninkrijk*, nr. 44647/98, 28 januari 2003; EHRM, *Köpke/Duitsland* (dec.), nr. 420/07, 5 oktober 2010; EDPS (2010), *The EDPS video-surveillance guidelines*, 17 maart 2010.

171 EHRM, *P.G. en J.H./Verenigd Koninkrijk*, nr. 44787/98, 25 september 2001, punten 59-60; EHRM, *Wisse/Frankrijk*, nr. 71611/01, 20 december 2005 (Franse taalversie).

172 Zie Groep artikel 29 (2007), *Advies 4/2007 over het begrip persoonsgegeven*, WP 136, 20 juni 2007, blz. 9; Raad van Europa, Aanbeveling Rec(2006)4 van het Comité van Ministers aan de lidstaten over het onderzoek aan biologische materialen van menselijke oorsprong, 15 maart 2006.

vens verband houden met de overgeërfde of verworven genetische kenmerken van die persoon, unieke informatie verschaffen over de fysiologie of de gezondheid van de persoon en voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon[173].

Anonimisering

Volgens het beginsel van de beperking van de opslag in zowel de algemene verordening gegevensbescherming als het Gemoderniseerd Verdrag 108 (meer in detail besproken in hoofdstuk 3), moeten gegevens worden bewaard "in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer dan nodig is voor de doelen waarvoor de persoonsgegevens worden verwerkt"[174]. Als gevolg hiervan zouden gegevens moeten worden gewist of geanonimiseerd indien een verwerkingsverantwoordelijke ze wil opslaan nadat ze niet langer nodig zijn en niet langer hun oorspronkelijke doeleinde dienen.

Het proces van het anonimiseren van gegevens houdt in dat alle te identificeren elementen worden verwijderd uit een geheel van persoonsgegevens, zodat de betrokkene niet meer identificeerbaar is[175]. In zijn Advies 05/2014 analyseert Groep artikel 29 de doeltreffendheid en grenzen van verschillende anonimiseringstechnieken[176]. Zij erkent de potentiële waarde van deze technieken, maar benadrukt dat bepaalde technieken niet noodzakelijkerwijs werken in alle gevallen. Om de optimale oplossing te vinden in een bepaalde situatie moet het passende proces van anonimisering per geval worden beslist. Identificatie moet onherroepelijk worden voorkomen, ongeacht de toegepaste techniek. Dit betekent dat de informatie in geanonimiseerde gegevens geen enkel element meer mag bevatten dat, door redelijke inspanningen te verrichten, kan dienen om de betrokken perso(o)n(en) opnieuw te identificeren[177]. Het risico van de nieuwe identificatie kan worden beoordeeld door rekening te houden met "de tijd, moeite of middelen die nodig zijn in het

173 Algemene verordening gegevensbescherming, artikel 4, punt 13.

174 *Ibid.*, artikel 5, lid 1, onder e); Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder e).

175 Algemene verordening gegevensbescherming, overweging 26.

176 Groep artikel 29 (2014), *Advies 05/2014 betreffende anonimiseringstechnieken*, WP 216, 10 april 2014.

177 Algemene verordening gegevensbescherming, overweging 26.

licht van de aard van de gegevens, in het kader van het gebruik ervan, de beschikbare technologieën voor de nieuwe identificatie en aanverwante kosten"[178].

Wanneer gegevens met succes anoniem worden gemaakt, vormen zij niet langer persoonsgegevens en is de wetgeving inzake gegevensbescherming niet langer van toepassing.

De algemene verordening gegevensbescherming bepaalt dat de persoon of organisatie die de controle uitoefent over de verwerking van persoonsgegevens, niet kan worden verplicht om aanvullende informatie ter identificatie van de betrokkene te handhaven, te verwerven of te verwerken uitsluitend ten behoeve van de naleving van de verordening. Deze regel heeft evenwel een belangrijke afwijking: telkens wanneer de betrokkene, met het oog op de uitoefening van het recht op toegang, rectificatie, uitwissing, beperking van de verwerking en de overdraagbaarheid van gegevens, nadere informatie verstrekt aan de verwerkingsverantwoordelijke om zijn identificatie mogelijk te maken, worden de gegevens die eerder werden geanonimiseerd opnieuw persoonsgegevens[179].

Persoonsgegevens pseudonimiseren

Persoonlijke informatie bevat gegevenskenmerken zoals naam, geboortedatum, geslacht, adres, of andere elementen die kunnen leiden tot identificatie. Het proces van pseudonimisering van persoonsgegevens houdt in dat deze eigenschappen worden vervangen door een pseudoniem.

Het Unierecht definieert "pseudonimisering" als "het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld"[180]. In tegenstelling tot geanonimiseerde gegevens zijn gepseudonimiseerde gegevens nog steeds persoonsgegevens en dus onderworpen aan de wetgeving inzake gegevensbescherming. Hoewel pseudonimisering de risico's voor

178 Raad van Europa, Comité voor Verdrag 108 (2017), *Richtsnoeren betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens in een wereld van "Big Data"*, 23 januari 2017, punt 6.2.

179 Algemene verordening gegevensbescherming, artikel 11.

180 *Ibid.*, artikel 4, lid 5.

de beveiliging van betrokkenen kan verminderen, valt deze techniek niet buiten het toepassingsgebied van de algemene verordening gegevensbescherming.

De algemene verordening gegevensbescherming erkent diverse toepassingen van het pseudonimiseren van persoonsgegevens als een gepaste technische maatregel om de gegevensbescherming te versterken, en wordt specifiek vermeld voor het ontwerp en de beveiliging van zijn gegevensverwerking[181]. Het is ook een passende waarborg die kan worden gebruikt om persoonsgegevens te verwerken voor andere doeleinden dan die waarvoor ze oorspronkelijk werden verzameld[182].

Persoonsgegevens pseudonimiseren wordt niet expliciet vermeld in de juridische definitie van het Gemoderniseerd Verdrag 108 van de **RvE**. De memorie van toelichting bij het Gemoderniseerd Verdrag 108 stelt echter duidelijk dat "het gebruik van een pseudoniem of van een digitale identificator/digitale identiteit niet leidt tot de anonimisering van de gegevens, aangezien de betrokkene nog kan worden geïdentificeerd of geïndividualiseerd"[183]. Eén manier om gegevens te pseudonimiseren is via de versleuteling van gegevens. Zodra de betreffende gegevens zijn gepseudonimiseerd, is de link naar een identiteit opgenomen in de vorm van een pseudoniem, vermeerderd met een sleutel voor decryptie. Zonder een dergelijke sleutel is het moeilijk om gepseudonimiseerde gegevens te achterhalen. Echter, voor diegenen die het recht hebben gebruik te maken van de sleutel voor decryptie, is een nieuwe identificatie gemakkelijk te bekomen. Er moet met name worden voorkomen dat onbevoegde personen versleutelingscodes gebruiken. Derhalve moeten "[p]seudonimeuze gegevens [...] beschouwd worden als persoonsgegevens [...]" en vallen onder het Gemoderniseerd Verdrag 108[184].

Authenticatie

Authenticatie is een procedure die een persoon in staat stelt te bewijzen dat hij of zij een bepaalde identiteit heeft en/of gemachtigd is om bepaalde handelingen te verrichten, zoals een beveiligd gebied betreden of geld van een bankrekening opnemen. Authenticatie kan worden gerealiseerd door het vergelijken van biometrische gegevens, zoals een foto of vingerafdrukken in een paspoort, met de gegevens

181 *Ibid.*, artikel 25, lid 1.

182 *Ibid.*, artikel 6, lid 4.

183 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 18.

184 *Ibid.*

die de persoon zelf presenteert, bijvoorbeeld bij een immigratiecontrole[185], of door informatie op te vragen die alleen bekend zou moeten zijn bij de persoon met een bepaalde identiteit of machtiging, zoals een persoonlijk identificatienummer (PIN) of een wachtwoord, of door te vereisen dat de persoon een bepaald "token" presenteert dat exclusief in het bezit is van de persoon met een bepaalde identiteit of machtiging, zoals een speciale chipkaart of de sleutel van een bankkluis. Naast wachtwoorden en chipkaarten, soms in combinatie met een PIN, vormen elektronische handtekeningen een bijzonder geschikt instrument om een persoon in een elektronische communicatieomgeving te identificeren.

2.1.2. Bijzondere categorieën persoonsgegevens

Zowel in het Unierecht als in **het RvE-recht** zijn er bijzondere categorieën persoonsgegevens die, gezien hun aard, een risico voor de betrokkene kunnen vormen wanneer ze worden verwerkt en die daarom beter moeten worden beschermd. Deze gegevens zijn onderworpen aan een verbodsbeginsel en er zijn een beperkt aantal omstandigheden waarin een dergelijke verwerking rechtmatig is.

In het kader van het Gemoderniseerd Verdrag 108 (artikel 6) en de algemene verordening gegevensbescherming (artikel 9), worden de volgende categorieën beschouwd als gevoelige gegevens:

- persoonsgegevens waaruit de raciale of etnische afkomst blijkt;
- persoonsgegevens waaruit de politieke, godsdienstige of een andere overtuiging blijkt, inclusief levensbeschouwelijke overtuigingen;
- persoonlijke gegevens waaruit het lidmaatschap van een vakvereniging blijkt;
- genetische karakteristieken en biometrische gegevens die worden verwerkt met het oog op de identificatie van een persoon;
- persoonsgegevens betreffende gezondheid, het seksuele leven of de seksuele geaardheid.

185 *Ibid.*, punten 56-57.

Voorbeeld: *Bodil Lindqvist*[186] betrof de verwijzing naar verschillende personen, met naam of met andere middelen, zoals hun telefoonnummer of informatie over hun hobby's op een webpagina. Het HvJ-EU heeft verklaard dat "de vermelding van het feit dat iemand zijn voet heeft bezeerd en met gedeeltelijk ziekteverlof is, [...] een persoonsgegeven betreffende de gezondheid [is]"[187].

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten

Het Gemoderniseerd Verdrag 108 omvat persoonsgegevens betreffende overtredingen, strafrechtelijke veroordelingen en strafbare feiten, en daarmee verband houdende beveiligingsmaatregelen die in de lijst van bijzondere categorieën persoonsgegevens voorkomen[188]. In het kader van de algemene verordening gegevensbescherming worden persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten niet als zodanig vermeld in de lijst van speciale categorieën gegevens, maar worden ze behandeld in een apart artikel. Artikel 10 van de algemene verordening gegevensbescherming bepaalt dat dergelijke gegevens alleen mogen worden verwerkt " onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden". Uitgebreide registers met informatie over strafrechtelijke veroordelingen daarentegen, kunnen enkel worden bijgehouden onder toezicht van specifieke officiële autoriteiten[189]. In de Europese Unie is de verwerking van persoonsgegevens in het kader van de rechtshandhaving onderworpen aan een specifiek rechtsinstrument, Richtlijn (EU) 2016/680[190]. De richtlijn voorziet in specifieke regels voor gegevensbescherming, die bindend zijn voor bevoegde autoriteiten wanneer zij persoonsgegevens verwerken, specifiek voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten (zie punt 8.2.1).

186 HvJ-EU, C-101/01, *Strafzaak tegen Bodil Lindqvist*, 6 november 2003, punt 51.

187 Voormalige Richtlijn 95/46/EG, artikel 8, lid 1, thans algemene verordening gegevensbescherming, artikel 9, lid 1.

188 Gemoderniseerd Verdrag 108, artikel 6, lid 1.

189 Algemene verordening gegevensbescherming, artikel 10.

190 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, PB L 119 van 2016.

2.2. Gegevensverwerking

Belangrijkste punten

- "Gegevensverwerking" heeft betrekking op alle soorten verwerkingen van persoonsgegevens.
- De term "verwerking" heeft betrekking op de geautomatiseerde en niet-geautomatiseerde verwerking.
- In het Unierecht heeft "verwerking" daarnaast ook betrekking op handmatige verwerking in gestructureerde bestanden van persoonsgegevens.
- In het recht van de Raad van Europa kan de betekenis van "verwerking" bij nationale wetgeving worden uitgebreid om ook handmatige verwerking te omvatten.

2.2.1. Het concept van gegevensverwerking

Het concept van gegevensverwerking is allesomvattend in **zowel het Unierecht als het recht van de Raad van Europa**: onder "verwerking van persoonsgegevens" wordt verstaan; "elke bewerking [...] zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorgifte, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, in verband brengen, alsmede het afschermen, wissen of vernietigen van gegevens"[191]. Het Gemoderniseerd Verdrag 108 voegt het bewaren van persoonsgegevens toe aan de definitie[192].

Voorbeeld: In *František Ryneš*[193] legde de heer Ryneš de afbeelding vast van twee individuen die ramen in zijn huis kapot hadden gemaakt via het CCTV-bewakingssysteem dat hij had geïnstalleerd om zijn eigendom te bewaken. Het HvJ-EU bepaalde dat video-bewaking met de registratie en opslag van persoonsgegevens wordt aanschouwd als geautomatiseerde gegevensverwerking die valt onder het toepassingsgebied van de EU-wetgeving inzake gegevensbescherming.

191 Algemene verordening gegevensbescherming, artikel 4, lid 2. Zie ook artikel 2, onder b), van het Gemoderniseerd Verdrag 108.

192 Gemoderniseerd Verdrag 108, artikel 2, onder b).

193 HvJ-EU, C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 december 2014, punt 25.

Voorbeeld: In *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*[194] verzocht de heer Manni de verwijdering van zijn persoonsgegevens uit de lijst van een onderneming voor kredietwaardigheidsbeoordelingen die hem koppelde aan het faillissement van een vastgoedbedrijf, wat een negatieve invloed had op zijn reputatie. Het HvJ-EU verklaarde dat "bij het inschrijven en bewaren van die informatie in het register en het in voorkomend geval op aanvraag daarvan verstrekken aan derden, de met het houden van dat register belaste autoriteit een "verwerking van persoonsgegevens" verricht waarvoor zij de "verwerkingsverantwoordelijke" is".

Voorbeeld: Werkgevers verzamelen en verwerken gegevens over hun werknemers, waaronder informatie over hun salarissen. Hun arbeidscontract creëert de rechtsgrondslag om dit op wettige wijze te doen.

Werkgevers moeten de salarisgegevens van hun werknemers doorgeven aan de belastingautoriteiten. Deze gegevensoverdracht zal ook "verwerking" zijn volgens de betekenis van deze term in Gemoderniseerd Verdrag 108 en de algemene verordening gegevensbescherming. De arbeidsovereenkomsten vormen echter niet de rechtsgrondslag voor deze openbaarmaking. Er moet een aanvullende rechtsgrondslag zijn voor verwerkingen die resulteren in de overdracht van salarisgegevens door de werkgever aan de belastingautoriteiten. Deze rechtsgrondslag schuilt over het algemeen in de bepalingen van de nationale belastingwetgeving. Zonder dergelijke bepalingen — en bij gebrek aan andere rechtsgrondslagen voor de verwerking van deze persoonsgegevens — zou deze openbaarmaking onwettige verwerking zijn.

2.2.2. Geautomatiseerde gegevensverwerking

De bescherming van gegevens in het kader van het Gemoderniseerd Verdrag 108 en de algemene verordening gegevensbescherming is volledig van toepassing op geautomatiseerde gegevensverwerking.

194 HvJ-EU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 maart 2017, punt 35.

In het kader van **het Unierecht** heeft geautomatiseerde gegevensverwerking betrekking op activiteiten die werden uitgevoerd "op de geheel of gedeeltelijk geautomatiseerde [...] verwerking van persoonsgegevens"[195]. Gemoderniseerd Verdrag 108 omvat een soortgelijke definitie[196]. In de praktijk betekent dit dat de verwerking van persoonsgegevens via geautomatiseerde weg met behulp van, bijvoorbeeld, een persoonlijke computer, een mobiel toestel of een router, onder de EU- en RvE-regelgeving inzake gegevensbescherming valt.

Voorbeeld: *Bodil Lindqvist*[197] betrof de verwijzing naar verschillende personen, met naam of met andere middelen, zoals hun telefoonnummer of informatie over hun hobby's op een wegpagina. Het HvJ-EU was van oordeel dat "het vermelden van verschillende personen op een internetpagina met hun naam of anderszins, bijvoorbeeld met hun telefoonnummer of informatie over hun werksituatie en hun hobby's, als een "geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens" in de zin van artikel 3, lid 1, van Richtlijn 95/46/EG is aan te merken"[198].

Voorbeeld: In *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[199] verzocht de heer González om de schrapping of wijziging van een verband tussen zijn naam in de Google zoekmachine en twee krantenpagina's die een veiling van onroerende goederen aankondigde voor de invordering van schulden bij de sociale zekerheid. Het HvJ-EU heeft verklaard dat "door geautomatiseerd, onophoudelijk en systematisch op het internet te zoeken naar aldaar gepubliceerde informatie, de exploitant van een zoekmachine dergelijke gegevens "verzamelt", die hij vervolgens volgens zijn indexeringsprogramma's "opvraagt", "vastlegt" en "ordent", op zijn servers "bewaart" en, in voorkomend geval, "verstrekt aan" en "ter beschikking stelt van" zijn gebruikers in de vorm van resultatenlijsten van hun zoekopdrachten"[200]. Het HvJ-EU concludeerde dat dergelijke acties

195 Algemene verordening gegevensbescherming, artikel 2, lid 1, en artikel 4, lid 2.

196 Gemoderniseerd Verdrag 108, artikel 2, onder b) en c); memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 21.

197 HvJ-EU, zaak C-101/01, *Strafzaak tegen Bodil Lindqvist*, 6 november 2003, punt 27.

198 Algemene verordening gegevensbescherming, artikel 2, lid 1.

199 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 13 mei 2014.

200 *Ibid.*, punt 28.

"verwerking" vormen, "zonder dat het daarbij van belang is dat de exploitant van de zoekmachine dezelfde verrichtingen tevens op andere soorten informatie toepast en daarbij geen onderscheid maakt tussen de informatie en de persoonsgegevens".

2.2.3. Niet-geautomatiseerde verwerking

De manuele verwerking van gegevens vereist ook gegevensbescherming.

In het Unierecht is gegevensbescherming geenszins beperkt tot geautomatiseerde gegevensverwerking. Bijgevolg is gegevensbescherming volgens het Unierecht van toepassing op de verwerking van persoonsgegevens in een handmatig bestand van persoonsgegevens, d.w.z. een daartoe speciaal gestructureerd papieren bestand[201]. Een gestructureerd bestand deelt een geheel van persoonsgegevens in zodat die toegankelijk worden volgens bepaalde criteria. Bijvoorbeeld, indien de werkgever een papieren dossier heeft, genaamd "vakantiedagen werknemers", waarin alle gegevens staan van de opgenomen vakantiedagen van zijn werknemers in het voorbije jaar en dat in alfabetische volgorde is gesorteerd, dan vormt dit dossier een manueel archiefsysteem dat valt onder de EU-regelgeving inzake gegevensbescherming. De reden voor deze uitbreiding van de gegevensbescherming is dat:

- papieren bestanden zodanig gestructureerd kunnen worden dat informatie snel en gemakkelijk kan worden gevonden;

- de opslag van persoonsgegevens in gestructureerde papieren bestanden het gemakkelijk maakt om de wettelijke beperkingen op geautomatiseerde gegevensverwerking te omzeilen[202].

In het **recht van de Raad van Europa** erkent de definitie van geautomatiseerde verwerking dat in de tijd tussen geautomatiseerde verwerkingen enkele fasen van handmatig gebruik van persoonsgegevens nodig kunnen zijn[203]. Artikel 2, onder c), van het Gemoderniseerd Verdrag 108 bepaalt dat "[w]aar er geen geautomatiseerde gegevensverwerking wordt gebruikt, betekent gegevensverwerking een verrichting of een reeks verrichtingen van persoonsgegevens in een gestructureerd

201 Algemene verordening gegevensbescherming, artikel 2, lid 1.

202 Algemene verordening gegevensbescherming, overweging 15.

203 Gemoderniseerd Verdrag 108, artikel 2, onder b) en c).

geheel van dergelijke gegevens die toegankelijk of opvraagbaar zijn volgens specifieke criteria".

2.3. Gebruikers van persoonsgegevens

Belangrijkste punten

- Diegene die de middelen en doeleinden van de verwerking van persoonsgegevens van anderen bepaalt, is een "verwerkingsverantwoordelijke" onder de gegevensbeschermingswetgeving; indien verschillende personen deze beslissing samen nemen, kunnen ze "gezamenlijke verwerkingsverantwoordelijken" zijn.
- Een "verwerker" is een natuurlijke persoon of rechtspersoon die ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verwerkt.
- Een verwerker wordt een verwerkingsverantwoordelijke indien hij de middelen en de doeleinden van de gegevensverwerking zelf vaststelt.
- Elke persoon aan wie de persoonsgegevens worden verstrekt, wordt een "ontvanger".
- Een "derde" is een natuurlijke persoon of rechtspersoon, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.
- De toestemming als rechtsgrond voor de verwerking van persoonsgegevens dient vrij, specifiek, op informatie berust en een ondubbelzinnige uitdrukking van wensen te zijn door een duidelijke bevestigende handeling die erop duidt dat men akkoord gaat met de verwerking.
- De verwerking van bijzondere categorieën gegevens op basis van toestemming vereist expliciete toestemming.

2.3.1. Verwerkingsverantwoordelijken en verwerkers

De status van de verwerkingsverantwoordelijke of verwerker heeft als belangrijkste gevolg dat de betrokken persoon of entiteit wettelijk verantwoordelijk is voor de naleving van de van toepassing zijnde verplichtingen uit hoofde van de gegevensbeschermingswetgeving. In de particuliere sector is dit gewoonlijk een natuurlijke persoon of rechtspersoon; in de openbare sector is dit gewoonlijk een autoriteit. Er bestaat een belangrijk onderscheid tussen een verwerkingsverantwoordelijke en een gegevensverwerker: de eerste is de natuurlijke persoon of rechtspersoon die de

doeleinden van de verwerking en de verwerkingsmiddelen bepaalt, de laatste is de natuurlijke of rechtspersoon die de gegevens voor rekening van de verwerkingverantwoordelijke verwerkt volgens strikte voorschriften. Het is in principe de verwerkingsverantwoordelijke die de controle op de verwerking moet uitvoeren en die hier verantwoordelijk voor is, met inbegrip van wettelijke aansprakelijkheid. Echter, met de hervorming van de regels inzake gegevensbescherming hebben verwerkers nu de verplichting om te voldoen aan veel van de vereisten die van toepassing zijn op verwerkingsverantwoordelijken. Bijvoorbeeld, in het kader van de algemene verordening gegevensbescherming moeten verwerkers een register van alle categorieën van verwerkingsactiviteiten bijhouden om nakoming van hun verplichtingen onder de verordening aan te tonen[204]. Verwerkers zijn verplicht ook passende technische en organisatorische maatregelen te nemen om de beveiliging van de verwerking te verzekeren[205], om een functionaris voor gegevensbescherming aan te wijzen in bepaalde gevallen[206], en om inbreuken in verband met persoonsgegevens aan de verwerkingsverantwoordelijke te melden[207].

De vraag of een persoon in staat is het doel van en de middelen voor de verwerking te bepalen en vast te stellen hangt af van de feiten of omstandigheden van de zaak. Volgens de definitie van de verwerkingsverantwoordelijke in de algemene verordening gegevensbescherming kunnen natuurlijke personen, rechtspersonen of een ander orgaan verwerkingsverantwoordelijke zijn. Groep artikel 29 heeft echter benadrukt dat, teneinde individuele personen een stabielere entiteit te geven voor de uitoefening van hun rechten, "de voorkeur dient te worden gegeven om de onderneming of de instantie als zodanig en niet een specifiek persoon binnenin de onderneming of de instantie als verwerkingsverantwoordelijke te beschouwen"[208]. Bijvoorbeeld, een bedrijf dat verpleegartikelen aan artsen verkoopt is de verwerkingsverantwoordelijke voor de opstelling en handhaving van de distributielijst van alle artsen in een bepaald gebied en niet de verkoopleider die de lijst werkelijk gebruikt en bijhoudt.

204 Algemene verordening gegevensbescherming, artikel 30, lid 2.

205 *Ibid.*, artikel 32.

206 *Ibid.*, artikel 37.

207 *Ibid.*, artikel 33, lid 2.

208 Groep artikel 29 (2010), *Advies 1/2010 over de begrippen "verwerkingsverantwoordelijke" en "verwerker"*, WP 169, Brussel, 16 februari 2010.

Voorbeeld: Wanneer de marketingafdeling van Zonneschijn B.V. van plan is gegevens te verwerken in het kader van een marktonderzoek, is Zonneschijn B.V., en zijn niet de werknemers op de marketingafdeling, de verwerkingsverantwoordelijke voor deze verwerking. De marketingafdeling kan niet de verwerkingsverantwoordelijke zijn, omdat ze geen afzonderlijke identiteit heeft.

Natuurlijke personen kunnen verwerkingsverantwoordelijke zijn in het kader van zowel het Unierecht als het recht van de Raad van Europa. Echter, bij het verwerken van gegevens over anderen met betrekking tot een louter persoonlijke of huishoudelijke activiteit vallen particulieren niet onder de regels van de algemene verordening gegevensbescherming en het Gemoderniseerd Verdrag 108, en worden ze niet beschouwd als verwerkingsverantwoordelijken[209]. Een individu die zijn/haar briefwisseling, een persoonlijk dagboek waarin gebeurtenissen met vrienden en collega's worden beschreven en gezondheidsgegevens van gezinsleden bijhoudt, kan worden vrijgesteld van gegevensbeschermingsregels, aangezien deze activiteiten uitsluitend persoonlijke of huishoudelijke activiteiten kunnen zijn. De algemene verordening gegevensbescherming bepaalt voorts dat tot persoonlijke of huishoudelijke activiteiten ook het sociaal netwerken en het houden van online-activiteiten kunnen behoren, indien deze plaatsvinden in de context van dergelijke activiteiten[210]. Gegevensbeschermingsregels zijn daarentegen volledig van toepassing op verwerkingsverantwoordelijken en verwerkers die voorzien in de middelen om persoonlijke gegevens voor persoonlijke of huishoudelijke activiteiten te verwerken (sociaalnetwerkplatforms bijvoorbeeld)[211].

De toegang van burgers tot het internet en de mogelijkheid om e-handelplatforms, sociale netwerken en blogs te gebruiken om persoonlijke informatie over zichzelf en andere individuen te delen, maken het steeds moeilijker om persoonlijke van niet persoonlijke verwerking te onderscheiden[212]. Of activiteiten al dan niet louter persoonlijk of huishoudelijk zijn, hangt af van de omstandigheden[213]. Activiteiten met commerciële of beroepskundige aspecten kunnen niet onder de huishoudelijke

209 Algemene verordening gegevensbescherming, overweging 18 en artikel 2, lid 2, onder c); Gemoderniseerd Verdrag 108, artikel 3, lid 2.

210 Algemene verordening gegevensbescherming, overweging 18.

211 *Ibid.*, overweging 18; memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 29.

212 Zie het overzicht van Groep artikel 29 inzake besprekingen met betrekking tot het hervormingspakket voor de gegevensbescherming (2013), *Bijlage 2: Wijzigingsvoorstellen met betrekking tot de uitzondering voor persoonlijke of huishoudelijke activiteiten*, 27 februari 2013.

213 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 28.

exceptie vallen[214]. Wanneer uit de omvang en de frequentie van de verwerking van gegevens zou blijken dat het wel om een beroepsmatige of voltijdse activiteit gaat, kan een particulier als verwerkingsverantwoordelijke worden beschouwd. In aanvulling op de beroepsmatige of commerciële aard van de gegevensverwerking moet een andere factor in aanmerking worden genomen, namelijk of persoonsgegevens ter beschikking worden gesteld aan een groot aantal personen die duidelijk buiten de persoonlijke levenssfeer van de betrokkene vallen. Jurisprudentie in het kader van de richtlijn gegevensbescherming heeft vastgesteld dat recht inzake gegevensbescherming van toepassing is wanneer een particulier, tijdens het gebruik van het internet, informatie over anderen op een openbare website publiceert. Het HvJ-EU heeft nog niet over soortgelijke feiten geoordeeld in het kader van de algemene verordening gegevensbescherming, die meer aanwijzingen geeft over de onderwerpen die kunnen worden beschouwd als buiten het toepassingsgebied van de gegevensbeschermingwetgeving vallend onder "huishoudelijke exceptie", zoals het gebruik van sociale media voor persoonlijke doeleinden.

Voorbeeld: *Bodil Lindqvist*[215] betrof de verwijzing naar verschillende personen, met naam of met andere middelen, zoals hun telefoonnummer of informatie over hun hobby's op een webpagina. Het HvJ-EU was van oordeel dat "het vermelden van verschillende personen op een internetpagina met hun naam of anderszins (...), is aan te merken als een "geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens"" in de zin van artikel 3, lid 1, van de richtlijn gegevensbescherming[216].

Deze persoonsgegevens vallen niet onder zuiver persoonlijke of huishoudelijke activiteiten, die buiten het toepassingsgebied van de Europese gegevensbeschermingregels vallen, aangezien deze uitzondering "derhalve aldus [moet] worden uitgelegd, dat zij uitsluitend betrekking heeft op activiteiten die tot het persoonlijke of gezinsleven van particulieren behoren, hetgeen klaarblijkelijk niet het geval is met de verwerking van

214 Zie Algemene verordening gegevensbescherming, overweging 18; memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 27.

215 HvJ-EU, zaak C-101/01, *Strafzaak tegen Bodil Lindqvist*, 6 november 2003.

216 *Ibid.*, punt 27; voormalige Richtlijn 95/46/EG, artikel 3, lid 1, thans algemene verordening gegevensbescherming, artikel 2, lid 1.

persoonsgegevens die bestaat uit hun openbaarmaking op het internet waardoor die gegevens voor een onbepaald aantal personen toegankelijk worden gemaakt[217].

Volgens het HvJ-EU kunnen de visuele opnames van een bewakingscamera die in een particuliere woning werd geïnstalleerd, ook worden gedekt door de EU-wetgeving inzake gegevensbescherming in bepaalde omstandigheden.

Voorbeeld: In *František Ryneš*[218] legde de heer Ryneš de afbeelding vast van twee individuen die ramen in zijn huis kapot hadden gemaakt via het CCTV-bewakingssysteem die hij had geïnstalleerd om zijn eigendom te bewaken. De vastlegging werd vervolgens overgedragen aan de politie en gebruikt tijdens de strafprocedure.

Het HvJ-EU heeft verklaard dat "voor zover het gebruik van een videobewakingssysteem de openbare ruimte bestrijkt – zelfs gedeeltelijk – en hierdoor buiten de privésfeer geraakt van diegene die door middel van dit systeem gegevens verwerkt, kan het niet worden beschouwd als een activiteit die met uitsluitend "persoonlijke of huishoudelijke doeleinden" wordt verricht [...]"[219].

Verwerkingsverantwoordelijke

In het Unierecht is een verwerkingsverantwoordelijke gedefinieerd als iemand die "alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt"[220]. Het besluit van een verwerkingsverantwoordelijke legt vast waarom en hoe de gegevens zullen worden verwerkt.

In het recht van de Raad van Europa definieert het Gemoderniseerd Verdrag 108 een "verwerkingsverantwoordelijke" als "de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam die, respectievelijk dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van

217 HvJ-EU, zaak C-101/01, *Strafzaak tegen Bodil Lindqvist*, 6 november 2003, punt 47.

218 HvJ-EU, C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 december 2014, punt 33.

219 Voormalige Richtlijn 95/46/EG, artikel 3, lid 2, tweede streepje, thans algemene verordening gegevensbescherming, artikel 2, lid 2, onder c).

220 Algemene verordening gegevensbescherming, artikel 4, lid 7.

persoonsgegevens vaststelt"[221]. Dit besluitvormingsvermogen heeft betrekking op de doeleinden en de middelen van de verwerking, alsook de gegevenscategorieën die verwerkt moeten worden en de toegang tot de gegevens[222]. De vraag of dit vermogen afkomstig is van een juridische kwalificatie of van feitelijke omstandigheden moet van geval tot geval worden bepaald[223].

> Voorbeeld: Een zaak werd aangespannen tegen *Google Spain*[224] door een Spaanse burger die een oude berichtgeving over zijn financiële geschiedenis uit Google wilde verwijderen.
>
> Het HvJ-EU werd gevraagd of Google, als exploitant van een zoekmachine, de "verwerkingsverantwoordelijke" van de gegevens was in de zin van artikel 2, onder d), van de richtlijn inzake gegevensbescherming[225]. Het HvJ-EU gebruikt een brede definitie van het begrip "verwerkingsverantwoordelijke" om een "doeltreffende en volledige bescherming van de betrokkenen te verzekeren"[226]. Het HvJ-EU van de Europese Unie stelde vast dat de exploitant van de zoekmachine de doeleinden en de middelen van de activiteit vaststelde en gegevens toonde die op internetpagina's van uitgevers van websites toegankelijk zijn voor elke gebruiker die een bevraging verricht op basis van de naam van de betrokken persoon[227]. Daarom heeft het HvJ-EU van de Europese Unie bepaald dat Google kan worden beschouwd als "verwerkingsverantwoordelijke"[228].

Als een verwerkingsverantwoordelijke of verwerker buiten de Europese Unie gevestigd is, moet de onderneming schriftelijk een vertegenwoordiger in de Europese Unie benoemen[229]. De algemene verordening gegevensbescherming bena-

221 Gemoderniseerd Verdrag 108, artikel 2, onder d).

222 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 22.

223 *Ibid.*

224 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 13 mei 2014.

225 Algemene verordening gegevensbescherming, artikel 4, lid 7; HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 13 mei 2014, punt 21.

226 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 13 mei 2014, punt 34.

227 *Ibid.*, punten 35-40.

228 *Ibid.*, punt 41.

229 Algemene verordening gegevensbescherming, artikel 27, lid 1.

drukt dat de vertegenwoordiger gevestigd moet zijn "in een van de lidstaten waar zich de betrokkenen bevinden wiens persoonsgegevens in verband met het hun aanbieden van goederen of diensten worden verwerkt, of wiens gedrag wordt geobserveerd"[230]. Als er geen vertegenwoordiger wordt aangewezen, kunnen er nog steeds juridische acties worden opgestart tegen de verwerkingsverantwoordelijke of de verwerker zelf[231].

Gezamenlijke verantwoordelijkheid voor de verwerking

De algemene verordening gegevensbescherming bepaalt dat wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen voor de verwerking bepalen, zij gezamenlijke verwerkingsverantwoordelijken zijn. Dat betekent dat ze samen beslissen om gegevens te verwerken voor een gedeeld doel[232]. Het toelichtend verslag van het Gemoderniseerd Verdrag 108 stelt dat meervoudige verwerkingsverantwoordelijken of gezamenlijke verantwoordelijkheid voor verwerking mogelijk is **in het kader van de RvE**[233].

Groep artikel 29 wijst erop dat de gezamenlijke verantwoordelijkheid voor de verwerking verschillende vormen kan aannemen en dat de deelname van verschillende verwerkingsverantwoordelijken in de controle van activiteiten ongelijk kan zijn[234]. Een dergelijke flexibiliteit maakt het mogelijk het hoofd te bieden aan de steeds complexere realiteiten inzake gegevensverwerking[235]. Gezamenlijke verwerkingsverantwoordelijken moeten daarom hun respectieve verantwoordelijkheden vaststellen om aan de verplichtingen van de verordening te voldoen in een specifieke overeenkomst[236].

Gezamenlijke verantwoordelijkheid voor de verwerking leidt tot gezamenlijke verantwoordelijkheid voor een verwerkingsactiviteit[237]. In het kader van het **Unierecht** houdt dit in dat elke verwerkingsverantwoordelijke of verwerker volledig

230 *Ibid.*, artikel 27, lid 3.

231 *Ibid.*, artikel 27, lid 5.

232 *Ibid.*, artikel 4, lid 7, en artikel 26.

233 Gemoderniseerd Verdrag 108, artikel 2, onder d); memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 22.

234 Groep artikel 29 (2010), *Advies 1/2010 over de begrippen "verwerkingsverantwoordelijke" en "verwerker"*, WP 169, Brussel, 16 februari 2010, blz. 19.

235 *Ibid.*

236 Algemene verordening gegevensbescherming, overweging 79.

237 *Ibid.*, punt 21.

aansprakelijk kan worden gesteld voor de volledige schade die wordt veroorzaakt door verwerkingen onder gedeelde verantwoordelijkheid om ervoor te zorgen dat de betrokkene effectief schadeloosgesteld wordt[238].

Voorbeeld: Een door verschillende kredietinstellingen beheerde databank over wanbetalende klanten is een gebruikelijk voorbeeld van gezamenlijke verantwoordelijkheid voor de verwerking. Wanneer iemand een kredietlijn aanvraagt bij een bank die één van de gezamenlijk verwerkingsverantwoordelijken is, controleert de bank de databank om een geïnformeerd besluit te kunnen nemen over de kredietwaardigheid van de aanvrager.

In de wettelijke bepalingen wordt niet uitdrukkelijk bepaald of het voor het bestaan van gezamenlijke verantwoordelijkheid voor verwerking noodzakelijk is dat het gedeelde doeleinde voor elk van de voor de verwerkingsverantwoordelijken hetzelfde is dan wel of het voldoende is dat hun doeleinden elkaar slechts gedeeltelijk overlappen. Tot dusver is er nog geen relevante rechtspraak beschikbaar op Europees niveau. In zijn advies van 2010 over verwerkingsverantwoordelijken en verwerkers stelt Groep artikel 29 dat gezamenlijk verwerkingsverantwoordelijken alle doeleinden en middelen voor verwerking mogen delen of slechts enkele doeleinden of middelen of een deel daarvan mogen delen[239]. Terwijl het eerste geval een erg hechte relatie tussen de verschillende actoren zou inhouden, duidt het laatste geval op een lossere relatie.

Groep artikel 29 pleit voor een bredere interpretatie van het begrip van gedeelde verantwoordelijkheid van verwerking met het doel om enige flexibiliteit mogelijk te maken om rekening te houden met de toenemende complexiteit van de huidige realiteit van gegevensverwerking[240]. Een zaak met de Society for Worldwide Interbank Financial Telecommunication (SWIFT) illustreert de positie van de Werkgroep.

Voorbeeld: In de zogenoemde SWIFT-zaak hadden Europese bankinstellingen SWIFT ingehuurd, oorspronkelijk als verwerker, om de doorgifte van gegevens in het kader van banktransacties te verzorgen. SWIFT droeg deze

238 *Ibid.*, artikel 82, lid 4.

239 Groep artikel 29 (2010), *Advies 1/2010 over de begrippen "verwerkingsverantwoordelijke" en "verwerkeer"*, WP 169, Brussel, 16 februari 2010, blz. 19.

240 *Ibid.*

gegevens over banktransacties, die waren opgeslagen in servers in de Verenigde Staten (VS), over aan het Amerikaanse ministerie van Financiën zonder dat de Europese bankinstellingen die SWIFT hadden gecontracteerd daar expliciet opdracht toe hadden gegeven. Groep artikel 29 kwam na het beoordelen van de rechtmatigheid van deze situatie tot de conclusie dat de Europese bankinstellingen die SWIFT hadden ingehuurd, evenals SWIFT zelf, moesten worden gezien als gezamenlijke verwerkingsverantwoordelijken die tegenover Europese klanten verantwoordelijk waren voor de doorgifte van hun gegevens aan de Amerikaanse autoriteiten[241].

Verwerker

Een verwerker wordt **in het Unierecht** gedefinieerd als iemand die persoonsgegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke[242]. De werkzaamheden die aan een verwerker worden toevertrouwd kunnen beperkt blijven tot een zeer specifieke taak of context of kunnen van vrij algemene en alomvattende aard zijn.

In het recht van de Raad van Europa is de betekenis van een verwerker hetzelfde als in het Unierecht[243].

Verwerkers zullen, naast gegevens verwerken voor anderen, zelf ook verwerkingsverantwoordelijken zijn in verband met de verwerkingen die ze uitvoeren voor hun eigen doeleinden, bijvoorbeeld voor de administratie van de eigen werknemers, verkopen en facturen.

Voorbeeld: Een onderneming is gespecialiseerd in gegevensverwerking in het kader van de administratie van HR-gegevens voor andere ondernemingen. In deze functie is de onderneming een verwerker. Wanneer de onderneming echter gegevens over haar eigen werknemers verwerkt, is ze de verwerkingsverantwoordelijke met het oog op het vervullen van de verplichtingen die ze als werkgever heeft.

241 Groep artikel 29 (2006), *Advies 10/2006 over de verwerking van persoonsgegevens door de Society for Worldwide Interbank Financial Telecommunication (SWIFT),* WP 128, Brussel, 22 november 2006.

242 Algemene verordening gegevensbescherming, artikel 4, lid 8.

243 Gemoderniseerd Verdrag 108, artikel 2, onder f).

De verhouding tussen de verwerkingsverantwoordelijke en de verwerker

Zoals we hebben gezien, is de verwerkingsverantwoordelijke gedefinieerd als degene die de doeleinden van de verwerking en de wijze van verwerking bepaalt. De algemene verordening gegevensbescherming stelt duidelijk dat de verwerker uitsluitend persoonsgegevens mag verwerken volgens de instructies van de verwerkingsverantwoordelijke, tenzij het Unierecht of het lidstatelijk recht dit van de verwerker vereist[244]. Het contract tussen de verwerkingsverantwoordelijke en de verwerker is een essentieel onderdeel van hun relatie, en is wettelijk verplicht[245].

Voorbeeld: De directeur van Zonneschijn B.V. besluit dat de Cloudy Company – specialist in cloudgebaseerde gegevensopslag – de klantgegevens van Zonneschijn B.V. moet beheren. Zonneschijn B.V. blijft de verwerkingsverantwoordelijke en Cloudy Company is enkel een verwerker, aangezien, volgens het contract, Cloudy enkel gebruik mag maken van de klantgegevens van Zonneschijn B.V. voor de doeleinden die Zonneschijn vastlegt.

Als de bevoegdheid om de wijze van verwerking te bepalen wordt gedelegeerd aan een verwerker, moet de verwerkingsverantwoordelijke niettemin een passende mate van controle kunnen uitvoeren over de beslissingen van de verwerker met betrekking tot de wijze van verwerking. De eindverantwoordelijkheid ligt nog steeds bij de verwerkingsverantwoordelijke, die toezicht moet houden op de verwerkers om ervoor te zorgen dat hun beslissingen voldoen aan de gegevensbeschermingswetgeving en aan zijn eigen instructies.

Voorts zal een verwerker, indien deze de voorwaarden voor de verwerking van gegevens als voorgeschreven door de verwerkingsverantwoordelijke niet respecteert, een verwerkingsverantwoordelijke moeten worden, althans voor zover het de inbreuk op de instructies van de verwerkingsverantwoordelijke betreft. Dit zal de verwerker naar alle waarschijnlijkheid tot een verwerkingsverantwoordelijke maken die onrechtmatig handelt. Op zijn beurt zal de oorspronkelijke verwerkingsverantwoordelijke moeten uitleggen hoe het mogelijk was dat de verwerker zijn/haar

244 Algemene verordening gegevensbescherming, artikel 29.

245 *Ibid.*, artikel 28, lid 3.

mandaat te buiten kon gaan[246]. Sterker nog, Groep artikel 29 veronderstelt in zulke gevallen veelal gezamenlijke verantwoordelijkheid voor de verwerking, aangezien dit leidt tot de beste bescherming van de belangen van de betrokkenen[247].

Ook kunnen er problemen ontstaan met de verdeling van de verantwoordelijkheid wanneer de verwerkingsverantwoordelijke een kleine onderneming is en de verwerker een grote onderneming die over de macht beschikt om de voorwaarden van de diensten te dicteren. In dergelijke omstandigheden stelt Groep artikel 29 echter dat de normen voor de verantwoordelijkheid voor de gegevensverwerking niet mogen worden versoepeld vanwege economische ongelijkheden en dat de uitleg van het begrip "verwerkingsverantwoordelijke" moet worden gehandhaafd[248].

Ten behoeve van de duidelijkheid en de transparantie moeten de details van de verhouding tussen een verwerkingsverantwoordelijke en een verwerker worden vastgelegd in een schriftelijke overeenkomst[249]. De overeenkomst moet in het bijzonder het onderwerp, de aard, het doel en de duur van de verwerking, het soort persoonsgegevens en de categorieën betrokkenen bevatten. Zij dient ook de verplichtingen en rechten van de verwerkingsverantwoordelijke en de verwerker te bepalen, zoals vereisten inzake vertrouwelijkheid en beveiliging. Het ontbreken van een dergelijke overeenkomst vormt een inbreuk op de verplichting van de verwerkingsverantwoordelijke om de gezamenlijke verantwoordelijkheden schriftelijk te documenteren, en kan leiden tot sancties. Wanneer schade wordt berokkend als gevolg van handelingen die buiten de rechtmatige instructies van de verwerkingsverantwoordelijke vallen of deze niet worden nageleefd, kan niet enkel de verwerker verantwoordelijk worden gehouden, maar ook de verwerkingsverantwoordelijke[250]. De verwerker moet alle categorieën verwerkingsactiviteiten bijhouden die hij voor rekening van de verwerkingsverantwoordelijke uitvoert[251]. Deze verslagen moeten beschikbaar worden gesteld op verzoek van de toezichthoudende autoriteit, aangezien de verwerkingsverantwoordelijke en de verwerker beiden moeten

246 *Ibid.*, artikel 82, lid 2.

247 Groep artikel 29 (2010), *Advies 1/2010 over de begrippen "verwerkingsverantwoordelijke" en "verwerker"*, WP 169, Brussel, 16 februari 2010, blz. 25; Groep artikel 29 (2006), *Advies 10/2006 over de verwerking van persoonsgegevens door de Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Brussel, 22 november 2006.

248 Groep artikel 29 (2010), *Advies 1/2010 over de begrippen "verwerkingsverantwoordelijke" en "verwerker"*, WP 169, Brussel, 16 februari 2010, blz. 26.

249 Algemene verordening gegevensbescherming, artikel 28, leden 3 en 9.

250 *Ibid.*, artikel 82, lid 2.

251 *Ibid.*, artikel 30, lid 2.

samenwerken met die autoriteit in de uitvoering van hun taken[252]. Verwerkingsverantwoordelijken en verwerkers kunnen ook een erkende gedragscode of een certificeringsmechanisme naleven die, respectievelijk dat, aantoont dat ze voldoen aan de voorwaarden inzake de algemene verordening gegevensbescherming[253].

Verwerkers zullen mogelijk bepaalde taken willen delegeren aan aanvullende subverwerkers. Dit is wettelijk toegestaan, mits passende contractuele bepalingen tussen de verwerkingsverantwoordelijke en de verwerker worden vastgelegd, inclusief of de machtiging van de verwerkingsverantwoordelijke in elk afzonderlijk geval noodzakelijk is dan wel dat alleen informeren volstaat. De algemene verordening gegevensbescherming bepaalt dat de eerste verwerker volledig aansprakelijk blijft ten opzichte van de verwerkingsverantwoordelijke in het geval dat een subverwerker niet voldoet aan zijn plichten inzake gegevensbescherming[254].

In het recht van de Raad van Europa is de interpretatie van de begrippen voor verwerkingsverantwoordelijke en verwerker, zoals hierboven uiteengezet, volledig van toepassing[255].

2.3.2. Ontvangers en derden

Het verschil tussen deze twee categorieën van personen of entiteiten, die zijn ingevoerd door de richtlijn gegevensbescherming, ligt voornamelijk in hun verhouding tot de verwerkingsverantwoordelijke en dientengevolge in hun bevoegdheid om toegang te verkrijgen tot gegevens die berusten bij de verwerkingsverantwoordelijke.

Een "derde" is iemand die verschilt van de verwerkingsverantwoordelijke en de verwerker. Volgens artikel 4, lid 10, van de algemene verordening gegevensbescherming is een derde "de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam, niet zijnde de betrokkene, noch de voor de verwerking verantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de voor de verwerking verantwoordelijke of de verwerker gemachtigd zijn om de gegevens te verwerken". Dit betekent dat personen die werkzaam zijn voor een

252 *Ibid.*, artikel 30, lid 4, en artikel 31.

253 *Ibid.*, artikel 28, lid 5, en artikel 42, lid 4.

254 *Ibid.*, artikel 28, lid 4.

255 Zie bijvoorbeeld Gemoderniseerd Verdrag 108, artikel 2, onder b) en f); Aanbeveling inzake profilering, artikel 1.

organisatie die niet dezelfde is als de verwerkingsverantwoordelijke, ook wanneer deze deel uitmaakt van hetzelfde concern of dezelfde holdingcompany, "derden" zullen zijn (of tot een derde zullen behoren). Anderzijds zijn kantoren van banken die de rekeningen van klanten verwerken onder rechtstreeks gezag van hun hoofdkantoor, geen "derden"[256].

"Ontvanger" is een bredere term dan "derde". Volgens artikel 4, lid 9, van de algemene verordening gegevensbescherming betekent ontvanger "de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam waaraan de gegevens worden meegedeeld, ongeacht of het al dan niet een derde betreft". Deze ontvanger kan ofwel een persoon buiten de verwerkingsverantwoordelijke of de verwerker zijn — dit zou dan een derde zijn — of iemand binnen de verwerkingsverantwoordelijke of de verwerker, zoals een werknemer of een andere afdeling van dezelfde onderneming of autoriteit.

Het onderscheid tussen ontvangers en derden is alleen van belang vanwege de voorwaarden voor rechtmatige doorgifte van gegevens. De werknemers van een verwerkingsverantwoordelijke of verwerker kunnen zonder verdere wettelijke vereisten ontvangers van persoonsgegevens zijn indien ze betrokken zijn bij verwerkingen van de verwerkingsverantwoordelijke of de verwerker. Anderzijds is een derde, die niet dezelfde is als de verwerkingsverantwoordelijke of de verwerker, niet bevoegd om gegevens te gebruiken die de verwerkingsverantwoordelijke verwerkt, tenzij op basis van een specifieke rechtsgrondslag in een specifiek geval.

Voorbeeld: Een werknemer van een verwerkingsverantwoordelijke die persoonsgegevens gebruikt binnen de taak die hem of haar door de werkgever is toevertrouwd, is een ontvanger van gegevens, maar geen derde, aangezien hij of zij de gegevens gebruikt namens en in opdracht van de verwerkingsverantwoordelijke. Indien bijvoorbeeld een werkgever persoonlijke gegevens van zijn werknemers vermeldt aan de personeelsdienst met het oog op toekomstige prestatie-analyses, zal de personeelsdienst ontvanger zijn van de persoonsgegevens, aangezien de gegevens zijn verstrekt in het kader van de verwerking voor de verwerkingsverantwoordelijke.

256 Groep artikel 29 (2010), *Advies 1/2010 over de begrippen "verwerkingsverantwoordelijke" en "verwerker"*, WP 169, Brussel, 16 februari 2010, blz. 31.

Indien de organisatie echter gegevens over haar werknemers verstrekt aan een opleidingsbedrijf dat deze zal gebruiken om een opleidingsprogramma voor de werknemers op te stellen, dan is het opleidingsbedrijf een derde partij. De reden hiervoor is dat het opleidingsbedrijf niet over een specifieke wettigheid of autorisatie beschikt (die in het geval van de personeelsdienst voortvloeit uit de arbeidsverhouding met de verwerkingsverantwoordelijke) om deze persoonsgegevens te verwerken. Met andere woorden, ze hebben de informatie niet ontvangen in het kader van hun professionele activiteit met de verwerkingsverantwoordelijke.

2.4. Toestemming

Belangrijkste punten

- De toestemming als rechtsgrond voor de verwerking van persoonsgegevens dient vrij, specifiek, op informatie berust en een ondubbelzinnige indicatie van wensen te zijn door een duidelijke bevestigende handeling die erop duidt dat men akkoord gaat met de verwerking.
- De verwerking van bijzondere categorieën gegevens vereist uitdrukkelijke toestemming.

Zoals in detail zal worden beschouwd in hoofdstuk 4, is toestemming een van de zes legitieme gronden voor de verwerking van persoonsgegevens. Toestemming betekent "elke vrije, specifieke, op informatie berustende en ondubbelzinnige wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt"[257].

In het Unierecht worden verschillende elementen genoemd die vervuld moeten zijn om een toestemming geldig te laten zijn, die ten doel hebben om te garanderen dat betrokkenen heel bewust hebben ingestemd met een specifiek gebruik van hun gegevens[258]:

257 Algemene verordening gegevensbescherming, artikel 4, lid 11. Zie ook Gemoderniseerd Verdrag 108, artikel 5, lid 2.

258 Algemene verordening gegevensbescherming, artikel 7.

- De toestemming dient te worden gegeven door middel van een duidelijk bevestigende handeling waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt. Een dergelijke handeling kan een actie of een verklaring zijn.

- De betrokkene dient het recht te hebben zijn toestemming te allen tijde in te trekken.

- In het kader van een schriftelijke verklaring die ook andere kwesties behandelt, zoals "servicevoorwaarden", moeten verzoeken tot toestemming in duidelijke en eenvoudige taal geformuleerd zijn en in een begrijpelijke en makkelijk toegankelijke vorm beschikbaar zijn, zodat de toestemming duidelijk onderscheiden wordt van andere kwesties. Indien een deel van deze verklaring in strijd is met de algemene verordening gegevensbescherming, is ze niet bindend.

De toestemming is enkel geldig in het kader van de wetgeving inzake gegevensbescherming indien aan elk van deze eisen is voldaan. Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om aan te tonen dat de betrokkene heeft ingestemd met de verwerking van zijn/haar gegevens[259]. De elementen van de geldige toestemming worden verder besproken in punt 4.1.1 over rechtmatige gronden voor de verwerking van persoonsgegevens.

Verdrag 108 bevat geen definitie van toestemming; dit wordt overgelaten aan het nationale recht. Echter, **in het recht van de Raad van Europa** komen de elementen van geldige toestemming overeen met de eerder toegelichte elementen[260].

Aanvullende eisen voor geldige toestemming in het civiele recht, zoals rechtshandelingsbekwaamheid, zijn uiteraard ook van toepassing in het kader van gegevensbescherming, aangezien deze eisen fundamentele juridische voorafgaande voorwaarden zijn. Ongeldige toestemming van personen die niet handelingsbekwaam zijn, zal resulteren in het ontbreken van een rechtsgrondslag voor de verwerking van gegevens over deze personen. Met betrekking tot de handelingsbevoegdheid van minderjarigen om contracten aan te gaan, bepaalt de algemene verordening gegevensbescherming dat de regels over de minimumleeftijd om geldige

259 *Ibid.*, artikel 7, lid 1.

260 Gemoderniseerd Verdrag 108, artikel 5, lid 2; memorie van toelichting bij Gemoderniseerd Verdrag 108, punten 42-45.

toestemming te krijgen geen invloed hebben op het algemene verbintenissenrecht van lidstaten[261].

Toestemming moet op een duidelijke manier worden gegeven zodat er geen twijfel bestaat over het voornemen van de betrokkene[262]. Toestemming moet uitdrukkelijk worden gegeven wanneer het gaat over de verwerking van gevoelige gegevens, en kan mondeling of schriftelijk worden gegeven[263]. Dit laatste kan gebeuren in elektronische vorm[264]. In het kader van zowel het **Unierecht** als **het recht van de Raad van Europa**, dient het akkoord voor de verwerking van de persoonsgegevens van de betrokkene te worden gegeven via een verklaring of een duidelijk bevestigende handeling[265]. Bijgevolg kan instemming niet worden afgeleid uit stilte, vooraf aangevinkte vakjes, vooraf ingevulde formulieren of inactiviteit[266].

261 Algemene verordening gegevensbescherming, artikel 8, lid 3.

262 *Ibid.*, artikel 6, lid 1, onder a), en artikel 9, lid 2, onder a).

263 *Ibid.*, overweging 32.

264 *Ibid.*

265 *Ibid.*, artikel 4, lid 11; memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 42.

266 Algemene verordening gegevensbescherming, overweging 32; memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 42.

3 De belangrijkste beginselen van de Europese gegevensbeschermingswetgeving

EU	Behandelde onderwerpen	RvE
Algemene verordening gegevensbescherming, artikel 5, lid 1, onder a)	Het beginsel van rechtmatigheid	Gemoderniseerd Verdrag 108, artikel 5, lid 3
Algemene verordening gegevensbescherming, artikel 5, lid 1, onder a)	Het beginsel van behoorlijkheid	Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder a) EHRM, *K.H. e.a./Slowakije*, nr. 32881/04, 2009
Algemene verordening gegevensbescherming, artikel 5, lid 1, onder a) HvJ-EU, zaak C-201/14, *Smaranda Bara e.a./Casa Națională de Asigurări de Sănătate e.a.*, 2015	Het transparantiebeginsel	Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder a), en artikel 8 EHRM, *Haralambie/Roemenië*, nr. 21737/03, 2009
Algemene verordening gegevensbescherming, artikel 5, lid 1, onder b)	Het beginsel van doelbinding	Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder b)
Algemene verordening gegevensbescherming, artikel 5, lid 1, onder c) HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland* en Kärntner Landesregierung e.a. [Grote kamer], 2014	Het beginsel van minimale gegevensverwerking	Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder c)

EU	Behandelde onderwerpen	RvE
Algemene verordening gegevensbescherming, artikel 5, lid 1, onder d) HvJ-EU, zaak C-553/07, *College van burgemeester en wethouders van Rotterdam/ M.E.E. Rijkeboer*, 2009	**Het beginsel van juistheid van de gegevens**	Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder d)
Algemene verordening gegevensbescherming, artikel 5, lid 1, onder e) HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland* en Kärntner Landesregierung e.a. [Grote kamer], 2014	**Het beginsel van opslagbeperking**	Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder e) EHRM, *S. en Marper/Verenigd Koninkrijk* [Grote kamer], nrs. 30562/04 en 30566/04, 2008
Algemene verordening gegevensbescherming, artikel 5, lid 1, onder f), en artikel 32	**Het beginsel van de beveiliging van gegevens (integriteit en vertrouwelijkheid)**	Gemoderniseerd Verdrag 108, artikel 7
Algemene verordening gegevensbescherming, artikel 5, lid 2	**De verantwoordings-plicht**	Gemoderniseerd Verdrag 108, artikel 10

Artikel 5 van de algemene verordening gegevensbescherming bevat de beginselen voor de verwerking van persoonsgegevens. Deze beginselen omvatten:

- rechtmatigheid, behoorlijkheid en transparantie;
- doelbinding;
- minimalisering van gegevens;
- juistheid van de gegevens;
- beperking van de opslagbeperking;
- integriteit en vertrouwelijkheid.

De beginselen dienen als uitgangspunt voor meer gedetailleerde bepalingen in de volgende artikelen van de verordening. Zij verschijnen tevens in de artikelen 5, 7, 8 en 10 van het Gemoderniseerd Verdrag 108. Alle latere

gegevensbeschermingswetgeving op RvE- of EU-niveau moet voldoen aan deze beginselen en deze beginselen moeten in aanmerking worden genomen bij de interpretatie van deze wetgeving. In het kader van de EU-wetgeving worden beperkingen op de gegevensverwerkingsbeginselen enkel toegestaan voor zover deze overeenkomen met de rechten en plichten in artikelen 12 tot 22 en ze moeten de essentie van de grondrechten en fundamentele vrijheden respecteren. Elke vrijstelling van en beperking op deze belangrijke beginselen kunnen worden vastgelegd op EU- of op nationaal niveau[267]; ze moeten bij wet worden gesteld, een rechtmatig doel dienen en noodzakelijke en geproportioneerde maatregelen zijn in een democratische maatschappij[268]. Alle drie deze voorwaarden moeten zijn vervuld.

3.1. De beginselen inzake verwerking van rechtmatigheid, behoorlijkheid en transparantie

Belangrijkste punten

- De beginselen van rechtmatigheid, behoorlijkheid en transparantie zijn van toepassing op elke verwerking van persoonsgegevens.
- In het kader van de algemene verordening gegevensbescherming vereist rechtmatigheid ofwel:
  - toestemming van de betrokkene;
  - noodzaak om een contract aan te gaan;
  - een wettelijke verplichting;
  - noodzaak om de vitale belangen van de betrokkene of een ander persoon te beschermen;
  - noodzaak om een taak van algemeen belang uit te voeren;
  - noodzaak voor de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde partij, indien zij niet worden tenietgedaan door de belangen en rechten van de betrokkene.

267 Gemoderniseerd Verdrag 108, artikel 11, lid 1; Algemene verordening gegevensbescherming, artikel 23, lid 1.

268 Algemene verordening gegevensbescherming, artikel 23, lid 1.

- De verwerking van persoonsgegevens moet gebeuren op een eerlijke manier.
  - De betrokkene dient te worden geïnformeerd over de risico's om ervoor te zorgen dat de verwerking geen onvoorziene ongunstige gevolgen heeft.
- De verwerking van persoonsgegevens moet gebeuren op een transparante manier.
  - De verwerkingsverantwoordelijken moeten betrokkenen informeren, voordat ze hun gegevens verwerken, over onder andere het doeleinde van de verwerking en de identiteit en het adres van de verwerkingsverantwoordelijke.
  - Informatie over de verwerking moet worden voorzien in duidelijke en eenvoudige taal zodat de betrokkenen de betrokken regels, risico's, rechten en waarborgen gemakkelijk kunnen begrijpen.
  - Betrokkenen hebben altijd het recht om hun gegevens in te zien wanneer deze worden verwerkt.

3.1.1. Rechtmatige verwerking

Het Unierecht en het recht van de Raad van Europa inzake gegevensbescherming eisen dat persoonsgegevens rechtmatig verwerkt worden[269]. Rechtmatige verwerking vereist de toestemming van de betrokkene of een andere legitieme reden conform de wetgeving op het gebied van de gegevensbescherming[270]. Artikel 6, lid 1, van de algemene verordening gegevensbescherming bevat vijf rechtmatige gronden voor de verwerking, in aanvulling op de toestemming, dat wil zeggen wanneer de verwerking van persoonsgegevens noodzakelijk is voor de uitvoering van een contract, voor de uitvoering van een opdracht als uitoefening van het openbaar gezag, om te voldoen aan een wettelijke verplichting, om de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of derden te behartigen of, indien nodig, ter bescherming van de vitale belangen van de betrokkene. Deze aspecten komen nader aan bod in punt 4.1.

3.1.2. Behoorlijkheid van de verwerking

In aanvulling op de rechtmatige verwerking eisen het Unierecht en het recht van de Raad van Europa inzake gegevensbescherming dat persoonsgegevens op een

269 Gemoderniseerd Verdrag 108, artikel 5, lid 3; algemene verordening gegevensbescherming, artikel 5, lid 1, onder a).

270 Handvest van de grondrechten van de Europese Unie, artikel 8, lid 2; algemene verordening gegevensbescherming, overweging 40 en artikel 6-9; Gemoderniseerd Verdrag 108, artikel 5, lid 2; memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 41.

billijke manier worden verwerkt[271]. Het beginsel van eerlijke verwerking bepaalt voornamelijk de relatie tussen de verwerkingsverantwoordelijke en de betrokkene.

Verwerkingsverantwoordelijken dienen de betrokkenen en het grote publiek in kennis te stellen dat ze gegevens op een wettelijke en transparante manier zullen verwerken en moeten in staat zijn om aan te tonen dat de verwerking geschiedt overeenkomstig de algemene verordening gegevensbescherming. Verwerkingen mogen niet in het geheim worden uitgevoerd en betrokkenen dienen zich bewust te zijn van mogelijke risico's. Voorts moeten verwerkingsverantwoordelijken, voor zover mogelijk, op een zodanige wijze handelen dat ze prompt tegemoetkomen aan de wensen van de betrokkene, vooral wanneer zijn/haar toestemming de rechtsgrondslag voor de gegevensverwerking vormt.

Voorbeeld: In de zaak *K.H. e.a./Slowakije*[272], waren de verzoeksters acht vrouwen van Roma-afkomst die in twee ziekenhuizen in het oosten van Slowakije waren behandeld tijdens hun zwangerschap en de bevalling. Naderhand kon geen van de vrouwen meer zwanger worden, ondanks herhaalde pogingen daartoe. De nationale rechtbanken hadden verordend dat de ziekenhuizen de verzoeksters en hun vertegenwoordigers inzage in de medische dossiers moesten bieden en daarbij de mogelijkheid kregen om handgeschreven aantekeningen te maken, maar hadden hun verzoek om fotokopieën te maken verworpen met het argument dat potentieel misbruik moest worden voorkomen. De positieve verplichtingen van de staat uit hoofde van artikel 8 van het EVRM omvatten noodzakelijkerwijs een verplichting om kopieën van de dossiers over de betrokkene beschikbaar te stellen. Het was aan de staat om de regelingen voor het kopiëren van persoonlijke dossiers te bepalen, of, indien passend, om zwaarwegende redenen aan te voeren om dit niet toe te staan. In het geval van de verzoeksters hadden de nationale rechtbanken het verbod op het maken van kopieën van medische dossiers voornamelijk gerechtvaardigd op grond van de noodzaak om de desbetreffende informatie te beschermen tegen misbruik. Het EHRM kon echter niet zien hoe de verzoeksters, die in elk geval inzage hadden gekregen in hun volledige medische dossiers, misbruik zouden kunnen maken van informatie over henzelf. Bovendien kon het risico van een dergelijk misbruik op andere wijze worden voorkomen dan door

271 Algemene verordening gegevensbescherming, artikel 5, lid 1, onder a); Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder a).

272 EHRM, *K.H. e.a./Slowakije*, nr. 32881/04, 28 april 2009.

de verzoeksters kopieën van de dossiers te ontzeggen, bijvoorbeeld door het aantal personen dat recht op toegang tot de dossiers had te beperken. De staat had verzuimd om het bestaan aan te tonen van voldoende zwaarwegende redenen voor het weigeren aan de verzoeksters van effectieve toegang tot informatie over hun gezondheid. Het Hof concludeerde dat er een inbreuk op artikel 8 had plaatsgevonden.

Met betrekking tot internetdiensten moeten de eigenschappen van de gegevensverwerkingssystemen het voor betrokkenen mogelijk maken om daadwerkelijk te begrijpen wat er met hun gegevens gebeurt. In ieder geval moet het beginsel van behoorlijkheid verder gaan dan transparantieverplichtingen en zou ook kunnen worden verbonden aan de verwerking van persoonsgegevens op een ethische manier.

Voorbeeld: Een onderzoeksafdeling in een universiteitsfaculteit voert een experiment uit over stemmingsveranderingen op 50 personen. Zij moeten elk uur, op gegeven tijden, hun gedachten opschrijven. De 50 personen gaven hun toestemming voor dit specifieke project en voor het specifieke gebruik van de gegevens door de universiteit. De onderzoeksafdeling ontdekt al snel dat het elektronisch registreren van gedachten zeer nuttig zou zijn voor een ander project dat zich toespitst op geestelijke gezondheid, onder coördinatie van een ander team. Hoewel de universiteit, als verwerkingsverantwoordelijke, dezelfde gegevens zou kunnen hebben gebruikt voor het werk van een ander team zonder verdere stappen te ondernemen om de rechtmatigheid van de verwerking van die gegevens te verzekeren, gezien het feit dat de doeleinden verenigbaar zijn, informeerde de universiteit de betrokkenen en vroeg voor een nieuwe toestemming, zich zo houdend aan zijn ethische onderzoekscode en het beginsel van eerlijke verwerking.

3.1.3. Transparantie van de verwerking

Het Unierecht en het recht van de Raad van Europa inzake gegevensbescherming eisen dat persoonsgegevens "op een transparante manier ten opzichte van de betrokkene" worden verwerkt[273].

273 Algemene verordening gegevensbescherming, artikel 5, lid 1, onder a); Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder a), en artikel 8.

Dit beginsel voert de verplichting in voor de verwerkingsverantwoordelijke om passende maatregelen te nemen om ervoor te zorgen dat de betrokkenen, die gebruikers, afnemers of cliënten kunnen zijn, geïnformeerd worden over de wijze waarop hun gegevens worden gebruikt[274]. Transparantie kan wijzen op de informatie die aan de persoon wordt gegeven vóór de start van de verwerking[275], op de informatie die gemakkelijk toegankelijk moet zijn voor betrokkenen tijdens de verwerking[276], maar ook op de informatie die aan betrokkenen wordt gegeven na een verzoek tot toegang tot hun gegevens[277].

Voorbeeld: In de zaak van *Haralambie/Roemenië*[278] kreeg de verzoeker enkel toegang tot de informatie die de geheime dienst van hem bijhield, vijf jaar na zijn aanvraag. Het EHRM herhaalde dat natuurlijke personen die het voorwerp waren van persoonlijke dossiers die door overheidsautoriteiten werden bewaard een vitaal belang hadden bij het hebben van toegang tot die dossiers. De autoriteiten hadden de plicht om te voorzien in een effectieve procedure voor het verkrijgen van toegang tot deze informatie. Het EHRM stelde dat noch de kwantiteit van de overgedragen dossiers, noch de tekortkomingen in het archiveringssysteem een vertraging van vijf jaar bij het inwilligen van het verzoek van verzoeker om zijn dossiers te kunnen inzien, rechtvaardigden. De autoriteiten hadden de verzoeker geen effectieve en toegankelijke procedure ter beschikking gesteld om hem in staat te stellen binnen een redelijke termijn inzage in zijn persoonlijke dossier te krijgen. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Verwerkingen moeten aan de betrokkenen worden uitgelegd op een gemakkelijk toegankelijke manier die ervoor zorgt dat ze begrijpen wat er met hun gegevens gebeurt. Dit betekent dat het specifieke doel van de verwerking van persoonsgegevens bekend moet zijn bij de betrokkene op het ogenblik dat de persoonsgegevens worden verzameld[279]. De transparantie van de verwerking vereist dat een duidelijke

274 Algemene verordening gegevensbescherming, artikel 12.

275 *Ibid.*, artikel 13 en 14.

276 Groep artikel 29, *Advies 2/2017 voor de gegevensverwerking op het werk*, WP 249, blz. 23.

277 Algemene verordening gegevensbescherming, artikel 15.

278 EHRM, *Haralambie/Roemenië*, nr. 21737/03, 27 oktober 2009.

279 Algemene verordening gegevensbescherming, overweging 39.

en eenvoudige taal wordt gebruikt[280]. Het moet duidelijk zijn voor de betrokkenen wat de risico's, regels, waarborgen en rechten zijn met betrekking tot de verwerking van hun persoonsgegevens[281].

Het recht van de Raad van Europa geeft ook aan dat bepaalde essentiële informatie verplicht moet worden verstrekt aan de betrokkenen op proactieve wijze door de verwerkingsverantwoordelijke. Informatie over de naam en het adres van de verwerkingsverantwoordelijke (of medeverwerkingsverantwoordelijken), de rechtsgrond en de doeleinden van de gegevensverwerking, de categorieën van gegevens die worden verwerkt en ontvangers, alsmede de wijze van uitoefening van de rechten kan worden verstrekt in een geschikte vorm (hetzij via een website, technologische instrumenten op eigen apparaten enz.) zolang de informatie op eerlijke en doeltreffende wijze wordt gepresenteerd aan de betrokkene. De gepresenteerde informatie moet gemakkelijk toegankelijk, leesbaar, begrijpelijk en aangepast aan de relevante betrokkenen zijn (met, indien nodig, een kindvriendelijke taal, bijvoorbeeld). Alle aanvullende informatie die nodig is om een eerlijke verwerking te waarborgen of die nuttig is voor een dergelijk doeleinde, zoals de periode van bewaring, de motivering van de gegevensverwerking of informatie over de doorgifte van gegevens naar een ontvanger in een andere partij of niet-partij (met inbegrip van de vraag of die specifieke niet-partij een passend niveau van bescherming biedt of de maatregelen genomen door de verwerkingsverantwoordelijke zo'n passend niveau van bescherming van gegevens garandeert) moet ook worden verstrekt[282].

Overeenkomstig het recht op toegang[283] heeft de betrokkene het recht om op zijn/haar verzoek van de verwerkingsverantwoordelijke te weten te komen of zijn/haar gegevens worden verwerkt en, zo ja, welke gegevens onderworpen zijn aan een dergelijke verwerking[284]. Daarnaast dienen, overeenkomstig het recht op informatie[285], de personen wiens gegevens worden verwerkt, proactief geïnformeerd te worden door verwerkingsverantwoordelijken of verwerkers over onder andere de doeleinden, de lengte en middelen voor de verwerking, in beginsel voor de verwerkingsactiviteit van start gaat.

280 *Ibid.*

281 *Ibid.*

282 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 68.

283 Algemene verordening gegevensbescherming, artikel 15.

284 Gemoderniseerd Verdrag 108, artikel 8 en artikel 9, lid 1, onder b).

285 Algemene verordening gegevensbescherming, artikelen 13 en 14.

Voorbeeld: De zaak *Smaranda Bara e.a./Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)*[286] betrof de overdracht van fiscale gegevens over het inkomen van zelfstandigen van de nationale belastingdienst naar het Nationale Ziekteverzekeringsfonds in Roemenië, op basis waarvan de betaling van achterstallige betalingen van de zorgverzekering werd vereist. Het HvJ-EU werd gevraagd om na te gaan of er voorafgaande informatie had moeten worden gegeven aan de betrokkene met betrekking tot de identiteit van de verwerkingsverantwoordelijke van de gegevens en het doel van de overdracht van de gegevens voordat het Nationaal Ziekteverzekeringsfonds de gegevens verwerkte. Het HvJ-EU oordeelde dat indien een overheidsdienst van een lidstaat persoonsgegevens overdraagt aan een andere overheidsdienst die deze gegevens verder verwerkt, de betrokkene in kennis moet worden gesteld over die overdracht of verwerking.

In bepaalde situaties kunnen derogaties worden toegestaan van de verplichting om betrokkenen te informeren over gegevensverwerking, en deze komen nader aan bod in punt 6.1 over de rechten van de betrokkene.

3.2. Het beginsel van doelbinding

Belangrijkste punten

- Het doeleinde van de verwerking van gegevens moet zijn omschreven voordat de verwerking van start gaat.
- Er kan geen verdere verwerking van gegevens zijn op een wijze die onverenigbaar is met het oorspronkelijke doeleinde, hoewel de algemene verordening gegevensbescherming uitzonderingen op deze regel voorziet voor het archiveren voor het algemeen belang, voor wetenschappelijke of historische onderzoeksdoeleinden en statistische doeleinden.
- In wezen betekent het beginsel van doelbinding dat elke verwerking van persoonsgegevens moet gebeuren voor een specifiek en duidelijk omschreven doeleinde en enkel voor aanvullende, gespecificeerde doeleinden die verenigbaar zijn met het originele doeleinde.

286 HvJ-EU, zaak C-201/14, *Smaranda Bara e.a./Casa Naţională de Asigurări de Sănătate e.a.*, 1 oktober 2015, punten 28-46.

Het beginsel van doelbinding is een van de fundamentele beginselen van de Europese wetgeving inzake gegevensbescherming. Het is sterk verbonden met transparantie, voorspelbaarheid en controle op de gebruikers: indien het doeleinde van de verwerking voldoende specifiek en duidelijk genoeg is, weten personen wat te verwachten en wordt de transparantie en rechtszekerheid vergroot. Tegelijkertijd is een duidelijke afbakening van het doeleinde belangrijk om betrokkenen in staat te stellen om daadwerkelijk hun rechten, zoals het recht om bezwaar te maken tegen de verwerking, uit te oefenen[287].

Het beginsel vereist dat elke verwerking van persoonsgegevens moet gebeuren voor een specifiek en duidelijk omschreven doeleinde en enkel voor aanvullende, gespecificeerde doeleinden die verenigbaar zijn met het originele doeleinde[288]. De verwerking van persoonsgegevens voor onbepaalde en/of onbeperkte doeleinden is dus onrechtmatig. Het verwerken van persoonsgegevens zonder een bepaald doel, slechts gebaseerd op de overweging dat ze op een bepaald moment van nut kunnen zijn in de toekomst, is ook niet rechtmatig. De rechtmatigheid van de verwerking van persoonsgegevens is afhankelijk van het doel van de verwerking, die expliciet, specifiek en rechtmatig moet zijn.

Elk nieuw doeleinde van de verwerking van gegevens dat niet verenigbaar is met het originele doeleinde, moet zijn eigen specifieke rechtsgrondslag hebben en mag niet worden gebaseerd op het feit dat de gegevens oorspronkelijk waren verworven of verwerkt voor een ander rechtmatig doeleinde. Op haar beurt is elke rechtmatige verwerking beperkt tot het oorspronkelijk gespecificeerde doeleinde en zal voor een nieuw doeleinde van de verwerking een afzonderlijke, nieuwe rechtsgrondslag nodig zijn. Bijvoorbeeld, de openbaarmaking van persoonsgegevens aan derde partijen voor een nieuwe toepassing zal zorgvuldig moeten worden overwogen, aangezien een dergelijke openbaarmaking waarschijnlijk een aanvullende rechtsgrondslag nodig zal hebben, verschillend van die voor het verzamelen van gegevens.

> Voorbeeld: Een luchtvaartmaatschappij verzamelt in het kader van het maken van boekingen gegevens van haar passagiers om de vlucht naar behoren te laten verlopen. De luchtvaartmaatschappij zal gegevens nodig hebben over: zitplaatsnummers van de passagiers, bijzondere fysieke belemmeringen zoals rolstoelbenodigdheden, en speciale voedingsvereisten zoals koosjer of halal voeding. Als luchtvaartmaatschappijen worden gevraagd om deze gegevens,

287 Groep artikel 29 (2013), *Advies 3/2013 over doelbinding*, WP 203, 2 april 2013.

288 Algemene verordening gegevensbescherming, artikel 5, lid 1, onder b).

die onderdeel zijn van de PNR, over te dragen aan de immigratieautoriteiten van de luchthaven waar het vliegtuig landt, zullen deze gegevens vervolgens worden gebruikt voor immigratie- en controledoeleinden, die afwijken van het doeleinde waarvoor de gegevens oorspronkelijk waren verzameld. Voor de overdracht van deze gegevens aan een immigratieautoriteit is daarom een nieuwe en afzonderlijke rechtsgrondslag nodig.

Bij het beoordeling van de reikwijdte en grenzen van een bepaald doeleinde, baseren het Gemoderniseerd Verdrag 108 en de algemene verordening gegevensbescherming zich op het concept van verenigbaarheid: het gebruik van gegevens voor verenigbare doeleinden is toegestaan op grond van de oorspronkelijke rechtsgrondslag. Verdere verwerking van de gegevens kan derhalve niet worden uitgevoerd op een manier die onverwacht, ongepast of verwerpelijk is voor de betrokkene[289]. Om te beoordelen of de verdere verwerking als verenigbaar wordt beschouwd, moet de verwerkingsverantwoordelijke rekening houden met (onder andere):

- "een eventuele koppeling tussen die doeleinden en de doeleinden van de voorgenomen verdere verwerking;
- het kader waarin de gegevens zijn verzameld; met name de redelijke verwachtingen van de betrokkenen op basis van hun verhouding met de verwerkingsverantwoordelijke betreffende het verdere gebruik ervan;
- de aard van de persoonsgegevens;
- de gevolgen van de voorgenomen verdere verwerking voor de betrokkenen, en
- passende waarborgen bij zowel de oorspronkelijke als de voorgenomen verdere verwerkingen"[290]. Dit kan worden gedaan dankzij, bijvoorbeeld, encryptie of pseudonimisering.

Voorbeeld: Zonneschijn B.V. verwerft klantgegevens tijdens het klantenbeheer (CRM). Het bedrijf verstrekt deze gegevens vervolgens aan een direct marketingbedrijf, Maanlicht B.V., dat deze gegevens wil gebruiken

289 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 49.

290 Algemene verordening gegevensbescherming, overweging 50 en artikel 6, lid 4; memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 49.

ter ondersteuning van de marketingcampagnes van derde bedrijven. De verstrekking van gegevens door Zonneschijn B.V. voor marketing door andere bedrijven vormt een verder gebruik van gegevens voor een nieuwe toepassing, die onverenigbaar is met de CRM, het oorspronkelijke doeleinde van Zonneschijn B.V. voor het verzamelen van klantengegevens. De doorgifte van de gegevens aan Maanlicht B.V. vereist derhalve een eigen, afzonderlijke rechtsgrondslag.

Het gebruik door Zonneschijn B.V. van haar klantgegevens voor marketingdoeleinden, d.w.z. het verzenden van reclameboodschappen over haar eigen producten aan haar eigen klanten, wordt daarentegen algemeen aanvaard als een verenigbaar doeleinde.

De algemene verordening gegevensbescherming en het Gemoderniseerd Verdrag 108 verklaren dat "de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden" *a priori* als verenigbaar wordt beschouwd met het oorspronkelijke doeleinde[291]. Passende waarborgen zoals de anonimisering, de versleuteling of pseudonimisering van gegevens en elke toegangsbeperking tot de gegevens dienen voorzien te worden bij verdere verwerking van persoonsgegevens[292]. De algemene verordening gegevensbescherming voegt hieraan toe dat "[w]anneer de betrokkene zijn toestemming heeft gegeven of wanneer de verwerking gebaseerd is op Unierecht of lidstatelijk recht dat in een democratische samenleving een noodzakelijke en evenredige maatregel vormt voor met name het waarborgen van belangrijke doelstellingen van algemeen belang, de verwerkingsverantwoordelijke de mogelijkheid moet hebben de persoonsgegevens verder te verwerken, ongeacht of dat verenigbaar is met de doeleinden"[293]. Bij het uitvoeren van verdere verwerking dient de betrokkene derhalve te worden geïnformeerd over de toepassing alsmede over zijn/haar rechten, zoals het recht om bezwaar te maken[294].

291 Algemene verordening gegevensbescherming, artikel 5, lid 1, onder b); Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder b). Een voorbeeld van dergelijke nationale bepalingen is de Oostenrijkse gegevensbeschermingswet (*Datenschutzgesetz*), Federal Law Gazette I nr. 165/1999, punt 46.

292 Algemene verordening gegevensbescherming, artikel 6, lid 4; Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder (b); memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 50.

293 Algemene verordening gegevensbescherming, overweging 50.

294 *Ibid.*

Voorbeeld: Zonneschijn B.V. heeft CRM-gegevens over haar klanten verzameld en opgeslagen. Het verdere gebruik van deze gegevens door Zonneschijn B.V. voor de statistische analyse van het koopgedrag van haar klanten is toegestaan, aangezien dit een statistisch en derhalve verenigbaar doeleinde is. Een aanvullende rechtsgrondslag, zoals toestemming van de betrokkenen, is niet nodig. Voor de verdere verwerking van persoonsgegevens voor statistische doeleinden dient Zonneschijn B.V evenwel in passende waarborgen voor de rechten en vrijheden van de betrokkene te voorzien. De technische en organisatorische maatregelen die Zonneschijn B.V. treft, kunnen de pseudonimisering van persoonsgegevens bevatten.

3.3. Het beginsel van gegevensminimalisatie

Belangrijkste punten

- De verwerking van gegevens moet worden beperkt tot hetgeen noodzakelijk is om te voldoen aan een rechtmatig doel.
- De verwerking van persoonsgegevens mag pas plaats vinden wanneer het doeleinde van de verwerking niet op redelijke wijze kan worden vervuld met andere middelen.
- De verwerking van gegevens mag niet onevenredig zwaar interfereren met de belangen, de rechten en vrijheden die hier spelen.

Alleen die gegevens worden verwerkt die "toereikend, ter zake dienend en niet bovenmatig (...) zijn, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt"[295]. De categorieën gegevens die voor de verwerking worden gekozen, moeten noodzakelijk zijn om de aangegeven algemene doelstelling van de verwerking te bereiken, en een verwerkingsverantwoordelijke moet de verzameling van gegevens strikt beperken tot de informatie die rechtstreeks verband houdt met het specifieke doeleinde van de verwerking.

295 Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder c); algemene verordening gegevensbescherming, artikel 5, lid 1, onder c).

Voorbeeld: In de zaak *Digital Rights Ireland*[296] oordeelde het HvJ-EU over de geldigheid van de richtlijn gegevensbewaring, die gericht is op de harmonisatie van de nationale bepalingen voor het bewaren van persoonsgegevens die zijn gegenereerd of verwerkt door publiek beschikbare elektronische communicatiediensten of -netwerken voor de eventuele overdracht aan bevoegde autoriteiten ter bestrijding van zware criminaliteit, zoals georganiseerde misdaad en terrorisme. Niettegenstaande het feit dat dit werd beschouwd als een doel dat daadwerkelijk voldoet aan een doelstelling van algemeen belang, werd de algemene manier waarop de richtlijn betrekking heeft op "alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel zware criminaliteit te bestrijden", als problematisch aangemerkt[297].

Voorts, door gebruik te maken van speciale privacybevorderende technologieën, is het soms mogelijk om het gebruik van persoonsgegevens te voorkomen, of om gebruik te maken van maatregelen die de mogelijkheid om gegevens aan een betrokkene toe te schrijven (bijvoorbeeld door de pseudonimisering van persoonsgegevens), verminderen, wat resulteert in een privacy-vriendelijke oplossing. Dit is met name passend in uitgebreidere verwerkingssystemen.

Voorbeeld: Een gemeentebestuur biedt regelmatige gebruikers van het openbaarvervoerssysteem van de gemeente tegen een bepaalde vergoeding een chipkaart aan. De naam van de gebruiker wordt vermeld op de kaart en ook in elektronische vorm in de chip. Steeds wanneer gebruik wordt gemaakt van een bus of een tram, moet de chipkaart voor het in het voertuig geïnstalleerde afleesapparaat worden gehouden. De gegevens die het apparaat afleest worden elektronisch gecontroleerd in een databank met de namen van de personen die de reiskaart hebben aangeschaft.

Dit systeem voldoet niet optimaal aan het beginsel van gegevensminimalisering: nagaan of een persoon gebruik mag maken van transportmogelijkheden kan gebeuren zonder de persoonsgegevens

296 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en Kärntner Landesregierung e.a. [Grote kamer], 8 april 2014.

297 *Ibid.*, punten 44 en 57.

op de chip van de kaart met een databank te vergelijken. Daarvoor zou het bijvoorbeeld volstaan om een in de chip van de kaart geïntegreerde speciale elektronische afbeelding, zoals een barcode, te laten aflezen door het afleesapparaat, waardoor zou worden bevestigd of de kaart geldig is of niet. In een dergelijk systeem zou niet worden vastgelegd wie welk vervoersmiddel gebruikt op welk tijdstip. Dit zou de optimale oplossing zijn in de zin van het beginsel van gegevensminimalisering, omdat dit beginsel resulteert in de verplichting om de gegevensverzameling te minimaliseren.

Artikel 5, lid 1, van het Gemoderniseerd Verdrag 108 bevat een evenredigheidsvereiste voor de verwerking van persoonsgegevens in verband met het rechtmatige doel dat wordt nagestreefd. Er moet een billijk evenwicht bestaan tussen alle betrokken belangen in alle stadia van de verwerking. Dit betekent dat "persoonsgegevens die passend en relevant zijn, maar zouden leiden tot een onevenredige inmenging in de grondrechten en fundamentele vrijheden in kwestie, als buitensporig zouden moeten worden aangemerkt"[298].

3.4. Het beginsel van juistheid van de gegevens

Belangrijkste punten

- Het beginsel inzake de juistheid van de gegevens moet worden toegepast door de verwerkingsverantwoordelijke in alle verwerkingsverrichtingen.
- Onjuiste gegevens moeten onverwijld worden gewist of rechtgezet.
- De gegevens moeten regelmatig worden gecontroleerd en bijgewerkt om de juistheid te waarborgen.

Een verwerkingsverantwoordelijke bij wie persoonlijke informatie berust mag die informatie niet gebruiken zonder stappen te ondernemen die er met redelijke zekerheid voor zorgen dat de gegevens nauwkeurig en actueel zijn[299].

298 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 52; algemene verordening gegevensbescherming, artikel 5, lid 1, onder c).

299 Algemene verordening gegevensbescherming, artikel 5, lid 1, onder d); Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder d).

De verplichting om voor de juistheid van de gegevens te zorgen moet worden gezien in de context van het doel van de gegevensverwerking.

Voorbeeld: In de zaak *Rijkeboer*[300] beoordeelde het HvJ-EU het verzoek van een Nederlandse burger om informatie van de lokale overheid van de stad Amsterdam te ontvangen over de identiteit van de personen aan wie de gegevens over hem, die in het bezit waren van de gemeente, tijdens de twee voorgaande jaren werden meegedeeld evenals over de inhoud van de meegedeelde gegevens. Het HvJ-EU heeft verklaard dat "het recht op privacy betekent dat de betrokkene kan worden verzekerd dat zijn persoonsgegevens worden verwerkt op een correcte en rechtmatige wijze, dat wil zeggen, met name, dat de hem betreffende basisgegevens juist zijn en dat ze zijn overgemaakt aan erkende ontvangers." Het HvJ-EU verwees toen naar de preambule van de richtlijn gegevensbescherming die bepaalt dat betrokkenen het recht moeten hebben op toegang tot hun persoonsgegevens om na te gaan dat de gegevens correct zijn[301].

Ook kunnen er gevallen zijn waarin het actualiseren van opgeslagen gegevens wettelijk is verboden omdat het doel van de opslag van de gegevens in essentie was om gebeurtenissen te documenteren als een historische opname.

Voorbeeld: Een medisch dossier van een operatie mag niet worden gewijzigd, of anders gezegd "geactualiseerd", ook niet als in het dossier genoemde bevindingen later verkeerd blijken te zijn. In dergelijke omstandigheden mogen uitsluitend aanvullingen op de opmerkingen in het dossier worden toegevoegd, zolang ze duidelijk worden gemarkeerd als in een later stadium toegevoegde bijdragen.

Anderzijds zijn er situaties waarin het regelmatig controleren van de juistheid van de gegevens, met inbegrip van het actualiseren ervan, een absolute noodzaak is vanwege de potentiële schade die kan worden veroorzaakt voor de betrokkene als de gegevens onnauwkeurig zouden zijn.

300 HvJ-EU, zaak C-553/07, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, 7 mei 2009.

301 Voormalige overweging 41, de preambule van Richtlijn 95/46/EG.

Voorbeeld: Als iemand een kredietovereenkomst wil sluiten met een bankinstelling, zal de bank doorgaans de kredietwaardigheid van de toekomstige klant controleren. Voor dit doel zijn speciale databanken beschikbaar met gegevens over de kredietgeschiedenis van particuliere personen. Indien een dergelijke databank onjuiste of verouderde gegevens over een persoon bevat, kan deze persoon met negatieve gevolgen worden geconfronteerd. Verwerkingsverantwoordelijken van dergelijke databanken moeten daarom bijzondere inspanningen verrichten om het beginsel van juistheid te volgen.

3.5. Het beginsel van de beperking van de opslag

Belangrijkste punten

- Het beginsel van de beperking van de opslag betekent dat persoonsgegevens gewist of geanonimiseerd moeten worden zodra ze niet langer noodzakelijk zijn voor de doeleinden waarvoor ze zijn verzameld.

Artikel 5, lid 1, onder e), van de algemene verordening gegevensbescherming en ook artikel 5, lid 4, onder e), van het Gemoderniseerd Verdrag 108 vereisen dat persoonsgegevens "die het mogelijk maken de betrokkenen te identificeren niet langer mogen worden bewaard dan voor de verwezenlijking van de beoogde doeleinden noodzakelijk is". De gegevens moeten daarom worden verwijderd of geanonimiseerd wanneer de doeleinden zijn verwezenlijkt. Met het oog daarop "dient de voor de verwerking verantwoordelijke termijnen vast te stellen voor het wissen van persoonsgegevens of voor een periodieke toetsing" om zich ervan te vergewissen dat gegevens niet langer dan nodig worden bewaard[302].

In zaak *S. en Marper* concludeerde het EHRM dat de kernbeginselen van de relevante instrumenten van de Raad van Europa en de wet en praktijken van de andere overeenkomst sluitende partijen vereisen dat de bewaring van gegevens evenredig

302 Algemene verordening gegevensbescherming, overweging 39.

is met het doeleinde van de gegevensverzameling en moet worden beperkt in de tijd, in het bijzonder in de politiesector[303].

> Voorbeeld: In *S. en Marper*[304] oordeelde het EHRM dat het onbeperkt opslaan van vingerafdrukken, monsters van cellen en DNA-profielen van de twee verzoekers onevenredig en onnodig was in een democratische samenleving, omdat de strafprocedures tegen beide verzoekers waren beëindigd door respectievelijk een vrijspraak en stopzetting.

De tijdsbeperking voor de opslag van persoonsgegevens is alleen van toepassing op gegevens die worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren. De rechtmatige opslag van gegevens die niet langer noodzakelijk zijn zou derhalve kunnen worden bereikt door anonimisering van de gegevens.

De archivering van gegevens voor het openbaar belang, voor wetenschappelijke of historische doeleinden of voor statistisch gebruik, mag gedurende langere tijd worden opgeslagen indien dergelijke gegevens uitsluitend voor de bovengenoemde doeleinden worden gebruikt[305]. Passende technische en organisatorische maatregelen voor de voortdurende opslag en het voortdurende gebruik van persoonsgegevens moeten worden uitgevoerd om de rechten en vrijheden van de betrokkenen te waarborgen.

Het Gemoderniseerd Verdrag 108 staat eveneens uitzonderingen op het beginsel van de beperking van de opslag toe, op voorwaarde dat ze door de wet worden voorzien, de essentie van de grondrechten en fundamentele vrijheden respecteren en noodzakelijk en evenredig zijn om een beperkt aantal rechtmatige doelen na te streven[306]. Deze omvatten, onder meer, de bescherming van de nationale veiligheid, het onderzoek naar en de vervolging van strafbare feiten, de uitvoering van strafrechtelijke sancties, de bescherming van betrokkenen en de rechten en fundamentele vrijheden van anderen.

303 EHRM, *S. en Marper/Verenigd Koninkrijk* [Grote kamer], nrs. 30562/04 en 30566/04, 4 december 2008; zie ook bijvoorbeeld: EHRM, *M.M./Verenigd Koninkrijk*, nr. 24029/07, 13 november 2012.

304 EHRM, *S. en Marper/Verenigd Koninkrijk* [Grote kamer], nrs. 30562/04 en 30566/04, 4 december 2008.

305 Algemene verordening gegevensbescherming, artikel 5, lid 1, onder e); Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder b), en artikel 11, lid 2.

306 Gemoderniseerd Verdrag 108, artikel 11.1; memorie van toelichting bij Gemoderniseerd Verdrag 108, punten 91-98.

Voorbeeld: In de zaak *Digital Rights Ireland*[307] herzag het HvJ-EU de geldigheid van de richtlijn gegevensbewaring, die gericht is op de harmonisatie van de nationale bepalingen voor de bewaring van persoonsgegevens die zijn gegenereerd of verwerkt door publiek beschikbare elektronische communicatiediensten of -netwerken ter bestrijding van zware criminaliteit, zoals georganiseerde misdaad en terrorisme. De richtlijn gegevensbewaring legde een bewaringstermijn op van "ten minste zes maanden [...], zonder dat enig onderscheid wordt gemaakt tussen de in artikel 5 van deze richtlijn genoemde categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel of naargelang van de betrokken personen"[308]. Het HvJ-EU voerde het ontbreken aan van objectieve criteria in de richtlijn gegevensbewaring, op basis waarvan de exacte periode van de bewaring van gegevens, die kan variëren van een minimum van zes maanden tot een maximum van 24 maanden, moet worden vastgesteld om ervoor te zorgen dat een dergelijke periode tot het strikt noodzakelijke is beperkt[309].

3.6. Het beginsel van gegevensbeveiliging

Belangrijkste punten

- De beveiliging en vertrouwelijkheid van persoonsgegevens zijn belangrijk om nadelige gevolgen voor de betrokkene te voorkomen.
- Beveiligingsmaatregelen kunnen van technische en/of organisatorische aard zijn.
- Pseudonimisering is een proces dat persoonsgegevens kan beschermen.
- De geschiktheid van de beveiligingsmaatregelen moeten per geval worden vastgesteld en regelmatig worden geëvalueerd.

Het beginsel van gegevensbeveiliging schrijft voor dat passende technische of organisatorische maatregelen worden genomen bij de verwerking van persoonsgegevens om de gegevens te beschermen tegen onopzettelijk(e), onbevoegd(e) of onrechtmatig(e) toegang, gebruik, wijziging, onthulling, verlies, vernietiging of

307 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en Kärntner Landesregierung e.a. [Grote kamer], 8 april 2014.

308 *Ibid.*, punt 63.

309 *Ibid.*, punt 64.

beschadiging[310]. De algemene verordening gegevensbescherming stelt dat de verwerkingsverantwoordelijke en de verwerker rekening moeten houden met "de stand van de techniek, de uitvoeringskosten alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen" bij het uitvoeren van zulke maatregelen[311]. Afhankelijk van de specifieke omstandigheden van elk geval kan men bij passende technische en organisatorische maatregelen spreken over, bijvoorbeeld, het pseudonimiseren en encrypteren van persoonsgegevens en/of het regelmatig toetsen en evalueren van de doeltreffendheid van de maatregelen om ervoor te zorgen dat de gegevensverwerking is beveiligd[312].

Zoals uiteengezet in punt 2.1.1, betekent de pseudonimisering van gegevens het vervangen van de eigenschappen in persoonsgegevens, die het mogelijk maken om de betrokkene door een pseudoniem te identificeren, en deze eigenschappen te scheiden via technische of organisatorische maatregelen. Het proces van de pseudonimisering van persoonsgegevens mag niet worden verward met het anonimiseringsproces, waar alle banden met de identificatie van de persoon worden verbroken.

Voorbeeld: De zin "Charles Spencer, geboren op dinsdag 3 april 1967, is de vader van een gezin met vier kinderen, twee jongens en twee meisjes" kan bijvoorbeeld op de volgende manier worden gepseudonimiseerd:

"C.S. 1967 is de vader van een gezin met vier kinderen, twee jongens en twee meisjes", of

"324 is de vader van een gezin met vier kinderen, twee jongens en twee meisjes", of

"YESz320l is de vader van een gezin met vier kinderen, twee jongens en twee meisjes".

310 Algemene verordening gegevensbescherming, overweging 39 en artikel 5, lid 1, onder f); Gemoderniseerd Verdrag 108, artikel 7.

311 Algemene verordening gegevensbescherming, artikel 32, lid 1.

312 *Ibid.*

Gebruikers die toegang tot gepseudonimiseerde gegevens hebben, zullen "Charles Spencer, geboren op 3 april 1967" doorgaans niet kunnen identificeren uit "324" of "YESz3201". Zulke gegevens zijn daarom veelal beter beveiligd tegen misbruik.

Het eerste voorbeeld is echter minder veilig. Indien in de zin "C.S. 1967 is de vader van een gezin met vier kinderen, twee jongens en twee meisjes" wordt gebruikt in het kleine dorp waar Charles Spencer woont, is de heer Spencer mogelijk eenvoudig herkenbaar. De methode die wordt gebruikt voor de pseudonimisering is van invloed op de effectiviteit van de gegevensbescherming.

Persoonsgegevens met versleutelde of afzonderlijk bewaarde eigenschappen worden gebruikt in tal van situaties als middel om persoonlijke identiteiten geheim te houden. Dit is met name nuttig als verwerkingsverantwoordelijken moeten zorgen dat ze met dezelfde betrokkenen te maken hebben, maar de echte identiteit van de betrokkenen niet nodig hebben of niet nodig zouden moeten hebben. Dit is bijvoorbeeld het geval wanneer een onderzoeker het verloop van een ziekte bestudeert bij patiënten van wie de identiteit alleen bekend is bij het ziekenhuis waar ze worden behandeld en waarvan de onderzoeker de gepseudonimiseerde ziektegeschiedenissen verkrijgt. Pseudonimisering is derhalve een krachtig instrument in het arsenaal van privacy-versterkende technologie. Het kan fungeren als een belangrijk element in de toepassing van "privacy door ontwerp". Privacy door ontwerp houdt in dat gegevensbescherming wordt ingebouwd in de structuur van gegevensverwerkingssystemen.

Artikel 25 van de algemene verordening gegevensbescherming, die gegevensbescherming door ontwerp behandelt, verwijst expliciet naar pseudonimisering als voorbeeld van een passende technische en organisatorische maatregel die verwerkingsverantwoordelijken moeten uitvoeren om tegemoet te komen aan de beginselen inzake gegevensbescherming en de nodige waarborgen te integreren. Daarmee voldoen verwerkingsverantwoordelijken aan de vereisten van de verordening en beschermen ze de rechten van de betrokkenen bij de verwerking van hun persoonsgegevens.

Inachtneming van een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme kan helpen om nakoming van de beveiliging van verwerkingsvoorwaarden aan te tonen[313]. In zijn Advies over de gevolgen voor gegevensbescherming van de verwerking van de persoonsgegevens van passagiers, geeft de

313 *Ibid.*, artikel 32, lid 3.

Raad van Europa andere voorbeelden van passende beveiligingsmaatregelen voor de bescherming van persoonsgegevens in systemen voor de verzameling van persoonsgegevens van passagiers. Dit omvat het bewaren van gegevens in een beveiligde fysieke ruimte, de beperking van de toegangscontrole via meervoudige logins en de bescherming van de communicatie van gegevens door sterke cryptografie[314].

> Voorbeeld: Sociale netwerksites en e-mailproviders maken het mogelijk voor gebruikers om een extra niveau van gegevensbeveiliging toe te voegen aan hun diensten door de invoering van een authenticatiemechanisme met twee niveaus. In aanvulling op het invoeren van een persoonlijk wachtwoord, moeten gebruikers een tweede aanmelding vervolledigen om hun persoonlijke account te openen. Dit kan, bijvoorbeeld, het invoeren van een beveiligingscode zijn die naar het mobiele nummer dat verbonden is aan de persoonlijke account, wordt verstuurd. Op die manier biedt de controle in twee stappen een betere bescherming van persoonsgegevens tegen ongeoorloofde toegang tot persoonlijke accounts via hacking.

De memorie van toelichting bij het Gemoderniseerd Verdrag 108 biedt bijkomende voorbeelden van passende waarborgen, zoals de uitvoering van een beroepsgeheimhoudingsplicht of de invoering van gekwalificeerde technische beveiligingsmaatregelen, zoals de versleuteling van persoonsgegevens[315]. Bij het instellen van specifieke veiligheidsmaatregelen moet de verwerkingsverantwoordelijke of — waar van toepassing — de verwerker rekening houden met verschillende elementen, zoals de aard en het volume van de verwerkte persoonsgegevens, mogelijke nadelige gevolgen voor betrokkenen en de noodzaak om een beperkte toegang tot de gegevens te hebben[316]. De huidige stand van vakkennis van gegevensbeveiligingsmethodes en -technieken voor gegevensverwerking moet in beschouwing worden genomen bij het nemen van passende veiligheidsmaatregelen. De kosten van dergelijke maatregelen moeten in verhouding staan tot de ernst en waarschijnlijkheid van potentiële risico's. Een regelmatige evaluatie van de beveiligingsmaatregelen is nodig zodat deze, indien nodig, kunnen worden bijgewerkt[317].

314 Raad van Europa, Comité voor Verdrag 108, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19 augustus 2016, blz. 9.

315 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 56.

316 *Ibid.*, punt 62.

317 *Ibid.*, punt 63.

In gevallen waarin een inbreuk op persoonsgegevens plaatsvindt, vereisen zowel het Gemoderniseerd Verdrag 108 als de algemene verordening gegevensbescherming dat de verwerkingsverantwoordelijke de bevoegde toezichthoudende autoriteit zonder nodeloze vertraging op de hoogte stelt van de inbreuk die risico's voor de rechten en vrijheden van personen met zich meebrengt[318]. Een gelijkaardige mededelingsverplichting aan de betrokkene bestaat indien de inbreuk waarschijnlijk een hoog risico inhoudt voor zijn/haar rechten en vrijheden[319]. Zulke inbreuken dienen in duidelijke en eenvoudige taal aan de betrokkenen te worden meegedeeld[320]. Indien de verwerker weet krijgt van een inbreuk in de persoonsgegevens, moet de verwerkingsverantwoordelijke onmiddellijk op de hoogte worden gesteld[321]. In bepaalde omstandigheden kunnen uitzonderingen op de kennisgevingsverplichting van toepassing zijn. De verwerkingsverantwoordelijke moet bijvoorbeeld de toezichthoudende autoriteit niet in kennis stellen indien "het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt"[322]. Het is ook niet nodig om de betrokkene in te lichten indien de uitgevoerde beveiligingsmaatregelen de gegevens onbegrijpelijk maken voor onbevoegden of wanneer verdere maatregelen ervoor zorgen dat het hoge risico niet langer kan worden verwezenlijkt[323]. Indien de mededeling van een inbreuk in verband met persoonsgegevens een onevenredige inspanning zou vergen van de verwerkingsverantwoordelijke, kan een openbare mededeling of een soortgelijke maatregel ervoor zorgen dat "betrokkenen even doeltreffend worden geïnformeerd"[324].

318 Gemoderniseerd Verdrag 108, artikel 7, lid 2; algemene verordening gegevensbescherming, artikel 33, lid 1.

319 Gemoderniseerd Verdrag 108, artikel 7, lid 2; algemene verordening gegevensbescherming, artikel 34, lid 1.

320 Algemene verordening gegevensbescherming, artikel 34, lid 2.

321 *Ibid.*, artikel 33, lid 1.

322 *Ibid.*

323 *Ibid.*, artikel 34, lid 3, onder a) en b).

324 *Ibid.*, artikel 34, lid 3, onder c).

3.7. De verantwoordingsplicht

Belangrijkste punten

- Verantwoordingsplicht vereist van de verwerkingsverantwoordelijken en de verwerkers dat ze voortdurend actief maatregelen uitvoeren om bescherming van gegevens in hun verwerkingsactiviteiten te bevorderen en te waarborgen.
- Verwerkingsverantwoordelijken en verwerkers zijn ervoor verantwoordelijk dat hun verwerkingsverrichtingen conform zijn met de wetgeving inzake gegevensbescherming en hun respectieve verplichtingen.
- Verwerkingsverantwoordelijken moeten te allen tijde kunnen aantonen dat ze conform zijn met de voorschriften inzake gegevensbescherming aan betrokkenen, het grote publiek en toezichthoudende autoriteiten. Verwerkers moeten tevens voldoen aan bepaalde verplichtingen die strikt verband houden met verantwoordingsplicht (zoals het bijhouden van een register van alle verwerkingen van persoonsgegevens en de benoeming van een functionaris voor gegevensbescherming).

De algemene verordening gegevensbescherming en het Gemoderniseerd Verdrag 108 verklaren dat de verwerkingsverantwoordelijke verantwoordelijk is voor, en moet kunnen aantonen dat hij conform is met, de beginselen voor gegevensverwerking die in dit hoofdstuk werden beschreven[325]. Hiervoor moet de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen nemen[326]. Hoewel het beginsel van de verantwoordingsplicht in artikel 5, lid 2, van de algemene verordening gegevensbescherming enkel gericht is aan de verwerkingsverantwoordelijken, wordt er van verwerkers ook verwacht dat ze verantwoording afleggen, aangezien zij moeten voldoen aan verschillende verplichtingen en ze nauw verbonden zijn met de verantwoordingsplicht.

Het Unierecht en het recht van de Raad van Europa inzake gegevensbescherming bepalen ook dat de verwerkingsverantwoordelijke verantwoordelijk is voor de inachtneming van de beginselen inzake gegevensbescherming besproken in punten 3.1 tot 3.6, en deze moet kunnen waarborgen[327]. Groep artikel 29 wijst erop dat "het

325 *Ibid.*, artikel 5, lid 2; Gemoderniseerd Verdrag 108, artikel 10, lid 1.

326 Algemene verordening gegevensbescherming, artikel 24.

327 *Ibid.*, artikel 5, lid 2; Gemoderniseerd Verdrag 108, artikel 10, lid 1.

soort procedures en mechanismen zou afhangen van de risico's die de verwerking en de aard van de gegevens met zich meebrengen"[328].

Verwerkingsverantwoordelijken kunnen de inachtneming van deze eis vergemakkelijken op verschillende manieren, waaronder:

- verwerkingsactiviteiten opslaan en ze beschikbaar stellen aan de toezichthoudende autoriteit op haar verzoek[329];
- in bepaalde situaties een functionaris voor gegevensbescherming aanwijzen die betrokken is bij alle kwesties in verband met de bescherming van persoonsgegevens[330];
- een gegevensbeschermingseffectbeoordeling verrichten voor de soorten verwerkingen die vermoedelijk zullen leiden tot een groot risico voor de rechten en vrijheden van natuurlijke personen[331];
- gegevensbescherming door ontwerp en door standaardinstellingen verzekeren[332];
- regels en procedures toepassen voor de uitoefening van de rechten van de betrokkenen[333];
- zich houden aan erkende gedragscodes of certificatiemechanismen[334].

Hoewel het verantwoordingsbeginsel in artikel 5, lid 2, van de algemene verordening gegevensbescherming niet specifiek gericht is aan de verwerkers, zijn er bepalingen betreffende de verantwoordingsplicht die ook verplichtingen voor hen inhouden, zoals het bijhouden van een register van de verwerkingsactiviteiten en het aanstellen van een functionaris voor gegevensbescherming voor alle

328 Groep artikel 29, *Advies 3/2010 over het verantwoordingsbeginsel*, WP 173, Brussel, 13 juli 2010, punt 12.

329 Algemene verordening gegevensbescherming, artikel 30.

330 *Ibid.*, artikelen 37-39.

331 *Ibid.*, artikel 35; Gemoderniseerd Verdrag 108, artikel 10, lid 2.

332 Algemene verordening gegevensbescherming, artikel 25; Gemoderniseerd Verdrag 108, artikel 10, leden 2 en 3.

333 *Ibid.*, artikel 12 en artikel 24.

334 *Ibid.*, artikel 40 en artikel 42.

verwerkingsactiviteiten die dit vereisen[335]. Verwerkers moeten er ook voor zorgen dat alle maatregelen werden uitgevoerd die nodig zijn om de veiligheid van de gegevens te verzekeren[336]. Het juridisch bindend contract tussen de verwerkingsverantwoordelijke en de verwerker moet vermelden dat de verwerker de verwerkingsverantwoordelijke zal bijstaan in bepaalde vereisten inzake naleving, zoals bij het uitvoeren van een gegevensbeschermingseffectbeoordeling van elke inbreuk in verband met persoonsgegevens zodra ze hiervan kennis nemen[337].

De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) heeft in 2013 privacyrichtsnoeren vastgesteld waarin wordt bepaald dat voor de verwerking verantwoordelijken een belangrijke rol hebben bij het in de praktijk laten werken van gegevensbescherming. De richtsnoeren bevatten een verantwoordingsbeginsel in de zin dat "een voor de verwerking verantwoordelijke verantwoording moet afleggen over de naleving van maatregelen die uitvoering geven aan de hierboven omschreven [materiële] beginselen"[338].

Voorbeeld: Een voorbeeld van wetgeving waarin het verantwoordingsbeginsel wordt onderstreept is de wijziging[339] van de e-Privacy-richtlijn (Richtlijn 2002/58/EG) van 2009. Volgens artikel 4 in zijn gewijzigde vorm legt de richtlijn een verplichting op om ervoor te zorgen dat er "een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens". Wat betreft de beveiligingsbepalingen van deze richtlijn heeft de wetgever dus besloten dat er een expliciete eis moest worden ingevoerd om een beveiligingsbeleid te hebben en uit te voeren.

335 *Ibid.*, artikel 5, lid 2, artikelen 30 en 37.

336 *Ibid.*, artikel 28, lid 3, onder c).

337 *Ibid.*, artikel 28, lid 3, onder d).

338 OESO (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data*, artikel 14.

339 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van donderdag 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, PB L 337 van 18.2.2009, blz. 11.

Volgens het advies van Groep artikel 29[340] is de essentie van verantwoording de verplichting van de voor de verwerking verantwoordelijke om:

- maatregelen te nemen die — onder normale omstandigheden — waarborgen dat de gegevensbeschermingsregels worden nageleefd in de context van verwerkingen, en

- over documenten te beschikken die aan de betrokkenen en aan de toezichthoudende autoriteiten laten zien welke maatregelen zijn genomen om naleving van de gegevensbeschermingsregels te verwezenlijken.

Het verantwoordingsbeginsel vereist derhalve van voor de verwerking verantwoordelijken dat ze actief laten zien dat ze deze regels naleven en daar niet mee wachten tot ze door betrokkenen of toezichthoudende autoriteiten op tekortkomingen worden gewezen.

340 Groep artikel 29, *Advies 3/2010 over het verantwoordingsbeginsel*, WP 173, Brussel, 13 juli 2010.

4

Voorschriften van Europese gegevensbeschermings-wetgeving

EU	Behandelde onderwerpen	RvE
Regels voor de rechtmatigheid van de verwerking van gegevens		
Algemene verordening gegevensbescherming, artikel 6, lid 1, onder a) HvJ-EU, zaak C-543/09, *Deutsche Telekom AG/Bondsrepubliek Duitsland*, 2011 HvJ-EU, zaak C-536/15, *Tele2 (Netherlands) BV e.a./Autoriteit Consument en Markt (ACM)*, 2017	**Toestemming**	Aanbeveling inzake profilering, artikelen 3.4, onder b), en 3.6 Gemoderniseerd Verdrag 108, artikel 5, lid 2
Algemene verordening gegevensbescherming, artikel 6, lid 1, onder b)	**(Pre-)contractuele relatie**	Aanbeveling inzake profilering, artikel 3.4, onder b)
Algemene verordening gegevensbescherming, artikel 6, lid 1, onder c)	**Wettelijke plichten van de verwerkings-verantwoordelijke**	Aanbeveling inzake profilering, artikel 3.4, onder a)
Algemene verordening gegevensbescherming, artikel 6, lid 1, onder d)	**Vitale belangen van de betrokkene**	Aanbeveling inzake profilering, artikel 3.4, onder b)
Algemene verordening gegevensbescherming, artikel 6, lid 1, onder e) HvJ-EU, zaak C-524/06, *Huber/ Bundesrepublik Deutschland* [Grote kamer], 2008	**Algemeen belang en uitoefening van officiële autoriteit**	Aanbeveling inzake profilering, artikel 3.4, onder b)

EU	Behandelde onderwerpen	RvE
Algemene verordening gegevensbescherming, artikel 6, lid 1, onder f) HvJ-EU, zaak C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA "Rīgas satiksme"*, 2017 HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 2011	**Gerechtvaardigde belangen van anderen**	Aanbeveling inzake profilering, artikel 3.4, onder b) EHRM, *Y/Turkije*, nr. 648/10, 2015
Algemene verordening gegevensbescherming, artikel 6, lid 4	**Uitzondering op doelbinding: verdere verwerking voor andere doeleinden**	Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder b)
Regels voor de rechtmatige verwerking van gevoelige gegevens		
Algemene verordening gegevensbescherming, artikel 9, lid 1	**Algemeen verbod op verwerking**	Gemoderniseerd Verdrag 108, artikel 6
Algemene verordening gegevensbescherming, artikel 9, lid 2	**Uitzonderingen op het algemene verbod**	Gemoderniseerd Verdrag 108, artikel 6
Regels voor beveiligde verwerking		
Algemene verordening gegevensbescherming, artikel 32	**Verplichting om beveiligde verwerking te verzekeren**	Gemoderniseerd Verdrag 108, artikel 7, lid 1 EHRM, *I/Finland*, nr. 20511/03, 2008
Algemene verordening gegevensbescherming, artikelen 28 en 32, lid 1, onder b)	**Verplichting tot vertrouwelijkheid**	Gemoderniseerd Verdrag 108, artikel 7, lid 1
Algemene verordening gegevensbescherming, artikel 34 Richtlijn betreffende de persoonlijke levenssfeer en elektronische communicatie, artikel 4, lid 2	**Kennisgevingen van inbreuken**	Gemoderniseerd Verdrag 108, artikel 7, lid 2
Regels betreffende de verantwoordingsplicht en de bevordering van de naleving ervan		
Algemene verordening gegevensbescherming, artikelen 12, 13 en 14	**Transparantie in het algemeen**	Gemoderniseerd Verdrag 108, artikel 8
Algemene verordening gegevensbescherming, artikelen 37, 38 en 39	**Gegevens-beschermings-functionarissen**	Gemoderniseerd Verdrag 108, artikel 10, lid 1

EU	Behandelde onderwerpen	RvE
Algemene verordening gegevensbescherming, artikel 30	Register van de verwerkings-activiteiten	
Algemene verordening gegevensbescherming, artikelen 35 en 36	Effectbeoordeling en voorafgaande raadpleging	Gemoderniseerd Verdrag 108, artikel 10, lid 2
Algemene verordening gegevensbescherming, artikelen 33 en 34	Kennisgevingen van inbreuken	Gemoderniseerd Verdrag 108, artikel 7, lid 2
Algemene verordening gegevensbescherming, artikelen 40 en 41	Gedragscodes	
Algemene verordening gegevensbescherming, artikelen 42 en 43	Attest	
Gegevensbescherming door ontwerp en door standaardinstellingen		
Algemene verordening gegevensbescherming, artikel 25, lid 1	Gegevens-bescherming door ontwerp	Gemoderniseerd Verdrag 108, artikel 10, lid 2
Algemene verordening gegevensbescherming, artikel 25, lid 2	Gegevens-bescherming door standaard-instellingen	Gemoderniseerd Verdrag 108, artikel 10, lid 3

Beginselen zijn noodzakelijkerwijs van algemene aard. De toepassing ervan op concrete situaties laat een zekere ruimte voor interpretatie en voor de keuze van de middelen. In het **recht van de Raad van Europa** wordt het aan de partijen bij Gemoderniseerd Verdrag 108 overgelaten om deze ruimte voor interpretatie in hun nationale wetgeving in te vullen. De situatie in het **Unierecht** is verschillend: bij de invoering van gegevensbescherming in de interne markt werd het noodzakelijk geacht om op EU-niveau meer gedetailleerde regels vast te stellen om het niveau van gegevensbescherming in de nationale wetgevingen van de lidstaten te harmoniseren. De algemene verordening gegevensbescherming legt een niveau van gedetailleerde regels vast, als bepaald in artikel 5, die rechtstreeks toepasselijk zijn in de nationale rechtsorde. De volgende opmerkingen over gedetailleerde gegevensbeschermingsregels op Europees niveau hebben dan ook voornamelijk betrekking op het Unierecht.

4.1. Regels voor de rechtmatigheid van de verwerking

Belangrijkste punten

- Persoonsgegevens kunnen rechtmatig verwerkt worden als zij voldoen aan één van de volgende criteria:
  - de verwerking is gebaseerd op toestemming van de betrokkene;
  - een contractuele relatie vereist de verwerking van persoonsgegevens;
  - de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting van de verwerkingsverantwoordelijke;
  - vitale belangen van betrokkenen of van een andere persoon vereisen de verwerking van hun gegevens;
  - de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang;
  - gerechtvaardigde belangen van verwerkingsverantwoordelijken of derde partijen zijn de reden voor de verwerking, maar alleen zolang het belang van bescherming van de grondrechten van de betrokkenen niet prevaleert.
- Voor de rechtmatige verwerking van gevoelige persoonsgegevens gelden speciale, strengere regels.

4.1.1. Rechtmatige gronden voor het verwerken van gegevens

Hoofdstuk II van de algemene verordening gegevensbescherming, met als titel "Beginselen", bepaalt dat alle verwerking van persoonsgegevens in de eerste plaats in overeenstemming moet zijn met de beginselen over de kwaliteit van de gegevens bedoeld in artikel 5 van de algemene verordening gegevensbescherming. Eén van de beginselen is dat persoonsgegevens moeten worden "verwerkt op een wijze die eerlijk, rechtmatig en transparant is". Ten tweede, om gegevens op een rechtmatige wijze te verwerken, moet de verwerking een van de rechtmatige gronden in

acht nemen om gegevensverwerking rechtmatig te maken, genoemd in artikel 6[341] voor niet-gevoelige persoonsgegevens, en in artikel 9 voor bijzondere categorieën van gegevens (of gevoelige gegevens). Evenzo wordt in hoofdstuk II van het Gemoderniseerd Verdrag 108 dat "de basisbeginselen voor de bescherming van persoonsgegevens" vastlegt, bepaald dat de gegevensverwerking slechts rechtmatig kan zijn indien ze "evenredig is aan het nagestreefde rechtmatige doel".

Ongeacht de rechtmatige gronden voor het verwerken waarop verwerkingsverantwoordelijke zich baseert om een gegevensverwerking te starten, dient de verwerkingsverantwoordelijke ook de waarborgen die in het algemene rechtsstelsel van gegevensbescherming worden gesteld, toe te passen.

Toestemming

In het recht van de Raad van Europa wordt toestemming vermeld in artikel 5, lid 2, van het Gemoderniseerd Verdrag 108. Er wordt ook naar verwezen in de rechtspraak van het EHRM en in verschillende aanbevelingen van de RvE[342]. **In het Unierecht** is toestemming als basis voor een rechtmatige gegevensverwerking stevig verankerd in artikel 6 van de algemene verordening gegevensbescherming en ook expliciet vermeld in artikel 8 van het Handvest. De kenmerken van geldige toestemming worden uitgelegd in de definitie van toestemming in artikel 4 van de algemene verordening gegevensbescherming, terwijl de voorwaarden om geldige toestemming te bekomen worden gepreciseerd in artikel 7 en de bijzondere regels voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij in artikel 8.

Zoals wordt uitgelegd in punt 2.4, dient toestemming vrij, geïnformeerd, specifiek en ondubbelzinnig te zijn. Toestemming moet een verklaring of een ondubbelzinnige actieve handeling zijn die duidelijk maakt dat er akkoord wordt gegaan met de verwerking, en de persoon heeft het recht om de toestemming te allen tijde

341 HvJ-EU, gevoegde zaken C-465/00, C-138/01 en C-139/01, *Rechnungshof/Österreichischer Rundfunk e.a.* en *Neukomm en Lauermann/Österreichischer Rundfunk*, 20 mei 2003, punt 65; HvJ-EU, zaak C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [Grote kamer], 16 december 2008, punt 48; HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 november 2011, punt 26.

342 Zie bijvoorbeeld, Raad van Europa, Comité van Ministers (2010), Aanbeveling CM/Rec(2010)13 van het Comité van Ministers aan de lidstaten over de bescherming van personen met betrekking tot de automatische verwerking van persoonsgegevens in het kader van profilering, 23 november 2010, artikel 3.4, onder b).

in te trekken. Verwerkingsverantwoordelijken hebben de verplichting om een controleerbaar register van de toestemming bij te houden.

Vrije toestemming

In het kader van het Gemoderniseerd Verdrag 108 van de **Raad van Europa**, dient toestemming van de betrokkene "de vrije uitdrukking van een bewuste keuze te vertegenwoordigen"[343]. Vrije toestemming kan alleen rechtsgeldig zijn "als de betrokkene een werkelijke keuze heeft en er geen sprake is van bedrog, intimidatie of dwang en de betrokkene ook niet het risico van aanzienlijke negatieve gevolgen loopt wanneer hij/zij niet toestemt"[344]. In dit verband bepaalt **het Unierecht** dat toestemming niet wordt geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen[345]. De algemene verordening gegevensbescherming beklemtoont dat "[b]ij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt *onder meer* ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst"[346]. Het toelichtend verslag van het Gemoderniseerd Verdrag 108 bepaalt dat er geen ongepaste beïnvloeding of druk (dit kan van economische of andere aard zijn), direct of indirect kan worden uitgeoefend op de betrokkene en toestemming mag niet worden beschouwd als vrijelijk gegeven indien de betrokkene geen echte keuze heeft of de toestemming niet kan weigeren of intrekken zonder voorbehoud[347].

Voorbeeld: Een aantal gemeenten in Staat A besluiten een verblijfskaart met een ingebedde chip te ontwikkelen. Het is niet verplicht voor ingezetenen die elektronische kaarten aan te schaffen. Echter, ingezetenen die niet beschikken over de kaart, hebben geen toegang tot een reeks belangrijke administratieve diensten, zoals de mogelijkheid tot het betalen van gemeentelijke belastingen online, tot het elektronisch indienen van klachten waarbij ze genieten van een termijn van drie dagen om het antwoord van

343 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 42.

344 Zie ook Groep artikel 29 (2011), *Advies 15/2011 over de definitie van "toestemming"*, WP 187, Brussel, 13 juli 2011, blz. 12.

345 Algemene verordening gegevensbescherming, overweging 42.

346 *Ibid.*, artikel 7, lid 4.

347 Memorie van toelichting bij Gemodernideerd Verdrag 108, punt 42.

de autoriteit te ontvangen, en zelfs tot het overslaan van wachtrijen, het kopen van verlaagde tickets bij een bezoek aan de gemeentelijke concerthal en het gebruik van de scanners bij de ingang.

De verwerking van persoonsgegevens door de gemeente kan in dit voorbeeld niet gebeuren op basis van toestemming. Aangezien er ten minste een indirecte druk bestaat voor ingezetenen om de elektronische kaart aan te schaffen en in te stemmen met de verwerking, is de toestemming niet vrij. De ontwikkeling door de gemeentes van een elektronisch kaartensysteem moet derhalve worden gebaseerd op een andere rechtmatige grond die de verwerking motiveert. Zij kunnen zich bijvoorbeeld beroepen op het feit dat de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang, wat een rechtmatige grond vormt voor de verwerking op grond van artikel 6, lid 1, onder e), van de algemene verordening gegevensbescherming[348].

Het bestaan van vrije toestemming zou ook kunnen worden bedreigd in situaties van ondergeschiktheid wanneer er een significante onevenwichtige economische of andere machtsverhouding bestaat tussen de verwerkingsverantwoordelijke die toestemming verkrijgt en de betrokkene die toestemming verleent[349]. Een typisch voorbeeld van dergelijke wanverhoudingen en ondergeschiktheid is de verwerking van persoonsgegevens door een werkgever in het kader van een arbeidsverhouding. Volgens Groep artikel 29 bevinden "[w]erknemers [...] zich bijna nooit in de positie om vrijelijk toestemming te geven, te weigeren of in te trekken, gezien de afhankelijkheid die eigen is aan de relatie tussen werkgever en werknemer. Gezien de ongelijke machtsverhouding kunnen werknemers enkel vrijelijk toestemming geven in uitzonderlijke omstandigheden, indien er in geen geval gevolgen zijn verbonden aan de aanvaarding of de afwijzing van een aanbod"[350].

348 Groep artikel 29 (2011), *Advies 15/2011 over de definitie van "toestemming"*, WP 187, Brussel, 13 juli 2011, blz. 16. Andere voorbeelden van gevallen waarin de verwerking van gegevens niet kan worden gebaseerd op toestemming, maar een verschillende rechtsgrondslag is vereist om de verwerking te legaliseren, kunnen worden gevonden op blz. 14 en 17 van het advies.

349 Zie ook Groep artikel 29 (2001), *Advies 8/2001 over de verwerking van persoonsgegevens in het kader van de werkgelegenheid*, WP 48, Brussel, 13 september 2001; Groep artikel 29 (2005), werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995, WP 114, Brussel, 25 november 2005; Groep artikel 29 (2017), *Advies 2/2017 over gegevensverwerking op het werk*, WP 249, Brussel, 8 juni 2017.

350 Groep artikel 29, *Advies 2/2017 over gegevensverwerking op het werk*, WP 249, Brussel, 8 juni 2017.

Voorbeeld: Een groot bedrijf wil een gids samenstellen met de namen van alle werknemers, hun functie in het bedrijf en hun zakelijke adressen, met als enig doel het verbeteren van de interne bedrijfscommunicatie. Het hoofd personeelszaken stelt voor ook een foto van elke werknemer in de gids op te nemen om het bijvoorbeeld makkelijker te maken collega's bij vergaderingen te herkennen. Werknemersvertegenwoordigers verlangen dat dit uitsluitend gebeurt met toestemming van de werknemers zelf.

In een dergelijke situatie dient de toestemming van een werknemer te worden erkend als rechtsgrondslag voor de verwerking van de foto's in de gids omdat het aannemelijk is dat de werknemer helemaal geen gevolgen zal ondervinden indien hij of zij besluit om wel of niet in te stemmen met het publiceren van zijn/haar foto in de gids.

Voorbeeld: Een onderneming is voornemens een bijeenkomst te organiseren tussen drie werknemers en de directeuren van onderneming B om een eventuele toekomstige samenwerking aan een project te bespreken. De vergadering zal plaatsvinden in het kantoor van onderneming B, die vraagt dat onderneming A de namen, cv's en foto's van de deelnemers aan de vergadering stuurt via e-mail. Onderneming B voert aan dat ze de namen en foto's van de deelnemers nodig heeft zodat het veiligheidspersoneel aan de ingang van het gebouw kan nagaan dat ze de juiste personen zijn, terwijl de cv's de directeuren toelaten om de vergadering beter voor te bereiden. In dit geval kan de overdracht van onderneming A van de persoonsgegevens van haar werknemers niet gebeuren op basis van toestemming. De toestemming kan niet worden beschouwd als "vrijelijk gegeven", aangezien het mogelijk is dat de werknemers negatieve gevolgen ondervinden indien zij het aanbod afwijzen (ze kunnen bijvoorbeeld vervangen worden door een andere collega, niet alleen om de vergadering bij te wonen, maar ook in de samenwerking met onderneming B en in de deelname aan het project in het algemeen). Daarom moet de verwerking worden gebaseerd op een andere rechtsgrondslag voor verwerking.

Dit betekent echter niet dat toestemming nooit rechtsgeldig kan zijn in omstandigheden waarin het niet verlenen van toestemming bepaalde negatieve gevolgen kan hebben. Als bijvoorbeeld het niet verlenen van toestemming voor het verkrijgen van een klantenkaart van een supermarkt er uitsluitend toe leidt dat de betrokkene geen kleine korting op de prijs van bepaalde artikelen krijgt, kan toestemming

nog steeds een geldige rechtsgrondslag zijn voor de verwerking van de persoonsgegevens van de klanten die er wel mee hebben ingestemd om een klantenkaart te ontvangen. Er bestaat geen rangorde tussen de onderneming en de klant en de gevolgen van de weigering van de toestemming zijn niet ernstig genoeg om de vrije keuze van de betrokkene te belemmeren (op voorwaarde dat de prijsverlaging klein genoeg is om geen invloed te hebben op hun vrije keuze).

Wanneer er evenwel enkel goederen of diensten kunnen worden bekomen indien bepaalde persoonsgegevens worden meegedeeld aan de verwerkingsverantwoordelijke of vervolgens aan derde partijen, kan de toestemming van de betrokkenen om hun gegevens mee te delen niet worden gezien als een vrije keuze en is die derhalve niet geldig onder de gegevensbeschermingswetgeving[351]. De algemene verordening gegevensbescherming is vrij strikt in haar verbod op het koppelen van toestemming aan de levering van goederen en diensten[352].

Voorbeeld: Door passagiers aan een luchtvaartmaatschappij verleende toestemming om zogeheten "passenger name records", d.w.z. gegevens over hun identiteit, eetgewoonten en gezondheidsproblemen, aan de immigratieautoriteiten van een specifiek derde land door te geven, kan niet worden beschouwd als geldige toestemming krachtens de gegevensbeschermingswetgeving, aangezien de passagiers geen keuze hebben als ze het desbetreffende land willen bezoeken. Om dergelijke gegevens op rechtmatige wijze door te sturen, is er een andere rechtsgrondslag dan toestemming vereist, naar alle waarschijnlijkheid een specifieke wetgeving.

Geïnformeerde toestemming

De betrokkene moet over voldoende informatie beschikken alvorens zijn/haar keuze te maken. Geïnformeerde toestemming zal meestal bestaan uit een nauwkeurige en begrijpelijke beschrijving van het onderwerp waarvoor instemming is vereist. Zoals Groep artikel 29 uitlegt, moet toestemming worden gebaseerd op een beoordeling en begrip van de feiten en de gevolgen van de actie van de betrokkene om met de verwerking in te stemmen. Daarom moet de betrokken persoon, op duidelijke en begrijpelijke wijze, nauwkeurig en volledig in kennis worden gesteld van alle relevante aspecten [...] zoals de aard van de gegevens die worden verwerkt, de

351 Algemene verordening gegevensbescherming, artikel 7, lid 4.

352 *Ibid.*

doeleinden van de verwerking, de mogelijke begunstigden en de rechten van de betrokkene[353]. Opdat de toestemming op een geïnformeerde wijze wordt gegeven, moeten personen ook op de hoogte zijn van de gevolgen indien ze niet toestemmen met de verwerking.

Gezien het belang van de geïnformeerde toestemming, hebben de algemene verordening gegevensbescherming en het toelichtend verslag van het Gemoderniseerd Verdrag 108 getracht het begrip te verduidelijken. De overwegingen van de algemene verordening gegevensbescherming bepalen dat geïnformeerde toestemming inhoudt dat "de betrokkene ten minste bekend [moet] zijn met de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking van de persoonsgegevens"[354].

In het uitzonderlijke geval dat de toestemming wordt gebruikt als een derogatie om een rechtsgrondslag voor een internationale doorgifte van gegevens te verzekeren, moet de verwerkingsverantwoordelijke de betrokkene informeren over de mogelijke risico's van een dergelijke doorgifte als gevolg van het ontbreken van een adequaatheidsbesluit en passende waarborgen, opdat die toestemming als geldig kan worden beschouwd[355].

Het toelichtend verslag van het Gemoderniseerd Verdrag 108 bepaalt dat informatie moet worden gegeven op basis van de gevolgen van het besluit van de betrokken, namelijk "wat toestemmen met zich meebrengt en in hoeverre toestemming wordt gegeven"[356].

De kwaliteit van de informatie is belangrijk. De kwaliteit van de informatie houdt in dat de taal van de informatie moet worden aangepast aan de te verwachten ontvangers. Informatie moet worden verstrekt zonder jargon, in een duidelijke en eenvoudige taal die een normale gebruiker moet kunnen begrijpen[357]. Informatie moet ook gemakkelijk toegankelijk zijn voor de betrokkene en kan mondeling of schriftelijk worden verstrekt. Toegankelijkheid en zichtbaarheid van de informatie zijn belangrijke elementen: de informatie moet goed zichtbaar en duidelijk zijn. In

353 Groep artikel 29 (2007), Werkdocument inzake de verwerking van persoonsgegevens betreffende gezondheid in elektronische medische dossiers, WP 131, Brussel, 15 februari 2007.

354 Algemene verordening gegevensbescherming, overweging 42.

355 *Ibid.*, artikel 49, lid 1, onder a).

356 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 42.

357 Groep artikel 29 (2011), *Advies 15/2011 over de definitie van "toestemming"*, WP 187, Brussel, 13 juli 2011, blz. 19.

een online-omgeving kunnen gelaagde vooraankondigingen een goede oplossing vormen, aangezien ze betrokkenen in staat stellen te kiezen of zij toegang willen krijgen tot beknopte of uitgebreidere versies van de informatie.

Specifieke toestemming

De toestemming is geldig indien zij ook specifiek wordt gegeven voor het doel van de verwerking, die duidelijk en op ondubbelzinnige wijze moet worden beschreven. Dit gaat hand in hand met de kwaliteit van de over het doel van de toestemming verstrekte informatie. In dit verband zijn de redelijke verwachtingen van een gemiddelde betrokkene relevant. De betrokkene moet opnieuw om toestemming worden gevraagd indien verwerkingsactiviteiten worden toegevoegd of gewijzigd op een manier die redelijkerwijs niet kon worden voorzien toen de oorspronkelijke toestemming werd verleend en vervolgens leiden tot een verandering van het doel. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend[358].

Voorbeelden: In *Deutsche Telekom AG*[359] onderzocht het Hof van Justitie of een telecomaanbieder die persoonsgegevens van abonnees moest doorgeven om ze in een gids te publiceren, opnieuw de toestemming van betrokkenen moest verkrijgen[360], aangezien de ontvangers van de gegevens oorspronkelijk niet bij naam werden genoemd toen de toestemming werd gegeven.

Het HvJ-EU verklaarde dat, overeenkomstig artikel 12 van de Richtlijn betreffende privacy en elektronische communicatie, hernieuwde toestemming niet vereist was voordat de gegevens werden doorgegeven. Aangezien de betrokkenen enkel konden instemmen met het doel van de verwerking, namelijk de publicatie van hun gegevens, konden ze niet kiezen uit verschillende gidsen waarin deze gegevens konden worden bekendgemaakt.

358 Algemene verordening gegevensbescherming, overweging 32.

359 HvJ-EU, zaak C-543/09, *Deutsche Telekom AG/Bondsrepubliek Duitsland*, 5 mei 2011. Zie met name punten 53 en 54.

360 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van zaterdag 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, PB L 201 van 2002 (richtlijn betreffende privacy en elektronische communicatie).

Zoals het HvJ-EU onderstreepte, "volgt uit een contextuele en systematische uitlegging van artikel 12 van de richtlijn betreffende privacy en elektronische communicatie dat de in artikel 12, lid 2, bedoelde toestemming betrekking heeft op het doel van de publicatie van de persoonsgegevens in een openbare telefoongids, en niet op de identiteit van een telefoongidsaanbieder in het bijzonder"[361]. In aanvulling "is [het] de publicatie zelf van persoonsgegevens in een telefoongids met een bijzondere doelstelling die schadelijk kan blijken voor een abonnee"[362], en niet de identiteit van de uitgever.

Tele2 (Nederland) BV, Ziggo BV, Vodafone Libertel BV/Autoriteit Consument en Markt (ACM)[363] betrof het verzoek van een Belgische onderneming dat nummerinlichtingendiensten en gidsen naar bedrijven toe die telefoonnummers toekennen in Nederland, haar toegang zouden verlenen tot gegevens van hun abonnees. De Belgische onderneming baseerde zich op een verplichting onder de Universeledienstrichtlijn[364]. Dit vereist dat ondernemingen die telefoonnummers toekennen, de cijfers beschikbaar stellen voor telefoongidsen die hen dit verzoeken, indien abonnees hebben ingestemd met de bekendmaking van hun nummers. De Nederlandse ondernemingen weigerden dit te doen en verklaarden dat ze niet verplicht waren om deze gegevens te verstrekken aan een onderneming die in een andere lidstaat gevestigd is. Zij voerden aan dat de gebruikers hun toestemming hadden gegeven voor de bekendmaking van hun nummers, met dien verstande dat zij zouden worden bekendgemaakt in een Nederlandse telefoongids. Het HvJ-EU oordeelde dat de Universeledienstrichtlijn betrekking heeft op alle verzoeken van nummerinlichtingendiensten, ongeacht de lidstaat waar zij gevestigd zijn. Het HvJ-EU was daarnaast van mening dat de doorgifte van dezelfde gegevens aan een andere onderneming die voornemens is om een publieke telefoongids bekend te maken zonder opnieuw toelating te krijgen van de abonnees, het recht op

361 HvJ-EU, zaak C-543/09, *Deutsche Telekom AG/Bondsrepubliek Duitsland*, 5 mei 2011, punt 61.

362 *Ibid.*, punt 62.

363 HvJ-EU, zaak C-536/15, *Tele2 (Nederland) BV e.a./Autoriteit Consument en Markt (ACM)*, 15 maart 2017.

364 Richtlijn 2002/22/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten (Universeledienstrichtlijn), PB L 108 van 2002, blz. 51, zoals gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 (Universeledienstrichtlijn), PB L 337 van 2009, blz. 11.

de bescherming van persoonsgegevens wezenlijk niet kan schaden[365]. Het is derhalve niet nodig voor de onderneming die telefoonnummers toekent aan zijn abonnees om in het verzoek voor toestemming van de abonnee een onderscheid te maken tussen de lidstaten naar wie de gegevens over hem of haar kunnen worden verzonden[366].

Ondubbelzinnige toestemming

Elke toestemming moet op ondubbelzinnige wijze worden gegeven[367]. Dit betekent dat er geen redelijke twijfel mag bestaan over het feit dat de betrokkene zijn/haar toestemming wilde geven om de verwerking van zijn/haar gegevens toe te staan. Bijvoorbeeld, inactiviteit van de betrokkene wijst niet op ondubbelzinnige toestemming.

Dit zou het geval zijn voor verwerkingsverantwoordelijken die toestemming verkrijgen met verklaringen in hun privacybeleid zoals "door gebruik te maken van onze diensten, stemt u in met de verwerking van uw persoonsgegevens". In dat geval moeten verwerkingsverantwoordelijken verzekeren dat gebruikers manueel en individueel toestemming hebben verleend voor dergelijk beleid.

Indien toestemming wordt gegeven in een schriftelijke vorm die deel uitmaakt van een overeenkomst, moet toestemming voor de verwerking van persoonsgegevens afzonderlijk worden behandeld en in ieder geval "dient te worden gewaarborgd dat de betrokkene zich ervan bewust is dat hij toestemming geeft en hoever deze toestemming reikt"[368].

Eisen voor toestemming voor kinderen

De algemene verordening gegevensbescherming biedt specifieke bescherming voor kinderen in het kader van het verlenen van diensten van de informatiemaatschappij, aangezien "zij zich allicht minder bewust zijn van de betrokken risico's, gevolgen, beschermingsmaatregelen en rechten in verband met de verwerking van

365 HvJ-EU, zaak C-536/15, *Tele2 (Nederland) BV e.a./Autoriteit Consument en Markt (ACM)*, 15 maart 2017, punt 36.

366 *Ibid.*, punten 40-41.

367 Algemene verordening gegevensbescherming, artikel 4, lid 11.

368 *Ibid.*, overweging 42.

persoonsgegevens"[369]. Daarom is volgens het **EU-recht** een verwerking van persoonsgegevens van kinderen jonger dan 16 jaar door aanbieders van informatiemaatschappijdiensten op basis van toestemming slechts rechtmatig "indien en voor zover de toestemming of machtiging tot toestemming in dit verband wordt verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt"[370]. Lidstaten kunnen in het nationale recht een lagere leeftijd voorzien, maar niet lager dan 13 jaar[371]. "In de context van preventieve of adviesdiensten die rechtstreeks aan een kind worden aangeboden", is de toestemming van de persoon die de ouderlijke verantwoordelijkheid draagt, niet vereist[372]. De informatie en communicatie, wanneer de verwerking specifiek tot een kind is gericht, moet in een duidelijke en eenvoudige taal worden gesteld dat het kind makkelijk kan begrijpen[373].

Het recht om toestemming te allen tijde in te trekken

De algemene verordening gegevensbescherming omvat een algemeen recht om toestemming te allen tijde in te trekken[374]. De betrokkene moet worden geïnformeerd over een dergelijk recht voordat de toestemming wordt gegeven en hij/zij kan dit recht naar eigen goeddunken uitoefenen. Er mag geen verplichting bestaan om redenen te geven voor een intrekking en er mag geen risico bestaan op negatieve gevolgen anders dan de beëindiging van de voordelen die mogelijk voortvloeiden uit het eerder overeengekomen gebruik van de gegevens. Toestemming intrekken dient even gemakkelijk te zijn als toestemming geven[375]. Er is geen sprake van vrije toestemming als de betrokkene zijn/haar toestemming niet kan intrekken zonder nadeel of als toestemming niet even eenvoudig kan worden ingetrokken als zij werd gegeven[376].

369 *Ibid.*, overweging 38.

370 *Ibid.*, artikel 8, lid 1, eerste streepje. Het begrip "diensten van de informatiemaatschappij" wordt gedefinieerd in artikel 4, lid 25, van de algemene verordening gegevensbescherming.

371 Algemene verordening gegevensbescherming, artikel 8, lid 1, tweede streepje.

372 *Ibid.*, overweging 38.

373 *Ibid.*, overweging 58. Zie ook Gemoderniseerd Verdrag 108, artikel 15, lid 2, onder e); memorie van toelichting bij Gemoderniseerd Verdrag 108, punten 68 en 125.

374 Algemene verordening gegevensbescherming, artikel 7, lid 3; memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 45.

375 Algemene verordening gegevensbescherming, artikel 7, lid 3.

376 Algemene verordening gegevensbescherming, overweging 42; memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 42.

Voorbeeld: Een klant stemt erin toe om reclamemateriaal te ontvangen op een adres dat hij of zij opgeeft aan de verwerkingsverantwoordelijke. Mocht de klant deze toestemming weer intrekken, dan moet de verwerkingsverantwoordelijke onmiddellijk stoppen met het verzenden van het reclamemateriaal. Daar mogen geen sancties op staan, zoals boetes of vergoedingen. De intrekking evenwel wordt uitgeoefend in de toekomst en heeft geen terugwerkende kracht. De periode waarin de persoonsgegevens van de klant op rechtmatige wijze werden verwerkt, vanwege de toestemming van de klant, was legitiem. De intrekking verhindert dat deze gegevens verder worden verwerkt, tenzij deze verwerking in overeenstemming is met het recht op gegevenswissing[377].

Noodzaak voor de uitvoering van een opdracht

In het kader van het Unierecht biedt artikel 6, lid 1, onder b) van de algemene verordening gegevensbescherming een andere grondslag voor rechtmatige verwerking, namelijk "wanneer dat noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is". Deze bepaling is ook van toepassing op precontractuele relaties. Bijvoorbeeld, in gevallen waar een partij van plan is een contract te sluiten, maar dat nog niet heeft gedaan, mogelijk omdat er nog enkele controles moeten worden uitgevoerd. Als een partij met het oog hierop gegevens moet verwerken, is deze verwerking rechtmatig zolang de verwerking "nodig is voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene"[378].

Het begrip van gegevensverwerking als een "gerechtvaardigde grondslag waarin de wet voorziet" in artikel 5, lid 2, van het Gemoderniseerd Verdrag 108 omvat ook "gegevensverwerking voor de vervulling van een contract (of precontractuele maatregelen op verzoek van de betrokkene) waarbij de betrokkene partij is"[379].

377 Algemene verordening gegevensbescherming, artikel 17, lid 1, onder b).

378 *Ibid.*, artikel 6, lid 1, onder b).

379 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 46; Raad van Europa, Comité van Ministers (2010), Aanbeveling CM/Rec(2010)13 van het Comité van Ministers aan de lidstaten over de bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens in het kader van profilering, 23 november 2010, artikel 3.4, onder b).

Wettelijke plichten van de verwerkingsverantwoordelijke

Het Unierecht noemt een ander beginsel voor het rechtmatig maken van gegevensverwerkingen, namelijk dat "de verwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke onderworpen is" (artikel 6, lid 1, onder c), van de algemene verordening gegevensbescherming). Deze bepaling heeft betrekking op verwerkingsverantwoordelijken die zowel in de particuliere als publieke sector opereren; de wettelijke verplichtingen van verwerkingsverantwoordelijken in de publieke sector kunnen ook vallen onder artikel 6, lid 1, onder e), van de algemene verordening gegevensbescherming. Er bestaan tal van voorbeelden van situaties waarin de wet verwerkingsverantwoordelijken uit de particuliere sector verplicht om gegevens over concrete betrokkenen te verwerken. Bijvoorbeeld, werkgevers moeten gegevens over hun werknemers verwerken voor de sociale zekerheid en om fiscale redenen, en het bedrijfsleven moet gegevens over hun klanten verwerken voor belastingdoeleinden.

De wettelijke verplichting kan afkomstig zijn uit het Unierecht of het recht van een lidstaat, wat de basis kan vormen voor een of meer verwerkingsverrichtingen. Het is aan het recht om het doel van verwerking te bepalen, specificaties vast te stellen om de verwerkingsverantwoordelijke, het soort persoonsgegevens die verwerkt mogen worden, de betrokkenen, de entiteiten aan wie gegevens mogen worden bekendgemaakt, de doelbindingen, de opslagperiode en andere maatregelen die een rechtmatige en eerlijke verwerking verzekeren, te bepalen[380]. Een dergelijk recht dat dient als basis voor de verwerking van persoonsgegevens moet voldoen aan de artikelen 7 en 8 van het Handvest en artikel 8 van het EVRM.

De wettelijke verplichtingen van de verwerkingsverantwoordelijke dienen ook als basis voor rechtmatige gegevensverwerking **volgens het recht van de Raad van Europa**[381]. Zoals eerder gesteld zijn de wettelijke verplichtingen van een verwerkingsverantwoordelijke in de private sector slechts één specifiek geval van de gerechtvaardigde belangen van anderen, als bedoeld in artikel 8, lid 2, van het EVRM. Het voorbeeld van werkgevers die gegevens over hun werknemers verwerken is daarom ook van belang voor het recht van de Raad van Europa.

380 Algemene verordening gegevensbescherming, overweging 45.

381 Raad van Europa, Comité van Ministers (2010), Aanbeveling CM/Rec(2010)13 van het Comité van Ministers aan de lidstaten over de bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens in het kader van profilering, 23 november 2010, artikel 3.4, onder a).

Vitale belangen van de betrokkene of een andere natuurlijke persoon

In het kader van het Unierecht bepaalt artikel 6, lid 1, onder d), van de algemene verordening gegevensbescherming dat de verwerking van persoonsgegevens rechtmatig is als het "noodzakelijk [is] om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen". Deze rechtsgrondslag mag enkel worden aangevoerd voor de verwerking van persoonsgegevens op basis van de vitale belangen van een andere natuurlijke persoon, als de verwerking "duidelijk niet op een andere rechtsgrond kan worden gebaseerd"[382]. Soms kan een soort verwerking worden gebaseerd op grond van zowel openbaar belang als de vitale belangen van de betrokkene of dat van een andere persoon. Dit is bijvoorbeeld het geval bij de observatie van epidemieën en de ontwikkeling ervan, of wanneer er sprake is van een humanitaire noodsituatie.

In het recht van de Raad van Europa worden de vitale belangen van de betrokkene niet genoemd in artikel 8 van het EVRM. De vitale belangen van de betrokkene worden echter geacht geïmpliceerd te zijn in het begrip "legitieme grondslag" van artikel 5, lid 2, van het Gemoderniseerd Verdrag 108, dat rechtmatigheid van het verwerken van persoonsgegevens behandelt[383].

Algemeen belang en uitoefening van officiële autoriteit

Gezien de vele mogelijke manieren om het openbaar bestuur te organiseren, bepaalt artikel 6, lid 1, onder e), van de algemene verordening gegevensbescherming dat persoonsgegevens rechtmatig mogen worden verwerkt indien "de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de voor de verwerking verantwoordelijke is opgedragen [...]"[384].

Voorbeeld: In *Huber/Bundesrepublik Deutschland*[385] had de heer Huber, een in Duitsland wonende onderdaan van Oostenrijk, het Federale Bureau voor immigratie en vluchtelingen verzocht gegevens over hem te verwijderen uit het centrale register van buitenlandse onderdanen (Ausländerzentralregister

382 Algemene verordening gegevensbescherming, overweging 46.

383 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 46.

384 Zie algemene verordening gegevensbescherming, overweging 45.

385 HvJ-EU, zaak C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [Grote kamer], 16 december 2008.

— hierna "het AZR"). Dit register, dat persoonsgegevens bevat van niet-Duitse EU-burgers die langer dan drie maanden in Duitsland verblijven, wordt gebruikt voor statistische doeleinden en door rechtshandhavings- en gerechtelijke autoriteiten met het oog op het onderzoeken en vervolgen van criminele activiteiten of activiteiten die een bedreiging voor de openbare veiligheid vormen. De doorverwijzende rechtbank vroeg of de verwerking van persoonsgegevens in een register als het betreffende centrale register, waartoe ook andere overheidsautoriteiten toegang hebben, verenigbaar was met het EU-recht, aangezien er niet een dergelijk register bestond voor Duitse onderdanen.

Het HvJ-EU oordeelde dat, volgens artikel 7, onder e), van de Richtlijn 95/46/EG[386], persoonsgegevens rechtmatig mogen worden verwerkt indien dit nodig is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag.

Volgens het HvJ-EU "kan het begrip noodzakelijkheid zoals dit naar voren komt uit artikel 7, onder e), van Richtlijn 95/46/EG[387] (...) niet een inhoud hebben die verschilt van lidstaat tot lidstaat. Het gaat bijgevolg om een autonoom begrip van het gemeenschapsrecht, dat moet worden uitgelegd op een wijze die volledig beantwoordt aan het doel van de richtlijn zoals omschreven in artikel 1, lid 1"[388].

Het HvJ-EU merkte op dat het recht op vrij verkeer van een burger van de Unie op het grondgebied van een lidstaat waarvan hij of zij geen onderdaan is, niet onvoorwaardelijk is en kan worden gebonden aan beperkingen en voorwaarden die in het Verdrag tot oprichting van de Europese Gemeenschap en de maatregelen ter uitvoering daarvan zijn vastgesteld. Als het voor een lidstaat dus in principe rechtmatig is om een register als het AZR te gebruiken ter ondersteuning van de autoriteiten die verantwoordelijk zijn voor de toepassing van de wetgeving inzake het recht op verblijf, mag een dergelijk register geen andere informatie bevatten dan die welke noodzakelijk is om dat specifieke doel te verwezenlijken. Het HvJ-EU concludeerde dat het bedoelde systeem voor de verwerking van persoonsgegevens voldoet aan

386 Voormalige richtlijn gegevensbescherming, artikel 7, onder e), thans algemene verordening gegevensbescherming, artikel 6, lid 1, onder e).

387 *Ibid.*

388 HvJ-EU, zaak C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [Grote kamer], 16 december 2008, punt 52.

het Unierecht als het uitsluitend de gegevens bevat die noodzakelijk zijn voor de uitvoering van de desbetreffende wetgeving en als de centrale aard ervan de toepassing van de wetgeving doeltreffender maakt. De nationale rechtbank moest zich ervan vergewissen of deze voorwaarden in dit specifieke geval waren vervuld. Indien dit niet het geval was, kon de opslag en verwerking van persoonsgegevens in een register als het AZR op geen enkele grond worden geacht noodzakelijk te zijn in de zin van artikel 7, onder e)[389], van Richtlijn 95/46/EG[390].

Tot slot, met betrekking tot het gebruik van de gegevens die in het register waren opgenomen voor criminaliteitsbestrijdingsdoeleinden, oordeelde het HvJ-EU dat deze doelstelling "noodzakelijkerwijs gericht [is] op de vervolging van gepleegde misdrijven en delicten, ongeacht de nationaliteit van de daders". Het betreffende register bevat geen persoonsgegevens over onderdanen van de betrokken lidstaat, en dit verschil in behandeling vormt een geval van discriminatie als verboden bij artikel 18 van het VWEU. Bijgevolg oordeelde het HvJ-EU dat deze bepaling "in de weg staat aan de invoering door een lidstaat van een systeem van verwerking van persoonsgegevens speciaal voor burgers van de Unie die niet de nationaliteit van die lidstaat bezitten, met als doel de bestrijding van de criminaliteit"[391].

Het gebruik van persoonsgegevens door autoriteiten die in de publieke arena werkzaam zijn is tevens onderworpen aan artikel 8 van het **EVRM** en is bedoeld om in voorkomend geval onder artikel 5, lid 2, van het Gemoderniseerd Verdrag 108 te vallen[392].

Door de verwerkingsverantwoordelijke of een derde nagestreefde gerechtvaardigde belangen

In het kader van het **Unierecht** is de betrokkene niet de enige met gerechtvaardigde belangen. Artikel 6, lid 1, onder f), van de algemene verordening gegevensbescherming bepaalt dat persoonsgegevens rechtmatig mogen worden verwerkt indien "de

389 Voormalige richtlijn gegevensbescherming, artikel 7, onder e), thans algemene verordening gegevensbescherming, artikel 6, lid 1, onder e).

390 HvJ-EU, zaak C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [Grote kamer], 16 december 2008, punten 54, 58-59 en 66-68.

391 *Ibid.*, punten 78 en 81.

392 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punten 46 en 47.

verwerking noodzakelijk [is] voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde [met uitzondering van overheidsinstanties bij de uitvoering van hun taken] aan wie de gegevens worden verstrekt, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen [...]"[393].

Het bestaan van een rechtmatig belang moet zorgvuldig worden beoordeeld in elk individueel geval[394]. Indien de gerechtvaardigde belangen van de verwerkingsverantwoordelijke werden geïdentificeerd, moet de afweging worden gemaakt tussen deze belangen en de belangen of grondrechten en fundamentele vrijheden van de betrokkene[395]. De redelijke verwachtingen van de betrokkene moeten in acht worden genomen tijdens een dergelijke beoordeling om vast te stellen of de belangen van de verwerkingsverantwoordelijke zwaarder wegen dan de belangen of grondrechten van de betrokkene[396]. Indien de rechten van de betrokkene zwaarder wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke, kan de verwerkingsverantwoordelijke maatregelen nemen en waarborgen invoeren om ervoor te zorgen dat de impact op de rechten van de betrokkene geminimaliseerd worden (bijvoorbeeld door het pseudonimiseren van gegevens) en het evenwicht omdraaien vooraleer hij zich rechtmatig kan beroepen op deze legitieme grondslag voor de verwerking. In haar advies over het begrip "gerechtvaardigde belangen van de verwerkingsverantwoordelijke" benadrukt Groep artikel 29 de cruciale rol van verantwoordingsplicht en transparantie en van het recht van betrokkene om bezwaar aan te tekenen tegen de verwerking, wijziging, schrapping of doorgifte van zijn/haar gegevens of het verlenen van toegang tot zijn/haar gegevens, bij de afweging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke en de belangen van de grondrechten van de betrokkene[397].

In de overwegingen van de algemene verordening gegevensbescherming worden enkele voorbeelden gegeven met betrekking tot de vraag wat een rechtmatig belang van de betrokken verwerkingsverantwoordelijke inhoudt. De verwerking van persoonsgegevens is bijvoorbeeld toegelaten zonder de toestemming van de

393 In vergelijking met Richtlijn 95/46/EG geeft de algemene verordening gegevensbescherming meer voorbeelden van gevallen die worden geacht een rechtmatig belang te vormen.

394 Algemene verordening gegevensbescherming, preambule, overweging 47.

395 Groep artikel 29 (2014), *Advies 06/2014 over het begrip gerechtvaardigde belangen van de verwerkingsverantwoordelijke overeenkomstig artikel 7 van Richtlijn 95/46/EG*, 4 april 2014.

396 *Ibid.*

397 *Ibid.*

betrokkene als dit gebeurt voor directe marketingdoeleinden of wanneer een dergelijke verwerking "strikt noodzakelijk is voor fraudevoorkoming"[398].

In zijn jurisprudentie is het HvJ-EU uitgebreid op de test ingegaan om te bepalen wat een gerechtvaardigd belang is.

Voorbeeld: De zaak *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] had betrekking op de schade die was veroorzaakt aan een trolleybus van de Rīgas Transport Company door het plotseling openen van een taxideur door een passagier. Rīgas satiksme wilde de schade verhalen op de passagier. De politie wilde echter enkel de naam van de passagier geven en weigerde het identificatienummer en adres te geven door aan te voeren dat de openbaarmaking ervan onrechtmatig zou zijn in de nationale wetgeving inzake gegevensbescherming.

De Letse verwijzende rechterlijke instantie verzocht het HvJ-EU een prejudiciële beslissing uit te spreken over de vraag of de EU-wetgeving inzake gegevensbescherming verplicht tot de openbaarmaking van alle persoonsgegevens die nodig zijn om burgerrechtelijke procedures te starten tegen de persoon die verantwoordelijk zou zijn voor een administratieve overtreding[400].

Het HvJ-EU verduidelijkte dat de EU-wetgeving inzake gegevensbescherming voorziet in de mogelijkheid — niet de verplichting — om gegevens door te geven aan een derde partij voor de behartiging van de gerechtvaardigde belangen van die partij[401]. Het HvJ-EU heeft drie cumulatieve voorwaarden vastgesteld die moeten worden vervuld opdat de verwerking van persoonsgegevens rechtmatig is op basis van "gerechtvaardigde belangen"[402]. Ten eerste moet de derde aan wie de gegevens worden verstrekt een gerechtvaardigd belang nastreven. In dit specifieke geval betekent dit dat het opvragen van persoonlijke informatie om een persoon te vervolgen voor het toebrengen van schade aan eigendommen, een

398 Algemene verordening gegevensbescherming, preambule, overweging 47.

399 HvJ-EU, zaak C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA "Rīgas satiksme"*, 4 mei 2017.

400 *Ibid.*, punt 23.

401 *Ibid.*, punt 26.

402 *Ibid.*, punten 28-34.

rechtmatig belang vormt van een derde partij. Ten tweede, de verwerking van persoonsgegevens moet noodzakelijk zijn voor de behartiging van het gerechtvaardigde belang dat wordt nagestreefd. In dit geval is het verkrijgen van persoonlijke informatie, zoals het adres en/of identificatienummer absoluut noodzakelijk om de persoon te identificeren. Ten derde mogen de grondrechten en vrijheden van de betrokkene geen voorrang hebben op de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde partijen. Het afwegen van de belangen moet gebeuren van geval tot geval, rekening houdend met elementen zoals de ernst van de overtreding van de rechten van de betrokkene of zelfs de leeftijd van de betrokkene onder bepaalde omstandigheden. In dit specifieke geval, echter, vond het HvJ-EU de weigering van de bekendmaking niet gerechtvaardigd alleen maar op basis van het feit dat de betrokkene minderjarig was.

In het vonnis van *ASNEF en FECEMD* besloot het HvJ-EU expliciet over gegevensverwerking op basis van de grondslag "gerechtvaardigde belangen" die toentertijd was vastgelegd in artikel 7, onder f), van de richtlijn gegevensbescherming[403].

Voorbeeld: In *ASNEF en FECEMD*[404] verduidelijkte het HvJ-EU dat in het nationale recht geen aanvullende voorwaarden mogen worden gesteld aan de voorwaarden die worden genoemd in artikel 7, onder f), van de richtlijn inzake de rechtmatige verwerking van gegevens[405]. Dit had betrekking op een situatie waarin de Spaanse gegevensbeschermingswetgeving een bepaling bevatte die andere private partijen alleen de mogelijkheid bood om een rechtmatig belang bij de verwerking van persoonsgegevens aan te voeren als de informatie reeds in openbare bronnen was opgenomen.

Het HvJ-EU merkte in de eerste plaats op dat het doel van Richtlijn 95/46/EG[406] is om ervoor te zorgen dat het niveau van de bescherming van de rechten en vrijheden van natuurlijke personen in verband met de verwerking van

403 Voormalige richtlijn gegevensbescherming, artikel 7, onder f), thans algemene verordening gegevensbescherming, artikel 6, lid 1, onder f).

404 HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 november 2011.

405 Voormalige richtlijn gegevensbescherming, artikel 7, onder f), thans algemene verordening gegevensbescherming, artikel 6, lid 1, onder f).

406 Voormalige richtlijn gegevensbescherming, thans algemene verordening gegevensbescherming.

persoonsgegevens gelijk is in alle lidstaten. Ook mag het beter op elkaar afstemmen van de nationale wetgeving die op dit gebied van toepassing is niet leiden tot een vermindering van de geboden bescherming. De nationale wetgeving moet juist gericht zijn op een hoog beschermingsniveau in de Unie[407]. Bijgevolg oordeelde het HvJ-EU als volgt: "Derhalve vloeit uit het doel om in alle lidstaten een gelijkwaardige bescherming te bieden voort, dat artikel 7 van Richtlijn 95/46/EG[408] een uitputtende lijst bevat van gevallen waarin een verwerking van persoonsgegevens als rechtmatig kan worden aangemerkt". Bovendien mogen "de lidstaten aan artikel 7 van Richtlijn 95/46/EG[409] geen nieuwe beginselen betreffende de toelaatbaarheid van de verwerking van persoonsgegevens (...) toevoegen, noch bijkomende vereisten (...) vaststellen die de reikwijdte van een van de zes in dat artikel vervatte beginselen zouden wijzigen[410]. Het HvJ-EU gaf toe dat "[w]at de door artikel 7, onder f), van Richtlijn 95/46/EG vereiste afweging betreft, (...) er rekening mee [kan] worden gehouden dat de ernst van de aantasting door die verwerking van de grondrechten van de betrokkene kan verschillen naargelang van de vraag of de desbetreffende gegevens reeds in voor het publiek toegankelijke bronnen zijn opgenomen".

Daarentegen verzet artikel 7, onder f), van die richtlijn "zich er (...) tegen dat een lidstaat voor bepaalde categorieën persoonsgegevens categorisch en generiek de mogelijkheid van verwerking uitsluit, zonder ruimte te bieden voor een afweging van de betrokken tegengestelde rechten en belangen in een concreet geval."

In het licht van deze overwegingen concludeerde het HvJ-EU dat artikel 7, onder f), van Richtlijn 95/46/EG[411] in die zin moet worden uitgelegd "dat het zich verzet tegen een nationale wettelijke regeling die, bij ontbreken van toestemming van de betrokkene, de mogelijkheid tot verwerking van diens persoonsgegevens, die noodzakelijk is voor de behartiging van een

407 HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 november 2011, punt 28. Zie de richtlijn gegevensbescherming, overwegingen 8 en 10.

408 Voormalige richtlijn gegevensbescherming, artikel 7, thans algemene verordening gegevensbescherming, artikel 6, lid 1, onder f).

409 Voormalige richtlijn gegevensbescherming, artikel 7, thans algemene verordening gegevensbescherming, artikel 6.

410 *Ibid.*

411 Voormalige richtlijn gegevensbescherming, artikel 7, onder f), thans algemene verordening gegevensbescherming, artikel 6, lid 1, onder f).

gerechtvaardigd belang van de voor die verwerking verantwoordelijke of van de derde(n) aan wie de gegevens zullen worden meegedeeld, niet alleen afhankelijk stelt van de voorwaarde dat de fundamentele rechten en vrijheden van de betrokkene niet worden geschonden, maar ook van het vereiste dat de gegevens in voor het publiek toegankelijke bronnen zijn opgenomen, en aldus elke verwerking van gegevens die niet in dergelijke voor het publiek toegankelijke bronnen zijn opgenomen, categorisch en algemeen uitsluit"[412].

Wanneer persoonsgegevens worden verwerkt op basis van de grondslag "gerechtvaardigd belang", heeft de betrokkene het recht om te allen tijde bezwaar aan te tekenen van de verwerking, om redenen die verband houden met zijn/haar bijzondere situatie, overeenkomstig artikel 21, lid 1, van de algemene verordening gegevensbescherming. De verwerkingsverantwoordelijke moet de verwerking stoppen, tenzij hij aantoont zwaarwegende rechtmatige redenen te hebben om de verwerking voort te zetten.

Met betrekking tot **het recht van de Raad van Europa** kunnen vergelijkbare formuleringen worden gevonden in het Gemoderniseerd Verdrag 108[413] en de aanbevelingen van de Raad van Europa. De Aanbeveling inzake profilering erkent de verwerking van persoonsgegevens voor profileringsdoeleinden als rechtmatig indien deze verwerking noodzakelijk is in verband met de gerechtvaardigde belangen van anderen, "uitgezonderd indien de fundamentele rechten en vrijheden van de betrokkenen prevaleren"[414]. Daarnaast geldt "de bescherming van de rechten en vrijheden van anderen" genoemd in artikel 8, lid 2, van het EVRM als een reden voor rechtmatige beperking van het recht op gegevensbescherming.

Voorbeeld: In *Y./Turkije*[415] was de verzoeker hiv-positief. Aangezien hij bewusteloos was toen hij in het ziekenhuis aankwam, informeerde de bemanning van de ziekenwagen het ziekenhuispersoneel dat hij hiv-positief

412 HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 november 2011, punten 40, 44 en 48-49.

413 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 46.

414 Raad van Europa, Comité van Ministers (2010), Aanbeveling CM/Rec(2010)13 en toelichting over de bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens in het kader van profilering, 23 november 2010, artikel 3.4, onder b), (aanbeveling inzake profilering).

415 EHRM, *Y./Turkije*, nr. 648/10, 17 februari 2015.

was. De aanvrager voerde aan voor het EHRM dat de mededeling van deze informatie zijn recht op eerbiediging van zijn privéleven had geschonden. Gezien de noodzaak om de veiligheid van het ziekenhuispersoneel te beschermen, werd het delen van deze informatie echter niet beschouwd als een schending van zijn rechten.

4.1.2. De verwerking van bijzondere categorieën gegevens (gevoelige gegevens)

Het recht van de Raad van Europa laat het aan het nationale recht om passende beschermingen te bepalen om gevoelige gegevens te gebruiken, mits de voorwaarden van artikel 6 van het Gemoderniseerd Verdrag 108 zijn vervuld, namelijk dat er voldoende waarborgen zijn in het nationale recht die de andere provisies van het Verdrag complementeren. **Het Unierecht** bevat in artikel 9 van de algemene verordening gegevensbescherming een gedetailleerd regime voor de verwerking van bijzondere categorieën gegevens (ook "gevoelige gegevens" genoemd). Uit deze data blijkt de raciale of etnische afkomst, politieke overtuigingen, de religieuze of levensbeschouwelijke overtuigingen en het lidmaatschap van een vakbond, evenals de verwerking van genetische en biometrische gegevens voor de toepassing van het uniek identificeren van een natuurlijke persoon, en voor gegevens betreffende gezondheid, het seksuele gedrag of de seksuele geaardheid. De verwerking van gevoelige gegevens is in beginsel verboden[416].

Er is evenwel een uitputtende lijst van uitzonderingen op dit verbod, die is opgenomen in artikel 9, lid 2, van de verordening en die op rechtmatige gronden voor de verwerking van gevoelige gegevens betrekking hebben. Deze uitzonderingen omvatten situaties waarin:

- de betrokkene uitdrukkelijk instemt met de verwerking van gegevens;
- de behandeling wordt verricht door een organisatie zonder winstoogmerk met politieke, levensbeschouwelijke, godsdienstige of vakbondsdoeleinden en alleen betrekking heeft op haar (vroegere) leden of op personen die regelmatig contact met haar opnemen voor zulke doeleinden;

416 Voormalige richtlijn gegevensbescherming, artikel 7, onder f), thans algemene verordening gegevensbescherming, artikel 9, lid 1.

- de verwerking gegevens betreft die uitdrukkelijk openbaar werden gemaakt door de betrokkene;

- de verwerking noodzakelijk is:

    - om de verplichtingen en de specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene in de context van werk, de sociale zekerheid en sociale bescherming uit te voeren;

    - ter bescherming van de vitale belangen van de betrokkene of een andere natuurlijke persoon (indien de betrokkene geen toestemming kan geven);

    - om rechtsvorderingen vast te stellen, uit te voeren of te verdedigen of wanneer gerechtelijke instanties handelen in rechterlijke hoedanigheid;

    - voor preventieve of arbeidsgeneeskundige doeleinden: "voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheids- of sociale zorg of behandeling dan wel het beheer van gezondheids- of socialezorgstelsels en -diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker";

    - voor archiefdoeleinden in het algemeen belang, wetenschappelijke of historische onderzoeksdoeleinden of statistische doeleinden;

    - om redenen van algemeen belang op het gebied van de volksgezondheid, of

    - om redenen van zwaarwegend algemeen belang.

Om bijzondere categorieën gegevens te verwerken, wordt een contractuele relatie met de betrokkene dus niet beschouwd als een rechtsgrondslag voor de rechtmatige verwerking van gevoelige gegevens, met uitzondering van een contract met een gezondheidswerker die onderworpen is aan de beroepsgeheimhoudingsplicht[417].

417 Algemene verordening gegevensbescherming, artikel 9, lid 2, onder h) en i).

Uitdrukkelijke toestemming van de betrokkene

In het kader van **het Unierecht** is de eerst mogelijke rechtsgrondslag voor de rechtmatige verwerking van gegevens, ongeacht of het niet-gevoelige of gevoelige gegevens betreft, toestemming van de betrokkene. In geval van gevoelige gegevens moet deze toestemming uitdrukkelijk zijn. Unierecht of lidstatelijk recht kan er echter in voorzien dat het verbod op de verwerking van bijzondere categorieën gegevens niet door het individu kan worden opgeheven[418]. Dit kan bijvoorbeeld het geval zijn indien de verwerking van gegevens buitengewone risico's inhoudt voor de betrokkene.

Het arbeidsrecht of het recht van sociale zekerheid en sociale bescherming

In het kader van **het Unierecht** kan het verbod in artikel 9, lid 1, worden opgeheven indien de verwerking noodzakelijk is voor de uitvoering van verplichtingen of rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van werkgelegenheid en sociale zekerheid. De verwerking moet echter goedgekeurd worden door het Unierecht, het nationaal recht of een collectieve overeenkomst onder het nationaal recht die passende waarborgen bepalen die de grondrechten en belangen van de betrokkene beschermen[419]. Tewerkstellingsoverzichten die door een organisatie worden bijgehouden, mogen gevoelige persoonsgegevens bevatten onder bepaalde voorwaarden die in de algemene verordening gegevensbescherming en het toepasselijke nationale recht worden gespecificeerd. Voorbeelden van gevoelige gegevens zijn onder andere informatie over lidmaatschap bij een vakbond of over gezondheid.

Vitale belangen van de betrokkene of van een andere persoon

Net als in het geval van niet-gevoelige gegevens mogen in het kader van **het recht van de Unie** ook gevoelige gegevens worden verwerkt vanwege de vitale belangen van de betrokkene of van een andere natuurlijke persoon[420]. Wanneer de verwerking is gebaseerd op de vitale belangen van een andere persoon, mag deze rechtsgrondslag enkel worden aangevoerd als de verwerking "duidelijk niet op een andere

418 *Ibid.*, artikel 9, lid 2, onder a).

419 Algemene verordening gegevensbescherming, artikel 9, lid 2, onder b).

420 *Ibid.*, artikel 9, lid 2, onder c).

rechtsgrond kan worden gebaseerd"[421]. In sommige gevallen kan de verwerking van persoonsgegevens zowel individuele als openbare belangen beschermen, bijvoorbeeld wanneer de verwerking noodzakelijk is voor humanitaire doeleinden[422].

Om de verwerking van gevoelige gegevens op deze grond rechtmatig te laten zijn, moet het onmogelijk zijn om de betrokkene om toestemming te vragen omdat, bijvoorbeeld, de betrokkene niet bij bewustzijn is, afwezig is of niet kan worden bereikt. Met andere woorden, de betrokkene is lichamelijk of juridisch niet in staat om toestemming te geven.

Liefdadigheidsorganisaties of instellingen zonder winstoogmerk

De verwerking van persoonsgegevens is ook toegestaan in het kader van de rechtmatige activiteiten van verenigingen, stichtingen of andere organisaties zonder winstoogmerk met een politieke, levensbeschouwelijke, godsdienstige of vakbondsdoelstelling. De verwerking moet echter enkel betrekking hebben op de leden of voormalige leden van de instanties, of op leden die regelmatig contact opnemen met de instantie[423]. De gevoelige gegevens kunnen niet openbaar worden gemaakt buiten deze instanties zonder de toestemming van de betrokkene.

Gegevens die duidelijk door de betrokkene zelf openbaar zijn gemaakt

Artikel 9, lid 2, onder e), van de algemene verordening gegevensbescherming bepaalt dat verwerking niet verboden is als ze betrekking heeft op gegevens die duidelijk door de betrokkene zelf openbaar zijn gemaakt. Hoewel de betekenis van "duidelijk door de betrokkene zelf openbaar zijn gemaakt" niet is gedefinieerd in de Verordening, aangezien het gaat om een uitzondering op het verbod om gevoelige gegevens te verwerken, moet het in enge zin worden uitgelegd dat de betrokkene met opzet zijn/haar persoonsgegevens publiek maakt. Bijgevolg, wanneer de televisie een video van een videobewakingscamera uitzendt die, onder andere, een brandweerman toont die gewond raakt tijdens de evacuatie van een gebouw, kan er niet worden geconcludeerd dat de brandweerman duidelijk de gegevens openbaar wilde maken. Daartegenover staat dat, indien de brandweerman besluit het incident te beschrijven en de video en foto's op een openbare internetpagina te

421 *Ibid.*, overweging 46.

422 *Ibid.*

423 *Ibid.*, artikel 9, lid 2, onder d).

publiceren, hij of zij een doelbewuste en bevestigende handeling zou maken om de persoonsgegevens openbaar te maken. Het is belangrijk erop te wijzen dat het openbaar maken van de gegevens van iemand geen toestemming vormt, maar het is een andere goedkeuring voor de verwerking van bijzondere categorieën gegevens.

Het feit dat de betrokkene de verwerkte persoonsgegevens openbaar heeft gemaakt, ontslaat verwerkingsverantwoordelijken niet van hun verplichtingen krachtens de wetgeving inzake gegevensbescherming. Het beginsel van doelbinding, bijvoorbeeld, blijft van toepassing op persoonsgegevens, ook als deze gegevens openbaar zijn gemaakt[424].

Rechtsvorderingen

De verwerking van bijzondere categorieën gegevens die "noodzakelijk [is] voor de instelling, uitoefening of onderbouwing van een rechtsvordering" in een gerechtelijke procedure dan wel in een administratieve of buitengerechtelijke procedure[425], wordt ook toegelaten in het kader van de algemene verordening gegevensbescherming[426]. In dit geval moet de verwerking relevant zijn voor een specifieke rechtsvordering en de uitoefening of de verdediging ervan, en kan worden aangevraagd door een van de partijen bij het geschil.

Bij de uitoefening van zijn rechterlijke bevoegdheid mag de rechter bijzondere categorieën gegevens verwerken in het kader van het oplossen van een juridisch conflict[427]. Tot deze speciale categorieën behoren bijvoorbeeld genetische gegevens bij de vaststelling van afstamming, of gegevens over de gezondheidstoestand wanneer een deel van het bewijs informatie over de verwonding van een misdaadslachtoffer betreft.

Redenen van zwaarwegend algemeen belang

Overeenkomstig artikel 9, lid 2, onder g) van de algemene verordening gegevensbescherming mogen lidstaten verder omstandigheden invoeren waarin gevoelige gegevens verwerkt mogen worden, zolang:

424 Groep artikel 29 (2013), *Advies 3/13 over doelbinding*, WP 203, Brussel, 2 april 2013, blz. 14.

425 Algemene verordening gegevensbescherming, preambule, overweging 52.

426 *Ibid.*, artikel 9, lid 2, onder f).

427 *Ibid.*

- de verwerking van gegevens gebeurt om redenen van zwaarwegend algemeen belang;

- dit is voorzien door het Unierecht of lidstatelijk recht;

- het Unierecht of lidstatelijk recht evenredig is, het recht op gegevensbescherming beschermt en passende en specifieke maatregelen voorziet om de rechten en belangen van de betrokkene te waarborgen[428].

Een duidelijk voorbeeld hiervan zijn de systemen voor elektronische medische dossiers. Dit systeem staat toe dat gezondheidsgegevens, die zijn verzameld tijdens de behandeling van een patiënt, op grote schaal, meestal op landelijk niveau, beschikbaar worden gesteld aan andere behandelaars van deze patiënt.

Groep artikel 29 besloot dat de totstandbrenging van dergelijke systemen niet kan plaatsvinden in het kader van de bestaande wettelijke regels voor het verwerken van gegevens over patiënten[429]. Het bestaan van elektronische systemen voor gezondheidsdossiers is echter mogelijk als ze gebaseerd zijn op "redenen van zwaarwegend algemeen belang"[430]. De totstandbrenging van dergelijke systemen zou een uitdrukkelijke rechtsgrondslag vereisen met de nodige waarborgen om ervoor te zorgen dat het systeem op een veilige manier wordt beheerd[431].

Andere redenen voor de verwerking van gevoelige gegevens

De algemene verordening gegevensbescherming bepaalt dat gevoelige gegevens kunnen worden verwerkt wanneer de verwerking noodzakelijk is voor/om[432]:

- preventieve of arbeidsgeneeskundige doeleinden, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheids- of sociale zorg of behandeling dan wel het beheer van gezondheids- of socialezorgstelsels en -diensten, op grond van

428 *Ibid.*, artikel 9, lid 2, onder g).

429 Groep artikel 29 (2007), *Werkdocument inzake de verwerking van persoonsgegevens betreffende gezondheid in elektronische medische dossiers (EPD)*, WP 131, Brussel, 15 februari 2007. Zie ook algemene verordening gegevensbescherming, artikel 9, lid 3.

430 Algemene verordening gegevensbescherming, artikel 9, lid 2, onder g).

431 Groep artikel 29 (2007), *Werkdocument inzake de verwerking van persoonsgegevens betreffende gezondheid in elektronische medische dossiers (EPD)*, WP 131, Brussel, 15 februari 2007.

432 Algemene verordening gegevensbescherming, artikel 9, lid 2, onder h), i) en j).

Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker;

- redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren van de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht. Het recht moet zorgen voor passende en specifieke maatregelen ter bescherming van de rechten van de betrokkene;

- archivering, wetenschappelijk of historisch onderzoek of statistische doeleinden op grond van het Unierecht of het lidstatelijk recht. De wet moet evenredig zijn met het beoogde doel, de essentie van het recht op gegevensbescherming respecteren en zorgen voor passende en specifieke maatregelen ter bescherming van de rechten en belangen van de betrokkene.

Aanvullende voorwaarden op grond van nationaal recht

De algemene verordening gegevensbescherming staat lidstaten ook toe om aanvullende voorwaarden in te voeren of te handhaven, met inbegrip van beperkingen op de verwerking van genetische, biometrische en gezondheidsgerelateerde gegevens[433].

433 *Ibid.*, artikel 9, lid 2, onder h), en 9, lid 4.

4.2. Regels voor de beveiliging van de verwerking

Belangrijkste punten

- De regels voor de beveiliging van de verwerking verplichten de verwerkingsverantwoordelijke en de verwerker om passende technische en organisatorische maatregelen te nemen om onbevoegde inmenging in verwerkingen te voorkomen.
- Het benodigde niveau van de gegevensbeveiliging wordt bepaald door:
  - de beveiligingskenmerken die beschikbaar zijn in de markt voor specifieke typen verwerkingen;
  - de kosten;
  - de risico's die de verwerking van de gegevens met zich meebrengt voor de grondrechten en fundamentele vrijheden van de betrokkenen.
- Het waarborgen van de vertrouwelijkheid van persoonsgegevens maakt deel uit van een algemeen beginsel dat is opgenomen in de algemene verordening gegevensbescherming.

In het kader van zowel het **Unierecht als het recht van de Raad van Europa** hebben de verwerkingsverantwoordelijken de algemene verplichting om transparant en verantwoordingsplichtig te zijn bij de verwerking van persoonsgegevens en, met name, bij inbreuken in verband met persoonsgegevens (datalekken) wanneer die inbreuken worden begaan. In geval van datalekken moeten de verwerkingsverantwoordelijken de toezichthoudende autoriteiten in kennis stellen, tenzij het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt. Betrokkenen moeten ook worden ingelicht over het datalek wanneer deze vermoedelijk zal leiden tot een groot risico voor de rechten en vrijheden van natuurlijke personen.

4.2.1. Elementen van gegevensbeveiliging

De relevante bepaling van **het Unierecht** luidt als volgt:

> *"Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten*

en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen [...]"[434].

Deze maatregelen omvatten onder meer:

- pseudonimisering en versleuteling van persoonsgegevens[435];
- zorgen dat het verwerkingssysteem en de verwerkingsdienst vertrouwelijk, integer, beschikbaar en veerkrachtig blijven[436];
- de beschikbaarheid van en de toegang tot persoonsgegevens tijdig herstellen in het geval van gegevensverlies[437];
- een proces voor het testen, beoordelen en evalueren van de doeltreffendheid van de maatregelen om te zorgen voor de beveiliging van de verwerking[438].

Het **recht van de Raad van Europa** bevat een vergelijkbare bepaling:

"Elke partij bepaalt dat de verwerkingsverantwoordelijke en, indien van toepassing, de verwerker passende beveiligingsmaatregelen neemt tegen risico's zoals onopzettelijk of niet-geautoriseerde toegang tot, vernietiging, verlies, gebruik, wijziging of bekendmaking van persoonsgegevens"[439].

In het kader van **het Unierecht en het recht van de Raad van Europa** is de verwerkingsverantwoordelijke verplicht om in geval van een inbreuk in verband met persoonsgegevens die gevolgen kan hebben voor de rechten en vrijheden van individuen, de toezichthoudende autoriteit op de hoogte te stellen (zie punt 4.2.3).

Vaak zijn er ook sectorale, nationale en internationale normen ontwikkeld om een veilige verwerking van gegevens mogelijk te maken. Het Europees privacyzegel (EuroPriSe) bijvoorbeeld is een eTEN (trans-Europese

434 *Ibid.*, artikel 32, lid 1.

435 *Ibid.*, artikel 32, lid 1, onder a).

436 *Ibid.*, artikel 32, lid 1, onder b).

437 *Ibid.*, artikel 32, lid 1, onder c).

438 *Ibid.*, artikel 32, lid 1, onder d).

439 Gemoderniseerd Verdrag 108, artikel 7, lid 1.

telecommunicatienetwerken)-project van de EU, waarin de mogelijkheden zijn onderzocht om producten, met name software, te certificeren in overeenstemming met de Europese gegevensbeschermingswetgeving. Het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa) is opgezet om het vermogen van de EU, de EU-lidstaten en het bedrijfsleven om problemen met netwerk- en informatiebeveiliging op te lossen te vergroten[440]. Enisa publiceert regelmatig analyses van actuele beveiligingsbedreigingen en adviseert over de aanpak ervan[441].

Gegevensbeveiliging wordt niet alleen bereikt door de juiste uitrusting — hardware en software — te hebben. Daarvoor zijn ook passende interne organisatorische voorschriften nodig. Deze interne voorschriften zouden idealiter de volgende punten moeten bestrijken:

- de regelmatige verstrekking van informatie aan alle werknemers over gegevensbeveiligingsregels en hun verplichtingen uit hoofde van de gegevensbeschermingswetgeving, met name hun verplichting om gegevens vertrouwelijk te behandelen;

- een duidelijke verdeling van verantwoordelijkheden en een duidelijke omschrijving van bevoegdheden op het gebied van gegevensverwerking, met name met betrekking tot besluiten om persoonsgegevens te verwerken en gegevens over te dragen aan derden of aan betrokkenen;

- het uitsluitend gebruiken van persoonsgegevens overeenkomstig de instructies van de bevoegde persoon of algemeen vastgestelde voorschriften;

- bescherming van de toegang tot locaties en tot hard- en software van de verwerkingsverantwoordelijke en de verwerker, met inbegrip van controles op toegangsmachtigingen;

- de waarborg dat machtigingen voor de toegang tot persoonsgegevens worden toegewezen door bevoegd personeel en passende documentatie vereisen;

440 Verordening (EU) nr. 526/2013 van het Europees Parlement en de Raad van 21 mei 2013 inzake het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) en tot intrekking van Verordening (EG) nr. 460/2004, PB L 165 van 2013.

441 Bijvoorbeeld, Enisa, (2016), cyberbeveiliging en bestendigheid van slimme auto's. Goede praktijken en aanbevelingen; Enisa (2016), Veiligheid van mobiele betalingen en digitale portemonnees.

- geautomatiseerde protocollen betreffende de elektronische toegang tot persoonsgegevens en regelmatige controles van deze protocollen door de interne toezichthoudende afdeling (alle gegevensverwerkende activiteiten dienen dus geregistreerd te worden);

- een zorgvuldige documentatie van andere vormen van overdracht dan via geautomatiseerde toegang tot gegevens om te kunnen aantonen dat er geen illegale gegevensoverdrachten plaatsvinden.

Ook het aanbieden van adequate opleidingen en onderwijs op het gebied van gegevensbeveiliging aan personeelsleden is een belangrijk element van een doeltreffende gegevensbeveiliging. Daarnaast moeten er verificatieprocedures zijn ingesteld om ervoor te zorgen dat passende maatregelen niet alleen op papier bestaan, maar in de praktijk worden toegepast en naar behoren werken (zoals interne en externe audits).

Maatregelen die het beveiligingsniveau van een voor de verwerking verantwoordelijke of verwerker kunnen verbeteren zijn bijvoorbeeld de aanstelling van een gegevensbeschermingsfunctionaris, de opleiding van werknemers op het gebied van gegevensbeveiliging, regelmatige audits, penetratietesten en kwaliteitszegels.

Voorbeeld: In *I./Finland*[442] was de verzoekster niet in staat gebleken te bewijzen dat andere werknemers van het ziekenhuis waar ze werkte illegaal inzage in haar medische dossier hadden gehad. Deze vermeende schending van haar recht op gegevensbescherming was om die reden door de nationale rechtbanken verworpen. Het EHRM concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM omdat het registratiesysteem voor de inzage in medische dossiers dat het ziekenhuis toepaste "zodanig was dat het niet mogelijk was om met terugwerkende kracht duidelijkheid te verkrijgen over het gebruik van patiëntendossiers, aangezien daarin slechts de vijf meest recente raadplegingen werden vermeld en deze informatie werd verwijderd nadat het dossier weer in de archieven was opgeslagen". Voor het Hof was het doorslaggevend dat het registratiesysteem van het ziekenhuis duidelijk niet in overeenstemming was met de wettelijke eisen van het nationale recht, een feit waar de nationale rechtbanken te weinig gewicht aan hadden toegekend.

442 EHRM, *I./Finland*, nr. 20511/03, 17 juli 2008.

De EU heeft de richtlijn van beveiliging van netwerk- en informatiesystemen (de NIS-richtlijn) ingevoerd[443], hetgeen het eerste juridische instrument in de EU is over cyberbeveiliging. De richtlijn beoogt de verbetering van de cyberbeveiliging op nationaal niveau enerzijds, en een verhoogde samenwerking binnen de EU anderzijds. Voorts legt het verplichtingen op aan exploitanten van essentiële diensten (met inbegrip van de marktdeelnemers in de sectoren energie, gezondheid, de bank-, vervoers- en digitale infrastructuursector enz.) en aanbieders van digitale diensten om risico's te beheren, voor de beveiliging van hun netwerk- en informatiesystemen te zorgen en veiligheidsincidenten te rapporteren.

Vooruitzichten

In September 2017 stelde de Europese Commissie een ontwerpverordening voor die is gericht op de hervorming van het mandaat van Enisa, om rekening te houden met de nieuwe bevoegdheden en verantwoordelijken van het agentschap krachtens de NIS-richtlijn. Het doel van de voorgestelde verordening is de ontwikkeling van de taken van Enisa en de versterking van zijn rol als "referentiepunt in het cyberbeveiligingsecosysteem in de EU"[444]. De voorgestelde verordening mag geen afbreuk doen aan de beginselen van de algemene verordening gegevensbescherming en, door de nodige elementen te verduidelijken waaruit de Europese cyberbeveiligingscertificering bestaat, moet ook de beveiliging van persoonsgegevens versterken. Tegelijkertijd heeft de Europese Commissie in september 2017 een ontwerpuitvoeringsverordening voorgesteld die de elementen voorziet waarmee aanbieders van digitale diensten rekening moeten houden om ervoor te zorgen dat hun netwerk en informatiesystemen zijn beveiligd, zoals artikel 16, lid 8, van de NIS-richtlijn vraagt. Ten tijde van het opstellen van het handboek, waren besprekingen over deze twee voorstellen gaande.

4.2.2. Vertrouwelijkheid

In het kader van het Unierecht erkent de algemene verordening gegevensbescherming vertrouwelijkheid van persoonsgegevens als onderdeel van een algemeen

443 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 met betrekking tot maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, PB L 194 van 2016.

444 Voorstel voor een verordening van het Europees Parlement en de Raad over Enisa, het "EU-cyberbeveiligingsagentschap", en tot intrekking van Verordening (EU) nr. 526/2013, en over informatie- en communicatietechnologie cyberbeveiligingscertificering (wet cyberbeveiliging), COM(2017) 477, 13 september 2017, blz. 6.

beginsel[445]. Aanbieders van publiek toegankelijke communicatiediensten moeten de vertrouwelijkheid waarborgen. Zij hebben ook de verplichting om de beveiliging van hun diensten te garanderen[446].

Voorbeeld: Een medewerkster van een verzekeringsmaatschappij ontvangt op haar werkplek een telefoontje van iemand die zegt een klant te zijn en informatie over zijn verzekeringspolis opvraagt.

De plicht om de gegevens van klanten vertrouwelijk te behandelen vereist dat de medewerkster ten minste minimumbeveiligingsmaatregelen toepast alvorens persoonsgegevens mee te delen. Dit zou bijvoorbeeld kunnen door aan te bieden om de klant terug te bellen op het telefoonnummer dat wordt vermeld in het dossier van de klant.

Op grond van artikel 5, lid 1, onder f), moeten persoonsgegevens op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ("integriteit en vertrouwelijkheid").

Op grond van artikel 32 moeten de verwerkingsverantwoordelijke en de verwerker technische en organisatorische maatregelen uitvoeren om te zorgen voor een hoog niveau van beveiliging. Deze maatregelen omvatten onder meer de pseudonimisering en versleuteling van persoonsgegevens, het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht te garanderen van de verwerking, de evaluatie en toetsing van de doeltreffendheid van de maatregelen en het vermogen om de verwerking te herstellen in het geval van een fysiek of technisch incident. Daarnaast kan de naleving van een goedgekeurde gedragscode of een goedgekeurde certificeringsregeling worden gebruikt als een element om aan te tonen dat het beginsel van integriteit en vertrouwelijkheid wordt nageleefd. Bovendien moet, overeenkomstig artikel 28 van de algemene verordening gegevensbescherming, het contract dat de verwerkingsverantwoordelijke bindt aan de verwerker voorzien dat verwerker ervoor moet zorgen dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben

445 Algemene verordening gegevensbescherming, artikel 5, lid 1, onder f).

446 Richtlijn betreffende privacy en elektronische communicatie, artikel 5, lid 1.

verbonden om vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid verbonden zijn.

De verplichting om persoonsgegevens vertrouwelijk te behandelen strekt zich niet uit tot situaties waarin gegevens ter kennis van iemand komen in zijn/haar hoedanigheid als particuliere persoon en niet als werknemer van een verwerkingsverantwoordelijke of verwerker. In dat geval zijn artikelen 32 en 28 van de algemene verordening gegevensbescherming niet van toepassing, omdat het gebruik van persoonsgegevens door particuliere personen volledig is uitgezonderd van het toepassingsgebied van de verordening indien dit gebruik binnen de grenzen van de zogeheten huishoudelijke exceptie valt[447]. De huishoudelijke exceptie is het gebruik van persoonsgegevens "door een natuurlijke persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden"[448]. Sinds de beslissing van het HvJ-EU in het arrest *Bodil Lindqvist*[449] moet deze uitzondering echter eng worden uitgelegd, met name ten aanzien van de openbaarmaking van gegevens. Met name zal de huishoudelijke exceptie zich niet uitstrekken tot de openbaarmaking van persoonsgegevens aan een onbeperkt aantal ontvangers op internet of tot gegevensverwerking die professionele of commerciële aspecten toont (voor nadere details van deze zaak, zie de punten 2.1.2, 2.2.2, 2.3.1).

"Het vertrouwelijke karakter van communicatie" is een ander aspect van de vertrouwelijkheid, die valt onder *lex specialis*. De bijzondere regels voor het waarborgen van de vertrouwelijkheid van elektronische communicatie in het kader van de e-Privacy-richtlijn zorgen ervoor dat de lidstaten iedere persoon die geen gebruiker is, of die geen toestemming heeft van de gebruikers, verbieden om communicaties en gerelateerde metagegevens te beluisteren, af te tappen, op te slaan of een ander soort onderschepping of bewaking toe te passen[450]. De nationale wetgeving kan enkel uitzonderingen op dit beginsel toestaan om redenen van nationale veiligheid, defensie of voor het voorkomen of opsporen van strafbare feiten, en enkel indien deze maatregelen nodig en evenredig zijn met de nagestreefde doelstellingen[451]. Dezelfde regels zijn ook van toepassing in het kader van de toekomstige e-Privacy-verordening, maar het toepassingsgebied van de wettelijke regeling over e-Privacy zal worden uitgebreid van openbaar beschikbare elektronische

447 Algemene verordening gegevensbescherming, artikel 2, lid 2, onder c).

448 *Ibid.*

449 HvJ-EU, zaak C-101/01, *Strafzaak tegen Bodil Lindqvist*, 6 november 2003.

450 Richtlijn betreffende privacy en elektronische communicatie, artikel 5, lid 1.

451 *Ibid.*, artikel 15, lid 1.

communicatiediensten tot communicatie via over-the-top-diensten (zoals mobiele toepassingen).

In het kader van het recht van de Raad van Europa is de verplichting om gegevens vertrouwelijk te behandelen inherent aan het begrip "beveiliging van gegevens" in artikel 7, lid 1, van het Gemoderniseerd Verdrag 108, dat betrekking heeft op gegevensbeveiliging.

Voor de verwerkende bedrijven betekent vertrouwelijkheid dat ze de gegevens niet kunnen doorgeven aan derden of andere afnemers zonder autorisatie. Voor de werknemers van een voor de verwerking verantwoordelijke of een verwerker betekent vertrouwelijkheid dat ze persoonsgegevens alleen mogen gebruiken in overeenstemming met de instructies van hun bevoegde leidinggevenden.

De verplichting om gegevens vertrouwelijk te behandelen moet worden opgenomen in elke overeenkomst tussen voor de verwerking verantwoordelijken en verwerkers. Voorts zullen verwerkingsverantwoordelijken en verwerkers specifieke maatregelen moeten nemen voor hun werknemers om een wettelijke plicht om gegevens vertrouwelijk te behandelen in te stellen, hetgeen normaliter wordt bereikt door de opneming van vertrouwelijkheidsclausules in het arbeidscontract.

Inbreuk op de beroepsplicht om gegevens vertrouwelijk te behandelen is in veel EU-lidstaten en andere partijen bij het Gemoderniseerd Verdrag 108 strafbaar gesteld.

4.2.3. Kennisgeving bij een inbreuk in verband met persoonsgegevens

"Inbreuk in verband met persoonsgegevens" (of: datalek) verwijst naar een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot verwerkte persoonsgegevens[452]. Hoewel nieuwe technologieën zoals encryptie nu meer mogelijkheden verschaffen om een veilige verwerking te garanderen, zijn datalekken nog steeds een gangbaar fenomeen. De oorzaken van

452 Algemene verordening gegevensbescherming, artikel 4, lid 12; zie ook Groep artikel 29 (2017), *Richtsnoeren voor kennisgeving van inbreuk in verband met persoonsgegevens in het kader van Verordening (EU) 2016/679*, WP 250, 3 oktober 2017, blz. 8.

datalekken variëren van toevallige fouten van mensen die werkzaam zijn binnen een organisatie tot externe dreigingen, zoals hackers en cybercriminele organisaties.

Datalekken kunnen erg nadelig zijn voor de persoonlijke levenssfeer en de rechten van personen op het gebied van gegevensbescherming die, als gevolg van de inbreuk, de controle verliezen over hun persoonsgegevens. Datalekken kunnen leiden tot identiteitsdiefstal of -fraude, financieel verlies of materiële schade, het verlies van vertrouwelijkheid van persoonsgegevens die onder het beroepsgeheim vallen en schade aan de reputatie van de betrokkene. In de richtsnoeren voor kennisgeving van inbreuk in verband met persoonsgegevens in het kader van Verordening (EU) 2016/679, legt Groep artikel 29 uit dat datalekken drie soorten gevolgen kunnen hebben voor persoonsgegevens: openbaarmaking, verlies en/of wijziging[453]. Naast de verplichting om maatregelen te treffen om de beveiliging van de verwerking te garanderen, zoals uiteengezet in punt 4.2, is het van even groot belang dat verwerkingsverantwoordelijken de inbreuken op passende wijze en tijdig oplossen.

De toezichthoudende autoriteiten en personen zijn dikwijls niet op de hoogte van een datalek waardoor het niet mogelijk is voor natuurlijke personen om stappen te ondernemen om zich te beschermen tegen de negatieve gevolgen ervan. Om de rechten van natuurlijke personen te verzekeren en de impact van datalekken te beperken, leggen de **EU en de Raad van Europa** een aanmeldingsverplichting op aan verwerkingsverantwoordelijken in bepaalde omstandigheden.

In het kader van het Gemoderniseerd Verdrag 108 van de **Raad van Europa** moeten verdragsluitende partijen ten minste eisen dat verwerkingsverantwoordelijken de bevoegde toezichthoudende autoriteit op de hoogte stellen van datalekken die een ernstige aantasting vormen op de rechten van de betrokkenen. Deze kennisgeving moet "onverwijld" worden uitgevoerd[454].

Het Unierecht voorziet in een gedetailleerd regime voor het reguleren van de timing en de inhoud van de kennisgevingen[455]. Bijgevolg moeten verwerkingsverantwoordelijken de toezichthoudende autoriteiten in kennis stellen van bepaalde datalekken zonder onnodige vertraging en, waar mogelijk, binnen 72 uur vanaf het moment

453 Groep artikel 29 (2017), *Richtsnoeren voor kennisgeving van inbreuk in verband met persoonsgegevens in het kader van Verordening (EU) 2016/679*, WP 250, 3 oktober 2017, blz. 6.

454 Gemoderniseerd Verdrag 108, artikel 7, lid 2; Memorie van toelichting bij Gemoderniseerd Verdrag 108, punten 64-66.

455 Algemene verordening gegevensbescherming, artikelen 33 en 34.

dat zij kennis krijgen van het datalek. Indien zij de termijn van 72 uur overschrijden, moet de kennisgeving vergezeld gaan van een verklaring voor de vertraging. De verwerkingsverantwoordelijken zijn enkel vrijgesteld van de aanmeldingsverplichting wanneer zij in staat zijn om aan te tonen dat het onwaarschijnlijk is dat het datalek een risico vormt voor de rechten en vrijheden van de betrokken personen.

De verordening bepaalt de minimale informatie die moet worden opgenomen in de kennisgeving zodat de toezichthoudende autoriteit de nodige maatregelen kan nemen[456]. De kennisgeving dient minstens een beschrijving te bevatten van de aard van het datalek en van de categorieën en het geschatte aantal getroffen betrokkenen, evenals een beschrijving van de mogelijke gevolgen van het datalek en van de door de verwerkingsverantwoordelijke uitgevoerde maatregelen om de gevolgen aan te pakken en te verminderen. Bovendien moeten de naam en contactgegevens van de functionaris voor gegevensbescherming of van een ander contactpunt worden verstrekt, zodat de bevoegde toezichthoudende instantie zo nodig verdere informatie kan verkrijgen.

Indien een datalek een hoog risico inhoudt voor de rechten en vrijheden van personen, dienen verwerkingsverantwoordelijken deze personen (de betrokkenen) onverwijld in te lichten van het datalek[457]. De informatie aan de betrokkenen, met inbegrip van de beschrijving van het datalek, moet in duidelijke en eenvoudige taal worden gesteld en informatie bevatten die aansluit op de informatie in kennisgevingen aan toezichthoudende autoriteiten. In bepaalde omstandigheden kunnen verwerkingsverantwoordelijken worden vrijgesteld van de verplichting tot kennisgeving aan de betrokkenen van deze datalekken. Vrijstellingen zijn toepasbaar wanneer de verwerkingsverantwoordelijke passende technische en organisatorische beschermingsmaatregelen heeft genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop het datalek betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling. Het optreden van de verwerkingsverantwoordelijke na het datalek om te garanderen dat de rechten van betrokkenen niet meer kunnen worden geschaad, kunnen de verwerkingsverantwoordelijke vrijstellen van de verplichting om de betrokkenen in kennis te stellen. Tot slot, indien de kennisgeving een onevenredige grote inspanning vereist van de verwerkingsverantwoordelijke, kunnen betrokkenen

456 *Ibid.*, artikel 33, lid 3.

457 *Ibid.*, artikel 34.

geïnformeerd worden over het datalek via andere middelen, zoals een openbare mededeling of soortgelijke maatregelen[458].

De verplichting tot aanmelding van datalekken aan de toezichthoudende autoriteiten en de betrokkenen is gericht aan de verwerkingsverantwoordelijken. Datalekken kunnen echter ontstaan, ongeacht of de behandeling wordt verricht door een verwerkingsverantwoordelijke of een verwerker. Om deze reden is het van essentieel belang om ervoor te zorgen dat verwerkers ook verplicht zijn om datalekken te rapporteren. In dit geval moeten verwerkers datalekken aan de verwerkingsverantwoordelijke melden zonder onnodige vertraging[459]. Vervolgens is de verwerkingsverantwoordelijke verantwoordelijk voor de melding bij de toezichthoudende autoriteiten en de getroffen betrokkenen, met inachtneming van de bovengenoemde regels en het bovengenoemde tijdschema.

4.3. Regels betreffende de verantwoordingsplicht en bevordering van de naleving

Belangrijkste punten

- Om verantwoording te waarborgen bij de verwerking van persoonsgegevens moeten verwerkingsverantwoordelijken en verwerkers een register bijhouden van alle verwerkingsactiviteiten die onder hun verantwoordelijkheid worden uitgevoerd en deze op verzoek aan de toezichthoudende autoriteit verstrekken.
- De algemene verordening gegevensbescherming beschrijft verschillende instrumenten ter bevordering van de naleving:
  - de benoemingen van functionarissen voor gegevensbescherming in bepaalde situaties;
  - de uitvoering van een effectbeoordeling vóór het begin van de verwerkingsactiviteiten die waarschijnlijk grote risico's inhouden voor de rechten en vrijheden van natuurlijke personen;

458 *Ibid.*, artikel 34, lid 3, onder c).

459 *Ibid.*, artikel 33, lid 2.

  - voorafgaande raadpleging van de betrokken toezichthoudende autoriteit indien uit de effectbeoordeling blijkt dat de verwerking risico's inhoudt die niet kunnen worden beperkt;
  - een gedragscode voor de verwerkingsverantwoordelijken en de verwerkers waarbij de toepassing van de verordening in de verschillende verwerkende sectoren wordt gespecificeerd;
  - certificeringsmechanismen, beschermingszegels en -merken.
- Het recht van de Raad van Europa stelt vergelijkbare instrumenten voor om de naleving van het Gemoderniseerd Verdrag 108 te bevorderen.

Het verantwoordingsbeginsel is van bijzonder belang voor de naleving van de gegevensbeschermingsregels in Europa. De verwerkingsverantwoordelijke is verantwoordelijk voor de inachtneming van de gegevensbeschermingsregels en moet kunnen aantonen dat hij ze naleeft. De verantwoordingsplicht dient niet pas een rol te spelen nadat een schending heeft plaatsgevonden. Integendeel, verwerkingsverantwoordelijken hebben de proactieve verplichting om in alle stadia van de gegevensverwerking passende beleidsmaatregelen met betrekking tot gegevensbeheer te volgen. Het Europees recht inzake gegevensbescherming vereist dat de verwerkingsverantwoordelijken technische en organisatorische maatregelen uitvoeren om ervoor te zorgen, en om te kunnen aantonen, dat de verwerking wordt verricht in overeenstemming met de wetgeving. Zo wordt onder meer voorgesteld om functionarissen voor gegevensbescherming te benoemen, registers en documentatie in verband met de verwerking bij te houden en een gegevensbeschermingseffectbeoordeling uit te voeren.

4.3.1. Gegevensbeschermingsfunctionarissen

Functionarissen voor gegevensbescherming (DPO's) zijn personen die advies geven over de naleving van de gegevensbeschermingsregels in organisaties die gegevens verwerken. Zij vormen "een hoeksteen van verantwoording", aangezien zij de naleving vergemakkelijken, terwijl ze ook optreden als tussenpersoon tussen de toezichthoudende autoriteiten, de betrokkenen en de organisatie door wie zij werden aangesteld.

In het kader van het recht **van de Raad van Europa** plaatst artikel 10, lid 1, van het Gemoderniseerd Verdrag 108 de algemene verantwoordelijkheid van de verantwoordingsplicht bij de verwerkingsverantwoordelijken en verwerkers. Hierdoor dienen verwerkingsverantwoordelijken en verwerkers alle passende maatregelen

te nemen om de gegevensbeschermingsregels die in het verdrag zijn vastgesteld, na te leven en in staat te zijn om aan te tonen dat de gegevensverwerking die onder hun controle gebeurt, voldoet aan de bepalingen van het verdrag. Hoewel de overeenkomst geen concrete maatregelen voorschrijft die de verwerkingsverantwoordelijken en verwerkers moeten nemen, geeft de Memorie van toelichting van het Gemoderniseerd Verdrag 108 aan dat de benoeming van een DPO de enige mogelijke maatregel is om aan te tonen dat aan deze bepalingen wordt voldaan. De DPO's moeten alle mogelijke middelen krijgen om hun mandaat uit te voeren[460].

In tegenstelling tot het recht van de Raad van Europa kunnen verwerkingsverantwoordelijken en verwerkers **in de EU** niet altijd een DPO aanstellen naar eigen goeddunken, want onder bepaalde omstandigheden is dit verplicht. De algemene verordening gegevensbescherming erkent dat de DPO een belangrijke rol speelt in het nieuwe beheerssysteem en omvat gedetailleerde bepalingen met betrekking tot de aanstelling, positie, plichten en taken van de functionaris[461].

De algemene verordening gegevensbescherming bepaalt dat de aanstelling van een DPO verplicht is in drie bijzondere gevallen: wanneer de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, wanneer een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die regelmatige en stelselmatige observatie op grote schaal van de betrokkenen vereisen, of wanneer hij/zij hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens of persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten[462]. Hoewel termen zoals "stelselmatige observatie op grote schaal" en "hoofdzakelijk belast met" niet in de verordening worden gedefinieerd, heeft Groep artikel 29 richtsnoeren uitgevaardigd over hoe ze moeten worden geïnterpreteerd[463].

Voorbeeld: Ondernemingen actief in sociale media en zoekmachines worden waarschijnlijk beschouwd als verwerkingsverantwoordelijken wiens verwerkingsverrichtingen de regelmatige en stelselmatige observatie van betrokkenen vereisen op grote schaal. Het bedrijfsmodel van deze ondernemingen is gebaseerd op de verwerking van grote hoeveelheden

460 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 87.

461 Algemene verordening gegevensbescherming, artikel 37-39.

462 *Ibid.*, artikel 37, lid 1.

463 Groep artikel 29 (2017), *Richtsnoeren over functionarissen voor gegevensbescherming (DPO's)*, WP 243 rev.01, laatst herzien en goedgekeurd op 5 april 2017.

persoonsgegevens en zij genereren aanzienlijke inkomsten via het aanbieden van gerichte reclame en door bedrijven toe te staan om op de websites reclame te maken. Gerichte reclame is een middel om advertenties te plaatsen op basis van demografische gegevens en eerdere aankopen of gedrag van de consument. Daarom vereist dit de stelselmatige observatie van de online gewoontes en het online gedrag van de betrokkenen.

Voorbeeld: Een ziekenhuis en een verzekeringsonderneming zijn typische voorbeelden van verwerkingsverantwoordelijken wiens activiteiten bestaan uit de grootschalige verwerking van bijzondere categorieën persoonsgegevens. Gegevens waaruit informatie over de gezondheid van een persoon blijkt, vormen bijzondere categorieën persoonsgegevens, zowel in het recht van de Raad van Europa als het Unierecht, en vereisen dus een betere bescherming. Het Unierecht erkent verder genetische en biometrische gegevens als bijzondere categorieën. Voor zover medische inrichtingen en verzekeringsmaatschappijen die gegevens op grote schaal verwerken, moeten zij onder de algemene verordening gegevensbescherming een functionaris voor gegevensbescherming benoemen.

Bovendien voorziet artikel 37, lid 4, van de algemene verordening gegevensbescherming dat in andere dan de in artikel 37, lid 1, bedoelde drie verplichte gevallen, indien dat Unierechtelijk of lidstaatrechtelijk is verplicht, dat de verwerkingsverantwoordelijke, de verwerker of verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen, een functionaris voor gegevensbescherming aanwijzen.

Alle andere organisaties zijn niet wettelijk verplicht een DPO aan te wijzen. De algemene verordening gegevensbescherming bepaalt echter dat verwerkingsverantwoordelijken en verwerkers ervoor kunnen kiezen om op vrijwillige basis een DPO aan te wijzen, terwijl de lidstaten ook de mogelijk wordt geboden om deze aanwijzing verplicht te maken voor meer categorieën organisaties dan die onder de verordening werden voorzien[464].

Wanneer een verwerkingsverantwoordelijke een DPO heeft aangewezen, moet deze ervoor zorgen dat hij of zij "naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens"

464 Algemene verordening gegevensbescherming, artikel 37, leden 3 en 4.

in de organisatie[465]. Zo moeten DPO's betrokken worden bij het verstrekken van advies over de uitvoering van gegevensbeschermingseffectbeoordelingen en bij het opstellen en bijhouden van registers van verwerkingsactiviteiten in een organisatie. Om functionarissen voor gegevensbescherming in staat te stellen hun taken efficiënt uit te voeren, moeten verwerkingsverantwoordelijken en verwerkers hen voorzien van de nodige middelen, met inbegrip van financiële middelen, infrastructuur en uitrusting. Aanvullende vereisten omvatten het verstrekken aan DPO's van voldoende tijd om hun taken te vervullen en een voortgezette opleiding om hen in staat te stellen hun deskundigheid te ontwikkelen en op de hoogte te blijven van alle ontwikkelingen in de wetgeving inzake gegevensbescherming[466].

De algemene verordening gegevensbescherming stelt een aantal fundamentele waarborgen vast om ervoor te zorgen dat de DPO onafhankelijk handelt. Verwerkingsverantwoordelijken en verwerkers moeten ervoor zorgen dat bij de uitoefening van hun taken met betrekking tot gegevensbescherming, de functionarissen voor gegevensbescherming geen enkele instructie krijgen van de onderneming, met inbegrip van personen op het hoogste leidinggevende niveau. Bovendien mogen zij op geen enkele manier worden uitgesloten of benadeeld voor de uitvoering van hun taken[467]. Neem bijvoorbeeld een geval waar de DPO de verwerkingsverantwoordelijke of verwerker aanraadt een gegevensbeschermingseffectbeoordeling uit te voeren, omdat hij of zij van mening is dat de verwerking waarschijnlijk zal leiden tot grote risico's voor de betrokkenen. De onderneming gaat niet akkoord met het advies van de DPO, vindt het niet gegrond en beslist bijgevolg om geen effectbeoordeling uit te voeren. De onderneming kan het advies negeren, maar kan de DPO niet ontslaan of straffen voor het verstrekken van het advies.

Ten slotte zijn de taken en verplichtingen van functionarissen omschreven in artikel 39 van de algemene verordening gegevensbescherming. Deze omvatten de vereisten om de bedrijven en werknemers die de verwerking uitvoeren, in te lichten en te adviseren over hun verplichtingen uit hoofde van de wetgeving en om toe te zien op de naleving van de Europese en nationale gegevensbeschermingsregels via de uitvoering van controles en het opleiden van werknemers die bij de verwerkingsverrichtingen betrokken zijn. Functionarissen voor gegevensbescherming moeten ook samenwerken met de toezichthoudende autoriteit en optreden als contactpunt

465 *Ibid.*, artikel 38, lid 1.

466 Groep artikel 29 (2017), *Richtsnoeren over functionarissen voor gegevensbescherming (DPO's)*, WP 243 rev.01, laatst herzien en goedgekeurd op 5 april 2017, punt 3.1.

467 Algemene verordening gegevensbescherming, artikel 38, leden 2 en 3.

voor de laatstgenoemde over aangelegenheden betreffende de verwerking van gegevens, zoals bijvoorbeeld een inbreuk.

Met betrekking tot de persoonsgegevens die door de EU-instellingen en -organen worden behandeld, bepaalt Verordening (EG) nr. 45/2001 dat elke instelling en elk orgaan van de Unie een functionaris voor gegevensbescherming dient aan te stellen. De functionaris voor gegevensbescherming is belast met het verzekeren van de correcte toepassing van de bepalingen van de verordening binnen de EU-instellingen en EU-organen en met het informeren van zowel de betrokkenen als de verwerkingsverantwoordelijken over hun rechten en plichten[468]. Hij of zij is ook verantwoordelijk voor het reageren op verzoeken van de EDPS en, waar nodig, de samenwerking met hem of haar. Net als bij de algemene verordening gegevensbescherming bevat Verordening (EG) nr. 45/2001 bepalingen over de onafhankelijkheid van functionarissen voor gegevensbescherming bij de uitvoering van hun taken en de noodzaak om hun de nodige personeelsleden en middelen te bieden[469]. Functionarissen voor gegevensbescherming dienen op de hoogte te worden gesteld voordat een EU-institutie of EU-orgaan (of diensten van deze organisaties) verwerkingsverrichtingen uitvoeren, en ze moeten een register bijhouden van alle aangemelde verwerkingsverrichtingen[470].

4.3.2. Register van de verwerkingsactiviteiten

Om de naleving van de regels aan te tonen en rekenschap af te kunnen leggen, zijn ondernemingen vaak wettelijk verplicht om hun activiteiten te documenteren en te registreren. Een belangrijk voorbeeld is de fiscale wetgeving en controle van jaarrekeningen, die vereisen dat alle ondernemingen uitgebreide documentatie en registers bijhouden. Het is ook belangrijk om soortgelijke vereisten in andere rechtsgebieden, met name de wetgeving inzake gegevensbescherming, vast te stellen aangezien het bijhouden van registers een belangrijk middel is om de naleving van de gegevensbeschermingsregels te vergemakkelijken. **Het Unierecht** bepaalt derhalve dat verwerkingsverantwoordelijken, of hun vertegenwoordigers, een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid werden uitgevoerd, dienen bij te houden[471]. Deze verplichting heeft als doel ervoor te zorgen dat,

468 Zie artikel 24, lid 1, van Verordening (EG) nr. 45/2001 voor de volledige lijst van taken van functionarissen voor gegevensbescherming.

469 Verordening (EG) nr. 45/2001, artikel 24, leden 6 en 7.

470 *Ibid.*, artikelen 25 en 26.

471 Algemene verordening gegevensbescherming, artikel 30.

indien nodig, de toezichthoudende autoriteiten beschikken over de nodige documentatie om de rechtmatigheid van de verwerking te kunnen bevestigen.

De informatie die moet worden gedocumenteerd, omvat het volgende:

- de naam en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, de gezamenlijke verwerkingsverantwoordelijke, de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
- doeleinden van de verwerking;
- beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens met betrekking tot de verwerking;
- informatie over de categorieën ontvangers aan wie de persoonsgegevens zijn of zullen worden bekendgemaakt;
- informatie over de vraag of er overdracht van persoonsgegevens naar derde landen of internationale organisaties werd of zal worden uitgevoerd;
- waar mogelijk, de vastgelegde termijnen voor de verwijdering van de verschillende categorieën persoonsgegevens, alsook een overzicht van de technische maatregelen die werden genomen om de beveiliging van de verwerking te verzekeren[472].

De verplichting om een register bij te houden van de verwerkingsactiviteiten die in het kader van de algemene verordening gegevensbescherming plaatsvinden, betreft niet alleen verwerkingsverantwoordelijken, maar ook verwerkers. Dit is een belangrijke ontwikkeling, aangezien de overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker, voorafgaand aan de vaststelling van de verordening, voornamelijk betrekking had op de verplichtingen van de verwerker. De verplichting om een register bij te houden is nu rechtstreeks voorzien in de wet.

De algemene verordening gegevensbescherming voorziet in een uitzondering op deze verplichting. De vereiste om registers bij te houden is niet van toepassing op een onderneming of organisatie (verwerkingsverantwoordelijke of verwerker) die

472 *Ibid.*, artikel 30, lid 1.

minder dan 250 personen tewerkstelt. De uitzondering is echter onderworpen aan de vereisten dat de betrokken organisatie geen verwerkingsactiviteiten onderneemt die waarschijnlijk zouden leiden tot een risico voor de rechten en vrijheden van de betrokkenen, dat de verwerking slechts een incidenteel karakter heeft en dat ze geen bijzondere categorieën gegevens als bedoeld in artikel 9, lid 1, of persoonlijke gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10, bevat.

Het bijhouden van registers van verwerkingsactiviteiten stelt verwerkingsverantwoordelijken en verwerkers in staat om de naleving van de verordening aan te tonen. Het stelt ook toezichthoudende autoriteiten in staat om toe te zien op de rechtmatigheid van de verwerking. Indien een toezichthoudende autoriteit toegang tot deze gegevens verzoekt, zijn de verwerkingsverantwoordelijken en de verwerkers verplicht om mee te werken en deze ter beschikking te stellen.

4.3.3. Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging

Verwerkingen houden een aantal inherente risico's in voor de rechten van personen. Persoonsgegevens kunnen worden verloren, bekendgemaakt aan onbevoegden of verwerkt op onwettige wijze. Het spreekt voor zich dat de risico's variëren naargelang de aard en omvang van de verwerking. Grootschalige operaties met betrekking tot de verwerking van gevoelige gegevens, hebben bijvoorbeeld een veel hogere mate van risico voor de betrokkenen ten opzichte van de potentiële risico's die bestaan wanneer een kleine onderneming de adressen en persoonlijke telefoonnummers van haar werknemers verwerkt.

Naarmate nieuwe technologieën ontstaan en de verwerking steeds ingewikkelder wordt, moeten verwerkingsverantwoordelijken dergelijke risico's aanpakken door de mogelijke gevolgen van de voorgenomen verwerking te onderzoeken alvorens de verwerking te beginnen. Dit stelt organisaties in staat om de risico's op voorhand naar behoren te identificeren, aan te pakken en te beperken, waardoor de waarschijnlijkheid van een negatief effect op personen als gevolg van de verwerking, wordt beperkt.

Zowel het recht van de Raad van Europa als het Unierecht voorziet in gegevensbeschermingseffectbeoordelingen. In het wettelijke kader van de Raad van Europa verplicht artikel 10, lid 2, van het Gemoderniseerd Verdrag 108 de verdragsluitende

partijen om ervoor te zorgen dat de verwerkingsverantwoordelijken en de verwerkers "de waarschijnlijke gevolgen voor de rechten en fundamentele vrijheden van de betrokkenen onderzoeken vóór de aanvang van dergelijke verwerking" en om, na de beoordeling, de verwerking op een zodanige wijze te ontwerpen dat de risico's die aan de verwerking verbonden zijn, worden voorkomen of tot een minimum beperkt.

Het Unierecht legt een vergelijkbare, meer gedetailleerde, verplichting op aan de verwerkingsverantwoordelijken die binnen het toepassingsgebied van de algemene verordening gegevensbescherming vallen. Artikel 35 bepaalt dat een effectbeoordeling moet worden uitgevoerd indien de verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De verordening bepaalt niet hoe de waarschijnlijkheid van risico's moet worden beoordeeld, maar geeft veeleer aan wat de risico's zouden kunnen zijn[473]. Hij bevat een lijst van verwerkingen die worden geacht een hoog risico te vormen en waarvoor een voorafgaande effectbeoordeling bijzonder noodzakelijk is, namelijk in gevallen waarin:

- persoonsgegevens worden verwerkt voor het nemen van besluiten over natuurlijke personen na een stelselmatige en uitgebreide evaluatie van persoonlijke aspecten van de personen (profilering);

- gevoelige gegevens of persoonlijke gegevens over strafrechtelijke veroordelingen en strafbare feiten op grote schaal worden verwerkt;

- de verwerking de grootschalige en stelselmatige observatie van publiek toegankelijke gebieden inhoudt.

De toezichthoudende autoriteiten moeten een lijst opstellen en publiceren van de soorten bewerkingsverrichtingen die een effectbeoordeling moeten ondergaan. Ze mogen ook een lijst opstellen van verwerkingsverrichtingen die van deze verplichting worden vrijgesteld[474].

Wanneer een effectbeoordeling is vereist, moeten de verwerkingsverantwoordelijken de noodzaak en evenredigheid van de verwerking en de mogelijke risico's voor de rechten van personen beoordelen. De effectbeoordeling moet bovendien de voorziene beveiligingsmaatregelen bevatten om de in kaart gebrachte risico's tegen

473 Algemene verordening gegevensbescherming, preambule, overweging 75.

474 *Ibid.*, artikel 35, leden 4 en 5.

te gaan. Om de lijsten vast te stellen moeten de toezichthoudende autoriteiten van de lidstaten samenwerken met elkaar en met het Europees Comité voor gegevensbescherming. Dit zal zorgen voor een consistente aanpak in heel de Europese Unie van de verrichtingen die een effectbeoordeling vereisen, en verwerkingsverantwoordelijken zullen aan dezelfde vereisten moeten voldoen, ongeacht hun locatie.

Indien na een effectbeoordeling blijkt dat de verwerking zal leiden tot hoge risico's voor de rechten van personen en dat er geen maatregelen werden genomen om het risico te beperken, moet de verwerkingsverantwoordelijke de betrokken toezichthoudende autoriteit raadplegen voor aanvang van de verwerking[475].

Groep artikel 29 heeft richtsnoeren uitgebracht voor gegevensbeschermingseffectboordelingen en over hoe te bepalen of de verwerking waarschijnlijk een hoog risico inhoudt[476]. Er zijn negen criteria ontwikkeld die helpen bepalen of in een bepaald geval een gegevensbeschermingseffectbeoordeling nodig is[477]: 1) evaluatie of puntenbeoordeling; 2) geautomatiseerde besluitvorming met rechtskracht of een soortgelijk belangrijk effect; 3) stelselmatige observatie; 4) gevoelige gegevens; 5) op grote schaal verwerkte gegevens; 6) gegevensbestanden die zijn gematcht of onderling vermengd; 7) gegevens met betrekking tot kwetsbare betrokkenen; 8) een meer innovatief gebruik of de toepassing van technische of organisatorische oplossingen; 9) indien de verwerking op zich "voorkomt dat de betrokkenen een recht uitoefenen of een dienst of een contract gebruiken". Groep artikel 29 voerde de vuistregel in dat verwerkingen die voldoen aan minder dan twee criteria, een lager risico inhouden en geen effectbeoordeling inzake gegevensbescherming vereisen, terwijl zij die aan twee of meer criteria voldoen, wel een dergelijke beoordeling vereisen. In gevallen waarin het niet duidelijk is of een effectbeoordeling inzake gegevensbescherming is vereist, beveelt Groep artikel 29 aan om een dergelijke beoordeling uit te voeren, omdat het gaat om "een nuttig instrument dat verwerkingsverantwoordelijken helpt om de gegevensbeschermingswetgeving in acht te nemen"[478]. Wanneer een nieuwe technologie voor gegevensverwerking wordt

475 *Ibid.*, artikel 36, lid 1; Groep artikel 29 (2017), *Richtsnoeren betreffende gegevensbeschermingseffectbeoordeling (DPIA) en om te bepalen of de verwerking "waarschijnlijk een hoog risico inhoudt" voor de toepassing van Verordening (EU) 2016/679*, WP 248 rev.01, Brussel, 4 oktober 2017.

476 Groep artikel 29 (2017), *Richtsnoeren betreffende gegevensbeschermingseffectbeoordeling (DPIA) en om te bepalen of de verwerking "waarschijnlijk een hoog risico inhoudt" voor de toepassing van Verordening (EU) 2016/679*, WP 248 rev.01, Brussel, 4 oktober 2017.

477 *Ibid.*, blz. 9-11.

478 *Ibid.*, blz. 9.

ingevoerd, is het belangrijk een effectbeoordeling inzake gegevensbescherming uit te voeren[479].

4.3.4. Gedragscodes

Gedragscodes zijn bedoeld voor gebruik in diverse industriesectoren om de toepassing van de algemene verordening gegevensbescherming te schetsen en te verduidelijken in hun specifieke sectoren. Voor de verwerkingsverantwoordelijken en de verwerkers van persoonsgegevens zal het opstellen van deze codes de naleving van de Europese gegevensbeschermingswetgeving aanzienlijk verbeteren, alsook de uitvoering ervan versterken. De deskundigheid van de leden van de sector zal bevorderlijk zijn voor het vinden van oplossingen die praktisch zijn en daarom eerder zullen worden gevolgd. De algemene verordening gegevensbescherming erkent het belang van dergelijke codes in de doeltreffende toepassing van de gegevensbeschermingwetgeving en verzoekt de lidstaten, de toezichthoudende autoriteiten, de Europese Commissie en het Europees Comité voor gegevensbescherming om de opstelling van gedragscodes aan te moedigen die zo kunnen bijdragen aan de juiste toepassing van de verordening in de EU[480]. De codes kunnen de toepassing van de verordening in specifieke sectoren vermelden, met inbegrip van kwesties zoals het verzamelen van persoonsgegevens, de te verstrekken informatie aan betrokkenen en aan het publiek, en de uitoefening van de rechten van betrokkenen.

Om ervoor te zorgen dat de gedragscodes voldoen aan de voorschriften die zijn vastgesteld in het kader van de algemene verordening gegevensbescherming, moeten de codes worden ingediend bij de bevoegde toezichthoudende autoriteit alvorens te worden vastgesteld. De toezichthoudende autoriteit brengt vervolgens een advies uit over de vraag of het ingediende ontwerp van de code de naleving van de verordening bevordert en, indien zij vaststelt dat de code passende garanties biedt, keurt ze de code goed[481]. De toezichthoudende autoriteiten moeten de gedragscodes die zijn goedgekeurd, alsook de criteria waarop de goedkeuring was gebaseerd, bekendmaken. Wanneer een ontwerp van gedragscode betrekking heeft op de verwerkingsactiviteiten in verschillende lidstaten, moet de bevoegde toezichthoudende autoriteit, vóór de goedkeuring, wijziging of uitbreiding van de gedragscode, de code aan het Europees Comité voor gegevensbescherming voorleggen dat een advies zal uitbrengen over de conformiteit van de code met de

479 *Ibid.*

480 Algemene verordening gegevensbescherming, artikel 40, lid 1.

481 *Ibid.*, artikel 40, lid 5.

algemene verordening gegevensbescherming. De Commissie kan bij uitvoeringshandelingen vaststellen dat de goedgekeurde gedragscode die haar zijn voorgelegd, binnen de Unie algemeen geldig zijn.

De inachtneming van een gedragscode biedt grote voordelen voor zowel de betrokkenen als voor de verwerkingsverantwoordelijken en de verwerkers. Deze codes bieden gedetailleerde richtsnoeren die de wettelijke vereisten aanpassen aan de specifieke sectoren en de transparantie van verwerkingsverrichtingen bevordert. Verwerkingsverantwoordelijken en verwerkers kunnen ook de naleving van de codes gebruiken als aantoonbaar bewijs dat zij het Unierecht in acht nemen en als middel ter bevordering van hun publieke imago van een organisatie die prioriteit geeft aan en zich verbindt tot de bescherming van gegevens in hun activiteiten. Goedgekeurde gedragscodes, samen met de bindende en afdwingbare verplichtingen, kunnen worden gebruikt als passende waarborgen voor de overdracht van gegevens naar derde landen. Om ervoor te zorgen dat organisaties die de gedragscodes in acht nemen, deze werkelijk naleven, kan een speciaal orgaan (erkend door de bevoegde toezichthoudende autoriteit) worden aangesteld om de naleving ervan op te volgen en te verzekeren. Om haar taken doeltreffend te kunnen uitvoeren, moet het orgaan onafhankelijk zijn, bewezen deskundigheid aantonen inzake de aangelegenheden waarop de gedragscode van toepassing is en over transparante procedures en structuren beschikken die het in staat stellen om klachten over schendingen van de code te behandelen[482].

Krachtens **het recht van de Raad van Europa** voorziet het Gemoderniseerd Verdrag 108 dat het door het nationaal recht gewaarborgde niveau van gegevensbescherming nuttig versterkt kan worden door vrijwillige regelgevende maatregelen, zoals codes inzake goede praktijken of beroepscodes. Zij vormen echter enkel vrijwillige maatregelen onder het Gemoderniseerd Verdrag 108: men kan geen wettelijke verplichtingen doen gelden om dergelijke maatregelen te nemen, hoewel het raadzaam is, en dergelijke maatregelen zijn op zich niet voldoende om het verdrag volledig na te leven[483].

4.3.5. Certificering

In aanvulling op gedragscodes vormen certificeringsmechanismen, gegevensbeschermingsverzegelingen en -merken een andere wijze waarmee

482 *Ibid.*, artikel 41, leden 1 en 2.

483 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 33.

verwerkingsverantwoordelijken en verwerkers kunnen aantonen dat ze de algemene verordening gegevensbescherming nakomen. Hiertoe voorziet de Verordening in vrijwillige certificeringsregelingen waarbij bepaalde organen of toezichthoudende autoriteiten mogen overgaan tot de afgifte van certificaten. Verwerkingsverantwoordelijken en verwerkers die ervoor kiezen om zich aan te sluiten bij een certificeringsmechanisme, kunnen aan zichtbaarheid en geloofwaardigheid winnen aangezien certificaten, zegels en merken de betrokkenen toelaten om snel een beoordeling te maken van het beveiligingsniveau van de gegevensverwerking van een organisatie. Het moet worden benadrukt dat het feit dat een verwerkingsverantwoordelijke of een verwerker een dergelijk certificaat bezit, niet betekent dat zijn taken en verantwoordelijkheden om alle voorschriften van de verordening na te leven, verminderen.

4.4. Gegevensbescherming door ontwerp en standaardinstellingen

Gegevensbescherming door ontwerp

Het Unierecht vereist dat verwerkingsverantwoordelijken maatregelen treffen om de beginselen inzake gegevensbescherming daadwerkelijk uit te voeren en om de nodige waarborgen te integreren om aan de vereisten van de verordening te voldoen en de rechten van de betrokkenen te beschermen[484]. Deze maatregelen moeten zowel op het tijdstip van de verwerking als bij het bepalen van de middelen voor de verwerking worden uitgevoerd. Bij de uitvoering van deze maatregelen moet de verwerkingsverantwoordelijke rekening houden met de huidige stand van de techniek, de kosten van de uitvoering, de aard, het bereik en de doeleinden van de verwerking van persoonsgegevens, evenals de risico's en de ernst voor de rechten en vrijheden van de betrokkene[485].

Het recht van de Raad van Europa vereist dat verwerkingsverantwoordelijken en verwerkers de waarschijnlijke gevolgen van de verwerking van persoonsgegevens op de rechten en vrijheden van de betrokkenen evalueren alvorens met de verwerking te starten. Daarnaast zijn verwerkingsverantwoordelijken en verwerkers

484 Algemene verordening gegevensbescherming, artikel 25, lid 1.

485 Zie Groep artikel 29 (2017), *Richtsnoeren betreffende gegevensbeschermingseffectbeoordeling (DPIA) en om te bepalen of de verwerking "waarschijnlijk een hoog risico inhoudt" voor de toepassing van Verordening (EU) 2016/679*, WP 248 rev.01, 4 oktober 2017. Zie ook Enisa (2015), Privacy en gegevensbescherming door ontwerp — van beleid tot productie, 12 januari 2015.

verplicht om de gegevensverwerking op zodanige wijze te ontwerpen dat het risico op inmenging met die rechten en vrijheden wordt voorkomen of tot een minimum beperkt wordt, en technische en organisatorische maatregelen te treffen die het effect op de bescherming van persoonsgegevens in ieder stadium meenemen[486].

Gegevensbescherming door standaardinstellingen

Het Unierecht vereist dat de verwerkingsverantwoordelijke passende maatregelen neemt om ervoor te zorgen dat enkel persoonsgegevens die noodzakelijk zijn voor de doeleinden, door standaardinstellingen worden verwerkt. Deze verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan[487]. Een dergelijke maatregel moeten garanderen dat, bijvoorbeeld, niet alle werknemers van de verwerkingsverantwoordelijke toegang hebben tot de persoonsgegevens van de betrokkenen. Nadere richtsnoeren zijn ontwikkeld door de EDPS in de *"Necessity Toolkit"*[488].

Het recht van de Raad van Europa vereist dat verwerkingsverantwoordelijken en verwerkers technische en organisatorische maatregelen uitvoeren om rekening te houden met de gevolgen van het recht op gegevensbescherming, en technische en organisatorische maatregelen treffen die het effect op de bescherming van persoonsgegevens in ieder stadium meenemen[489].

In 2016 publiceerde Enisa een verslag over beschikbare privacyhulpmiddelen en -diensten[490]. Die beoordeling bevat, naast andere overwegingen, een lijst van criteria en parameters die indicatoren vormen voor goede of slechte privacypraktijken. Terwijl sommige criteria rechtstreeks verband houden met bepalingen van de algemene verordening gegevensbescherming — zoals het gebruik van pseudonimisering en van goedgekeurde certificeringsmechanismen — bieden andere meer innovatieve initiatieven aan om privacy te garanderen door ontwerp en

486 Gemoderniseerd Verdrag 108, artikel 10, leden 2 en 3; Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 89.

487 Algemene verordening gegevensbescherming, artikel 25, lid 2.

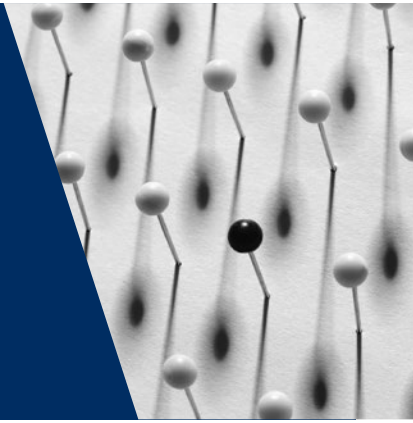
488 Europese Toezichthouder voor gegevensbescherming (EDPS), (2017), *Necessity Toolkit*, Brussel, 11 april 2017.

489 Gemoderniseerd Verdrag 108, artikel 10, lid 3, Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 89.

490 Enisa, PETs controls matrix: A systematic approach for assessing online and mobile privacy tools, 20 december 2016.

standaardinstellingen. Zo kan het criterium van de bruikbaarheid, dat weliswaar niet rechtstreeks verband houdt met privacy, privacy-versterkend zijn, aangezien het de bredere invoering van een privacyhulpmiddel of -dienst mogelijk kan maken. Het is inderdaad mogelijk dat het algemene publiek moeilijk de overstap maakt naar privacyhulpmiddelen die in de praktijk moeilijk uit te voeren zijn, zelfs indien ze erg sterke privacywaarborgen bieden. Bovendien is het criterium van de looptijd en de stabiliteit van het privacyhulpmiddel van essentieel belang. Hiermee bedoelt men de manier waarop een hulpmiddel evolueert in de loop der tijd en reageert op bestaande of nieuwe uitdagingen in verband met privacy. Andere privacybevorderende technologieën, bijvoorbeeld in het kader van de beveiligde communicatie, omvatten eind-tot-eindversleuteling (communicatie waarbij enkel de communicerende mensen de berichten kunnen lezen); klant-server-versleuteling (het communicatiekanaal versleutelen dat tussen een klant en een server werd vastgesteld); authenticatie (controle van de identiteiten van de communicerende partijen), en anonieme communicatie (geen enkele derde partij kan de communicerende partijen identificeren).

5 Onafhankelijk toezicht



EU	Behandelde onderwerpen	RvE
Handvest, artikel 8, lid 3 Verdrag betreffende de werking van de Europese Unie, artikel 16, lid 2 Algemene verordening gegevensbescherming, artikelen 51-59 HvJ-EU, zaak C-518/07, *Europese Commissie/Bondsrepubliek Duitsland* [Grote kamer], 2010 HvJ-EU, zaak C-614/10, *Europese Commissie/Republiek Oostenrijk* [Grote kamer], 2012 HvJ-EU, zaak C-288/12, *Europese Commissie/Hongarije* [Grote kamer], 2014 HvJ-EU, zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer], 2015	**Toezichthoudende autoriteiten**	Gemoderniseerd Verdrag 108, artikel 15
Algemene verordening gegevensbescherming, artikelen 60-67	**De samenwerking tussen toezichthoudende autoriteiten**	Gemoderniseerd Verdrag 108, artikelen 16-21.
Algemene verordening gegevensbescherming, artikelen 68-76	**Europees Comité voor gegevens-bescherming**	

Belangrijkste punten

- Onafhankelijk toezicht is een essentieel onderdeel van de Europese gegevensbeschermingswetgeving en is vastgelegd in artikel 8, lid 3, van het Handvest.
- Om een doeltreffende gegevensbescherming te waarborgen, moeten krachtens het nationaal recht toezichthoudende autoriteiten worden aangesteld.
- Toezichthoudende autoriteiten moeten volledig onafhankelijk kunnen optreden, hetgeen moet worden gegarandeerd door de wet waarbij ze zijn ingesteld en tot uiting moet komen in de organisatiestructuur van de toezichthoudende autoriteit.
- Toezichthoudende autoriteiten beschikken over specifieke bevoegdheden en taken. Deze omvatten onder meer:
  - het houden van toezicht op en het bevorderen van gegevensbescherming op nationaal niveau;
  - het verstrekken van adviezen aan betrokkenen, verwerkingsverantwoordelijken, de overheid en het algemene publiek;
  - het behandelen van klachten en het bijstaan van betrokkenen bij vermeende inbreuken op gegevensbeschermingsrechten;
  - het houden van toezicht op verwerkingsverantwoordelijken en verwerkers.
- Toezichthoudende autoriteiten hebben ook de bevoegdheid om indien nodig in te grijpen door:
  - verwerkingsverantwoordelijken en verwerkers waarschuwingen te geven, te berispen of zelfs boetes op te leggen;
  - opdracht te geven om gegevens te rectificeren, af te schermen of uit te wissen;
  - een verbod op de verwerking of een administratieve boete op te leggen;
  - zaken naar de rechter door te verwijzen.
- Aangezien bij de verwerking van persoonsgegevens de verwerkingsverantwoordelijken, verwerkers en betrokkenen zich vaak in verschillende staten bevinden, moeten toezichthoudende autoriteiten met elkaar samenwerken in grensoverschrijdende zaken om te zorgen voor een doeltreffende bescherming van natuurlijke personen in Europa.

- In de Europese Unie stelt de algemene verordening gegevensbescherming een één-loketmechanisme in voor zaken omtrent grensoverschrijdende verwerking. Sommige ondernemingen voeren grensoverschrijdende verwerkingsactiviteiten uit als gevolg van de verwerking van persoonsgegevens in het kader van activiteiten van vestigingen in meer dan één lidstaat of in het kader van een enkele vestiging in de Unie, maar die betrokkenen in meer dan één lidstaat wezenlijk aantast. In het kader van het mechanisme zullen dergelijke ondernemingen enkel nog te maken hebben met een nationale toezichthoudende autoriteit voor gegevensbescherming.

- Een samenwerkings- en coherentiemechanisme zal zorgen voor een gecoördineerde aanpak tussen alle betrokken toezichthoudende autoriteiten die in de zaak zijn betrokken. De leidende toezichthoudende autoriteit, van de hoofdvestiging of van de enige vestiging, raadpleegt en legt zijn ontwerpbesluit voor aan de andere betrokken toezichthoudende autoriteiten.

- Net als bij de huidige Groep artikel 29 zal de toezichthoudende autoriteit van elke lidstaat en de Europese Toezichthouder voor gegevensbescherming (EDPS) deel uitmaken van het Europees Comité voor gegevensbescherming.

- De taken van het Europees Comité voor gegevensbescherming omvatten bijvoorbeeld de monitoring van de juiste toepassing van de verordening, het adviseren van de Commissie over relevante kwesties en het uitbrengen van adviezen, richtsnoeren of beste praktijken over diverse onderwerpen.

- Het belangrijkste verschil is dat het Europees Comité voor gegevensbescherming niet enkel adviezen uitbrengt, als in het kader van Richtlijn 95/46/EG. Het zal ook bindende beslissingen vaststellen met betrekking tot zaken waar een toezichthoudende autoriteit een relevant en gemotiveerd bezwaar heeft ingediend in één-loketzaken; waar tegenstrijdige standpunten bestaan over wie van de toezichthoudende autoriteiten de leiding neemt, en, ten slotte, waar de bevoegde toezichthoudende autoriteit het advies van de EDPB niet vraagt of opvolgt. Het doel is te zorgen voor een consistente toepassing van de verordening in alle lidstaten.

Onafhankelijk toezicht is een essentieel onderdeel van de Europese gegevensbeschermingswetgeving. Zowel het Unierecht als het recht van de Raad van Europa beschouwen het bestaan van onafhankelijke toezichthoudende autoriteiten als onmisbaar voor de doeltreffende bescherming van de rechten en vrijheden van natuurlijke personen met betrekking tot de verwerking van hun persoonsgegevens. Aangezien gegevensverwerking nu alom vertegenwoordigd is en steeds ingewikkelder wordt voor natuurlijke personen om te begrijpen, zijn deze autoriteiten de waakhonden van het digitale tijdperk. In de Europese Unie wordt het bestaan van onafhankelijke toezichthoudende autoriteiten beschouwd als een van de meest essentiële onderdelen van het recht op bescherming van persoonsgegevens die zijn vastgelegd in het primaire Unierecht. Artikel 8, lid 3, van het EU-Handvest van de grondrechten, en artikel 16, lid 2, van het VWEU erkennen de bescherming van

persoonsgegevens als een fundamenteel recht en bevestigen dat de naleving van de regels inzake gegevensbescherming moet worden onderworpen aan controle door een onafhankelijke autoriteit.

Het belang van onafhankelijk toezicht voor de gegevensbeschermingswetgeving is ook erkend in de jurisprudentie.

Voorbeeld: In *Schrems*[491] was het HvJ-EU begaan met de vraag of de doorgifte van persoonsgegevens aan de Verenigde Staten (VS) onder het eerste EU-VS "veiligehavenakkoord" in overeenstemming was met de EU-wetgeving inzake gegevensbescherming, gezien de onthullingen van Edward Snowden over de grootschalige controle uitgevoerd door het National Security Agency van de Verenigde Staten. De doorgifte van persoonsgegevens aan de VS was gebaseerd op een beschikking van de Europese Commissie uit 2000 waardoor persoonsgegevens konden worden overgedragen van de EU naar VS-organisaties die zichzelf certificeren onder de "veiligehavenregeling", in de veronderstelling dat de regeling een passend beschermingsniveau voor persoonsgegevens waarborgt. Toen werd gevraagd om het verzoek van de indiener te onderzoeken, wees de Ierse toezichthoudende autoriteit de klacht af op grond van het feit dat het bestaan van de beschikking van de Commissie over de gepastheid van het stelsel voor gegevensbescherming van de Verenigde Staten, zoals weerspiegeld in de "veiligehavenbeginselen" (de "veiligehavenbeschikking"), haar niet toeliet de klacht verder te onderzoeken.

Het HvJ-EU heeft echter verklaard dat het bestaan van een beschikking van de Commissie waarbij de doorgifte van gegevens naar derde landen, die zorgen voor een toereikend niveau van bescherming, wordt toegelaten, de bevoegdheden van nationale toezichthoudende autoriteiten niet vermindert of wegneemt. Het HvJ-EU merkte op dat de bevoegdheden van deze autoriteiten om de naleving van de EU-gegevensbeschermingsregels te controleren en te garanderen, afkomstig zijn van het primaire recht van de Europese Unie, met name artikel 8, lid 3, van het Handvest en artikel 16,

491 HvJ-EU, zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner*, [Grote kamer], 6 oktober 2015.

lid 2, van het VWEU. "[...] de instelling van onafhankelijke toezichthoudende autoriteiten [is] dus van wezenlijk belang voor de eerbiediging van de bescherming van personen bij de verwerking van persoonsgegevens"[492].

Het HvJ-EU besloot daarom dat, zelfs wanneer de doorgifte van persoonsgegevens deel uitmaakte van een beschikking van de Commissie betreffende de passende bescherming van persoonsgegevens, als een klacht is ingediend bij een nationale toezichthoudende autoriteit, de autoriteit de klacht zorgvuldig dient te onderzoeken. De toezichthoudende autoriteit kan de klacht verwerpen indien zij vaststelt dat hij ongegrond is. In dat geval heeft het HvJ-EU benadrukt dat het recht op een effectief beroep in rechte vereist dat natuurlijke personen in staat moeten zijn om een dergelijk besluit aan te vechten bij de nationale rechterlijke instanties die de zaak kunnen doorverwijzen naar het Hof van Justitie voor een prejudiciële beslissing over de geldigheid van het besluit van de Commissie. Indien de toezichthoudende autoriteit van mening is dat de klacht gegrond is, moet zij in staat zijn om in rechte op te treden en de zaak voor te leggen aan de nationale rechterlijke instanties. De nationale rechterlijke instanties kunnen de zaak naar het HvJ-EU doorverwijzen, aangezien dit het enige orgaan is dat bevoegd is om te beslissen over de geldigheid van een beschikking van de Commissie betreffende de passende bescherming van persoonsgegevens[493].

Het HvJ-EU heeft vervolgens de geldigheid van de "veiligehavenbeschikking" onderzocht om vast te stellen of het systeem voor overdrachten in overeenstemming was met de EU-regels inzake gegevensbescherming. Het stelde vast dat artikel 3 van de "veiligehavenbeschikking" de (op grond van de richtlijn gegevensbescherming toegekende) bevoegdheden van de nationale toezichthoudende autoriteiten om maatregelen te nemen om gegevensoverdrachten te voorkomen in het geval van een onvoldoende beschermingsniveau voor persoonsgegevens in de VS, beperkt. Gezien het belang van de onafhankelijke toezichthoudende autoriteiten in de naleving van de gegevensbeschermingwetgeving heeft het HvJ-EU verklaard dat, in het kader van de richtlijn inzake gegevensbescherming en gelezen in het licht van het Handvest, de Commissie niet over de bevoegdheid beschikt om de bevoegdheden van de onafhankelijke toezichthoudende autoriteiten

492 HvJ-EU, zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer], 6 oktober 2015, punt 41.

493 *Ibid.*, punten 53-66.

op zodanige wijze te beperken. De beperking van de bevoegdheden van de toezichthoudende autoriteiten was een van de redenen waarom het HvJ-EU de "veiligehavenbeschikking" nietig verklaarde.

Het Europees recht vereist onafhankelijk toezicht als een belangrijk mechanisme om een doeltreffende gegevensbescherming te waarborgen. Onafhankelijke toezichthoudende autoriteiten zijn het eerste contactpunt voor betrokkenen in geval van inbreuken op de privacy[494]. In het kader van het Unierecht en het recht van de Raad van Europa is de inrichting van toezichthoudende autoriteiten verplicht. Beide juridische kaders beschrijven de taken en bevoegdheden van deze autoriteiten op soortgelijke wijze als deze die zijn opgenomen in de algemene verordening gegevensbescherming. In beginsel moeten toezichthoudende autoriteiten derhalve volgens het Unierecht en het RvE-recht op dezelfde manier functioneren[495].

5.1. Onafhankelijkheid

Het Unierecht en **het recht van de Raad van Europa** eisen dat elke toezichthoudende autoriteit volledig onafhankelijk optreedt bij de uitoefening van haar taken en bevoegdheden[496]. De onafhankelijkheid van de toezichthoudende autoriteit en haar leden, alsmede van het personeel, ten opzichte van directe of indirecte externe beïnvloeding, is van fundamenteel belang voor het waarborgen van volledige objectiviteit bij besluiten inzake gegevensbescherming. Niet alleen moet de wet die aan de grondslag ligt van de oprichting van een toezichthoudende autoriteit bepalingen bevatten die haar onafhankelijkheid specifiek waarborgen, maar uit de organisatiestructuur van de autoriteit moet ook haar onafhankelijkheid blijken. In 2010 onderzocht het HvJ-EU, voor de eerste keer, in hoeverre toezichthoudende autoriteiten voor gegevensbescherming onafhankelijk moeten zijn[497]. De benadrukte voorbeelden illustreren de definitie van de betekenis van "volledige onafhankelijkheid" van het HvJ-EU.

494 Algemene verordening gegevensbescherming, artikel 13, lid 2, onder d).

495 *Ibid.*, artikel 51, Gemoderniseerd Verdrag 108, artikel 15.

496 Algemene verordening gegevensbescherming, artikel 52, lid 1; Gemoderniseerd Verdrag 108, artikel 15, lid 5.

497 FRA (2010), *Grondrechten: uitdagingen en resultaten in 2010*, Jaarlijks verslag 2010, blz. 59; FRA (2010), *Gegevensbescherming in de Europese Unie: de rol van de nationale gegevensbeschermingsautoriteiten*, mei 2010.

Voorbeeld: In *Europese Commissie/Bondsrepubliek Duitsland* [498] verzocht de Europese Commissie het HvJ-EU om te verklaren dat Duitsland de eis van "volledige onafhankelijkheid" van de toezichthoudende autoriteiten voor gegevensbescherming niet correct had omgezet in Duits recht en derhalve zijn verplichting uit hoofde van artikel 28, lid 1, van de richtlijn gegevensbescherming niet had vervuld. De Commissie was van oordeel dat het feit dat Duitsland de toezichthoudende autoriteiten, die toezien op de verwerking van persoonsgegevens in de verschillende federale staten (*Länder*), onder staatstoezicht had geplaatst om de naleving van de gegevensbeschermingswetgeving te verzekeren, de onafhankelijkheidsvereiste schond.

Het HvJ-EU wees erop dat de woorden "met volledige onafhankelijkheid" moeten worden geïnterpreteerd op basis van de huidige bewoording van die bepaling en van de doelstellingen en de opzet van de EU-wetgeving inzake gegevensbescherming[499]. Het Hof van Justitie benadrukte dat de toezichthoudende autoriteiten "de bewakers" zijn van rechten in verband met de verwerking van persoonsgegevens. Daarom wordt hun inrichting in lidstaten beschouwd als "van wezenlijk belang voor de eerbiediging van de bescherming van personen bij de verwerking van persoonsgegevens"[500]. Het HvJ-EU concludeerde dat de toezichthoudende autoriteiten "[b]ij de uitoefening van hun taken (...) bijgevolg objectief en onpartijdig [moeten] handelen. Daartoe moeten zij vrij zijn van beïnvloeding van buitenaf, daar onder begrepen de directe of indirecte beïnvloeding door de staat of de Länder"[501].

Ook oordeelde het HvJ-EU dat de betekenis van "volledige onafhankelijkheid" moet worden uitgelegd in het licht van de onafhankelijkheid van de EDPS als omschreven in de op de EU-instellingen toepasselijke verordening gegevensbescherming. In deze verordening vereist het concept van onafhankelijkheid dat de EDPS instructies van anderen kan vragen noch aanvaarden.

498 HvJ-EU, zaak C-518/07, *Europese Commissie/Bondsrepubliek Duitsland* [Grote kamer], 9 maart 2010, punt 27.

499 *Ibid.*, punten 17 en 29.

500 *Ibid.*, punt 23.

501 *Ibid.*, punt 25.

Bijgevolg heeft het HvJ-EU geoordeeld dat de toezichthoudende autoriteiten in Duitsland, door het toezicht door de overheid, niet volledig onafhankelijk zijn in de zin van de EU-wetgeving inzake gegevensbescherming.

Voorbeeld: In *Europese Commissie/Republiek Oostenrijk*[502] wees het HvJ-EU op soortgelijke problemen in verband met de onafhankelijkheid van bepaalde leden en personeel van de Oostenrijkse gegevensbeschermingsautoriteit (Datenschutzkommission, DSK). Het HvJ-EU is tot de conclusie gekomen dat het feit dat de Federale Kanselarij het personeel heeft geleverd aan de toezichthoudende autoriteit, de onafhankelijkheidsvereiste die voorzien is in de EU-wetgeving inzake gegevensbescherming, ondermijnt. Het HvJ-EU was daarnaast van mening dat de eis om de Kanselarij te allen tijde te informeren over zijn werk, geen rekening hield met de volledige onafhankelijkheid van de toezichthoudende autoriteit.

Voorbeeld: In de *Europese Commissie/Hongarije*[503] werden soortgelijke nationale praktijken die afbreuk deden aan de onafhankelijkheid van het personeel, verboden. Het HvJ-EU wees erop dat "het vereiste [...] dat moet worden gewaarborgd dat elke toezichthoudende autoriteit de haar opgedragen taken in volledige onafhankelijkheid vervult, impliceert dat de betrokken lidstaat verplicht is de duur van het mandaat van een dergelijke autoriteit te eerbiedigen tot het aanvankelijk voorziene einde daarvan". Het HvJ-EU heeft ook verklaard dat "Hongarije, door het mandaat van de toezichthoudende autoriteit voor de bescherming van persoonsgegevens voortijdig te hebben beëindigd, de verplichtingen niet is nagekomen die op hem rusten krachtens Richtlijn 95/46/EG [...]."

Het begrip en de criteria van "volledige onafhankelijkheid" zijn nu uitdrukkelijk opgenomen in de algemene verordening gegevensbescherming, waarin de beginselen zijn opgenomen die zijn vastgesteld doorheen de beschreven arresten van het HvJ-EU. Uit hoofde van de verordening houdt volledige onafhankelijkheid in de uitoefening van hun taken en bevoegdheden in dat[504]:

502 HvJ-EU, zaak C-614/10, *Europese Commissie/Republiek Oostenrijk* [Grote kamer], 16 oktober 2012, punten 59 en 63.

503 HvJ-EU, zaak C-288/12, *Europese Commissie/Hongarije* [Grote kamer], 8 april 2014, punten 50 en 67.

504 Algemene verordening gegevensbescherming, artikel 52.

- de leden van elke toezichthoudende autoriteit vrij moeten zijn van externe beïnvloeding, direct of indirect, en geen instructies van anderen mogen aannemen;

- de leden van elke toezichthoudende autoriteit zich dienen te onthouden van iedere handeling die onverenigbaar is met hun functie, ter voorkoming van belangenconflicten;

- lidstaten elke toezichthoudende autoriteit van de nodige menselijke, technische en financiële middelen en infrastructuur voor de efficiënte uitoefening van hun taken moeten voorzien;

- lidstaten ervoor moeten zorgen dat elke toezichthoudende autoriteit zijn eigen personeel kiest;

- de financiële controle waaraan elke toezichthoudende autoriteit krachtens het nationale recht is onderworpen, geen afbreuk mag doen aan haar onafhankelijkheid. Toezichthoudende autoriteiten moeten beschikken over afzonderlijke en openbare jaarlijkse begrotingen om goed te kunnen functioneren.

De onafhankelijkheid van toezichthoudende autoriteiten wordt ook beschouwd als een essentiële vereiste in het kader van het recht van de Raad van Europa. Het Gemoderniseerd Verdrag 108 vereist dat toezichthoudende autoriteiten "met volledige onafhankelijkheid en onpartijdigheid handelen bij het uitoefenen van hun taken en bevoegdheden", zonder dat ze instructies vragen of aanvaarden[505]. Op deze manier erkent het verdrag dat de autoriteiten de rechten en vrijheden van natuurlijke personen in verband met de verwerking van gegevens niet op efficiente wijze kunnen waarborgen, tenzij ze hun taken volledig onafhankelijk uitoefenen. Het toelichtend verslag van het Gemoderniseerd Verdrag 108 formuleert een aantal elementen die bijdragen tot het waarborgen van deze onafhankelijkheid. Die elementen omvatten de mogelijkheid voor toezichthoudende autoriteiten om hun eigen personeel aan te werven en om beslissingen te nemen zonder beïnvloed te worden door externe inmenging, evenals factoren met betrekking tot de duur van de uitoefening van hun taken en de voorwaarden waaronder zij hun werkzaamheden mogen stopzetten[506].

505 Gemoderniseerd Verdrag 108, artikel 15, lid 5.

506 Memorie van toelichting bij Gemoderniseerd Verdrag 108.

5.2. Competentie en bevoegdheden

In het Unierecht beschrijft de algemene verordening gegevensbescherming de competenties en organisatorische structuur van toezichthoudende autoriteiten en eist dat zij competent zijn en de bevoegdheden bezitten om de vereiste taken in het kader van de verordening uit te voeren.

De toezichthoudende autoriteit is het belangrijkste orgaan in de nationale wetgeving die de naleving van de EU-wetgeving inzake gegevensbescherming garandeert. De toezichthoudende autoriteiten beschikken over een uitgebreide lijst van taken en bevoegdheden die verder gaan dan alleen het toezicht houden, waaronder proactieve en preventieve toezichtsactiviteiten. Om deze taken uit te voeren moeten toezichthoudende autoriteiten over passende onderzoeks-, corrigerende en adviserende bevoegdheden beschikken zoals opgesomd in artikelen 57 en 58 van de algemene verordening gegevensbescherming, zoals[507]:

- verwerkingsverantwoordelijken en betrokkenen adviezen verstrekken over alle gegevensbeschermingsaangelegenheden;
- standaardcontractbepalingen, bindende bedrijfsvoorschriften of administratieve regelingen goedkeuren;
- verwerkingen controleren en dienovereenkomstig ingrijpen;
- eisen dat alle informatie die relevant is voor het toezicht op verwerkingsverantwoordelijken wordt ingediend;
- verwerkingsverantwoordelijken waarschuwen of berispen en gelasten dat kennisgevingen van inbreuken op persoonsgegevens aan de betrokkenen worden toegezonden;
- de rectificatie, afscherming, uitwissing of vernietiging van gegevens gelasten;
- een tijdelijk of definitief verwerkingsverbod of administratieve boetes opleggen;
- de zaak doorverwijzen naar de rechter.

507 Algemene verordening gegevensbescherming, artikel 57 en 58. Zie voorts Verdrag 108, Aanvullend Protocol, artikel 1.

Om haar taken te kunnen vervullen, moet een toezichthoudende autoriteit toegang hebben tot alle persoonsgegevens en informatie die noodzakelijk is om een onderzoek te verrichten, evenals toegang tot alle bedrijfsruimten waar een voor de verwerking verantwoordelijke relevante informatie bewaart. Volgens het HvJ-EU moeten de bevoegdheden van de toezichthoudende autoriteit breed worden geïnterpreteerd om volledige doeltreffendheid van de gegevensbescherming voor betrokkenen in de EU te garanderen.

Voorbeeld: In *Schrems* was het HvJ-EU begaan met de vraag of de overdracht van persoonsgegevens aan de VS onder het eerste EU-VS-veiligehavenakkoord in overeenstemming was met de EU-wetgeving inzake gegevensbescherming in het licht van de onthullingen van Edward Snowden. Het HvJ-EU redeneerde dat nationale toezichthoudende autoriteiten, die handelen in hun hoedanigheid als onafhankelijke toezichthouders van gegevensverwerking door verwerkingsverantwoordelijken, kunnen voorkomen dat persoonsgegevens worden overgedragen aan een derde land ondanks het bestaan van een adequaatheidsbesluit indien er redelijke aanwijzingen zijn dat de passende bescherming niet langer is gegarandeerd in het derde land[508].

Elke toezichthoudende autoriteit is bevoegd om onderzoeks- en handelingsbevoegdheden op haar grondgebied uit te voeren. Echter, aangezien de werkzaamheden van verwerkingsverantwoordelijken en verwerkers vaak een grensoverschrijdend karakter hebben en gegevensverwerking invloed heeft op betrokkenen die in verschillende lidstaten gevestigd zijn, rijst de vraag of de bevoegdheden tussen de verschillende toezichthoudende instanties moeten worden verdeeld. Het HvJ-EU kreeg de gelegenheid om deze kwestie in de zaak *Weltimmo* te onderzoeken.

Voorbeeld: In *Weltimmo*[509] boog het HvJ-EU zich over de bevoegdheid van nationale toezichthoudende autoriteiten om aangelegenheden te behandelen waarbij organisaties zijn betrokken die niet in hun rechtsgebied liggen. Weltimmo was een onderneming die in Slowakije stond geregistreerd en een website voor vastgoedtransacties voor Hongaarse eigendommen beheerde.

508 HvJ-EU, zaak C-362/14, *Maximilian Schrems/Data Protection Commissioner* [Grote kamer], 6 oktober 2015, punten 26-36 en 40-41.

509 HvJ-EU, zaak C-230/14, *Weltimmo s.r.o./Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 oktober 2015.

Adverteerders dienden een klacht in bij de Hongaarse toezichthoudende autoriteit voor gegevensbescherming voor het overtreden van de Hongaarse gegevensbeschermingswetgeving, en de autoriteit heeft Weltimmo een geldboete opgelegd. De onderneming betwistte de geldboete voor de nationale rechter en de zaak werd voorgelegd aan het HvJ-EU om vast te stellen of de Europese richtlijn inzake gegevensbescherming toelaat dat de toezichthoudende autoriteiten van een lidstaat hun eigen nationale recht inzake gegevensbescherming toepassen op een onderneming die in een andere lidstaat staat geregistreerd.

Het HvJ-EU interpreteerde artikel 4, lid 1, onder a), van de richtlijn inzake gegevensbescherming dat het de toepassing van een gegevensbeschermingswetgeving van een andere lidstaat dan de lidstaat waar de verwerkingsverantwoordelijke is geregistreerd toelaat, "voor zover bedoelde verantwoordelijke via een duurzame vestiging op het grondgebied van die lidstaat een, zelfs geringe, reële en daadwerkelijke activiteit uitoefent, in het kader waarvan die verwerking plaatsvindt". Het HvJ-EU merkte op dat, op basis van de informatie waarover het beschikte, Weltimmo een reële en daadwerkelijke activiteit in Hongarije uitoefende aangezien de onderneming een vertegenwoordiger in Hongarije in het Slowaakse handelsregister had laten opnemen met een Hongaars adres evenals een Hongaarse bankrekening en postbus, en activiteiten in Hongarije nastreefde die in het Hongaars waren geschreven. Deze informatie duidde op het bestaan van een vestiging waardoor de activiteit van Weltimmo onderworpen is aan de Hongaarse gegevensbeschermingswetgeving en het gerechtsgebied van de Hongaarse toezichthoudende autoriteit. Het HvJ-EU oordeelde echter dat het aan de nationale rechter is om de informatie na te gaan en te bepalen of Weltimmo inderdaad een vestiging in Hongarije had.

Indien de verwijzende rechter constateerde dat Weltimmo een vestiging in Hongarije had, zou de Hongaarse toezichthoudende autoriteit de bevoegdheid hebben om een geldboete op te leggen. Indien echter de nationale rechter het tegendeel zou besluiten, d.w.z. dat Weltimmo geen vestiging in Hongarije had, zou bijgevolg de toepasselijke wetgeving die van de lidstaat zijn waar de onderneming is geregistreerd. In dit geval, aangezien de bevoegdheden van toezichthoudende autoriteiten moeten worden uitgeoefend in overeenstemming met de territoriale soevereiniteit van andere lidstaten, zou de Hongaarse autoriteit niet in staat zijn tot het opleggen van sancties. Aangezien de richtlijn inzake gegevensbescherming

een verplichting omvat voor toezichthoudende autoriteiten om samen te werken, kan de Hongaarse autoriteit zijn Slowaakse tegenhanger echter vragen om de zaak te onderzoeken, een inbreuk naar Slowaaks recht vast te stellen en de sancties opleggen waarin de Slowaakse wetgeving voorziet.

Met de invoering van de algemene verordening gegevensbescherming zijn er nu gedetailleerde regels van kracht betreffende de bevoegdheid van toezichthoudende autoriteiten in grensoverschrijdende zaken. De verordening stelt een "één-loketmechanisme" in en omvat bepalingen waarmee de samenwerking tussen de verschillende toezichthoudende instanties wordt bepaald. Voor een doeltreffende samenwerking in grensoverschrijdende zaken vereist de Algemene Verordening Gegevensverwerking dat de toezichthoudende autoriteit van de hoofdvestiging of van de enige vestiging van de verwerkingsverantwoordelijke of verwerker als leidende toezichthoudende autoriteit kan worden beschouwd[510]. De leidende toezichthoudende autoriteit is verantwoordelijk voor grensoverschrijdende zaken, is het enige aanspreekpunt voor de verwerkingsverantwoordelijke of verwerker en coördineert de samenwerking met betrokken toezichthoudende autoriteiten om consensus te bereiken. De samenwerking omvat het uitwisselen van informatie, wederzijdse bijstand bij onderzoeken, en het nemen van bindende besluiten[511].

In het recht van de Raad van Europa zijn de competenties en bevoegdheden van de toezichthoudende autoriteiten opgenomen in artikel 15 van het Gemoderniseerd Verdrag 108. Deze bevoegdheden sluiten aan bij die van de toezichthoudende autoriteiten in het kader van de EU-wetgeving, met inbegrip van onderzoeks- en interventiebevoegdheden, bevoegdheden om besluiten te nemen en administratieve sancties op te leggen ten aanzien van schendingen van het verdrag en bevoegdheden om in rechte op te treden. Onafhankelijke toezichthoudende autoriteiten zijn tevens bevoegd om verzoeken en klachten ingediend door betrokkenen te behandelen, om het publiek bewust te maken van de wetgeving inzake gegevensbescherming en om advies te verstrekken aan nationale beleidsmakers voor elke wettelijke of administratieve maatregel die voorziet in de verwerking van persoonsgegevens.

510 Algemene verordening gegevensbescherming, artikel 56, lid 1.

511 *Ibid.*, artikel 60.

5.3. Samenwerking

De algemene verordening gegevensbescherming (AVG) vormt een algemeen kader voor de samenwerking tussen toezichthoudende autoriteiten en stelt specifiekere regels vast over de samenwerking van toezichthoudende autoriteiten in zaken betreffende grensoverschrijdende gegevensverwerking.

In het kader van de AVG zullen toezichthoudende autoriteiten elkaar wederzijdse bijstand verlenen en relevante informatie delen om de verordening op een consistente manier uit te voeren en toe te passen[512]. Dit houdt onder meer in dat de bevoegde toezichthoudende autoriteit informatie inwint en inspecties en onderzoeken uitvoert. Toezichthoudende autoriteiten kunnen gezamenlijke werkzaamheden uitvoeren, met inbegrip van gezamenlijk onderzoek en gezamenlijke handhavingsmaatregelen waarbij personeelsleden van alle toezichthoudende autoriteiten zijn betrokken[513].

In de Europese Unie werken verwerkingsverantwoordelijken en verwerkers in toenemende mate op transnationaal niveau samen. Dit vereist een nauwe samenwerking tussen de bevoegde toezichthoudende autoriteiten in de lidstaten om ervoor te zorgen dat de verwerking van persoonsgegevens in overeenstemming is met de vereisten van de AVG. Indien in het kader van het "één-loketmechanisme" van de verordening een verwerkingsverantwoordelijke of verwerker vestigingen in meerdere lidstaten heeft, of een enkele vestiging waarbij de verwerkingsoperaties substantiële gevolgen hebben voor de betrokkenen in meer dan één lidstaat, dan is de toezichthoudende autoriteit van de hoofdvestiging (of enkele vestiging) de leidende toezichthoudende autoriteit voor de grensoverschrijdende activiteiten van de verwerkingsverantwoordelijke of de verwerker. Leidende autoriteiten hebben de bevoegdheid om handhavingsmaatregelen te nemen tegen de verwerkingsverantwoordelijke of de verwerker. Het één-loketmechanisme richt zich op de verbeterde harmonisatie en de uniforme toepassing van de EU-wetgeving inzake gegevensbescherming in de lidstaten. Het is ook gunstig voor bedrijven aangezien ze enkel met de leidende autoriteit te maken krijgen in plaats van met meerdere toezichthoudende autoriteiten. Dit verhoogt de rechtszekerheid voor bedrijven en in de praktijk moet dit ook zorgen voor een snellere besluitvorming en vermijden dat bedrijven niet worden geconfronteerd met verschillende toezichthoudende autoriteiten die tegengestelde eisen opleggen.

512 *Ibid.*, artikelen 61, lid 1-3, en 62, lid 1.

513 *Ibid.*, artikel 62, lid 1.

Voor de identificatie van de leidende autoriteit moet de plaats van de hoofdvestiging van een bedrijf in de EU worden bepaald. De term "hoofdvestiging" wordt gedefinieerd in de AVG. Daarnaast heeft Groep artikel 29 richtsnoeren uitgevaardigd voor het vaststellen van een leidende toezichthoudende autoriteit voor de verwerkingsverantwoordelijke of de verwerker, met inbegrip van de criteria voor de identificatie van de hoofdvestiging[514].

Om te zorgen voor een hoog niveau van gegevensbescherming treedt de leidende toezichthoudende autoriteit niet alleen op. Hij moet samenwerken met de andere betrokken toezichthoudende autoriteiten om besluiten te nemen over de verwerking van persoonsgegevens bij verwerkingsverantwoordelijken en verwerkers door te trachten om consensus te bereiken en te zorgen voor samenhang. Samenwerking tussen de relevante toezichthoudende autoriteiten omvat de uitwisseling van informatie, wederzijdse bijstand, de uitvoering van gezamenlijke onderzoeken en toezichtsactiviteiten[515]. Bij het verlenen van wederzijdse bijstand moeten toezichthoudende autoriteiten verzoeken om informatie van andere toezichthoudende autoriteiten adequaat behandelen en toezichthoudende maatregelen, zoals bijvoorbeeld voorafgaande toestemmingen en voorafgaand overleg met de verwerkingsverantwoordelijke over zijn verwerkingsactiviteiten, controles of onderzoeken, uitvoeren. Wederzijdse bijstand aan toezichthoudende autoriteiten in andere lidstaten moet onverwijld worden verstrekt en uiterlijk één maand na ontvangst van het verzoek[516].

Wanneer de verwerkingsverantwoordelijke vestigingen in verschillende lidstaten heeft, kunnen de toezichthoudende autoriteiten gezamenlijke onderzoeken en gezamenlijke handhavingsmaatregelen uitvoeren waarbij personeelsleden van de toezichthoudende autoriteiten van andere lidstaten worden betrokken[517].

Samenwerking tussen de verschillende toezichthoudende autoriteiten is een belangrijke verplichting in het kader van het recht van de Raad van Europa. Het Gemoderniseerd Verdrag 108 bepaalt dat de toezichthoudende autoriteiten onderling dienen samen te werken voor zover nodig is om hun taken uit te voeren[518].

514 Groep artikel 29 (2016), *Richtsnoeren voor de vaststelling van de leidende toezichthoudende autoriteit van de verwerkingsverantwoordelijke of verwerker*, WP 244, Brussel, 13 december 2016, herzien op 5 april 2017.

515 Algemene verordening gegevensbescherming, artikel 60, lid 1-3.

516 *Ibid.*, artikel 61, leden 1 en 2.

517 *Ibid.*, artikel 62, lid 1.

518 Gemoderniseerd Verdrag 108, artikelen 16 en 17.

Dit moet bijvoorbeeld gebeuren door elkaar alle relevante en nuttig informatie te verstrekken, door onderzoeken te coördineren en gezamenlijke acties uit te voeren[519].

5.4. Het Europees Comité voor gegevensbescherming

Het belang van de onafhankelijke toezichthoudende autoriteiten en de belangrijkste bevoegdheden waarover ze beschikken op grond van de Europese wetgeving inzake gegevensbescherming zijn eerder in dit hoofdstuk beschreven. Het Europees Comité voor gegevensbescherming (EDPB) is een andere belangrijke speler die ervoor moet zorgen dat de regels inzake gegevensbescherming effectief en consistent worden toegepast in de hele EU.

De AVG stelt het EDPB in als een EU-orgaan met rechtspersoonlijkheid[520]. Het is de opvolger van Groep artikel 29[521], die door de richtlijn gegevensbescherming was opgericht om de Commissie te adviseren over EU-maatregelen die de rechten van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en privacy beïnvloeden, om de uniforme toepassing van de richtlijn te bevorderen en om de Commissie van deskundig advies te voorzien over aspecten in verband met gegevensbescherming. Groep artikel 29 bestond uit vertegenwoordigers van de toezichthoudende autoriteiten van de lidstaten, samen met vertegenwoordigers van de Commissie en het EDPS.

Net als Groep artikel 29 bevat het Comité de voorzitters van de toezichthoudende autoriteiten van elke lidstaat en de Europese Toezichthouder voor gegevensbescherming (EDPS), of hun vertegenwoordigers[522]. De EDPS heeft gelijk stemrecht, met uitzondering van gevallen met betrekking tot geschillenbeslechting, waar hij enkel mag stemmen over besluiten inzake op de EU-instellingen toepasselijke beginselen en voorschriften die inhoudelijk overeenkomen met die van de AVG. De

519 *Ibid.*, artikel 12 bis, lid 7.

520 Algemene verordening gegevensbescherming, artikel 68.

521 In het kader van Richtlijn 95/46/EG moest Groep artikel 29 de Commissie adviseren over de EU-maatregelen die de rechten van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en privacy beïnvloeden om de uniforme toepassing van de richtlijn te bevorderen en deskundig advies aan de Commissie te geven over aspecten in verband met gegevensbescherming. Groep artikel 29 bestond uit vertegenwoordigers van de toezichthoudende autoriteiten van de lidstaten, samen met de Commissie en de Europese Toezichthouder voor gegevensbescherming.

522 Algemene verordening gegevensbescherming, artikel 68, lid 3.

Commissie heeft het recht om deel te nemen aan de activiteiten en vergaderingen van het Comité, maar heeft geen stemrecht[523]. Het Comité kiest een voorzitter (die belast is met de vertegenwoordiging van het Comité) en twee vicevoorzitters uit zijn leden bij gewone meerderheid van stemmen voor een termijn van vijf jaar. Verder heeft het Comité ook een secretariaat ter beschikking dat door de Europese Toezichthouder voor gegevensbescherming wordt verzorgd om het Comité analytische, administratieve en logistieke steun te bieden[524].

De taken van het Comité zijn vermeld in de artikelen 64, 65 en 70 van de AVG en omvatten uitgebreide rechten die kunnen worden opgedeeld in drie hoofdactiviteiten:

- **Coherentie:** Het Comité kan bindende beslissingen vaststellen in drie gevallen: waar een toezichthoudende autoriteit een relevant en gemotiveerd bezwaar heeft ingediend in één-loketzaken; waar tegenstrijdige standpunten bestaan over wie van de toezichthoudende autoriteiten de leiding neemt, en, ten slotte, waar de bevoegde toezichthoudende autoriteit het advies van het Comité niet vraagt of opvolgt[525]. De hoofdverantwoordelijkheid van het Comité is ervoor te zorgen dat de AVG overal in de EU consistent wordt toegepast en het speelt een belangrijke rol in het coherentiemechanisme, zoals beschreven in punt 5.5.

- **Raadpleging:** De taken van het Comité omvatten het verlenen van advies aan de Commissie over alle kwesties die verband houden met de bescherming van persoonsgegevens in de Unie, zoals wijzigingen aan de AVG, herzieningen van de EU-wetgeving die betrekking hebben op de verwerking van gegevens en in strijd kunnen zijn met de EU-regels inzake gegevensbescherming of het nemen van adequaatheidsbesluiten van de Commissie die de overdracht van persoonsgegevens naar een derde land of een internationale organisatie mogelijk maakt.

- **Richtsnoer:** Het Comité geeft ook richtsnoeren, aanbevelingen en beste praktijken ter bevordering van de consistente toepassing van de verordening en bevordert de samenwerking en uitwisseling van kennis tussen de toezichthoudende autoriteiten. Bovendien moet het verenigingen van verwerkingsverantwoordelijken of verwerkers aanmoedigen om gedragscodes op te stellen, alsook certificeringsmechanismen voor gegevensverwerking en merktekens vast te stellen.

523 *Ibid.*, artikel 68, leden 4 en 5.

524 *Ibid.*, artikelen 73 en 75.

525 *Ibid.*, artikel 65.

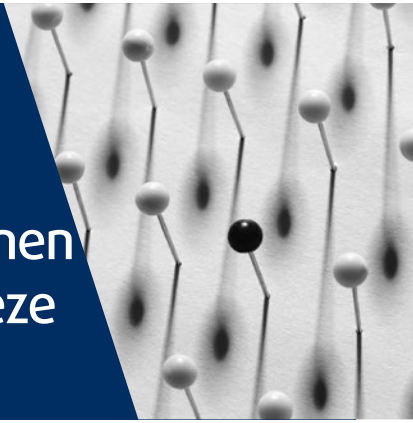
Besluiten van het Comité kunnen worden aangevochten voor het HvJ-EU.

5.5. Het coherentiemechanisme van de AVG

De AVG stelt een coherentiemechanisme in waarbij de toezichthoudende autoriteiten met elkaar en waar passend met de Commissie samenwerken om ervoor te zorgen dat de verordening in alle lidstaten consequent wordt toegepast. Het coherentiemechanisme wordt gebruikt in twee situaties. De eerste betreft adviezen van het Comité wanneer een bevoegde toezichthoudende autoriteit maatregelen wil nemen, zoals het opstellen van een lijst van verwerkingen die een gegevensbeschermingseffectbeoordeling vereisen, of standaardcontractbepalingen wil vastleggen. De tweede betreft bindende besluiten van het Comité voor toezichthoudende autoriteiten in één-loketzaken en wanneer een toezichthoudende autoriteit geen gevolg geeft aan een advies van het Comité of geen advies vraagt aan het Comité.

6

De rechten van betrokkenen en de handhaving van deze rechten



EU	Behandelde onderwerpen	RvE
Het recht om te worden geïnformeerd		
Algemene verordening gegevensbescherming, artikel 12 HvJ-EU, zaak C-473/12, *Beroepsinstituut van vastgoedmakelaars (BIV)/Englebert*, 2013 HvJ-EU, zaak C-201/14, *Smaranda Bara e.a./Casa Națională de Asigurări de Sănătate e.a.*, 2015	**Transparantie van informatie**	Gemoderniseerd Verdrag 108, artikel 8
Algemene verordening gegevensbescherming, artikel 13, leden 1 en 2, en artikel 14, leden 1 en 2	**Inhoud van de informatie**	Gemoderniseerd Verdrag 108, artikel 8, lid 1
Algemene verordening gegevensbescherming, artikel 13, lid 1, en artikel 14, lid 3	**Moment van de informatie-verstrekking**	Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder b)
Algemene verordening gegevensbescherming, artikel 12, leden 1, 5 en 7	**Manieren om informatie te verstrekken**	Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder b)
Algemene verordening gegevensbescherming, artikel 13, lid 2, onder d), en artikel 14, lid 2, onder e), artikelen 77, 78 en 79	**Het recht om een klacht in te dienen**	Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder f)

EU	Behandelde onderwerpen	RvE
Recht van toegang		
Algemene verordening gegevensbescherming, artikel 15, lid 1 HvJ-EU, zaak C-553/07, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, 2009 HvJ-EU, gevoegde zaken C-141/12 en C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel* en *Minister voor Immigratie, Integratie en Asiel/M en S*, 2014 HvJ-EU, zaak C-434/16, *Peter Nowak/Data Protection Commissioner*, 2017	**Recht op toegang tot eigen persoonsgegevens**	Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder b) EHRM, *Leander/Zweden*, nr. 9248/81, 1987
Recht op rectificatie		
Algemene verordening gegevensbescherming, artikel 16	**Rectificatie van onjuiste persoonsgegevens**	Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder e) EHRM, *Cemalettin Canli/Turkije*, nr. 22427/04, 2008 EHRM, *Ciubotaru/Moldavië*, nr. 27138/04, 2010
Recht op wissing		
Algemene verordening gegevensbescherming, artikel 17, lid 1	**Het wissen van persoonsgegevens**	Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder e) EHRM, *Segerstedt-Wiberg e.a./Zweden*, nr. 62332/00, 2006
HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 2014 HvJ-EU, zaak C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 2017	**Het recht om te worden vergeten**	

EU	Behandelde onderwerpen	RvE
Recht op beperking van de verwerking		
Algemene verordening gegevensbescherming, artikel 18, lid 1	Recht op een beperking van het gebruik van persoonsgegevens	
Algemene verordening gegevensbescherming, artikel 19	Kennisgevings-verplichting	
Recht op gegevensportabiliteit		
Algemene verordening gegevensbescherming, artikel 20	Recht op gegevens-portabiliteit	
Recht van bezwaar		
Algemene verordening gegevensbescherming, artikel 21, lid 1 HvJ-EU, zaak C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni* 2017	Recht van bezwaar op grond van de bijzondere situatie van de betrokkene	Aanbeveling inzake profilering, artikel 5.3 Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder d)
Algemene verordening gegevensbescherming, artikel 21, lid 2	Recht van bezwaar tegen verder gebruik van gegevens met het oog op direct marketing	Aanbeveling inzake direct marketing, artikel 4.1
Algemene verordening gegevensbescherming, artikel 21, lid 5	Recht van bezwaar via geautomatiseerde weg	
Rechten met betrekking tot geautomatiseerde besluitvorming en profilering		
Algemene verordening gegevensbescherming, artikel 22	Rechten met betrekking tot geautomatiseerde besluitvorming en profilering	Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder a)
Algemene verordening gegevensbescherming, artikel 21	Recht om bezwaar te maken tegen automatische besluitvorming	
Algemene verordening gegevensbescherming, artikel 13, lid 2, onder f)	Recht op een zinvolle toelichting	Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder c)

EU	Behandelde onderwerpen	RvE
Corrigerende maatregelen, aansprakelijkheid, sancties en schadeloosstelling		
Handvest, artikel 47 HvJ-EU, zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner*, [Grote kamer], 2015 Algemene verordening gegevensbescherming, artikelen 77-84	**Voor inbreuken op nationale gegevens-beschermings-wetgeving**	EVRM, artikel 13 (alleen voor lidstaten van de RvE) Gemoderniseerd Verdrag 108, artikelen 9, lid 1, onder f), 12, 15, 16-21 EHRM, *K.U./Finland*, nr. 2872/02, 2008 EHRM, *Biriuk/Litouwen*, nr. 23373/03, 2008
Verordening Gegevensbescherming EU-instellingen, artikelen 34 en 49 HvJ-EU, zaak C-28/08 P, *Europese Commissie/The Bavarian Lager Co. Ltd* [Grote kamer], 2010	**Voor inbreuken op EU-wetgeving door EU-instellingen en -organen**	

De effectiviteit van wettelijke voorschriften in het algemeen en rechten van betrokkenen in het bijzonder is in aanzienlijke mate afhankelijk van het bestaan van passende mechanismen om ze te handhaven. In het digitale tijdperk is gegevensverwerking overal aanwezig en steeds moeilijker te begrijpen voor individuen. Teneinde de machtsverschillen tussen betrokkenen en verwerkingsverantwoordelijken te beperken, kregen individuen bepaalde rechten om een grotere zeggenschap uit te oefenen over de verwerking van hun persoonsgegevens. Het recht op toegang tot de eigen gegevens en het recht op de herziening ervan zijn verankerd in artikel 8, lid 2, van het EU-Handvest van de grondrechten, een document dat primair EU-recht is en voorrang heeft in de rechtsorde van de EU. De secundaire wetgeving van de EU, de algemene verordening gegevensbescherming in het bijzonder, heeft een samenhangend wettelijk kader opgesteld dat betrokkenen in staat stelt van hun rechten gebruik te maken door hun rechten toe te kennen met betrekking tot de verwerkingsverantwoordelijken. Naast het recht tot toegang en rectificatie erkent de AVG een reeks andere rechten, zoals het recht op wissing ("het recht om te worden vergeten"), het recht van bezwaar tegen of het recht op beperking van gegevensverwerking, alsmede de rechten met betrekking tot geautomatiseerde besluitvorming en profilering. Gelijkaardige garanties die betrokkenen in staat stellen om het feitelijk gezag uit te oefenen over hun gegevens zijn ook opgenomen in het Gemoderniseerd Verdrag 108. Artikel 9 bevat de rechten die individuen moeten kunnen uitoefenen met betrekking tot de verwerking van hun persoonsgegevens. De verdragsluitende partijen moeten ervoor zorgen dat deze rechten ter beschikking

worden gesteld van elke betrokkene binnen hun rechtsgebied en vergezeld gaan van doeltreffende juridische en praktische middelen, zodat betrokkenen die rechten kunnen uitoefenen.

Naast het gunnen van rechten aan individuen is het evenzeer van belang dat er mechanismen worden ingesteld die betrokkenen in staat stellen om inbreuken op hun rechten aan te vechten, verwerkingsverantwoordelijken verantwoordelijk te houden en een schadevergoeding te eisen. Het recht op een doeltreffende voorziening in rechte, als gegarandeerd door het EVRM en het Handvest, vereist dat aan iedere persoon rechtsmiddelen ter beschikking staan.

6.1. De rechten van betrokkenen

Belangrijkste punten

- Elke betrokkene heeft recht op informatie over alle verwerkingen van zijn/haar persoonsgegevens die de verwerkingsverantwoordelijke uitvoert, behoudens beperkte uitzonderingen.
- Betrokkenen hebben het recht om:
  - toegang te krijgen tot hun eigen gegevens en bepaalde informatie over de verwerking te verkrijgen;
  - hun gegevens te laten rectificeren door de verwerkingsverantwoordelijke die hun gegevens verwerkt als de gegevens onjuist zijn;
  - de verwerkingsverantwoordelijke hun gegevens te laten verwijderen, voor zover van toepassing, indien de verwerkingsverantwoordelijke hun gegevens onrechtmatig verwerkt;
  - tijdelijk de verwerking te beperken;
  - hun gegevens over te dragen naar een andere verwerkingsverantwoordelijke onder bepaalde voorwaarden.
- Voorts hebben betrokkenen het recht om bezwaar te maken tegen verwerking:
  - om redenen die verband houden met hun specifieke situatie;
  - voor het gebruik van hun gegevens voor directmarketingdoeleinden.

- Betrokkenen hebben het recht om niet te worden onderworpen aan de besluiten die uitsluitend op geautomatiseerde gegevensverwerking zijn gebaseerd, met inbegrip van de profilering, die rechtsgevolgen hebben of die hem/haar aanzienlijk beïnvloeden. Betrokkenen hebben ook het recht om:
  - menselijke interventie te verkrijgen door de verwerkingsverantwoordelijke;
  - hun mening uit te drukken en een besluit te betwisten dat gebaseerd is op geautomatiseerde gegevensverwerking.

6.1.1. Het recht om te worden geïnformeerd

Zowel volgens **het recht van de Raad van Europa** als **het Unierecht** zijn verwerkingsverantwoordelijken verplicht om de betrokkene in kennis te stellen van de voorgenomen verwerking op het ogenblik dat de persoonsgegevens worden verzameld. Deze verplichting is niet afhankelijk van een verzoek van de betrokkene, maar moet eerder proactief worden nagekomen door de verwerkingsverantwoordelijke, ongeacht of de betrokkene belangstelling toont voor de informatie of niet.

In het kader van het recht van de Raad van Europa, op grond van artikel 8 van het Gemoderniseerd Verdrag 108, moeten verdragsluitende partijen ervoor zorgen dat verwerkingsverantwoordelijken de betrokkenen informeren over hun identiteit en woonplaats, de rechtsgrondslag en het doel van de verwerking, de te verwerken categorieën persoonsgegevens (indien van toepassing) en de wijze waarop ze hun rechten kunnen doen laten gelden krachtens artikel 9 dat het recht op toegang, rectificatie en rechtsmiddel omvat. Elke andere aanvullende informatie die noodzakelijk wordt geacht om te zorgen voor een eerlijke en transparante verwerking van persoonsgegevens, dient ook te worden meegedeeld aan de betrokkenen. De memorie van toelichting bij het Gemoderniseerd Verdrag 108 verduidelijkt dat de informatie die aan de betrokkenen wordt verstrekt, "toegankelijk, begrijpelijk, verstaanbaar en aangepast aan de relevante betrokkenen moet zijn"[526].

In het kader van het Unierecht vereist het transparantiebeginsel dat alle verwerkingen van persoonsgegevens in de regel transparant moeten zijn voor individuen. Individuen hebben het recht te weten hoe en welke persoonsgegevens worden verzameld, gebruikt of anderszins verwerkt, alsook te worden gewezen op de risico's, waarborgen en hun rechten met betrekking tot de verwerking[527]. Artikel 12 van de AVG stelt op die manier een brede volledige verplichting in voor

526 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 68.

527 Algemene verordening gegevensbescherming, overweging 39.

verwerkingsverantwoordelijken om transparante informatie te verstrekken en/of om te communiceren over hoe betrokkenen hun rechten kunnen laten gelden[528]. De informatie moet beknopt, transparant, begrijpelijk en gemakkelijk toegankelijk zijn, in duidelijke en eenvoudige taal. Ze moet worden verstrekt in schriftelijke vorm, ook in voorkomend geval elektronisch, en kan zelfs mondeling worden verstrekt op verzoek van de betrokkene en indien zijn/haar identiteit onomstotelijk bewezen is. De informatie zal worden verstrekt zonder bovenmatige vertraging of buitensporige uitgave[529].

Artikel 13 en artikel 14 van de AVG behandelen het recht van betrokkenen om te worden geïnformeerd, hetzij in situaties waarin persoonsgegevens rechtstreeks via hen werden verzameld of in situaties waarin de gegevens niet via hen werden verkregen.

Het toepassingsgebied van het recht op informatie en de beperkingen ervan in het kader van het Unierecht zijn verduidelijkt in de rechtspraak van het HvJ-EU.

Voorbeeld: In *Institut professionnel des agents immobiliers (IPI)/Englebert*[530] moest het HvJ-EU artikel 13, lid 1, van Richtlijn 95/46/EG interpreteren. Dit artikel gaf lidstaten de keuze om al dan niet wettelijke maatregelen te treffen om het toepassingsgebied te beperken van het recht om geïnformeerd te worden waar nodig teneinde, onder andere, de rechten en vrijheden van anderen te beschermen en om strafbare feiten of ethische inbreuken voor gereglementeerde beroepen te voorkomen. IPI is een beroepsvereniging van vastgoedmakelaars in België die verantwoordelijk is voor de naleving van de goede uitoefening van het beroep van makelaar. Zij vroeg een nationale rechterlijke instantie te verklaren dat de verweerders beroepsregels hadden geschonden en hun te gelasten om diverse makelaarsactiviteiten stop te zetten. De actie was gebaseerd op bewijsmateriaal van privédetectives die IPI had gebruikt.

528 *Ibid.*, artikelen 13 en 14; Gemoderniseerd Verdrag 108, artikel 8, lid 1, onder b).

529 Algemene verordening gegevensbescherming, artikel 12, lid 5; Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder b).

530 HvJ-EU, zaak C-473/12, *Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert e.a.*, 7 november 2013.

De nationale rechterlijke instantie had twijfels over de waarde van het bewijsmateriaal van de detectives, aangezien de mogelijkheid bestond dat het was verkregen zonder de vereisten inzake gegevensbescherming van de Belgische wetgeving na te leven, met name de verplichting om betrokkenen te informeren over de verwerking van hun persoonsgegevens voor het verzamelen van die informatie. Het HvJ-EU merkte op dat artikel 13, lid 1, bepaalt dat lidstaten in hun nationale recht uitzonderingen "kunnen", maar niet moeten, voorzien op de verplichting tot het informeren van betrokkenen over de verwerking van hun gegevens. Aangezien artikel 13, lid 1, het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of ethische inbreuken omvat als gronden waarop lidstaten de rechten van individuen kunnen beperken, kon de activiteit van een orgaan zoals de IPI en de privédetectives die in zijn naam optreden, zich op die bepaling beroepen. Indien een lidstaat echter niet voorziet in een dergelijke uitzondering, moeten de betrokkenen geïnformeerd worden.

Voorbeeld: In *Smaranda Bara e.a./Casa Națională de Asigurări de Sănătate e.a.*[531] verduidelijkte het HvJ-EU of het Unierecht een nationaal openbaar administratief orgaan verbiedt om persoonsgegevens aan een ander openbaar administratief orgaan over te dragen voor verdere verwerking, zonder de betrokkenen over die overdracht en verwerking te informeren. In die zaak had het Nationale Agentschap voor Administratie vóór de overdracht de aanvrager niet geïnformeerd over de doorgifte van hun gegevens aan het nationale ziekteverzekeringsfonds.

Het HvJ-EU oordeelde dat de verplichting uit hoofde van het Unierecht om de betrokkenen te informeren over de verwerking van hun persoonsgegevens "immers een noodzakelijke voorwaarde [is] voor de uitoefening voor die betrokkenen van het recht van toegang tot en rectificatie van de verwerkte gegevens [...] en van hun recht tot verzet tegen de verwerking van die gegevens". Het beginsel van eerlijke verwerking vereist de betrokkenen te informeren over de overdracht van hun gegevens aan een andere overheidsinstantie voor verdere verwerking. Overeenkomstig artikel 13, lid 1, van Richtlijn 95/46/EG kunnen lidstaten het recht om geïnformeerd te worden beperken indien dit nodig wordt geacht om een belangrijk economisch belang van de staat te beschermen, met inbegrip van fiscale

531 HvJ-EU, zaak C-201/14, *Smaranda Bara e.a./Casa Națională de Asigurări de Sănătate e.a.*, 1 oktober 2015.

aangelegenheden. Dergelijke beperkingen moeten echter worden opgelegd door wettelijke maatregelen. Aangezien noch de definitie van de gegevens die moesten worden overgedragen, noch de gedetailleerde regelingen voor de overdracht waren vastgelegd in een wetgevende maatregel, maar uitsluitend in een protocol tussen de twee overheidsdiensten, werd er niet voldaan aan de uitzonderingsvoorwaarden in het kader van het Unierecht. De aanvragers hadden van tevoren moeten worden geïnformeerd over de overdracht van hun gegevens aan het nationale ziekteverzekeringsfonds en verdere verwerking van deze gegevens door de instelling.

Inhoud van de informatie

Op grond van artikel 8, lid 1, van het Gemoderniseerd Verdrag 108, is de verwerkingsverantwoordelijke verplicht om de betrokkene alle informatie te geven die de eerlijke en transparante verwerking van persoonsgegevens garandeert, met inbegrip van:

- de identiteit en gewone verblijfsplaats of vestiging van de verwerkingsverantwoordelijke;
- de rechtsgrondslag en de doeleinden van de beoogde verwerking;
- de categorieën van verwerkte persoonsgegevens;
- in voorkomend geval, de ontvangers of categorieën ontvangers van de persoonsgegevens;
- de wijze waarop betrokkenen hun rechten kunnen uitoefenen.

Wanneer in het kader van de AVG persoonsgegevens van een betrokkene worden verzameld, is de verwerkingsverantwoordelijke verplicht om de volgende informatie aan de betrokkene te verstrekken op het moment dat de persoonsgegevens worden verkregen[532]:

- de identiteit en contactgegevens van de verwerkingsverantwoordelijke, met inbegrip van de gegevens van de DPO, indien van toepassing;

532 Algemene verordening gegevensbescherming, artikel 13, lid 1; Gemoderniseerd Verdrag 108, artikel 7 bis, lid 1.

- het doeleinde van en de rechtsgrondslag voor de verwerking, dat wil zeggen, een contract of een wettelijke verplichting;
- de rechtmatige belangen van de verwerkingsverantwoordelijke, indien deze de basis vormen voor de verwerking;
- de uiteindelijke ontvangers of categorieën ontvangers van de persoonsgegevens;
- de vraag of de gegevens zullen worden overgedragen aan een derde land of een internationale organisatie, en of deze is gebaseerd op een adequaatheidsbesluit of steunt op passende waarborgen;
- de periode waarvoor de persoonsgegevens worden opgeslagen, en indien de vaststelling van die termijn niet mogelijk is, de criteria om die termijn te bepalen;
- de rechten van betrokkenen met betrekking tot de verwerking, zoals het recht op toegang, rectificatie, uitwissing en om de verwerking te beperken of om er bezwaar tegen te maken;
- de vraag of de verstrekking van persoonsgegevens is vereist bij wet of contract, of de betrokkene is verplicht om zijn/haar persoonsgegevens te geven, evenals de gevolgen in geval van niet-verlening van de persoonsgegevens;
- het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering;
- het recht om een klacht in te dienen bij een toezichthoudende autoriteit;
- het bestaan van het recht om toestemming in te trekken.

In geval van automatische besluitvorming, met inbegrip van profilering, moeten de betrokkenen betekenisvolle informatie ontvangen over de logica van de profilering, de betekenis ervan en de gevolgen waaraan zij zich blootstellen door de verwerking.

In gevallen waarin de persoonsgegevens niet rechtstreeks van de betrokkene zijn verkregen, moet de verwerkingsverantwoordelijke het individu op de hoogte brengen van de oorsprong van de persoonsgegevens. In ieder geval moet de verwerkingsverantwoordelijke, onder meer, betrokkenen informeren over het bestaan van

geautomatiseerde besluitvorming, met inbegrip van profilering[533]. Tot slot, indien de verwerkingsverantwoordelijke persoonsgegevens wenst te verwerken voor een ander doeleinde dan oorspronkelijk opgegeven aan de betrokkene, vereisen de beginselen van doelbeperking en transparantie dat de verwerkingsverantwoordelijke de betrokkene informatie verstrekt over dit nieuwe doeleinde. Verwerkingsverantwoordelijken moeten informatie verstrekken vóór verdere verwerking. Met andere woorden, wanneer de betrokkene toestemming heeft gegeven voor de verwerking van persoonsgegevens, moet de verwerkingsverantwoordelijke de vernieuwde toestemming van de betrokkene ontvangen indien het doeleinde van de gegevensverwerking verandert of indien andere doeleinden worden toegevoegd.

Moment van de informatieverstrekking

De AVG maakt onderscheid tussen twee scenario's en twee tijdstippen waarop de verwerkingsverantwoordelijke informatie moet verstrekken aan de betrokkene:

- Wanneer persoonsgegevens rechtstreeks van de betrokkene worden verkregen, moet de verwerkingsverantwoordelijke de betrokkene in kennis stellen van alle verwante informatie over hem/haar en zijn/haar rechten in het kader van de AGV op het moment dat de persoonsgegevens worden verkregen[534].

  Indien de verwerkingsverantwoordelijke de persoonsgegevens verder wil verwerken voor een ander doeleinde, zal de verwerkingsverantwoordelijke alle relevante informatie verstrekken vóór de verwerking plaatsvindt.

- Indien de persoonsgegevens niet rechtstreeks werden verkregen van de betrokkene, moet de verwerkingsverantwoordelijke de informatie over de verwerking aan de betrokkene "binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens" verstrekken of vooraleer gegevens aan derden bekend worden gemaakt[535].

De memorie van toelichting bij Gemoderniseerd Verdrag 108 bepaalt dat, indien de inkennisstelling van betrokkenen niet mogelijk is bij het begin van de verwerking,

533 Algemene verordening gegevensbescherming, artikel 13, lid 2, en artikel 14, lid 2, onder f).

534 *Ibid.*, artikel 13, leden 1 en 2, inleidende formule waarin de algemene verordening gegevensbescherming wijst op de informatie die verplicht moet worden verstrekt "op het moment dat de persoonsgegevens worden verkregen".

535 *Ibid.*, artikel 13, lid 3, en artikel 14, lid 3; zie ook de verwijzing naar redelijke tussenpozen en zonder bovenmatige vertraging onder het Gemoderniseerd Verdrag 108, artikel 8, lid 1, onder b).

dit in een later stadium kan gebeuren, zoals wanneer de verwerkingsverantwoordelijke contact opneemt met de betrokkene om welke reden ook[536].

Verschillende manieren om informatie te verstrekken

In het kader van zowel het recht van de Raad van Europa als het Unierecht moet de informatie die de verwerkingsverantwoordelijke aan betrokkenen moet verstrekken, beknopt, transparant, begrijpelijk en gemakkelijk toegankelijk zijn. Hij moet schriftelijk worden verstrekt, of op een andere wijze, met inbegrip van elektronische middelen, in duidelijke, eenvoudige en begrijpelijke taal. Bij het verstrekken van informatie kan de verwerkingsverantwoordelijke gestandaardiseerde iconen gebruiken om de informatie op een duidelijk zichtbare en begrijpelijke wijze te verstrekken[537]. Zo kan een icoon dat een slot voorstelt worden gebruikt om aan te geven dat de gegevens veilig worden verzameld en/of versleuteld. De betrokkenen kunnen verzoeken om de informatie mondeling te verkrijgen. Informatie moet gratis worden verstrekt, tenzij de verzoeken van de betrokkenen duidelijk ongegrond of buitensporig (d.w.z. van repetitieve aard) zijn[538]. Gemakkelijk toegang tot de verstrekte informatie is van essentieel belang voor de betrokkene om zijn/haar rechten uit hoofde van de EU-wetgeving inzake gegevensbescherming uit te oefenen.

Het beginsel van eerlijke verwerking vereist dat informatie gemakkelijk te begrijpen is voor de betrokkenen. Het taalgebruik moet passend zijn voor de geadresseerden. Het niveau van het taalgebruik en het type taalgebruik zullen anders moeten zijn naar gelang het beoogde publiek bestaat uit, bijvoorbeeld, een volwassene of een kind, het algemene publiek of een academische expert. De vraag hoe aan dit aspect van verstaanbare informatie kan worden tegemoet gekomen, komt aan bod in het advies van Groep artikel 29 over meer geharmoniseerde informatiebepalingen. Het bevordert het idee van zogenaamde gelaagde verklaringen[539], die de betrokkene in staat stelt te beslissen welke mate van detaillering hij/zij verkiest. Deze manier om informatie weer te geven ontslaat de verwerkingsverantwoordelijke evenwel niet van zijn verplichting onder artikel 13 en artikel 14 van de AVG. De

536 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 70.

537 De Europese Commissie zal de informatie die de iconen dienen weer te geven en via welke procedures de gestandaardiseerde iconen tot stand dienen te komen, verder uitwerken door middel van gedelegeerde handelingen; zie algemene verordening gegevensbescherming, artikel 12, lid 8.

538 Algemene verordening gegevensbescherming, artikel 12, leden 1, 5 en 7, en Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder b).

539 Groep artikel 29 (2004), *Advies 10/2004 over meer geharmoniseerde informatiebepalingen*, WP 100, Brussel, 25 november 2004.

verwerkingsverantwoordelijke dient nog steeds alle informatie aan de betrokkene te verstrekken.

Een van de meest efficiënte manieren om informatie te verstrekken is om passende informatiebepalingen te publiceren op de homepage van de verwerkingsverantwoordelijke, zoals een privacyverklaring. Een significant deel van de bevolking maakt evenwel geen gebruik van internet, en in het informatiebeleid van een onderneming of een overheidsautoriteit zou hiermee rekening moeten worden gehouden.

Een privacyverklaring over de verwerking van persoonsgegevens op een website kan er als volgt uitzien:

Wie zijn wij?

De verwerkingsverantwoordelijke van de gegevensverwerking is Bed&Breakfast C&U, met vestiging in [Adres: xxx], Tel: xxx; Fax: xxx; E-mailadres op info@c&u.com; De contactgegevens van de Functionaris voor gegevensbescherming: [xxx].

De bekendmaking van persoonsgegevens maakt deel uit van de algemene voorwaarden die van toepassing zijn op onze hotelservices.

Welke gegevens verzamelen wij van u?

Wij verzamelen de volgende gegevens met betrekking tot u: uw naam, adres, telefoonnummer, e-mailadres, informatie over uw verblijf, het nummer van uw creditcard en debetkaart en de IP-adressen of domeinnamen van de computers waarmee u zich met onze website hebt verbonden.

Waarom verzamelen wij uw gegevens?

Wij verwerken uw gegevens op basis van uw instemming en met het oog op de uitvoering van reserveringen, het sluiten en de uitvoering van contracten in verband met de diensten die we u aanbieden en de naleving van de bij wet opgelegde vereisten, bijvoorbeeld betreffende de lokale belastingen, waardoor wij verplicht zijn om persoonsgegevens te verzamelen teneinde betaling van de toeristenbelasting voor accommodatie mogelijk te maken.

Hoe verwerken wij uw gegevens?

Uw persoonsgegevens worden opgeslagen gedurende drie maanden. Uw gegevens zijn niet onderworpen aan automatische besluitvormingsprocedures.

Onze Bed&Breakfast C&U volgt strenge beveiligingsprocedures om ervoor te zorgen dat uw persoonlijke gegevens niet worden beschadigd, vernietigd of aan een derde partij worden bekendgemaakt, tenzij u toestemming hiervoor verleent, en om onbevoegde toegang tot uw gegevens te voorkomen. De computers die de informatie opslaan worden bewaard in een beveiligde plaats met beperkte fysieke toegang. We gebruiken veilige firewalls en andere maatregelen om elektronische toegang te beperken. Indien de gegevens moeten worden overgedragen aan een derde partij, moet zij beschikken over vergelijkbare maatregelen om uw persoonsgegevens te beschermen.

Alle informatie die wij verzamelen of opnemen is beperkt tot onze kantoren. Alleen personen die de informatie nodig hebben om hun taak uit te voeren uit hoofde van dit contract, krijgen toegang tot persoonsgegevens. Wij zullen u uitdrukkelijk vragen wanneer we informatie nodig hebben om u te identificeren. We kunnen u vragen om deel te nemen aan veiligheidscontroles vóór we informatie aan u verstrekken. U kunt de persoonlijke informatie die u ons geeft op elk moment bijwerken door rechtstreeks contact op te nemen.

Wat zijn uw rechten?

U hebt het recht om toegang te krijgen tot uw gegevens, een kopie van uw gegevens te verkrijgen, hun uitwissing of rectificatie te vragen of uw gegevens over te dragen naar een andere verwerkingsverantwoordelijke.

U kunt contact met ons opnemen op info@c&u.com met uw verzoeken. Wij moeten uw verzoek binnen één maand beantwoorden, maar indien uw verzoek te ingewikkeld is of indien we te veel verzoeken ontvangen, zullen we u informeren dat deze periode kan worden verlengd met nog eens twee maanden.

Toegang krijgen tot uw persoonsgegevens

U hebt het recht op toegang tot uw gegevens, om op verzoek uitleg te krijgen over de motivering van de gegevensverwerking, om hun uitwissing of rectificatie te verzoeken en het recht om niet te worden onderworpen aan een uitsluitend geautomatiseerd besluit zonder dat er rekening wordt gehouden met uw standpunten. U kunt contact met ons opnemen op info@c&u.com met uw verzoeken. U heeft ook recht van bezwaar tegen de verwerking, het recht om uw toestemming in te trekken en een klacht in te dienen bij de nationale toezichthoudende autoriteit indien u van mening bent dat deze gegevensverwerking in strijd is met de wetgeving, en om een eis tot schadevergoeding in te dienen voor de schade die u hebt opgelopen als gevolg van de onrechtmatige verwerking.

Het recht om een klacht in te dienen

De AVG bepaalt dat de verwerkingsverantwoordelijke de betrokkenen informeert over de handhavingsmechanismen in het kader van het nationale recht en het Unierecht voor gevallen van inbreuken op persoonsgegevens. De verwerkingsverantwoordelijke moet de betrokkenen informeren over hun recht om een klacht in te dienen over een inbreuk op persoonsgegevens bij een toezichthoudende autoriteit en, indien nodig, bij een nationale rechterlijke instantie[540]. Het recht van de RvE omvat ook het recht van betrokkenen om geïnformeerd te worden over de manier waarop zij hun rechten kunnen uitoefenen, inclusief het recht op een doeltreffende corrigerende maatregel zoals vastgelegd in artikel 9, lid 1, onder f).

Uitzonderingen op de informatieverplichting

De AVG voorziet in uitzonderingen op de informatieverplichting. Onder artikel 13, lid 4, en artikel 14, lid 5, van de AVG is de verplichting om betrokkenen te informeren niet van toepassing indien de betrokkene reeds over de relevante informatie beschikt[541]. Daarbij, indien de persoonsgegevens niet werden verkregen van de betrokkene, is de informatieplicht niet van toepassing indien de verstrekking van informatie onmogelijk of onevenredig is, met name wanneer de persoonsgegevens worden verwerkt voor archiveringsdoeleinden in het algemeen belang,

540 Algemene verordening gegevensbescherming, artikel 13, lid 2, onder d), en artikel 14, lid 2, onder e); Gemoderniseerd Verdrag 108, artikel 8, lid 1, onder f).

541 *Ibid.*, artikel 13, lid 4, en artikel 14, lid 5, onder a).

voor wetenschappelijke of historische onderzoeksdoeleinden of voor statistische doeleinden[542].

Voorts beschikken lidstaten over een beoordelingsmarge in het kader van de AVG om verplichtingen en rechten verleend aan individuen, te beperken in het kader van de verordening indien dit een noodzakelijke en evenredige maatregel is in een democratische samenleving, bijvoorbeeld ter vrijwaring van de nationale en de openbare veiligheid, defensie, de bescherming van gerechtelijke onderzoeken en procedures of de bescherming van economische en financiële belangen, alsmede van particuliere belangen die dwingender zijn dan de belangen van de gegevensbescherming[543].

Uitzonderingen of beperkingen moeten noodzakelijk zijn in een democratische samenleving en moeten evenredig zijn aan het nagestreefde doel. In zeer uitzonderlijke gevallen, bijvoorbeeld wegens medische indicaties, kan de bescherming van de betrokkene zelf een beperking van de transparantie vereisen; dit betreft met name de beperking van het recht op toegang van elke betrokkene[544]. Als minimale bescherming moet de nationale wetgeving de essentie van de grondrechten en fundamentele vrijheden die krachtens het Unierecht beschermd zijn, evenwel respecteren[545]. Dit betekent dat de nationale wetgeving in specifieke bepalingen moet voorzien die het doeleinde van de verwerking, de categorieën persoonsgegevens, de waarborgen en andere procedurele vereisten verduidelijken[546].

Wanneer gegevens worden verzameld voor wetenschappelijke of historische onderzoeksdoeleinden, statistische doeleinden of archiveringsdoeleinden in het algemeen belang, kan het Unierecht of het nationale recht van de lidstaten voorzien in derogaties van de informatieverplichting indien zij de verwezenlijking van specifieke doeleinden onmogelijk zou maken of ernstig zou belemmeren[547].

Het recht van de RvE kent vergelijkbare beperkingen, waar de rechten die zijn toegekend aan betrokkenen onder artikel 9 van Gemoderniseerd Verdrag 108 onder strikte voorwaarden aan mogelijke beperkingen onderhevig kunnen zijn op

542 *Ibid.*, artikel 14, lid 5, onder b)-e).

543 Algemene verordening gegevensbescherming, artikel 15, lid 4.

544 Algemene verordening gegevensbescherming, artikel 15.

545 Algemene verordening gegevensbescherming, artikel 23, lid 1.

546 *Ibid.*, artikel 23, lid 2.

547 *Ibid.*, artikel 89, leden 2 en 3.

grond van artikel 11 van Gemoderniseerd Verdrag 108. Daarnaast geldt de verplichting tot transparantie van gegevensverwerking die aan verwerkingsverantwoordelijken wordt opgelegd onder artikel 8, lid 2, van Gemoderniseerd Verdrag 108 niet als de betrokkene de informatie al heeft.

Recht op toegang tot eigen persoonsgegevens

In het kader van het recht van de Raad van Europa is het recht op toegang tot de eigen persoonsgegevens expliciet erkend in artikel 9 van het Gemoderniseerd Verdrag 108. Dit bepaalt dat elk individu het recht heeft om, op verzoek, informatie te krijgen over de verwerking van zijn of haar persoonsgegevens die op een begrijpelijke manier worden meegedeeld. Het recht op toegang is erkend, niet alleen in de bepalingen van het Gemoderniseerd Verdrag 108, maar ook in de rechtspraak van de EHRM. De EHRM heeft herhaaldelijk geoordeeld dat individuen recht hebben op toegang tot informatie over hun persoonsgegevens en dat dit recht voortvloeit uit de noodzaak om de persoonlijke levenssfeer te eerbiedigen[548]. Het recht op toegang tot persoonsgegevens die zijn opgeslagen door openbare of particuliere organisaties mag in bepaalde gevallen evenwel worden beperkt[549].

In het kader van het Unierecht is het recht op toegang tot eigen gegevens expliciet erkend in artikel 15 van de AVG en vormt het ook een element van het grondrecht op bescherming van persoonsgegevens in artikel 8, lid 2, van het EU-Handvest van grondrechten[550]. Het recht van een individu om toegang te krijgen tot zijn/haar eigen persoonsgegevens vormt een essentieel element van de Europese wetgeving inzake gegevensbescherming[551].

De AVG bepaalt dat elke betrokkene het recht heeft op toegang tot zijn/haar persoonsgegevens en tot bepaalde informatie over de verwerking die verwerkingsverantwoordelijken moeten verlenen en verstrekken[552]. Elke betrokkene heeft met

548 EHRM, *Gaskin/Verenigd Koninkrijk*, nr. 10454/83, 7 juli 1989; EHRM, *Odièvre/Frankrijk* [Grote kamer], nr. 42326/98, 13 februari 2003; EHRM, *K.H. e.a./Slowakije*, nr. 32881/04, 28 april 2009; EHRM, *Godelli/Italië*, nr. 33783/09, 25 september 2012.

549 EHRM, *Leander/Zweden*, nr. 9248/81, 26 maart 1987.

550 Zie ook HvJ-EU in de gevoegde zaken C-141/12 en C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel* en *Minister voor Immigratie, Integratie en Asiel/M en S*, 17 juli 2014; HvJ-EU, zaak C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Europese Autoriteit voor voedselveiligheid (EFSA), Europese Commissie*, 16 juli 2015.

551 HvJ-EU in de gevoegde zaken C-141/12 en C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel* en *Minister voor Immigratie, Integratie en Asiel/M en S*, 17 juli 2014.

552 Algemene verordening gegevensbescherming, artikel 15, lid 1.

name het recht om (van de verwerkingsverantwoordelijke) bevestiging te krijgen of gegevens over hem/haar worden verwerkt, en informatie over minstens het volgende:

- verwerkingsdoeleinden;
- betrokken gegevenscategorieën;
- ontvangers of categorieën ontvangers aan wie de gegevens worden verstrekt;
- periode gedurende welke het de bedoeling is dat de persoonsgegevens worden opgeslagen, of, indien dit niet mogelijk is, de criteria voor het bepalen van die periode;
- bestaan van rechten om persoonsgegevens te rectificeren of te wissen of om de verwerking van persoonsgegevens te beperken;
- recht om een klacht in te dienen bij de toezichthoudende autoriteit;
- alle beschikbare informatie over de bron van de gegevens die verwerking ondergaan indien de gegevens niet worden verzameld bij de betrokkene;
- in geval van geautomatiseerde besluiten, de logica die aan de grondslag ligt van de geautomatiseerde gegevensverwerking.

De verwerkingsverantwoordelijke moet de betrokkene een kopie verstrekken van de persoonsgegevens die worden verwerkt. Elke inlichting die aan de betrokkene wordt meegedeeld, moet worden verstrekt in een begrijpelijke vorm, wat betekent dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de betrokkene de verstrekte informatie kan begrijpen. Gecodeerde termen of acroniemen bijvoorbeeld, met inbegrip van technische termen, naar aanleiding van een verzoek om toegang, zullen meestal niet volstaan, tenzij de betekenis van deze termen wordt uitgelegd. Wanneer geautomatiseerde beslissingen worden verricht, met inbegrip van profilering, zal de algemene logica van het geautomatiseerde beslissingsproces moeten worden uitgelegd, met inbegrip van de specifieke criteria die zijn toegepast bij het evalueren van de betrokkene. Soortgelijke voorschriften gelden krachtens **het recht van de Raad van Europa**[553].

553 Zie Gemoderniseerd Verdrag 108, artikel 8, lid 1, onder c).

Voorbeeld: De toegang tot zijn/haar persoonlijke gegevens zullen de betrokkene in staat stellen om te bepalen of de gegevens accuraat zijn. Het is daarom van essentieel belang dat de betrokkene op een begrijpelijke manier in kennis wordt gesteld, niet enkel van de persoonsgegevens die worden verwerkt, maar ook van de categorieën waaronder deze persoonsgegevens worden verwerkt, zoals de naam, het IP-adres, de geolocalisatiecoördinaten, creditcardnummer enz.

Informatie over de bron van de gegevens, wanneer de gegevens niet bij de betrokkene worden verzameld, moet na een verzoek om toegang worden verstrekt voor zover deze informatie beschikbaar is. Deze bepaling moet worden begrepen in de context van de beginselen van eerlijkheid, transparantie en verantwoording. Een verwerkingsverantwoordelijke mag geen informatie vernietigen over de gegevensbron om te worden vrijgesteld van de bekendmaking ervan, tenzij de verwijdering zou hebben plaatsgevonden ongeacht het verzoek om toegang te hebben gekregen, en de vereisten inzake de algemene verantwoordingsplicht moeten nog steeds worden nageleefd.

Zoals uiteengezet in de rechtspraak van het HvJ-EU mag het recht op toegang tot persoonsgegevens niet onnodig worden beperkt door tijdslimieten. De betrokkenen moeten ook een redelijke kans krijgen om informatie over gegevensverwerkingsoperaties die in het verleden plaatsvonden, te verkrijgen.

Voorbeeld: In de zaak *Rijkeboer*[554] werd het HvJ-EU gevraagd om te bepalen of het recht van een natuurlijke persoon op toegang tot informatie over de ontvangers of categorieën ontvangers van persoonsgegevens en over de inhoud van de gegevens kan worden beperkt tot een jaar voorafgaand aan zijn/haar verzoek om toegang.

Om te bepalen of het Unierecht de vaststelling van een dergelijke limiet toestaat, besloot het HvJ-EU om artikel 12 uit te leggen in het licht van de doeleinden van de richtlijn. Het HvJ-EU merkte in de eerste plaats op dat het recht op toegang noodzakelijk is om de betrokkene in staat te stellen het recht uit te oefenen om de verwerkingsverantwoordelijke zijn/haar gegevens te laten rectificeren, uitwissen of afschermen of om aan derden aan wie de

554 HvJ-EU, zaak C-553/07, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, 7 mei 2009.

gegevens zijn verstrekt mee te delen dat de gegevens zijn gerectificeerd, uitgewist of afgeschermd. Een daadwerkelijk recht op toegang is ook nodig om de betrokkene in staat te stellen om zijn/haar recht op bezwaar tegen de verwerking van zijn/haar persoonsgegevens of op het recht om een klacht in te dienen en schadevergoeding te vorderen, uit te oefenen[555].

Om de praktische gevolgen van de hierboven genoemde rechten van de betrokkenen te waarborgen, oordeelde het HvJ-EU dat "dit recht noodzakelijkerwijs voor het verleden moet gelden. Anders zou de betrokkene zijn recht om gegevens waarvan hij vermoedt dat zij onrechtmatig of onjuist zijn, te laten rectificeren, uitwissen of afschermen, en om zich met het oog op vergoeding van de geleden schade tot de rechter te wenden, niet doeltreffend kunnen uitoefenen".

6.1.2. Recht op rectificatie

In het kader van het Unierecht en **het recht van de Raad van Europa** hebben betrokkenen het recht om hun persoonsgegevens te rectificeren. De juistheid van persoonsgegevens is van essentieel belang om een hoog niveau van gegevensbescherming voor betrokkenen te garanderen[556].

Voorbeeld: In *Ciubotaru/Moldavië*[557] was het de verzoeker niet gelukt om de registratie van zijn etnische afkomst in officiële registers te wijzigen van Moldavisch naar Roemeens, omdat hij zou hebben nagelaten zijn verzoek te motiveren. Het EHRM achtte het aanvaardbaar dat staten objectief bewijs konden verlangen alvorens iemands etnische identiteit te registreren. Als een dergelijke claim was gebaseerd op zuiver subjectieve en niet-onderbouwde gronden, konden de autoriteiten de registratie weigeren. De claim van de indiener was evenwel gebaseerd op meer dan de subjectieve perceptie van zijn eigen etniciteit; Hij had objectief controleerbare banden met de Roemeense etnische groep kunnen aantonen, zoals de taal, naam, empathie en andere banden. Het nationale recht vereiste echter bewijs van de verzoeker dat zijn ouders tot de Roemeense etnische groep hadden behoord.

555 Algemene verordening gegevensbescherming, artikel 15, lid 1, onder c) en f), artikel 16, artikel 17, lid 2, en artikel 21, en hoofdstuk VIII.

556 *Ibid.*, artikel 16 en overweging 65; Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder e).

557 EHRM, *Ciubotaru/Moldavië*, nr. 27138/04, 27 april 2010, punten 51 en 59.

Gezien de historische realiteiten van Moldavië had deze vereiste een onneembaar obstakel gecreëerd voor de registratie van een andere etnische identiteit dan die welke door de Sovjetautoriteiten was geregistreerd in verband met zijn ouders. Door te voorkomen dat de claim van de verzoeker werd getoetst aan objectief verifieerbaar bewijs, had de staat verzuimd te voldoen aan zijn positieve verplichting om de effectieve eerbiediging van het privéleven van de verzoeker te waarborgen. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

In bepaalde gevallen zal het voor de betrokkene volstaan om de rectificatie van bijvoorbeeld de spelling van een naam, een adres of een telefoonnummer te verzoeken. Volgens het **Unierecht** en **het recht van de Raad van Europa** moeten onjuiste persoonsgegevens worden gecorrigeerd zonder onnodige of buitensporige vertraging[558]. Als dergelijke verzoeken echter verband houden met wettelijk belangrijke aangelegenheden, zoals de wettelijke identiteit van de betrokkene of de juiste verblijfplaats voor de bezorging van documenten, zijn verzoeken tot rectificatie mogelijk niet voldoende en kan de verwerkingsverantwoordelijke het recht hebben om naar bewijs van de vermeende onjuistheid te vragen. Dergelijke verzoeken mogen geen onredelijke bewijslast voor de betrokkene vormen en het daarom voor de betrokkene onmogelijk maken om zijn/haar gegevens te laten rectificeren. Het EHRM heeft in verschillende zaken waarin de verzoeker of verzoekster niet in staat was de juistheid van in geheime registers bewaarde informatie te betwisten, inbreuken op artikel 8 van het EVRM vastgesteld[559].

Voorbeeld: In *Cemalettin Canli/Turkije*[560] oordeelde het EHRM dat artikel 8 van het EVRM was geschonden als gevolg van onjuiste rapportage door de politie in een strafrechtelijke procedure.

De verzoeker was tweemaal betrokken geweest bij een strafrechtelijke procedure wegens vermeend lidmaatschap van illegale organisaties, maar was nooit veroordeeld. Toen de verzoeker opnieuw werd aangehouden en een ander strafbaar feit ten laste werd gelegd, verstrekte de politie de rechtbank die de strafzaak behandelde een rapport getiteld "*Informatie*

558 Algemene verordening gegevensbescherming, artikel 16; Gemoderniseerd Verdrag 108, artikel 9, lid 1.

559 EHRM, *Rotaru/Roemenië* [Grote kamer], nr. 28341/95, 4 mei 2000.

560 EHRM, *Cemalettin Canli/Turkije*, nr. 22427/04, 18 november 2008, punten 33 en 42-43; EHRM, *Dalea/Frankrijk*, nr. 964/07, 2 februari 2010.

over andere delicten", waarin de verzoeker werd genoemd als lid van twee illegale organisaties. Het verzoek van de verzoeker om kopieën van het rapport en van de politiedossiers leverde niets op. Het EHRM oordeelde dat de informatie in het verslag van de politie viel onder het toepassingsgebied van artikel 8 van het EVRM, aangezien systematisch verzamelde openbare gegevens die worden opgeslagen in bestanden die door de autoriteiten worden beheerd, ook kunnen vallen onder de definitie van "persoonlijke levenssfeer". Bovendien was de opstelling van het politierapport onjuist en was het overleggen ervan aan de rechtbank niet in overeenstemming met het nationale recht geweest. Het Hof concludeerde dat er een inbreuk op artikel 8 had plaatsgevonden.

Tijdens een civiele gerechtelijke procedure of een administratieve procedure bij een overheidsautoriteit waarin moet worden beslist of gegevens al dan niet juist zijn, kan de betrokkene verzoeken dat er een aantekening in zijn/haar dossier wordt opgenomen dat de juistheid van de gegevens wordt bestreden en dat gewacht wordt op een officiële beslissing[561]. Tijdens deze periode mag de verwerkingsverantwoordelijke de gegevens niet voorstellen als "juist" of "niet onderworpen aan wijzigingen", zeker niet ten overstaan van derden.

6.1.3. Recht op gegevenswissing ("het recht om te worden vergeten")

Betrokkenen het recht toekennen om hun eigen gegevens te laten wissen, is bijzonder belangrijk voor de doeltreffende toepassing van beginselen inzake gegevensbescherming, met name het beginsel van de gegevensminimalisering (persoonsgegevens moeten beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor die data worden verwerkt). Een recht op gegevenswissing is derhalve opgenomen in de rechtsinstrumenten van zowel de Raad van Europa als de EU[562].

Voorbeeld: In *Segerstedt-Wiberg e.a./Zweden*[563] waren de verzoekers aangesloten bij bepaalde liberale en communistische politieke partijen. Zij vermoedden dat informatie over hen in de registers van de veiligheidspolitie

561 Algemene verordening gegevensbescherming, artikel 16, tweede zin.

562 *Ibid.*, artikel 17.

563 EHRM, *Segerstedt-Wiberg e.a./Zweden*, nr. 62332/00, 6 juni 2006, punten 89 en 90; zie ook, bijvoorbeeld, EHRM, *M.K./Frankrijk*, nr. 19522/09, 18 april 2013.

terecht was gekomen en vroegen de uitwissing ervan. Het EHRM vergewiste zich ervan dat de opslag van de gegevens in kwestie een rechtsgrondslag had en een rechtmatig doel diende. Met betrekking tot enkele verzoekers oordeelde het EHRM echter dat het blijven bewaren van de gegevens een onevenredige inmenging in hun privéleven vormde. Zo hadden de autoriteiten in het geval van één verzoeker informatie bewaard die inhield dat hij in 1969 zou hebben gepleit voor gewelddadig verzet tegen de politie tijdens demonstraties. Het EHRM oordeelde dat deze informatie geen relevant belang van nationale veiligheid diende, met name gezien het historische karakter ervan. Het Hof van Justitie oordeelde dat een overtreding van artikel 8 van het EVRM had plaatsgevonden ten aanzien van vier van de vijf verzoekers aangezien, gelet op de lange tijd die was verstreken sinds de vermeende handelingen van de verzoekers, de bewaring van hun gegevens niet relevant was.

Voorbeeld: In *Brunet/Frankrijk*[564] hekelde de verzoeker de bewaring van zijn persoonlijke informatie in een gegevensbestand van de politie die informatie over veroordeelden, beklaagden en slachtoffers bevatte. Hoewel de strafrechtelijke procedure tegen de verzoeker was stopgezet, verschenen zijn gegevens in het gegevensbestand. Het EHRM concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM. In zijn conclusie oordeelde het Hof van Justitie dat het in de praktijk niet mogelijk was voor de verzoeker om zijn persoonsgegevens uit het gegevensbestand te laten verwijderen. Het EHRM nam ook de aard van de informatie in het gegevensbestand in overweging en achtte dat deze een inbreuk vormde op de privacy van de verzoeker, aangezien zij bijzonderheden over zijn identiteit en persoonlijkheid bevatte. Bovendien was het van mening dat de aanhoudperiode voor persoonlijke dossiers in het gegevensbestand, die 20 jaar bedroeg, buitensporig lang was, met name omdat geen enkel gerecht de verzoeker ooit had veroordeeld.

Het Gemoderniseerd Verdrag 108 erkent uitdrukkelijk dat elke natuurlijke persoon het recht heeft op de wissing van onjuiste, valse of onrechtmatig verwerkte gegevens[565].

564 EHRM, *Brunet/Frankrijk*, nr. 21010/10, 18 september 2014.

565 Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder e).

In het kader van het Unierecht geeft artikel 17 van de AVG uitvoering aan de verzoeken van betrokkenen om hun gegevens te laten wissen of verwijderen. Het recht om zijn/haar persoonsgegevens te laten wissen zonder onnodige vertraging, is van toepassing wanneer:

- persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- de betrokkene de toestemming waarop de verwerking is gesteund, terugtrekt en er geen andere rechtsgrond bestaat voor de verwerking;
- de betrokkene bezwaar maakt tegen de verwerking en er geen zwaarwegende rechtmatige redenen bestaan voor de verwerking;
- de persoonsgegevens onrechtmatig werden verwerkt;
- de persoonsgegevens gewist moeten worden om te voldoen aan een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- de persoonsgegevens verzameld werden in verband met het aanbod van diensten van de informatiemaatschappij aan kinderen, op grond van artikel 8 van de AVG[566].

De bewijslast voor de rechtmatigheid van de gegevensverwerking zal bij de verwerkingsverantwoordelijke liggen, aangezien deze verantwoordelijk is voor de rechtmatigheid van de verwerking[567]. Volgens het aansprakelijkheidsbeginsel moet de verwerkingsverantwoordelijke op elk moment in staat zijn om aan te tonen dat er een stevige rechtsgrond voor zijn gegevensverwerking bestaat; anders moet de verwerking worden beëindigd[568]. De AVG bepaalt uitzonderingen op het recht om te worden vergeten, ook wanneer de verwerking van persoonsgegevens nodig is voor:

- het uitoefenen van het recht op vrijheid van meningsuiting en informatie;

566 Algemene verordening gegevensbescherming, artikel 17, lid 1.

567 *Ibid.*

568 *Ibid.*, artikel 5, lid 2.

- het nakomen van een in een het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust, of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;

- overwegingen van openbaar belang op het gebied van de volksgezondheid;

- archivering in het algemeen belang, wetenschappelijke of historische doeleinden of voor statistische doeleinden;

- de instelling, uitoefening of onderbouwing van een rechtsvordering[569].

Het HvJ-EU heeft het belang bevestigd van het recht op gegevenswissing om een hoog niveau van gegevensbescherming te garanderen.

Voorbeeld: In de zaak *Google Spain*[570] onderzocht het Hof van Justitie of Google verouderde informatie over financiële problemen van de verzoeker uit de resultatenlijst moest verwijderen. Google betwistte onder andere de verantwoordelijkheid en argumenteerde dat enkel een hyperlink naar de website van de uitgever ter beschikking is gesteld die de informatie bevat, in dit geval een krantenartikel over de insolventieproblemen van de verzoeker[571]. Google voerde aan dat het verzoek tot schrapping van verouderde gegevens van een website dient te worden ingediend bij de eigenaar van de website en niet bij Google, die uitsluitend een link naar de oorspronkelijke pagina ter beschikking stelt. Het Hof van Justitie concludeerde dat Google, wanneer het net wordt doorzocht voor informatie en websites, en wanneer inhoud wordt geïndexeerd om zoekresultaten ter

569 *Ibid.*, artikel 17, lid 3.

570 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 13 mei 2014, punten 55-58.

571 Google plaatste ook vraagtekens bij de toepassing van de EU-regels inzake gegevensbescherming als gevolg van het feit dat Google Inc. gevestigd is in de VS en de verwerking van persoonsgegevens in het kader van de zaak ook in de VS werd uitgevoerd. Een tweede argument voor de niet-toepasselijkheid van de EU-wetgeving inzake gegevensbescherming hield verband met de stelling dat zoekmachines niet kunnen worden beschouwd als "verwerkingsverantwoordelijken" voor de gegevens vermeld in hun resultaten, aangezien zij geen kennis hebben over de gegevens en er evenmin controle over uitoefenen. Het Hof van Justitie wees beide argumenten af, want het stelde dat Richtlijn 95/46/EG van toepassing was in die zaak, en onderzocht verder de omvang van de rechten die werden gegarandeerd, in het bijzonder het recht op gegevenswissing.

beschikking te stellen, een verwerkingsverantwoordelijke wordt op wie de verantwoordelijkheden en verplichtingen in het kader van het Unierecht van toepassing zijn.

Het Hof van Justitie verklaarde dat via internetzoekmachines en zoekresultaten die persoonsgegevens bevatten, een gedetailleerd profiel van een natuurlijke persoon kan worden opgesteld[572]. Zoekmachines maken de informatie die in een dergelijke resultatenlijst vervat zit, alomtegenwoordig. In het licht van de potentiële ernst ervan, kan deze inmenging niet worden gerechtvaardigd door enkel het economische belang die de beheerder van een dergelijke machine heeft bij die verwerking. Een billijk evenwicht moet worden nagestreefd, met name tussen het rechtmatige belang van de internetgebruikers op toegang tot informatie en de grondrechten van de betrokkenen in het kader van de artikelen 7 en 8 van het EU-Handvest van de grondrechten. In een steeds meer gedigitaliseerde samenleving is het van fundamenteel belang dat persoonsgegevens correct zijn en niet verder gaan dan nodig is (d.w.z. voor vrij toegankelijke informatie) om een hoog niveau van gegevensbescherming van natuurlijke personen te kunnen waarborgen. De "voor deze verwerking verantwoordelijke [moet], [...] binnen het kader van zijn verantwoordelijkheden, bevoegdheden en mogelijkheden verzekeren dat deze verwerking aan de vereisten [...] voldoet" van het Unierecht, zodat de daarin vervatte wettelijke waarborgen hun volle werking kunnen krijgen[573]. Dit betekent dat het recht om zijn/haar persoonsgegevens te laten wissen wanneer de verwerking in onbruik is geraakt of niet langer noodzakelijk is, ook van toepassing is op verwerkingsverantwoordelijken die de informatie dupliceren[574].

Het onderzoek naar de vraag of Google verplicht moest worden de koppelingen met betrekking tot de verzoeker te verwijderen, bracht het HvJ-EU tot het oordeel dat natuurlijke personen onder bepaalde omstandigheden het recht hebben om te verzoeken om de verwijdering van hun persoonsgegevens. Op dit recht kan een beroep worden gedaan

572 *Ibid.*, punten 36, 38, 80-81 en 97.

573 *Ibid.*, punten 81-83.

574 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 13 mei 2014, punt 88. Zie ook Groep gegevensbescherming artikel 29 (2014), *Richtsnoeren voor de uitvoering van het HvJ-EU-arrest over "Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González", zaak C-131/12*, WP 225, Brussel, 26 november 2014 en aanbeveling CM/Rec 2012(3) van het Comité van Ministers aan de lidstaten over de bescherming van de mensenrechten ten aanzien van zoekmachines, 4 april 2012.

wanneer informatie over een natuurlijke persoon niet correct, toereikend of ter zake dienend is, of bovenmatig is, uitgaande van de doeleinden van de gegevensverwerking. Het Hof van Justitie erkende dat dit recht geen absolute gelding heeft. Het dient te worden afgewogen tegen andere rechten en belangen, met name het belang van het publiek bij toegang tot bepaalde informatie. Verzoeken om uitwissing moeten van geval tot geval worden beoordeeld, zodat een evenwicht kan worden gevonden tussen enerzijds het grondrecht op bescherming van persoonsgegevens en eerbiediging van de persoonlijke levenssfeer van de betrokkene en anderzijds de gerechtvaardigde belangen van alle internetgebruikers, uitgevers inbegrepen. Het Hof van Justitie verduidelijkte welke factoren in de afweging dienen te worden meegenomen tijdens deze evenwichtsoefening. Met name de aard van de gegevens is een belangrijke factor. Wanneer het gaat om gegevens uit de persoonlijke levenssfeer van een natuurlijke persoon en de beschikbaarheid van de informatie geen algemeen belang dient, krijgen gegevensbescherming en privacy voorrang op het recht van het publiek op toegang tot de informatie. Als daarentegen blijkt dat de betrokkene een bekend persoon is, of dat de informatie van dien aard is dat de toegang ertoe voor het publiek gerechtvaardigd is, dan kan het doorslaggevende belang van het publiek in de toegang tot de informatie de inbreuk met de grondrechten op gegevensbescherming en privacy rechtvaardigen.

Volgend op dit arrest heeft Groep artikel 29 richtsnoeren aangenomen voor de uitvoering van de uitspraak van het HvJ-EU[575]. De richtsnoeren omvatten onder meer een lijst van gemeenschappelijke criteria die toezichthoudende autoriteiten kunnen hanteren bij het afhandelen van klachten in verband met verwijderingsverzoeken van natuurlijke personen. Die criteria leggen uit wat het recht op wissing inhoudt en dienen als leidraad bij het afwegen van rechten. De richtsnoeren herhalen dat de beoordelingen per geval moeten worden gemaakt. Aangezien het recht om te worden vergeten niet absoluut is, kan het resultaat van een verzoek verschillen afhankelijk van de zaak waarover het gaat. Dit wordt geïllustreerd door de rechtspraak van het HvJ-EU na Google.

575 Groep artikel 29 (2014), *Richtsnoeren voor de uitvoering van het HvJ-EU-arrest over "Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González"*, zaak C-131/12, WP 225, Brussel, 26 november 2014.

Voorbeeld: In *Camera di Commercio di Lecce/Manni*[576] moest het HvJ-EU onderzoeken of een natuurlijke persoon het recht had op verwijdering van zijn persoonsgegevens die in een openbaar register van ondernemingen waren gepubliceerd, zodra zijn onderneming ophield te bestaan. De heer Manni had de Kamer van Koophandel van Lecce verzocht om zijn persoonsgegevens te verwijderen uit dat register, aangezien hij had ontdekt dat potentiële klanten het register consulteerden en konden zien dat hij eerder de beheerder van een bedrijf was geweest dat meer dan tien jaar geleden failliet was verklaard. De verzoeker was van mening dat deze informatie potentiële klanten zou afschrikken.

Bij het zoeken naar een evenwicht tussen het recht van de heer Manni op bescherming van zijn persoonsgegevens en het algemene belang tot toegang tot de informatie, onderzocht het HvJ-EU eerst het doel van het publieke register. Het wees op het feit dat de openbaring ervan in de wet was voorzien, met name door een EU-richtlijn die gericht is op het toegankelijker maken van informatie over vennootschappen voor derden. Derden moeten derhalve toegang hebben en in staat zijn om kennis te nemen van de voornaamste akten van een vennootschap, alsmede andere informatie over de vennootschap, "met name de identiteit van de personen die de bevoegdheid hebben haar te verbinden". Het doel van de openbaarmaking was tevens om rechtszekerheid te garanderen vanwege versterkte handel tussen lidstaten, door ervoor te zorgen dat derden toegang hebben tot alle relevante informatie over vennootschappen in de EU.

Het HvJ-EU merkte verder op dat zelfs na het verstrijken van de tijd, en ook nadat een vennootschap wordt ontbonden, de rechten en wettelijke verplichtingen met betrekking tot de vennootschap vaak blijven bestaan. Geschillen in verband met de ontbinding kunnen lang duren en vragen omtrent een vennootschap, haar beheerders en vereffenaars kunnen opduiken tot jaren nadat de vennootschap heeft opgehouden te bestaan. Het HvJ-EU oordeelde dat, gezien alle mogelijke scenario's en de uiteenlopende verjaringstermijnen in elke lidstaat, "het thans onmogelijk [lijkt] om te komen tot één vanaf de ontbinding van een vennootschap lopende termijn na het verstrijken waarvan de inschrijving in het register en openbaarmaking van de genoemde gegevens niet meer nodig zou zijn". Als gevolg van

576 HvJ-EU, zaak C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 maart 2017.

het rechtmatige doel van de openbaarmaking en de moeilijkheden bij het vaststellen van een periode waarna de persoonsgegevens uit het register kunnen worden verwijderd zonder nadelige gevolgen voor het algemeen belang van derden, vond het HvJ-EU dat de EU-regels inzake gegevensbescherming geen recht garandeerden op de verwijdering van persoonsgegevens voor personen die zich in de situatie van de heer Manni bevinden.

Wanneer de verwerkingsverantwoordelijke persoonsgegevens publiek heeft gemaakt en wordt gevraagd om de informatie te verwijderen, is de verwerkingsverantwoordelijke verplicht en moet hij "redelijke" stappen ondernemen om andere verwerkingsverantwoordelijken die dezelfde gegevens verwerken, te informeren over het verwijderingsverzoek van de betrokkene. De activiteiten van de verwerkingsverantwoordelijke moeten rekening houden met de beschikbare technologieën en de kosten van de uitvoering[577].

6.1.4. Recht op beperking van de verwerking

Artikel 18 van de AVG machtigt de betrokkenen om een verwerkingsverantwoordelijke tijdelijk een beperking van de verwerking van hun persoonsgegevens op te leggen. Betrokkenen kunnen de verwerkingsverantwoordelijke verzoeken om de verwerking te beperken wanneer:

- de juistheid van de persoonsgegevens wordt betwist;
- de verwerking onwettig is en de betrokkene verzoekt om het gebruik van de persoonsgegevens te beperken in plaats van ze te wissen;
- de gegevens moeten worden bewaard voor de uitoefening of onderbouwing van een rechtsvordering;
- een besluit hangende is over de vraag of het rechtmatige belang van de verwerkingsverantwoordelijke voorrang heeft op het belang van de betrokkene[578].

De methoden waarmee een verwerkingsverantwoordelijke de verwerking van persoonsgegevens kan beperken, omvatten, onder meer, de tijdelijke verplaatsing

577 Algemene verordening gegevensbescherming, artikel 17, lid 2, en overweging 66.

578 *Ibid.*, artikel 18, lid 1.

van de geselecteerde gegevens naar een ander verwerkingssysteem waardoor de gegevens niet beschikbaar zijn voor gebruikers of de tijdelijke verwijdering van persoonsgegevens[579]. De verwerkingsverantwoordelijke moet de betrokkene in kennis stellen voordat de beperking op verwerking wordt opgeheven[580].

Verplichting tot kennisgeving over de rectificatie of wissing van persoonsgegevens of over de beperking van de verwerking

De verwerkingsverantwoordelijke moet elke rectificatie of wissing van persoonsgegevens of elke beperking van de verwerking meedelen aan elke ontvanger aan wie de verwerkingsverantwoordelijke de persoonsgegevens openbaar maakte, voor zover dit niet onmogelijk of onevenredig is[581]. Indien de betrokkene om informatie over die ontvangers verzoekt, moet de verwerkingsverantwoordelijke hem/haar die informatie verstrekken[582].

6.1.5. Recht op gegevensportabiliteit

In het kader van de AVG hebben betrokkenen het recht op gegevensportabiliteit in situaties waarin de persoonsgegevens die zij aan een verwerkingsverantwoordelijke hebben verstrekt, worden verwerkt op geautomatiseerde wijze op basis van toestemming of waarin de verwerking van persoonsgegevens noodzakelijk is voor de uitvoering van een contract en op geautomatiseerde wijze wordt uitgevoerd. Dit betekent dat het recht op gegevensportabiliteit niet van toepassing is in situaties waar de verwerking van persoonsgegevens gebeurt op basis van een andere rechtsgrond dan toestemming of een contract[583].

Indien het recht op gegevensportabiliteit van toepassing is, hebben de betrokkenen het recht om hun persoonsgegevens rechtstreeks van één verwerkingsverantwoordelijke naar een andere te laten overdragen indien dit technisch haalbaar is[584]. Om dit te vergemakkelijken moet de verwerkingsverantwoordelijke interoperabele formaten ontwikkelen die de overdraagbaarheid van gegevens voor betrokkenen

579 *Ibid.*, overweging 67.

580 *Ibid.*, artikel 18, lid 3.

581 Ad-hoccommissie voor gegevensbescherming (CAHDATA), memorie van toelichting bij het Gemoderniseerd Verdrag voor de bescherming van personen met betrekking tot de automatische verwerking van persoonsgegevens, punt 79.

582 Algemene verordening gegevensbescherming, artikel 19.

583 *Ibid.*, overweging 68 en artikel 20, lid 1.

584 *Ibid.*, artikel 20, lid 2.

mogelijk maken[585]. De AVG bepaalt dat deze formaten gestructureerd, algemeen gebruikt en machinaal leesbaar moeten zijn om interoperabiliteit te vergemakkelijken[586]. Interoperabiliteit kan in brede zin worden omschreven als het vermogen van het informatiesysteem om gegevens uit te wisselen en het delen van informatie mogelijk te maken[587]. Hoewel het doel van de gebruikte formaten het bereiken van interoperabiliteit is, legt de AVG geen bijzondere aanbevelingen op over het specifieke formaat dat moet worden verstrekt: formaten kunnen verschillen afhankelijk van de sector[588].

Volgens de richtsnoeren van Groep artikel 29 onderschrijft het recht op gegevensportabiliteit de keuze, de controle en de beslissingsbevoegdheid van de gebruiker en heeft het als doel betrokkenen de controle over hun eigen persoonsgegevens te geven[589]. De richtsnoeren verklaren de hoofdelementen van de overdraagbaarheid van gegevens, namelijk:

- het recht van betrokkenen om hun eigen verwerkte persoonsgegevens in een gestructureerd, algemeen gebruikt, machinaal leesbaar en interoperabel formaat van de verwerkingsverantwoordelijke te ontvangen;

- het recht om zonder beperking persoonsgegevens over te dragen van de ene verwerkingsverantwoordelijke naar de andere, indien dit technisch haalbaar is;

- het regime van verwerkingsverantwoordelijkheid — wanneer een verwerkingsverantwoordelijke een verzoek tot gegevensportabiliteit beantwoordt, handelen ze op instructie van de betrokkene waardoor ze niet verantwoordelijk zijn voor de naleving van de wetgeving inzake gegevensbescherming door de ontvanger, aangezien de betrokkene beslist naar wie de gegevens worden overgedragen;

- de uitoefening van het recht op gegevensportabiliteit mag geen afbreuk doen aan andere rechten, zoals het geval is met alle andere rechten in de AVG.

585 *Ibid.*, overweging 68 en artikel 20, lid 1.

586 *Ibid.*, overweging 68.

587 Europese Commissie, Mededeling over "Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid", COM(2016) 205 def., 2 april 2016.

588 Groep artikel 29 (2016), *Richtsnoeren inzake het recht op gegevensportabiliteit*, WP 242, 13 december 2016 en herzien op 5 april 2017, blz. 13.

589 *Ibid.*

6.1.6. Recht van bezwaar

Betrokkenen kunnen zich beroepen op hun recht om bezwaar te maken tegen de verwerking van persoonsgegevens op grond van hun specifieke situatie, en tegen de verwerking van gegevens voor directmarketingdoeleinden. Het recht van bezwaar kan op geautomatiseerde wijze worden uitgeoefend.

Het recht van bezwaar om redenen die verband houden met de specifieke situatie van de betrokkenen

Betrokkenen hebben geen algemeen recht om bezwaar te maken tegen de verwerking van hun gegevens[590]. Artikel 21, lid 1, van de AVG machtigt de betrokkene om op grond van zijn specifieke situatie bezwaar aan te tekenen wanneer de rechtsgrond voor de verwerking de vervulling door de verwerkingsverantwoordelijke van een taak van algemeen belang is of wanneer de verwerking gebaseerd is op de gerechtvaardigde belangen van de verwerkingsverantwoordelijke[591]. Het recht van bezwaar is van toepassing op profileringsactiviteiten. Een soortgelijk recht is erkend in het Gemoderniseerd Verdrag 108[592].

Het recht van bezwaar om redenen die verband houden met de bijzondere situatie van de betrokkene heeft tot doel om te streven naar het juiste evenwicht tussen de rechten inzake gegevensbescherming van de betrokkene en de rechtmatige rechten van anderen bij de verwerking van hun gegevens. Het HvJ-EU heeft evenwel verklaard dat de rechten van de betrokkene in de regel voorrang hebben op de economische belangen van een verwerkingsverantwoordelijke, afhankelijk van de aard van de informatie in kwestie en de gevoeligheid ervan voor de persoonlijke levenssfeer van de betrokkene en van het algemeen belang van het bezitten van die informatie[593]. In het kader van de AVG ligt de bewijslast bij de verwerkingsverantwoordelijken die dwingende redenen moeten kunnen aantonen om de verwerking

590 Zie ook EHRM, *M.S./Zweden*, nr. 20837/92, 27 augustus 1997 [waarin medische gegevens waren meegedeeld zonder toestemming of de mogelijkheid om bezwaar te maken], EHRM, *Leander/Zweden*, nr. 9248/81, 26 maart 1987, EHRM, *Mosley/Verenigd Koninkrijk*, nr. 48009/08, 10 mei 2011.

591 Algemene verordening gegevensbescherming, overweging 69; artikel 6, lid 1, onder e) en f).

592 Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder d); Aanbeveling inzake profilering, artikel 5, lid 3.

593 HvJ-EU, zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 13 mei 2014, punt 81.

voort te zetten[594]. Ook het toelichtend verslag van het Gemoderniseerd Verdrag 108 verklaart dat men gegronde redenen voor de gegevensverwerking (die voorrang kunnen hebben op het recht van bezwaar van de betrokkene) per geval moet kunnen aantonen[595].

Voorbeeld: In *Manni*[596] oordeelde het HvJ-EU dat, wegens het rechtmatige doeleinde van de openbaarmaking van persoonsgegevens in het handelsregister, met name de noodzaak om de belangen van derden te beschermen en rechtszekerheid te waarborgen, de heer Manni niet het recht had op de wissing van zijn persoonsgegevens uit het handelsregister. Het erkende evenwel het bestaan van een recht van bezwaar tegen de verwerking, met het argument "dat [...] niet [valt uit te sluiten] dat er uitzonderlijke situaties kunnen zijn waarin zwaarwegende en gerechtvaardigde redenen die verband houden met het specifieke geval van de betrokkene, bij wijze van uitzondering rechtvaardigen dat de toegang tot de hem betreffende persoonsgegevens in het register, na verloop van een voldoende lange termijn [...] wordt beperkt tot derden die een aantoonbaar belang hebben bij inzage in die gegevens".

Het HvJ-EU achtte het de verantwoordelijkheid van de nationale rechterlijke instanties om elke zaak te beoordelen, rekening houdend met alle relevante omstandigheden van de betrokkene, en om na te gaan of er rechtmatige en dwingende redenen bestaan die, bij wijze van uitzondering, een beperkte toegang van derden tot persoonsgegevens in handelsregisters kunnen rechtvaardigen. Het verduidelijkte evenwel dat in de zaak van de heer Manni, het loutere feit dat de openbaarmaking van zijn persoonsgegevens in het register zijn klanten zou beïnvloeden, niet kan worden beschouwd als een rechtmatige en dwingende reden. Potentiële klanten van de heer Manni hebben er rechtmatig belang bij om toegang te krijgen tot de informatie over het faillissement van zijn oude vennootschap.

594 Zie ook Gemoderniseerd Verdrag 108, artikel 98, lid 1, onder d), waarin wordt verklaard dat de betrokkene bezwaar kan maken tegen de verwerking van zijn/haar gegevens, "tenzij de verwerkingsverantwoordelijke gegronde redenen aantoont voor de verwerking ervan die voorrang hebben op zijn/haar belangen of rechten en fundamentele vrijheden".

595 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 78.

596 HvJ-EU, zaak C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 maart 2017, punten 47 en 60.

Het effect van een succesvol bezwaar is dat de verwerkingsverantwoordelijke niet langer de gegevens in kwestie mag verwerken. De verwerkingen die voorafgaand aan het bezwaar tegen de gegevens van de betrokkene werden uitgevoerd, blijven evenwel rechtmatig.

Het recht van bezwaar voor de verwerking van gegevens voor directmarketingdoeleinden

Artikel 21, lid 2, van de AVG voorziet in een specifiek recht van bezwaar voor het gebruik van persoonsgegevens voor directmarketingdoeleinden, en biedt hiermee nadere toelichting bij artikel 13 van de e-Privacy-richtlijn. Dit recht is ook vastgelegd in het Gemoderniseerd Verdrag 108, alsook in de Aanbeveling over direct marketing van de RvE[597]. De memorie van toelichting bij Gemoderniseerd Verdrag 108 verklaart dat bezwaren tegen gegevensverwerking voor directmarketingdoeleinden moeten leiden tot een onvoorwaardelijke wissing of verwijdering van de persoonsgegevens in kwestie[598].

De betrokkene heeft op elk moment en kosteloos recht van bezwaar tegen het gebruik van zijn/haar persoonsgegevens voor directmarketingdoeleinden. De betrokkenen moeten op duidelijke wijze, gescheiden van alle andere informatie, worden geïnformeerd over dit recht.

Het recht van bezwaar tegen geautomatiseerde wijze

Wanneer persoonsgegevens worden gebruikt en verwerkt voor de diensten van de informatiemaatschappij, kan de betrokkene zijn/haar recht van bezwaar tegen de verwerking van zijn/haar persoonsgegevens op geautomatiseerde wijze uitoefenen.

Diensten van de informatiemaatschappij worden omschreven als elke dienst die gewoonlijk tegen vergoeding, op afstand, langs elektronische weg en op individueel verzoek van een afnemer van diensten wordt aangeboden[599].

597 RvE, Comité van Ministers (1985), Aanbeveling Rec(85)20 aan de lidstaten inzake de bescherming van persoonsgegevens die worden gebruikt met het oog op direct marketing, 25 oktober 1985, artikel 4, lid 1.

598 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 79.

599 Richtlijn 98/34/EG zoals gewijzigd bij Richtlijn 98/48/EG betreffende een informatieprocedure op het gebied van technische normen en voorschriften, artikel 1, lid 2.

Verwerkingsverantwoordelijken die diensten van de informatiemaatschappij aanbieden, moeten over passende technische maatregelen en procedures beschikken om ervoor te zorgen dat het recht van bezwaar tegen geautomatiseerde wijze daadwerkelijk kan worden uitgeoefend[600]. Het kan bijvoorbeeld gaan om het blokkeren van cookies op webpagina's of om het uitschakelen van het volgen van het browsegedrag op internet.

Het recht van bezwaar voor wetenschappelijke of historische onderzoeksdoeleinden of statistische doeleinden

In het kader van het Unierecht moet wetenschappelijk onderzoek ruim worden opgevat en bijvoorbeeld technologische ontwikkeling en demonstratie, fundamenteel onderzoek, toegepast onderzoek en uit particuliere middelen gefinancierd onderzoek omvatten[601]. Historisch onderzoek omvat ook onderzoek voor genealogische doeleinden, met dien verstande dat deze verordening niet van toepassing mag zijn op overleden personen[602]. Onder statistische doeleinden wordt verstaan het verzamelen en verwerken van persoonsgegevens die nodig zijn voor statistische onderzoeken en voor het produceren van statistische resultaten[603]. Ook de bijzondere situatie van een betrokkene vormt de rechtsgrondslag aangaande het recht van bezwaar tegen de verwerking van persoonsgegevens voor onderzoeksdoeleinden[604]. De enige uitzondering is de noodzaak van de verwerking voor de uitvoering van een taak om redenen van algemeen belang. Het recht op wissing is echter niet van toepassing wanneer de verwerking noodzakelijk is (met of zonder redenen van algemeen belang) voor wetenschappelijke of historische onderzoeksdoeleinden of statistische doeleinden[605].

De AVG weegt de vereisten van wetenschappelijk, statistisch of historisch onderzoek af tegen de rechten van betrokkenen met specifieke waarborgen en derogaties in artikel 89. Bijgevolg kan het Unierecht of het lidstatelijk recht voorzien in derogaties van het recht van bezwaar voor zover dit recht de verwezenlijking van onderzoeksdoeleinden onmogelijk maakt of er een ernstige belemmering

600 Algemene verordening gegevensbescherming, artikel 21, lid 5.

601 *Ibid.*, overweging 159.

602 *Ibid.*, overweging 160.

603 *Ibid.*, overweging 162.

604 *Ibid.*, artikel 21, lid 6.

605 *Ibid.*, artikel 17, lid 3, onder d).

voor vormt en indien deze derogaties noodzakelijk zijn voor de vervulling van die doeleinden.

In het kader van het **recht van de Raad van Europa** bepaalt artikel 9, lid 2, van het Gemoderniseerd Verdrag 108 dat beperkingen op de rechten van betrokkenen, waaronder het recht van bezwaar, bij wet voorzien kunnen worden met betrekking tot de gegevensverwerking voor archiveringsdoelstellingen in het algemeen belang, wetenschappelijke of historische onderzoeksdoeleinden of statistische doeleinden wanneer er geen herkenbaar risico is van inbreuk op de rechten en fundamentele vrijheden van de betrokkenen.

De memorie van toelichting (punt 41) erkent evenwel ook dat betrokkenen de gelegenheid moeten hebben om hun toestemming te verlenen aan slechts bepaalde onderzoeksgebieden of delen van onderzoekprojecten voor zover dat het bedoelde doeleinde dit toelaat, en bezwaar te uiten indien zij vinden dat de verwerking te veel inbreuk pleegt op hun rechten en vrijheden zonder rechtsgrondslag.

Met andere woorden, een dergelijke verwerking zou dus a priori verenigbaar zijn op voorwaarde dat er andere waarborgen bestaan en dat de activiteiten in beginsel geen gebruik maken van de verkregen informatie voor beslissingen of maatregelen met betrekking tot een bepaalde persoon.

6.1.7. Geautomatiseerde individuele besluitvorming, waaronder profilering

Geautomatiseerde besluiten zijn besluiten die worden genomen door persoonsgegevens uitsluitend met elektronische middelen te verwerken, zonder menselijke tussenkomst. **In het kader van het Unierecht** mogen betrokkenen niet worden onderworpen aan geautomatiseerde besluiten die rechtsgevolgen hebben of gelijkaardige belangrijke gevolgen. Als dergelijke besluiten een belangrijke invloed op de levens van natuurlijke personen kunnen hebben, omdat ze bijvoorbeeld verband houden met hun kredietwaardigheid, personeelwerving via internet, hun prestaties op het werk, of de analyse van hun gedrag of hun betrouwbaarheid, is bijzondere bescherming nodig om negatieve gevolgen te voorkomen. Geautomatiseerde besluitvorming omvat profilering die bestaat uit elke vorm van geautomatiseerde evaluatie van persoonlijke aspecten van de betrokkene, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke

voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen[606].

Voorbeeld: Om snel de kredietwaardigheid van een toekomstige klant te beoordelen, verzamelen kredietbeoordelaars bepaalde gegevens, zoals de wijze waarop de afnemer zijn/haar tegoedrekeningen en werkingskas heeft gehandhaafd, de bijzonderheden van de voorgaande adressen van de klant, alsmede informatie uit openbare bronnen, zoals de kiezerslijst, openbare registers (met inbegrip van rechterlijke beslissingen) of faillissements- en insolventiegegevens. Deze persoonsgegevens worden vervolgens ingevoerd in een algoritme waarmee een totale score wordt berekend die de kredietwaardigheid van een potentiële klant representeert.

Volgens Groep artikel 29 komt het recht om niet te worden onderworpen aan besluiten die uitsluitend gebaseerd zijn op geautomatiseerde gegevensverwerking die rechtsgevolgen voor de betrokkene kan hebben of belangrijke gevolgen voor hem/haar kan hebben, overeen met een algemeen verbod en moet de betrokkene niet proactief naar een bezwaar zoeken tegen een dergelijke beslissing[607].

Niettemin kan, volgens de AVG, geautomatiseerde besluitvorming met rechtsgevolgen of met aanzienlijke gevolgen voor personen aanvaardbaar zijn indien ze noodzakelijk is om een contract aan te gaan of om een contract tussen de verwerkingsverantwoordelijke en de betrokkene uit te voeren, of indien de betrokkene uitdrukkelijk toestemming heeft gegeven. Ook is geautomatiseerde besluitvorming aanvaardbaar als zij bij wet is toegestaan en indien de rechten, vrijheden en gerechtvaardigde belangen van de betrokkene naar behoren worden gewaarborgd[608].

De AVG bepaalt ook dat de verplichtingen van de verwerkingsverantwoordelijken met betrekking tot de informatie die moet worden verstrekt wanneer persoonsgegevens worden verzameld, onder andere inhouden dat betrokkenen over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, op de

606 *Ibid.*, overweging 71, artikel 4, lid 4, en artikel 22.

607 Groep artikel 29, *Richtsnoeren over geautomatiseerde individuele besluitvorming en profileren voor de toepassing van Verordening (EU) 2016/679*, WP 251, 3 oktober 2017, blz. 15.

608 Algemene verordening gegevensbescherming, artikel 22, lid 2.

hoogte moeten worden gesteld[609]. Het recht op toegang tot de persoonsgegevens die door de verwerkingsverantwoordelijke worden verwerkt, blijft onaangetast[610]. De informatie dient niet enkel weer te geven dat profilering zal plaatsvonden, ze moet ook betekenisvolle informatie bevatten over de opzet van de profilering en de verwachte gevolgen voor natuurlijke personen van de verwerking[611]. Zo moet een zorgverzekeraar die geautomatiseerde besluitvorming gebruikt voor verzoeken, de betrokkenen algemene informatie verstrekken over de manier waarop het algoritme werkt en welke factoren het algoritme gebruikt om hun verzekeringspremie te berekenen. Evenzo kunnen betrokkenen bij de uitoefening van hun recht van toegang informatie opvragen bij de verwerkingsverantwoordelijke over het bestaan van geautomatiseerde besluitvorming en betekenisvolle informatie over de opzet ervan[612].

De informatie verstrekt aan betrokkenen moet transparantie geven en de betrokkenen in staat stellen om een geïnformeerde toestemming te verlenen, indien dit het geval is, of om menselijke interventie te verkrijgen. De verwerkingsverantwoordelijke moet passende maatregelen nemen om de rechten, vrijheden en gerechtvaardigde belangen van de betrokkene te waarborgen. Dit omvat ten minste het recht om menselijke tussenkomst te verkrijgen van de verwerkingsverantwoordelijke en de mogelijkheid voor de betrokkene om een standpunt kenbaar te maken en een besluit dat gebaseerd is op de geautomatiseerde verwerking van hun persoonsgegevens, aan te vechten[613].

Groep artikel 29 heeft nadere richtsnoeren uitgewerkt over het gebruik van geautomatiseerde besluitvorming in het kader van de AVG[614].

In het kader van het recht van de Raad van Europa hebben natuurlijke personen het recht om niet te worden onderworpen aan een besluit dat belangrijke gevolgen voor hen zal hebben en dat uitsluitend is gebaseerd op geautomatiseerde verwerking zonder dat hun standpunten in aanmerking werden genomen[615]. De vereiste om rekening te houden met de mening van de betrokkene wanneer besluiten

609 *Ibid.*, artikel 12.

610 *Ibid.*, artikel 15.

611 *Ibid.*, artikel 13, lid 2, onder f).

612 *Ibid.*, artikel 15, lid 1, onder h).

613 *Ibid.*, artikel 22, lid 3.

614 Groep artikel 29 (2017), *Richtsnoeren over geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, WP 251, 3 oktober 2017.

615 Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder a).

enkel zijn gebaseerd op geautomatiseerde verwerking, houdt in dat de betrokkene het recht heeft om een dergelijk besluit aan te vechten en in staat moet zijn om elke onjuistheid in de persoonsgegevens die de verwerkingsverantwoordelijke gebruikt, te betwisten en de relevantie van het op hem toegepaste profiel in twijfel te trekken[616]. Een natuurlijke persoon kan dit recht echter niet uitoefenen indien het geautomatiseerde besluit is toegestaan door een wet die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten, vrijheden en gerechtvaardigde belangen van de betrokkene. Daarnaast hebben de betrokkenen het recht om op verzoek kennis te nemen van de onderliggende motivering van de gegevensverwerking[617]. De Memorie van toelichting van het Gemoderniseerd Verdrag 108 geeft het voorbeeld van de kredietwaardigheid. Natuurlijke personen moeten het recht hebben om niet enkel de positieve of negatieve score over zichzelf te kennen, maar ook de *redenering* die werd gevolgd tijdens de verwerking van hun persoonsgegevens en tot een dergelijk besluit heeft geleid. "Een beter begrip van deze elementen draagt bij tot de daadwerkelijke uitoefening van andere fundamentele waarborgen, zoals het recht van bezwaar en het recht om een klacht in te dienen bij een bevoegde autoriteit"[618].

De aanbeveling over het opstellen van profielen, zij het juridisch niet bindend, bepaalt de voorwaarden voor de verzameling en verwerking van persoonsgegevens in het kader van profilering[619]. Zo stelt de aanbeveling dat de verwerking in het kader van profilering eerlijk, rechtmatig en evenredig moet zijn en alleen voor gespecificeerde en gerechtvaardigde doeleinden mag geschieden. De aanbeveling bevat tevens bepalingen over de informatie die verwerkingsverantwoordelijken moeten verstrekken aan betrokkenen. Het beginsel van de kwaliteit van gegevens, dat de verwerkingsverantwoordelijke verplicht om maatregelen te nemen om onjuiste gegevens te verbeteren, om de risico's op fouten die profilering kan opleveren, te beperken, en om regelmatig de kwaliteit van de gegevens en de gebruikte algoritmes te evalueren, komt ook aan bod in de aanbeveling.

616 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 75.

617 Gemoderniseerd Verdrag 108, artikel 9, lid 1, onder c).

618 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 77.

619 Raad van Europa, Aanbeveling CM/Rec(2010)13 van het Comité van Ministers aan de lidstaten over de bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens in het kader van profilering, artikel 5, lid 5.

6.2. Corrigerende maatregelen, aansprakelijkheid, corrigerende sancties en schadeloosstelling

Belangrijkste punten

- Volgens het Gemoderniseerd Verdrag 108 moet het nationale recht van de verdragsluitende partijen voorzien in passende oplossingen en straffen voor inbreuken op het recht op gegevensbescherming.
- In de Europese Unie voorziet de AVG in corrigerende maatregelen voor betrokkenen in geval van schending van hun rechten, alsmede straffen tegen verwerkingsverantwoordelijken en verwerkers die niet voldoen aan de bepalingen van de verordening. Zij voorziet ook in het recht op schadeloosstelling en de aansprakelijkheid.
    - Betrokkenen hebben het recht om een klacht in te dienen bij een toezichthoudende autoriteit voor vermeende inbreuken op de verordening, alsmede het recht op een doeltreffend rechtsmiddel en op schadeloosstelling.
    - Bij de uitoefening van hun recht op een doeltreffende corrigerende maatregel mogen natuurlijke personen worden vertegenwoordigd door organisaties zonder winstoogmerk die actief zijn op het gebied van gegevensbescherming.
    - De verwerkingsverantwoordelijke of verwerker is aansprakelijk voor alle materiele en niet-materiële schade als gevolg van de inbreuk.
    - De toezichthoudende autoriteiten hebben de bevoegdheid om administratieve boetes op te leggen voor inbreuken op de verordening tot 20 miljoen euro of in het geval van een onderneming, 4 % van de totale jaarlijkse wereldwijde omzet — indien dit meer is.
- Als laatste redmiddel en onder bepaalde voorwaarden kunnen betrokkenen inbreuken op gegevensbeschermingswetgeving aanhangig maken bij het EHRM.
- Iedere natuurlijke persoon of rechtspersoon heeft het recht om bij het HvJ-EU een klacht in te dienen tegen een besluit van het Europees Comité voor gegevensbescherming, onder de in de Verdragen voorziene voorwaarden.

Aanneming van wetgevingsinstrumenten volstaat niet om de bescherming van persoonsgegevens in Europa te garanderen. Om de Europese regels inzake gegevensbescherming doeltreffend te maken, is het noodzakelijk om te voorzien in mechanismen die natuurlijke personen in staat stellen zich tegen schendingen van hun rechten uit te spreken en schadeloosstelling te vorderen voor de geleden schade.

Het is ook belangrijk dat toezichthoudende autoriteiten de bevoegdheid hebben om sancties op te leggen die doeltreffend, afschrikkend en evenredig zijn aan de inbreuk in kwestie.

Rechten onder de wetgeving inzake gegevensbescherming kunnen worden uitgeoefend door de personen van wie de rechten in het geding zijn; dit is de betrokkene. Andere personen, die voldoen aan de vereisten in het kader van het nationale recht, kunnen evenwel ook de betrokkene vertegenwoordigen bij de uitoefening van hun rechten. In het kader van een aantal nationale wetgevingen moeten kinderen en personen met een verstandelijke handicap worden vertegenwoordigd door hun voogden[620]. In het kader van de Europese wetgeving inzake gegevensbescherming mag een vereniging, die het rechtmatige doel heeft om de rechten inzake gegevensbescherming te bevorderen, betrokkenen vertegenwoordigen voor een toezichthoudende autoriteit of een rechterlijke instantie[621].

6.2.1. Recht om een klacht in te dienen bij een toezichthoudende autoriteit

In het kader van zowel **het recht van de Raad van Europa** als **het Unierecht** hebben natuurlijke personen het recht om verzoeken en klachten in te dienen bij de bevoegde toezichthoudende autoriteit indien zij van mening zijn dat de verwerking van hun persoonsgegevens niet gebeurt overeenkomstig de wet.

Het Gemoderniseerd Verdrag 108 erkent het recht van betrokkenen om te genieten van de bijstand van een toezichthoudende autoriteit bij de uitoefening van hun rechten uit hoofde van het verdrag, ongeacht hun nationaliteit of woonplaats[622]. Een verzoek om bijstand kan enkel worden geweigerd in uitzonderlijke omstandigheden, en betrokkenen hoeven de aan de bijstand verbonden kosten en honoraria niet op zich te nemen[623].

Soortgelijke bepalingen zijn opgenomen in de rechtsorde van de EU. De AVG bepaalt dat toezichthoudende autoriteiten maatregelen moeten nemen om de indiening van

620 FRA (2015), Handboek over het Europese recht inzake de rechten van het kind, Luxemburg, Bureau voor publicaties van de Europese Unie; FRA (2013), Legal capacity of persons with intellectual disabilities and persons with mental health problems, Luxemburg, Bureau voor publicaties van de Europese Unie.

621 Algemene verordening gegevensbescherming, artikel 80.

622 Gemoderniseerd Verdrag 108, artikel 18.

623 *Ibid.*, artikel 16-17.

klachten te vergemakkelijken, zoals het creëren van een elektronisch klachtenformulier[624]. De betrokkene kan de klacht indienen bij de toezichthoudende autoriteit in de lidstaat van zijn/haar gewone verblijfplaats, werkplek of de plaats van de vermeende inbreuk[625]. Klachten moeten worden onderzocht en de toezichthoudende autoriteit moet de betrokken persoon informeren over de uitkomst van de procedure die de klacht behandelt[626].

Mogelijke inbreuken bij EU-instellingen of -organen kunnen ter kennis van de Europese Toezichthouder voor gegevensbescherming worden gebracht[627]. Indien de EDPS niet binnen zes maanden antwoordt, betekent dit dat de klacht is afgewezen. Beroepen tegen de beslissingen van de EDPS kunnen worden ingesteld bij het HvJ-EU in het kader van de Verordening (EG) nr. 45/2001 die de EU-instellingen en -organen verplicht om de regels inzake gegevensbescherming na te leven.

Het moet mogelijk zijn om beroep aan te tekenen bij de rechter tegen besluiten van een nationale toezichthoudende autoriteit. Dit is van toepassing voor zowel de betrokkene als de verwerkingsverantwoordelijken en verwerkers die partij zijn geweest in een procedure bij een toezichthoudende autoriteit.

Voorbeeld: In september 2017 beboette de Spaanse gegevensbeschermingsautoriteit Facebook voor het schenden van verscheidene verordeningen inzake gegevensbescherming. De toezichthoudende autoriteit veroordeelde het sociale netwerk voor het verzamelen, opslaan en verwerken van persoonsgegevens, met inbegrip van bijzondere categorieën persoonsgegevens, voor reclamedoeleinden en zonder toestemming te verkrijgen van de betrokkene. Het besluit was gebaseerd op een onderzoek dat op eigen initiatief door de toezichthoudende autoriteit was uitgevoerd.

624 Algemene verordening gegevensbescherming, artikel 57, lid 2.

625 *Ibid.*, artikel 77, lid 1.

626 *Ibid.*, artikel 77, lid 2.

627 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, PB L 8 van 12.1.2001.

6.2.2. Recht op een doeltreffende voorziening in rechte

Naast het recht om een klacht in te dienen bij de toezichthoudende autoriteit moeten personen het recht hebben op een doeltreffende voorziening in rechte en hun zaak voor een rechterlijke instantie aanhangig kunnen maken. Het recht op een voorziening in rechte is verankerd in de Europese juridische tradities en is erkend als een grondrecht, zowel in het kader van artikel 47 van het EU-Handvest van de grondrechten als artikel 13 van het EVRM[628].

In het kader van het Unierecht is het belang om betrokkenen bij een schending van hun rechten een doeltreffende voorziening in rechte te verstrekken onbetwistbaar in zowel de bepalingen van de AVG, die voorziet in een recht op een doeltreffende voorziening in rechte tegen toezichthoudende autoriteiten, verwerkingsverantwoordelijken en verwerkers, als in de rechtspraak van het HvJ-EU.

Voorbeeld: In *Schrems*[629] verklaarde het HvJ-EU het adequaatheidsbesluit inzake de Veilige Haven ongeldig. Dit besluit had de internationale doorgifte van gegevens van de EU naar organisaties in de VS, die zichzelf hadden gecertificeerd onder de veiligehavenregeling, toegestaan. Het HvJ-EU oordeelde dat de veiligehavenregeling diverse tekortkomingen vertoonde die de grondrechten van EU-burgers met betrekking tot bescherming van de privacy, bescherming van persoonsgegevens en het recht op een doeltreffende voorziening in rechte, in het gedrang bracht.

Met betrekking tot de schending van de rechten op privacy en gegevensbescherming benadrukt het HvJ-EU dat de VS-wetgeving bepaalde overheidsinstanties toegang bood tot de persoonsgegevens die waren overgedragen door de lidstaten aan de Verenigde Staten om ze te verwerken op een wijze die onverenigbaar was met het oorspronkelijke doeleinde van de doorgifte en verder ging dan wat strikt noodzakelijk en evenredig was voor de bescherming van de binnenlandse veiligheid. Inzake het recht op een doeltreffende voorziening in rechte merkte het op dat de betrokkenen geen administratieve middelen of rechtsmiddelen hadden om toegang te krijgen tot de hen betreffende gegevens en ze te rectificeren, dan wel te

628 Zie bijvoorbeeld EHRM, *Karabeyoğlu/Turkije*, nr. 30083/10, 7 juni 2016; EHRM, *Mustafa Sezgin Tanrıkulu/Turkije*, nr. 27473/06, 18 juli 2017.

629 HvJ-EU, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer], 6 oktober 2015.

laten wissen. Het HvJ-EU heeft geconcludeerd dat wetgeving die niet in beroepsmogelijkheden voorziet om toegang tot persoonsgegevens, of rectificatie of verwijdering van die gegevens, te verkrijgen "de wezenlijke inhoud van het grondrecht op een effectieve voorziening in rechte, zoals neergelegd in artikel 47 van het Handvest van de grondrechten van de Europese Unie, niet [eerbiedigt]". Het benadrukte dat het bestaan van een beroepsmogelijkheid die de naleving van wettelijke voorschriften garandeert, inherent is aan de rechtstaat.

Natuurlijke personen, verwerkingsverantwoordelijken of verwerkers die het juridisch bindende besluit van een toezichthoudende autoriteit willen aanvechten, kunnen een procedure starten bij een rechtbank[630]. Het begrip "besluit" moet breed worden geïnterpreteerd en dekt de uitvoering van de onderzoeks-, sanctie- en vergunningsbevoegdheden van de toezichthoudende autoriteit, alsook besluiten om een klacht te weigeren of te verwerpen. Juridisch niet-bindende maatregelen, zoals standpunten of adviezen van de toezichthoudende autoriteit, kunnen evenwel niet het voorwerp uitmaken van een gerechtelijke procedure[631]. De gerechtelijke procedure moet worden ingesteld bij de gerechten van de lidstaat waar de relevante toezichthoudende autoriteit is gevestigd[632].

In gevallen waarin een verwerkingsverantwoordelijke of een verwerker inbreuk maakt op de rechten van een betrokkene, kunnen betrokkenen een klacht voorleggen aan een rechtbank[633]. Voor procedures die tegen een verwerkingsverantwoordelijke of een verwerker worden opgestart, is het uitermate belangrijk dat personen de keuze hebben over de plaats waar de vordering wordt ingesteld. Ze kunnen ervoor kiezen dit te doen, hetzij in de lidstaat waar de verwerkingsverantwoordelijke of verwerker een vestiging heeft, hetzij in de lidstaat waar de betrokkenen hun gewone verblijfplaats hebben[634]. De tweede mogelijkheid vereenvoudigt aanzienlijk de uitoefening van de rechten van de personen, aangezien het hen in staat stelt om naar de rechter te stappen in de staat waar ze verblijven en in een vertrouwd gerechtsgebied. Door de locatie voor een procedure tegen verwerkingsverantwoordelijken en verwerkers te beperken tot de lidstaat waarin zij een vestiging hebben, kunnen betrokkenen die in een andere lidstaat wonen, ontmoedigd raken om een

630 Algemene verordening gegevensbescherming, artikel 78.

631 *Ibid.*, overweging 143.

632 *Ibid.*, artikel 78, lid 223.

633 *Ibid.*, artikel 79.

634 *Ibid.*, artikel 79, lid 2.

rechtszaak aan te spannen, aangezien dit reiskosten en bijkomstige kosten met zich mee zou brengen en de procedure eventueel in een vreemde taal en een vreemd gerechtsgebied zou worden gevoerd. De enige uitzondering betreft gevallen waarin de verwerkingsverantwoordelijke of de verwerker overheidsinstanties zijn en de verwerking wordt uitgevoerd in de uitoefening van hun openbaar gezag. In dit geval zijn enkel de rechterlijke instanties van de lidstaat van de relevante overheidsinstantie bevoegd om de klacht te behandelen[635].

Terwijl, in de meeste gevallen, zaken betreffende regels inzake gegevensbescherming zullen worden behandeld bij de rechterlijke instanties van de lidstaten, kunnen sommige zaken worden ingesteld bij het HvJ-EU. De eerste mogelijkheid is wanneer een betrokkene, een verwerkingsverantwoordelijke, een verwerker of een toezichthoudende autoriteit streeft naar een nietigverklaring van een besluit van het Europees Comité voor gegevensbescherming (EDPB). Deze actie is echter onderworpen aan de voorwaarden van artikel 263 van het VWEU, hetgeen betekent dat, om in aanmerking te worden genomen, deze personen en entiteiten moeten aantonen dat het besluit van het Comité hen rechtstreeks en individueel raakt.

Het tweede scenario heeft betrekking op gevallen van EU-instellingen of -organen die onrechtmatig persoonsgegevens verwerken. In gevallen waarin de EU-instellingen inbreuk maken op de wetgeving inzake gegevensbescherming, kunnen de betrokkenen rechtstreeks een vordering instellen bij het Gerecht van de Europese Unie (het Gerecht maakt deel uit van het HvJ-EU). Het gerecht is in eerste instantie verantwoordelijk voor klachten over inbreuken op het Unierecht door EU-instellingen. Klachten tegen de EDPS, zijnde een EU-instelling, kunnen dus ook worden ingesteld bij het Gerecht van de Europese Unie[636].

Voorbeeld: In *Bavarian Lager*[637] vroeg de vennootschap aan de Europese Commissie om toegang te verlenen tot het volledige proces-verbaal van een bijeenkomst die de Commissie had gehouden en naar verluidt verband hield met juridische kwesties die relevant waren voor de vennootschap. De Commissie weigerde het verzoek van de vennootschap voor toegang op grond van hogere belangen van gegevensbescherming[638]. Onder

635 *Ibid.*

636 Verordening (EG) nr. 45/2001, artikel 32, lid 3.

637 HvJ-EU, zaak C-28/08 P, *Europese Commissie/The Bavarian Lager Co. Ltd* [Grote kamer], 2010.

638 Voor een analyse van het argument, zie de EDPS (2011), *Toegang van het publiek tot documenten die persoonsgegevens bevatten na de Bavarian Lager-uitspraak*, Brussel, EDPS.

artikel 32 van de op de EU-instellingen toepasselijke Verordening gegevensbescherming, diende Bavarian Lager een klacht in bij het Gerecht van eerste aanleg (de voorloper van het Gerecht) met betrekking tot dat besluit. In zijn beslissing (zaak T-194/04, *The Bavarian Lager Co.Ltd/ Commissie van de Europese Gemeenschappen*) had het Gerecht van eerste aanleg het besluit van de Commissie om het toegangsverzoek te weigeren, vernietigd. De Europese Commissie heeft beroep aangetekend tegen deze beslissing bij het HvJ-EU.

Het HvJ-EU deed zijn uitspraak (in de Grote kamer) en vernietigde de uitspraak van het Gerecht van eerste aanleg en bevestigde de afwijzing van de Europese Commissie van het verzoek tot toegang tot het volledige procesverbaal van de vergadering, ter bescherming van de persoonsgegevens van de personen tijdens de vergadering. Het HvJ-EU oordeelde dat de Commissie terecht de openbaarmaking van die informatie had geweigerd, aangezien de deelnemers hun instemming om hun persoonsgegevens openbaar te maken, niet hadden gegeven. Bovendien had Bavarian Lager de noodzaak om toegang te krijgen tot die informatie, niet aangetoond.

Tot slot mogen betrokkenen, toezichthoudende autoriteiten, verwerkingsverantwoordelijken of verwerkers in de loop van nationale procedures de nationale rechterlijke instantie vragen om verduidelijking van het HvJ-EU over de interpretatie en geldigheid van handelingen van EU-instellingen, -organen, kantoren of agentschappen. Deze verduidelijkingen zijn bekend als prejudiciële beslissingen. Dit is geen direct beroep in rechte voor de klager, maar het stelt de nationale rechtbanken in staat ervoor te zorgen dat ze de correcte interpretatie van het Unierecht toepassen. Het is via dit mechanisme van prejudiciële beslissingen dat invloedrijke zaken, zoals *Digital Rights Ireland* en Kärntner Landesregierung e.a.[639] en *Schrems*[640], die grote invloed hadden op de ontwikkeling van de EU-wetgeving inzake gegevensbescherming, het HvJ-EU bereikten.

639 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en Kärntner Landesregierung e.a. [Grote kamer], 8 april 2014.

640 HvJ-EU, zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer], 6 oktober 2015.

Voorbeeld: *Digital Rights Ireland* en *Kärntner Landesregierung e.a.*[641] was een gevoegde zaak die door het Ierse Hooggerechtshof en het Oostenrijks Grondwettelijk Hof was ingediend met betrekking tot de conformiteit van Richtlijn 2006/24/EG (richtlijn gegevensbewaring) met de EU-wetgeving inzake gegevensbescherming. Het Oostenrijks Grondwettelijk Hof legde vragen voor aan het HvJ-EU met betrekking tot de geldigheid van de artikelen 3 tot en met 9 van Richtlijn 2006/24/EG in het licht van de artikelen 7, 9 en 11 van het EU-Handvest van de grondrechten. Deze omvatten onder meer of bepaalde bepalingen van het Oostenrijkse federale telecommunicatierecht tot omzetting van de richtlijn gegevensbewaring onverenigbaar waren met aspecten van de voormalige richtlijn inzake gegevensbescherming en de op EU-instellingen toepasbare verordening gegevensbescherming.

In het geval van *Kärntner Landesregierung e.a.* stelde de heer Seitlinger, een van de verzoekers in de procedure voor het Grondwettelijk Hof, dat hij de telefoon, het internet en de e-mail voor zowel zijn werk als zijn privéleven gebruikte. Dientengevolge verstuurde en ontving hij informatie via openbare telecommunicatienetwerken. Volgens de Oostenrijkse telecommunicatiewet van 2003 was zijn telecommunicatieaanbieder wettelijk verplicht om gegevens over zijn gebruik van het netwerk te verzamelen en op te slaan. De heer Seitlinger vond dat de inzameling en opslag van zijn persoonsgegevens niet nodig was voor de technische toepassing van het verzenden en ontvangen van informatie via het netwerk. Noch was de verzameling en de opslag van deze gegevens noodzakelijk voor factureringsdoeleinden. De heer Seitlinger verklaarde dat hij niet had ingestemd met dit gebruik van zijn persoonsgegevens, die uitsluitend op grond van de Telecommunicatiewet van 2003 werden verzameld en opgeslagen.

De heer Seitlinger heeft daarom een procedure aanhangig gemaakt bij het Oostenrijks Grondwettelijk Hof waarin hij aanvoert dat de wettelijke verplichtingen voor zijn telecommunicatieaanbieder een inbreuk vormen op zijn grondrechten uit hoofde van artikel 8 van het Handvest van de grondrechten. Gezien het feit dat de Oostenrijkse wetgeving het Unierecht (de voormalige richtlijn gegevensbewaring) uitvoerde, legde het Oostenrijks Grondwettelijk Hof de zaak voor aan het HvJ-EU om te

641 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en *Kärntner Landesregierung e.a.* [Grote kamer], 8 april 2014.

beslissen over de verenigbaarheid van de richtlijn met het recht op privacy en gegevensbescherming dat is vastgelegd in het EU-Handvest van de grondrechten.

De Grote kamer van het HvJ-EU velde het vonnis dat heeft geleid tot de nietigverklaring van de EU-richtlijn gegevensbewaring. Het HvJ-EU stelde vast dat de richtlijn leidde tot een uitzonderlijk ernstige verstoring van de fundamentele rechten op privacy en gegevensbescherming, zonder dat deze interferentie wordt beperkt tot het strikt noodzakelijke. De richtlijn beoogde een rechtmatig doel, aangezien het nationale autoriteiten aanvullende mogelijkheden gaf om ernstige misdrijven te onderzoeken en te vervolgen en was daarom een nuttig instrument bij strafonderzoeken. Het HvJ-EU merkte echter op dat beperkingen van de grondrechten enkel mogen worden toegepast indien dit strikt noodzakelijk is en gepaard moeten gaan met duidelijke en nauwkeurige regels met betrekking tot het toepassingsgebied ervan, samen met de waarborgen voor natuurlijke personen.

Volgens het HvJ-EU voldeed de richtlijn niet aan deze noodzakelijkheidstoets. Ten eerste legde hij geen duidelijke en nauwkeurige regels vast die het toepassingsgebied van de tussenkomst beperkte. In plaats van een relatie te vereisen tussen de bewaarde gegevens en zware criminaliteit, was de richtlijn van toepassing op alle metagegevens van alle gebruikers van alle elektronische communicatiemiddelen. Hij vormde dus een belemmering met de rechten op privacy en gegevensbescherming van nagenoeg de gehele EU-bevolking, wat als onevenredig kon worden beschouwd. Hij bevatte geen voorwaarden om het aantal personen met toegang tot de persoonsgegevens te beperken, noch was deze toegang onderhevig aan procedurele voorwaarden zoals de verplichting om de goedkeuring van een administratieve autoriteit of rechtbank te krijgen voorafgaand aan de toegang. Ten slotte werden in de richtlijn de waarborgen voor de bescherming van de bewaarde gegevens niet duidelijk omschreven. Hij slaagde er daarom niet in om een daadwerkelijke bescherming van de gegevens tegen het risico van misbruik en tegen ongeoorloofde toegang tot en gebruik van de gegevens te waarborgen[642].

642 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en *Kärntner Landesregierung e.a.* [Grote kamer], 8 april 2014, punt 69.

In principe moet het HvJ-EU voorgelegde vragen beantwoorden en kan het niet weigeren om een prejudiciële beslissing te geven op grond van het feit dat dit antwoord niet relevant noch tijdig zou zijn ten aanzien van de oorspronkelijke zaak. Het kan echter wel weigeren als de vraag niet onder zijn bevoegdheid valt[643]. Het besluit van het HvJ-EU heeft enkel betrekking op de bestanddelen van het verzoek dat wordt voorgelegd voor een prejudiciële beslissing terwijl de nationale rechtbank zijn bevoegdheid behoudt om te beslissen over de oorspronkelijke zaak[644].

In het kader van het recht van de Raad van Europa moeten verdragsluitende partijen passende gerechtelijke en buitengerechtelijke oplossingen vaststellen voor schendingen van de bepalingen van het Gemoderniseerd Verdrag 108[645]. Beweerde schendingen van de gegevensbeschermingsrechten die in strijd zijn met artikel 8 van het EVRM ten opzichte van een verdragsluitende partij bij het EVRM, kunnen ook voor het EHRM worden gebracht wanneer alle beschikbare binnenlandse rechtsmiddelen zijn uitgeput. Een betoog voor de schending van artikel 8 van de EVRM voor het EHRM moet ook voldoen aan de andere ontvankelijkheidscriteria (artikelen 34-35 van de EVRM)[646].

Hoewel verzoeken aan het EHRM alleen gericht kunnen zijn tegen partijen bij het EVRM, kunnen ze indirect ook betrekking hebben op handelingen of nalatigheid door private partijen, voor zover een verdragspartij zijn positieve verplichtingen uit hoofde van het EVRM niet heeft vervuld en onvoldoende bescherming heeft geboden tegen inbreuken op in zijn nationale recht vastgestelde gegevensbeschermingsrechten.

Voorbeeld: In *K.U./Finland*[647] beklaagde de minderjarige verzoeker zich erover dat een seksueel getinte advertentie in zijn naam op een internetdatingsite was gezet. De serviceprovider maakte de identiteit van de plaatser van de informatie niet bekend vanwege de vertrouwelijkheidsvoorschriften uit hoofde van het Finse recht. De verzoeker stelde dat het nationale recht onvoldoende bescherming bood tegen acties waarbij een privépersoon

643 HvJ-EU, zaak C-244/80, *Pasquale Foglia tegen Mariella Novello (nr. 2)*, 16 december 1981; HvJ-EU, zaak C-467/04, *Strafzaak tegen Gasparini e.a.*, 28 september 2006.

644 HvJ-EU, zaak C-438/05, *Internationale Federatie van vervoerswerknemers, de Finse Unie van zeelieden/Viking Line ABP, OÜ Viking Line Eesti* [Grote kamer], 11 december 2007, punt 85.

645 Gemoderniseerd Verdrag 108, artikel 12.

646 EVRM, artikel 34-37.

647 EHRM, *K.U./Finland*, nr. 2872/02, 2 december 2008.

compromitterende gegevens over de verzoeker op internet plaatst. Het EHRM oordeelde dat staten niet alleen verplicht zijn zich te onthouden van willekeurige inmenging in de privélevens van natuurlijke personen, maar ook zijn onderworpen aan positieve verplichtingen, waaronder "de vaststelling van maatregelen ter verzekering van de eerbiediging van andermans privéleven op het gebied van de onderlinge relaties van individuele personen". In het geval van de verzoeker vereiste zijn praktische en doeltreffende bescherming dat er effectieve stappen werden ondernomen om de dader te identificeren en te vervolgen. Deze bescherming was door de staat echter niet geboden, en het Hof concludeerde dat er een inbreuk op artikel 8 van het EVRM had plaatsgevonden.

Voorbeeld: In *Köpke tegen Duitsland*[648] werd de verzoekster verdacht van diefstal op haar werkplek en was ze onderworpen aan surveillance met behulp van een verborgen camera. Het EHRM concludeerde dat "niets er op wijst dat de binnenlandse autoriteiten geen goed evenwicht hebben gevonden, binnen hun beoordelingsmarge, tussen het recht van verzoekster op eerbiediging van haar privéleven op grond van artikel 8 en zowel het belang van haar werkgever in het beschermen van zijn eigendomsrechten als het algemene belang van een behoorlijke rechtspraak". Het verzoek werd om die reden niet-ontvankelijk verklaard.

Als het EHRM oordeelt dat een verdragsluitende partij een door het EVRM beschermd recht heeft geschonden, is deze verdragsluitende partij verplicht om uitvoering te geven aan het arrest van het EHRM (artikel 46 van het EVRM). Uitvoeringsmaatregelen moeten eerst een eind maken aan de schending en daarnaast, voor zover mogelijk, de negatieve gevolgen voor de verzoeker corrigeren. De tenuitvoerlegging van arresten kan ook algemene maatregelen vereisen om soortgelijke schendingen als die welke door het Hof zijn vastgesteld te voorkomen, door middel van wetswijzigingen, jurisprudentie of anderszins.

Wanneer het EHRM een schending van het EVRM vaststelt, voorziet artikel 41 van het EVRM erin dat het Hof billijke genoegdoening aan de benadeelde kan toekennen op kosten van de verdragsluitende partij.

648 EHRM, *Köpke/Duitsland* (dec.), nr. 420/07, 5 oktober 2010.

Recht om een orgaan, organisatie of vereniging zonder winstoogmerk te mandateren

De AVG stelt natuurlijke personen die een klacht indienen bij een toezichthoudende autoriteit of een zaak aanhangig maken bij een rechterlijke instantie in staat om een orgaan, organisatie of vereniging zonder winstoogmerk te mandateren om hen te vertegenwoordigen[649]. Deze instellingen zonder winstoogmerk moeten statutaire doelstellingen hebben met betrekking tot het algemeen belang en actief zijn op het gebied van gegevensbescherming. Zij kunnen de klacht indienen of het recht op een beroep in rechte uitoefenen voor rekening van de betrokken persoon (personen). De verordening geeft de lidstaten de mogelijkheid te besluiten, overeenkomstig het nationale recht, of een orgaan klachten kan indienen voor rekening van betrokkenen, zonder dat zij werden gemandateerd door deze betrokkenen.

Dit recht op vertegenwoordiging stelt natuurlijke personen in staat om gebruik te maken van de deskundigheid en de organisatorische en financiële capaciteiten van dergelijke entiteiten zonder winstoogmerk, waardoor het de natuurlijke personen enorm wordt vergemakkelijkt bij de uitoefening van hun rechten. De AVG stelt deze entiteiten in staat om collectieve vorderingen in te stellen voor rekening van verschillende betrokkenen. Dit geeft ook voordelen voor de werking en doeltreffendheid van het gerechtelijk apparaat, aangezien soortgelijke vorderingen zijn gegroepeerd en samen worden onderzocht.

6.2.3. Aansprakelijkheid en het recht op schadevergoeding

Het recht op een doeltreffende voorziening in rechte moet natuurlijke personen in staat stellen tot het eisen van een schadevergoeding voor geleden schade als gevolg van de verwerking van hun persoonsgegevens op een wijze die de toepasselijke wetgeving schendt. De aansprakelijkheid van verwerkingsverantwoordelijken en verwerkers voor onrechtmatige verwerking wordt uitdrukkelijk erkend in de AVG[650]. De verordening geeft natuurlijke personen het recht om schadevergoeding te krijgen van de verwerkingsverantwoordelijke of verwerker voor zowel materiële als immateriële schade, terwijl haar overwegingen bepalen dat "het begrip "schade" ruim moet worden uitgelegd in het licht van de rechtspraak van het Hof van Justitie,

649 Algemene verordening gegevensbescherming, artikel 80.

650 *Ibid.*, artikel 82.

op een wijze die ten volle recht doet aan de doelstellingen van deze verordening"[651]. Verwerkingsverantwoordelijken zijn aansprakelijk en kunnen onderworpen worden aan eisen voor schadevergoeding indien ze niet voldoen aan hun verplichtingen uit hoofde van de verordening. Een verwerker van persoonsgegevens is slechts aansprakelijk voor de schade die door verwerking is veroorzaakt wanneer bij de verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van deze verordening, of waar buiten dan wel in strijd met de rechtmatige instructies van de verwerkingsverantwoordelijke is gehandeld. Indien een verwerkingsverantwoordelijke of verwerker de volledige vergoeding heeft betaald, voorziet de AVG dat de verwerkingsverantwoordelijke of verwerker het deel van de vergoeding dat beantwoordt aan de mate van de verantwoordelijkheid van de schade van de andere verwerkingsverantwoordelijken of verwerkers die in dezelfde verwerking zijn betrokken, kan terugvorderen[652]. Tegelijkertijd zijn uitzonderingen op de aansprakelijk zeer strikt en onder voorbehoud van het bewijs dat de verwerkingsverantwoordelijke of de verwerker niet verantwoordelijk is voor de gebeurtenis die aanleiding heeft gegeven tot de schade.

Compensatie moet "volledig en effectief" zijn met betrekking tot de geleden schade. Wanneer de schade wordt veroorzaakt door de verwerking van verscheidene verwerkingsverantwoordelijken en verwerkers, moet elke verwerkingsverantwoordelijke of verwerker verantwoordelijk worden gesteld voor de gehele schade. Deze regel moet zorgen voor een doeltreffende compensatie voor de betrokkenen en voor een gecoördineerde aanpak van de naleving van de regels door de verwerkingsverantwoordelijken en verwerkers die betrokken zijn bij de verwerkingsactiviteiten.

Voorbeeld: Betrokkenen moeten de zaak en hun verzoek voor schadevergoeding niet instellen voor alle entiteiten die verantwoordelijk zijn voor de schade, aangezien dit dure en langdurige procedures tot gevolg kan hebben. Het is voldoende om een zaak tegen een van de gezamenlijke verwerkingsverantwoordelijken in te stellen, die vervolgens voor de volledige schade aansprakelijk kan worden gesteld. In dergelijke gevallen kan de verwerkingsverantwoordelijke of verwerker die de schade betaalt, de betaalde som terugvorderen bij de andere entiteiten die zijn betrokken in de verwerking en verantwoordelijk zijn voor de schending, elk voor hun deel van de verantwoordelijkheid van de schade. Deze procedures tussen de

651 *Ibid.*, overweging 146.

652 *Ibid.*, artikel 82, leden 2 en 5.

verschillende gezamenlijke verwerkingsverantwoordelijken en verwerkers vinden plaats nadat de betrokkene een vergoeding heeft ontvangen en de betrokkene geen deel van hen uitmaakt.

In het juridische kader van het recht van de Raad van Europa vereist artikel 12 van Gemoderniseerd Verdrag 108 dat verdragsluitende partijen passende corrigerende maatregelen vaststellen voor inbreuken op de nationale wetgeving ter uitvoering van de voorschriften van dit verdrag. Uit de Memorie van toelichting van het Gemoderniseerd Verdrag 108 blijkt dat corrigerende maatregelen de mogelijkheid moeten omvatten om een besluit of praktijk gerechtelijk te betwisten, terwijl er ook in buitengerechtelijke corrigerende maatregelen moet worden voorzien[653]. De modaliteiten en verschillende regels met betrekking tot de toegang tot deze corrigerende maatregelen, samen met de te volgen procedure, worden overgelaten aan het oordeel van de verdragsluitende partijen. Verdragsluitende partijen en nationale rechtelijke instanties moeten ook rekening houden met bepalingen voor de financiële schadevergoeding voor materiële en immateriële schade die door de verwerking worden veroorzaakt, evenals de mogelijkheid om collectieve vorderingen in te stellen[654].

6.2.4. Sancties

In het kader van het recht van de Raad van Europa bepaalt artikel 12 van Gemoderniseerd Verdrag 108 dat elke verdragsluitende partij zich moet verbinden aan passende sancties en corrigerende maatregelen voor de schending van bepalingen van het interne recht waarmee uitvoering wordt gegeven aan de grondbeginselen van gegevensbescherming als vervat in Verdrag 108. Er wordt geen bepaalde reeks sancties vastgelegd of opgelegd door het verdrag. Integendeel, het geeft duidelijk aan dat elke verdragsluitende partij de mogelijkheid heeft om de aard van de gerechtelijke of buitengerechtelijke sancties vast te leggen; deze sancties kunnen strafrechtelijk, administratief of civiel zijn. In de memorie van toelichting van het Gemoderniseerd Verdrag 108 is bepaald dat sancties doeltreffend, evenredig en afschrikkend moeten zijn[655]. Verdragsluitende partijen moeten dit beginsel respecteren bij het bepalen van de aard en de ernst van de sancties in hun interne rechtsorde.

653 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 100.

654 *Ibid.*

655 *Ibid.*

In het kader van het Unierecht geeft artikel 83 van de AVG de toezichthoudende autoriteiten van de lidstaten de mogelijkheid om administratieve boetes op te leggen in geval van overtredingen van de verordening. De hoogte van de boetes en de omstandigheden waarmee de nationale autoriteiten rekening houden bij de overweging om al dan niet een boete op te leggen, evenals het maximumniveau van die boete, wordt ook vastgelegd in artikel 83. Daarom is de sanctieregeling in de EU geharmoniseerd.

De AVG volgt een trapsgewijze aanpak voor boetes. De toezichthoudende autoriteiten hebben de bevoegdheid om administratieve boetes op te leggen voor inbreuken op de verordening tot 20 miljoen euro of, in het geval van een onderneming, 4 % van de totale jaarlijkse wereldwijde omzet, indien dit meer is. Inbreuken die aanleiding kunnen geven tot deze boete, omvatten inbreuken op de grondbeginselen van de verwerking en op de voorwaarden voor toestemming, inbreuken op de rechten van betrokkenen en op de bepalingen van de verordening betreffende de doorgifte van persoonsgegevens aan ontvangers in derde landen. Voor andere inbreuken mogen de toezichthoudende autoriteiten boetes opleggen tot 10 miljoen euro of, in het geval van een onderneming, 2 % van de totale jaarlijkse omzet, indien dit meer is.

Bij het bepalen van het soort boete en het niveau van de opgelegde boete moeten toezichthoudende autoriteiten rekening houden met een aantal factoren[656]. Ze moeten bijvoorbeeld naar behoren rekening houden met de aard, ernst en duur van de schending, de getroffen categorieën persoonsgegevens en de vraag of de schending opzettelijk dan wel door nalatigheid heeft plaatsgevonden. Wanneer een verwerkingsverantwoordelijke of verwerker maatregelen heeft genomen om de schade aan de betrokkenen te beperken, moet men hier rekening mee houden. Op vergelijkbare wijze zijn de mate van samenwerking met de toezichthoudende autoriteit na een inbreuk en de manier waarop de toezichthoudende autoriteit op de hoogte werd gesteld van de inbreuk (bijvoorbeeld, werd deze gemeld door de entiteit die verantwoordelijk was voor de verwerking of door de betrokkene wiens rechten werden geschonden) andere belangrijke factoren die de toezichthoudende autoriteiten sturen in hun beslissing[657].

656 Algemene verordening gegevensbescherming, artikel 83, lid 2.

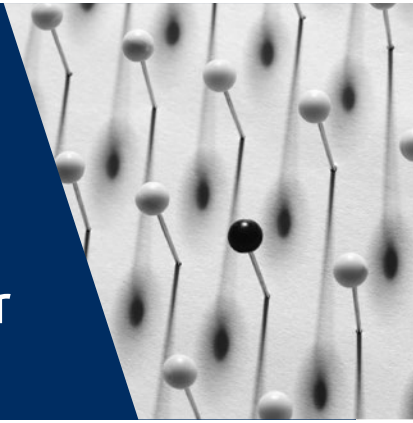
657 Groep artikel 29 (2017), Richtsnoeren voor de toepassing en vaststelling van administratieve geldboetes voor de toepassing van de Verordening (EU) 2016/679, WP 253, 3 oktober 2017.

Naast de mogelijkheid tot het opleggen van administratieve geldboetes, beschikken de toezichthoudende autoriteiten over een groot aantal andere corrigerende bevoegdheden. De zogeheten "corrigerende" bevoegdheden van de toezichthoudende autoriteiten zijn vastgesteld in artikel 58 van de AVG. Ze variëren van het geven van bevelen, waarschuwingen en berispingen aan verwerkingsverantwoordelijken en verwerkers tot de instelling van tijdelijke of zelfs permanente verboden op verwerkingsactiviteiten.

Sancties voor inbreuken op het Unierecht door EU-instellingen of -organen kunnen, vanwege het bijzondere toepassingsgebied van de Verordening gegevensbescherming van de EU-instellingen, alleen voorzien worden in de vorm van disciplinaire maatregelen. Volgens artikel 49 van de verordening kan "de ambtenaar of een ander personeelslid van de Europese Gemeenschappen die, opzettelijk of uit nalatigheid, de bij of krachtens deze verordening op hem rustende verplichtingen niet nakomt, [...] aan een tuchtmaatregel worden onderworpen [...]".

7

Internationale doorgifte en internationaal verkeer van persoonsgegevens



EU	Behandelde onderwerpen	RvE
Doorgifte van persoonsgegevens		
Algemene verordening gegevensbescherming artikel 44	Concept	Gemoderniseerd Verdrag 108, artikel 14, leden 1 en 2
Vrij verkeer van persoonsgegevens		
Algemene verordening gegevensbescherming, artikel 1, lid 3, en overweging 170	Tussen EU-lidstaten	
	Tussen partijen bij Verdrag 108	Gemoderniseerd Verdrag 108, artikel 14, lid 1
Doorgifte van persoonsgegevens aan derde landen of internationale organisaties		
Algemene verordening gegevensbescherming, artikel 45 Zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer], 2015	Adequaatheidsbesluit/derde landen of internationale organisaties met een passend beschermingsniveau	Gemoderniseerd Verdrag 108, artikel 14, lid 2
Algemene verordening gegevensbescherming, artikel 46, lid 1, en artikel 46, lid 2	Passende waarborgen, met inbegrip van afdwingbare rechten en rechtsmiddelen voor betrokkenen, verstrekt door standaardcontractbepalingen, bindende bedrijfsvoorschriften, gedragscodes en certificeringsmechanismen	Gemoderniseerd Verdrag 108, artikel 14, leden 2, 3, 5 en 6

EU	Behandelde onderwerpen	RvE
Algemene verordening gegevensbescherming, artikel 46, lid 3	**Onder voorbehoud van de toestemming van de bevoegde toezichthoudende autoriteit: de contractbepalingen en voorzieningen die zijn opgenomen in de administratieve regelingen tussen overheidsdiensten**	
Algemene verordening gegevensbescherming, artikel 46, lid 5	**Bestaande toestemmingen op grond van Richtlijn 95/46/EG**	
Algemene verordening gegevensbescherming, artikel 47	**Bindende bedrijfsvoorschriften**	
Algemene verordening gegevensbescherming, artikel 49	**Derogaties voor specifieke situaties**	Gemoderniseerd Verdrag 108, artikel 14, lid 4
Voorbeelden: PNR-overeenkomst tussen de EU en de VS SWIFT-overeenkomst tussen de EU en de VS	**Internationale overeenkomsten**	Gemoderniseerd Verdrag 108, artikel 14, lid 3, onder a)

In het kader van het Unierecht voorziet de algemene verordening gegevensbescherming in het vrije verkeer van gegevens binnen de Europese Unie. Het bevat echter specifieke voorschriften met betrekking tot de overdracht van persoonsgegevens naar derde landen buiten de EU en internationale organisaties. De verordening erkent het belang van deze overdrachten, met name in het licht van de internationale handel en samenwerking, maar erkent ook het verhoogde risico voor de persoonsgegevens. De verordening heeft daarom tot doel om persoonsgegevens die aan derde landen worden doorgegeven, hetzelfde beschermingsniveau te bieden als binnen de EU[658]. Het recht van de Raad van Europa erkent ook het belang van uitvoeringsvoorschriften voor grensoverschrijdende gegevensstromen die gebaseerd zijn op het vrije verkeer tussen partijen en specifieke vereisten voor doorgifte aan derde landen.

658 Algemene verordening gegevensbescherming, overwegingen 101 en 116.

7.1. Aard van de doorgifte van persoonsgegevens

Belangrijkste punten

- Het Unierecht en het recht van de Raad van Europa hebben regels voor doorgifte van persoonsgegevens aan ontvangers in derde landen of internationale organisaties.
- De garantie dat de rechten van betrokkenen worden veiliggesteld bij de doorgifte van gegevens buiten de EU, stelt de bescherming waarin het Unierecht voorziet in staat om de persoonsgegevens uit de EU te volgen.

In het kader van **het recht van de Raad van Europa** worden grensoverschrijdende gegevensstromen beschreven als doorgiften van persoonsgegevens aan ontvangers die onderworpen zijn aan een ander rechtsgebied[659]. Grensoverschrijdende gegevensstromen naar een ontvanger die niet onderworpen is aan het rechtsgebied van een verdragsluitende partij zijn slechts toegestaan indien er sprake is van een passend beschermingsniveau[660].

Het Unierecht regelt doorgiften van "[p]ersoonsgegevens die aan verwerking worden onderworpen of die bestemd zijn om na doorgifte naar een derde land of naar een internationale organisatie te worden verwerkt [...]"[661]. Deze gegevensstromen zijn alleen toegestaan als zij voldoen aan de voorschriften van hoofdstuk V van de AVG.

Het grensoverschrijdende verkeer van persoonsgegevens is toegelaten naar een ontvanger die valt onder het rechtsgebied van een verdragsluitende partij of een lidstaat uit hoofde van respectievelijk het recht van de Raad van Europa of het Unierecht. Beide rechtsstelsels staan ook toe dat gegevens worden overgedragen naar een land dat geen verdragsluitende partij of een lidstaat is, mits aan bepaalde voorwaarden is voldaan.

659 Memorie van toelichting bij Gemoderniseerd Verdrag 108, punt 102.

660 Gemoderniseerd Verdrag 108, artikel 14, lid 2.

661 Algemene verordening gegevensbescherming, artikel 44.

7.2. Vrij verkeer van persoonsgegevens tussen lidstaten of verdragsluitende partijen

Belangrijkste punten

- Het verkeer van persoonsgegevens in de Europese Unie, alsmede doorgiften van persoonsgegevens tussen verdragsluitende partijen bij Gemoderniseerd Verdrag 108, mogen geen beperkingen opgelegd krijgen. Aangezien echter niet alle verdragsluitende partijen bij het Gemoderniseerd Verdrag 108 lidstaten van de EU zijn, zijn doorgiften van een EU-lidstaat naar een derde land dat evenwel een verdragsluitende partij bij het Verdrag 108 is, niet mogelijk tenzij ze aan de voorwaarden in de AVG voldoen.

In het kader van het recht van de Raad van Europa moet er een vrij verkeer van persoonsgegevens bestaan tussen verdragsluitende partijen bij Gemoderniseerd Verdrag 108. De doorgifte kan echter verboden worden als er een reëel en ernstig risico bestaat dat de doorgifte aan een andere partij zou leiden tot het omzeilen van de bepalingen van het verdrag of als een partij dit moet doen volgens geharmoniseerde beschermingregels van staten die deel uitmaken van een regionale internationale organisatie[662].

In het kader van het Unierecht zijn beperkingen of verbodsbepalingen inzake het vrije verkeer van persoonsgegevens tussen EU-lidstaten verboden om redenen die verband houden met de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens[663]. **Het gebied voor het vrije verkeer van gegevens werd uitgebreid door de** Overeenkomst betreffende de Europese Economische Ruimte (EER)[664], waarbij IJsland, Liechtenstein en Noorwegen onder de interne markt vallen.

662 Gemoderniseerd Verdrag 108, artikel 14, lid 1.

663 Algemene verordening gegevensbescherming, artikel 1, lid 3.

664 Besluit van de Raad en de Commissie van 13 december 1993 betreffende de sluiting van de Overeenkomst over de Europese Economische Ruimte tussen de Europese Gemeenschappen, hun lidstaten en de Republiek Oostenrijk, de Republiek Finland, de Republiek IJsland, het Vorstendom Liechtenstein, het Koninkrijk Noorwegen, het Koninkrijk Zweden en de Zwitserse Bondsstaat, PB L 1 van 1994.

Voorbeeld: Als een onderneming die deel uitmaakt van een internationale groep van ondernemingen met vestigingen in verschillende lidstaten, waaronder Slovenië en Frankrijk, persoonsgegevens doorgeeft van Slovenië naar Frankrijk, mag dit verkeer van gegevens niet door het Sloveense nationale recht worden beperkt of verboden om redenen die verband houden met de bescherming van persoonsgegevens.

Indien evenwel dezelfde Sloveense onderneming dezelfde persoonsgegevens wenst door te geven aan de moedermaatschappij in Maleisië, dan moet de Sloveense gegevensexporteur rekening houden met de voorschriften van hoofdstuk V van de AVG. Deze bepalingen zijn bedoeld ter bescherming van de persoonsgegevens van betrokkenen die zijn onderworpen aan het gerechtsgebied van de EU.

In het kader van het Unierecht is verkeer van persoonsgegevens naar lidstaten van de EER voor doeleinden met betrekking tot de preventie, het onderzoek, het opsporen of het vervolgen van strafbare feiten of de tenuitvoerlegging van strafrechtelijke sancties onderworpen aan Richtlijn (EU) 2016/680[665]. Dit garandeert ook dat de uitwisseling van persoonsgegevens door bevoegde autoriteiten binnen de Unie niet beperkt of verboden wordt om redenen van gegevensbescherming. In het kader van het Unierecht valt de verwerking van alle persoonsgegevens (met inbegrip van het grensoverschrijdende verkeer met andere partijen bij Verdrag 108), zonder uitzonderingen gebaseerd op doelstellingen of actiegebieden, onder het toepassingsgebied van Verdrag 108, hoewel uitzonderingen gemaakt kunnen worden door de verdragsluitende partijen. Alle lidstaten van de EER zijn partij bij Verdrag 108.

665 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, PB L 119 van 2016.

7.3. Doorgifte van persoonsgegevens aan derde landen/staten die geen partij zijn of aan internationale organisaties

Belangrijkste punten

- Zowel de **Raad van Europa** als de **EU** staan de doorgifte van persoonsgegevens aan derde landen of internationale organisaties toe, mits aan bepaalde voorwaarden voor de bescherming van persoonsgegevens wordt voldaan.
  - **In het kader van het recht van de Raad van Europa** kan een passend beschermingsniveau worden bereikt door het recht van de staat of de internationale organisatie of door middel van passende normen.
  - **In het kader van het Unierecht** kunnen doorgiften plaatsvinden indien het derde land een passend beschermingsniveau biedt of indien de verwerkingsverantwoordelijke of verwerker passende garanties biedt, met inbegrip van afdwingbare rechten voor betrokkenen en rechtsmiddelen door middel van, onder andere, modelbepalingen inzake gegevensbescherming of bindende bedrijfsvoorschriften.
- **Zowel het recht van de Raad van Europa als het Unierecht** voorzien in derogatieclausules die de doorgifte van persoonsgegevens in specifieke omstandigheden toelaten, zelfs bij afwezigheid van zowel een passend beschermingsniveau als passende garanties.

Hoewel zowel het recht van de Raad van Europa als het Unierecht het verkeer van gegevens naar derde landen of naar internationale organisaties toelaten, leggen ze verschillende voorwaarden vast. Elke reeks voorwaarden houdt rekening met de verschillende structuur en doeleinden van de desbetreffende organisatie.

In het kader van het **Unierecht** bestaan er in principe twee mogelijkheden om de doorgifte van persoonsgegevens naar derde landen of internationale organisaties toe te laten. Doorgiften van persoonsgegevens kunnen plaatsvinden op basis van: een adequaatheidsbesluit door de Europese Commissie[666], of, bij gebreke van een dergelijk adequaatheidsbesluit, wanneer de verwerkingsverantwoordelijke of verwerker passende garanties biedt, met inbegrip van afdwingbare rechten en rechtsmiddelen voor de betrokkene[667]. Bij gebrek aan een adequaatheidsbesluit of passende waarborgen bestaat er een aantal derogaties.

666 Algemene verordening gegevensbescherming, artikel 45.

667 *Ibid.*, artikel 46.

In het kader van **het recht van de Raad van Europa** zijn vrije doorgiften van gegevens aan niet-verdragspartijen evenwel enkel toegestaan op basis van:

- het recht van die staat of een internationale organisatie, met inbegrip van de toepasselijke internationale verdragen of overeenkomsten die passende garanties bieden;

- ad-hoc of goedgekeurde gestandaardiseerde garanties verstrekt door juridisch bindende en afdwingbare instrumenten die werden vastgesteld en uitgevoerd door de personen die betrokken zijn in de doorgifte en de verdere verwerking[668].

Op dezelfde wijze als in het Unierecht is er, bij gebrek aan een passend beschermingsniveau van gegevens, een aantal derogaties beschikbaar.

7.3.1. Doorgifte op basis van adequaatheidsbesluiten

In het kader van het Unierecht voorziet artikel 45 van de AVG in het vrije verkeer van persoonsgegevens naar derde landen met een passend niveau van gegevensbescherming. Het HvJ-EU heeft verduidelijkt dat de term "passend niveau van bescherming" inhoudt dat het derde land een beschermingsniveau van de fundamentele rechten en vrijheden moet garanderen dat "grotendeels gelijkwaardig"[669] is aan de garanties die door het Unierecht worden gegarandeerd. Tegelijkertijd kunnen de middelen waarop een derde land beroep doet om een dergelijk beschermingsniveau te garanderen afwijken van die welke binnen de EU worden gebruikt. De adequaatheidsstandaard vereist geen punt-naar-puntherhaling van de EU-regels[670].

De Europese Commissie beoordeelt het niveau van gegevensbescherming in derde landen door te kijken naar het nationale recht en toepasselijke internationale verplichtingen. Er moet ook rekening worden gehouden met de deelname van een land in multilaterale of regionale systemen, met name met betrekking tot de bescherming van persoonsgegevens. Indien de Europese Commissie van oordeel is dat het derde land of de internationale organisatie een passend beschermingsniveau

668 Gemoderniseerd Verdrag 108, artikel 14, lid 3, onder a) en b).

669 HvJ-EU, zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner*, [Grote kamer], 6 oktober 2015, punt 96.

670 *Ibid.*, punt 74. Zie ook de Europese Commissie (2017), Mededeling van de Commissie aan het Europees Parlement en de Raad — Uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld, COM(2017)7 def. van 10 januari 2017, blz. 6.

garandeert, kan ze een adequaatheidsbesluit uitgeven, dat een bindend gevolg heeft[671]. Niettemin heeft het HvJ-EU verklaard dat nationale toezichthoudende autoriteiten nog steeds de bevoegdheid hebben om de vordering van een persoon met betrekking tot de bescherming van zijn persoonsgegevens die werden doorgegeven aan een derde land waarvan de Commissie acht dat het een passend beschermingsniveau heeft, te onderzoeken indien die persoon beweert dat de geldende wet en praktijken in dat derde land geen passend beschermingsniveau garanderen[672].

De Europese Commissie kan ook de adequaatheid van een gebied in een derde land beoordelen of zich beperken tot specifieke sectoren, zoals het geval was voor de Canadese particuliere handelswetgeving bijvoorbeeld[673]. Er zijn ook adequaatheidsbesluiten voor overdrachten die gebaseerd zijn op overeenkomsten tussen de EU en derde landen. Deze besluiten hebben uitsluitend betrekking op één enkel type doorgifte van gegevens, zoals de doorgifte van passagiersgegevens (Passenger Name Records — PNR) door luchtvaartmaatschappijen aan grenscontroleautoriteiten van derde landen wanneer de vlucht wordt gemaakt van de EU naar bepaalde overzeese bestemmingen (zie paragraaf 7.3.4).

Adequaatheidsbesluiten zijn onderworpen aan doorlopend toezicht. De Europese Commissie evalueert deze besluiten regelmatig om ontwikkelingen die gevolgen kunnen hebben voor hun status, op te volgen. Indien de Europese Commissie dus vaststelt dat het derde land of de internationale organisatie niet langer aan de voorwaarden voldoet die het adequaatheidsbesluit rechtvaardigen, kan ze het besluit wijzigen, opschorten of intrekken. Voorts kan de Commissie onderhandelen met het betrokken derde land of de betrokken internationale organisatie om het probleem waarop haar beslissing is gebaseerd, op te lossen.

De adequaatheidsbesluiten die de Europese Commissie op grond van Richtlijn 95/46/EG heeft vastgesteld, blijven van kracht, totdat zij worden gewijzigd, vervangen of ingetrokken door een besluit van de Commissie dat wordt vastgesteld overeenkomstig de regels in artikel 45 van de AVG.

---

671 Voor een voortdurend geactualiseerde lijst van landen waarvoor een positieve bevinding is afgegeven, zie de homepage van de Europese Commissie, directoraat-generaal Justitie.

672 HvJ-EU, zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer], 6 oktober 2015, punten 63 en 65-66.

673 Europese Commissie (2002), Beschikking 2002/2/EG van 20 december 2001 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming van persoonsgegevens geboden door de Canadese Personal Information and Electronic Documents Act, PB L 2 van 2002.

Tot nu toe heeft de Europese Commissie Andorra, Argentinië, Canada (commerciële organisaties die vallen onder het toepassingsgebied van de Personal Information and Electronic Documents Act — PIPEDA), Faeröer, Guernsey, Isle of Man, Israël, Jersey, Nieuw-Zeeland, Zwitserland en Uruguay erkend als landen die een passende bescherming bieden. Met betrekking tot de doorgifte naar de VS, heeft de Europese Commissie in 2000 een gepastheidsbeschikking vastgesteld die de doorgifte toestond naar bedrijven die middels zelfcertificering verklaarden dat zij vanuit de EU doorgegeven persoonsgegevens zouden beschermen en dat zij de veiligehavenbeginselen zouden naleven[674]. Het HvJ-EU verklaarde dit besluit ongeldig in 2015 en een nieuw adequaatheidsbesluit werd aangenomen in juli 2016, waardoor ondernemingen konden toetreden met ingang van 1 augustus 2016.

Voorbeeld: In *Schrems*[675] was Maximillian Schrems, een Oostenrijkse staatsburger, al sinds jaren een gebruiker van Facebook. Sommige of alle gegevens die de heer Schrems aan Facebook gaf, werden door de Ierse dochteronderneming van Facebook overgeheveld naar servers in de VS, waar ze werden verwerkt. De heer Schrems diende een klacht in bij de Ierse autoriteit voor gegevensbescherming, omdat hij van oordeel was dat, in het licht van de onthullingen van de Amerikaanse klokkenluider Edward Snowden over de bewakingsactiviteiten van de Amerikaanse inlichtingendiensten, de Amerikaanse wetgeving en gangbare praktijken niet voldoende bescherming bieden van de gegevens die aan dat land worden doorgegeven. De Ierse autoriteit wees de klacht af op grond van het feit dat de Commissie in haar beschikking van 26 juli 2000 van oordeel was dat in het kader van de veiligehavenregeling de VS een passend beschermingsniveau voor de doorgegeven persoonsgegevens garandeerde. De zaak werd aanhangig gemaakt bij het Ierse Hooggerechtshof, die de zaak naar het HvJ-EU verwees voor een prejudiciële beslissing.

674 Beschikking 2000/520/EG van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende Vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd, PB L 215. De beschikking werd ongeldig verklaard door het HvJ-EU in zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer].

675 HvJ-EU, zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer], 6 oktober 2015.

Het HvJ-EU besliste dat de beschikking van de Commissie over de gepastheid van de veiligehavenregeling ongeldig was. Ten eerste merkte het HvJ-EU op dat de beschikking toeliet dat de toepasbaarheid van de Veiligehavenbeginselen inzake gegevensbescherming beperkt kan worden op basis van nationale veiligheid, openbaar belang of rechtshandhaving of op basis van de nationale VS-wetgeving. Het besluit liet derhalve interferentie toe met de fundamentele rechten van die personen van wie persoonsgegevens waren of konden worden overgedragen aan de VS[676]. Het wees er verder op dat het besluit geen bevindingen bevatte over bestaande regels in de VS die dergelijke interferentie dienen te beperken, noch over het bestaan van een doeltreffende wettelijke bescherming tegen dergelijke interferentie[677]. Het HvJ-EU benadrukte dat het beschermingsniveau van de fundamentele rechten en vrijheden die in de EU worden gegarandeerd, vereiste dat wetgevingen die leiden tot aantasting van artikelen 7 en 8, duidelijke en nauwkeurige regels vaststellen die de reikwijdte en toepassing van een maatregel bepaalt en minimale garanties, derogaties en beperkingen met betrekking tot de bescherming van persoonsgegevens opleggen[678]. Gezien het feit dat het besluit van de Commissie niet stelde dat de VS in feite een dergelijk beschermingsniveau garandeert door middel van zijn nationale wetgeving of zijn internationale verbintenissen, oordeelde het HvJ-EU dat het niet voldeed aan de vereisten van het desbetreffende kettingbeding in de richtlijn inzake gegevensbescherming, en werd derhalve nietig verklaard[679].

Het beschermingsniveau van de VS was dus niet "grotendeels gelijkwaardig" aan de fundamentele rechten en vrijheden die door de EU worden gegarandeerd[680]. Het HvJ-EU stelde dat verscheidene artikelen van het Handvest van de grondrechten van de EU waren geschonden. Ten eerste kwam de essentie van artikel 7 in het gedrang, aangezien in de VS-wetgeving "de autoriteiten veralgemeend toegang kunnen krijgen tot de inhoud van elektronische communicatie". Ten tweede werd ook de essentie van artikel 47 geschonden, aangezien de wetgeving geen rechtsmiddelen ter beschikking stelde van natuurlijke personen met betrekking tot de toegang tot persoonsgegevens of de rectificatie of wissing van persoonsgegevens.

676 *Ibid.*, punt 84.

677 *Ibid.*, punten 88-89.

678 *Ibid.*, punten 91-92.

679 *Ibid.*, punten 96-97.

680 *Ibid.*, punten 73-74 en 96.

Ten slotte, gezien het feit dat de veiligehavenregeling de bovengenoemde artikelen had geschonden, werden persoonsgegevens niet langer rechtmatig verwerkt, hetgeen resulteert in een schending van artikel 8.

Nadat het HvJ-EU de veiligehavenregeling nietig had verklaard, bereikten de Commissie en de VS overeenstemming over een nieuw kader, het EU-VS-privacyschild. Op 12 juli 2016 stelde de Commissie een besluit vast dat verklaart dat de VS een passend beschermingsniveau garandeert voor persoonsgegevens die van de Unie naar organisaties in de VS worden doorgegeven in het kader van het EU-VS-privacyschild[681].

Net als bij de veiligehavenregeling heeft het EU-VS-privacyschild als doel persoonsgegevens te beschermen die voor commerciële doeleinden van de EU naar de VS worden doorgegeven[682]. Amerikaanse ondernemingen kunnen zelf vrijwillig hun toetreding tot de privacyschildlijst certificeren door zich ertoe te verbinden aan de desbetreffende normen inzake gegevensbescherming te voldoen. De bevoegde Amerikaanse autoriteiten controleren en verifiëren of de gecertificeerde ondernemingen deze standaarden naleven.

De privacyschildregeling voorziet in het bijzonder in:

- verplichtingen inzake gegevensbescherming voor ondernemingen die persoonsgegevens uit de EU ontvangen;

- bescherming en schadeloosstelling voor natuurlijke personen, met name de oprichting van een ombudsman die onafhankelijk is van de Amerikaanse inlichtingendiensten en klachten oplost van individuen die menen dat hun persoonsgegevens op een onrechtmatige wijze door de Amerikaanse autoriteiten op het gebied van nationale veiligheid werden gebruikt;

681 Uitvoeringsverordening (EU) 2016/1250 van de Commissie van 12 juli 2016 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming, PB L 207. Groep artikel 29 was ingenomen met de verbeteringen van het privacyschildmechanisme ten opzichte van de veiligehavenbeschikking en prees de Commissie en de VS-autoriteiten, omdat in de definitieve versie van de privacyschilddocumenten rekening was gehouden met de bezwaren die de groep had geuit in hun advies WP 238 over het ontwerpbesluit over de gepastheid van het EU-VS-privacyschild. Toch wees de groep op een aantal openstaande bezwaren. Voor meer details, zie *Advies 01/2016 inzake het ontwerpbesluit over de adequaatheid van het EU-VS-privacyschild* van Groep artikel 29, aangenomen op 13 april 2016, 16/EN WP 238.

682 Voor meer informatie, zie de EU-VS-privacyschild factsheet.

- een jaarlijkse gezamenlijke evaluatie om de uitvoering van het kader op te volgen[683]; de eerste evaluatie vond plaats in september 2017[684].

De Amerikaanse overheid heeft schriftelijke verbintenissen en garanties opgesteld die bij het privacyschildbesluit horen. Deze bieden beperkingen en waarborgen voor de toegang tot persoonsgegevens van de Amerikaanse overheid voor de rechtshandhaving en de nationale veiligheid.

7.3.2. Doorgifte onderworpen aan passende waarborgen

Zowel in het **Unierecht** als in het **recht van de Raad van Europa** worden passende waarborgen tussen de gegevensuitvoerende verwerkingsverantwoordelijke en de ontvanger in het derde land of de internationale organisatie erkend als een mogelijke manier om ervoor te zorgen dat een toereikend niveau van gegevensbescherming voor de ontvanger wordt gegarandeerd.

In het kader van het **Unierecht** zijn doorgiften van persoonsgegevens aan een derde land of een internationale organisatie toegestaan indien de verwerkingsverantwoordelijke of verwerker in passende waarborgen en afdwingbare rechten voorziet en indien er doeltreffende rechtsmiddelen ter beschikking worden gesteld aan de betrokkenen[685]. De lijst van aanvaardbare "passende waarborgen" wordt uitsluitend in de EU-wetgeving inzake gegevensbescherming verstrekt. Passende waarborgen kunnen worden vastgesteld door:

- een juridisch bindend en afdwingbaar instrument tussen overheidsinstanties of -organen;
- bindende bedrijfsvoorschriften;
- standaardbepalingen inzake gegevensbescherming die zijn vastgesteld door de Europese Commissie of door een toezichthoudende autoriteit;

683 Voor meer informatie, zie de webpagina van de Europese Commissie over het EU-VS-privacyschild.

684 Europese Commissie, Verslag van de Commissie aan het Europees Parlement en de Raad betreffende de eerste jaarlijkse evaluatie van de werking van het EU-VS-privacyschild, COM(2017)611 def., 18 oktober 2017

685 Algemene verordening gegevensbescherming, artikel 46.

- gedragscodes;
- certificeringsmechanismen[686].

Op maat gemaakte contractbepalingen tussen de verwerkingsverantwoordelijke of de verwerker in de EU en de ontvanger van de gegevens in een derde land zijn een ander middel voor het verstrekken van passende waarborgen. Dergelijke contractuele bepalingen moeten echter worden toegestaan door de bevoegde toezichthoudende autoriteit voordat zij kunnen worden gebruikt als instrument voor de doorgifte van persoonsgegevens. Op soortgelijke wijze kunnen overheden gebruik maken van bepalingen inzake gegevensbescherming die in hun administratieve regelingen zijn opgenomen, zolang ze door de toezichthoudende autoriteit zijn goedgekeurd[687].

In het kader van het recht van de Raad van Europa zijn gegevensstromen naar staten of internationale organisaties toegestaan die geen partij zijn bij het Gemoderniseerd Verdrag 108, op voorwaarde dat een passend beschermingsniveau wordt gewaarborgd. Dit kan worden bereikt door:

- het recht van de staat of een internationale organisatie, of
- ad-hoc of gestandaardiseerde waarborgen die in een juridisch bindend document zijn ingebouwd[688].

Doorgifte onderworpen aan contractbepalingen

Zowel het **recht van de Raad van Europa** als het **Unierecht** erkennen contractbepalingen tussen de gegevensuitvoerende verwerkingsverantwoordelijke en de ontvanger in het derde land als een mogelijk middel om een voldoende niveau van gegevensbescherming voor de ontvanger te waarborgen[689].

Op **EU-niveau** heeft de Europese Commissie, met ondersteuning van Groep artikel 29, modelbepalingen inzake gegevensbescherming ontwikkeld die officieel zijn

686 Algemene verordening gegevensbescherming, artikel 46, lid 1, onder c), d), lid 2, onder a), b), e), f) en artikel 47.

687 *Ibid.*, artikel 46, lid 3.

688 Gemoderniseerd Verdrag 108, artikel 14, lid 3, onder b).

689 Algemene richtlijn inzake gegevensbescherming, artikel 46, lid 3; Gemoderniseerd Verdrag 108, artikel 14, lid 3, onder b).

gecertificeerd door een besluit van de Commissie als bewijs voor een passende gegevensbescherming[690]. Aangezien besluiten van de Commissie in al hun onderdelen verbindend zijn voor de lidstaten, moeten de nationale autoriteiten die belast zijn met het toezicht op doorgifte van gegevens, deze standaardcontractbepalingen in hun procedures toepassen[691]. Als de gegevensuitvoerende verwerkingsverantwoordelijke en de ontvanger in het derde land overeenstemming bereiken en deze bepalingen ondertekenen, zou dit voor de toezichthoudende autoriteit voldoende bewijs moeten zijn dat voor passende waarborgen is gezorgd. Maar in de zaak *Schrems* oordeelde het HvJ-EU dat de Europese Commissie niet de bevoegdheid heeft om de bevoegdheden van de nationale toezichthoudende autoriteiten te beperken teneinde toe te zien op de doorgifte van persoonsgegevens aan een derde land dat het onderwerp is geweest van een adequaatheidsbesluit van de Commissie[692]. Daarom worden de nationale toezichthoudende autoriteiten niet belet hun bevoegdheden uit te voeren, met inbegrip van de bevoegdheid om een doorgifte van persoonsgegevens op te schorten of te verbieden wanneer de doorgifte een inbreuk vormt op de nationale of EU-wetgeving inzake gegevensbescherming, bijvoorbeeld wanneer de gegevensimporteur de standaardcontractbepalingen niet naleeft[693].

Het bestaan van modelbepalingen inzake gegevensbescherming in het rechtskader van de EU weerhoudt verwerkingsverantwoordelijken er niet van om andere ad hoc, individuele contractbepalingen te formuleren, zolang de toezichthoudende autoriteit met deze bepalingen heeft ingestemd[694]. Ze moeten echter hetzelfde beschermingsniveau als de standaardbepalingen inzake gegevensbescherming waarborgen. Bij de goedkeuring van ad-hocbepalingen moeten toezichthoudende autoriteiten de conformiteitstoetsing toepassen teneinde te zorgen voor een consistente regelgevende aanpak in de EU[695]. Dit betekent dat de bevoegde toezichthoudende autoriteit zijn ontwerpbesluit betreffende de bepalingen aan het

690 *Ibid.*, artikel 46, lid 2, onder b), en artikel 46, lid 5.

691 *Ibid.*, artikel 46, lid 3; Ad-hoccommissie voor gegevensbescherming (CAHDATA), memorie van toelichting bij het Gemoderniseerd Verdrag voor de bescherming van personen met betrekking tot de automatische verwerking van persoonsgegevens, punt 105.

692 HvJ-EU, zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer], 6 oktober 2015, punten 96-98 en 102-105.

693 Om rekening te houden met het standpunt van het HvJ-EU in de zaak *Schrems*, wijzigde de Commissie haar besluit over standaardcontractbepalingen. Uitvoeringsbesluit (EU) 2016/2297 van de Commissie van 16 december 2016 tot wijziging van Besluit 2001/497/EG en Besluit 2010/87/EU betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen en aan in derde landen gevestigde verwerkers, krachtens Richtlijn 95/46/EG van het Europees Parlement en de Raad, PB L 344 van 2016.

694 Algemene verordening gegevensbescherming, artikel 46, lid 3, onder a).

695 *Ibid.*, artikel 63 en artikel 64, lid 1, onder e).

Europees Comité voor gegevensbescherming (EDPB) moet doorgeven. Het EDPB zal een advies over de zaak geven en de toezichthoudende autoriteit moet zoveel mogelijk rekening houden met dit advies bij het nemen van haar besluit. Indien zij niet voornemens is om het advies van het EDPB te volgen, wordt het geschillenbeslechtingsmechanisme van het EDPB geactiveerd en zal het Comité een bindend besluit nemen[696].

De belangrijkste kenmerken van een standaardcontractbepaling zijn de volgende:

- een derdenbeding dat betrokkenen in staat stelt om contractuele rechten uit te oefenen, ook als ze geen partij bij het contract zijn;

- de ontvanger of importeur van de gegevens stemt ermee in om in geval van een geschil te worden onderworpen aan het gezag van de toezichthoudende autoriteit en/of de bevoegde rechtbanken van de verwerkingsverantwoordelijke die de gegevens exporteert.

Er zijn nu voor doorgiften tussen verwerkingsverantwoordelijken twee reeksen standaardcontractbepalingen beschikbaar waaruit de gegevensuitvoerende verwerkingsverantwoordelijke kan kiezen[697]. Voor overdrachten van verwerkingsverantwoordelijke naar verwerker bestaat er slechts één reeks standaardcontractbepalingen[698]. Deze standaardcontractbepalingen zijn momenteel echter het onderwerp van een gerechtelijke procedure.

696 *Ibid.*, artikel 64 en artikel 65.

697 Reeks I is opgenomen in de bijlage bij de Europese Commissie (2001), Beschikking 2001/497/EG van 15 juni 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan derde landen krachtens Richtlijn 95/46/EG, PB L 181 van 2001; Reeks II is opgenomen in de bijlage bij de Europese Commissie (2004), Besluit 2004/915/EG van 27 december 2004 tot wijziging van Besluit 2001/497/EG betreffende de invoering van een reeks alternatieve modelcontractbepalingen voor de doorgifte van persoonsgegevens aan derde landen, PB L 385 van 2004.

698 Europese Commissie (2010), Besluit 2010/87 van de Commissie van 5 februari 2010 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG van het Europees Parlement en de Raad, PB L 39 van 2010. Ten tijde van de opstelling van het handboek was het gebruik van modelcontractbepalingen voor de doorgifte van persoonsgegevens aan de VS het onderwerp van een juridische procedure voor het Ierse Hooggerechtshof.

Voorbeeld: Nadat het HvJ-EU de veiligehavenbeschikking nietig had verklaard[699], kon de doorgifte van persoonsgegevens aan de VS niet langer gebeuren op basis van die gepastheidsbeschikking. Terwijl de onderhandelingen met de Amerikaanse autoriteiten gaande waren en in afwachting van de vaststelling van een nieuw adequaatheidsbesluit (dat uiteindelijk op 12 juli 2016 werd aangenomen)[700], konden doorgiften enkel plaatsvinden op andere rechtsgrondslagen zoals standaardcontractbepalingen of bindende bedrijfsvoorschriften. Verschillende bedrijven, waaronder Facebook Ireland (tegen wie de zaak aanhangig was gemaakt die tot de nietigverklaring van de veiligehavenbeschikking zou leiden), schakelden over op standaardcontractbepalingen om hun EU-VS-doorgifte van gegevens voort te zetten.

De heer Schrems diende een klacht in bij de Ierse toezichthoudende autoriteit met het verzoek om de doorgifte van gegevens aan de VS op basis van standaardcontractbepalingen op te schorten. In wezen voerde hij aan dat bij de doorgifte van zijn persoonlijke gegevens van de Ierse dochteronderneming van Facebook naar Facebook Inc. en servers in de Verenigde Staten, er geen garantie bestond dat die gegevens zouden worden beschermd. Facebook Inc. is gebonden door het Amerikaanse recht dat hem kan verplichten om persoonsgegevens te verstrekken aan Amerikaanse wetshandhavingsinstanties en er bestaat geen beschikbaar rechtsmiddel voor Europese personen om deze praktijk te betwisten[701]. Om deze redenen heeft het HvJ-EU de veiligehavenbeschikking nietig verklaard, en hoewel het arrest van de rechtbank zich beperkte tot het onderzoeken van die beschikking, achtte de verzoeker de aan de orde gestelde punten even relevant bij op contractbepalingen gebaseerde doorgiften. Op het moment waarop dit handboek werd geschreven, werd de zaak onderzocht door het Ierse Hooggerechtshof. De verzoeker is kennelijk voornemens de zaak bij het HvJ-EU aanhangig te maken om de geldigheid van het besluit van de

699 HvJ-EU, zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner*, [Grote kamer], 6 oktober 2015.

700 Uitvoeringsbesluit van de Commissie (EU) 2016/1250 van 12 juli 2016 ingevolge Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door het EU-VS-privacyschild, PB L 207.

701 Voor meer informatie, zie de herziene klacht van de Ierse commissaris voor gegevensbescherming tegen Facebook Ireland Ltd en Maximillian Schrems op 1 december 2015.

Europese Commissie over standaardcontractbepalingen aan te vechten. Zoals beschreven in hoofdstuk 5 heeft enkel het HvJ-EU de bevoegdheid om een EU-instrument ongeldig te verklaren.

Doorgifte onderworpen aan bindende bedrijfsvoorschriften

Het **Unierecht** laat ook doorgiften van persoonsgegevens toe op basis van bindende bedrijfsvoorschriften voor internationale doorgiften die plaatsvinden binnen dezelfde groep ondernemingen of bedrijven die deel uitmaken van een gezamenlijke economische activiteit[702]. Voordat bindende bedrijfsvoorschriften kunnen worden gebruikt als een instrument voor de doorgifte van persoonsgegevens, moeten ze worden goedgekeurd door de bevoegde toezichthoudende autoriteit, in overeenstemming met bindende bedrijfsvoorschriften en waarbij gebruik wordt gemaakt van het coherentiemechanisme.

Om te worden goedgekeurd moeten bindende bedrijfsvoorschriften juridisch bindend zijn, alle essentiële beginselen inzake gegevensbescherming beslaan en van toepassing zijn op, en worden gehandhaafd door, elk lid van de groep. Ze moeten uitdrukkelijk afdwingbare rechten verlenen aan betrokkenen, alle essentiële beginselen inzake gegevensbescherming beslaan en voldoen aan bepaalde formele vereisten, zoals het vermelden van de structuur van de onderneming, het beschrijven van de doorgiften en hoe de beginselen inzake gegevensbescherming zullen worden toegepast. Dit omvat het verstrekken van dergelijke informatie aan betrokkenen. Bindende bedrijfsvoorschriften moeten, onder andere, de rechten en bepalingen inzake de aansprakelijkheid van betrokkenen vermelden bij elke inbreuk op de regels[703]. Bij de goedkeuring van bindende bedrijfsvoorschriften wordt de conformiteitstoetsing voor de samenwerking tussen toezichthoudende autoriteiten (beschreven in hoofdstuk 5) geactiveerd.

In het kader van de conformiteitstoetsing evalueert de toezichthoudende autoriteit die de leiding heeft, de voorgestelde bindende bedrijfsvoorschriften, stelt een ontwerpbesluit vast en deelt deze mee aan het EDPB. Het Comité brengt een advies uit over de kwestie en de toezichthoudende autoriteit die de leiding heeft, kan formeel de bindende bedrijfsvoorschriften vaststellen, terwijl ze zoveel mogelijk rekening houdt met het advies van het Comité. Dit advies is juridisch niet bindend, maar indien de toezichthoudende autoriteit voornemens is om geen rekening te houden

702 Algemene verordening gegevensbescherming, artikel 47.

703 Voor een meer gedetailleerde beschrijving, zie algemene verordening gegevensbescherming, artikel 47.

met het advies, wordt het geschillenbeslechtingsmechanisme geactiveerd en zal het Comité een juridisch bindende beslissing moeten nemen met een tweederde meerderheid van zijn leden[704].

In het kader van **het recht van de Raad van Europa** bevatten de ad-hoc of gestandaardiseerde waarborgen, die verankerd zijn in een juridisch bindend document[705], ook bindende bedrijfsvoorschriften.

7.3.3. Derogaties voor specifieke situaties

In het kader van het Unierecht kunnen doorgiften van persoonsgegevens aan een derde land worden gerechtvaardigd, zelfs indien er geen adequaatheidsbeslissing of waarborgen zijn, zoals standaardcontractbepalingen of bindende bedrijfsvoorschriften, in een van de volgende omstandigheden:

- de betrokkene geeft uitdrukkelijk toestemming voor de doorgifte van gegevens;
- de betrokkene sluit een contract af, of is voornemens een contract af te sluiten, waarbij de doorgifte van gegevens aan het buitenland noodzakelijk is;
- bij het afsluiten van een contract tussen een verwerkingsverantwoordelijke en een derde partij in het belang van de betrokkene;
- om gewichtige redenen van algemeen belang;
- voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- ter bescherming van de vitale belangen van de betrokkene;
- voor de doorgifte van gegevens uit openbare registers (dit is een geval van doorslaggevend algemeen belang om toegang te krijgen tot informatie die in openbare registers is opgeslagen)[706].

704 *Ibid.*, artikel 57, lid 1, onder s), artikel 58, lid 1, onder j), artikel 64, lid 1, onder f), artikel 65, leden 1 en 2.

705 Gemoderniseerd Verdrag 108, artikel 14, lid 3, onder b).

706 Algemene verordening gegevensbescherming, artikel 49.

Indien geen van deze voorwaarden kan worden toegepast en indien de doorgifte niet kan worden gebaseerd op een adequaatheidsbesluit of passende waarborgen, mag een doorgifte enkel plaatsvinden indien deze niet wordt herhaald, een beperkt aantal betrokkenen betreft en nodig is voor de toepassing van de dwingende gerechtvaardigde belangen van de verwerkingsverantwoordelijke, op voorwaarde dat de rechten van de betrokkene hier geen voorrang op hebben[707]. In deze gevallen moet de verwerkingsverantwoordelijke de omstandigheden rond de overdracht evalueren en in waarborgen voorzien. Verder moeten de toezichthoudende autoriteit en de betrokkenen in kennis worden gesteld van zowel de doorgifte als de rechtmatige belangen die de doorgifte rechtvaardigen.

Het feit dat derogaties een laatste redmiddel vormen voor rechtmatige doorgiften[708] (die enkel kunnen worden gebruikt bij gebrek aan een adequaatheidsbesluit of indien er geen andere waarborgen zijn), benadrukt hun uitzonderlijke aard, en dit wordt verder onderstreept in de overwegingen van de AVG. Derogaties worden als zodanig aanvaard om doorgiften "in bepaalde gevallen" mogelijk te maken op basis van toestemming en wanneer "de doorgifte incidenteel en noodzakelijk is"[709] in het kader van een overeenkomst of van een rechtsvordering.

Daarnaast moet, volgens de richtsnoeren van Groep artikel 29, het gebruik van derogaties voor specifieke situaties uitzonderlijk zijn, gebaseerd op individuele zaken, en kunnen ze niet worden gebruikt voor grootschalige of repetitieve doorgiften[710]. De Europese Toezichthouder voor gegevensbescherming benadrukt ook het uitzonderlijke karakter van derogaties als rechtsgrond voor overdrachten onder Verordening (EU) nr. 45/2001 en merkt op dat deze oplossing "in een beperkt aantal gevallen" en "voor incidentele overdrachten" moet worden gebruikt[711].

Voorbeeld: Een dienstverlenend bedrijf op het gebied van Global Distribution Systems (GDS) met hoofdkantoor in de VS, beheert het online reserveringssysteem voor meerdere luchtvaartmaatschappijen, hotels en cruises over de hele wereld en verwerkt de gegevens van tientallen

707 *Ibid.*

708 *Ibid.*, artikel 49, lid 1.

709 *Ibid.*

710 Groep artikel 29 (2005), *Werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995*, WP 114, Brussel, 25 november 2005.

711 Europese Toezichthouder voor gegevensbescherming, *De overdracht van persoonsgegevens naar derde landen en internationale organisaties door EU-instellingen en -organen*, standpuntnota, Brussel, 14 juli 2014, blz. 15.

miljoenen mensen in de EU. Voor de aanvankelijke overdracht van gegevens naar hun servers in de VS, baseerde het GDS-bedrijf zich op een derogatie als een rechtmatige basis voor doorgiften, aangezien dit nodig was om een overeenkomst af te sluiten. Het voert dus geen andere waarborgen aan voor de persoonsgegevens die uit Europa komen, aan de VS worden overgedragen en vervolgens herverdeeld worden in hotels over de hele wereld (dit wil zeggen dat er ook geen waarborgen bestaan voor de verdere doorgifte). Het GDS-bedrijf komt de vereiste voor rechtmatige internationale doorgifte van gegevens uit de AVG niet na, omdat het zich baseert op een derogatie als rechtmatige grond voor grootschalige doorgifte.

Tenzij een adequaatheidsbeslissing wordt ingesteld, zijn de EU of de lidstaten bevoegd om de doorgifte van specifieke categorieën persoonsgegevens naar een derde land te beperken, ondanks het feit dat werd voldaan aan andere voorwaarden voor zulke doorgiften, om belangrijke redenen van algemeen belang. Deze limieten moeten als uitzonderlijk worden beschouwd en lidstaten moeten de relevante bepalingen aan de Commissie meedelen[712].

Het **recht van de Raad van Europa** staat gegevensstromen naar gebieden die geen passende gegevensbescherming hebben toe, in het geval dat:

- de betrokkene zijn toestemming heeft verleend;
- het belang van de betrokkene een dergelijke doorgifte vereist;
- er prevalerende gerechtvaardigde belangen zijn, met name zwaarwegende algemene belangen, bepaald bij wet;
- dit een noodzaak en een evenredige maatregel vormt in een democratische samenleving[713].

712 Algemene verordening gegevensbescherming, artikel 49, lid 5.

713 Gemoderniseerd Verdrag 108, artikel 14, lid 4.

7.3.4. Doorgiften op basis van internationale overeenkomsten

De Europese Unie kan internationale overeenkomsten sluiten met derde landen inzake de doorgifte van persoonsgegevens voor specifieke doeleinden. Deze overeenkomsten moeten passende waarborgen bevatten om te zorgen voor de bescherming van de persoonsgegevens van de betrokken personen. De AVG bestaat zonder afbreuk te doen aan deze internationale overeenkomsten[714].

De lidstaten kunnen ook internationale overeenkomsten met derde landen of internationale organisaties afsluiten die een passend niveau van bescherming van de fundamentele rechten en vrijheden van natuurlijke personen bevatten, voor zover deze overeenkomsten geen afbreuk doen aan de toepassing van de AVG.

Een soortgelijke regel is voorzien in artikel 12, lid 3, onder a), van Gemoderniseerd Verdrag 108.

Voorbeelden van internationale overeenkomsten die de overdracht van persoonsgegevens met zich meebrengen zijn de PNR-overeenkomsten.

Persoonsgegevens van passagiers

Persoonsgegevens van passagiers (Passenger Name Records — PNR) worden verzameld door luchtvaartmaatschappijen tijdens het reserveringsproces van de vlucht en omvatten, onder andere, de namen, adressen, creditcardgegevens en stoelnummers van passagiers. Luchtvaartmaatschappijen verzamelen deze informatie ook voor hun eigen commerciële doeleinden. De Europese Unie heeft overeenkomsten gesloten met bepaalde derde landen (Australië, Canada en de VS) voor de doorgifte van PNR-gegevens om terroristische misdrijven of ernstige grensoverschrijdende criminaliteit te voorkomen, op te sporen, te onderzoeken en te vervolgen. Daarnaast stelde de Unie in 2016 Richtlijn (EU) 2016/861 in, bekend als de EU-PNR-richtlijn[715]. Deze richtlijn voorziet in een wettelijk kader voor EU-lidstaten voor de doorgifte van PNR-gegevens aan de bevoegde autoriteiten in andere derde landen om op vergelijkbare wijze terroristische misdrijven en ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken of te vervolgen. PNR-doorgiften aan de autoriteiten van

714 Algemene verordening gegevensbescherming, overweging 102.

715 Richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, PB L 119 van 2016.

derde landen worden per geval bekeken en zijn onderworpen aan een individuele beoordeling van de vraag of de doorgifte noodzakelijk is voor de toepassing van deze richtlijn en op voorwaarde dat de grondrechten in acht worden genomen.

Met betrekking tot de PNR-overeenkomsten tussen de Europese Unie en derde landen, werd hun verenigbaarheid met de grondrechten op privacy en gegevensbescherming die zijn vastgelegd in het EU-Handvest van grondrechten, betwist. Toen, na onderhandelingen met Canada, de EU een overeenkomst tekende betreffende de doorgifte en verwerking van PNR-gegevens in 2014, besloot het Europees Parlement om de zaak voor te leggen aan het HvJ-EU om de wettigheid van de overeenkomst met de EU-wetgeving, en met name met de artikelen 7 en 8 van het Handvest, te beoordelen.

Voorbeeld: In zijn advies over de wettigheid van de PNR-overeenkomst tussen de EU en Canada[716] oordeelde het HvJ-EU dat de overeenkomst in zijn huidige vorm onverenigbaar was met de grondrechten die het Handvest erkende, en daarom niet kon worden gesloten. Aangezien het ging om de verwerking van persoonsgegevens, vormde het een aantasting van het recht op bescherming van persoonsgegevens die worden beschermd onder artikel 8 van het Handvest. Tegelijkertijd vormt het ook een beperking op het recht op de eerbiediging van het privéleven, zoals neergelegd in artikel 7, gezien het feit dat, in zijn geheel, PNR-gegevens mogen worden samengevoegd en geanalyseerd op een wijze waaruit reisgewoontes, relaties tussen verschillende natuurlijke personen, informatie over hun financiële situatie, eetgewoonten en de gezondheidssituatie blijkt, waardoor er afbreuk wordt gedaan aan hun persoonlijke levenssfeer.

De aantasting van de grondrechten die de voorgenomen overeenkomst met zich meebracht, streefde een doelstelling na van algemeen belang, met name de openbare veiligheid en de strijd tegen terrorisme en ernstige grensoverschrijdende criminaliteit. Het HvJ-EU herinnerde er echter aan dat de aantasting tot het strikt noodzakelijke beperkt moet blijven om de nagestreefde doelstelling te verwezenlijken. Na bestudering van de bepalingen, besloot het HvJ-EU dat de voorgenomen overeenkomst niet voldeed aan het "strikt noodzakelijke" criterium. De factoren die het HvJ-EU beoordeelde om tot deze conclusie te komen waren, onder andere:

716 HvJ-EU, *Advies 1/15 van het Hof (Grote kamer)*, 26 juli 2017.

- Het feit dat de voorgenomen overeenkomst de doorgifte van gevoelige gegevens inhield. De PNR-gegevens verzameld op grond van de voorgenomen overeenkomst kunnen gevoelige gegevens bevatten, zoals gegevens waaruit de raciale of etnische afkomst, de godsdienstige overtuiging, of de gezondheidstoestand van een passagier blijken. De doorgifte en verwerking van gevoelige gegevens door de Canadese autoriteiten kan een risico inhouden voor het beginsel van non-discriminatie en dus een precieze en gedegen rechtvaardiging vereisen die gebaseerd is op andere gronden dan openbare veiligheid en de strijd tegen ernstige criminaliteit. De voorgenomen overeenkomst bevatte een dergelijke rechtvaardiging niet[717].

- Het feit dat de PNR-gegevens van alle passagiers opgeslagen zouden blijven voor een periode van vijf jaar, zelfs nadat de passagiers zijn vertrokken uit Canada, werd ook gezien als een overschrijding van de limieten van het strikt noodzakelijke. Het HvJ-EU oordeelde dat het toegestaan zou zijn voor de Canadese autoriteiten om de gegevens te bewaren van passagiers waarvan objectieve bewijzen aantonen dat ze een gevaar voor de openbare veiligheid kunnen vormen, zelfs nadat deze personen uit Canada zijn vertrokken. De opslag van persoonsgegevens van *alle* passagiers daarentegen, voor wie er zelfs geen indirect bewijs bestaat dat ze een risico vormen voor de openbare veiligheid, is niet gerechtvaardigd[718].

Het Raadgevend Comité voor Verdrag 108 heeft een advies uitgebracht over de gevolgen voor gegevensbescherming van PNR-overeenkomsten in het kader van het recht van de Raad van Europa[719].

Berichtenverkeer

De in België gevestigde Society for Worldwide Interbank Financial Telecommunication (SWIFT), die de verwerker is voor het grootste deel van de wereldwijde geldovermakingen door Europese banken, werkte met een gelijkaardig centrum in de VS en werd geconfronteerd met het verzoek om gegevens te verstrekken aan

717 *Ibid.*, punt 165.

718 *Ibid.*, punten 204-207.

719 Raad van Europa, *Advies uitgebracht over de gevolgen van de verwerking van persoonsgegevens van passagiers*, T-PD(2016)18rev, 19 augustus 2016.

het Amerikaanse ministerie van Financiën voor onderzoeksdoeleinden in verband met terrorismebestrijding in het kader van het programma voor het opsporen van de financiering van terroristische activiteiten[720].

Vanuit EU-perspectief was er geen afdoende rechtsgrondslag voor de openbaarmaking van deze gegevens aan de VS, voornamelijk over EU-burgers, enkel om de eenvoudige reden dat een van de gegevensverwerkende centra van SWIFT daar was gelegen.

In 2010 werd een bijzondere overeenkomst tussen de EU en de VS gesloten, bekend als de "SWIFT-overeenkomst", om voor de noodzakelijke rechtsgrondslag te zorgen en passende standaarden voor gegevensbescherming te waarborgen[721].

In het kader van deze overeenkomst blijft men de door SWIFT opgeslagen financiële gegevens verstrekken aan het Amerikaanse ministerie van Financiën met het oog op het voorkomen, onderzoeken, opsporen of vervolgen van terrorisme of terrorismefinanciering. Het Amerikaanse ministerie van Financiën kan financiële gegevens opvragen bij SWIFT, mits een dergelijk verzoek:

- zo duidelijk mogelijk vermeldt welke financiële gegevens noodzakelijk zijn;
- een duidelijke motivering omvat van de omstandigheden waarin de gegevens nodig zijn;
- zorgvuldig op maat wordt gesneden opdat zo weinig mogelijk gegevens worden opgevraagd;

720 Zie in dit verband Groep artikel 29 (2011), *Advies 14/2011 over gegevensbeschermingskwesties die verband houden met het voorkomen van het witwassen van geld en van het financieren van terrorisme*, WP 186, Brussel, 13 juni 2011; Groep artikel 29 (2006), *Advies 10/2006 over de verwerking van persoonsgegevens door de Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Brussel, 22 november 2006, en de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer *(Commission de la protection de la vie privée)* (2008), *Beslissing betreffende de controle en de aanbevelingsprocedure ingeleid met betrekking tot de maatschappij SWIFT CVBA*, 9 december 2008.

721 Besluit 2010/412/EU van de Raad van 13 juli 2010 betreffende de sluiting van de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer van de Europese Unie naar de Verenigde Staten ten behoeve van het programma voor het traceren van terrorismefinanciering, PB L 195 van 2010, blz. 3 en 4. De tekst van de overeenkomst is gehecht aan dit besluit, PB L 195 van 2010, blz. 5-14.

- in geen geval betrekking heeft op gegevens betreffende de eengemaakte eurobetalingsruimte (Single Euro Payment Area — SEPA)[722].

Europol moet een kopie van elk verzoek van het Amerikaanse ministerie van Financiën ontvangen en controleren of de beginselen van de SWIFT-overeenkomst worden nageleefd[723]. Indien wordt bevestigd dat dit zo is, moet SWIFT de financiële gegevens rechtstreeks aan het Ministerie van Financiën van de VS geven. Het ministerie moet de financiële gegevens opslaan in een beveiligde fysieke omgeving waar alleen analisten die onderzoek naar terrorisme en terrorismefinanciering uitvoeren toegang toe hebben, en de financiële gegevens mogen niet worden gekoppeld aan enige andere databank. Over het algemeen moeten financiële gegevens van SWIFT niet later dan vijf jaar na de ontvangst ervan worden uitgewist. Financiële gegevens die relevant zijn voor specifieke onderzoeken of vervolgingen mogen enkel zo lang worden bewaard als noodzakelijk is voor het specifieke onderzoek of de specifieke vervolging waarvoor ze worden gebruikt.

Het Amerikaanse ministerie van Financiën kan informatie uit de van SWIFT ontvangen gegevens verder doorgeven aan specifieke autoriteiten die bevoegd zijn voor rechtshandhaving, openbare veiligheid of terrorismebestrijding in of buiten de VS, en uitsluitend ten behoeve van onderzoek, opsporing, voorkoming of vervolging van terrorisme of terrorismefinanciering. Wanneer de informatie die verder wordt doorgegeven betrekking heeft op een burger of ingezetene van een EU-lidstaat, is voor het delen van deze informatie met de autoriteiten van een derde land de voorafgaande instemming van de bevoegde autoriteiten van de betrokken lidstaat vereist. Hierop kan een uitzondering worden gemaakt wanneer het uitwisselen van de gegevens van wezenlijk belang is voor het keren van een onmiddellijke en ernstige dreiging voor de openbare veiligheid.

Onafhankelijke toezichthouders, waaronder een door de Europese Commissie aangewezen persoon, controleren de naleving van de beginselen van de SWIFT-overeenkomst. Zij hebben de mogelijkheid om onmiddellijk en met terugwerkende kracht alle bevragingen van de verstrekte gegevens te controleren, om aanvullende informatie die het verband tussen deze opvragingen en terrorisme staaft, aan te vragen en de autoriteit om meerdere of alle opvragingen die een inbreuk vormen op de waarborgen die verankerd zijn in de overeenkomst, te blokkeren.

722 *Ibid.*, artikel 4, lid 2.

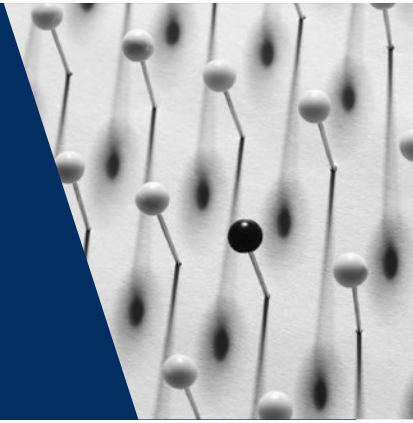
723 Het gemeenschappelijk controleorgaan van Europol heeft audits in verband met de activiteiten van Europol op dit gebied uitgevoerd.

Betrokkenen hebben het recht om van de bevoegde EU-toezichthoudende autoriteit bevestiging te verkrijgen dat hun gegevensbeschermingsrechten zijn geëerbiedigd. Ook hebben betrokkenen het recht te verlangen dat hun persoonsgegevens die door het Amerikaanse ministerie van Financiën overeenkomstig de SWIFT-overeenkomst zijn verwerkt en opgeslagen, worden gecorrigeerd, gewist of afgeschermd. De toegangsrechten van betrokkenen kunnen echter aan bepaalde wettelijke beperkingen worden gebonden. Indien de toegang tot persoonsgegevens wordt geweigerd, moet de betrokkene schriftelijk in kennis worden gesteld van die weigering en van de administratieve en gerechtelijke beroepsmogelijkheden waarover hij of zij in de VS beschikt.

De SWIFT-overeenkomst is geldig gedurende vijf jaar, de eerste periode van geldigheid duurde tot augustus 2015. De overeenkomst wordt automatisch verlengd met opeenvolgende perioden van één jaar, tenzij een van de partijen de andere ten minste zes maanden van tevoren schriftelijk in kennis stelt van zijn voornemen om de overeenkomst niet te verlengen. De automatische verlenging is in augustus 2015, 2016 en 2017 toegepast en waarborgt de geldigheid van de SWIFT-overeenkomst ten minste tot augustus 2018[724].

724 *Ibid.*; artikel 23, lid 2.

8 Gegevensbescherming in het kader van politiële en strafrechtelijke aangelegenheden



EU	Behandelde onderwerpen	RvE
Richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten	**Algemeen**	Gemoderniseerd Verdrag 108
	Politie	Politieaanbeveling Praktische handleiding over gebruik persoonlijke gegevens in de politiesector
	Bewaking	EHRM, *B.B./Frankrijk*, nr. 5335/06, 2009 EHRM, *S. en Marper/Verenigd Koninkrijk* [Grote kamer], nrs. 30562/04 en 30566/04, 2008 EHRM, *Allan/Verenigd Koninkrijk*, nr. 48539/99, 2002 EHRM, *Malone/Verenigd Koninkrijk*, nr. 8691/79, 1984 EHRM, *Klass e.a./Duitsland*, nr. 5029/71, 1978 EHRM, *Szabó en Vissy/Hongarije*, nr. 37138/14, 2016 EHRM, *Vetter/Frankrijk*, nr. 59842/00, 2005
	Cybercriminaliteit	Verdrag inzake cybercriminaliteit

EU	Behandelde onderwerpen	RvE
Andere specifieke rechtsinstrumenten		
Prüm-besluit	**Voor bijzondere gegevens: vingerafdrukken, DNA, hooliganisme, luchtpassagiers-informatie, telecommunicatie-gegevens enz.**	Gemoderniseerd Verdrag 108, artikel 6 Politieaanbeveling, Praktische handleiding over gebruik persoonlijke gegevens in de politiesector
Zweeds initiatief (Kaderbesluit 2006/960/JBZ van de Raad)	**Vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de wetshandhavings-instanties**	EHRM, *S. en Marper/Verenigd Koninkrijk* [Grote kamer], nrs. 30562/04 en 30566/04, 2008
Richtlijn (EU) 2016/681 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland* en Kärntner Landesregierung e.a. [Grote kamer], 2014 HvJ-EU, gevoegde zaken C-203/15 en C-698/15, *Tele2 Sverige* en *Home Department/Tom Watson e.a.* [Grote kamer], 2016	**Bewaring van persoonsgegevens**	EHRM, *B.B./Frankrijk*, nr. 5335/06, 2009
Europol-verordening Eurojust-besluit	**Door speciale agentschappen**	Politieaanbeveling
Schengen II-besluit VIS-verordening Eurodac-verordening DIS-besluit	**Door speciale gemeenschappelijke informatiesystemen**	Politieaanbeveling EHRM, *Dalea/Frankrijk*, No. 964/07, 2010

Om de belangen van personen bij gegevensbescherming en de belangen van de samenleving bij gegevensverzameling ten behoeve van criminaliteitsbestrijding en het waarborgen van de nationale en openbare veiligheid tegen elkaar af te wegen, hebben de Raad van Europa en de EU specifieke rechtsinstrumenten vastgesteld.

Dit punt geeft een overzicht van het recht van de Raad van Europa (punt 8.1) en de EU-wetgeving (punt 8.2) met betrekking tot gegevensbescherming bij politiële en strafrechtelijke aangelegenheden.

8.1. Recht van de Raad van Europa inzake gegevensbescherming en nationale veiligheid, politiële en strafrechtelijke aangelegenheden

Belangrijkste punten

- Het Gemoderniseerd Verdrag 108 en de Politieaanbeveling van de Raad van Europa zijn van toepassing op de gegevensbescherming op alle gebieden van politiewerk.
- Het Verdrag inzake cybercriminaliteit (Verdrag van Boedapest) is een bindend internationaal rechtsinstrument dat betrekking heeft op strafbare feiten die zijn gepleegd tegen en door middel van elektronische netwerken. Het is ook van belang voor het onderzoek naar niet-cybercriminaliteit waarbij het gaat om elektronische bewijsmiddelen.

Een belangrijk onderscheid tussen het recht van de Raad van Europa en het Unierecht is dat **het recht van de Raad van Europa**, in tegenstelling tot het Unierecht, ook van toepassing is op het gebied van nationale veiligheid. Dit betekent dat de verdragsluitende partijen binnen het toepassingsgebied van artikel 8 van het EVRM moeten blijven, ook voor activiteiten in verband met de nationale veiligheid. Verscheidene arresten van de EHRM hebben betrekking op activiteiten van de staat op de gevoelige gebieden van de toepasselijke wetten en praktijken van de nationale veiligheid[725].

Met betrekking tot politiële en strafrechtelijke aangelegenheden, bestrijkt Verdrag 108 op Europees niveau alle gebieden van de verwerking van persoonsgegevens, en de bepalingen ervan beogen de verwerking van persoonsgegevens in het algemeen te reguleren. Bijgevolg is Verdrag 108 van toepassing op gegevensbescherming op het gebied van politiële en strafrechtelijke aangelegenheden. De verwerking van genetische gegevens, persoonsgegevens met betrekking tot

725 Zie, bijvoorbeeld, EHRM, *Klass e.a./Duitsland*, nr. 5029/71, 6 september 1978; EHRM, *Rotaru/Roemenië* [Grote kamer], nr. 28341/95, 4 mei 2000, en EHRM, *Szabó en Vissy/Hongarije*, nr. 37138/14, 12 januari 2016.

misdrijven en strafrechtelijke procedures en daarmee samenhangende veiligheidsmaatregelen, biometrische gegevens die een persoon op een unieke manier identificeren, alsook alle gevoelige persoonsgegevens, is enkel toegestaan indien er passende waarborgen bestaan tegen de risico's die de verwerking van dergelijke gegevens met zich kan meebrengen voor de belangen, rechten en fundamentele vrijheden van de betrokkene; met name het risico op discriminatie[726].

De wettelijke taken van de politiële en strafrechtelijke autoriteiten vereisen vaak de verwerking van persoonsgegevens, wat ernstige gevolgen voor de betrokken personen met zich mee kan brengen. De Politieaanbeveling die de Raad van Europa in 1987 heeft vastgesteld, bevat richtsnoeren voor de lidstaten over de wijze waarop ze gevolg zouden moeten geven aan de beginselen van Gemoderniseerd Verdrag 108 in het kader van de verwerking van persoonsgegevens door politieautoriteiten[727]. De aanbeveling werd begeleid door een praktische handleiding over het gebruik van persoonsgegevens in de politiesector, aangenomen door het Raadgevend Comité voor Verdrag 108[728].

Voorbeeld: In *D.L./Bulgarije*[729] plaatsten de sociale diensten de verzoeker in een beveiligde onderwijsinstelling overeenkomstig een rechterlijke uitspraak. Alle schriftelijke correspondentie en telefoongesprekken werden onderworpen aan algemeen en willekeurig toezicht door de instelling. De EHRM oordeelde een schending van artikel 8, aangezien de maatregel in kwestie niet noodzakelijk was in een democratische samenleving. Het Hof bepaalde dat alles in het werk moest worden gesteld om in een instelling geplaatste minderjarigen voldoende contact met de buitenwereld te geven, aangezien dit integraal deel uitmaakt van hun recht om met waardigheid te worden behandeld en essentieel is in de voorbereiding van hun re-integratie in de samenleving. Dit geldt zowel voor bezoeken als voor schriftelijke correspondentie of telefoongesprekken. Bovendien maakte de bewaking geen onderscheid tussen contact met familieleden en met

726 Gemoderniseerd Verdrag 108, artikel 6.

727 Raad van Europa, Comité van Ministers (1987), Aanbeveling Rec(87)15 aan de lidstaten tot regeling van het gebruik van persoonsgegevens op politieel gebied, 17 september 1987.

728 Raad van Europa (2018), Raadgevend Comité voor Verdrag 108, *Praktische handleiding over gebruik persoonlijke gegevens in de politiesector*, T-PD(2018)1.

729 EHRM, *D.L./Bulgarije*, nr. 7472/14, 19 mei 2016.

ngo's die de rechten van kinderen verdedigen of advocaten. Bovendien was het besluit om de communicatie af te luisteren niet gebaseerd op een geïndividualiseerde analyse van de risico's in elk afzonderlijk geval.

Voorbeeld: In *Dragojević/Kroatië*[730] werd de verzoeker ervan verdacht betrokken te zijn bij drugshandel. Hij werd schuldig bevonden nadat een onderzoeksrechter het gebruik van geheime toezichtmaatregelen had gerechtigd om de telefoongesprekken van de verzoeker af te luisteren. Het EHRM oordeelde dat de maatregel, waartegen een klacht was ingediend, een inbreuk vormde op het recht op de eerbiediging van het privéleven en correspondentie. De vergunning die werd verleend door de onderzoeksrechter was uitsluitend gebaseerd op de verklaring van de vervolgende autoriteit dat "het onderzoek niet op een andere manier kon worden uitgevoerd". Het EHRM wees er ook op dat de rechtbank zijn beoordeling met betrekking tot het gebruik van de toezichtmaatregelen had beperkt en dat de overheid de beschikbare oplossingen niet had aangevoerd. Bijgevolg werd artikel 8 geschonden.

8.1.1. De Politieaanbeveling

Het EHRM heeft steeds gesteld dat de opslag en bewaring van persoonsgegevens door de politie of nationale veiligheidsautoriteiten een inmenging in artikel 8, lid 1, van het EVRM vormt. Een groot aantal arresten van het EHRM heeft betrekking op de rechtvaardiging van dergelijke inmengingen[731].

Voorbeeld: In *B.B./Frankrijk*[732] was de aanvrager veroordeeld voor seksuele delicten tegen 15-jarige minderjarigen als een persoon in een positie van vertrouwen. Hij heeft zijn gevangenisstraf in 2000 beëindigd. Een jaar later verzocht hij dat de vermelding van deze veroordeling uit zijn strafregister zou worden verwijderd, maar dit verzoek werd afgewezen. In 2004 stelde een Franse wet een nationale gerechtelijke databank van zedendelinquenten in en de aanvrager werd op de hoogte gebracht dat hij hierin was opgenomen. Het EHRM oordeelde dat het opnemen van een veroordeelde zedendelinquent

730 EHRM, *Dragojević/Kroatië*, nr. 68955/11, 15 januari 2015.

731 Zie, bijvoorbeeld, EHRM, *Leander/Zweden*, nr. 9248/81, 26 maart 1987; EHRM, *M.M./Verenigd Koninkrijk*, nr. 24029/07, 13 november 2012; EHRM, *M.K./Frankrijk*, nr. 19522/09, 18 april 2013, of EHRM, *Aycaguer/Frankrijk*, nr 8806/12, 22 juni 2017.

732 EHRM, *B.B./Frankrijk*, nr. 5335/06, 17 december 2009.

in een nationale gerechtelijke databank onder artikel 8 van het EVRM valt. Aangezien echter voldoende waarborgen voor de gegevensbescherming ten uitvoer waren gelegd, zoals het recht van de betrokkene om uitwissing van de gegevens te verlangen, de beperkte opslagtermijn en de beperkte toegang tot de gegevens, was een billijk evenwicht bereikt tussen de tegenstrijdige persoonlijke en algemene belangen die in het geding waren. Het Hof concludeerde dat artikel 8 van het EVRM niet was geschonden.

Voorbeeld: In *S. en Marper/Verenigd Koninkrijk*[733] waren beide verzoekers strafbare feiten ten laste gelegd, maar was geen van beiden daarvoor veroordeeld. Niettemin werden hun vingerafdrukken, celmonsters en dna-profielen bewaard en opgeslagen door de politie. De onbeperkte bewaring van de bovengenoemde biometrische gegevens was wettelijk toegestaan indien een persoon werd verdacht van het plegen van een strafbaar feit, ook al was de verdachte later vrijgesproken of van rechtsvervolging ontslagen. Het EHRM oordeelde dat de algemene en ongedifferentieerde bewaring van persoonsgegevens, die niet tijdsgebonden was en waarbij vrijgesproken personen slechts over beperkte mogelijkheden beschikten om te verzoeken om uitwissing, een onevenredige inmenging in het recht van de verzoekers op eerbiediging van hun privéleven vormde. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Een cruciaal punt in de context van elektronische communicatie is de inmenging door de openbare overheid met de rechten op privacy en gegevensbescherming. Middelen ter surveillance of interceptie van communicatie, zoals afluisterapparatuur, zijn enkel toelaatbaar indien dit bij wet is voorzien en indien het gaat om een noodzakelijke maatregel in een democratische samenleving in het belang van:

- de bescherming van de nationale veiligheid;
- de openbare veiligheid;
- de geldelijke belangen van de staat;
- de bestrijding van strafbare feiten, of
- ter bescherming van de betrokkene of van de rechten en vrijheden van anderen.

733 EHRM, *S. en Marper/Verenigd Koninkrijk* [Grote kamer], nrs. 30562/04 en 30566/04, 4 december 2008, punten 119 en 125.

Diverse andere arresten van het EHRM hebben betrekking op de rechtvaardiging van inmenging in het recht op privacy door surveillance te verrichten.

Voorbeeld: In *Allan/Verenigd Koninkrijk*[734] nam de overheid heimelijk privégesprekken op tussen een gevangene en een vriend in de bezoekersruimte van de gevangenis, en met een medeverdachte in een gevangeniscel. Het EHRM oordeelde dat het gebruik van de audio- en video-opnameapparatuur in de cel van de verzoeker en de bezoekersruimte van de gevangenis en op het lichaam van een medegevangene inmenging in het recht op een privéleven van de verzoeker inhield. Aangezien er geen wettelijk systeem bestond om het gebruik van geheime opnameapparatuur door de politie te reguleren, was deze inmenging niet in overeenstemming met de wet. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Voorbeeld: In *Roman Zakharov/Rusland*[735] stelde de aanvrager gerechtelijke procedures in tegen drie mobiele netwerkbedrijven. Hij voerde aan dat zijn recht op de privacy van zijn telefoongesprekken was geschonden, aangezien de bedrijven apparatuur hadden geïnstalleerd die de federale veiligheidsdienst in staat stelde om zijn telefoongesprekken af te luisteren zonder voorafgaande gerechtelijke toestemming. Het EHRM oordeelde dat de nationale wettelijke bepalingen die de interceptie van communicatie regelt, geen passende en daadwerkelijke garanties boden tegen willekeur en het risico op misbruik. In het bijzonder schreef de nationale wetgeving geen verplichting voor tot schrapping van de opgeslagen gegevens nadat de doelstelling van de opslag was bereikt. Hoewel gerechtelijke toestemming was vereist, was de gerechtelijke toetsing bovendien beperkt.

Voorbeeld: In *Szabó en Vissy/Hongarije*[736] voerden de aanvragers aan dat de Hongaarse wetgeving artikel 8 van het EVRM schond, aangezien ze niet voldoende gedetailleerd of nauwkeurig was. Voorts werd aangevoerd dat de wetgeving geen voldoende waarborgen voorzag tegen misbruik en willekeur. Het EHRM oordeelde dat de Hongaarse wetgeving niet vereiste dat surveillance onderworpen was aan een machtiging van een rechter. Niettemin heeft het Hof opgemerkt dat dit toezicht, hoewel onderworpen aan de goedkeuring van de Minister van Justitie, bij uitstek van politieke aard

734 EHRM, *Allan/Verenigd Koninkrijk*, nr. 48539/99, 5 november 2002.

735 EHRM, *Roman Zakharov/Rusland*, nr. 47143/06, 4 december 2015.

736 EHRM, *Szabó en Vissy/Hongarije*, nr. 37138/14, 12 januari 2016.

was en niet in staat was de vereiste evaluatie van "strikt noodzakelijk" te waarborgen. Voorts voorziet de nationale wetgeving niet in een rechterlijke toetsing, gezien het feit dat er geen kennisgeving wordt gezonden naar de betrokkenen. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Omdat gegevensverwerking door politiële autoriteiten significante gevolgen kan hebben voor de betrokken personen, zijn gedetailleerde gegevensbeschermingsvoorschriften voor de verwerking van persoonsgegevens op dit gebied bijzonder noodzakelijk. De Politieaanbeveling van de Raad van Europa wilde een oplossing voor dit probleem vinden door richtsnoeren uit te vaardigen over de wijze waarop persoonsgegevens moeten worden verzameld voor de werkzaamheden van de politie; de wijze waarop gegevensbestanden op dit gebied dienen te worden bewaard; wie er toegang mag krijgen tot deze bestanden, met inbegrip van de voorwaarden voor de doorgifte van persoonsgegevens aan buitenlandse politiële autoriteiten; de wijze waarop betrokkenen hun rechten inzake gegevensbescherming moeten kunnen uitoefenen; en de wijze waarop controle door onafhankelijke autoriteiten moet worden uitgevoerd. De verplichting om te zorgen voor voldoende gegevensbescherming is ook in aanmerking genomen.

De aanbeveling voorziet niet in de onbeperkte, willekeurige verzameling van persoonsgegevens door de politiediensten. Ze beperkt de verzameling van persoonsgegevens door de politiediensten tot wat noodzakelijk is voor de voorkoming van een reëel gevaar of voor de vervolging van een strafbaar feit. Het verzamelen van aanvullende gegevens moet zijn gebaseerd op specifieke nationale wetgeving. De verwerking van gevoelige gegevens moet worden beperkt tot wat absoluut noodzakelijk is in het kader van een specifiek onderzoek.

Wanneer persoonsgegevens worden verzameld zonder dat de betrokkene daarvan op de hoogte is, moet de betrokkene in kennis van de gegevensverzameling worden gesteld zodra deze kennisgeving niet langer een belemmerend effect op een onderzoek heeft. Ook de verzameling van gegevens door technische surveillance of andere geautomatiseerde middelen moet zijn gebaseerd op specifieke wettelijke bepalingen.

Voorbeeld: In *Versini-Campinchi en Crasnianski/Frankrijk*[737] had de aanvrager, een advocaat, een telefoongesprek met een cliënt van wie de telefoonlijn werd afgeluisterd op verzoek van een onderzoeksrechter. Uit het transcript van het gesprek bleek dat ze informatie had onthuld die werd beschermd door de vertrouwelijkheid van de communicatie tussen advocaat en cliënt. De aanklager verzond deze informatie naar de Raad van de balies van de Europese Unie die de aanvrager een boete oplegde. Het EHRM erkende het bestaan van een inbreuk op het recht op eerbiediging van privéleven en correspondentie, niet enkel van de persoon van wie de telefoon werd afgeluisterd, maar ook van de aanvrager van wie het gesprek werd afgeluisterd en getranscribeerd. De inbreuk was in overeenstemming met de wet en diende het rechtmatige doel van de preventie van wanordelijkheden. De aanvrager verkreeg een evaluatie van de rechtmatigheid van de indiening van de getranscribeerde, afgeluisterde telefoongegevens in het kader van de tuchtprocedure die tegen haar was ingesteld. Hoewel zij niet in staat was een aanvraag in te dienen om het transcript van het telefoongesprek te annuleren, oordeelde het EHRM dat er sprake was van een daadwerkelijke controle die de ten laste gelegde inbreuk kon beperken tot wat noodzakelijk was in een democratische maatschappij. Het EHRM verklaarde dat het argument dat de mogelijkheid van een strafrechtelijke procedure tegen een advocaat op basis van een transcript een remmend effect kon hebben op de vrijheid van communicatie tussen een advocaat en zijn/haar cliënt en dus op de rechten van de verdediging van laatstgenoemde, niet geloofwaardig was, aangezien de onthulling van de advocaat zelf kon leiden tot onwettig gedrag van haar kant. Bijgevolg werd er geen schending van artikel 8 vastgesteld.

De Politieaanbeveling van de RvE bepaalt dat, bij het opslaan van persoonsgegevens, er een duidelijk onderscheid moet worden gemaakt tussen: administratieve gegevens en politiegegevens; de persoonsgegevens van verschillende soorten betrokkenen, zoals verdachten, veroordeelden, slachtoffers en getuigen, en gegevens die worden beschouwd als harde feiten en gegevens die berusten op vermoedens of speculatie.

Het doel waarvoor de politiegegevens kunnen worden gebruikt, moet strikt worden beperkt. Dit heeft gevolgen voor de bekendmaking van politiegegevens aan derde partijen: de doorgifte of bekendmaking van dergelijke gegevens binnen de

737 EHRM, *Versini-Campinchi en Crasnianski/Frankrijk*, nr. 49176/11, 16 juni 2016.

politiesector moet worden geregeld door de vraag of er een rechtmatig belang is bij de uitwisseling van de informatie. De overdracht of bekendmaking van deze gegevens buiten de politiesector mag enkel worden toegestaan indien er een duidelijke wettelijke verplichting of machtiging voor bestaat.

> Voorbeeld: In *Karabeyoğlu/Turkije*[738] werden de telefoonlijnen van de aanvrager, een rechter, afgeluisterd in het kader van een strafrechtelijk onderzoek naar een illegale organisatie waarvan werd vermoed dat hij er deel van uitmaakte of er bijstand en ondersteuning aan gaf. Na het besluit om niet te vervolgen, vernietigde de openbare aanklager die belast was met het strafrechtelijk onderzoek de opnames in kwestie. Een kopie bleef echter in het bezit van de gerechtelijke onderzoekers, die het relevante materiaal gebruikten in het kader van een disciplinair onderzoek tegen de aanvrager. Het EHRM oordeelde dat de desbetreffende wetgeving was geschonden, aangezien de informatie werd gebruikt voor andere doeleinden dan die waarvoor ze werd verzameld, en niet was vernietigd binnen een voorgeschreven termijn. De inmenging in het recht van de aanvrager op eerbiediging van zijn privéleven was niet in overeenstemming met de wet voor zover het ging over de tuchtprocedure die tegen hem liep.

Internationale doorgifte of bekendmaking moet worden beperkt tot politiële autoriteiten van derde landen en moet zijn gebaseerd op bijzondere wettelijke bepalingen, mogelijkerwijs internationale overeenkomsten, tenzij de overdracht noodzakelijk is om een ernstig en dreigend gevaar te voorkomen.

Om naleving van de nationale gegevensbeschermingswetgeving te waarborgen, moet gegevensverwerking door de politie zijn onderworpen aan onafhankelijk toezicht. Betrokkenen moeten alle in het Gemoderniseerd Verdrag 108 vervatte toegangsrechten kunnen uitoefenen. Wanneer de toegangsrechten van betrokkenen overeenkomstig artikel 9 van Verdrag 108 zijn beperkt in het belang van doeltreffende politieonderzoeken en de uitoefening van strafrechtelijke sancties, moet de betrokkene krachtens het nationale recht het recht hebben om beroep in te kunnen gaan bij de nationale toezichthouder voor gegevensbescherming of een ander onafhankelijk orgaan.

738 EHRM, *Karabeyoğlu/Turkije*, nr. 30083/10, 7 juni 2016.

8.1.2. Het Verdrag van Boedapest inzake cybercriminaliteit

Aangezien bij criminele activiteiten in toenemende mate gebruik wordt gemaakt van elektronische gegevensverwerkingssystemen en deze activiteiten er steeds sterker op van invloed zijn, zijn nieuwe strafrechtelijke wettelijke bepalingen nodig om deze uitdaging het hoofd te kunnen bieden. Om die reden heeft de RvE een internationaal rechtsinstrument aangenomen, het Verdrag inzake cybercriminaliteit — ook bekend als het Verdrag van Boedapest — als antwoord op het probleem om misdrijven tegen en door middel van elektronische netwerken aan te pakken[739]. Dit verdrag staat ook open voor toetreding door niet-leden van de RvE. Begin 2018 waren 14 staten die geen deel uitmaakten van de RvE[740] bij het verdrag aangesloten en zeven andere niet-leden waren uitgenodigd om toe te treden.

Het Verdrag inzake cybercriminaliteit blijft het meest invloedrijke internationale verdrag inzake inbreuken op de wet via internet of andere informatienetwerken. Het verdrag vereist van de verdragsluitende partijen dat ze hun strafrechtelijke bepalingen tegen hacken en andere inbreuken, waaronder inbreuken op het auteursrecht, computergerelateerde fraude, Child pornography | The IT Law Wiki | Fandom (wikia.org) en andere illegale cyberactiviteiten, actualiseren en harmoniseren. Ook voorziet het verdrag in procedurele bevoegdheden voor het doorzoeken van computernetwerken en het onderscheppen van communicatie in het kader van de bestrijding van cybercriminaliteit. Tot slot maakt het verdrag doeltreffende internationale samenwerking mogelijk. Een aanvullend protocol bij het verdrag heeft betrekking op de strafbaarstelling van racistische en xenofobische propaganda in computernetwerken.

Hoewel het verdrag geen instrument is voor de bevordering van gegevensbescherming, stelt het activiteiten strafbaar die het recht van een betrokkene op bescherming van zijn/haar persoonsgegevens mogelijk kunnen schenden. Voorts bepaalt het dat verdragsluitende partijen wettelijke maatregelen moeten treffen om hun nationale autoriteiten in staat te stellen gegevensverkeer en inhoudelijke gegevens te onderscheppen[741]. Ook worden de verdragsluitende partijen verplicht om bij de

739 Raad van Europa, Comité van Ministers (2001), Verdrag inzake cybercriminaliteit, CETS nr. 185, Boedapest, 23 november 2001, in werking getreden op 1 juli 2004.

740 Australië, Canada, Chili, de Dominicaanse Republiek, Israël, Japan, Mauritius, de Republiek Panama, Senegal, Sri Lanka, Tonga en de Verenigde Staten. Zie Lijst van ondertekeningen en ratificaties van Verdrag 185, status op juli 2017.

741 Raad van Europa, Comité van Ministers (2001), Verdrag inzake cybercriminaliteit, CETS nr. 185, Boedapest, 23 november 2001, artikelen 20 en 21.

tenuitvoerlegging van het verdrag te voorzien in een passende bescherming van mensenrechten en vrijheden, waaronder door het EVRM gegarandeerde rechten, zoals het recht op gegevensbescherming[742]. De verdragsluitende partijen hoeven geen partij te zijn bij Verdrag 108 om aan te sluiten bij het Verdrag van Boedapest inzake cybercriminaliteit.

8.2. EU-wetgeving inzake gegevensbescherming in het kader van politiële en strafrechtelijke aangelegenheden

Belangrijkste punten

- Binnen de Europese Unie wordt gegevensbescherming in de sector van politiële en strafrechtelijke aangelegenheden gereguleerd in het kader van zowel nationale als grensoverschrijdende verwerking door politiediensten en strafrechtelijke autoriteiten in strafzaken van de lidstaten en EU-actoren.
- Op het niveau van de lidstaten dient de richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten te worden opgenomen in het nationale recht.
- Specifieke wetgevingen inzake gegevensbescherming reglementeren de politiële en judiciële grensoverschrijdende samenwerking, met name ter bestrijding van terrorisme en grensoverschrijdende criminaliteit.
- Er bestaan bijzondere gegevensbeschermingsregelingen voor de Europese Politiedienst (Europol), de Europese Eenheid voor justitiële samenwerking (Eurojust), en het nieuw opgerichte Europees Openbaar Ministerie, de EU-organen die bijstand verlenen aan grensoverschrijdende wetshandhaving en deze bevorderen.
- Ook bestaan er bijzondere gegevensbeschermingsregels voor de gemeenschappelijke informatiesystemen die op EU-niveau zijn ingesteld voor grensoverschrijdende informatie-uitwisseling tussen bevoegde politiële en justitiële autoriteiten. Belangrijke voorbeelden zijn het Schengeninformatiesysteem II (SIS II), het Visuminformatiesysteem (VIS) en Eurodac, een centraal systeem waarin de vingerafdrukgegevens van onderdanen van derde landen en staatloze personen die asiel aanvragen in een van de EU-lidstaten, worden bewaard.
- De Europese Unie is bezig met de aanpassing van de hierboven vermelde bepalingen inzake gegevensbescherming, zodat zij in overeenstemming zijn met de bepalingen van de richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten.

742 *Ibid.*, artikel 15, lid 1.

8.2.1. De richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten

Richtlijn (EU) 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens (de richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten)[743] streeft ernaar persoonsgegevens die voor strafrechtelijke doeleinden worden verzameld en verwerkt, te beschermen, variërend van:

- de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
- de uitvoering van een strafrechtelijke sanctie, en
- gevallen waarin de politie of andere wetshandhavingsautoriteiten handelen ter handhaving van het recht en ter bescherming tegen bedreigingen van de openbare veiligheid en de grondrechten van de maatschappij die een strafbaar feit zouden kunnen vormen.

De richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten beschermt de persoonsgegevens van verschillende categorieën personen die betrokken zijn bij een strafrechtelijke procedure, zoals getuigen, informanten, slachtoffers, verdachten en medeplichtigen. Politiële en strafrechtelijke autoriteiten zijn verplicht te voldoen aan de bepalingen van de richtlijn wanneer ze dergelijke persoonsgegevens voor rechtshandhavingsdoeleinden verwerken, in zowel het persoonlijke als het materiële toepassingsgebied van de richtlijn[744].

Het gebruik van gegevens voor een ander doel is evenwel ook toegestaan onder bepaalde voorwaarden. De verwerking van gegevens voor een ander rechtshandhavingsdoeleinde dan dat waarvoor zij werden verzameld, is enkel

743 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, PB L 119 van 2016, blz. 89 (richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten).

744 Richtlijn betreffende gegevensbescherming voor politiële en strafrechtelijke autoriteiten, artikel 2, lid 1.

toegestaan indien deze rechtmatig, noodzakelijk en evenredig is overeenkomstig het nationale of het Unierecht[745]. Voor andere doeleinden zijn de regels van de algemene verordening gegevensbescherming van toepassing. Het bijhouden van logboeken en het documenteren van gemeenschappelijk gegevensgebruik is een van de specifieke taken van de bevoegde autoriteiten met het oog op de verduidelijking van verantwoordelijkheden naar aanleiding van klachten.

Bevoegde autoriteiten die werkzaam zijn in het politiële en strafrechtelijke systeem zijn openbare autoriteiten of autoriteiten die krachtens de nationale wetgeving en openbare bevoegdheden de functies van een openbare autoriteit uitoefenen[746], bijvoorbeeld particulier beheerde gevangenissen[747]. De richtlijn is zowel van toepassing op gegevensverwerking op nationaal niveau en grensoverschrijdende verwerking tussen de politiële en strafrechtelijke autoriteiten van de lidstaten als op internationale doorgiften door de bevoegde autoriteiten aan derde landen en internationale organisaties[748]. Het is niet van toepassing op nationale veiligheid of op de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Europese Unie[749].

De richtlijn doet in grote mate beroep op de beginselen en definities van de algemene verordening gegevensbescherming, waarbij rekening wordt gehouden met de specifieke aard van het politiële en strafrechtelijke gebied. Toezicht kan worden uitgeoefend door dezelfde autoriteiten van de lidstaat die hier ook mee zijn belast in het kader van de AVG. De benoeming van functionarissen voor gegevensbescherming en de uitvoering van gegevensbeschermingseffectbeoordelingen werden in de richtlijn ingevoerd als nieuwe verplichtingen voor politiële en strafrechtelijke autoriteiten[750]. Hoewel deze begrippen zijn geïnspireerd op de AVG, heeft de richtlijn betrekking op de specifieke aard van politiële en strafrechtelijke autoriteiten. In

745 *Ibid.*, artikel 4, lid 2.

746 *Ibid.*, artikel 3, lid 7.

747 Europese Commissie (2016), Mededeling van de Commissie aan het Europees Parlement op grond van artikel 294, lid 6, van het Verdrag betreffende de werking van de Europese Unie betreffende de positie van de Raad over de vaststelling van een richtlijn van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten in het kader van het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten en tenuitvoerlegging van strafrechtelijke sancties, en betreffende het vrije verkeer van die gegevens, en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, COM(2016) 213 def., Brussel, 11 april 2016.

748 Richtlijn betreffende gegevensbescherming voor politiële en strafrechtelijke autoriteiten, hoofdstuk V.

749 *Ibid.*, artikel 2, lid 3.

750 *Ibid.*, in respectievelijk artikel 32 en artikel 27.

vergelijking met de verwerking van gegevens voor commerciële doeleinden, die wordt geregeld door de verordening, kunnen verwerkingen die verband houden met veiligheid enige mate van flexibiliteit vereisen. Als betrokkenen bijvoorbeeld hetzelfde beschermingsniveau krijgen in termen van het recht op informatie, toegang tot of verwijdering van hun persoonsgegevens in het kader van de AVG, kan dit betekenen dat een bewakingsoperatie uitgevoerd voor rechtshandhavingsdoeleinden niet doeltreffend zou worden in het kader van de wetshandhaving. De richtlijn bevat derhalve het beginsel van transparantie niet. Ook de beginselen van gegevensminimalisering en doelbinding, die vereisen dat persoonsgegevens slechts worden beperkt tot hetgeen noodzakelijk is met betrekking tot het doel waarvoor zij worden verwerkt, en worden verwerkt voor specifieke en uitdrukkelijke doelstellingen, moeten ook flexibel worden toegepast in veiligheidsgerelateerde verwerkingen. De informatie die wordt verzameld en opgeslagen door bevoegde autoriteiten voor een bepaalde zaak, kan uiterst nuttig zijn voor de oplossing van toekomstige zaken.

Beginselen inzake verwerking

De richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten beschrijft een aantal essentiële waarborgen inzake het gebruik van persoonsgegevens. Het bepaalt ook de beginselen die de verwerking van dergelijke gegevens aansturen. De lidstaten moeten ervoor zorgen dat persoonsgegevens:

- rechtmatig en eerlijk worden verwerkt;
- voor welbepaalde, uitdrukkelijk omschreven en rechtmatige doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt;
- toereikend, ter zake dienend en niet bovenmatig zijn in verhouding tot de doeleinden waarvoor zij worden verwerkt;
- juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren;
- worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt;

- met gebruikmaking van passende technische of organisatorische middelen op een dusdanige manier worden verwerkt dat de beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging[751].

In het kader van de richtlijn is de verwerking enkel rechtmatig wanneer deze wordt toegepast in de mate die nodig is om de desbetreffende opdracht uit te voeren. Bovendien moet dit gebeuren door een bevoegde autoriteit in lijn met de doelstellingen die in de richtlijn staan beschreven en op basis van het Unierecht of het nationaal recht[752]. Gegevens mogen niet langer dan nodig bewaard worden en moeten worden verwijderd of regelmatig worden gecontroleerd binnen bepaalde termijnen. Ze mogen enkel worden gebruikt door een bevoegde autoriteit en voor het doeleinde waarvoor de gegevens werden verzameld, verstrekt of beschikbaar gesteld.

Rechten van de betrokkenen

De richtlijn beschrijft ook de rechten van de betrokkene. Deze omvatten:

- Het recht op informatie. Lidstaten moeten de verwerkingsverantwoordelijke verplichten om de betrokkene te informeren over 1) de identiteit en contactgegevens van de verwerkingsverantwoordelijke, 2) de contactgegevens van de functionaris voor gegevensbescherming, 3) de doeleinden van de beoogde verwerking, 4) het recht om een klacht neer te leggen bij de toezichthoudende autoriteit en zijn contactgegevens en 5) het recht op toegang tot persoonsgegevens, op de rectificatie of wissing ervan en de beperking van de verwerking ervan[753]. Naast deze algemene informatieverplichtingen bepaalt de richtlijn dat, in specifieke gevallen en om de uitoefening van hun rechten mogelijk te maken, verwerkingsverantwoordelijken de betrokkenen informatie moeten geven over de wettelijke basis voor de verwerking en over hoe lang de gegevens zullen worden opgeslagen. Indien persoonsgegevens moeten worden verstrekt aan andere ontvangers, ook in derde landen of internationale organisaties, moeten de betrokkenen op de hoogte worden gesteld van de categorieën ontvangers. Ten slotte moeten verwerkingsverantwoordelijken alle aanvullende informatie verstrekken, rekening houdend met de omstandigheden waarin de gegevens worden verwerkt, bijvoorbeeld wanneer

751 *Ibid.*, artikel 4, lid 1.

752 *Ibid.*, artikel 8.

753 *Ibid.*, artikel 13, lid 1.

persoonsgegevens werden verzameld tijdens het schaduwen van personen, dat wil zeggen zonder medeweten van de betrokkene. Dit garandeert een eerlijke verwerking met betrekking tot de betrokkene[754].

- Het recht op toegang tot persoonsgegevens. Lidstaten moeten ervoor zorgen dat de betrokkene het recht geniet te weten of zijn/haar persoonsgegevens worden verwerkt. Als ze worden verwerkt, moet de betrokkene toegang krijgen tot bepaalde informatie, zoals de categorieën gegevens die worden verwerkt.[755] Dit recht kan echter worden beperkt, bijvoorbeeld om te voorkomen dat een onderzoek wordt belemmerd of de vervolging van een misdaad in het gedrang komt, of om de openbare veiligheid en de rechten en vrijheden van anderen te beschermen[756].

- Het recht op rectificatie van persoonsgegevens. Lidstaten zijn verplicht om ervoor te zorgen dat een betrokkene, zonder onnodige vertraging, de rectificatie van onjuiste persoonsgegevens kan verkrijgen. Voorts heeft de betrokkene ook het recht om onvolledige persoonsgegevens te vervolledigen[757].

- Het recht om persoonsgegevens te wissen en de verwerking te beperken. In sommige gevallen moet de verwerkingsverantwoordelijke persoonsgegevens wissen. Voorts kan de betrokkene ervoor zorgen dat zijn/haar persoonsgegevens worden gewist, maar enkel als ze onrechtmatig worden verwerkt[758]. In bepaalde situaties kan de verwerking van persoonsgegevens beperkt worden in plaats van gewist. Dit kan gebeuren wanneer 1) de juistheid van de persoonsgegevens wordt betwist, maar dit niet kan worden vastgesteld of 2) de persoonsgegevens dienen als bewijsmateriaal[759].

Wanneer de verwerkingsverantwoordelijke weigert de persoonsgegevens te rectificeren of te wissen, of de verwerking van de gegevens weigert te beperken, moet de betrokkene schriftelijk in kennis worden gesteld. Lidstaten mogen dit recht op informatie beperken om, onder meer, de openbare veiligheid of de rechten en

754 *Ibid.*, artikel 13, lid 2.
755 *Ibid.*, artikel 14.
756 *Ibid.*, artikel 15.
757 *Ibid.*, artikel 16, lid 1.
758 *Ibid.*, artikel 16, lid 2.
759 *Ibid.*, artikel 16, lid 3.

vrijheden van anderen te beschermen, om dezelfde redenen als voor de beperking van het recht op toegang[760].

De betrokkene heeft normaal gesproken recht op informatie over de verwerking van zijn persoonsgegevens en heeft recht op toegang, de rectificatie, de wissing of de beperking van de verwerking, die hij/zij rechtstreeks bij de verwerkingsverantwoordelijke kan uitoefenen. Als uitwijkmogelijkheid is de indirecte uitoefening van de rechten van de betrokkene, via de toezichthoudende autoriteit voor gegevensbescherming, ook mogelijk in het kader van de richtlijn betreffende politiële en justitiële gegevensbescherming en wordt zij van kracht wanneer de verwerkingsverantwoordelijke het recht van de betrokkene beperkt[761]. Artikel 17 van de richtlijn bepaalt dat lidstaten maatregelen moeten vaststellen om ervoor te zorgen dat de rechten van betrokkenen ook kunnen worden uitgeoefend door middel van hun toezichthoudende autoriteit. Daarom moet de verwerkingsverantwoordelijke de betrokkene informeren over de mogelijkheid van indirecte toegang.

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

In het kader van de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten, zijn de verwerkingsverantwoordelijken bevoegde overheidsinstanties of andere instanties met relevante overheidsbevoegdheden en openbaar gezag die de doeleinden en middelen van de verwerking van persoonsgegevens bepalen. De richtlijn voorziet in verschillende verplichtingen voor verwerkingsverantwoordelijken om te zorgen voor een hoog beschermingsniveau van persoonsgegevens voor rechtshandhavingsdoeleinden.

De bevoegde autoriteiten dienen de verwerkingen die ze verrichten bij te houden met systemen voor geautomatiseerde gegevensverwerking. Deze logbestanden moeten ten minste de inzameling, verandering, raadpleging, openbaarmaking, met inbegrip van overdrachten, samenstellingen en uitwissing van persoonsgegevens bevatten[762]. De richtlijn bepaalt dat de logbestanden van raadpleging en bekendmaking het mogelijk moeten maken om de datum en het tijdstip van de handelingen, de redenen en, indien mogelijk, de identiteit van de persoon die het systeem heeft geraadpleegd of de persoonsgegevens heeft bekendgemaakt, en de

760 *Ibid.*, artikel 16, lid 4.

761 *Ibid.*, artikel 17.

762 *Ibid.*, artikel 25, lid 1.

ontvangers van die persoonsgegevens vast te stellen. De logbestanden worden uitsluitend gebruikt om te controleren of de verwerking rechtmatig is, voor interne controles, ter waarborging van de integriteit en de beveiliging van de persoonsgegevens en voor strafrechtelijke procedures[763]. Op aanvraag van de toezichthoudende autoriteit moeten de verwerkingsverantwoordelijke en de verwerker de logbestanden ter beschikking stellen.

In het bijzonder is er een algemene verplichting voor verwerkingsverantwoordelijken om passende technische en organisatorische maatregelen toe te passen om ervoor te zorgen dat de verwerking wordt uitgevoerd in overeenstemming met de richtlijn en om de rechtmatigheid van deze verwerking aan te tonen[764]. Bij het ontwerpen van deze maatregelen moeten ze de aard, de reikwijdte, de context van de verwerking en, belangrijker nog, de mogelijke risico's voor de rechten en vrijheden van natuurlijke personen in aanmerking nemen. Verwerkingsverantwoordelijken moeten een intern beleid vaststellen en maatregelen nemen die de naleving van de beginselen inzake gegevensbescherming vergemakkelijken, met name het beginsel van gegevensbescherming door ontwerp en door standaardinstellingen[765]. Wanneer een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten van natuurlijke personen, bijvoorbeeld door het gebruik van een nieuwe technologie, moeten verwerkingsverantwoordelijken een gegevensbeschermingseffectbeoordeling uitvoeren alvorens met de verwerking te beginnen[766]. De richtlijn bevat ook de maatregelen die moeten worden uitgevoerd door de verwerkingsverantwoordelijken om de beveiliging van de verwerking te waarborgen. Ze bevatten maatregelen om onbevoegde toegang tot door hen verwerkte persoonsgegevens te voorkomen, om ervoor te zorgen dat geautoriseerde personen uitsluitend toegang krijgen tot de persoonsgegevens waarop hun toegangsbevoegdheid betrekking heeft, dat de functies van het verwerkingssysteem naar behoren werken en dat opgeslagen persoonsgegevens niet kunnen worden beschadigd door een storing in het systeem[767]. Indien er toch een inbreuk op persoonsgegevens plaatsvindt, moeten verwerkingsverantwoordelijken de toezichthoudende autoriteiten binnen drie dagen in kennis stellen met een beschrijving van de aard van de inbreuk, de waarschijnlijke gevolgen, de betrokken categorieën persoonsgegevens en het geschatte aantal betrokkenen. De inbreuk op persoonsgegevens moet ook "zonder onnodige vertraging"

763 *Ibid.*, artikel 25, lid 2.

764 *Ibid.*, artikel 19.

765 *Ibid.*, artikel 20.

766 *Ibid.*, artikel 27.

767 *Ibid.*, artikel 29.

worden meegedeeld aan de betrokkene indien de inbreuk waarschijnlijk een hoog risico inhoudt voor zijn/haar rechten en vrijheden[768].

De richtlijn bevat het verantwoordingsbeginsel dat de verwerkingsverantwoordelijkheden verplicht om maatregelen uit te voeren met het oog op de naleving van dit beginsel. Verwerkingsverantwoordelijken moeten een register bijhouden van alle categorieën verwerkingsactiviteiten die onder hun verantwoordelijkheden worden uitgevoerd: de gedetailleerde inhoud van dergelijke registers is vermeld in artikel 24 van de richtlijn. De registers moeten op verzoek beschikbaar worden gesteld aan de toezichthoudende autoriteit, zodat deze kan toezien op de verwerkingsprocessen van de verwerkingsverantwoordelijke. Een andere belangrijke maatregel om de verantwoordingsplicht te vergroten, is de aanwijzing van een functionaris voor gegevensbescherming (DPO). Verwerkingsverantwoordelijken moeten een DPO aanstellen, hoewel de richtlijn lidstaten toelaat een uitzondering hierop te maken voor rechtbanken en andere onafhankelijke gerechtelijke autoriteiten[769]. De taken van de DPO lijken op de taken die voorzien zijn in het kader van de AVG. Hij/zij ziet toe op de naleving van de richtlijn, verstrekt informatie en geeft advies aan werknemers die gegevens verwerken over hun verplichtingen onder de wetgeving inzake gegevensbescherming. De DPO verstrekt ook advies over de noodzaak om een gegevensbeschermingseffectbeoordeling uit te voeren en fungeert als contactpunt voor de toezichthoudende autoriteit.

Doorgifte aan derde landen of aan internationale organisaties

Net als bij de AVG stelt de richtlijn voorwaarden vast voor de doorgifte van persoonsgegevens aan derde landen of aan internationale organisaties. Indien persoonsgegevens vrij buiten de rechtsmacht van de EU worden doorgegeven, kunnen de waarborgen en sterke bescherming die in het kader van het Unierecht worden voorzien, ondermijnd worden. De voorwaarden zelf wijken evenwel sterk af van die in de AVG. De doorgifte van persoonsgegevens aan derde landen of internationale organisaties is toegestaan indien[770]:

- de doorgifte noodzakelijk is voor de doelstellingen van de richtlijn;

768 *Ibid.*, artikelen 30 en 31.

769 *Ibid.*, artikel 32.

770 *Ibid.*, artikel 35.

- de persoonsgegevens worden doorgegeven aan een bevoegde autoriteit, in de zin van de richtlijn, van het derde land of de internationale organisatie, hoewel er een derogatie op deze regel bestaat in individuele en specifieke gevallen[771];

- doorgifte aan derde landen of internationale organisaties van persoonsgegevens die werden verkregen in de loop van grensoverschrijdende samenwerking de toelating vereist van de lidstaat waaruit de gegevens afkomstig zijn, hoewel er uitzonderingen bestaan in dringende gevallen;

- een adequaatheidsbesluit werd genomen door de Europese Commissie, passende waarborgen werden vastgesteld, of de derogatie voor doorgiften in specifieke situaties van toepassing is;

- verdere doorgiften van persoonsgegevens aan een ander derde land of internationale organisatie de voorafgaande toestemming van de verzendende bevoegde autoriteit vereisen, die rekening zal houden met, onder andere, de ernst van de inbreuk en het niveau van gegevensbescherming in het land van bestemming van de tweede internationale doorgifte[772].

In het kader van de richtlijn kunnen doorgiften van persoonsgegevens plaatsvinden indien aan een van de drie voorwaarden wordt voldaan. De eerste is wanneer de Europese Commissie een adequaatheidsbesluit in het kader van de richtlijn heeft genomen. Het besluit kan van toepassing zijn op het gehele grondgebied van een derde land of op specifieke sectoren van een derde land of van een internationale organisatie. Dit kan echter enkel gebeuren als een gepaste bescherming wordt verzekerd en wordt voldaan aan de voorwaarden die in de richtlijn staan beschreven[773]. In dergelijke gevallen is de doorgifte van persoonsgegevens niet onderworpen aan de toestemming van de lidstaat[774]. De Europese Commissie moet toezicht houden op de ontwikkelingen die gevolgen kunnen hebben voor de werking van adequaatheidsbesluiten. Bovendien moet het besluit een mechanisme voor periodieke beoordeling bevatten. De Commissie kan ook het besluit intrekken, wijzigen of opschorten indien uit de beschikbare informatie blijkt dat de voorwaarden in het derde land of de internationale organisatie niet langer een passende bescherming

771 *Ibid.*, artikel 39.

772 *Ibid.*, artikel 35, lid 1.

773 *Ibid.*, artikel 36.

774 *Ibid.*, artikel 36, lid 1.

bieden. Indien dit het geval is, moet de Commissie overleg plegen met het derde land of de internationale organisatie en trachten de situatie te verhelpen.

Bij gebreke van een adequaatheidsbesluit kunnen doorgiften gebaseerd worden op passende waarborgen. Zij kunnen worden vastgesteld in een juridisch bindend instrument of de verwerkingsverantwoordelijke kan zelf een beoordeling uitvoeren van de omstandigheden waaronder de doorgifte van persoonsgegevens plaatsvond, en concluderen dat er passende waarborgen in plaats zijn. De zelfbeoordeling kan rekening houden met mogelijke samenwerkingsovereenkomsten die werden afgesloten tussen Europol of Eurojust en het derde land of de internationale organisatie, het bestaan van geheimhoudingsverplichtingen en doelbinding alsmede garanties dat de gegevens niet zullen worden gebruikt voor enige vorm van wrede en onmenselijke behandelingen, met inbegrip van de doodstraf[775]. In dit laatste geval moet de verwerkingsverantwoordelijke de bevoegde toezichthoudende autoriteit op de hoogte stellen van de categorieën van doorgiften in het kader van deze categorie[776].

Indien geen adequaatheidsbesluit werd genomen of geen passende waarborgen zijn vastgesteld, kunnen doorgiften nog steeds worden toegestaan in specifieke situaties die de richtlijn beschrijft. Deze omvatten onder meer de bescherming van de vitale belangen van betrokkenen of andere personen, en de voorkoming van een onmiddellijk en ernstig gevaar voor de openbare veiligheid van de lidstaat of een derde land[777].

In individuele en specifieke gevallen kunnen er doorgiften plaatsvinden door bevoegde autoriteiten aan ontvangers in derde landen die geen bevoegde autoriteit zijn indien, naast het feit dat er aan een van de hierboven beschreven drie voorwaarden werd voldaan, er ook wordt voldaan aan de aanvullende voorwaarden uit artikel 39 van de richtlijn. In het bijzonder moet de doorgifte strikt noodzakelijk zijn voor de vervulling van een taak van de bevoegde autoriteit die de doorgifte uitvoert en die ook verantwoordelijk is voor de vaststelling dat de grondrechten of fundamentele vrijheden van natuurlijke personen niet zwaarder wegen dan het openbare belang dat de doorgifte rechtvaardigt. Dergelijke doorgiften moeten

775 *Ibid.*, overweging 71.

776 *Ibid.*, artikel 37, lid 1.

777 *Ibid.*, artikel 38, lid 1.

worden gedocumenteerd en de bevoegde autoriteit die de doorgifte uitvoert moet de bevoegde toezichthoudende autoriteit in kennis stellen[778].

Tot slot, en met betrekking tot derde landen en internationale organisaties, vereist de richtlijn ook de ontwikkeling van internationale samenwerkingsmechanismen om de doeltreffende handhaving van de wetgeving te vergemakkelijken en om de toezichthoudende autoriteiten inzake gegevensbescherming te helpen samenwerken met hun buitenlandse tegenhangers[779].

Onafhankelijk toezicht en oplossingen voor de betrokkenen

Elke lidstaat moet ervoor zorgen dat een of meer onafhankelijke toezichthoudende autoriteiten belast worden met het verstrekken van adviezen over en het houden van toezicht op de toepassing van de bepalingen die krachtens de richtlijn zijn vastgesteld[780]. De toezichthoudende autoriteit die wordt opgericht uit hoofde van de AVG mag dezelfde zijn als de toezichthoudende autoriteit die is opgericht voor de toepassing van de richtlijn. De lidstaten mogen echter een andere autoriteit benoemen, mits deze aan de criteria van onafhankelijkheid voldoet. Ook behandelen toezichthoudende autoriteiten klachten van personen over de bescherming van hun rechten en vrijheden in het kader van de verwerking van persoonsgegevens door bevoegde autoriteiten.

Wanneer de uitoefening van de rechten van de betrokkene om dwingende redenen wordt geweigerd, moet de betrokkene het recht hebben om in beroep te gaan bij de bevoegde nationale toezichthoudende autoriteit en/of een rechtbank. Indien een persoon schade lijdt ten gevolge van een schending van de nationale wetgeving ter uitvoering van de richtlijn, heeft hij/zij recht op een schadevergoeding van de verwerkingsverantwoordelijke of een andere bevoegde autoriteit in het kader van het recht van de lidstaat[781]. Over het algemeen moeten betrokkenen in geval van schending van hun rechten die hun door nationale wetgeving ter uitvoering van de richtlijn worden gegarandeerd, toegang hebben tot een rechtsmiddel[782].

778 *Ibid.*, artikel 37, lid 3.

779 *Ibid.*, artikel 40.

780 *Ibid.*, artikel 41.

781 *Ibid.*, artikel 56.

782 *Ibid.*, artikel 54.

8.3. Andere specifieke rechtsinstrumenten inzake gegevensbescherming bij strafzaken

In aanvulling op de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten is de uitwisseling van informatie die door de lidstaten in specifieke gebieden wordt beheerd, geregeld door een aantal rechtsinstrumenten — zoals Kaderbesluit 2009/315/JBZ van de Raad betreffende de organisatie en de inhoud van uitwisseling van gegevens uit het strafregister tussen de lidstaten, Besluit 2000/642/JBZ van de Raad inzake een regeling voor samenwerking tussen de financiële inlichtingeneenheden van de lidstaten bij de uitwisseling van gegevens, en Kaderbesluit 2006/960/JBZ van de Raad van 18 december 2006 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de wetshandhavingsinstanties van de lidstaten van de Europese Unie[783].

Belangrijk is dat bij grensoverschrijdende samenwerking[784] tussen bevoegde autoriteiten steeds vaker immigratiegegevens worden uitgewisseld. Dit rechtsdomein wordt niet gezien als onderdeel van de politiële en justitiële samenwerking in strafzaken, maar is in veel opzichten relevant voor het werk van politiële en justitiële autoriteiten. Hetzelfde geldt voor gegevens over goederen die in de EU worden in- of uitgevoerd. De afschaffing van de interne grenscontroles binnen het Schengengebied heeft het risico op fraude verhoogd, waardoor het noodzakelijk is dat de lidstaten hun samenwerking intensiveren, met name door de grensoverschrijdende informatie-uitwisseling te versterken, om schendingen van de nationale en EU-douanewetgeving beter te kunnen opsporen en vervolgen. Daarnaast is er in de afgelopen jaren een stijging van ernstige en georganiseerde misdaad en terrorisme in de wereld die betrekking kan hebben op het internationale reizigersverkeer, en in veel

783 De Raad van de Europese Unie (2009), Kaderbesluit 2009/315/JBZ van de Raad van 26 februari 2009 betreffende de organisatie en de inhoud van uitwisseling van gegevens uit het strafregister tussen de lidstaten, PB L 93 van 2009; de Raad van de Europese Unie (2000), Besluit 2000/642/JBZ van de Raad van 17 oktober 2000 betreffende een regeling voor samenwerking tussen de financiële inlichtingeneenheden van de lidstaten bij de uitwisseling van gegevens, PB L 271 van 2000; Kaderbesluit 2006/960/JBZ van de Raad van 18 december 2006 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de wetshandhavingsinstanties van de lidstaten van de Europese Unie, PB L 386.

784 Europese Commissie (2012), Mededeling van de Commissie aan het Europees Parlement en de Raad — Versterking van de samenwerking inzake rechtshandhaving in de Europese Unie: het Europees model voor informatie-uitwisseling (EIXM), COM(2012) 735 def., Brussel, 7 december 2012.

gevallen heeft dit aangetoond dat er behoefte is aan meer grensoverschrijdende samenwerking tussen politie en rechtshandhaving[785].

Het Prüm-besluit

Een belangrijk voorbeeld van geïnstitutionaliseerde grensoverschrijdende samenwerking door de uitwisseling van nationaal bewaarde gegevens is Besluit 2008/615/JBZ van de Raad, samen met de uitvoeringsbepaling in Besluit 2008/615/JBZ, inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit (Prüm-besluit), waarbij het Verdrag van Prüm in 2008 in het Unierecht is geïntegreerd[786]. Het Verdrag van Prüm was een internationaal politiesamenwerkingsakkoord dat in 2005 door België, Duitsland, Frankrijk, Luxemburg, Nederland, Oostenrijk en Spanje werd ondertekend[787].

Het Prüm-besluit streeft ernaar de informatie-uitwisseling tussen ondertekenende lidstaten te verbeteren met het oog op de preventie en bestrijding van criminaliteit op drie gebieden: terrorisme, grensoverschrijdende criminaliteit en illegale migratie. Hiertoe bevat het besluit bepalingen inzake:

- geautomatiseerde toegang tot dna-profielen, vingerafdrukgegevens en bepaalde gegevens uit nationale kentekenregisters;
- de verstrekking van gegevens in samenhang met grootschalige evenementen met een grensoverschrijdende dimensie;
- de verstrekking van gegevens ter voorkoming van terroristische strafbare feiten;
- andere maatregelen om de grensoverschrijdende politiesamenwerking te intensiveren.

785 Zie Europese Commissie (2011), Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende het gebruik van persoonsgegevens van passagiers voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, COM(2011) 32 def., Brussel, 2 februari 2011, blz. 1.

786 Raad van de Europese Unie (2008), Besluit 2008/615/JBZ van de Raad van 23 juni 2008 betreffende de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit, PB L 210 van 2008.

787 Verdrag tussen het Koninkrijk België, de Bondsrepubliek Duitsland, het Koninkrijk Spanje, de Republiek Frankrijk, het Groothertogdom Luxemburg, het Koninkrijk der Nederlanden en de Republiek Oostenrijk inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van het terrorisme, de grensoverschrijdende criminaliteit en de illegale migratie.

De databanken die beschikbaar worden gesteld onder het Prüm-besluit worden volledig beheerst door het nationale recht, maar de uitwisseling van gegevens wordt tevens bestuurd door het besluit waarvan de verenigbaarheid met de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten moet worden beoordeeld. De bevoegde organen voor het houden van toezicht op dit gegevensverkeer zijn de nationale toezichthoudende autoriteiten voor gegevensbescherming.

Kaderbesluit 2006/960/JBZ — Het Zweeds initiatief

Kaderbesluit 2006/960/JBZ (Zweeds initiatief)[788] vormt een ander voorbeeld van grensoverschrijdende samenwerking met betrekking tot de uitwisseling van gegevens op nationaal niveau door de wetshandhavingsinstanties. Het Zweeds initiatief spitst zich uitdrukkelijk toe op de uitwisseling van inlichtingen en informatie en voorziet in specifieke regels inzake gegevensbescherming in artikel 8.

Volgens dit instrument moet het gebruik van de uitgewisselde informatie en inlichtingen onderworpen zijn aan de nationale bepalingen inzake gegevensbescherming van de lidstaat die de inlichtingen ontvangt, volgens dezelfde regels, alsof ze werden verzameld in die lidstaat. Artikel 8 gaat nog een stap verder door te stellen dat wanneer informatie en inlichtingen worden verstrekt, de bevoegde wetshandhavingsinstantie voorwaarden mag opleggen die in overeenstemming zijn met de nationale wetgeving inzake hun gebruik door de ontvangende bevoegde wetshandhavingsinstantie. Deze voorwaarden kunnen ook van toepassing zijn op de rapportage van het resultaat van het strafrechtelijk onderzoek of op de criminele inlichtingenactiviteiten waarvoor de uitwisseling van informatie en inlichtingen vereist was. Wanneer het nationale recht evenwel voorziet in uitzonderingen op de beperkingen op het gebruik (bv. voor rechterlijke instanties, wetgevende organen enz.), mogen de informatie en de inlichtingen enkel worden gebruikt na voorafgaande raadpleging met de verstrekkende lidstaat.

De verstrekte informatie en inlichtingen kunnen worden gebruikt:

- voor het doel waarvoor zij zijn verstrekt, of
- om een onmiddellijke en ernstige bedreiging van de openbare veiligheid te voorkomen.

788 Raad van de Europese Unie (2006), Kaderbesluit 2006/960/JBZ van de Raad van 18 december 2006 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de wetshandhavingsinstanties van de lidstaten van de Europese Unie, PB L 386 van 29.12.2006, blz. 89.

Verwerkingen voor andere doeleinden kunnen worden toegestaan, maar enkel na voorafgaande toestemming van de verstrekkende lidstaat.

Het Zweeds initiatief stelt voorts dat de verwerkte persoonsgegevens moeten worden beschermd overeenkomstig de internationale instrumenten, zoals:

- het Verdrag van de Raad van Europa tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens[789];
- het Aanvullend Protocol van 8 november 2001 bij dat Verdrag, met betrekking tot de toezichthoudende autoriteiten en grensoverschrijdende gegevensstromen[790];
- Aanbeveling nr. R (87) 15 van de Raad van Europa over het gebruik van persoonsgegevens in de politiële sector[791].

EU-richtlijn inzake PNR-gegevens

Persoonsgegevens van passagiers (PNR) hebben betrekking op de informatie over vliegtuigpassagiers die wordt verzameld en bewaard in de boekings- en vertrekcontrolesystemen voor hun eigen commerciële doeleinden. Deze gegevens bevatten verschillende soorten informatie zoals reisdata, reisschema's, ticketinformatie, contactgegevens, het reisagentschap waar de reis werd geboekt, betaalmiddelen, stoelnummers en bagage[792]. De verwerking van PNR-gegevens kan wetshandhavingsinstanties helpen om bekende of potentiële verdachten te identificeren en om beoordelingen te verrichten op basis van reispatronen en andere indicatoren die vaak geassocieerd worden met strafbare feiten. Een analyse van PNR-gegevens maakt het ook mogelijk om de reisroutes en contacten van personen die ervan worden verdacht betrokken te zijn in criminele activiteiten, achteraf op te sporen

789 Raad van Europa (1981), Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, CETS nr. 108.

790 Raad van Europa (2001), Aanvullend Protocol bij het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, betreffende toezichthoudende autoriteiten en grensoverschrijdende gegevensstromen, CETS nr. 108.

791 Raad van Europa (1987), Aanbeveling nr. R (87) 15 van het Comité van Ministers aan de lidstaten over het gebruik van persoonsgegevens in de politiële sector (goedgekeurd door het Comité van Ministers op 17 september 1987 op de 410e vergadering van de afgevaardigden van de ministers).

792 Europese Commissie (2011), Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende het gebruik van persoonsgegevens van passagiers voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, COM(2011) 32 def., Brussel, 2 februari 2011, blz. 1.

waardoor wetshandhavingsinstanties in staat zijn criminele netwerken te identificeren[793]. De Europese Unie heeft een aantal overeenkomsten met derde landen afgesloten voor de uitwisseling van PNR-gegevens, zoals uiteengezet in punt 7. Daarnaast werd de PNR-gegevensverwerking binnen de EU ingevoerd door middel van Richtlijn (EU) 2016/681 betreffende het gebruik van PNR-gegevens voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit (EU-richtlijn inzake PNR-gegevens)[794]. Deze richtlijn voorziet in verplichtingen voor de luchtvaartmaatschappijen om PNR-gegevens door te geven aan de bevoegde autoriteiten en strenge waarborgen inzake gegevensbescherming vast te stellen voor het verzamelen en verwerken van die gegevens. De EU-richtlijn inzake PNR-gegevens is van toepassing op internationale vluchten van en naar de EU, maar ook op vluchten binnen de EU indien een lidstaat daartoe besluit[795].

De PNR-gegevens die zijn verzameld, mogen enkel de informatie bevatten die door de EU-richtlijn inzage PNR-gegevens wordt toegestaan. Ze moeten in één enkele informatie-eenheid worden bewaard, op een veilige plaats in elke lidstaat. PNR-gegevens moeten zes maanden na hun doorgifte door de luchtvaartmaatschappij geanonimiseerd worden en mogen voor een maximumperiode van vijf jaar worden bewaard[796]. PNR-gegevens worden uitgewisseld tussen de lidstaten; tussen de lidstaten en Europol, en met derde landen, maar per individueel geval.

De overdracht en verwerking van de PNR-gegevens en de rechten die voor de betrokkenen worden gewaarborgd, moeten in overeenstemming zijn met de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten en moeten zorgen voor het hoge niveau van bescherming van de persoonlijke levenssfeer en de persoonsgegevens die vereist zijn in het Handvest, het Gemoderniseerd Verdrag 108 en het EVRM.

De onafhankelijke nationale toezichthoudende autoriteiten die bevoegd zijn in het kader van de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten, zijn ook verantwoordelijk voor het verstrekken van advies over en het

793 Europese Commissie (2015), Informatieblad bestrijding van terrorisme op EU-niveau, een overzicht van de acties, maatregelen en initiatieven van de Commissie, Brussel, 11 januari 2015.

794 Richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 betreffende het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, PB L 119 van 2016, blz. 132.

795 PNR-richtlijn, L 119, blz. 132, artikel 1, lid 1, en artikel 2, lid 1.

796 *Ibid.*, artikel 12, lid 1, en artikel 12, lid 2.

toezicht op de toepassing van de bepalingen die door de lidstaten werden vastgesteld krachtens de EU-richtlijn inzake PNR-gegevens.

Het bewaren van telecommunicatiegegevens

De richtlijn gegevensbewaring[797] — nietig verklaard op 8 april 2014 in *Digital Rights Ireland* — verplichtte de verleners van communicatiediensten ertoe metagegevens beschikbaar te houden met het specifieke doel van de bestrijding van ernstige criminaliteit, voor minstens zes, maar niet meer dan 24 maanden, ongeacht de vraag of de aanbieder deze gegevens nog steeds nodig had voor factureringsdoeleinden of om de dienst technisch aan te bieden.

Het bewaren van telecommunicatiegegevens is duidelijk een inmenging in het recht op gegevensbescherming[798]. Of deze inmenging al dan niet gerechtvaardigd is, werd in verschillende rechtsprocedures in EU-lidstaten betwist[799].

Voorbeeld: In *Digital Rights Ireland* en *Kärntner Landesregierung e.a.*[800] brachten the Digital Rights-groep en de heer Seitlinger een zaak voor respectievelijk het Hooggerechtshof in Ierland en het Constitutioneel Gerechtshof in Oostenrijk om de wettigheid van de nationale maatregelen die de bewaring van elektronische telecommunicatiegegevens mogelijk maakte, aan te vechten. Digital Rights vroeg het Ierse gerechtshof om Richtlijn 2006/24/EG en het deel over het nationale strafrecht in verband met terroristische misdrijven nietig te verklaren. Evenzo vochten de heer Seitlinger en meer dan 11 000 andere aanvragers een bepaling aan van de Oostenrijkse wetgeving inzake telecommunicatie die de richtlijn 2006/24 omzette, en verzochten om de nietigverklaring ervan.

797 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken, en tot wijziging van Richtlijn 2002/58/EG, PB L 105 van 2006.

798 EDPS (2011), *Advies van 31 mei 2011 over het evaluatieverslag van de Commissie aan de Raad en het Europees Parlement over de richtlijn gegevensbewaring (Richtlijn 2006/24/EG)*, 31 mei 2011.

799 Duitsland, Constitutioneel Gerechtshof (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 maart 2010; Roemenië, Constitutioneel Gerechtshof (*Curtea Constituțională a României*), nr. 1258, 8 oktober 2009; de Tsjechische Republiek, Constitutioneel Gerechtshof (Ústavní soud České republiky), 94/2011 Coll., 22 maart 2011.

800 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en *Kärntner Landesregierung e.a.* [Grote kamer], 8 april 2014, punt 65.

Bij de behandeling van deze verzoeken om prejudiciële beslissingen, verklaarde het HvJ-EU de richtlijn gegevensbewaring ongeldig. Volgens het HvJ-EU gaven de gegevens die in het kader van de richtlijn konden worden bewaard, over het geheel nauwkeurige informatie over natuurlijke personen. Voorts heeft het HvJ-EU de ernst van de inmenging in de grondrechten op eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens onderzocht. Het stelde vast dat de bewaring een doel van algemeen belang diende, met name de strijd tegen ernstige vormen van criminaliteit, en dus de openbare veiligheid. Niettemin heeft het HvJ-EU verklaard dat de EU-wetgever het evenredigheidsbeginsel heeft geschonden door de vaststelling van de richtlijn. Hoewel de richtlijn aangewezen kan zijn om de gewenste doelstelling te bereiken, is "de ruime en bijzonder ernstige inmenging van de richtlijn in het fundamentele recht op eerbiediging van het privéleven en de bescherming van persoonsgegevens niet voldoende omkaderd om te waarborgen dat de inmenging beperkt wordt tot het strikt noodzakelijke."

Bij gebrek aan een specifieke wetgeving betreffende de bewaring van gegevens, is deze bewaring toegestaan als een uitzondering op de vertrouwelijkheid van telecommunicatiegegevens in het kader van Richtlijn 2002/58/EG (richtlijn betreffende de privacy en elektronische communicatie)[801] als preventiemaatregel, maar uitsluitend met het oog op de bestrijding van ernstige criminaliteit. Een dergelijke bewaring moet beperkt blijven tot het strikt noodzakelijke met betrekking tot de categorieën van de bewaarde gegevens, de betrokken communicatiemiddelen, de betrokkenen en de gekozen duur van de bewaring. De nationale autoriteiten mogen toegang hebben tot de bewaarde gegevens onder strikte voorwaarden, met inbegrip van voorafgaande beoordeling door een onafhankelijke instantie. De gegevens moeten worden bewaard in de EU.

Voorbeeld: Na de uitspraak in de zaak *Digital Rights Ireland* en *Kärntner Landesregierung e.a.*[802] werden nog twee andere zaken voorgelegd aan het HvJ-EU met betrekking tot de algemene verplichting in Zweden

801 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), PB L 201 van 2002.

802 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a. en Kärntner Landesregierung e.a.* [Grote kamer], 8 april 2014.

en het VK voor aanbieders van elektronische communicatiediensten om telecommunicatiegegevens te bewaren, zoals vereist door de nietigverklaarde richtlijn gegevensbewaring. In *Tele2 Sverige* en *Home Department/Tom Watson e.a.*[803] oordeelde het HvJ-EU dat de nationale wetgeving die de algemene en willekeurige bewaring van gegevens voorschrijft zonder een verband tussen de te bewaren gegevens en een gevaar voor de openbare veiligheid aan te tonen, evenals zonder een voorwaarde te vermelden — bv. de termijn voor de bewaring, het geografische gebied, de groep personen die wellicht betrokken zijn bij een ernstig misdrijf — de grens overschrijdt van het strikt noodzakelijke en niet kan worden gerechtvaardigd in een democratische maatschappij, zoals vereist door Richtlijn 2002/58/EG, gelezen in het licht van het EU-Handvest van de grondrechten.

Vooruitzichten

In januari 2017 heeft de Europese Commissie een voorstel voor een verordening met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie gepubliceerd, die is bedoeld ter intrekking en vervanging van Richtlijn 2002/58/EG[804]. Het voorstel bevat geen specifieke bepalingen inzake gegevensbewaring. Het bepaalt echter dat lidstaten bepaalde verplichtingen en rechten in het kader van de verordening bij wet mogen beperken, wanneer een dergelijke beperking een noodzaak en een evenredige maatregel vormt ter bescherming van een specifiek algemeen belang, met inbegrip van de nationale veiligheid, defensie, openbare veiligheid en het voorkomen, opsporen of vervolgen van strafbare feiten of de tenuitvoerlegging van strafrechtelijke sancties[805]. Daarom kunnen lidstaten nationale kaders voor de bewaring van gegevens, die gerichte retentiemaatregelen bieden, houden of instellen, voor zover die kaders in overeenstemming zijn met het Unierecht, daarbij rekening houdend met de jurisprudentie van het HvJ-EU over de interpretatie van de e-Privacy-richtlijn

803 HvJ-EU, gevoegde zaken C-203/15 en C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen* en *Secretary of State for the Home Department/Tom Watson e.a.* [Grote kamer], 21 december 2016.

804 Europese Commissie (2017), *Voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie)*, COM(2017) 10 def., Brussel, 10 januari 2017.

805 *Ibid.*, overweging 26.

en het EU-Handvest van de grondrechten[806]. Ten tijde van het opstellen van het handboek, was de vaststelling van de richtlijn gaande.

EU-VS-raamovereenkomst inzake de bescherming van voor wetshandhavingsdoeleinden uitgewisselde persoonsgegevens

Op 1 februari 2017 werd de EU-VS-raamovereenkomst inzake de verwerking van persoonsgegevens voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten in de VS van kracht[807]. De EU-VS-raamovereenkomst is bedoeld om een hoog niveau van gegevensbescherming voor EU-burgers te waarborgen en tegelijkertijd de samenwerking van de rechtshandhavingsautoriteiten van de EU en de VS te versterken. Hij vormt een aanvulling op bestaande overeenkomsten tussen rechtshandhavingsautoriteiten van de EU en de VS of van een lidstaat en de VS, terwijl de overeenkomst ook in duidelijke en geharmoniseerde regels inzake gegevensbescherming wil voorzien voor toekomstige overeenkomsten op dit gebied. In dat verband heeft de overeenkomst tot doel een blijvend wettelijk kader vast te stellen ter vergemakkelijking van de uitwisseling van informatie.

De overeenkomst bevat zelf geen passende rechtsgrondslag voor de uitwisseling van persoonsgegevens, maar biedt de betrokken personen passende waarborgen inzake gegevensbescherming. Hij heeft betrekking op alle verwerking van persoonsgegevens die noodzakelijk is voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, met inbegrip van terrorisme[808].

De overeenkomst bevat verschillende waarborgen om ervoor te zorgen dat persoonsgegevens enkel worden gebruikt voor de genoemde doelstellingen in de overeenkomst. Met name de volgende bescherming wordt aan EU-burgers geboden:

806 Zie de toelichting bij het voorstel voor een verordening betreffende privacy en elektronische communicatie COM(2017) 10 def., punt 1.3.

807 Zie de Raad van de EU (2016), *"Betere rechten inzake gegevensbescherming voor de EU-burgers bij de samenwerking op het gebied van wetshandhaving: EU en VS tekenen de "raamovereenkomst""*, Persbericht 305/16 van 2 juni 2016.

808 Overeenkomst tussen de Verenigde Staten van Amerika en de Europese Unie over de bescherming van persoonlijke informatie in verband met de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten van 18 mei 2016, (OR.en) 8557/16, artikel 3, lid 1. Zie ook de mededeling van de Commissie over de onderhandelingen voor de EU-VS-overeenkomst inzake gegevensbescherming van 26 mei 2010, MEMO/10/216, en het persbericht van de Europese Commissie (2010) over de hoge privacynormen in de EU-VS-overeenkomst inzake gegevensbescherming van 26 mei 2010, IP/10/609.

- beperkingen op het gebruik van gegevens: persoonsgegevens mogen uitsluitend worden gebruikt met het oog op het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten;

- bescherming tegen willekeurige en ongerechtvaardigde discriminatie;

- verdere doorgiften: een verdere doorgifte aan een land dat niet de VS is en geen EU-land of internationale organisatie moet onderworpen zijn aan voorafgaande toestemming van de bevoegde autoriteit van het land dat de gegevens oorspronkelijk heeft doorgegeven;

- kwaliteit gegevens: persoonsgegevens moeten worden bewaard met inachtneming van hun relevantie, juistheid, tijdigheid en volledigheid;

- de beveiliging van de verwerking, met inbegrip van de kennisgeving van inbreuken op persoonsgegevens;

- de verwerking van gevoelige gegevens is uitsluitend toegestaan onder passende waarborgen overeenkomstig het recht;

- bewaringstermijnen: persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk of passend is;

- de rechten van toegang en rectificatie: elke natuurlijke persoon heeft, onder bepaalde voorwaarden, recht op toegang tot zijn/haar persoonsgegevens, en kan verzoeken om rectificatie van de gegevens indien zij onjuist zijn;

- geautomatiseerde besluiten vereisen passende waarborgen, met inbegrip van de mogelijkheid tot het verkrijgen van menselijke tussenkomst;

- een doeltreffend toezicht, met inbegrip van de samenwerking tussen EU- en VS-toezichthouders, en

- gerechtelijk beroep en afdwingbaarheid: EU-burgers hebben het recht[809] om bij een rechterlijke instantie in de VS in beroep te gaan in zaken waarin

809 De Amerikaanse wet inzake gerechtelijk beroep werd ondertekend door president Obama op 24 februari 2016.

VS-autoriteiten weigeren toegang te verlenen of wijzigingen te maken, of onrechtmatig hun persoonsgegevens openbaar maken.

In het kader van de "raamovereenkomst" werd er ook een systeem opgezet om de bevoegde toezichthoudende autoriteiten in de lidstaat van de betrokken persoon, indien nodig, in kennis te stellen van alle inbreuken op de bescherming van gegevens. De juridische garanties die door de overeenkomst worden verstrekt zorgen voor de gelijke behandeling van EU-burgers in de VS in geval van een privacyschending[810].

8.3.1. Gegevensbescherming in de justitiële en wetshandhavingsinstanties van de Europese Unie

Europol

Europol, het rechtshandhavingsagentschap van de EU, heeft zijn hoofdkantoor in Den Haag, terwijl in elke lidstaat nationale Europol-eenheden (NEE's) zijn ingesteld. Europol is opgericht in 1998; de huidige juridische status als EU-instelling is gebaseerd op de verordening betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol-verordening)[811]. Het doel van Europol is ondersteuning te verlenen bij het voorkomen en onderzoeken van georganiseerde criminaliteit, terrorisme en andere vormen van ernstige criminaliteit als vermeld in bijlage I bij de Europol-verordening waarbij twee of meer EU-lidstaten betrokken zijn. Het doet dit door de uitwisseling van informatie en door te handelen als het informatieknooppunt van de EU dat inlichtingen, analyses en dreigingsevaluaties verstrekt.

---

810 De Europese Toezichthouder voor gegevensbescherming heeft een advies uitgebracht over de EU-VS-overeenkomst waarin onder meer de volgende aanpassingen worden aanbevolen: 1) "voor de specifieke doeleinden waarvoor zij zijn doorgegeven" toevoegen aan het artikel dat betrekking heeft op het niet langer dan nodig en passend bewaren van gegevens, en 2) de doorgifte in bulk van gevoelige gegevens, wat mogelijk is, uitsluiten. Zie Europese Toezichthouder gegevensbescherming, Advies 1/2016, *Voorlopig advies over de overeenkomst tussen de Verenigde Staten van Amerika en de Europese Unie inzake de bescherming van persoonsgegevens met betrekking tot het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten*, § 35.

811 Verordening (EU) 2016/794 van het Europees Parlement en de Raad van 11 mei 2016 betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol), en tot vervanging en intrekking van de Besluiten 2009/371/JBZ, 2009/934/JBZ, 2009/935/JBZ, 2009/936/JBZ en 2009/968/JBZ van de Raad, PB L 135 van 2016, blz. 53.

Om deze doelen te verwezenlijken, heeft Europol het Europol-informatiesysteem opgezet, dat een databank omvat waarin de lidstaten inlichtingen en informatie over criminele activiteiten kunnen uitwisselen via hun NEE's. Het Europol-informatiesysteem kan worden gebruikt om gegevens beschikbaar te stellen die verband houden met personen die worden verdacht van of zijn veroordeeld voor een strafbaar feit dat onder de bevoegdheid van Europol valt of met personen ten aanzien van wie er feitelijke aanwijzingen zijn dat zij dergelijke strafbare feiten zullen plegen. Europol en de NEE's kunnen gegevens rechtstreeks invoeren in het Europol-informatiesysteem en gegevens uit het systeem opvragen. Alleen de partij die de gegevens in het systeem heeft ingevoerd, mag deze wijzigen, corrigeren of verwijderen. EU-instellingen, derde landen en internationale organisaties kunnen ook informatie verstrekken aan Europol.

Informatie, met inbegrip van persoonsgegevens, kan ook worden verkregen door Europol uit algemeen toegankelijke bronnen zoals het internet. De doorgifte van persoonsgegevens aan de EU-instellingen zijn alleen toegestaan indien dit noodzakelijk is voor het vervullen van de taken van Europol of het ontvangende EU-orgaan. De doorgifte van persoonsgegevens aan derde landen of internationale organisaties is uitsluitend toegestaan indien de Europese Commissie besluit dat het land of de betrokken internationale organisatie een passend niveau van gegevensbescherming biedt (adequaatheidsbesluit), of indien er een internationale of samenwerkingsovereenkomst is. Europol kan persoonsgegevens ontvangen en verwerken van private partijen en privépersonen onder de strikte voorwaarden dat deze gegevens door een NEE zijn doorgegeven in overeenkomst met de nationale wetgeving, door een contactpunt in een derde land of een internationale organisatie waarmee een samenwerking door middel van een samenwerkingsovereenkomst is vastgesteld, of door een autoriteit van een derde land of een internationale organisatie die onderworpen is aan een adequaatheidsbesluit of waarmee de EU een internationale overeenkomst heeft gesloten. Alle informatie-uitwisseling gebeurt door middel van een applicatie voor veilige informatie-uitwisseling (SIENA).

Naar aanleiding van nieuwe ontwikkelingen werden er gespecialiseerde centra opgericht binnen Europol. Het Europees Centrum voor de bestrijding van cybercriminaliteit werd binnen Europol opgericht in 2013[812]. Dit centrum fungeert als het EU-knooppunt voor informatie over cybercriminaliteit, en draagt bij tot snellere reacties in geval van via het internet gepleegde strafbare feiten, de ontwikkeling en

812 Zie ook de EDPS (2012), *Advies van de Europese Toezichthouder voor gegevensbescherming (EDPS) over de mededeling van de Europese Commissie aan de Raad en het Europees Parlement over de oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit*, Brussel, 29 juni 2012.

inzet van forensische capaciteit en de ontwikkeling van beste praktijken in onderzoeken naar cybercriminaliteit. Het centrum concentreert zich op cybercriminaliteit die:

- wordt gepleegd door georganiseerde groepen en die zeer winstgevend is, zoals internetfraude;
- de slachtoffers ernstige schade berokkent, zoals seksuele uitbuiting van kinderen via het internet;
- de kritieke infrastructuur- of informatiesystemen in de Unie schaadt.

Het Europees Centrum voor terrorismebestrijding (ECTC) werd opgericht in januari 2016 met als doel operationele steun aan lidstaten te geven bij onderzoeken in verband met terroristische misdrijven. Het voert kruiscontroles uit van "levende" operationele gegevens met de gegevens die Europol reeds bezit, waardoor er snel financiële aanknopingspunten aan het licht komen, en het analyseert alle beschikbare onderzoeksgegevens om tot een gestructureerd beeld van een terreurnetwerk te komen[813].

Het Europees Centrum tegen migrantensmokkel (EMSC) is opgericht in februari 2016, na een bijeenkomst van de Raad in november 2015, met als doel de lidstaten te ondersteunen bij de bepaling en ontmanteling van criminele netwerken die betrokken zijn bij migrantensmokkel. Het fungeert als informatieknooppunt dat de bureaus van de regionale taskforce van de Europese Unie in Catania (Italië) en Piraeus (Griekenland) bijstaat, die hulp bieden aan nationale autoriteiten in verschillende domeinen, met inbegrip van de uitwisseling van inlichtingen, criminele onderzoeken en de vervolging van criminele netwerken voor mensensmokkel[814].

Het stelsel voor gegevensbescherming dat de activiteiten van Europol bestrijkt, wordt verstrekt door en bouwt voort op de beginselen van de Verordening Gegevensbescherming EU-instellingen[815] en stemt ook overeen met de richtlijn

813 Zie de website van Europol op de ECTC.

814 Zie de website van Europol op de EMSC.

815 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, PB L 8 van 2001.

gegevensbescherming voor politiële en strafrechtelijke autoriteiten, het Gemoderniseerd Verdrag 108 en de Politieaanbeveling.

De verwerking van persoonsgegevens in verband met slachtoffers van een strafbaar feit, getuigen of andere personen die informatie kunnen verstrekken over strafbare feiten, of in verband met personen jonger dan achttien jaar, wordt toegestaan als dit strikt noodzakelijk en evenredig is voor de preventie of bestrijding van criminaliteit die onder de doelstellingen van Europol valt[816]. De verwerking van gevoelige persoonsgegevens is verboden, tenzij dit strikt noodzakelijk en evenredig is ter voorkoming of bestrijding van misdaad die onder de bevoegdheid van Europol valt en deze gegevens andere door Europol verwerkte persoonsgegevens aanvullen[817]. In beide gevallen kan enkel Europol toegang krijgen tot de relevante gegevens[818].

De opslag van gegevens is enkel toegestaan voor een periode die noodzakelijk en evenredig is en de voortzetting ervan is onderworpen aan een evaluatie om de drie jaar zonder welke de gegevens automatisch worden gewist[819].

Europol kan onder bepaalde voorwaarden persoonsgegevens rechtstreeks doorgeven aan een EU-orgaan of aan een autoriteit van een derde land of aan een internationale organisatie[820]. Indien inbreuken op gegevens waarschijnlijk de rechten en vrijheden van de betrokkenen ernstig en ongunstig beïnvloeden, moeten zij zonder nodeloze vertraging aan hen worden gecommuniceerd[821]. Op het niveau van de lidstaten wordt een nationale toezichthoudende autoriteit aangesteld om toe te zien op de verwerking van persoonsgegevens van Europol[822].

De EDPS is verantwoordelijk voor het toezien op en het verzekeren van de bescherming van de grondrechten en fundamentele vrijheden van natuurlijke personen bij de verwerking van persoonsgegevens door Europol, alsmede voor het verstrekken van advies aan Europol en aan de betrokkenen over alles wat de verwerking van persoonsgegevens betreft. Daartoe treedt de EDPS op als een onderzoekend

816 Europol-verordening, artikel 30, lid 1.

817 *Ibid.*, artikel 30, lid 2.

818 *Ibid.*, artikel 30, lid 3.

819 *Ibid.*, artikel 31.

820 *Ibid.*, respectievelijk artikel 24 en artikel 25.

821 *Ibid.*, artikel 35.

822 Europol-verordening, artikel 42.

en buitengerechtelijk orgaan en handelt in nauwe samenwerking met de nationale toezichthoudende autoriteiten[823]. EDPS en de nationale toezichthoudende autoriteiten komen ten minste twee keer per jaar bijeen in de Samenwerkingscommissie, die een adviserende functie heeft[824]. Lidstaten zijn verplicht een toezichthoudende autoriteit bij wet in te stellen die bevoegd is om toe te zien op de rechtmatigheid van de doorgifte van persoonsgegevens van het nationale niveau naar Europol en op het ophalen van en alle communicatie met Europol over persoonsgegevens door de lidstaat[825]. Lidstaten worden ook verplicht toe te zien dat de nationale toezichthoudende autoriteit volledig onafhankelijk kan optreden bij het uitvoeren van haar taken en verplichtingen uit hoofde van de Europol-verordening[826]. Om de rechtmatigheid van de gegevensverwerking na te gaan, zelf toe te zien op zijn activiteiten en de integriteit en beveiliging van gegevens te waarborgen, houdt Europol logboeken of documenten van zijn gegevensverwerkingsactiviteiten bij. Deze logboeken bevatten informatie over verwerkingen in geautomatiseerde verwerkingssystemen met betrekking tot de verzameling, wijziging, raadpleging, bekendmaking, samenstelling en wissing ervan[827].

Een beroep tegen een beslissing van de EDPS kan worden ingesteld bij het HvJ-EU[828]. Elke persoon die schade heeft ondervonden als gevolg van een onrechtmatige gegevensverwerking, heeft recht op schadevergoeding voor de geleden schade, hetzij van Europol dan wel van de verantwoordelijke lidstaat, door een vordering in te stellen bij het HvJ-EU in het eerste geval of bij de bevoegde nationale rechterlijke instantie in het tweede geval[829]. Bovendien kan een gespecialiseerde Gezamenlijke Parlementaire Controlegroep (GPC) van de nationale parlementen en het Europees Parlement de activiteiten van Europol onderzoeken[830]. Eenieder heeft recht op toegang tot de persoonsgegevens die Europol mogelijk over hem of haar heeft opgeslagen, naast het recht om te verzoeken dat deze gegevens worden gecontroleerd, gecorrigeerd of verwijderd. Deze rechten kunnen onderhevig zijn aan uitzonderingen en beperkingen.

823 *Ibid.*, artikelen 43 en 44.
824 *Ibid.*, artikel 45.
825 *Ibid.*, artikel 42, lid 1.
826 *Ibid.*, artikel 42, lid 1.
827 *Ibid.*, artikel 40.
828 *Ibid.*, artikel 48.
829 *Ibid.*, artikel 50.
830 *Ibid.*, artikel 51.

Eurojust

Eurojust, opgericht in 2002, is een in Den Haag gevestigd EU-orgaan. Ze bevordert justitiële samenwerking in onderzoeken en vervolgingen in verband met ernstige criminaliteit waarbij ten minste twee lidstaten betrokken zijn[831]. Eurojust is bevoegd om:

- de coördinatie van onderzoeken en vervolgingen tussen de bevoegde autoriteiten van de verschillende lidstaten te bevorderen en te verbeteren;

- de uitvoering van verzoeken en besluiten in verband met justitiële samenwerking te vergemakkelijken.

De functies van Eurojust worden uitgevoerd door de nationale leden. Elke lidstaat vaardigt één rechter of openbare aanklager af bij Eurojust, die is onderworpen aan het nationale recht en over de nodige bevoegdheden beschikt om de taken uit te voeren die noodzakelijk zijn om de justitiële samenwerking te bevorderen en te verbeteren. Daarnaast treden de nationale leden gezamenlijk op, als een college, bij de uitvoering van bijzondere taken van Eurojust.

Eurojust kan persoonsgegevens verwerken voor zover dat noodzakelijk is om zijn doelstellingen te verwezenlijken. Dit is echter beperkt tot specifieke informatie over personen die verdacht worden van het plegen van of deelnemen aan het plegen van, of die veroordeeld zijn voor, een strafbaar feit dat onder de bevoegdheid van Eurojust valt. Eurojust kan ook bepaalde informatie verwerken met betrekking tot getuigen of slachtoffers van strafbare feiten die onder de bevoegdheid van Eurojust vallen[832]. In uitzonderlijke omstandigheden kan Eurojust echter ook, gedurende een beperkte periode, andere persoonsgegevens betreffende de omstandigheden van een strafbaar feit verwerken wanneer die van onmiddellijk belang zijn voor en deel uitmaken van lopende onderzoeken. Binnen zijn bevoegdheidsgebied kan Eurojust

831 De Raad van de Europese Unie (2002), Besluit 2002/187/JBZ van de Raad van 28 februari 2002 betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken, PB L 63 van 2002; Raad van de Europese Unie (2003), Besluit 2003/659/JBZ van de Raad van 18 juni 2003 tot wijziging van Beschikking 2002/187/JBZ betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken, PB L 44 van 2003; Raad van de Europese Unie (2009), Besluit 2009/426/JBZ van de Raad van 16 december 2008 inzake het versterken van Eurojust en tot wijziging van Beschikking 2002/187/JBZ betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken, PB L 138 van 2009 (Eurojust-besluiten).

832 Geconsolideerde versie van Besluit 2002/187/JBZ van de Raad als gewijzigd bij Besluit 2003/659/JBZ van de Raad en bij Besluit 2009/426/JBZ van de Raad, artikel 15, lid 2.

samenwerken en persoonsgegevens uitwisselen met andere EU-instellingen, -organen en -agentschappen. Ook kan Eurojust samenwerken en persoonsgegevens uitwisselen met derde landen en organisaties.

Wat betreft gegevensbescherming moet Eurojust een beschermingsniveau waarborgen dat ten minste gelijk is aan de beginselen van Gemoderniseerd Verdrag 108 en de latere wijzigingen daarvan. In geval van gegevensuitwisseling moeten specifieke regels en beperkingen in acht worden genomen die zijn neergelegd in samenwerkingsovereenkomsten of werkregelingen in overeenstemming met de Eurojust-besluiten van de Raad en de gegevensbeschermingsvoorschriften van Eurojust[833].

Binnen Eurojust is een onafhankelijk Gemeenschappelijk Controleorgaan (GCO) ingesteld, dat als taak heeft om toezicht te houden op de verwerking van persoonsgegevens door Eurojust. Betrokkenen kunnen bij het GCO in beroep gaan als ze niet tevreden zijn met het besluit van Eurojust op een verzoek om toegang tot of correctie, afscherming of uitwissing van persoonsgegevens. Wanneer Eurojust onrechtmatig persoonsgegevens verwerkt, is Eurojust aansprakelijk overeenkomstig het nationale recht van de lidstaat waar zijn hoofdkantoor is gevestigd, Nederland, voor schade die aan de betrokkene is toegebracht.

Vooruitzichten

De Europese Commissie diende een voorstel in voor een verordening tot hervorming van Eurojust in juli 2013. Dit voorstel ging vergezeld van een voorstel tot oprichting van een Europees Openbaar Ministerie (zie hieronder). Deze verordening heeft tot doel de taken en structuur te stroomlijnen om in overeenstemming te zijn met het Verdrag van Lissabon. Daarnaast is het doel van de hervorming om een duidelijke scheiding vast te stellen tussen de operationele taken van Eurojust, uitgevoerd door het college van Eurojust, en de administratieve taken. Dit zal de lidstaten ook in staat stellen om zich te concentreren op de operationele taken. Een nieuwe Uitvoerende Raad zal worden ingesteld om het college bij te staan bij de uitvoering van de administratieve taken[834].

833 Intern reglement betreffende de verwerking en bescherming van persoonsgegevens bij Eurojust, PB C 68 van 19.3.2005, blz. 1.

834 Zie de webpagina van de Europese Commissie over Eurojust.

Europees Openbaar Ministerie

De lidstaten hebben exclusieve bevoegdheid voor de vervolging van strafbare feiten, fraude en misbruik van de toepassing van de EU-begroting, die eveneens grensoverschrijdende gevolgen kunnen hebben. Het belang van het onderzoeken, vervolgen en voor het gerecht brengen van de daders van dergelijke strafbare feiten is toegenomen, vooral gezien de huidige economische crisis[835]. De Europese Commissie heeft een verordening voorgesteld betreffende de oprichting van een onafhankelijk Europees Openbaar Ministerie (EOM)[836] dat als doel heeft het bestrijden van strafbare feiten die de financiële belangen van de EU schaden. Het EOM zal worden opgericht door middel van de procedure voor nauwere samenwerking, waardoor een minimum van negen lidstaten een nauwere samenwerking in een domein binnen de EU-structuren kan instellen, zonder dat andere EU-landen hierbij betrokken zijn[837]. België, Bulgarije, Kroatië, Cyprus, Tsjechië, Estland, Finland, Frankrijk, Duitsland, Griekenland, Letland, Litouwen, Luxemburg, Portugal, Roemenië, Slovenië, Slowakije en Spanje zijn lid van de nauwere samenwerking; Oostenrijk en Italië hebben de intentie uitgesproken om toe te treden[838].

Het EOM zal bevoegd zijn voor het onderzoeken en vervolgen van EU-fraude en andere strafbare feiten die de financiële belangen van de EU schaden, met als doel het doeltreffend coördineren van onderzoeken en vervolgingen tussen de verschillende nationale rechtsstelsels en de verbetering van het gebruik van middelen en de uitwisseling van informatie op Europees niveau[839].

Het EOM zal onder leiding staan van een Europese openbare aanklager met ten minste één afgevaardigde Europese aanklager in elke lidstaat die belast is met het uitvoeren van de onderzoeken en vervolgingen in die lidstaat.

---

835 Zie Europese Commissie (2013), Voorstel voor een verordening van de Raad tot instelling van het Europees Openbaar Ministerie, COM(2013) 534 def., Brussel, 17 juli 2013, blz. 1 en de website over het EOM van de Commissie.

836 Europese Commissie (2013), Voorstel voor een verordening van de Raad tot instelling van het Europees Openbaar Ministerie, COM(2013) 534 def., Brussel, 17 juli 2013.

837 Verdrag betreffende de werking van de Europese Unie, artikel 86, lid 1, en artikel 329, lid 1.

838 Zie Raad van de Europese Unie (2017), "*20 lidstaten het eens over details voor instelling van Europees Openbaar Ministerie (EOM)*", persbericht van 8 juni 2017.

839 Europese Commissie (2013), Voorstel voor een verordening van de Raad tot instelling van het Europees Openbaar Ministerie, COM(2013) 534 def., Brussel, 17 juli 2013, blz. 1 en blz. 51-51. Zie ook de website over het EOM van de Commissie.

Het voorstel bevat sterke garanties ter waarborging van de rechten van de personen die betrokken zijn bij de onderzoeken van het EOM, zoals bepaald in het nationale recht, het Unierecht en het EU-Handvest van de grondrechten. Onderzoeksmaatregelen die voornamelijk betrekking hebben op de grondrechten vereisen voorafgaande toestemming van een nationale rechterlijke instantie[840]. De onderzoeken van het EOM worden onderworpen aan rechterlijke toetsing door de nationale rechterlijke instanties[841].

De verordening gegevensbescherming EU-instellingen[842] is van toepassing op de verwerking van administratieve persoonsgegevens die het EOM uitvoert. Voor de verwerking van persoonsgegevens met betrekking tot operationele aangelegenheden, zoals Europol, zal het EOM beschikken over een eigen stelsel voor gegevensbescherming dat vergelijkbaar is met het stelsel van toepassing op de activiteiten van Europol en Eurojust, gezien het feit dat de uitoefening van de functies van het EOM de verwerking van persoonsgegevens met de wetshandhavings- en vervolgingsautoriteiten op lidstaatniveau omvat. De EOM-voorschriften inzake gegevensbescherming zijn dus nagenoeg identiek aan de voorschriften van de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke instanties. Volgens het voorstel voor de oprichting van het EOM moet de verwerking van persoonsgegevens in overeenstemming zijn met de beginselen van rechtmatigheid en eerlijkheid, doelbinding, gegevensminimalisering, juistheid en vertrouwelijkheid. Het EOM moet, voor zover mogelijk, een duidelijk onderscheid maken tussen de persoonsgegevens van verschillende soorten betrokkenen, zoals personen die veroordeeld zijn voor een strafbaar feit, personen die louter verdacht zijn, slachtoffers en getuigen. Het moet ook de kwaliteit van de verwerkte persoonsgegeven nagaan en, voor zover mogelijk, een onderscheid maken tussen persoonsgegevens die gebaseerd zijn op feiten en persoonsgegevens die gebaseerd zijn op een persoonlijk oordeel.

Het voorstel bevat bepalingen inzake de rechten van betrokkenen, met name het recht op informatie, toegang tot hun persoonsgegevens, rectificatie, wissing en beperking van de verwerking, en bepaalt dat dergelijke rechten ook indirect kunnen worden uitgeoefend via de EDPS. Het belichaamt de beginselen van beveiliging van de verwerking en verantwoordingsplicht, op grond waarvan het EMO passende

840 Europese Commissie (2013), Voorstel voor een verordening van de Raad tot instelling van het Europees Openbaar Ministerie, COM(2013) 534 def., Brussel, 17 juli 2013, artikel 26, lid 4.

841 *Ibid.*, artikel 36.

842 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, PB L 8 van 2001.

technische en organisatorische maatregelen moet invoeren om te zorgen voor een passend niveau van beveiliging tegen de risico's van de verwerking, om alle verwerkingsactiviteiten bij te houden en voorafgaand aan de verwerking een gegevensbeschermingseffectbeoordeling uit te voeren wanneer een bepaalde verwerking (bijvoorbeeld verwerkingen met gebruik van nieuwe technologieën) waarschijnlijk een hoog risico inhoudt voor de rechten van natuurlijke personen. Ten slotte voorziet het voorstel in de aanwijzing van een functionaris voor gegevensbescherming door het college, die naar behoren moet worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens en ervoor moet zorgen dat het EOM de toepasselijke wetgeving inzake gegevensbescherming naleeft.

8.3.2. De bescherming van gegevens in gemeenschappelijke informatiesystemen op EU-niveau

Naast de gegevensuitwisseling tussen lidstaten en de oprichting van gespecialiseerde EU-autoriteiten voor de bestrijding van grensoverschrijdende criminaliteit, zoals Europol, Eurojust en het EOM, zijn op EU-niveau diverse gemeenschappelijke informatiesystemen opgezet die de samenwerking en de uitwisseling van gegevens tussen de bevoegde nationale en EU-autoriteiten voor gespecificeerde doeleinden op het gebied van grensbeveiliging, immigratie, asiel en douane mogelijk moeten maken en vergemakkelijken. Aangezien het Schengengebied aanvankelijk in het leven werd geroepen door een internationale overeenkomst die onafhankelijk van het Unierecht functioneerde, kwam het Schengeninformatiesysteem (SIS) voort uit multilaterale overeenkomsten en werd het vervolgens onderworpen aan het Unierecht. Het Visuminformatiesysteem (VIS), Eurodac, Eurosur en het douane-informatiesysteem (CIS) zijn opgericht als instrumenten die beheerst worden door het Unierecht.

Het toezicht op deze systemen wordt verdeeld tussen de nationale toezichthoudende autoriteiten en de EDPS. Om te zorgen voor een hoog niveau van bescherming, werken deze autoriteiten samen binnen de Coördinatiegroep voor toezicht (SCG) die verwijst naar de volgende grootschalige IT-systemen: 1) Eurodac; 2) Visuminformatiesysteem; 3) Schengeninformatiesysteem; 4) douaneinformatiesysteem, en 5) Informatiesysteem interne markt[843]. De SCG's komen gewoonlijk tweemaal per jaar bijeen, onder de autoriteit van een gekozen voorzitter, en legt richtsnoeren

843 Zie de website over de Coördinatie van het toezicht van de Europese Toezichthouder voor gegevensbescherming.

vast, bespreekt grensoverschrijdende gevallen of stelt gemeenschappelijke kaders voor inspecties vast.

Het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA)[844], dat in 2012 is opgericht, is belast met het beheer van het Schengeninformatiesysteem van de tweede generatie (SIS II), het Visuminformatiesysteem (VIS) en Eurodac. De kerntaak van eu-LISA is om te zorgen voor de effectieve, veilige en continue werking van grootschalige IT-systemen. Ook is het agentschap verantwoordelijk voor het nemen van de noodzakelijke maatregelen om de beveiliging van de systemen en van de gegevens te waarborgen.

Het Schengeninformatiesysteem

In 1985 hebben verschillende lidstaten van de voormalige Europese Gemeenschap (de staten van de Benelux Economische Unie, Duitsland en Frankrijk) een overeenkomst gesloten betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen (Schengenovereenkomst), die als doel had een ruimte te creëren voor het vrije verkeer van personen, ongehinderd door grenscontroles, binnen het Schengengebied[845]. Als tegengewicht voor de bedreigingen voor de openbare veiligheid die kunnen ontstaan als gevolg van open grenzen, werden versterkte grenscontroles aan de buitengrenzen ingevoerd, evenals een nauwe samenwerking tussen de nationale politiële en strafrechtelijke autoriteiten.

Als gevolg van de toetreding van nieuwe staten tot de Schengenovereenkomst is het Schengensysteem uiteindelijk in het Verdrag van Amsterdam geïntegreerd in het wettelijk kader van de EU[846]. De uitvoering van dit besluit gebeurde in 1999. De nieuwste versie van het Schengeninformatiesysteem, het zogeheten SIS II, trad in werking op 9 april 2013. Het systeem wordt nu gebruikt door de meeste

844 Verordening (EU) nr. 1077/2011 van het Europees Parlement en de Raad van 25 oktober 2011 tot oprichting van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht, PB L 286 van 2011.

845 Overeenkomst tussen de regeringen van de staten van de Benelux Economische Unie, de Bondsrepubliek Duitsland en de Franse Republiek betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen, PB L 239 van 2000.

846 Europese Gemeenschappen (1997), Verdrag van Amsterdam houdende wijziging van het Verdrag betreffende de Europese Unie, de Verdragen tot oprichting van de Europese Gemeenschappen en sommige bijbehorende akten, PB C 340 van 1997.

EU-lidstaten[847] plus IJsland, Liechtenstein, Noorwegen en Zwitserland[848]. Ook Europol en Eurojust hebben toegang tot het SIS II.

Het SIS II bestaat uit een centraal systeem (C.SIS), een nationaal systeem (N.SIS) in elke lidstaat en een communicatie-infrastructuur tussen het centrale systeem en de nationale systemen. Het C.SIS bevat bepaalde door de lidstaten ingevoerde gegevens over personen en voorwerpen. Het SIS wordt gebruikt door nationale grenscontrole-, politiële, douane-, visum- en gerechtelijke autoriteiten in de hele Schengenruimte. Elke lidstaat beheert een nationale kopie van het C.SIS, die gezamenlijk bekend staan als de nationale Schengeninformatiesystemen (N.SIS) en voortdurend worden bijgewerkt, waarmee ook het C.SIS wordt bijgewerkt. Er bestaan verschillende soorten signaleringen in SIS:

- de persoon heeft geen recht om de Schengenruimte binnen te komen of erin te verblijven, of
- de persoon of het voorwerp wordt gezocht door rechterlijke of rechtshandhavingsautoriteiten (bv. de Europese aanhoudingsbevelen, verzoeken om onopvallende controles), of
- de persoon is als vermist opgegeven, of
- goederen, zoals bankbiljetten, auto's, bestelwagens, vuurwapens en identiteitsdocumenten, zijn opgegeven als gestolen of verloren.

Wanneer er een signalering is, wordt een follow-up geïnitieerd via de Sirene-bureaus. SIS II heeft nieuwe functies, zoals de mogelijkheid om toegang te hebben tot: biometrische gegevens, zoals vingerafdrukken en foto's, of nieuwe categorieën signaleringen, zoals gestolen vaartuigen, luchtvaartuigen, containers of de wijze van betaling; verbeterde signaleringen van personen en voorwerpen, en kopieën van de

847 Kroatië, Cyprus en Ierland voeren de voorbereidende werkzaamheden tot integratie in SIS II uit, maar maken er nog geen deel van uit. Zie de informatie over het Schengeninformatiesysteem die beschikbaar is op de website van het directoraat-generaal Migratie en Binnenlandse Zaken van de Europese Commissie.

848 Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II), PB L 381 van 2006, en Raad van de Europese Unie (2007), Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II), PB L 205 van 2007.

Europese aanhoudingsbevelen voor personen die gezocht worden met het oog op hun aanhouding, overlevering of uitlevering.

SIS II is gebaseerd op twee instrumenten die elkaar aanvullen: het SIS II-besluit[849] en de SIS II-verordening[850]. De EU-wetgever gebruikte een andere rechtsgrond voor de vaststelling van het besluit en de verordening. Het besluit regelt het gebruik van SIS II voor doeleinden in het kader van de politiële en justitiële samenwerking in strafzaken (de voormalige derde pijler van de Europese Unie). De verordening is van toepassing op procedures die vallen onder het visum-, asiel-, immigratie- en ander beleid dat verband houdt met het vrije verkeer van personen (voorheen de eerste pijler). De signaleringsprocedures voor elke pijler moesten worden geregeld door aparte instrumenten, aangezien de twee rechtshandelingen werden vastgesteld vóór het Verdrag van Lissabon en de afschaffing van de pijlerstructuur.

Beide rechtshandelingen bevatten regels inzake gegevensbescherming. Het SIS II-besluit verbiedt de verwerking van gevoelige gegevens[851]. De verwerking van persoonsgegevens valt onder het toepassingsgebied van Gemoderniseerd Verdrag 108[852]. Voorts hebben natuurlijke personen het recht op toegang tot hen betreffende persoonsgegevens die in SIS II werden ingevoerd[853].

De SIS II-verordening regelt de voorwaarden en procedures voor het invoeren en verwerken van signaleringen met betrekking tot weigeringen van toegang of verblijf van niet-EU-burgers. Het bepaalt ook regels voor de uitwisseling van aanvullende en bijkomende informatie voor de doeleinden van toegang of verblijf in een lidstaat[854]. Deze verordening bevat ook regels inzake gegevensbescherming. Gevoelige gegevenscategorieën, als bedoeld in artikel 9, lid 1, van de algemene verordening gegevensbescherming, mogen niet worden verwerkt[855]. De SIS II-verordening bevat ook bepaalde rechten ten behoeve van de betrokkene, te weten:

849 Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II), PB L 205, 7 augustus 2007.

850 Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II), PB L 381 van 28 december 2006.

851 SIS II-besluit, artikel 56; SIS II-verordening, artikel 40.

852 SIS II-besluit, artikel 57.

853 SIS II-besluit, artikel 58; SIS II-verordening, artikel 41.

854 SIS II-verordening, artikel 2.

855 *Ibid.*, artikel 40.

- het recht op toegang tot persoonsgegevens die verband houden met de betrokkene[856];

- het recht om feitelijk onjuiste gegevens te corrigeren[857];

- het recht om onrechtmatig bewaarde gegevens te wissen[858], en

- het recht om te worden geïnformeerd indien er sprake is van een signalering tegen de betrokkene. De informatie wordt schriftelijk verstrekt en gaat vergezeld van een kopie van of een verwijzing naar het nationale besluit om de signalering uit te vaardigen[859].

Het recht op informatie wordt niet verstrekt indien 1) de persoonsgegevens niet werden verkregen van de betrokkene en het onmogelijk is of een onevenredig grote inspanning vergt om die informatie te verstrekken, 2) de betrokkene reeds beschikt over de informatie of 3) de nationale wetgeving in een beperking voorziet op basis van, onder andere, het waarborgen van de nationale veiligheid of de voorkoming van strafbare feiten[860].

Voor zowel het SIS II-besluit als de SIS II-verordening kunnen de toegangsrechten van natuurlijke personen in het kader van SIS II worden uitgeoefend in elke lidstaat, en worden deze behandeld in overeenstemming met de nationale wetgeving van die lidstaat[861].

Voorbeeld: In *Dalea/Frankrijk*[862] had de verzoeker geen visum voor Frankrijk gekregen, omdat de Franse autoriteiten aan het Schengeninformatiesysteem hadden gemeld dat hem de toegang tot het land moest worden geweigerd. De verzoeker had zonder succes bij de Franse Commissie gegevensbescherming, en uiteindelijk bij de Franse Raad van State, verzocht om toegang tot en rectificatie of uitwissing van de gegevens. Het EHRM oordeelde dat de aanmelding van de verzoeker bij het Schengeninformatiesysteem in

856 *Ibid.*, artikel 41, lid 1.

857 *Ibid.*, artikel 41, lid 5.

858 *Ibid.*, artikel 41, lid 5.

859 *Ibid.*, artikel 42, lid 1.

860 *Ibid.*, artikel 42, lid 2.

861 SIS II-verordening, artikel 41, lid 1, en het SIS II-besluit, artikel 58.

862 EHRM, *Dalea/Frankrijk*, nr. 964/07, 2 februari 2010.

overeenstemming met de wet was geweest en het rechtmatige doel had gediend om de nationale veiligheid te beschermen. Aangezien de verzoeker niet had aangetoond hoe hij feitelijk was benadeeld door de weigering van toegang tot de Schengenruimte, was de inmenging in het recht op eerbiediging van het privéleven evenredig geweest. De klacht van de verzoeker op grond van artikel 8 werd daarom niet-ontvankelijk verklaard.

De bevoegde nationale toezichthoudende autoriteit in elke lidstaat houdt toezicht op het eigen N.SIS. De nationale toezichthoudende autoriteit moet ervoor zorgen dat ten minste elke vier jaar een audit van de gegevensverwerkingen binnen het eigen N.SIS wordt verricht[863]. De nationale toezichthoudende autoriteiten en de EDPS werken samen en zorgen voor een gecoördineerd toezicht op het N.SIS, terwijl de EDPS verantwoordelijk is voor het toezicht op het C.SIS. Met het oog op de transparantie wordt om de twee jaar een gezamenlijk activiteitenverslag toegezonden aan het Europees Parlement, de Raad en eu-LISA. De Coördinatiegroep voor toezicht (SCG) van het SIS II is opgezet om de coördinatie van het toezicht van het SIS te waarborgen en komt maximaal twee keer per jaar samen. Deze groep is samengesteld uit de EDPS en vertegenwoordigers van de toezichthoudende autoriteiten van de lidstaten die SIS II hebben uitgevoerd, alsmede IJsland, Liechtenstein, Noorwegen en Zwitserland, aangezien het SIS ook op hen van toepassing is en zij lid zijn van Schengen[864]. Cyprus, Kroatië en Ierland maken nog geen deel uit van SIS II en nemen daarom slechts als waarnemer deel aan de SCG. In het kader van de SCG werken de EDPS en de nationale toezichthoudende autoriteiten actief samen door informatie uit te wisselen, elkaar bij te staan in de uitvoering van audits en inspecties, geharmoniseerde voorstellen voor gemeenschappelijke oplossingen voor potentiële problemen te ontwerpen en het bewustzijn van gegevensbeschermingsrechten te bevorderen[865]. De SIS II-SCG stelt ook richtsnoeren vast om betrokkenen bij te staan. Een voorbeeld hiervan is de gids om betrokkenen bij te staan in de uitvoering van hun toegangsrechten[866].

863 SIS II-verordening, artikel 60, lid 2.

864 Zie de wegsite over het Schengeninformatiesysteem van de Europese Toezichthouder voor gegevensbescherming.

865 SIS II-verordening, artikel 46 en SIS II-besluit, artikel 62.

866 Zie SIS II SCG, *Het Schengeninformatiesysteem. Een leidraad voor de uitoefening van het recht op toegang*, beschikbaar op de website van de EDPS.

Vooruitzichten

In 2016 voerde de Europese Commissie een evaluatie van het SIS[867] uit waaruit bleek dat nationale mechanismen waren ingevoerd die betrokkenen in staat stelden om toegang te krijgen tot hun persoonsgegevens in SIS, deze te verbeteren en te wissen of om schadevergoeding te verkrijgen voor onjuiste gegevens. Ter verbetering van de efficiëntie en doeltreffendheid van het SIS II, heeft de Europese Commissie drie voorstellen voor verordeningen ingediend:

- een verordening betreffende de oprichting, werking en het gebruik van het SIS op het gebied van grenscontroles, die de intrekking van de SIS II-verordening tot gevolg zal hebben;

- een verordening betreffende de oprichting, werking en het gebruik van SIS op het gebied van politiële en justitiële samenwerking in strafzaken, die de intrekking van met name het SIS II-besluit tot gevolg zal hebben, en

- een verordening inzake het gebruik van het SIS voor de terugkeer van illegaal verblijvende onderdanen van derde landen.

Belangrijker nog, de voorstellen maken de verwerking van andere categorieën biometrische gegevens mogelijk — naast foto's en vingerafdrukken, die reeds deel uitmaken van het huidige SIS II-stelsel. Vingerafdrukken, palmafdrukken en DNA-profielen zullen ook in de SIS-gegevensbank worden opgeslagen. Hoewel de SIS II-verordening en het SIS II-besluit voorzien in de mogelijkheid om te zoeken met vingerafdrukken om een persoon te identificeren, maken de voorstellen deze doorzoeking bovendien verplicht indien de identiteit van de persoon niet op een andere wijze kan worden vastgesteld. Gezichtsbeelden, foto's en palmafdrukken zullen worden gebruikt om het systeem te doorzoeken en mensen te identificeren, wanneer dit technisch mogelijk wordt. De nieuwe regels inzake het gebruik van biometrische kenmerken houden bijzondere risico's in voor de rechten van natuurlijke personen. In zijn advies over de voorstellen van de Commissie[868] merkt de EDPS op dat biometrische gegevens zeer gevoelig zijn en dat hun invoering in een dergelijke

867 Europese Commissie (2016), Verslag van de Commissie aan het Europees Parlement en de Raad over de evaluatie van het Schengeninformatiesysteem van de tweede generatie (SIS II) overeenkomstig artikel 24, lid 5, artikel 43, lid 3, en artikel 50, lid 5, van Verordening (EG) nr. 1987/2006, en artikel 59, lid 3, en artikel 66, lid 5, van Besluit 2007/533/JBZ, COM(2016) 880 def., Brussel, 21 december 2016.

868 EDPS (2017), Advies van de EDPS over de nieuwe rechtsgrond van het Schengeninformatiesysteem, Advies 7/2017, 2 mei 2017.

grootschalige gegevensbank gebaseerd moet zijn op een op wetenschappelijk bewijs gebaseerde beoordeling van de noodzaak om ze in het SIS op te nemen. Met andere woorden, de noodzaak van de verwerking van nieuwe eigenschappen moet worden aangetoond. De EDPS is ook van mening dat het noodzakelijk is om verder te verduidelijken welke soort informatie kan worden opgenomen in het DNA-profiel. Aangezien de DNA-profielen ook gevoelige informatie kunnen bevatten (het meest opvallende voorbeeld zou informatie zijn die gezondheidskwesties onthult), moeten de DNA-profielen die zijn opgeslagen in het SIS, het volgende bevatten: "Enkel de minimale informatie die strikt noodzakelijk is voor de identificatie van de vermiste personen en expliciet informatie over gezondheid, raciale afkomst en andere gevoelige informatie uitsluit"[869]. De voorstellen stellen echter aanvullende waarborgen vast om de verzameling en verdere verwerking van gegevens te beperken tot dat wat strikt noodzakelijk en operationeel vereist is, en toegang is beperkt tot personen die een operationele noodzaak hebben om de persoonsgegevens te verwerken[870]. De voorstellen machtigen eu-LISA ook op gezette tijden verslagen op te stellen over de kwaliteit van de gegevens, ter controle van signaleringen om de kwaliteit van gegevens te waarborgen[871].

Het Visuminformatiesysteem

Het Visuminformatiesysteem (VIS), dat eveneens wordt beheerd door eu-LISA, is ontwikkeld om de uitvoering van een gemeenschappelijk EU-visumbeleid te ondersteunen[872]. Het VIS laat Schengenstaten toe om gegevens over visumaanvragers uit te wisselen via een volledig gecentraliseerd systeem dat de buiten de EU gelegen consulaten en ambassades van de Schengenstaten verbindt met de externe grensdoorlaatposten van alle Schengenstaten. Het VIS verwerkt gegevens

869 *Ibid.*, punt 22.

870 Europese Commissie (2016), Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële samenwerking en justitiële samenwerking in strafzaken, tot wijziging van Verordening (EU) nr. 515/2014 en tot intrekking van Verordening (EG) nr. 1986/2006, Besluit 2007/533/JBZ van de Raad, en Besluit 2010/261/EU van de Commissie, COM(2016) 883 def., Brussel, 21 december 2016.

871 *Ibid.*, blz.15.

872 De Raad van de Europese Unie (2004), Besluit 2004/512/EG van de Raad van 8 juni 2004 tot vaststelling van het Visuminformatiesysteem (VIS), PB L 213 van 2004; Verordening (EG) nr. 767/2008 van het Europees Parlement en de Raad van 9 juli 2008 betreffende het Visuminformatiesysteem (VIS) en de uitwisseling van gegevens tussen de lidstaten inzake visa voor kort verblijf, PB L 218 van 2008 (VIS-verordening); Raad van de Europese Unie (2008), Besluit 2008/633/JBZ van de Raad van 23 juni 2008 betreffende de toegang voor raadpleging van het Visuminformatiesysteem (VIS) door de aangewezen autoriteiten van de lidstaten en door Europol, met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten, PB L 218 van 2008.

over aanvragen voor visa voor kort verblijf met het oog op verblijf in of doorreis door de Schengenruimte. Het VIS biedt grensautoriteiten de mogelijkheid om met behulp van biometrische gegevens, met name vingerafdrukken, te controleren of de persoon die een visum toont al dan niet de rechtmatige houder is en om personen zonder of met frauduleuze documenten te identificeren.

Verordening (EG) nr. 767/2008 van het Europees Parlement en de Raad betreffende het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf (VIS-verordening) regelt de voorwaarden en procedures voor de doorgifte van persoonsgegevens met betrekking tot toepassingen voor visa voor kort verblijf. De verordening ziet ook toe op de besluiten die worden genomen over aanvragen, met inbegrip van besluiten tot nietigverklaring, intrekking of verlenging van het visum[873]. De VIS-verordening heeft voornamelijk betrekking op gegevens over de aanvrager, zijn/haar visa, foto's, vingerafdrukken, links naar eerdere aanvragen en de aanvraagdossiers van personen die hem/haar vergezellen of gegevens over de uitnodigende personen[874]. De toegang tot het VIS om gegevens in te voeren, te wijzigen of uit te wissen is beperkt tot uitsluitend de visumautoriteiten, terwijl de toegang tot de raadpleging van gegevens is voorbehouden aan de visumautoriteiten en de autoriteiten die bevoegd zijn voor controles aan de externe grensdoorlaatposten, immigratiecontroles en asielzaken.

Onder bepaalde omstandigheden kunnen nationale bevoegde politieautoriteiten en Europol toegang verzoeken tot in het VIS ingevoerde gegevens met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten[875]. Aangezien het VIS bedoeld is als een instrument om de uitvoering van het gemeenschappelijk visumbeleid te ondersteunen, zou het beginsel van doelbinding (dat, zoals uitgelegd in hoofdstuk 3.2, vereist dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verwerkt en toereikend, ter zake dienend en niet overmatig moeten zijn met betrekking tot de doelstelling waarvoor de gegevens worden verwerkt) worden geschonden indien het VIS in een rechtshandhavingsinstrument zou veranderen. Om die reden krijgen de nationale wetshandhavingsinstanties en Europol niet

873 VIS-verordening, artikel 1.

874 Artikel 5 van Verordening (EG) nr. 767/2008 van het Europees Parlement en de Raad van 9 juli 2008 betreffende het opzetten van het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf (VIS-verordening), PB L 218 van 2008.

875 Raad van de Europese Unie (2008), Besluit 2008/633/JBZ van de Raad van 23 juni 2008 over de toegang tot het Visuminformatiesysteem (VIS) voor raadpleging door aangewezen autoriteiten van de lidstaten en door Europol, met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten, PB L 218 van 2008.

routinematige toegang tot de VIS-gegevensbank. De toegang kan slechts per geval worden verleend en moet vergezeld gaan van strikte waarborgen. De voorwaarden en waarborgen voor toegang tot en raadpleging van het VIS door deze autoriteiten werden geregeld in Besluit 2008/633/JBZ van de Raad[876].

Bovendien voorziet de VIS-verordening in rechten van de betrokkenen. Dit zijn:

- Het recht op informatie door de verantwoordelijke lidstaat over de identiteit en contactgegevens van de verwerkingsverantwoordelijke die belast is met de verwerking van persoonsgegevens in de betrokken lidstaat, de doeleinden waarvoor de persoonsgegevens zullen worden verwerkt in het VIS, de categorieën personen aan wie de gegevens mogen worden doorgegeven (ontvangers) en de bewaringstermijn. Bovendien moeten visumaanvragers geïnformeerd worden over het feit dat de verzameling van hun persoonsgegevens in het kader van het VIS verplicht is voor het onderzoek van hun aanvraag, terwijl lidstaten hen ook moeten informeren over het bestaan van hun recht op toegang tot hun gegevens, op de rectificatie of wissing ervan en over de procedures die hen in staat stellen om deze rechten uit te oefenen[877].

- Het recht op toegang tot de met hen betreffende persoonsgegevens die in het VIS werden opgeslagen[878].

- Het recht op de rechtzetting van onjuiste gegevens[879].

- Het recht op wissing van onrechtmatig bewaarde gegevens[880].

Om te zorgen voor toezicht op het VIS, werd de VIS-SCG opgericht. Deze is samengesteld uit vertegenwoordigers van de EDPS en de nationale toezichthoudende autoriteiten, die twee keer per jaar bijeen komen. Deze groep bestaat uit vertegenwoordigers van de 28 EU-lidstaten en uit IJsland, Liechtenstein, Noorwegen en Zwitserland.

876 *Ibid.*

877 VIS-verordening, artikel 37.

878 *Ibid.*, artikel 38, lid 1.

879 *Ibid.*, artikel 38, lid 2.

880 *Ibid.*, artikel 38, lid 2.

Eurodac

Eurodac staat voor Europese Dactyloscopie[881]. Eurodac is een centraal systeem waarin de vingerafdrukken van onderdanen van derde landen en staatloze personen die in een van de EU-lidstaten asiel aanvragen, worden opgeslagen[882]. Het systeem is sinds januari 2003 operationeel, met de goedkeuring van Verordening (EG) nr. 2725/2000 van de Raad; een herziening werd van toepassing in 2015. Het doel ervan is in de eerste plaats te helpen bepalen welke lidstaat verantwoordelijk is voor de behandeling van een asielaanvraag in het kader van verordening (EG) nr. 604/2013. Die verordening stelt de criteria en instrumenten vast om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend (Dublin III-verordening)[883]. Persoonsgegevens in Eurodac dienen hoofdzakelijk om de toepassing van de Dublin III-verordening te vergemakkelijken[884].

Nationale rechtshandhavingsinstanties en Europol mogen vingerafdrukken die verband houden met strafrechtelijke onderzoeken vergelijken met de vingerafdrukken in Eurodac, doch uitsluitend met het oog op het voorkomen, opsporen of onderzoeken van terroristische of andere ernstige strafbare feiten. Aangezien Eurodac is ontworpen als een instrument ter ondersteuning van de uitvoering van het asielbeleid

881 Zie de website over Eurodac van de Europese Toezichthouder voor gegevensbescherming.

882 Verordening (EG) nr. 2725/2000 van de Raad van 11 december 2000 betreffende de oprichting van Eurodac voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van de overeenkomst van Dublin, PB L 316 van 2000; Verordening (EG) nr. 407/2002 van de Raad van 28 februari 2002 tot vaststelling van uitvoeringsbepalingen voor Verordening (EG) nr. 2725/2000 betreffende de oprichting van Eurodac voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van de overeenkomst van Dublin, PB L 62 van 2002 (Eurodac-verordeningen), Verordening (EU) nr. 603/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van Verordening (EU) nr. 604/2013 tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend en betreffende verzoeken van rechtshandhavingsinstanties van de lidstaten en Europol om vergelijkingen van Eurodac-gegevens ten behoeve van rechtshandhaving, en tot wijziging van Verordening (EU) nr. 1077/2011 tot instelling van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht, PB L 180 van 2013, blz. 1 (herschikte Eurodac-verordening).

883 Verordening (EU) nr. 604/2013 van het Europees Parlement en de Raad van 26 juni 2013 tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend, PB L 180 van 2013, (Dublin III-verordening).

884 Herschikte Eurodac-verordening, PB L 180 van 2013, blz. 1, artikel 1, lid 1.

van de EU en niet als rechtshandhavingsinstrument, krijgen rechtshandhavingsinstanties uitsluitend voor specifieke gevallen, onder specifieke omstandigheden en onder strikte voorwaarden toegang tot de databank[885]. Voor het verdere gebruik van de gegevens voor rechtshandhavingsdoeleinden is de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten van toepassing, terwijl de gegevens die voornamelijk worden gebruikt om de uitvoering van de Dublin III-verordening te vergemakkelijken, worden beschermd in het kader van de algemene verordening gegevensbescherming. Verdere doorgifte van persoonsgegevens die worden verkregen door een lidstaat of Europol op grond van de herschikte Eurodac-verordening, aan een derde land, internationale organisatie of particuliere instantie die binnen of buiten de EU is gelegen, is verboden[886].

Eurodac bestaat uit een centrale eenheid voor het opslaan en vergelijken van vingerafdrukken, die wordt beheerd door eu-LISA, en een systeem voor elektronische doorzending van gegevens tussen de lidstaten en de centrale databank. De lidstaten nemen vingerafdrukken af en zenden deze door van iedere persoon van 14 jaar of ouder die asiel aanvraagt op hun grondgebied, en van elke onderdaan van een niet-EU-lidstaat of staatloze persoon van 14 jaar of ouder die is aangehouden wegens het illegaal overschrijden van hun buitengrens. Ook kunnen de lidstaten vingerafdrukken afnemen en doorzenden van onderdanen van niet-EU-lidstaten of staatloze personen die zonder verblijfsvergunning op hun grondgebied verblijven.

Hoewel alle lidstaten Eurodac kunnen raadplegen en vergelijkingen van vingerafdrukgegevens kunnen aanvragen, heeft enkel de lidstaat die de vingerafdrukken heeft verzameld en doorgegeven naar de centrale eenheid het recht om de gegevens te wijzigen, door ze te corrigeren, aan te vullen of te wissen[887]. eu-LISA houdt registers bij van alle gegevensverwerkingen om de gegevensbescherming te controleren en gegevensbeveiliging te waarborgen[888]. De nationale toezichthoudende autoriteiten staan betrokkenen bij en adviseren hun inzake de uitoefening van hun rechten[889]. De verzameling en doorgifte van vingerafdrukgegevens is onderworpen aan rechterlijke toetsing door de nationale rechterlijke instanties[890]. De

885 *Ibid.*, artikel 1, lid 2.
886 *Ibid.*, artikel 35.
887 *Ibid.*, artikel 27.
888 *Ibid.*, artikel 28.
889 *Ibid.*, artikel 29.
890 *Ibid.*, artikel 29.

verordening gegevensbescherming EU-instellingen[891] en toezicht door de EDPS zijn van toepassing op de verwerkingsactiviteiten van het centrale systeem, dat wordt beheerd door eu-LISA met betrekking tot Eurodac[892]. Indien een persoon schade lijdt als gevolg van een onrechtmatige verwerking of een handeling die in strijd is met de Eurodac-verordening, dan heeft deze persoon recht op een schadevergoeding van de lidstaat die verantwoordelijk is voor de schade[893]. Er moet worden benadrukt dat asielzoekers deel uitmaken van een bijzonder kwetsbare groep die vaak een lange en riskante reis hebben ondernomen. Vanwege hun kwetsbaarheid en de precaire situatie waarin ze zich vaak bevinden tijdens het onderzoek van hun asielaanvraag, kan de uitoefening van hun rechten, met inbegrip van het recht op vergoeding, in de praktijk moeilijk blijken.

Om Eurodac te gebruiken voor rechtshandhavingsdoeleinden moeten lidstaten de autoriteiten aanwijzen die het recht zullen hebben om toegang te vragen, evenals de autoriteiten die zullen controleren dat de verzoeken om vergelijking rechtmatig zijn[894]. De toegang van nationale autoriteiten en van Europol tot de vingerafdrukgegevens van Eurodac is onderworpen aan zeer strenge voorwaarden. De verzoekende autoriteit dient pas een gemotiveerd elektronisch verzoek in te dienen na de gegevens te hebben vergeleken met die in andere beschikbare informatiesystemen, zoals nationale vingerafdrukgegevensbanken en het VIS. Er moet een doorslaggevend openbaarveiligheidsbelang zijn dat deze vergelijking evenredig maakt. De vergelijking moet werkelijk noodzakelijk zijn, betrekking hebben op een specifieke zaak en er moeten redelijke gronden zijn om te veronderstellen dat de vergelijking wezenlijk zal bijdragen tot de voorkoming, opsporing of het onderzoek van een van de betrokken strafbare feiten, met name wanneer er een gegrond vermoeden bestaat dat de verdachte, dader of het slachtoffer van een terroristische misdaad of een ander ernstig strafbaar feit in een categorie valt die is onderworpen aan de verzameling vingerafdrukken in het Eurodac-systeem. De vergelijking mag uitsluitend worden gemaakt met vingerafdrukgegevens. Europol moet ook een vergunning verkrijgen van de lidstaat die de vingerafdrukgegevens verzamelt.

891 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, PB L 8 van 2001.

892 Herschikte Eurodac-verordening, PB L 180 van 2013, blz. 1, artikel 31.

893 *Ibid.*, artikel 37.

894 Roots, L. (2015), "The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination", *Baltic Journal of European Studies Tallinn University of Technology*, Vol. 5, nr. 2, blz. 108-129.

In Eurodac opgeslagen persoonsgegevens die verband houden met asielaanvragen worden gedurende tien jaar bewaard vanaf de datum waarop de vingerafdrukken zijn afgenomen, tenzij de betrokkene het burgerschap van een EU-lidstaat verwerft. In dat geval moeten de gegevens onmiddellijk worden gewist. Gegevens over onderdanen van derde landen die illegaal de buitengrens zijn overschreden, worden gedurende 18 maanden opgeslagen. Deze gegevens moeten onmiddellijk worden gewist als de betrokkene een verblijfsvergunning verkrijgt, het grondgebied van de EU verlaat of het burgerschap van een EU-lidstaat verwerft. De gegevens van de personen die asiel verkregen, blijven gedurende drie jaar beschikbaar voor de vergelijking in het kader van het voorkomen, opsporen en onderzoeken van terroristische en andere ernstige strafbare feiten.

Behalve alle EU-lidstaten passen ook IJsland, Noorwegen, Liechtenstein en Zwitserland Eurodac toe op basis van internationale overeenkomsten.

De Eurodac SCG is ingesteld om te zorgen voor toezicht op Eurodac. Deze is samengesteld uit vertegenwoordigers van de EDPS en de nationale toezichthoudende autoriteiten, die twee keer per jaar bijeen komen. Deze groep bestaat uit vertegenwoordigers van de 28 EU-lidstaten en uit IJsland, Liechtenstein, Noorwegen en Zwitserland[895].

Vooruitzichten

In mei 2016 heeft de Commissie een voorstel voor een nieuwe herschikte Eurodac-verordening uitgevaardigd als onderdeel van een hervorming die gericht is op de verbetering van de werking van het gemeenschappelijk Europees asielstelsel (CEAS)[896]. De voorgestelde herschikking is belangrijk, aangezien het toepassingsgebied van de oorspronkelijke Eurodac-databank hierdoor aanzienlijk zal worden uitgebreid. Eurodac was oorspronkelijk opgericht ter ondersteuning van de uitvoering van het CEAS, door te voorzien in vingerafdrukbewijzen die hielpen vast te stellen welke

895 Zie de website over Eurodac van de Europese Toezichthouder voor gegevensbescherming.

896 Europese Commissie, Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van [Verordening (EU) nr. 604/2013 tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend], voor de identificatie van een illegaal verblijvende onderdaan van een derde land of staatloze en betreffende verzoeken van rechtshandhavingsinstanties van de lidstaten en Europol om vergelijkingen van Eurodac-gegevens ten behoeve van rechtshandhaving (herschikking), COM(2016) def., 4 mei 2016.

lidstaat verantwoordelijk was voor het onderzoek van een in de EU ingediend asielverzoek. De voorgestelde herschikking breidt het toepassingsgebied van de databank uit om de terugkeer van illegale migranten te vergemakkelijken[897]. De nationale autoriteiten zullen in staat zijn de databank te raadplegen om te bepalen welke onderdanen van derde landen illegaal in de EU verblijven of wie de EU op een onregelmatige wijze is binnengekomen teneinde bewijsmateriaal te verkrijgen om lidstaten bij te staan bij de terugkeer van deze personen. Terwijl de huidige wettelijke regeling enkel de verzameling en bewaring van vingerafdrukken vereist, bestaat het voorstel uit de verzameling van de gezichtsopnames van natuurlijke personen[898], wat een ander soort biometrisch gegeven is. Het voorstel zou ook de minimumleeftijd van kinderen waarvan de biometrische gegevens kunnen worden genomen, verlagen naar zes jaar[899] in plaats van 14 jaar, wat de minimumleeftijd is onder de verordening van 2013. Het uitgebreide toepassingsgebied van het voorstel houdt in dat het een inmenging vormt in de rechten op privacy en de gegevensbescherming voor meer personen die mogelijk in het gegevensbestand worden opgenomen. Om deze inmenging te compenseren, trachten het voorstel en de door de Commissie LIBE van de Europese Unie voorgestelde amendementen[900] de voorschriften inzake gegevensbescherming te versterken. Ten tijde van het opstellen van het handboek, waren de besprekingen over het voorstel bij het Parlement en de Raad gaande.

897 Zie de toelichting bij het voorstel, blz. 3.

898 Europese Commissie, Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van [Verordening (EU) nr. 604/2013 tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend], voor de identificatie van een illegaal verblijvende onderdaan van een derde land of staatloze en betreffende verzoeken van rechtshandhavingsinstanties van de lidstaten en Europol om vergelijkingen van Eurodac-gegevens ten behoeve van rechtshandhaving (herschikking), COM(2016) def., 4 mei 2016, artikel 2, lid 1.

899 *Ibid.*, artikel 2, lid 2.

900 Europees Parlement, *verslag over het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van [Verordening (EU) nr. 604/2013 tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend], voor de identificatie van een illegaal verblijvende onderdaan van een derde land of staatloze en betreffende verzoeken van rechtshandhavingsinstanties van de lidstaten en Europol om vergelijkingen van Eurodac-gegevens ten behoeve van rechtshandhaving (herschikking),* PE 597.620v03-00, 9 juni 2017.

Eurosur

Het Europees grensbewakingssysteem (Eurosur)[901] is ontworpen om de controle van de buitengrenzen van de Schengenruimte te versterken door de opsporing, voorkoming en bestrijding van illegale immigratie en grensoverschrijdende criminaliteit. Eurosur is opgezet om de informatie-uitwisseling en operationele samenwerking tussen nationale coördinatiecentra en Frontex, het EU-agentschap dat is belast met de ontwikkeling en toepassing van het nieuwe concept van geïntegreerd grensbeheer, te verbeteren[902]. De algemene doelstellingen zijn de volgende:

- het verminderen van het aantal illegale immigranten dat onopgemerkt de EU binnenkomt;
- het verminderen van het aantal sterfgevallen onder illegale migranten door meer levens op zee te redden;
- het verbeteren van de interne veiligheid van de EU als geheel door bij te dragen tot de preventie van grensoverschrijdende criminaliteit[903].

Eurosur startte zijn werkzaamheden op 2 december 2013 in alle lidstaten met buitengrenzen, en op 1 december 2014 in alle andere lidstaten. De verordening is van toepassing op controles aan de land-, zee- en luchtbuitengrenzen van de EU. Eurosur wisselt persoonsgegevens uit en verwerkt ze in zeer beperkte mate, aangezien lidstaten en Frontex uitsluitend scheepsidentificatienummers mogen uitwisselen. Eurosur wisselt operationele informatie uit, zoals de locatie van patrouilles en incidenten, en als algemene regel kan de uitgewisselde informatie geen

901 Verordening (EG) nr. 1052/2013 van het Europees Parlement en de Raad van 22 oktober 2013 tot instelling van het Europees grensbewakingssysteem (Eurosur), PB L 295 2013.

902 Verordening (EU) nr. 2916/1624 van het Europees Parlement en de Raad van 14 september 2016 betreffende de Europese grens- en kustwacht, tot wijziging van Verordening (EU) 2016/399 van het Europees Parlement en de Raad en tot intrekking van Verordening (EG) nr. 863/2007 van het Europees Parlement en de Raad, Verordening (EG) nr. 2007/2004 van de Raad en Besluit 2005/267/EG van de Raad, PB L 251.

903 Zie ook: Europese Commissie (2008), Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's — Onderzoek naar de mogelijkheden tot instelling van een Europees grensbewakingssysteem (Eurosur), COM(2008) 68 def., Brussel, 13 februari 2008; Europese Commissie (2011), *Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur)*, werkdocument van de diensten van de Commissie, SEC(2011) 1536 def., Brussel, 12 december 2011, blz. 18.

persoonsgegevens bevatten[904]. In de uitzonderlijke gevallen waarin persoonsgegevens worden uitgewisseld in het kader van Eurosur, voorziet de verordening erin dat het algemene juridische kader van de EU inzake gegevensbescherming volledig van toepassing is[905].

Eurosur zorgt dus voor het recht op gegevensbescherming, met name door te stellen dat uitwisselingen van persoonsgegevens moeten voldoen aan de criteria en waarborgen die zijn ingesteld door de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten en de AVG[906].

Douane-informatiesysteem

Een ander belangrijk informatiesysteem dat op EU-niveau is opgezet, is het Douane-informatiesysteem (DIS)[907]. In de loop van de totstandbrenging van de interne markt werden alle controles en formaliteiten met betrekking tot goederen die op het EU-grondgebied circuleerden, afgeschaft, wat leidde tot een verhoogd risico op fraude. Dit risico is tegengegaan door een versterkte samenwerking tussen de douanediensten van de lidstaten. Het doel van het DIS is om de lidstaten bij te staan bij het voorkomen, onderzoeken en vervolgen van ernstige inbreuken op douane- en landbouwwetgeving van de lidstaten en van de EU. Het DIS is opgericht door twee rechtshandelingen die werden vastgesteld op basis van uiteenlopende rechtsgrondslagen: Verordening (EG) nr. 515/97 van de Raad heeft betrekking op de samenwerking tussen de verschillende nationale overheidsdiensten voor de bestrijding van fraude in het kader van de douane-unie en het gemeenschappelijk landbouwbeleid, terwijl Besluit 2009/917/JBZ van de Raad tot doel heeft bijstand te verlenen in het voorkomen, onderzoeken en vervolgen van ernstige overtredingen van de douanewetgeving. Dit betekent dat DIS niet alleen betrekking heeft op de rechtshandhaving.

904 Europese Commissie, *EUROSUR: Protecting the Schengen external borders — protecting migrant's lives. EUROSUR in a nutshell*, 29 november 2013.

905 Verordening (EU) nr. 1052/2013, overweging 13 en artikel 13.

906 *Ibid.*, overweging 13 en artikel 13.

907 Raad van de Europese Unie (1995), Akte van de Raad van 26 juli 1995 tot vaststelling van het Verdrag inzake het gebruik van informatica op douanegebied, PB C 316 van 1995, gewijzigd door de Raad van de Europese Unie (2009), Verordening (EG) nr. 515/97 van 13 maart 1997 betreffende de wederzijdse bijstand tussen de administratieve autoriteiten van de lidstaten en de samenwerking tussen deze autoriteiten en de Commissie met het oog op de juiste toepassing van de douane- en landbouwvoorschriften, Besluit 2009/917/JBZ van de Raad van 30 november 2009 inzake het gebruik van informatica op douanegebied, PB L 323 van 2009 (CIS-besluit).

De informatie in het DIS omvat persoonsgegevens met betrekking tot goederen, vervoersmiddelen, bedrijven, personen en ingehouden, in beslag genomen of geconfisqueerde goederen en contanten. De categorieën gegevens die kunnen worden verwerkt, zijn duidelijk gedefinieerd en bevatten de namen, nationaliteit, het geslacht, de geboorteplaats en -datum van de betrokken personen, de reden voor de opneming van hun gegevens in het systeem en het registratienummer van het vervoermiddel[908]. Deze informatie mag uitsluitend worden gebruikt voor de melding van waarnemingen of voor het verrichten van gerichte controles en strategische of operationele analyses met betrekking tot personen die worden verdacht van het overtreden van de douanevoorschriften.

Toegang tot het DIS wordt alleen verleend aan de nationale douane-, belasting-, landbouw-, volksgezondheids- en politiële autoriteiten, evenals aan Europol en Eurojust.

De verwerking van persoonsgegevens moet voldoen aan de specifieke voorschriften van Verordening (EG) nr. 515/97 en Besluit 2009/917/JBZ van de Raad, evenals aan de bepalingen van de algemene verordening gegevensbescherming, de verordening gegevensbescherming EU-instellingen, Gemoderniseerd Verdrag 108 en de Politieaanbeveling. De EDPS is verantwoordelijk voor het toezicht op de naleving van Verordening (EG) nr. 45/2001 door DIS. Minstens eenmaal per jaar wordt er een vergadering belegd met alle nationale toezichthoudende autoriteiten die bevoegd zijn inzake toezichtkwesties met betrekking tot DIS.

Interoperabiliteit tussen de EU-informatiesystemen

Migratiebeheer, geïntegreerd grensbeheer van de buitengrenzen van de EU en de bestrijding van terrorisme en grensoverschrijdende criminaliteit vormen belangrijke uitdagingen die steeds complexer worden in een geglobaliseerde wereld. In de afgelopen jaren heeft de Europese Unie gewerkt aan een nieuwe allesomvattende aanpak om veiligheid te waarborgen en in stand te houden zonder de waarden en fundamentele vrijheden van de EU in het gedrang te brengen. Bij deze inspanningen zijn doeltreffende informatieuitwisselingen tussen nationale rechtshandhavingsinstanties en tussen lidstaten en de relevante EU-agentschappen van cruciaal

908 Zie CIS-besluit, artikelen 24, 25 en 28.

belang[909]. De bestaande EU-informatiesystemen voor grensbeheer en interne veiligheid hebben hun respectieve doelstellingen, institutionele structuur, betrokkenen en gebruikers. De EU heeft gewerkt aan het verhelpen van tekortkomingen in de functionaliteiten van een gefragmenteerd EU-gegevensbeheer tussen de verschillende informatiesystemen zoals SIS II, VIS en Eurodac door de mogelijkheden voor interoperabiliteit te verkennen[910]. Het belangrijkste doel is ervoor te zorgen dat de bevoegde politiële, douane- en gerechtelijke autoriteiten systematisch over de nodige informatie beschikken om hun taken uit te voeren, met behoud van een evenwicht met betrekking tot de rechten op privacy, gegevensbescherming en andere grondrechten.

Interoperabiliteit is "het vermogen van informatiesystemen om onderling gegevens uit te wisselen en het delen van informatie mogelijk te maken"[911]. Deze uitwisseling mag geen afbreuk doen aan de onvermijdelijk strenge voorschriften voor toegang en gebruik die worden gewaarborgd door de AVG, de richtlijn gegevensbescherming voor politiële en strafrechtelijke autoriteiten, het Handvest van de grondrechten van de EU en alle andere relevante regelgevingen. Elke geïntegreerde oplossing voor het beheer van gegevens mag geen afbreuk doen aan de beginselen van doelbinding, gegevensbescherming door ontwerp of gegevensbescherming door standaardinstellingen[912].

---

909 Europese Commissie (2016), Mededeling van de Commissie aan het Europees Parlement en de Raad — Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid, COM(2016) 205 def., Brussel, 6 april 2016, Europese Commissie (2016), Communicatie van de Commissie aan het Europees Parlement, de Europese Raad en de Raad: Versterking van de veiligheid in een door mobiliteit gekenmerkte wereld door betere informatie-uitwisseling in de strijd tegen terrorisme en door sterkere buitengrenzen, COM(2016) 602 def., Brussel, 14 september 2016, Europese Commissie (2016), Voorstel voor een verordening van het Europees Parlement en de Raad inzake het gebruik van het Schengeninformatiesysteem voor de terugkeer van illegaal verblijvende onderdanen van derde landen. Zie ook Mededeling van de Commissie aan het Europees Parlement, de Europese Raad en de Raad — Zevende verslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie, COM(2017) 261 def., Brussel, 16 mei 2017.

910 Raad van de Europese Unie (2005), Het Haagse programma: Versterking van vrijheid, veiligheid en recht in de Europese Unie, PB C 53 van 2005, Europese Commissie (2010), Mededeling van de Commissie aan het Europees Parlement en de Raad — Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht, COM(2010) 385 def., Europese Commissie (2016), Mededeling van de Commissie aan het Europees Parlement en de Raad — Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid, COM(2016) 205 def., Brussel, 6 april 2016, Europese Commissie (2016), Besluit van de Commissie van 17 juni 2016 tot oprichting van de deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit, PB C 257 van 2016.

911 Europese Commissie (2016), Mededeling van de Commissie aan het Europees Parlement en de Raad — Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid, COM(2016) 205 def., Brussel, 6 april 2016, blz. 14.

912 *Ibid.*, blz. 4-5.

In aanvulling op de verbetering van de functionaliteiten van de drie belangrijkste informatiesystemen — SIS II, VIS en Eurodac — heeft de Commissie voorgesteld om een vierde gecentraliseerd grensbeheersysteem op te richten dat zich richt op de onderdanen van derde landen: het inreis-uitreissysteem (EES)[913] dat naar verwachting tegen 2020 ten uitvoer zal worden gebracht[914]. De Commissie heeft ook een voorstel ingediend voor de oprichting van een Europees Systeem voor reisinformatie en -autorisatie (ETIAS)[915], een systeem dat informatie zal verzamelen over personen die zonder visumplicht naar de EU reizen om illegale migratie en veiligheidscontroles vooraf mogelijk te maken.

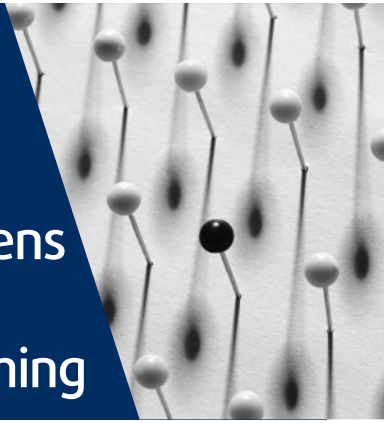
913 Europese Commissie (2016), Voorstel voor een verordening van het Europees Parlement en de Raad tot instelling van een inreis-uitreissysteem (EES) voor de registratie van inreis- en uitreisgegevens en van gegevens over weigering van toegang ten aanzien van onderdanen van derde landen die de buitengrenzen van de Europese Unie overschrijden en tot vaststelling van de voorwaarden voor toegang tot het EES voor rechtshandhavingsdoeleinden en tot wijziging van Verordening (EG) nr. 767/2008 en Verordening (EU) nr. 1077/2011, COM(2016) 194 def., Brussel, 6 april 2016.

914 Europese Commissie (2016), Mededeling van de Commissie aan het Europees Parlement en de Raad — Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid, COM(2016) 205 def., Brussel, 6 april 2016, blz. 5.

915 Europese Commissie (2016), Voorstel voor een verordening van het Europees Parlement en de Raad tot instelling van een Europees systeem voor reisinformatie en -autorisatie (ETIAS) en tot wijziging van de verordeningen (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/794 en (EU) 2016/1624, COM(2016) 731 def., 16 november 2016.

9

Specifieke soorten gegevens en desbetreffende regels inzake gegevensbescherming



EU	Behandelde onderwerpen	RvE
Algemene verordening gegevensbescherming Richtlijn betreffende privacy en elektronische communicatie	**Elektronische communicatie**	Gemoderniseerd Verdrag 108 Aanbeveling inzake telecommunicatie-diensten
Algemene verordening gegevensbescherming, artikel 88	**Arbeids-verhoudingen**	Gemoderniseerd Verdrag 108 Aanbeveling inzake arbeidsgegevens EHRM, *Copland tegen het Verenigd Koninkrijk*, nr. 62617/00, 2007
Algemene verordening gegevensbescherming, artikel 9, lid 2, onder h) en i)	**Medische gegevens**	Gemoderniseerd Verdrag 108 Aanbeveling inzake medische gegevens EHRM, *Z./Finland*, nr. 22009/93, 1997
Verordening inzake klinische proeven	**Klinische proeven**	
Algemene verordening gegevensbescherming, artikel 6, lid 4, artikel 89	**Statistieken**	Gemoderniseerd Verdrag 108 Aanbeveling inzake statistische gegevens
Verordening (EG) nr. 223/2009 betreffende de Europese statistiek HvJ-EU, zaak C-524/06, *Huber/Bundesrepublik Deutschland* [Grote kamer], 2008	**Officiële statistieken**	Gemoderniseerd Verdrag 108 Aanbeveling inzake statistische gegevens

EU	Behandelde onderwerpen	RvE
Richtlijn 2014/65/EG betreffende markten voor financiële instrumenten Verordening (EU) nr. 648/2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters Verordening (EG) nr. 1060/2009 inzake ratingbureaus Richtlijn 2007/64/EG betreffende betalingsdiensten in de interne markt	**Financiële gegevens**	Gemoderniseerd Verdrag 108 Aanbeveling 90(19) inzake de bescherming van persoonsgegevens die worden gebruikt voor betalingen en andere, aanverwante verrichtingen EHRM, *Michaud/Frankrijk*, nr. 12323/11, 2012

Op Europees niveau zijn diverse bijzondere rechtsinstrumenten vastgesteld om de algemene beginselen van Gemoderniseerd Verdrag 108 en de algemene verordening gegevensbescherming meer in detail toe te passen op specifieke situaties.

9.1. Elektronische communicatie

Belangrijkste punten

- Specifieke voorschriften voor de gegevensbescherming op het gebied van telecommunicatie, en in het bijzonder telefoniediensten, zijn opgenomen in de aanbeveling van de RvE van 1995.
- De verwerking van persoonsgegevens in verband met de verrichting van telecommunicatiediensten op EU-niveau wordt gereguleerd in de richtlijn betreffende privacy en elektronische communicatie.
- De vertrouwelijkheid van elektronische communicaties geldt niet alleen voor de inhoud van een communicatie, maar ook voor metagegevens, zoals informatie over wie met wie heeft gecommuniceerd, en wanneer en hoe lang, met inbegrip van locatiegegevens, zoals waar de gegevens zijn gecommuniceerd.

Communicatienetwerken hebben een verhoogd potentieel voor ongerechtvaardigde inmenging in de persoonlijke levenssfeer van de gebruikers, aangezien ze krachtige technische mogelijkheden bieden om de communicatie die in deze netwerken plaatsvindt af te luisteren en te bewaken. Dientengevolge werden bijzondere gegevensbeschermingsregels noodzakelijk geacht om de specifieke risico's voor gebruikers van communicatiediensten aan te pakken.

In 1995 heeft de **RvE** een aanbeveling uitgebracht inzake gegevensbescherming op het gebied van telecommunicatie, met bijzondere nadruk op telefoondiensten[916]. Volgens deze aanbeveling moeten de doeleinden van het verzamelen en verwerken van persoonsgegevens in het kader van telecommunicatie worden beperkt tot het verbinden van een gebruiker met het netwerk, het beschikbaar stellen van de specifieke telecommunicatiedienst, facturering, controle, zorgen voor een optimale technische exploitatie en het ontwikkelen van het netwerk en de dienst.

Ook wordt bijzondere aandacht geschonken aan het gebruik van communicatienetwerken voor het verzenden van boodschappen in het kader van direct marketing. Als algemene regel mogen directmarketingberichten niet worden gericht aan abonnees die uitdrukkelijk te kennen hebben gegeven dat ze deze niet wensen te ontvangen. Geautomatiseerde apparaten voor het verzenden van vooraf opgenomen reclameboodschappen mogen alleen worden gebruikt als een abonnee daar uitdrukkelijk toestemming voor heeft gegeven. In het nationale recht moeten gedetailleerde voorschriften op dit gebied worden vastgesteld.

In het **wettelijk kader van de EU** is in 2002, na een eerste poging in 1997, de richtlijn betreffende privacy en elektronische communicatie vastgesteld (die in 2009 is gewijzigd) om de bepalingen van de vorige richtlijn gegevensbescherming voor de telecommunicatiesector aan te vullen en te specificeren[917].

De toepassing van de richtlijn betreffende privacy en elektronische communicatie is beperkt tot communicatiediensten op openbare elektronische netwerken.

In de richtlijn betreffende privacy en elektronische communicatie wordt onderscheid gemaakt tussen drie hoofdcategorieën gegevens die tijdens een communicatie worden gegenereerd:

916 Raad van Europa, Comité van Ministers (1995), Aanbeveling Rec(95)4 aan de lidstaten inzake de bescherming van persoonsgegevens op het gebied van telecommunicatiediensten, met bijzondere nadruk op telefoondiensten, 7 februari 1995.

917 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, PB L 201 van 2002 (richtlijn betreffende privacy en elektronische communicatie), als gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, PB L 337 van 2009.

- de gegevens die de inhoud vormen van de in de communicatie verzonden berichten — deze gegevens zijn strikt vertrouwelijk;

- de gegevens die nodig zijn voor het opstellen en bijhouden van de communicatie — zogenaamde metagegevens, aangeduid als "verkeersgegevens" in de richtlijn — zoals informatie over de communicerende partijen, het tijdstip en de duur van de communicatie;

- in de metagegevens zijn er gegevens die specifiek betrekking hebben op de locatie van het communicatie-instrument, de zogenaamde locatiegegevens — deze gegevens zijn tegelijkertijd gegevens over de locatie van de gebruikers van de communicatie-instrumenten, met name wanneer het gaat over gebruikers van mobiele communicatie-instrumenten.

Verkeersgegevens kunnen door de dienstverrichter alleen worden gebruikt voor facturering en om de dienst technisch te kunnen aanbieden. Indien de betrokkene daar toestemming voor geeft, kunnen deze gegevens echter ook worden verstrekt aan andere verwerkingsverantwoordelijken die diensten met toegevoegde waarde aanbieden, zoals informatie over de locatie van het dichtstbijzijnde metrostation of de dichtstbijzijnde apotheek, of weersvoorspellingen voor deze locatie.

Volgens artikel 15 van de e-Privacy-richtlijn moet andere toegang tot gegevens over communicatie in elektronische netwerken voldoen aan de eisen van gerechtvaardigde inmenging in het recht op gegevensbescherming als neergelegd in artikel 8, lid 2, van het EVRM en bevestigd door het EU-Handvest van de grondrechten in de artikelen 8 en 52. Dergelijke toegang kan toegang omvatten met het oog op het onderzoeken van misdrijven.

Met de wijzigingen van 2009 van de richtlijn betreffende privacy en elektronische communicatie[918] werd het volgende ingevoerd:

- De beperkingen op het verzenden van e-mails voor directmarketingdoeleinden zijn uitgebreid tot sms-diensten, multimediaberichtdiensten en andere,

918 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, PB L 337 van 2009.

vergelijkbare typen toepassingen; marketing-e-mails zijn verboden, tenzij voorafgaande toestemming werd verkregen. Zonder deze toestemming mogen alleen eerdere klanten worden benaderd met e-mails met het oog op direct marketing, indien deze hun e-mailadres ter beschikking hebben gesteld en geen bezwaar maken.

- Aan de lidstaten is een verplichting opgelegd om ervoor te zorgen dat betrokkenen rechtsvorderingen kunnen instellen in verband met inbreuken op het verbod op verzending van ongevraagde boodschappen[919].

- Het installeren van cookies, software die het gebruik van een computer door een gebruiker monitort en registreert, is niet langer toegestaan zonder toestemming van de gebruiker van de computer. Het nationale recht moet meer gedetailleerd regelen hoe de toestemming moet worden uitgedrukt en verkregen om voor voldoende bescherming te zorgen[920].

Wanneer een inbreuk op gegevensbeschermingswetgeving plaatsvindt als gevolg van onbevoegde toegang tot of verlies of vernietiging van gegevens, moet de toezichthoudende autoriteit onmiddellijk worden geïnformeerd. De abonnees moeten indien mogelijk worden geïnformeerd wanneer een dergelijke inbreuk mogelijk tot schade voor hen leidt[921].

De richtlijn gegevensbewaring[922] vereist dat verleners van communicatiediensten metagegevens bewaren. Deze richtlijn is echter nietig verklaard door het HvJ-EU (voor meer details, zie punt 8.3).

Vooruitzichten

In Januari 2017 stelde de Europese Commissie een nieuw voorstel vast voor een e-Privacy-verordening ter vervanging van de oude e-Privacy-richtlijn. Het doel blijft

919 Zie de gewijzigde richtlijn, artikel 13.

920 Zie *Ibid.*, artikel 5; zie ook Groep artikel 29 (2012), *Advies 04/2012 over ontheffing van de toestemmingsverplichting voor cookies*, WP 194, Brussel, 7 juni 2012.

921 Zie ook Groep artikel 29 (2011), *Werkdocument 01/2011 betreffende het momenteel in de EU van kracht zijnde juridisch kader met betrekking tot schendingen van persoonsgegevens en aanbevelingen voor in de toekomst te ondernemen acties*, WP 184, Brussel, 5 april 2011.

922 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (richtlijn gegevensbewaring), PB L 105 van 2006.

de bescherming van "grondrechten en fundamentele vrijheden van natuurlijke personen en rechtspersonen in het aanbieden en gebruik van elektronische communicatiediensten en, met name, het recht op de eerbiediging van het privéleven en de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens". Hiernaast is het doel te zorgen voor het vrije verkeer van elektronische communicatiegegevens en elektronische communicatiediensten in de Unie[923]. Hoewel de AVG primair betrekking heeft op artikel 8 van het EU-Handvest van de grondrechten, beoogt de voorgestelde verordening artikel 7 van het Handvest in het afgeleide recht van de EU te verwerken.

De verordening zou de bepalingen van de voorgaande verordening aanpassen aan de nieuwe technologieën en de reële marktsituatie, en zou een alomvattend en coherent kader creëren met de algemene verordening gegevensbescherming (AVG). In deze zin zou de e-Privacy-verordening *lex specialis* zijn met betrekking tot de AVG, op maat gemaakt voor elektronische communicatiegegevens die de persoonsgegevens vormen. De nieuwe verordening heeft betrekking op de verwerking van "elektronische communicatiegegevens", met inbegrip van inhoud en metagegevens van elektronische communicatie die niet noodzakelijkerwijs persoonsgegevens zijn. Het territoriaal toepassingsgebied is beperkt tot de EU, met inbegrip van gegevens die zijn verkregen in de EU en buiten de EU worden verwerkt, en strekt zich uit tot over-the-top-communicatiedienstverleners. Dit zijn dienstverleners die inhoud, diensten of applicaties via internet leveren zonder directe betrokkenheid van een netwerkexploitant of een internetaanbieder (isp). Voorbeelden van dergelijke dienstverleners omvatten Skype (spraak- en video-oproepen), WhatsApp (berichten), Google (zoekopdrachten), Spotify (muziek) of Netflix (video). De handhavingsmechanismen van de AVG zouden op de nieuwe verordening van toepassing zijn.

De e-Privacy-verordening zal worden aangenomen vóór 25 mei 2018, waarna de AVG in alle 28 lidstaten van toepassing zal zijn. Dit is echter afhankelijk van de instemming van zowel het Europees Parlement als de Raad[924].

923 Voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie), COM(2017) 10 def., artikel 1.

924 Voor meer informatie, zie Europese Commissie (2017), "Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions", persbericht, 10 januari 2017.

9.2. Arbeidsgegevens

Belangrijkste punten

- Specifieke regels voor gegevensbescherming in arbeidsverhoudingen zijn vervat in de Aanbeveling inzake arbeidsgegevens van de RvE.
- In de AVG worden arbeidsverhoudingen alleen specifiek genoemd in het kader van de verwerking van gevoelige gegevens.
- De geldigheid van toestemming, die vrijelijk moet zijn gegeven, als een rechtsgrondslag voor de verwerking van gegevens over werknemers, kan twijfelachtig zijn, gezien de economische ongelijkheid tussen werkgever en werknemer. De omstandigheden rond de verlening van toestemming moeten zorgvuldig worden beoordeeld.

De gegevensverwerking in het kader van de werkgelegenheid is onderworpen aan de algemene EU-wetgeving inzake de bescherming van persoonsgegevens. Eén verordening[925] is evenwel specifiek gericht op de bescherming van de verwerking van persoonsgegevens door de Europese instellingen in het kader van (onder meer) de werkgelegenheid. In de AVG worden arbeidsverhoudingen specifiek vermeld in artikel 9, lid 2, waarin is vastgelegd dat persoonsgegevens mogen worden verwerkt bij de uitvoering van verplichtingen of bij de uitoefening van de specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van werkgelegenheid.

In het kader van de AVG moet de werknemer in staat worden gesteld om duidelijk onderscheid te maken tussen de gegevens waarmee hij/zij vrijwillig instemt met de verwerking/opslag en de doeleinden waarvoor zijn/haar gegevens worden opgeslagen. Werknemers dienen ook te worden geïnformeerd over hun rechten en hoe lang de gegevens worden opgeslagen, voordat toestemming kan worden gegeven. Indien een inbreuk op persoonsgegevens hoogstwaarschijnlijk een groot risico zal vormen voor de rechten en vrijheden van natuurlijke personen, dient de werkgever deze inbreuk aan de werknemer mee te delen. Artikel 88 van de verordening stelt lidstaten in staat om meer specifieke regels vast te stellen om te zorgen voor de bescherming van de rechten en vrijheden van werknemers met betrekking tot hun persoonsgegevens in het kader van de werkgelegenheid.

925 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen, en betreffende het vrije verkeer van die gegevens, PB L 8 van 2001.

Voorbeeld: In de zaak *Worten*[926] bevatten de gegevens een register van de werktijden met de dagelijkse werk- en rusttijden, die persoonsgegevens vormen. De nationale wetgeving kan van een werkgever verlangen dat deze registers met werktijden ter beschikking worden gesteld van de nationale autoriteiten die verantwoordelijk zijn voor het toezicht op de arbeidsomstandigheden. Dit houdt in dat er onmiddellijke toegang tot de betrokken persoonsgegevens wordt gegeven. De toegang tot de persoonsgegevens is echter nodig om de nationale autoriteit in staat te stellen om de wetgeving inzake arbeidsvoorwaarden op te volgen[927].

De **RvE** heeft in 1989 de Aanbeveling inzake arbeidsgegevens aangenomen, die in 2015 werd geactualiseerd[928]. De aanbeveling heeft betrekking op de verwerking van persoonsgegevens voor werkgelegenheidsdoeleinden in zowel de particuliere als openbare sectoren. De verwerking moet voldoen aan bepaalde beginselen en beperkingen, zoals het beginsel van transparantie en de raadpleging van vertegenwoordigers van de werknemers alvorens controlesystemen op de werkplek worden geïnstalleerd. In de aanbeveling wordt ook gesteld dat werknemers preventieve maatregelen moeten toepassen, zoals filters, in plaats van de monitoring van het internetgebruik van werknemers.

Een enquête over de meest voorkomende problemen die specifiek zijn voor de arbeidscontext is te vinden in een werkdocument van Groep artikel 29[929]. De Werkgroep analyseerde het belang van toestemming als rechtsgrond voor de verwerking van arbeidsgegevens[930]. Hij oordeelde dat de economische ongelijkheid tussen de werkgever die om toestemming vraagt en de werknemer die toestemming geeft in veel gevallen vragen zal oproepen over of de toestemming vrijelijk is gegeven of niet. Bij het beoordelen van de geldigheid van toestemming in de arbeidscontext moeten de omstandigheden waaronder toestemming is vereist als rechtsgrondslag voor gegevensverwerking, derhalve zorgvuldig worden onderzocht.

926 HVJ, zaak C-342/12, *Worten — Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT)*, 30 mei 2013, punt 19.

927 *Ibid.*, punt 43.

928 Raad van Europa, Comité van Ministers (2015), Aanbeveling Rec(2015)5 aan de lidstaten inzake de verwerking van persoonsgegevens in arbeidscontext, april 2015.

929 Groep artikel 29 (2017), *Advies 2/2017 over gegevensverwerking op het werk*, WP 249, Brussel, 8 juni 2017.

930 Groep artikel 29 (2005), *Werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995*, WP 114, Brussel, 25 november 2005.

Een veel voorkomend gegevensbeschermingsprobleem in de typische werkomgeving van nu is in hoeverre de elektronische communicatie van werknemers op de werkplek rechtmatig kan worden gemonitord. Vaak wordt gesteld dat dit probleem gemakkelijk kan worden opgelost door het privégebruik van communicatiefaciliteiten op het werk te verbieden. Een dergelijk algemeen verbod zou echter onevenredig en onrealistisch kunnen zijn. De uitspraken van het EHRM in *Copland/Verenigd Koninkrijk* en Bărbulescu/Roemenië zijn in deze context van bijzonder belang.

Voorbeeld: In *Copland/Verenigd Koninkrijk*[931] was het telefoon-, e-mail- en internetgebruik van een werkneemster van een school heimelijk gemonitord om vast te stellen of zij buitensporig veel gebruikmaakte van schoolfaciliteiten voor persoonlijke doeleinden. Het EHRM oordeelde dat telefoongesprekken vanuit bedrijfsruimten onder de begrippen privéleven en correspondentie vielen. Dergelijke vanaf het werk gevoerde gesprekken en verstuurde e-mails, evenals uit de monitoring van persoonlijk internetgebruik afgeleide informatie, worden daarom beschermd door artikel 8 van het EVRM. In het geval van de verzoekster bestonden er geen bepalingen die de omstandigheden reguleerden waaronder werkgevers het telefoon-, e-mail- en internetgebruik van werknemers konden monitoren. De inmenging was derhalve niet in overeenstemming met de wet. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Voorbeeld: In *Bărbulescu/Roemenië*[932] was de verzoeker ontslagen omdat hij tijdens werkuren gebruik had gemaakt van het internet op zijn werkplek, wat in strijd was met de interne voorschriften. De werkgever monitorde zijn communicatie. De verslagen, die berichten tonen die louter privé van aard zijn, werden tijdens de binnenlandse procedure getoond. Het EHRM oordeelde dat artikel 8 van toepassing was en liet daarmee de vraag open of de verzoeker gezien de beperkende voorschriften van de werkgever een redelijke mate van privacy had kunnen verwachten. Het oordeelde echter dat de voorschriften van een werkgever het persoonlijke sociale leven van werknemers op de werkplek niet tot nul konden reduceren.

Wat de gegrondheid betreft, moest de verdragsluitende staten een ruime beoordelingsmarge worden verleend bij het bepalen van de noodzaak tot vaststelling van een rechtskader ter regulering van de voorwaarden

931 EHRM, *Copland/Verenigd Koninkrijk*, nr. 62617/00, 3 april 2007.

932 EHRM, *Bărbulescu/Roemenië* [Grote kamer], nr. 61496/08, 5 september 2017, punt 121.

onder welke een werkgever de niet-werkgerelateerde communicatie van werknemers, in elektronische of andere vorm, op de werkplek mag reglementeren. Niettemin moesten de nationale autoriteiten verzekeren dat de invoering door werkgevers van maatregelen ter monitoring van correspondentie en andere communicatie, ongeacht de omvang en duur van dergelijke maatregelen, vergezeld ging van passende en voldoende waarborgen tegen misbruik. Evenredigheid en procedurele waarborgen tegen willekeur zijn essentiële voorwaarden en het EHRM stelde een aantal factoren vast die in de gegeven omstandigheden van belang waren. Deze omvatten onder meer de omvang van de monitoring door de werkgever en de mate waarin inbreuk wordt gepleegd op de privacy van de werknemer, de consequenties voor de werknemer en de vraag of in adequate waarborgen werd voorzien. Nationale autoriteiten moesten er bovendien voor zorgen dat een werknemer wiens communicatie was gemonitord toegang had tot een rechtsmiddel bij een rechterlijke instantie die bevoegd was te bepalen in hoeverre, in ieder geval in beginsel, de genoemde criteria in acht waren genomen en of de betwiste maatregelen rechtmatig waren.

In deze zaak oordeelde het EHRM dat artikel 8 was geschonden, omdat de nationale autoriteiten de verzoeker geen adequate bescherming hadden geboden van het recht op eerbiediging van zijn privéleven en zijn communicatie, en daardoor geen rechtvaardig evenwicht tussen de verschillende belangen hadden verzekerd.

Volgens de Aanbeveling inzake arbeidsgegevens van de RvE moeten persoonsgegevens die worden verzameld voor arbeidsdoeleinden rechtstreeks bij de individuele werknemers worden verkregen.

De verzameling van persoonsgegevens voor aanwervingsdoeleinden moet worden beperkt tot de informatie die noodzakelijk is om de geschiktheid van kandidaten en hun carrièrepotentieel te beoordelen.

Ook wordt in de aanbeveling specifiek verwezen naar op oordeelsvorming gebaseerde gegevens met betrekking tot de prestaties of het potentieel van individuele werknemers. Op oordeelsvorming gebaseerde gegevens moeten zijn gebaseerd op eerlijke en redelijke evaluaties en mogen niet beledigend geformuleerd zijn. Dit wordt vereist door de beginselen van eerlijke gegevensverwerking en juistheid van gegevens.

Een specifiek aspect van gegevensbeschermingswetgeving in de verhouding werkgever-werknemer is de rol van werknemersvertegenwoordigers. Deze vertegenwoordigers kunnen de persoonsgegevens van werknemers enkel ontvangen voor zover dit noodzakelijk is om de belangen van de werknemers te vertegenwoordigen of indien dergelijke gegevens noodzakelijk zijn om de verplichtingen die zijn vastgelegd in collectieve arbeidsovereenkomsten, te vervullen of te controleren.

Gevoelige persoonsgegevens die worden verzameld voor arbeidsdoeleinden, mogen alleen in specifieke gevallen worden verwerkt en zijn onderworpen aan de in het nationale recht neergelegde waarborgen. Werkgevers mogen werknemers of sollicitanten enkel vragen naar hun gezondheidstoestand of hen medisch onderzoeken indien dit noodzakelijk is. Dit kan zijn om; hun geschiktheid voor het werk te bepalen; te voldoen aan de vereisten van ziektepreventie; de vitale belangen van de betrokkene of andere werknemers en natuurlijke personen te waarborgen; de mogelijkheid te geven op sociale uitkeringen, of om te reageren op gerechtelijke verzoeken. Gezondheidsgegevens mogen niet worden verzameld uit andere bronnen dan de betrokken werknemer, behoudens wanneer uitdrukkelijke en geïnformeerde toestemming is verkregen of het nationale recht daarin voorziet.

Volgens de Aanbeveling inzake arbeidsgegevens moeten werknemers worden geïnformeerd over het doeleinde van de verwerking van hun persoonsgegevens, het type verzamelde persoonsgegevens, de entiteiten waaraan de gegevens regelmatig worden meegedeeld en het doeleinde en de rechtsgrondslag van deze openbaarmakingen. Elektronische communicatie kan alleen worden geraadpleegd op grond van veiligheid of andere rechtmatige redenen, en dergelijke raadpleging is enkel toegestaan nadat werknemers op de hoogte werden gesteld dat de werknemer toegang kan hebben tot dergelijke mededelingen.

Werknemers moeten recht op toegang tot hun arbeidsgegevens hebben, evenals een recht op rectificatie of uitwissing. Indien op oordeelsvorming gebaseerde gegevens worden verwerkt, moeten werknemers voorts het recht hebben om het oordeel aan te vechten. Deze rechten mogen echter tijdelijk worden beperkt voor interne onderzoeksdoeleinden. Indien een werknemer toegang, rectificatie of uitwissing van persoonlijke arbeidsgegevens wordt geweigerd, moet het nationale recht voorzien in passende procedures om de weigering te betwisten.

9.3. Gezondheidsgegevens

Belangrijkste punt

- Medische gegevens zijn gevoelige gegevens en genieten daarom specifieke bescherming.

Persoonsgegevens die de gezondheid van de betrokkene betreffen worden door artikel 9, lid 1, van de AVG en artikel 6 van het Gemoderniseerd Verdrag 108 aangemerkt als gevoelige gegevens. Medische gegevens zijn daarom onderworpen aan strengere gegevensverwerkingsregels dan niet-gevoelige gegevens. De AVG verbiedt de verwerking van "persoonsgegevens betreffende gezondheid" (d.w.z. "alle gegevens [...]die betrekking hebben op de gezondheidstoestand van een betrokkene en die informatie geven over de lichamelijke of geestelijke gezondheidstoestand van de betrokkene in het verleden, het heden en de toekomst")[933], evenals genetische en biometrische gegevens, tenzij het is toegestaan op grond van artikel 9, lid 2. Beide soorten gegevens werden opgenomen in de lijst van "bijzondere categorieën gegevens"[934].

Voorbeeld: In *Z./Finland*[935] had de ex-echtgenoot van de verzoekster, die besmet was met hiv, een aantal seksuele misdrijven gepleegd. Vervolgens was hij veroordeeld voor doodslag op grond van het feit dat hij zijn slachtoffers bewust had blootgesteld aan het risico van een hiv-infectie. De nationale rechtbank had verordend dat de volledige gerechtelijke uitspraak en de zaakgerelateerde documenten gedurende een termijn van tien jaar vertrouwelijk moesten blijven, ondanks verzoeken van de verzoekster om een langere termijn vast te stellen. Het hof van beroep wees deze verzoeken af en in het arrest van het hof werden de volledige namen van zowel de verzoekster als haar ex-echtgenoot genoemd. Het EHRM oordeelde dat de inmenging niet noodzakelijk moest worden geacht in een democratische samenleving, aangezien de bescherming van medische gegevens van

933 Algemene verordening gegevensbescherming, overweging 35.

934 *Ibid.*, artikel 2.

935 EHRM, *Z./Finland*, nr. 22009/93, 25 februari 1997, punten 94 en 112; zie ook EHRM, *M.S./Zweden*, nr. 20837/92, 27 augustus 1997; EHRM, *L.L./Frankrijk*, nr. 7508/02, 10 oktober 2006; EHRM, *I./Finland*, nr. 20511/03, 17 juli 2008; EHRM, *K.H. e.a./Slowakije*, nr. 32881/04, 28 april 2009; EHRM, *Szuluk/Verenigd Koninkrijk*, nr. 36936/05, 2 juni 2009.

wezenlijk belang is voor de uitoefening van het recht op eerbiediging van het privé-, familie- en gezinsleven, met name wanneer het gaat om hiv-infecties, gezien het stigma dat daar in veel samenlevingen op rust. Daarom heeft het hof geconcludeerd dat het toestaan van toegang tot het arrest van het hof, dat de identiteit en medische toestand van de verzoekster beschreef, tot tien jaar na de afgifte van het vonnis, zou indruisen tegen artikel 8 van het EVRM.

In het **Unierecht** staat artikel 9, lid 2, onder h), van de AVG de verwerking van medische gegevens toe wanneer dit noodzakelijk is voor de doeleinden van preventieve geneeskunde of medische diagnose, het verstrekken van zorg of behandelingen, of het beheer van gezondheidsdiensten. Deze verwerking is echter alleen toegestaan wanneer de gegevens worden verwerkt door een gezondheidswerker die onderworpen is aan het beroepsgeheim, of door een andere persoon voor wie een gelijkwaardige geheimhoudingsplicht geldt[936].

In het **recht van** de RvE past de Aanbeveling van de RvE inzake medische gegevens van 1997 de beginselen van Verdrag 108 meer in detail toe op gegevensverwerking op medisch gebied[937]. De voorgestelde regels zijn in overeenstemming met die van de AVG wat betreft het rechtmatige doeleinde van de verwerking van medische gegevens, het noodzakelijk beroepsgeheim voor personen die gezondheidsgegevens gebruiken, en de rechten van de betrokkenen op transparantie, toegang, rectificatie en uitwissing. Voorts mogen medische gegevens die rechtmatig door gezondheidswerkers worden verwerkt niet worden overgedragen aan rechtshandhavingsautoriteiten, tenzij er "voldoende waarborgen worden geboden om openbaarmaking die niet consistent is met (...) de eerbiediging van het privéleven als gegarandeerd door artikel 8 van het EHRM, te voorkomen"[938]. De nationale wetgeving moet ook "worden geformuleerd met voldoende nauwkeurigheid en passende rechtsbescherming geven tegen willekeur"[939].

Voorts bevat de Aanbeveling inzake medische gegevens bijzondere bepalingen ten aanzien van de medische gegevens van ongeboren kinderen en wilsonbekwame personen, en van de verwerking van generieke gegevens. Wetenschappelijk

936 Zie ook EHRM, *Biriuk/Litouwen*, nr. 23373/03, 25 november 2008.

937 Raad van Europa, Comité van Ministers (1997), Aanbeveling Rec(97)5 aan de lidstaten tot bescherming van de medische gegevens, 13 februari 1997. Deze Aanbeveling wordt op dit moment herzien.

938 EHRM, *Avilkina e.a./Rusland*, nr. 1585/09, 6 juni 2013, punt 53.

939 EHRM, *L.H./Letland*, nr. 52019/07, 29 april 2014, punt 59.

onderzoek wordt uitdrukkelijk erkend als een reden om gegevens langer te bewaren dan dat ze nodig zijn, hoewel dit doorgaans anonimisering zal vereisen. Artikel 12 van de Aanbeveling inzake medische gegevens bevat gedetailleerde regels voor situaties waarin onderzoekers persoonsgegevens nodig hebben en geanonimiseerde gegevens onvoldoende zijn.

Pseudonimisering kan een passend middel zijn om wetenschappelijke behoeften te vervullen en tegelijkertijd de belangen van de betrokken patiënten te beschermen. Het concept pseudonimisering in het kader van gegevensbescherming wordt nader toegelicht in punt 2.1.1.

De aanbeveling van de RvE uit 2016 inzake gegevens uit genetisch onderzoek is ook van toepassing op de verwerking van gegevens op medisch gebied[940]. Deze aanbeveling is van groot belang voor e-gezondheidszorg, waarbij ICT wordt gebruikt om de medische zorg te vergemakkelijken. Een voorbeeld is het verzenden van de testresultaten van een patiënt van de ene zorgaanbieder naar de andere. Deze aanbeveling is gericht op het beschermen van de rechten van personen wier persoonsgegevens worden verwerkt voor verzekeringsdoeleinden voor verzekeringen tegen risico's in verband met de gezondheid van een persoon, de fysieke integriteit, ouderdom of overlijden. Verzekeraars moeten de verwerking van gezondheidsgerelateerde gegevens rechtvaardigen en deze moeten evenredig zijn aan de aard en het belang van het risico dat wordt overwogen. De verwerking van dit soort gegevens is afhankelijk van de toestemming van de betrokkene. Verzekeraars moeten ook waarborgen voorzien voor de opslag van gezondheidsgerelateerde gegevens.

Klinische proeven — die betrekking hebben op de beoordeling van de effecten van nieuwe geneesmiddelen op patiënten in gedocumenteerde onderzoeksomgevingen — hebben aanzienlijke gevolgen op het gebied van gegevensbescherming. Klinische proeven van medische producten voor menselijk gebruik worden gereguleerd door verordening (EU) nr. 536/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende klinische proeven met geneesmiddelen voor menselijk gebruik en

940 Raad van Europa, Comité van Ministers (2016), Aanbeveling Rec(2016)8 aan de lidstaten inzake de verwerking van persoonlijke gezondheidsgerelateerde gegevens voor verzekeringsdoeleinden, met inbegrip van gegevens uit genetische tests, 26 oktober 2016.

tot intrekking van Richtlijn 2001/20/EG (verordening inzake klinische proeven)[941]. De belangrijkste elementen van de verordening inzake klinische proeven zijn:

- een gestroomlijnde aanvraagprocedure via het EU-portaal[942];
- termijnen voor de beoordeling van de aanvragen voor klinische proeven[943];
- een ethisch comité dat deel uitmaakt van de beoordeling, in overeenstemming met het recht van de lidstaten (en met het Unierecht dat de termijnen bepaalt)[944], en
- verbeterde transparantie van klinische proeven en de resultaten ervan[945].

De AVG bepaalt dat voor de toepassing van de instemming om aan wetenschappelijk onderzoek deel te nemen in klinische proeven, Verordening (EU) nr. 536/2014 van toepassing is[946].

Tal van andere wetgevende en andere initiatieven over persoonsgegevens in de gezondheidssector zijn aanhangig op EU-niveau[947].

Elektronische medische dossiers

Elektronische medische dossiers worden gedefinieerd als "een volledig medisch dossier of soortgelijke documentatie van de fysieke en mentale gezondheidstoestand van een individu in het heden en het verleden, dat in elektronische vorm is opgezet en deze gegevens onmiddellijk beschikbaar maakt ten behoeve van medische behandeling en andere nauw daarmee samenhangende doeleinden"[948].

941 Verordening (EU) nr. 536/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende klinische proeven met geneesmiddelen voor menselijk gebruik en tot intrekking van Richtlijn 2001/20/EG (verordening inzake klinische proeven), PB L 158 van 2014.

942 Verordening inzake klinische proeven, artikel 5, lid 1.

943 *Ibid.*, artikel 5, leden 2-5.

944 *Ibid.*, artikel 2, lid 11.

945 *Ibid.*, artikel 9, lid 1, en overweging 67.

946 Algemene verordening gegevensbescherming, overwegingen 156 en 161.

947 EDPS (2013), *Advies van de Europese Toezichthouder voor gegevensbescherming inzake de mededeling van de Commissie over een "Actieplan e-gezondheidszorg 2012-2020 — Innovatieve gezondheidszorg voor de 21e eeuw"*, Brussel, 27 maart 2013.

948 Aanbeveling van de Commissie van 2 juli 2008 betreffende de grensoverschrijdende interoperabiliteit van systemen voor elektronische medische dossiers, punt 3, onder c).

Elektronische gezondheidsdossiers zijn elektronische versies van de medische geschiedenis van patiënten en mogen klinische gegevens met betrekking tot deze personen bevatten, zoals medische achtergrond, problemen en omstandigheden, medicatie en behandelingen, evenals onderzoeks- en laboratoriumresultaten en -verslagen. Deze elektronische bestanden, die kunnen variëren van volledige dossiers tot loutere extracten of samenvattingen, kunnen worden geraadpleegd door de huisarts, apotheker en andere gezondheidswerkers. Bij het begrip "e-gezondheidszorg" gaat het ook om deze medische dossiers.

Voorbeeld: De heer A heeft een verzekeringspolis afgesloten bij onderneming B, de verzekeraar. Deze laatste zal bepaalde gezondheidsgerelateerde informatie van A verzamelen, zoals huidige gezondheidsproblemen of ziektes. De verzekeraar moet persoonsgegevens met betrekking tot de gezondheid van A apart opslaan van andere gegevens. De verzekeraar moet persoonsgegevens met betrekking tot de gezondheid ook apart opslaan van andere persoonsgegevens. Dit houdt in dat enkel de persoon die de zaak van A behandelt, toegang zal hebben tot de gezondheidsgerelateerde gegevens van A.

Niettemin bestaan er bepaalde gegevensbeschermingskwesties bij elektronische medische dossiers, zoals hun toegankelijkheid, correcte opslag en toegang door de betrokkene.

Naast de elektronische medische dossiers, heeft de Europese Commissie op 10 april 2014 een Groenboek gepubliceerd met betrekking tot mobiele gezondheidszorg (m-gezondheidszorg), gezien het feit dat m-gezondheidszorg een nieuw en snelgroeiend gebied is dat het potentieel heeft om de gezondheidszorg om te vormen en de efficiëntie en kwaliteit ervan te verhogen. De term dekt de medische en openbare gezondheidszorg ondersteund door mobiele toestellen, zoals mobiele telefoon, patiëntenbewakingsapparatuur, personal digital assistants en andere draadloze toestellen, evenals applicaties (bv. welzijnsapplicaties) die aan medische toestellen of sensoren kunnen worden verbonden[949]. De paper beschrijft de risico's van het recht op bescherming van persoonsgegevens die de ontwikkeling van m-gezondheidszorg met zich mee kan brengen en bepaalt dat, gezien het gevoelige karakter van gezondheidsgegevens, de ontwikkeling gepaard moet gaan met specifieke en passende beveiligingswaarborgen voor de gegevens van patiënten,

949 Europese Commissie (2014), *Groenboek over mobiele gezondheid ("mHealth")*, COM(2014) 219 def., Brussel, 10 april 2014.

zoals encryptie, en passende authenticatiemechanismen van de patiënt om beveiligingsrisico's te beperken. De naleving van de regels inzake gegevensbescherming, met inbegrip van de verplichting om informatie te verstrekken aan de betrokkene, gegevensbeveiliging en het beginsel van de rechtmatige verwerking van persoonsgegevens is van vitaal belang voor de opbouw van vertrouwen in m-gezondheidszorgoplossingen[950]. Hiervoor werd een gedragscode opgesteld door de industrie, op basis van de input van een uitgebreide groep belanghebbenden, met vertegenwoordigers die deskundig zijn op het vlak van gegevensbescherming, zelf- en coregulering, ICT en gezondheidszorg[951]. Op het moment van de opstelling van het handboek was het ontwerp van de gedragscode voor commentaar voorgelegd aan Groep artikel 29, in afwachting van de formele goedkeuring ervan.

9.4. Gegevensverwerking voor onderzoek en statistische doeleinden

Belangrijkste punten

- Gegevens die worden verwerkt voor statistische, wetenschappelijke of historische doeleinden mogen niet voor andere doeleinden worden gebruikt.
- Gegevens die rechtmatig werden verzameld voor andere doeleinden, mogen verder worden gebruikt voor statistisch, wetenschappelijk of historisch onderzoek, mits passende waarborgen worden ingevoerd. Anonimisering of pseudonimisering vóór de doorgifte van gegevens aan derde partijen kan deze waarborgen geven.

Het Unierecht voorziet in de verwerking van gegevens voor statistisch en wetenschappelijk of historisch onderzoek, mits passende waarborgen voor de rechten en vrijheden van de betrokkenen aanwezig zijn. Deze kunnen pseudonimisering inhouden[952]. Het Unierecht of het nationale recht kan in bepaalde derogaties van de rechten van betrokkenen voorzien indien deze rechten de verwezenlijking van het rechtmatige doel van het onderzoek waarschijnlijk onmogelijk maken of het ernstig in het gedrang kunnen brengen[953]. Derogaties kunnen worden ingevoerd op het recht op toegang door de betrokkene, het recht op rectificatie, het recht op de beperking van de verwerking en het recht om bezwaar te maken.

950 *Ibid.*, blz. 8.

951 Ontwerp gedragscode inzake privacy voor mobiele gezondheidsapplicaties, 7 juni 2016.

952 Algemene verordening gegevensbescherming, artikel 89, lid 1.

953 *Ibid.*, artikel 89, lid 2.

Hoewel gegevens die op rechtmatige wijze door een verwerkingsverantwoordelijke voor een bepaald doel verzameld werden door deze verwerkingsverantwoordelijke mogen worden hergebruikt voor zijn eigen statistisch, wetenschappelijk of historisch onderzoek, moeten de gegevens worden geanonimiseerd of aan maatregelen worden onderworpen, zoals pseudonimisering, afhankelijk van de context, voordat ze aan een derde partij worden doorgegeven voor statistisch, wetenschappelijk of historisch onderzoek, tenzij de betrokkene hiermee heeft ingestemd of dit specifiek is voorzien in het nationale recht. Gegevens die gepseudonimiseerd worden, blijven onderworpen aan de AVG, in tegenstelling tot geanonimiseerde gegevens[954].

De verordening kent dus een bijzondere behandeling toe aan onderzoek met betrekking tot de algemene regels inzake gegevensbescherming om beperkingen op onderzoeksontwikkeling te voorkomen en om te voldoen aan de doelstelling van de totstandbrenging van een Europese onderzoeksruimte, als bedoeld in artikel 179 van het VWEU. Er wordt voorzien in de ruime interpretatie van de verwerking van persoonsgegevens voor wetenschappelijke doeleinden, met inbegrip van de technologische ontwikkeling en demonstratie, fundamenteel onderzoek, toegepast onderzoek en uit particuliere middelen gefinancierd onderzoek. Voorts wordt het belang erkend van de verzameling van gegevens in registers voor onderzoeksdoeleinden en de eventuele moeilijkheid om het latere doel van de verwerking van persoonsgegevens voor wetenschappelijk onderzoek op het moment van gegevensverzameling volledig te identificeren[955]. Om deze reden staat de verordening de verwerking van gegevens voor deze doeleinden toe, zonder de toestemming van de betrokkenen, mits de passende waarborgen aanwezig zijn.

Een belangrijk voorbeeld van het gebruik van gegevens voor statistische doeleinden zijn officiële statistieken die door de bureaus voor statistiek op nationaal en EU-niveau zijn verkregen op grond van nationale en EU-wetgeving inzake officiële statistieken. Volgens deze wetgeving zijn burgers en ondernemingen doorgaans verplicht om gegevens aan de relevante statistische autoriteiten te verstrekken. Ambtenaren die bij bureaus voor de statistiek werken zijn gebonden aan een bijzonder beroepsgeheim dat zorgvuldig moet worden nageleefd, aangezien dat essentieel is voor een hoog niveau van vertrouwen onder burgers, dat weer nodig is om gegevens ter beschikking te stellen van de statistische autoriteiten[956].

954 *Ibid.*, overweging 26.

955 *Ibid.*, overwegingen 33, 157 en 159.

956 *Ibid.*, artikel 90.

Verordening (EG) nr. 223/2009 betreffende de Europese statistiek bevat essentiële voorschriften voor gegevensbescherming in de context van officiële statistieken, en kan derhalve ook als relevant worden beschouwd voor bepalingen inzake officiële statistieken op nationaal niveau[957]. De verordening handhaaft het beginsel dat officiele statistische activiteiten een voldoende duidelijke rechtsgrond moeten hebben[958].

Voorbeeld: In *Huber/Bundesrepublik Deutschland*[959] klaagde een Oostenrijkse zakenman die naar Duitsland verhuisde dat de verzameling en bewaring door de Duitse autoriteiten van persoonsgegevens van buitenlanders in een centraal register (AZR) die ook voor statistische doeleinden werden gebruikt, zijn rechten onder de richtlijn gegevensbescherming schond. Overwegende dat Richtlijn 95/46/EG bedoeld is om een gelijkwaardig niveau van gegevensbescherming in alle lidstaten te waarborgen, oordeelde het HvJ-EU dat, om een hoog niveau van bescherming in de EU te waarborgen, het concept van noodzaak in artikel 7, onder e), geen verschillende betekenis kan hebben in de lidstaten. Het is dus een begrip dat zijn eigen onafhankelijke betekenis heeft in het Unierecht, en moet worden geïnterpreteerd op een manier die volledig overeenstemt met de doelstelling van Richtlijn 95/46/EG. Het HvJ-EU, dat opmerkte dat alleen anonieme gegevens moeten worden gevraagd voor statistische doeleinden, oordeelde dat het Duitse register niet verenigbaar was met het noodzakelijkheidsvereiste op grond van artikel 7, onder e).

In het kader van de **RvE** kunnen gegevens verder worden verwerkt voor wetenschappelijke, historische of statistische doeleinden wanneer dit in het algemeen belang is, en moeten ze worden onderworpen aan passende waarborgen[960]. De

957 Verordening (EG) nr. 223/2009 van het Europees Parlement en de Raad van 11 maart 2009 betreffende de Europese statistiek en tot intrekking van Verordening (EG, Euratom) nr. 1101/2008 van het Europees Parlement en de Raad betreffende de toezending van onder de statistische geheimhoudingsplicht vallende gegevens aan het Bureau voor de Statistiek van de Europese Gemeenschappen, Verordening (EG) nr. 322/97 van de Raad betreffende de communautaire statistiek en Besluit 89/382/EEG, Euratom van de Raad tot oprichting van een Comité statistisch programma van de Europese Gemeenschappen, PB L 87 van 2009, als gewijzigd bij Verordening (EU) 2015/759 van het Europees Parlement en de Raad van 29 april 2015 tot wijziging van Verordening (EG) nr. 223/2009 inzake Europese statistieken, PB L 123 van 2015.

958 Dit beginsel wordt verder uitgewerkt in de Praktijkcode voor Europese statistiek van Eurostat, die overeenkomstig artikel 11 van de verordening betreffende de Europese statistiek een ethische leidraad biedt voor het opstellen van officiële statistieken, met inbegrip van het weloverwogen gebruik van persoonsgegevens.

959 HvJ-EU, zaak C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [Grote kamer], 16 december 2008; zie voornamelijk punt 68.

960 Gemoderniseerd Verdrag 108, artikel 5, lid 4, onder b).

rechten van betrokkenen mogen ook beperkt worden bij de verwerking van gegevens voor statistische doeleinden, op voorwaarde dat er geen herkenbaar risico bestaat op inbreuken op hun rechten en vrijheden[961].

De Aanbeveling inzake statistische gegevens uit 1997 heeft betrekking op de prestaties van statistische activiteiten in de openbare en private sectoren[962].

Gegevens die worden verwerkt door een verwerkingsverantwoordelijke voor statistische doeleinden mogen niet voor andere doeleinden worden gebruikt. Gegevens die worden verzameld voor niet-statistische doeleinden dienen beschikbaar te zijn voor verdere statistische doeleinden. De Aanbeveling inzake statistische gegevens staat ook toe dat gegevens aan derden worden meegedeeld als dit uitsluitend voor statistische doeleinden is. In dergelijke gevallen moeten de partijen overeenstemming bereiken over het rechtmatige verdere gebruik voor statistische doeleinden en dit schriftelijk vastleggen. Aangezien dit de toestemming door de betrokkene, indien nodig, niet kan vervangen, moeten er passende waarborgen zijn vastgelegd in de nationale wetgeving om de risico's van verkeerd gebruik van persoonsgegevens te minimaliseren, zoals een verplichting om gegevens voorafgaand aan een openbaarmaking te anonimiseren of te pseudonimiseren.

Professionals op het gebied van statistisch onderzoek moeten volgens de nationale wetgeving aan speciale verplichtingen inzake beroepsgeheim zijn gebonden — zoals gewoonlijk het geval is voor officiële statistieken. Dit dient zich ook uit te strekken tot interviewers en andere verzamelaars van persoonsgegevens indien deze betrokken zijn bij de verzameling van gegevens van betrokkenen of andere personen.

Als een statistische enquête waarin gebruik wordt gemaakt van persoonsgegevens niet wettelijk is toegestaan, zouden betrokkenen toestemming moeten geven voor het gebruik van hun gegevens om dit gebruik rechtmatig te maken of zou hun ten minste de mogelijkheid kunnen worden geboden om zich tegen het gebruik van hun gegevens te verzetten. Indien persoonsgegevens worden verzameld voor statistische doeleinden door personen te interviewen, moet aan deze personen duidelijk worden meegedeeld of de verstrekking van gegevens volgens het nationale recht verplicht is of niet.

961 *Ibid.*, artikel 11, lid 2.

962 Raad van Europa, Comité van Ministers (1997), Aanbeveling Rec(97)18 aan de lidstaten inzake de bescherming van persoonsgegevens die worden verzameld en verwerkt voor statistische doeleinden, 30 september 1997.

Wanneer een statistische enquête niet kan worden uitgevoerd met gegevens over anonieme personen, en persoonsgegevens absoluut noodzakelijk zijn, moeten de gegevens die voor dit doeleinde worden verzameld zo spoedig mogelijk worden geanonimiseerd. De resultaten van de statistische enquête mogen op geen enkele wijze de identificatie van enige betrokkene mogelijk maken, tenzij hier duidelijk geen risico's aan verbonden zijn.

Nadat de statistische analyse is verricht, moeten de gebruikte persoonsgegevens ofwel worden uitgewist, ofwel worden geanonimiseerd. In zulke gevallen wordt in de Aanbeveling inzake statistische gegevens voorgesteld dat identificatiegegevens gescheiden van andere persoonsgegevens worden opgeslagen. Dit betekent bijvoorbeeld dat de encryptiesleutel of de lijst met de identificerende synoniemen apart moet worden opgeslagen van de andere gegevens.

9.5. Financiële gegevens

Belangrijkste punten

- Hoewel financiële gegevens geen gevoelige gegevens zijn in het kader van Gemoderniseerd Verdrag 108 of de AVG, moeten passende waarborgen worden geboden voor de verwerking ervan met het oog op de juistheid en de beveiliging van de gegevens.
- Elektronische betalingssystemen in het bijzonder moeten voorzien in ingebouwde gegevensbescherming, dat wil zeggen privacy en gegevensbescherming door ontwerp en door standaardinstellingen.
- Op dit gebied kunnen zich bijzondere gegevensbeschermingsvraagstukken voordoen door de noodzaak om over passende authenticatiemechanismen te beschikken.

Voorbeeld: In *Michaud/Frankrijk*[963] betwistte de verzoeker, een Franse advocaat, zijn verplichting uit hoofde van het Franse recht om verdenkingen over mogelijke witwasactiviteiten door zijn cliënten te melden. Het EHRM merkte op dat een verplichting voor advocaten om informatie met betrekking tot een andere persoon, die in hun bezit is gekomen door middel van beroepsuitwisselingen met die persoon, aan de administratieve autoriteiten

963 EHRM, *Michaud/Frankrijk*, nr. 12323/11, 6 december 2012. Zie ook EHRM, *Niemietz/Duitsland*, nr. 13710/88, 16 december 1992, punt 29, en EHRM, *Halford/Verenigd Koninkrijk*, nr. 20605/92, 25 juni 1997, punt 42.

te melden, een inmenging in het recht van advocaten op eerbiediging van hun correspondentie en privéleven als neergelegd in artikel 8 van het EVRM vormde, aangezien dat begrip ook beroeps- of zakelijke activiteiten omvatte. De inmenging was echter in overeenstemming met de wet en diende een rechtmatig doel, namelijk de preventie van wanordelijkheden en strafbare feiten. Gezien het feit dat de advocaten slechts in zeer specifieke omstandigheden zijn onderworpen aan de verplichting tot melding van verdachte activiteiten, oordeelde het EHRM dat deze verplichting evenredig was. Het Hof concludeerde dat er geen inbreuk op artikel 8 had plaatsgevonden.

Voorbeeld: In *M.N. e.a./San Marino*[964] sloot de aanvrager, een Italiaanse burger, een fiduciaire overeenkomst met een onderneming waarvoor het onderzoek werd verricht. Dit betekende dat de onderneming onderhevig was aan huiszoekingen en inbeslagneming van (elektronische) documentatie. De aanvrager diende een klacht in bij de rechtbank van San Marino met het argument dat er geen verband bestaat tussen hem en de vermeende strafbare feiten. Het Hof verklaarde echter zijn klacht niet ontvankelijk, aangezien hij geen "belanghebbende partij" was. Het EHRM was van mening dat de aanvrager, in vergelijking met een "belanghebbende", een aanzienlijk nadeel ondervond met betrekking tot rechterlijke bescherming, maar zijn gegevens waren nog steeds onderhevig aan de huiszoekings- en inbeslagnemingsacties. Bijgevolg heeft het Hof geoordeeld dat artikel 8 was geschonden.

Voorbeeld: In *G.S.B./Zwitserland*[965] werden de bankgegevens van de aanvrager doorgegeven aan de belastingsautoriteiten in de VS op basis van de administratieve samenwerkingsovereenkomst tussen Zwitserland en de VS. Het EHRM was van oordeel dat de doorgifte niet in strijd was met artikel 8 van het EVRM, want de inmenging met het recht op privacy van de aanvrager was wettelijk voorgeschreven, streefde een rechtmatig doel na en was evenredig met het openbaar belang.

De toepassing van het algemene wettelijke kader voor gegevensbescherming, zoals uiteengezet in Verdrag 108, op de context van betalingen, is door de **RvE** ontwikkeld

964 EHRM, *M.N. e.a./San Marino*, nr. 28005/12, 7 juli 2015.

965 EHRM, *G.S.B./Zwitserland*, nr. 28601/11, 22 december 2015.

in Aanbeveling Rec(90)19 van 1990[966]. In deze aanbeveling wordt het toepassingsgebied van de rechtmatige verzameling en het rechtmatig gebruik van gegevens in het kader van betalingen, in het bijzonder betalingen door middel van creditcards, verduidelijkt. Voorts worden de nationale wetgevers voorzien van gedetailleerde aanbevelingen over de regels inzake de openbaarmaking van betalingsgegevens aan derden, termijnen voor het bewaren van deze gegevens, transparantie, gegevensbeveiliging en grensoverschrijdend gegevensverkeer, en toezicht en rechtsmiddelen. De RvE heeft ook een advies over de overdracht van belastinggegevens opgesteld[967] dat aanbevelingen en kwesties formuleert waarmee rekening moet worden gehouden, bij de doorgifte van belastinggegevens.

Het EHRM staat de doorgifte van financiële gegevens — voornamelijk de details van iemands bankrekening — toe onder artikel 8 van het EVRM, als dit bij wet is voorgeschreven, een rechtmatig doel nastreeft en evenredig is met het openbaar belang[968].

In termen van **het Unierecht** moeten elektronische betalingssystemen die persoonsgegevens verwerken, voldoen aan de AVG. Daarom moeten deze systemen zorgen voor gegevensbescherming door ontwerp en door standaardinstellingen. Gegevensbescherming door ontwerp verplicht de verwerkingsverantwoordelijke om in passende technische en organisatorische maatregelen te voorzien om de beginselen inzake gegevensbescherming uit te voeren. Gegevensbescherming door standaardinstellingen betekent dat de verwerkingsverantwoordelijke ervoor moet zorgen dat alleen de persoonsgegevens die noodzakelijk zijn voor een bepaald doel, automatisch kunnen worden verwerkt (zie punt 4.4). Met betrekking tot financiële gegevens oordeelde het HvJ-EU dat doorgegeven belastinggegevens als persoonsgegevens kunnen worden beschouwd[969]. De Groep gegevensbescherming artikel 29 heeft gerelateerde richtlijnen uitgevaardigd voor lidstaten, met inbegrip van criteria voor de naleving van de regels inzake gegevensbescherming bij de geautomatiseerde uitwisseling van persoonsgegevens voor belastingdoeleinden via

966 Raad van Europa, Comité van Ministers (1990), Aanbeveling Rec(90)19 inzake de bescherming van persoonsgegevens die worden gebruikt voor betalingen en aanverwante activiteiten, 13 september 1990.

967 Raad van Europa, Raadgevend Comité voor Verdrag 108 (2014), Advies over de mogelijke gevolgen voor gegevensbescherming van mechanismen voor de automatische uitwisseling van gegevens tussen lidstaten van gegevens voor administratieve en fiscale doeleinden, 4 juni 2014.

968 EHRM, *G.S.B./Zwitserland*, nr. 28601/11, 22 december 2015.

969 HvJ-EU, zaak C-201/14, *Smaranda Bara e.a./Casa Națională de Asigurări de Sănătate e.a.*, 1 oktober 2015, punt 29.

geautomatiseerde weg[970]. Bovendien werden een aantal rechtsinstrumenten aangenomen om de financiële markten en de activiteiten van kredietinstellingen en beleggingsondernemingen te reguleren[971]. Andere rechtsinstrumenten zijn bedoeld om de bestrijding van handel met voorkennis en marktmanipulatie te ondersteunen[972]. De belangrijkste gebieden die van invloed zijn op de bescherming van gegevens zijn:

- de bewaring van bestanden van financiële transacties;
- de doorgifte van persoonsgegevens aan derde landen;
- het opnemen van telefoongesprekken of elektronische communicaties, met inbegrip van de bevoegdheid van de bevoegde autoriteiten om bestanden van telefoon- en gegevensverkeer op te vragen;
- het meedelen van persoonlijke informatie, waaronder de publicatie van sancties;
- de toezicht- en onderzoeksbevoegdheden van de bevoegde autoriteiten, met inbegrip van inspecties ter plaatse en het betreden van private ruimten om documenten in beslag te nemen;
- de mechanismen voor het melden van inbreuken, d.w.z. klokkenluidersregelingen, en
- de samenwerking tussen bevoegde autoriteiten van de lidstaten en de Europese Autoriteit voor effecten en markten (ESMA).

970 Groep gegevensbescherming artikel 29 (2015), Verklaring van de WP29 over automatische interstatelijke uitwisseling van persoonsgegevens voor belastingdoeleinden, 14/EN WP 230.

971 Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU, PB L 173 van 2014; Verordening (EU) nr. 600/2014 van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Verordening (EU) nr. 648/2012, PB L 173 van 2014; Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot de werkzaamheden van kredietinstellingen en het prudentieel toezicht op kredietinstellingen en beleggingsondernemingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van Richtlijnen 2006/48/EG en 2006/49/EG, PB L 176 van 2013.

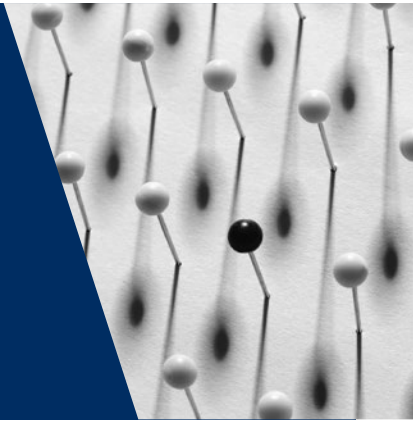
972 Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (Verordening marktmisbruik) en houdende intrekking van Richtlijn 2003/6/EG van het Europees Parlement en de Raad en Richtlijnen 2003/124/EG, 2003/125/EG en 2004/72/EG van de Commissie, PB L 173 van 2014.

Er zijn andere onderwerpen in dit gebied die ook specifiek zijn gereguleerd, zoals de verzameling van gegevens over de financiële status van betrokkenen[973] of grensoverschrijdende betalingen door middel van bankoverschrijvingen, die onvermijdelijk tot verkeer van persoonsgegevens leiden[974].

973 Verordening (EG) nr. 1060/2009 van het Europees Parlement en de Raad van 16 september 2009 inzake ratingbureaus, PB L 302 van 2009, en laatstelijk gewijzigd bij Richtlijn 2014/51/EU van het Europees Parlement en de Raad van 16 april 2014 tot wijziging van de Richtlijnen 2003/71/EG en 2009/138/EG en Verordeningen (EG) nr. 1060/2009, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 met betrekking tot de bevoegdheid van de Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen) en de Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), PB L 153 van 2014; Verordening (EU) nr. 462/2013 van het Europees Parlement en de Raad van 21 mei 2013 tot wijziging van Verordening (EG) nr. 1060/2009 inzake ratingbureaus, PB L 146 van 2013.

974 Richtlijn 2007/64/EG van het Europees Parlement en de Raad van 13 november 2007 betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 97/5/EG, PB L 319 van 2007, zoals gewijzigd bij Richtlijn 2009/111/EG van het Europees Parlement en de Raad van 16 september 2009 tot wijziging van de Richtlijnen 2006/48/EG, 2006/49/EG en 2007/64/EG wat betreft banken die zijn aangesloten bij centrale instellingen, bepaalde eigenvermogensbestanddelen, grote risico's, het toezichtkader en het crisisbeheer, PB L 302 van 2009.

10 Moderne uitdagingen bij de bescherming van persoonsgegevens



Het digitale tijdperk, of het tijdperk van de informatietechnologie, wordt gekenmerkt door het wijdverbreide gebruik van computers, het internet en digitale technologie. Dit omvat het verzamelen en verwerken van enorme hoeveelheden gegevens, met inbegrip van persoonsgegevens. De verzameling en verwerking van persoonsgegevens in een gemondialiseerde economie betekent dat de grensoverschrijdende gegevensstromen toenemen. Die verwerking kan aanzienlijke en duidelijk zichtbare voordelen in het dagelijkse leven met zich meebrengen: zoekmachines vergemakkelijken de toegang tot grote hoeveelheden informatie en kennis, socialenetwerkdiensten stellen mensen uit heel de wereld in staat om te communiceren, meningen uit te drukken en steun te mobiliseren voor sociale, ecologische en politieke doelen, terwijl ondernemingen en consumenten profiteren van effectieve en doeltreffende marketingtechnieken die de economie een impuls geven. Technologie en de verwerking van persoonsgegevens zijn ook onmisbaar voor de overheidsinstanties bij de bestrijding van criminaliteit en terrorisme. Evenzo kan big data — de verzameling, opslag en analyse van grote hoeveelheden informatie voor de identificatie van patronen en om gedrag te voorspellen — "een bron zijn van aanzienlijke waarde voor de samenleving, en de productiviteit, de prestaties van de openbare sector en de sociale participatie verbeteren"[975].

Ondanks de verschillende voordelen die het met zich meebrengt, stelt het digitale tijdperk ook uitdagingen inzake privacy en gegevensbescherming, aangezien enorme hoeveelheden persoonlijke informatie worden verzameld en verwerkt op steeds meer complexe en ondoorzichtige manieren. De technologische vooruitgang

975 Raad van Europa, Raadgevend Comité voor Verdrag 108, *Richtsnoeren betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens in de wereld van big data*, T-PD(2017)01, Straatsburg, 23 januari 2017.

heeft geleid tot de ontwikkeling van grootschalige bestanden die gemakkelijk vergeleken kunnen worden en verder worden geanalyseerd om patronen te zoeken, of voor de vaststelling van beslissingen op basis van algoritmes, die een ongekend inzicht in het menselijk gedrag en privéleven kunnen bieden[976].

Nieuwe technologieën zijn krachtig en kunnen bijzonder gevaarlijk zijn indien zij in de verkeerde handen vallen. Staatsinstellingen die op grote schaal bewakingsactiviteiten uitvoeren en die gebruik maken van deze technologieën, zijn een voorbeeld van de ernstige gevolgen die deze technologieën kunnen hebben op de rechten van natuurlijke personen. In 2013 zorgden de onthullingen van Edward Snowden over de uitvoering van grootschalige bewakingsprogramma's via internet en telefoon door inlichtingendiensten in bepaalde lidstaten voor grote bezorgdheid over de gevaren die bewakingsactiviteiten inhouden voor privacy, het democratisch bestuur en de vrijheid van meningsuiting. Grootschalige bewaking en technologieën die een gemondialiseerde opslag en verwerking van persoonsgegevens en massale toegang tot gegevens mogelijk maken, kunnen afbreuk doen aan de essentie van het recht op privacy[977]. Daarnaast kunnen ze een negatief effect hebben op de politieke cultuur en een schrikbarend effect op de democratie, creativiteit en innovatie[978]. De loutere vrees dat de staat voortdurend het gedrag en acties van burgers kan opsporen en analyseren, kan burgers ontmoedigen om hun mening te uiten over bepaalde aangelegenheden en leiden tot achterdocht en voorzichtigheid[979]. Deze uitdagingen hebben een aantal openbare instellingen, onderzoekscentra en maatschappelijke organisaties ertoe aangezet om de mogelijke effecten van nieuwe technologieën op de samenleving te analyseren. In 2015 heeft de Europese Toezichthouder voor gegevensbescherming een aantal initiatieven gelanceerd die gericht zijn op de beoordeling van de impact van big data en het internet der dingen op ethiek. Met name is een adviesgroep inzake ethiek opgericht die zich richt op het stimuleren van "een open en gefundeerde discussie over digitale ethiek, waarmee de EU de voordelen van technologie voor de samenleving en de economie kan realiseren en

976 Europees Parlement (2017), Resolutie over de gevolgen van big data voor de grondrechten: persoonlijke levenssfeer, gegevensbescherming, non-discriminatie, veiligheid en rechtshandhaving (P8_TA-PROV(2017)0076, Straatsburg, 14 maart 2017.

977 Zie VN, Algemene Vergadering, *Rapport van de Speciale rapporteur inzake de bevordering en bescherming van mensenrechten en fundamentele vrijheden bij de bestrijding van terrorisme*, Ben Emmerson, A/69/397, 23 september 2014, punt 59. Zie ook EHRM, *Factsheet on Mass surveillance*, juli 2017.

978 EDPS (2015), *Meeting the challenges of big data*, Advies 7/2015, Brussel, 19 november 2015.

979 Zie met name HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en Kärntner Landesregierung e.a. [Grote kamer], 8 april 2014, punt 37.

tegelijkertijd de rechten en vrijheden van personen versterkt, in het bijzonder hun recht op privacy en gegevensbescherming"[980].

De verwerking van persoonsgegevens is ook een krachtig instrument in handen van ondernemingen. Tegenwoordig kan het gedetailleerde informatie over de gezondheid of de financiële situatie van een persoon onthullen, informatie die daarna gebruikt wordt door ondernemingen om belangrijke beslissingen voor natuurlijke personen te nemen, zoals de verzekeringspremie die moet worden toegepast of hun kredietwaardigheid. Technieken voor gegevensverwerking kunnen ook gevolgen hebben voor de democratische processen wanneer ze gebruikt worden door politici of ondernemingen om verkiezingen te beïnvloeden — bijvoorbeeld via "micro-targeting" van mededelingen aan kiezers. Met andere woorden, terwijl privacy aanvankelijk werd beschouwd als een recht op bescherming van personen tegen ongerechtvaardigde inmenging door de overheid, kan dit recht in het moderne tijdperk ook worden bedreigd door de krachten van private actoren. Hierdoor rijzen er vragen over het gebruik van technologie en voorspellende controles in besluiten die gevolgen hebben voor het dagelijkse leven van natuurlijke personen, en versterkt de noodzaak om ervoor te zorgen dat bij elke verwerking van persoonsgegevens de vereisten op het gebied van grondrechten geëerbiedigd worden.

Gegevensbescherming is onlosmakelijk verbonden met technologische, sociale en politieke veranderingen. Daarom zou het onmogelijk zijn om een volledige lijst van toekomstige uitdagingen op te stellen. Dit hoofdstuk kijkt naar geselecteerde gebieden met betrekking tot big data, sociale netwerken op internet en de digitale eengemaakte markt van de EU. Het is geen diepgaande beoordeling van deze gebieden uit een oogpunt van gegevensbescherming, maar benadrukt de hoeveelheid van mogelijke interacties tussen nieuwe of herziene menselijke activiteiten en gegevensbescherming.

980 EDPS, Besluit van 3 december 2015 tot oprichting van een externe adviesgroep voor de ethische aspecten van gegevensbescherming ("de adviesgroep ethiek"), 3 december 2015, overweging 5.

10.1. Big data, algoritmen en artificiële intelligentie

Belangrijkste punten

- Ontwrichtende innovaties in ICT vormen een nieuwe manier van leven waar sociale betrekkingen, het bedrijfsleven, particuliere en openbare diensten digitaal verbonden zijn, zodat een groeiende hoeveelheid gegevens, waaronder veel persoonsgegevens, geproduceerd wordt.
- Overheden, ondernemingen en burgers zijn in toenemende mate actief in een gegevensgestuurde economie, waar de gegevens zelf waardevolle activa zijn geworden.
- Het concept big data verwijst naar zowel de gegevens als analyse daarvan.
- Persoonsgegevens die worden verwerkt door middel van big data-analyse, vallen onder het Unierecht en het recht van de RvE.
- Derogaties van de regels en rechten inzake gegevensbescherming zijn beperkt tot bepaalde geselecteerde rechten en tot specifieke situaties waarin de tenuitvoerlegging van een recht onmogelijk zou blijken of onevenredige inspanningen zou vereisen bij verwerkingsverantwoordelijken.
- Volledig geautomatiseerde besluitvorming is over het algemeen verboden, behalve in specifieke gevallen.
- Het bewustzijn van en de controle door natuurlijke personen zijn van essentieel belang om de handhaving van rechten te waarborgen.

In onze wereld die steeds meer gedigitaliseerd is, laat elke activiteit een digitaal spoor achter dat verzameld, verwerkt en geëvalueerd of geanalyseerd kan worden. Met nieuwe informatie- en communicatietechnologieën, worden steeds meer gegevens verzameld en opgeslagen[981]. Tot voor kort was technologie niet in staat de massa aan gegevens te analyseren of evalueren of om nuttige conclusies te trekken. De gegevens waren gewoonweg te talrijk om ze te evalueren, te complex, te slecht gestructureerd en te snel om ontwikkelingen en gewoontes te identificeren.

981 Europese Commissie, Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's — Naar een bloeiende dataeconomie, COM(2014) 442 def., Brussel, 2 juli 2014.

10.1.1. Big data, algoritmen en kunstmatige intelligentie definiëren

Big data

De term "big data" is een modewoord dat kan verwijzen naar verschillende concepten, naargelang de context. Het omvat over het algemeen "de groeiende technologische mogelijkheid om te verzamelen, te verwerken en om nieuwe en voorspellende kennis uit een groot volume, grote snelheid en een grote diversiteit aan gegevens te halen"[982]. Daarom dekt het concept "big data" zowel de gegevens zelf als de analyse van gegevens.

De **bronnen** zijn verschillende soorten gegevens en omvatten mensen en hun persoonsgegevens, machines of sensoren, klimatologische informatie, satellietbeelden, digitale foto's of video's, of GPS-signalen. Een groot deel van de gegevens en informatie betreft echter persoonsgegevens — alles van een naam, foto, e-mailadres, bankgegevens, GPS-gegevens, berichten op socialenetwerksites, medische informatie of het IP-adres van een computer[983].

Big data heeft ook betrekking op de **verwerking**, analyse en evaluatie van de massagegevens en beschikbare informatie, d.w.z. om nuttige informatie te verkrijgen voor de toepassing van big data-analyse. Dit betekent dat de verzamelde gegevens en informatie kunnen worden gebruikt voor andere doeleinden dan de oorspronkelijk beoogde doeleinden, bv. statistieke trends of meer op maat gemaakte diensten, zoals reclame. In feite, waar de technologieën bestaan om big data te verzamelen, verwerken en evalueren, kan elk soort informatie worden gecombineerd en opnieuw worden geëvalueerd: financiële transacties, kredietwaardigheid, medische behandeling, privégebruik, beroepsactiviteiten, opsporing en gevolgde routes, internetgebruik, elektronische kaarten en smartphones, video- of communicatiebewaking. De analyse van big data brengt een nieuwe hoeveelheid gegevens met zich

982 Raad van Europa, Raadgevend Comité voor Verdrag 108, Richtsnoeren betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens in een wereld van big data, 23 januari 2017, blz. 2; Europese Commissie, Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's — Naar een bloeiende data-economie, COM(2014) 442 def., Brussel, 2 juli 2014, blz. 4; Internationale Telecommunicatie-unie (2015), Aanbeveling Y.3600. Big data — Cloud computing op basis van behoeften en bekwaamheden.

983 Informatieblad van de Europese Commissie betreffende de hervorming van de EU inzake gegevensbescherming en big data; Raad van Europa, Raadgevend Comité voor Verdrag 108, Richtsnoeren betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens in een wereld van big data, 23 januari 2017, blz. 2.

mee die kan worden geëvalueerd en gebruikt in real-time voor, bijvoorbeeld, op maat gemaakte diensten aan consumenten.

Algoritmen en kunstmatige intelligentie

Kunstmatige intelligentie (artificial intelligence, AI) verwijst naar de intelligentie van machines die als "intelligent orgaan" optreden. Als intelligent orgaan kunnen bepaalde apparaten, met de hulp van software, hun omgeving waarnemen en actie ondernemen volgens algoritmen. De term AI wordt toegepast wanneer een machine "cognitieve" functies nabootst — zoals leren en een probleem oplossen — die normaal gezien worden geassocieerd met natuurlijke personen[984]. Om besluitvorming na te bootsen, gebruiken moderne technologie en software algoritmen die toestellen gebruiken voor het nemen van "geautomatiseerde besluiten". Een algoritme wordt het best omschreven als een stapsgewijze procedure voor berekening, gegevensverwerking, evaluatie en geautomatiseerde redenering en besluitvorming.

Net als bij de analyse van big data, vereisen AI en de geautomatiseerde besluitvorming die hieruit voortkomt, de verzameling en verwerking van grote hoeveelheden gegevens. Deze gegevens kunnen afkomstig zijn van het apparaat zelf (warmte van de remmen, brandstof enz.) of van de omgeving. Profilering is bijvoorbeeld een proces dat zich beroept op een geautomatiseerde besluitvorming volgens vooraf vastgestelde modellen of factoren.

Voorbeeld: Profilering en gerichte reclame

Profilering op basis van big data omvat het zoeken naar patronen die "kenmerken van een soort persoonlijkheid" weerspiegelen — bijvoorbeeld wanneer online winkelbedrijven producten voorstellen "die u misschien ook leuk vindt" op basis van gegevens die verzameld werden van de eerder gekozen producten in het winkelwagentje van een klant. Hoe meer gegevens, hoe duidelijker de mozaïek. De smartphone werkt bijvoorbeeld als een krachtige vragenlijst die natuurlijke personen bij elk gebruik bewust en onbewust invullen.

De moderne psychografie — de wetenschap van de bestudering van persoonlijkheden — gebruikt de OCEAN-methode op basis waarvan het soort persoonlijkheid waarmee men te maken heeft, wordt bepaald. De

984 Stuart Russel en Peter Norvig, *Artificial Intelligence: A Modern Approach (2e ed.)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, blz. 27, 32-58, 968-972; Stuart Russel en Peter Norvig, *Artificial Intelligence: A Modern Approach (3e ed.)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, blz. 2.

"Big Five"-persoonlijkheidsdimensies hebben betrekking op Openheid (hoe open een persoon staat voor nieuwe ervaringen), Zorgvuldigheid (in welke mate een persoon perfectionistisch is), Extraversie (hoe sociaal een persoon is), Servicegerichtheid (hoe aangenaam een persoon is) en Emotionele stabiliteit (hoe gevoelig een persoon is). Deze informatie profileert de persoon in kwestie, zijn/haar behoeften en angsten, hoe hij/zij zal handelen, enz. Vervolgens wordt dit aangevuld door andere informatie over de persoon, afkomstig van andere beschikbare bronnen, van datahandelaren, sociale netwerken (met inbegrip van de "vind-ik-leuks" op berichten en gepubliceerde foto's), tot de muziek waar online naar wordt geluisterd of GPS en traceergegevens.

De enorme hoeveelheid aan profielen die worden gecreëerd door big data-analysetechnieken wordt vervolgens vergeleken teneinde vergelijkbare patronen te identificeren en clusters van persoonlijkheden te vormen. De informatie over het gedrag en attitudes van bepaalde persoonlijkheden wordt derhalve omgezet. Met de toegang tot en het gebruik van big data vindt er een omzetting van de persoonlijkheidstest plaats, aangezien de informatie over gedrag en attitudes nu wordt gebruikt om de persoonlijkheid van de persoon te beschrijven. Met de combinatie van informatie over "vind-ik-leuks" op sociale netwerken, de traceergegevens, de muziek beluisterd of films bekeken, kan een duidelijk beeld tot stand komen van de persoonlijkheid van een persoon waardoor bedrijven op maat gemaakte reclame en/of informatie kunnen aanbieden op basis van de "persoonlijkheid" van die persoon. Bovenal kan deze informatie onmiddellijk verwerkt worden[985].

10.1.2. Afweging van de voordelen en risico's van big data

Moderne verwerkingstechnieken kunnen grote hoeveelheden gegevens aan, snel nieuwe gegevens importeren, een onmiddellijke verwerking van gegevens verzorgen in een korte reactietijd (zelfs in geval van complexe verzoeken), in verschillende en gelijktijdige verzoeken voorzien, en verschillende soorten informatie (foto's, teksten of nummers) analyseren. Deze technologische innovaties maken het mogelijk om massa's gegevens en informatie onmiddellijk te structureren, te verwerken

985 Verwerkingstechnieken en nieuwe software evalueren onmiddellijk de informatie over wat een persoon leuk vindt, waar hij/zij naar kijkt tijdens het online winkelen of wat hij/zij aan zijn/haar winkelwagentje toevoegt, en kunnen "producten" voorstellen die hem/haar misschien interesseren op basis van de verzamelde informatie.

en te evalueren[986]. Door de hoeveelheid beschikbare en geanalyseerde gegevens exponentieel te verhogen, kan men nu resultaten verkrijgen die onmogelijk zouden zijn bij kleinschaligere analyses. Big data heeft bijgedragen tot de ontwikkeling van een nieuw ondernemingsveld, waarin nieuwe diensten voor bedrijven en consumenten tegelijkertijd kunnen ontstaan. De waarde van de persoonsgegevens van de EU-burgers heeft de mogelijkheid om jaarlijks tot bijna 1 biljoen EUR te stijgen tegen 2020[987]. Derhalve kan big data nieuwe **kansen** bieden die voortvloeien uit de evaluatie van gegevens over de massa voor nieuwe sociale, economische of wetenschappelijke inzichten die voor zowel natuurlijke personen als bedrijven en regeringen voordelen kunnen bieden[988].

Big data-analyse kan patronen tussen verschillende bronnen en gegevensreeksen aan het licht brengen, zodat nuttige inzichten op gebieden zoals de wetenschap en de geneeskunde mogelijk worden gemaakt. Dit geldt bijvoorbeeld voor domeinen zoals gezondheid, voedselzekerheid, intelligente vervoerssystemen, energie-efficiëntie of stadsplanning. Deze onmiddellijke analyse van informatie kan worden gebruikt om ingestelde systemen te verbeteren. Op het gebied van onderzoek kunnen nieuwe inzichten worden opgedaan door grote hoeveelheden gegevens met statistische evaluatie te combineren, met name in disciplines waarin veel van die gegevens tot op heden slechts handmatig werden beoordeeld. Nieuwe behandelingen kunnen worden ontwikkeld en op maat gemaakt voor individuele patiënten, gebaseerd op vergelijkingen met de massa aan beschikbare informatie. Ondernemingen hopen dat de analyse van big data hun een concurrentievoordeel zal geven, potentiële besparingen zal genereren en nieuwe bedrijfsactiviteiten zal creëren via

986 De ontwikkeling van software voor de verwerking van big data staat nog in de kinderschoenen. Niettemin werden onlangs analytische programma's ontwikkeld, met name voor de onmiddellijke analyse van gegevens en informatie op grote schaal van de activiteiten van natuurlijke personen. De mogelijkheid om big data op een gestructureerde manier te analyseren en verwerken, heeft nieuwe mogelijkheden gegeven voor profilering en gerichte reclame. Europese Commissie, Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's — Naar een bloeiende data-economie, COM(2014) 442 def., Brussel, 2 juli 2014; informatieblad van de Europese Commissie betreffende de hervorming van de EU inzake gegevensbescherming en big data, en Raad van Europa, Richtsnoeren inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens in een wereld van big data, 23 januari 2017, blz. 2.

987 Informatieblad van de Europese Commissie betreffende de hervorming van de EU inzake gegevensbescherming en big data.

988 Internationale conferentie van commissarissen voor de bescherming van gegevens en de persoonlijke levenssfeer (2014), resolutie over big data en de Europese Commissie, Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's — Naar een bloeiende data-economie, COM(2014) 442 def., Brussel, 2 juli 2014, blz.2; informatieblad van de Europese Commissie betreffende de hervorming van de EU inzake gegevensbescherming en big data, en Raad van Europa, Richtsnoeren inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens in een wereld van big data, 23 januari 2017, blz. 1.

rechtstreekse, persoonlijke dienstverlening. Overheidsagentschappen hopen de verbetering van het strafrechtstelsel te verwezenlijken. De strategie voor een digitale eengemaakte markt voor Europa van de Commissie erkent het potentieel van datagestuurde technologieën, diensten en big data die fungeren als katalysator voor economische groei, innovatie en digitalisering in de EU[989].

Big data draagt echter ook **risico's** met zich mee die over het algemeen worden geassocieerd met deze drie eigenschappen: omvang, snelheid en diversiteit van de verwerkte gegevens. Het volume heeft betrekking op de hoeveelheid verwerkte gegevens, diversiteit op de aantallen en de diversiteit in de soorten gegevens, terwijl snelheid betrekking heeft op de snelheid van de gegevensverwerking. Specifieke overwegingen voor gegevensbescherming ontstaan voornamelijk wanneer big data-analyses worden gebruikt voor grote reeksen gegevens om nieuwe en voorspellende kennis voor besluitvorming met betrekking tot natuurlijke personen en/of groepen te extraheren[990]. De risico's voor gegevensbescherming en privacy met betrekking tot big data zijn naar voren gekomen in de adviezen van de EDPS en Groep artikel 29, verordeningen van het Europees Parlement en in de beleidsdocumenten van de Raad van Europa[991].

Risico's zijn onder meer het misbruik van big data door personen met toegang tot de massa aan informatie via manipulatie, discriminatie of onderdrukking van natuurlijke personen of specifieke groepen in de samenleving[992]. Wanneer massa's persoonsgegevens of informatie over individueel gedrag worden verzameld, verwerkt en geëvalueerd, kan de exploitatie ervan leiden tot belangrijke schendingen van grondrechten en fundamentele vrijheden die verder reiken dan het recht op privacy. Het is onmogelijk om precies te meten in hoeverre gegevens over de persoonlijke levenssfeer en persoonsgegevens in het gedrang kunnen komen. Het Europees

989 Resolutie van het Europees Parlement van 14 maart 2017 over de gevolgen van big data voor de grondrechten: persoonlijke levenssfeer, gegevensbescherming, non-discriminatie, veiligheid en rechtshandhaving (2016/2225(INI)).

990 Raad van Europa, Raadgevend Comité voor Verdrag 108, Richtsnoeren betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens in een wereld van big data, 23 januari 2017, blz. 2.

991 Zie bijvoorbeeld EDPS (2015), *Het hoofd bieden aan de uitdagingen van big data*, Advies 7/2015, 19 november 2015; EDPS (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, Advies 8/2016, 23 september 2016; Europees Parlement (2016), Verordening over de gevolgen van big data voor de grondrechten: persoonlijke levenssfeer, gegevensbescherming, non-discriminatie, veiligheid en rechtshandhaving, P8_TA(2017)0076, Straatsburg, 14 maart 2017; Raad van Europa, Raadgevend Comité voor Verdrag 108, Richtsnoeren betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens in een wereld van big data, T-PD(2017)01, Straatsburg, 23 januari 2017.

992 Internationale conferentie van de Raad van commissarissen voor gegevensbescherming en privacy (2014), resolutie over big data.

Parlement wees op een gebrek aan methodologie om een empirisch onderbouwde evaluatie te maken van de totale impact van big data, maar er zijn aanwijzingen dat de big data-analyse belangrijke horizontale gevolgen kan hebben in de openbare en private sector[993].

De algemene verordening gegevensbescherming bevat bepalingen over het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming, met inbegrip van profilering[994]. Het privacyprobleem ontstaat wanneer de uitoefening van het recht op bezwaar menselijke tussenkomst vereist waarbij de betrokkene zijn/haar standpunt kan uitdrukken en het besluit kan betwisten[995]. Dit kan aanleiding geven tot problemen bij het waarborgen van een adequaat niveau van bescherming van persoonsgegevens wanneer, bijvoorbeeld, geen menselijk ingrijpen mogelijk is of wanneer de algoritmen te complex zijn en de hoeveelheid gegevens te groot is om natuurlijke personen motiveringen te geven voor bepaalde beslissingen en/of voorafgaand informatie te verstrekken om hun toestemming te verkrijgen. Een voorbeeld van het gebruik van AI en geautomatiseerde besluitvorming is te vinden in de recente ontwikkelingen in hypotheekaanvragen of tijdens wervingsprocessen. Aanvragen worden geweigerd of afgewezen op basis van het feit dat de aanvragers niet voldoen aan vooraf vastgestelde parameters of factoren.

10.1.3. Aangelegenheden inzake gegevensbescherming

Wat de bescherming van gegevens betreft, zijn vooral de omvang en diversiteit van de verwerkte persoonsgegevens enerzijds, en de verwerking en de resultaten anderzijds, van belang. De invoering van complexe algoritmes en software om gegevens over de massa om te zetten tot een middel voor besluitvorming heeft invloed op natuurlijke personen en groepen in het bijzonder, met name in gevallen van profilering of etikettering, en roept tot slot veel vragen op in verband met gegevensbescherming[996].

993 Resolutie van het Europees Parlement van 14 maart 2017 over de gevolgen van big data voor de grondrechten: persoonlijke levenssfeer, gegevensbescherming, non-discriminatie, veiligheid en rechtshandhaving (2016/2225(INI)).

994 Algemene verordening gegevensbescherming, artikel 22.

995 *Ibid.*, artikel 22, lid 3.

996 Raad van Europa, Raadgevend Comité voor Verdrag 108, Richtsnoeren betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens in een wereld van big data, 23 januari 2017, blz. 2.

De identificatie van verwerkingsverantwoordelijken en verwerkers, en hun aansprakelijkheid

Big data en AI roepen verscheidene vragen op in verband met de identificatie van verwerkingsverantwoordelijken en verwerkers, evenals hun aansprakelijkheid: wanneer een dergelijke grote omvang aan gegevens wordt verzameld en verwerkt, wie is dan de eigenaar van de gegevens? Wanneer gegevens worden verwerkt door intelligentiemachines en software, wie is dan de verwerkingsverantwoordelijke? Wat zijn de precieze verantwoordelijkheden van elke actor in de verwerking? En voor welke doeleinden mag big data worden gebruikt?

De kwestie van aansprakelijkheid in het kader van AI wordt des te meer een uitdaging wanneer een AI een besluit neemt op grond van gegevensverwerking die het zelf heeft ontwikkeld. De algemene verordening gegevensbescherming biedt een juridisch kader voor de aansprakelijkheid van de verwerkingsverantwoordelijke en de verwerker. De onrechtmatige verwerking van persoonsgegevens geeft aanleiding tot aansprakelijkheid van de verwerkingsverantwoordelijke en de verwerker[997]. Kunstmatige intelligentie en geautomatiseerde besluitvorming doen vragen rijzen over wie aansprakelijk is voor schendingen van de persoonlijke levenssfeer van de betrokkenen waarbij de complexiteit en de omvang van de verwerkte gegevens niet met zekerheid kan worden bepaald. Wanneer AI en algoritmes als producten worden gezien, werpt dit vragen op over persoonlijke aansprakelijkheid, die onder de algemene verordening gegevensbescherming wordt geregeld, en productaansprakelijkheid, die hier niet onder valt[998]. Hiervoor zouden regels inzake aansprakelijkheid moeten worden opgesteld om de kloof te dichten tussen persoonlijke aansprakelijkheid en productaansprakelijkheid voor robotica en AI, bijvoorbeeld met inbegrip van geautomatiseerde besluitvorming[999].

Impact op beginselen inzake gegevensbescherming

De aard, de analyse en het gebruik van big data zoals hierboven beschreven vormen een uitdaging voor de toepassing van sommige traditionele, fundamentele

997 Algemene verordening gegevensbescherming, artikelen 77-79 en artikel 82.

998 Europees Parlement, European Civil Law Rules in Robotics, Directoraat-generaal intern beleid, (oktober 2016), blz. 14.

999 Toespraak van Roberto Viola op het media-seminar over het Europese recht inzake robotica in het Europees Parlement. (SPEECH 16/02/2017); Aankondiging van het Europees Parlement op het verzoek aan de Commissie voor een voorstel betreffende voorschriften inzake burgerlijke aansprakelijkheid voor robotica en AI.

beginselen van de Europese wetgeving inzake gegevensbescherming[1000]. Deze uitdaging heeft voornamelijk betrekking op de beginselen van rechtmatigheid, gegevensminimalisering, doelbinding en transparantie.

Het beginsel van gegevensminimalisering vereist dat persoonsgegevens adequaat, relevant en beperkt blijven tot hetgeen noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Het bedrijfsmodel van big data kan echter als de antithese van gegevensminimalisering worden gezien, aangezien het steeds meer gegevens vereist, vaak voor niet-gespecificeerde doeleinden.

Hetzelfde geldt voor het beginsel van doelbinding, dat vereist dat gegevens moeten worden verwerkt voor specifieke doeleinden en niet kunnen worden gebruikt voor doeleinden die onverenigbaar zijn met het oorspronkelijke doel van de verzameling, tenzij een dergelijke verwerking is gebaseerd op een rechtsgrond — zoals, maar niet beperkt tot, de toestemming van de betrokkene (zie punt 4.1.1).

Ten slotte vormt big data ook een uitdaging voor het beginsel van de juistheid van gegevens, aangezien big data-applicaties de neiging hebben om gegevens uit diverse bronnen te verzamelen zonder de mogelijkheid te hebben om ze na te gaan en/of de juistheid van de verzamelde gegevens te bewaren[1001].

Specifieke voorschriften en rechten

De algemene regel blijft dat persoonsgegevens die via big data-analyse worden verwerkt, onder het toepassingsgebied van de wetgeving inzake gegevensbescherming vallen. Het Unierecht en het RvE-recht hebben echter specifieke voorschriften of derogaties voor specifieke gevallen met betrekking tot complexe algoritmische gegevensverwerking opgenomen.

In het RvE-recht worden nieuwe rechten aan betrokkenen toegekend door Gemoderniseerd Verdrag 108 om hen in staat te stellen hun persoonsgegevens effectiever te controleren in het "big data"-tijdperk. Dit is bijvoorbeeld duidelijk het geval met artikel 9, lid 1, onder a), c) en d), van het Gemoderniseerd Verdrag over het recht om niet te worden onderworpen aan een besluit dat een aanzienlijk effect

1000 Raad van Europa, *Richtsnoeren inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens in een wereld van big data*, T-PD (2017)01, Straatsburg, 23 januari 2017.

1001 EDPS (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, Advies 8/2016, 23 september 2016, blz. 8.

heeft op de persoon in kwestie, uitsluitend gebaseerd op een geautomatiseerde gegevensverwerking, zonder rekening te houden met zijn of haar mening; het recht om, op verzoek, kennis te nemen van de aan de gegevensverwerking ten grondslag liggende redenering waar de resultaten van een dergelijke verwerking op hem of haar worden toegepast, alsmede het recht om bezwaar te maken. Andere bepalingen van Gemoderniseerd Verdrag 108, met name over transparantie en bijkomende verplichtingen zijn complementaire elementen van het beschermingsmechanisme ingesteld onder Gemoderniseerd Verdrag 108 om digitale uitdagingen aan te pakken.

In het recht van de Europese Unie moet er, naast de gevallen genoemd in artikel 23 van de algemene verordening gegevensbescherming, gezorgd worden voor **transparantie** voor alle verwerkingen van persoonsgegevens. Het is vooral van belang met betrekking tot diensten via het internet en andere complexe geautomatiseerde gegevensverwerking, zoals het gebruik van algoritmen voor besluitvorming. Hier moeten de eigenschappen van de gegevensverwerkingssystemen het voor betrokkenen mogelijk maken om daadwerkelijk te begrijpen wat er met hun gegevens gebeurt. Om te zorgen voor een eerlijke en transparante verwerking, vereist de algemene verordening gegevensbescherming dat de verwerkingsverantwoordelijke relevante informatie over de opzet van de geautomatiseerde besluitvorming, met inbegrip van profilering, aan de betrokkene verstrekt[1002]. In zijn aanbeveling over de bescherming en bevordering van het recht op vrijheid van meningsuiting en het recht op persoonlijke levenssfeer, met betrekking tot netneutraliteit, heeft het Comité van Ministers van de Raad van Europa aanbevolen dat aanbieders van internetdiensten "gebruikers duidelijke, volledige en openbaar toegankelijke informatie verschaffen met betrekking tot alle methoden voor verkeersbeheer die gevolgen kunnen hebben voor de toegang tot en verdeling van inhoud, applicaties of diensten"[1003]. De verslagen over methoden voor verkeersbeheer van het internet die door de bevoegde autoriteiten in alle lidstaten worden opgesteld, moeten op een open en transparante wijze worden samengesteld en gratis openbaar dienen te worden gemaakt[1004].

1002 Algemene verordening gegevensbescherming, artikel 13, lid 2, onder f).

1003 Raad van Europa, Comité van Ministers (2016), Aanbeveling CM/Rec(2016)1 van het Comité van Ministers van de lidstaten inzake de bescherming en bevordering van het recht op vrijheid van meningsuiting en het recht op persoonlijke levenssfeer met betrekking tot netneutraliteit, 13 januari 2016, punt 5.1.

1004 *Ibid.*, punt 5.2.

Verwerkingsverantwoordelijken moeten de betrokkenen niet enkel **informeren** — of de gegevens van hen werden verzameld of niet — over de specifieke informatie over de gegevens die werden verzameld en de beoogde verwerking (zie punt 6.1.1), maar ook, in voorkomend geval, over het bestaan van geautomatiseerde besluitvormingsprocessen, en hen op de hoogte stellen van de logica erachter[1005], de doelstellingen en de mogelijke gevolgen van dergelijke processen. De AVG verduidelijkt ook (enkel in gevallen waar persoonsgegevens niet werden verkregen van de betrokkene) dat de verwerkingsverantwoordelijke niet verplicht is om de betrokkene dergelijke informatie te verstrekken wanneer "de verstrekking van informatie aan de betrokkene onmogelijk blijkt of onevenredig veel moeite kost"[1006]. Zoals echter beklemtoond door Groep artikel 29 in zijn *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, mag de complexiteit van de verwerking op zichzelf de verwerkingsverantwoordelijke niet verhinderen om de betrokkene duidelijke uitleg te geven over de doelstellingen en de in de verwerking gebruikte analyse[1007].

De rechten van betrokkenen op **toegang**, **rectificatie** en **wissing** van hun persoonsgegevens, evenals hun recht op een **beperking** van de verwerking, omvat geen dergelijke vrijstelling. De verplichting van de verwerkingsverantwoordelijke om de betrokkene te informeren over een rectificatie of wissing van zijn/haar persoonsgegevens (zie punt 6.1.4) mag evenwel ook worden opgeheven indien een dergelijke kennisgeving "onmogelijk blijkt of onevenredig veel moeite kost"[1008].

Betrokkenen hebben ook een recht op **bezwaar**, zoals bepaald in artikel 21 van de AVG (zie punt 6.1.6), voor elke verwerking van hun persoonsgegevens, ook in het geval van big data-analyse. Hoewel verwerkingsverantwoordelijken kunnen worden vrijgesteld van deze verplichting indien zij dwingende gerechtvaardigde belangen kunnen aantonen, geldt een dergelijke vrijstelling niet bij verwerkingen die voor directmarketingdoeleinden worden gebruikt.

Specifieke derogaties van deze rechten kunnen worden aangehaald door verwerkingsverantwoordelijken bij de verwerking van persoonsgegevens met het oog op

1005 Algemene verordening gegevensbescherming, artikel 13, lid 2, onder f), en artikel 14, lid 2, onder g).

1006 *Ibid.*, artikel 14, lid 5, onder b).

1007 Groep artikel 29, *Richtsnoeren over geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, WP 251, 3 oktober 2017, blz. 14.

1008 Algemene verordening gegevensbescherming, artikel 19.

archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden[1009].

Met betrekking tot **profilering en geautomatiseerde besluitvorming** heeft de AVG specifieke regels ingevoerd: In artikel 22, lid 1, wordt bepaald dat de betrokkene "het recht [heeft] niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking [...] gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden". Zoals wordt onderstreept door de richtsnoeren van Groep artikel 29, stelt dit artikel een algemeen verbod op volledig geautomatiseerde besluitvorming[1010]. Verwerkingsverantwoordelijken kunnen enkel worden vrijgesteld van een dergelijk verbod in drie specifieke gevallen: wanneer de beslissing: 1) noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke, 2) toegestaan is krachtens een EU- of nationale wetgeving, of 3) gebaseerd is op een expliciete instemming[1011].

Individuele controle

De complexiteit van en het gebrek aan transparantie rond big data-analyse kan ervoor zorgen dat de ideeën over de individuele controle van persoonsgegevens heroverwogen moeten worden. Dit gegeven moet worden afgestemd op de sociale en technologische context, rekening houdend met het gebrek aan kennis van individuele personen. Daarom moet de gegevensbescherming met betrekking tot big data een ruimer begrip van controle over het gebruik van gegevens aannemen, op grond van welke individuele controle evolueert tot een meer complex proces van meerdere effectbeoordelingen van de risico's die bestaan in verband met het gebruik van gegevens[1012].

Hoe goed een big data-applicatie is, hangt af van hoe goed zij de wensen of het gedrag van testpersonen (of consumenten) kan voorspellen. Huidige voorspellingsmodellen die gebaseerd zijn op big data-analyse worden voortdurend verfijnd. Recente ontwikkelingen omvatten niet alleen het gebruik van gegevens om persoonlijkheden te categoriseren (d.w.z. het gedrag en de attitudes), maar analyseren

1009 *Ibid.*, artikel 89, leden 2 en 3.

1010 Groep artikel 29, *Richtsnoeren over geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, WP 251, 3 oktober 2017, blz. 9.

1011 Algemene verordening gegevensbescherming, artikel 22, lid 2.

1012 Raad van Europa, Raadgevend Comité voor Verdrag 108, *Richtsnoeren inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens in een wereld van big data*, T-PD(2017)01, Straatsburg, 23 januari 2017.

gedrag door de analyse van stempatronen en de intensiteit waarmee berichten worden geschreven of de lichaamstemperatuur. Al deze informatie kan onmiddellijk worden gebruikt samen met de kennis die men opdoet uit big data-evaluaties om de kredietwaardigheid te beoordelen tijdens bijvoorbeeld een onderhoud met een bankvertegenwoordiger. De beoordeling is niet gebaseerd op de verdiensten van de natuurlijke persoon die een krediet aanvraagt, maar eerder op de gedragskenmerken die worden ontleend aan de analyse en evaluatie van big data-informatie, d.w.z. of de kandidaat met een sterke of kalmerende stem spreekt, zijn/haar lichaamstaal of lichaamstemperatuur.

Profilering en gerichte reclame is niet noodzakelijkerwijs een probleem als natuurlijke personen **zich ervan bewust** zijn dat ze onderworpen zijn aan gerichte advertenties. Profilering wordt een probleem wanneer het wordt gebruikt om individuen te manipuleren, d.w.z. wanneer bepaalde persoonlijkheden of groepen mensen worden gezocht om politieke campagne te voeren. Groepen zwevende kiezers bijvoorbeeld kunnen worden aangesproken via politieke berichten die zijn opgesteld op basis van hun "persoonlijkheid" en attitudes. Een andere kwestie is het gebruik van dergelijke profilering om de toegang te weigeren tot goederen en diensten voor bepaalde personen. Een garantie die bescherming kan bieden tegen misbruik van big data en persoonlijke informatie is pseudonimisering (zie punt 2.1.1)[1013]. Indien persoonsgegevens daadwerkelijk zijn geanonimiseerd, d.w.z. dat er geen informatie meer is die kan leiden tot de betrokkene, vallen deze gevallen buiten het toepassingsgebied van de AVG. De instemming van de betrokkenen en van de natuurlijke personen bij de verwerking van big data vormt ook een uitdaging voor de wetgeving inzake gegevensbescherming. Deze instemming omvat gerichte advertenties en profilering die kunnen worden gerechtvaardigd omwille van de "klantenervaring", en instemming met het gebruik van de massa's persoonsgegevens om op informatie gebaseerde analytische instrumenten te verfijnen en te ontwikkelen. Het besef, of het ontbreken daarvan, van de big data-verwerking doet verschillende vragen rijzen over de manier waarop betrokkenen hun rechten kunnen uitoefenen, aangezien de verwerking van big data zich baseert op zowel gepseudonimiseerde als geanonimiseerde informatie die onderworpen is aan algoritmes. Terwijl gepseudonimiseerde gegevens vallen onder de algemene verordening gegevensbescherming, is de verordening niet van toepassing op geanonimiseerde gegevens. Individuele zeggenschap over, en het besef van, de verwerking van persoonsgegevens is van cruciaal belang in big data-analyse: zonder deze elementen zal men

1013 *Ibid.*, blz. 2.

geen duidelijk idee hebben over wie de verwerkingsverantwoordelijke of verwerker is, waardoor ze hun rechten niet doeltreffend kunnen uitoefenen.

10.2. Web 2.0 en 3.0: sociale netwerken en het internet der dingen

Belangrijkste punten

- Socialenetwerkdiensten (SNS) zijn online communicatieplatforms waar personen zich kunnen aansluiten bij netwerken van gelijkgezinde gebruikers of die ze kunnen creëren.
- Het internet der dingen is de verbinding van voorwerpen met internet, en de onderlinge koppeling van voorwerpen met elkaar.
- De toestemming van betrokkenen is de meest gangbare rechtsgrondslag voor rechtmatige gegevensverwerking door verwerkingsverantwoordelijken op sociale netwerken.
- Sociale netwerkgebruikers worden over het algemeen beschermd door de "huishoudelijke exceptie"; deze derogatie kan echter in bepaalde situaties worden opgeheven.
- Aanbieders van sociale netwerken worden niet beschermd door de "huishoudelijke exceptie".
- Privacy door ontwerp en door standaardinstellingen is van cruciaal belang om te zorgen voor de beveiliging van gegevens op dit gebied.

10.2.1. Het definiëren van Web 2.0 en 3.0

Socialenetwerkdiensten

Aanvankelijk was het internet bedoeld als netwerk om computers met elkaar te verbinden en berichten te verzenden met beperkte mogelijkheden voor de uitwisseling van gegevens, terwijl websites personen enkel de mogelijkheid gaven om de inhoud ervan passief te bekijken[1014]. In het Web 2.0-tijdperk ontwikkelde het internet zich tot een forum waar gebruikers met elkaar communiceren, samenwerken en input genereren. Dit tijdperk wordt gekenmerkt door het opmerkelijke succes en

1014 Europese Commissie (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 def.

wijdverbreide gebruik van socialenetwerkdiensten die nu een essentieel onderdeel uitmaken van het dagelijkse leven van miljoenen mensen.

Socialenetwerkdiensten (SNS) of "sociale media" kunnen ruim worden gedefinieerd als "online communicatieplatforms die personen in staat stellen om zich aan te sluiten bij netwerken van gelijkgezinde gebruikers of die ze kunnen creëren"[1015]. Om deel uit te maken van een netwerk of om een netwerk op te richten, moeten natuurlijke personen persoonsgegevens verstrekken en een profiel aanmaken. SNS stellen gebruikers in staat om digitale "inhoud" te genereren, variërend van foto's en video's tot links naar artikelen en persoonlijke berichten om hun mening uit te drukken. Door deze online communicatieplatforms kunnen gebruikers communiceren en interageren met verschillende andere gebruikers. Belangrijk is dat het grootste deel van de populaire SNS geen registratiekosten vereist. In plaats van dat gebruikers moeten betalen om zich bij het netwerk aan te sluiten, genereren leveranciers van SNS het grootste deel van hun inkomsten uit gerichte reclame. Adverteerders kunnen veel voordeel halen uit de persoonlijke informatie die dagelijks op deze websites wordt onthuld. De informatie over de leeftijd, het geslacht, de locatie en de interesses van een gebruiker stelt hen in staat om de "juiste" mensen te bereiken met hun advertenties.

Het Comité van Ministers van de Raad van Europa heeft een aanbeveling aangenomen over mensenrechtenbescherming met betrekking tot sociale netwerkdiensten[1016] met daarin een specifieke sectie over bescherming van persoonsgegevens; in 2018 werd deze gecomplementeerd met nog een aanbeveling over de rol en verplichtingen van tussenpersonen op internet[1017].

Voorbeeld: Nora is heel gelukkig omdat haar partner heeft gevraagd of ze met hem wilde trouwen. Ze wil het goede nieuws met haar vrienden en familie delen en besluit een emotioneel bericht op een sociaal netwerk te plaatsen waarin ze haar blijdschap uitdrukt en haar status wijzigt naar "verloofd". De dagen daarna, wanneer zij haar account opent, ziet Nora advertenties over trouwjurken en bloemenwinkels. Hoe komt dit?

1015 Groep artikel 29 (2009), *Advies 5/2009 over sociale netwerken op het internet*, WP 163, 12 juni 2009, blz. 4.

1016 Raad van Europa, Comité van Ministers, Aanbeveling CM/Rec(2012)4 van het Comité van Ministers aan de lidstaten over mensenrechtenbescherming met betrekking tot sociale netwerkdiensten, 4 april 2012.

1017 Raad van Europa, Comité van Ministers, Aanbeveling CM/Rec(2018)2 van het Comité van Ministers aan de lidstaten over de rol en verantwoordelijkheden van tussenpersonen op internet, 7 maart 2018.

Wanneer een advertentie op Facebook wordt gecreëerd, selecteren de bedrijven gespecialiseerd in trouwjurken en bloemen bepaalde parameters die hen in staat stellen om mensen, zoals Nora, te bereiken. Als Nora's profiel aanduidt dat ze een vrouw is, verloofd, in Parijs woont, vlakbij de winkels die trouwjurken en bloemen verkopen en de advertenties plaatsen, ziet ze onmiddellijk de advertenties.

Het internet der dingen

Het internet der dingen (IoT) staat voor de volgende stap in de ontwikkeling van internet: het Web 3.0-tijdperk. Met het IoT kunnen apparaten verbonden worden en communiceren met andere apparaten via het internet. Hierdoor kunnen voorwerpen en mensen verbonden worden met elkaar via communicatienetwerken, om te berichten over hun status en/of de status van hun omgeving[1018]. Het IoT en de verbonden apparaten zijn reeds een realiteit en men verwacht dat ze aanzienlijk zullen groeien in de komende jaren met de creatie en de verdere ontwikkeling van slimme apparaten die zullen leiden tot de ontwikkeling van slimme steden, slimme huizen en slimme bedrijven.

Voorbeeld: IoT kan bijzonder gunstig zijn voor de gezondheidszorg. Ondernemingen hebben reeds apparaten, sensoren en applicaties gecreëerd waarmee de gezondheid van een patiënt kan worden bewaakt. Door het gebruik van een draagbare alarmknop en andere draadloze sensoren in huis, kan men de dagelijkse routine van oudere alleenwonende mensen volgen en waarschuwingen genereren wanneer ernstige storingen worden gedetecteerd in hun dagelijkse schema. Sensoren die vallen registreren worden bijvoorbeeld vaak gebruikt bij oudere mensen. Deze sensoren kunnen vallen nauwkeurig detecteren en de dokter en/of familie van de persoon informeren over de val.

Voorbeeld: Barcelona is een van de meest gangbare voorbeelden van een slimme stad. Sinds 2012 heeft de stad het gebruik van innovatieve technologieën toegepast, met als doel het creëren van een systeem van slim openbaar vervoer, afvalbeheer, parkeren en slimme straatverlichting. Om bijvoorbeeld het beheer van afval te verbeteren, gebruikt de stad

1018 Europese Commissie, werkdocument van de Commissiediensten, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19 april 2016.

slimme vuilnisbakken. Zij zijn in staat de niveaus van het afval op te volgen om de inzamelroutes te optimaliseren. Als de vuilnisbakken bijna vol zijn, zenden ze een signaal via het mobiele communicatienetwerk naar de softwaretoepassing die door het afvalverwerkingsbedrijf wordt gebruikt. Zo kan het bedrijf de beste route voor afvalinzameling plannen, inzamelingen prioriteren en/of alleen de afvalbakken ophalen die daadwerkelijk dienen te worden geleegd.

10.2.2. Afweging van de voordelen en risico's

De ruime verspreiding en het grote succes van SNS in de laatste tien jaar wijst erop dat ze **aanzienlijke voordelen** bieden. Gerichte reclame bijvoorbeeld (zoals beschreven in het uitgelichte voorbeeld), is een bijzonder innovatieve manier voor ondernemingen om hun doelpubliek te bereiken en hun een meer gerichte markt aan te bieden. Het kan voorts in het belang van de consumenten zijn om advertenties voorgelegd te krijgen die relevanter en interessanter voor hen zijn. Belangrijker nog, socialenetwerkdiensten en sociale media kunnen een positieve impact op de samenleving en op veranderingen hebben. Ze stellen gebruikers in staat om te communiceren, interageren, en groepen en evenementen te organiseren over kwesties die voor hen belangrijk zijn.

Zo wordt van het IoT ook verwacht dat het aanzienlijke voordelen voor de economie met zich zal meebrengen en maakt het deel uit van de EU-strategie voor de ontwikkeling van een digitale eengemaakte markt. Binnen de Europese Unie zal naar verwachting het aantal IoT-verbindingen toenemen tot 6 miljard in 2020. Men verwacht dat deze uitbreiding van de connectiviteit belangrijke economische voordelen met zich zal meebrengen via de ontwikkeling van innoverende diensten en toepassingen, betere gezondheidszorg, een beter inzicht in de behoeften van consumenten en een verhoogde efficiëntie.

Tegelijkertijd, gezien de enorme hoeveelheid persoonsgegevens die door gebruikers van sociale media worden gegenereerd en die vervolgens door de exploitanten van de diensten worden verwerkt, gaat de uitbreiding van SNS gepaard met een **groeiende bezorgdheid** over de wijze waarop privacy en persoonsgegevens kunnen worden beschermd. SNS kunnen een bedreiging vormen voor het recht op privéleven en het recht op vrijheid van meningsuiting. Dergelijke bedreigingen kunnen bestaan uit: "een gebrek aan juridische en procedurele waarborgen bij processen die kunnen leiden tot de uitsluiting van gebruikers; onvoldoende bescherming

van kinderen en jongeren tegen schadelijke inhoud of gedragingen; een gebrek aan respect voor de rechten van derden; een gebrek aan privacyvriendelijke standaardinstellingen; een gebrek aan transparantie over de doeleinden waarvoor persoonsgegevens worden verzameld en verwerkt"[1019]. Het Europees recht inzake gegevensbescherming heeft geprobeerd te antwoorden op de uitdagingen inzake privacy/gegevensbescherming die de sociale media bieden. Beginselen zoals goedkeuring, privacy/gegevensbescherming door ontwerp en door standaardinstellingen, en de rechten van natuurlijke personen zijn bijzonder belangrijk in het kader van sociale media en netwerkdiensten.

In het kader van het IoT brengt de enorme hoeveelheid persoonsgegevens die uit de verschillende onderling verbonden apparaten wordt gegenereerd, risico's met zich mee voor privacy en gegevensbescherming. Hoewel transparantie een belangrijk beginsel is in het Europese recht inzake gegevensbescherming, is het, vanwege de veelheid van verbonden apparaten, niet altijd duidelijk wie in staat is om de door IoT-apparaten verzamelde gegevens te verzamelen, te raadplegen en te gebruiken[1020]. In het kader van het Unierecht en het recht van de Raad van Europa stelt het transparantiebeginsel echter een verplichting vast voor verwerkingsverantwoordelijken om de betrokkenen te informeren over de manier hoe hun gegevens worden gebruikt, in duidelijke en eenvoudige taal. De risico's, regels, waarborgen en rechten met betrekking tot de verwerking van hun persoonsgegevens moeten duidelijk worden gemaakt aan de betrokken personen. Apparaten die verbonden zijn met het IoT en de diverse betrokken verwerkingsactiviteiten en gegevens kunnen ook een uitdaging vormen voor de eis om duidelijke en geïnformeerde toestemming voor gegevensverwerking — wanneer een dergelijke verwerking gebaseerd is op toestemming. Natuurlijke personen hebben vaak een gebrek aan kennis over de technische werking van een dergelijke verwerking en dus over de gevolgen van hun instemming.

Een andere belangrijke bezorgdheid is beveiliging, aangezien verbonden apparaten bijzonder kwetsbaar zijn voor beveiligingsrisico's. Verbonden apparaten hebben verschillende niveaus van beveiliging. Aangezien zij buiten de standaard IT-infrastructuur werken, beschikken zij mogelijk niet over voldoende verwerkingskracht en opslagvermogen voor beveiligingssoftware of om technieken toe te passen zoals

1019 Raad van Europa, Aanbeveling Rec(2012)4 aan de lidstaten inzake de bescherming van de mensenrechten met betrekking tot socialenetwerkdiensten, 4 april 2012.

1020 Europese Toezichthouder voor gegevensbescherming (2017), *Understanding the internet of Things*.

encryptie, pseudonimisering of anonimisering ter bescherming van de persoonlijke gegevens van gebruikers.

Voorbeeld: In Duitsland besloten de regelgevende instanties een verbod op te leggen op speelgoed dat verbonden was met het internet nadat men diepe bezorgdheid had geuit over de impact van het speelgoed op de eerbiediging van het privéleven van kinderen. Regelgevende instanties waren van oordeel dat een via internet verbonden pop, Cayla genaamd, daadwerkelijk een verborgen spionagetoestel vormde. De pop functioneerde door de gesproken vragen van het kind dat ermee speelde, naar een app op een digitaal toestel te sturen, die het vertaalde naar tekst en op het internet zocht naar een antwoord. De app zond vervolgens een antwoord naar de pop, die het antwoord aan het kind vertelde. Door middel van deze pop konden de gesprekken van het kind, evenals die van de volwassenen in de buurt, worden opgenomen en doorgegeven aan de app. Indien de fabrikanten van de pop geen adequate beveiligingsmaatregelen hadden genomen, kon de pop door iedereen worden gebruikt om de gesprekken te beluisteren.

10.2.3. Aangelegenheden die verband houden met gegevensbescherming

Toestemming

In Europa is de verwerking van persoonsgegevens rechtmatig enkel indien dit is toegestaan in het kader van de Europese wetgeving inzake gegevensbescherming. Voor aanbieders van SNS vormt de toestemming van de betrokkenen in het algemeen een rechtmatige basis voor de gegevensverwerking. Toestemming moet uit vrije wil worden gegeven en specifiek, geïnformeerd en eenduidig zijn (zie punt 4.1.1)[1021]. Onder "vrije wil" bedoelt men hoofdzakelijk dat betrokkenen de mogelijkheid moeten hebben om een reële en daadwerkelijke keuze te maken. Toestemming is "specifiek" en "geïnformeerd" wanneer het begrijpelijk is en duidelijk en nauwkeurig verwijst naar het volledige toepassingsgebied, de doelstellingen en de gevolgen van de gegevensverwerking. In het kader van sociale media kan men zich afvragen of de toestemming vrij, specifiek en geïnformeerd is voor alle soorten

1021 Algemene verordening gegevensbescherming, artikelen 4 en 7; Gemoderniseerd Verdrag 108, artikel 5.

verwerkingen die door de exploitant van SNS-netwerken en derde partijen worden uitgevoerd.

Voorbeeld: Om deel te nemen en toegang te krijgen tot een SNS moeten natuurlijke personen vaak instemmen met verschillende soorten verwerkingen van hun persoonsgegevens, vaak zonder de nodige specificaties of alternatieve opties te hebben gekregen. Een voorbeeld hiervan is de noodzaak toe te stemmen met het ontvangen van op surfgedrag gebaseerde reclame om zich bij een SNS te kunnen registreren. Zoals Groep artikel 29 opmerkt in zijn advies over de definitie van toestemming, "gelet op het belang van sommige sociale netwerken, zullen sommige categorieën gebruikers (zoals tieners) de ontvangst van op surfgedrag gebaseerde reclame aanvaarden om het risico te vermijden om gedeeltelijk van sociale interacties uitgesloten te worden. De gebruiker zou vrije en specifieke toestemming moeten kunnen geven om op surfgedrag gebaseerde reclame te ontvangen, ongeacht van zijn toegang tot de socialenetwerkdienst"[1022].

In het kader van de AVG kunnen persoonsgegevens van kinderen jonger dan 16 jaar in beginsel niet worden verwerkt op basis van hun toestemming[1023]. Indien voor de verwerking toestemming nodig is, moet deze worden gegeven door de ouders of de voogd van het kind. Kinderen verdienen specifieke bescherming door het feit dat ze misschien minder op de hoogte zijn van de risico's en gevolgen van de verwerking van gegevens. Dit is zeer belangrijk in het kader van sociale media, aangezien kinderen kwetsbaarder zijn voor sommige negatieve effecten die het gebruik van dergelijke media met zich kan meebrengen, zoals online pesten, online stalken of identiteitsdiefstal.

Beveiliging en privacy/gegevensbescherming door ontwerp en door standaardinstellingen

Inherent aan de verwerking van persoonsgegevens zijn de beveiligingsrisico's, gezien de voortdurende mogelijkheid van een inbreuk op de beveiliging die leidt tot onopzettelijk(e) of onrechtmatig(e) vernietiging, verlies, wijziging, ongeoorloofde toegang of openbaarmaking van de persoonsgegevens die worden verwerkt. In het

1022 Groep artikel 29 (2011), *Advies 15/2011 over de definitie van "toestemming"*, WP 187, 13 juli 2011, blz. 18.

1023 Zie algemene verordening gegevensbescherming, artikel 8. De lidstaten kunnen deze leeftijd via de wetgeving verlagen, op voorwaarde dat dit niet onder de 13 jaar is.

kader van de Europese wetgeving inzake gegevensbescherming moeten verwerkingsverantwoordelijken en verwerkers passende technische en organisatorische maatregelen nemen om onbevoegde inmenging in verwerkingen te voorkomen. Socialenetwerkdiensten die onder het toepassingsgebied van de Europese regels inzake gegevensbescherming vallen, moeten ook voldoen aan deze verplichting.

Door de beginselen van privacy/gegevensbescherming door ontwerp en door standaardinstellingen moeten verwerkingsverantwoordelijken beveiliging in het design van hun producten toevoegen en automatisch passende privacy- en gegevensbeschermingsinstellingen toepassen. Dit betekent dat wanneer een persoon besluit zich aan te sluiten bij een sociaal netwerk, de dienstverlener niet automatisch alle informatie over de nieuwe dienstgebruiker beschikbaar mag maken voor alle gebruikers. Wanneer men zich bij de dienst aansluit, moeten de standaard privacy- en gegevensbeschermingsinstellingen zo zijn ingesteld dat de informatie enkel beschikbaar is voor de contacten die de persoon kiest. De toegang verlenen aan mensen buiten deze lijst is enkel mogelijk nadat de gebruiker manueel de standaard privacy- en gegevensbeschermingsinstellingen heeft veranderd. Dit kan ook invloed hebben in geval van een datalek ondanks de beveiligingsmaatregelen. In dergelijke gevallen moeten de dienstverleners de betrokken gebruikers informeren wanneer de inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkene inhoudt[1024].

Privacy/gegevensbescherming door ontwerp en door standaardinstellingen is van bijzonder belang in de context van SNS, aangezien, naast de risico's op onrechtmatige toegang bij de meeste soorten verwerkingen, het delen van persoonlijke informatie op sociale media bijkomende beveiligingsrisico's met zich meebrengt. Deze zijn vaak het gevolg van een gebrek aan kennis van de persoon over *wie* toegang heeft tot zijn informatie, en hoe deze personen ze mogen gebruiken. Door het wijdverbreide gebruik van sociale media is het aantal incidenten met betrekking tot identiteitsdiefstal en het aantal slachtoffers toegenomen.

Voorbeeld: Identiteitsdiefstal is een fenomeen waarbij een persoon informatie, gegevens of documenten verkrijgt die behoren tot een andere persoon (het slachtoffer), en vervolgens deze informatie gebruikt om zich voor te doen als het slachtoffer om goederen en diensten in diens naam te verkrijgen. Neem Paul bijvoorbeeld, die een account heeft

1024 *Ibid.*, artikel 34.

op een sociale media-website. Paul is leraar en een actief lid van zijn gemeenschap, hij is extravert en niet bijzonder bezorgd over de privacy en de gegevensbeschermingsinstellingen van zijn sociale media-account. Hij heeft een lange lijst van contacten, met inbegrip van mensen die hij niet noodzakelijk persoonlijk kent. Aangezien hij op een grote school werkt en populair is als coach van het voetbalteam van de school, denkt hij dat deze mensen waarschijnlijk ouders of vrienden zijn van de school. Het e-mailadres en de verjaardagsdatum van Paul worden op zijn sociale media-account weergegeven. Daarnaast plaatst Paul regelmatig foto's van zijn hond Toby op zijn account, vergezeld van tekstjes zoals "Ik en Toby tijdens onze ochtendjogging". Paul besefte niet dat "wat is de naam van je huisdier" een van de meest populaire beveiligingsvragen is om zijn e-mail of mobiele telefoon te beschermen. Met de beschikbare informatie op het sociale media-profiel van Paul kan Nick gemakkelijk de accounts van Paul hacken.

Rechten van personen

SNS-aanbieders moeten de rechten van personen respecteren (zie punt 6.1), met inbegrip van het recht om geïnformeerd te worden over het doeleinde van de verwerking en hoe persoonsgegevens kunnen worden gebruikt voor directmarketingdoeleinden. Betrokkenen moeten ook het recht krijgen op toegang tot de persoonsgegevens die ze hebben gegenereerd op de sociale netwerken en de verwijdering ervan op hun verzoek. Zelfs wanneer personen hebben ingestemd met de verwerking van persoonsgegevens en informatie online hebben geüpload, moeten zij kunnen vragen om "te worden vergeten" indien zij niet langer de diensten van het sociale netwerk wensen te ontvangen. Het recht op gegevensportabiliteit stelt gebruikers verder in staat om een kopie van de persoonsgegevens die ze aan de aanbieder van de socialenetwerkdienst hebben gegeven, in een gestructureerd, algemeen gebruikt en machinaal leesbaar formaat te ontvangen en om hun gegevens van de ene verlener van socialenetwerkdiensten naar de andere over te dragen[1025].

Verwerkingsverantwoordelijken

Een moeilijke en vaak terugkomende vraag in het kader van sociale media is de vraag wie de verwerkingsverantwoordelijke is, d.w.z.: wie is de persoon die de

1025 Algemene verordening gegevensbescherming, artikel 21.

verplichting heeft en verantwoordelijkheid is om de regels inzake gegevensbescherming op te volgen. In de Europese wetgeving inzake gegevensbescherming worden verleners van socialenetwerkdiensten beschouwd als verwerkingsverantwoordelijken. Dit is vanzelfsprekend gezien de ruime definitie van "verwerkingsverantwoordelijke" en het feit dat deze dienstverleners het doeleinde van en de middelen voor de verwerking van persoonsgegevens die door personen worden gedeeld, bepalen. In het kader van het Unierecht moeten verwerkingsverantwoordelijken, indien zij diensten aanbieden aan betrokkenen in de EU, voldoen aan de bepalingen van de AVG, zelfs indien zijn niet in de EU gevestigd zijn.

Kunnen gebruikers van socialenetwerkdiensten echter ook als verwerkingsverantwoordelijken worden beschouwd? Wanneer personen persoonsgegevens verwerken "tijdens een zuiver persoonlijke of huishoudelijke activiteit", zijn de regels inzake gegevensbescherming niet van toepassing. Dit staat in de Europese wetgeving inzake gegevensbescherming bekend als "huishoudelijke exceptie". In sommige gevallen valt een gebruiker van een dienst voor sociale netwerken echter niet onder de huishoudelijke exceptie.

Gebruikers delen hun persoonlijke informatie vrijwillig online. Gedeelde informatie bevat echter vaak persoonlijke informatie van andere personen.

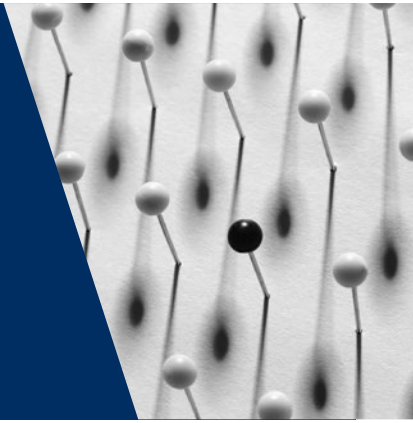
Voorbeeld: Paul heeft een account op een erg populair sociaal netwerk. Paul wil graag acteur worden en gebruikt zijn account om foto's, video's en berichten te plaatsen die zijn passie voor kunst uitleggen. Populariteit is belangrijk voor zijn toekomst; hij heeft dus besloten dat zijn profiel toegankelijk moet zijn, niet enkel voor zijn beperkte lijst van contacten, maar voor alle internetgebruikers, ongeacht of ze lid zijn van het netwerk of niet. Kan Paul foto's en video's van hem met zijn vriendin Sarah op zijn account plaatsen zonder haar toestemming? Als leerkracht van een lagere school probeert Sarah haar privéleven gescheiden te houden van haar werkgever, leerlingen en hun ouders. Nu kan men zich voorstellen dat Sarah, die geen sociale netwerken gebruikt, van hun gemeenschappelijke vriend Nick te weten kan komen dat een foto van haar en Paul op een feestje online werd gezet. In dat geval valt de gegevensverwerking van Paul niet onder het Unierecht, aangezien deze valt onder de "huishoudelijke exceptie".

Het blijft evenwel van belang om zich ervan bewust te zijn dat het uploaden van informatie over andere personen zonder hun toestemming een inbreuk kan

vormen op de privacy en het recht op gegevensbescherming van deze personen. Zelfs wanneer de huishoudelijke exceptie geldt — indien bijvoorbeeld een gebruiker een profiel heeft dat alleen openbaar wordt gemaakt aan een lijst van door hem/haar gekozen contacten — kan de publicatie van persoonlijke informatie over anderen de gebruiker nog steeds aansprakelijk maken. Hoewel de regels inzake gegevensbescherming niet van toepassing zijn in geval van een huishoudelijke exceptie, kan men nog steeds aansprakelijk worden gesteld door de toepassing van andere nationale voorschriften, zoals smaad of inbreuk op persoonlijkheid. Ten slotte, enkel gebruikers van SNS worden beschermd door de huishoudelijke exceptie: verwerkingsverantwoordelijken en verwerkers die de mogelijkheid geven voor een dergelijke privéverwerking, vallen onder de EU-wetgeving inzake gegevensbescherming[1026].

Met de hervorming van de richtlijn betreffende privacy en elektronische communicatie zouden de voorschriften inzake de bescherming van persoonsgegevens, privacy en beveiliging die van toepassing zijn op aanbieders van telecommunicatiediensten in het kader van de huidige wetgeving, ook van toepassing zijn op de communicatie van machine tot machine en elektronische communicatiediensten, met inbegrip van, bijvoorbeeld, over-the-top-diensten.

1026 *Ibid.*, overweging 18.



Aanbevolen literatuur

Hoofdstuk 1

Araceli Mangas, M., *Carta de los derechos fundamentales de la Unión Europea*, Fundación BBVA, Bilbao, (ed.) (2008).

Berka, W., *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Manzsche Verlags- und Universitätsbuchhandlung, Wenen, 2012.

Docksey, C., "Four fundamental rights: finding the balance", *International Data Privacy Law*, Vol. 6, nr. 3, blz. 195-209.

González Fuster, G., en Gellert, G., "The fundamental right of data protection in the European Union: in search of an uncharted right", *International Review of Law, Computers and Technology*, Vol. 26 (1), 2012, blz. 73-82.

Gutwirth, S., Poullet, Y., Hert, P. de, Terwangne, C. de, en Nouwt, S. (eds.), *Reinventing Data Protection*, Springer, 2009.

Hijmans, H., *The European Union as Guardian of Internet Privacy — the Story of Art 16 TFEU*, Springer, 2016.

Hustinx, P., "EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation", 2016.

Kranenborg, H., "Google and the Right to be Forgotten", *European Data Protection Law Review*, Vol. 1, nr. 1, 2015, blz. 70-79.

Lynskey, O., "Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, Vol. 63, nr. 3, 2014, blz. 569-597.

Lynskey, O., *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015.

Kokott, J., en Sobotta, C., "The distinction between privacy and data protection in the case law of the CJEU and the ECtHR", *International Data Privacy Law*, Vol. 3, nr. 4, 2013, blz. 222–228.

EDRi, *An introduction to data protection*, Brussel.

Frowein, J., en Peukert, W., *Europäische Menschenrechtskonvention*, N. P. Engel Verlag, Berlijn, 2009.

Grabenwarter, C., en Pabel, K., *Europäische Menschenrechtskonvention*, C. H. Beck, München, 2012.

Harris, D., O'Boyle, M., Warbrick, C., en Bates, E., *Law of the European Convention on Human Rights*, Oxford University Press, Oxford, 2009.

Jarass, H., *Charta der Grundrechte der Europäischen Union*, C. H. Beck, München, 2010.

Mayer, J., *Charta der Grundrechte der Europäischen Union*, Nomos, Baden-Baden, 2011.

Mowbray, A., *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford University Press, Oxford, 2012.

Nowak, M., Januszewski, K., en Hofstätter, T., *All human rights for all — Vienna manual on human rights*, Neuer Wissenschaftlicher Verlag, intersentia N. V., Antwerpen, 2012.

Picharel, C., en Coutron, L., *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Emile Bruylant, Brussel, 2010.

Simitis, S., "Die EU-Datenschutz-Richtlinie — Stillstand oder Anreiz?", *Neue Juristische Wochenschrift*, nr 5, 1997, blz. 281-288.

Warren, S., en Brandeis, L., "The right to privacy", *Harvard Law Review,* Vol. 4, nr. 5, 1890, blz. 193-220.

White, R., en Ovey, C., *The European Convention on Human Rights*, Oxford University Press, Oxford, 2010.

Hoofdstuk 2

Acquisty, A., en Gross, R., "Predicting Social Security numbers from public data", *Proceedings of the National Academy of Science*, 7 juli 2009.

Carey, P., *Data protection: A practical guide to UK and EU law*, Oxford University Press, Oxford, 2009.

Delgado, L., *Vida privada y protección de datos en la Unión Europea*, Dykinson S. L., Madrid, 2008.

De Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., en Blondel V. D., "Unique in the Crowd: the Privacy Bounds of Human Mobility", *Nature Scientific Reports*, Vol. 3, 2013.

Desgens-Pasanau, G., *La protection des données à caractère personnel*, LexisNexis, Parijs, 2012.

Di Martino, A., *Datenschutz im europäischen Recht*, Nomos, Baden-Baden, 2005.

González Fuster, G., *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer, 2014.

Morgan, R., en Boardman, R., *Data protection strategy: Implementing data protection compliance*, Sweet & Maxwell, Londen, 2012.

Ohm, P., "Broken promises of privacy: Responding to the surprising failure of anonymization", *UCLA Law Review*, Vol. 57, nr. 6, 2010, blz. 1701-1777.

Samarati, P., en Sweeney, L., "Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression", Technical Report SRI-CSL-98-04, 1998.

Sweeney, L., "K-Anonimiteit: A Model for Protecting Privacy", *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, Vol. 10, nr. 5, 2002, blz. 557-570.

Tinnefeld, M., Buchner, B., en Petri, T., *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Oldenbourg Wissenschaftsverlag, München, 2012.

United Kingdom Information Commissioner's Office, *Anonymisation: managing data protection risk. Praktijkrichtlijn, 2012.*

Hoofdstukken 3 tot en met 6

Brühann, U., "Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" in: Grabitz, E., Hilf, M., en Nettesheim, M., (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, C. H. Beck, München, 2012.

Conde Ortiz, C., *La protección de datos personales*, Dykinson, Cadiz, 2008.

Coudray, L., *La protection des données personnelles dans l'Union européenne*, Éditions universitaires européennes, Saarbrucken, 2010.

Curren, L., en Kaye, J., "Revoking consent: a 'blind spot' in data protection law?", *Computer Law & Security Review*, Vol. 26, nr. 3, 2010, blz. 273-283.

Dammann, U., en Simitis, S., *EG-Datenschutzrichtlinie*, Nomos, Baden-Baden, 1997.

Hert, P. de, en Papakonstantinou, V., "The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, Vol. 22, nr. 6, 2012, blz. 1-5.

Hert, P. de, en Papakonstantinou, V., "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, Vol. 28, nr. 2, 2012, blz. 130-142.

Feretti, F., "A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously", *European Review of Private Law*, Vol. 20, nr. 2, 2012, blz. 473-506.

FRA (Bureau van de Europese Unie voor de grondrechten), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Bureau voor publicaties van de Europese Unie (Publicatiebureau), Luxemburg, 2010.

FRA, *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conferentie-editie), FRA, Wenen, 2010.

FRA, *Access to justice in Europe: an overview of challenges and opportunities*, Bureau voor publicaties van de Europese Unie, Luxemburg, 2011.

Irish Health Information and Quality Authority, Guidance on Privacy Impact Assessment in Health and Social Care, 2010.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I., en Saxby, S., "30 years on — The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Review*, Vol. 27, nr. 3, 2011, blz. 223-231.

Simitis, S., *Bundesdatenschutzgesetz*, Nomos, Baden-Baden, 2011.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*.

Hoofdstuk 7

Europese Toezichthouder voor gegevensbescherming, Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies, 2014.

Gutwirth, S., Poullet, Y., Hert, P. de, Terwangne, C. de, en Nouwt, S., *Reinventing data protection?*, Springer, Berlijn, 2009.

Kuner, C., *European data protection law*, Oxford University Press, Oxford, 2007.

Kuner, C., *Transborder data flow regulation and data privacy law*, Oxford University Press, Oxford, 2013.

Groep artikel 29 (2005), *Werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995*.

Hoofdstuk 8

Blasi Casagran, C., *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, Routledge, Londen, 2016.

Boehm, F., *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Springer, Berlijn, 2012.

Europol, *Data Protection at Europol*, Bureau voor publicaties van de Europese Unie, Luxemburg, 2012.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Eurojust, Den Haag.

Hert, P. de, en Papakonstantinou, V., "The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, Vol. 22, nr. 6, 2012, blz. 1-5.

Drewer, D., en Ellermann, J., "Europol's data protection framework as an asset in the fight against cybercrime", *ERA Forum*, Vol. 13, nr. 3, 2012, blz. 381-395.

Gutiérrez Zarza, A., *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Springer, Berlijn, 2015.

Gutwirth, S., Poullet, Y., en Hert, P. de, *Data protection in a profiled world*, Springer, Dordrecht, 2010.

Gutwirth, S., Poullet, Y., Hert, P. de, en Leenes, R., *Computers, privacy and data protection: An element of choice*, Springer, Dordrecht, 2011.

Konstadinides, T., "Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, Vol. 36, nr. 5, 2011, blz. 722-776.

Santos Vara, J., *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers, 2013/2.

Hoofdstuk 9

Büllesbach, A., Gijrath, S., Poullet, Y., en Hacon, R., *Concise European IT law*, Kluwer Law International, Amsterdam, 2010.

Gutwirth, S., Leenes, R., Hert, P. de, en Poullet, Y., *European data protection: In good health?*, Springer, Dordrecht, 2012.

Gutwirth, S., Poullet, Y., en Hert, P. de, *Data protection in a profiled world*, Springer, Dordrecht, 2010.

Gutwirth, S., Poullet, Y., Hert, P. de, en Leenes, R., *Computers, privacy and data protection: An element of choice*, Springer, Dordrecht, 2011.

Konstadinides, T., "Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, Vol. 36, nr. 5, 2011, blz. 722-776.

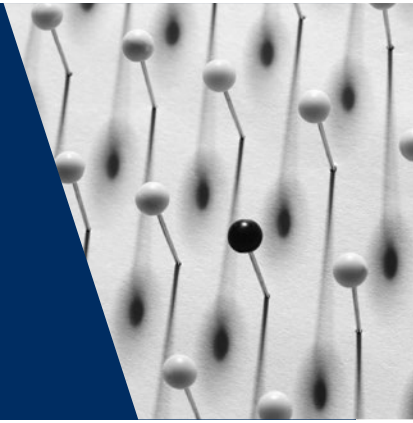
Rosemary, J., en Hamilton, A., *Data protection law and practice*, Sweet & Maxwell, Londen, 2012.

Hoofdstuk 10

El Emam, K., en Álvarez, C., "A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", *International Data Privacy Law*, Vol. 5, nr. 1, 2015, blz. 73-87.

Mayer-Schönberger, V., en Cate, F., "Notice and consent in a world of Big Data", *International Data Privacy Law*, Vol. 3, nr. 2, 2013, blz. 67-73.

Rubinstein, I., "Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, Vol. 3, nr. 2, 2013, blz. 74-87.



Jurisprudentie

Geselecteerde jurisprudentie van het Europees Hof voor de Rechten van de Mens

Toegang tot persoonsgegevens
Gaskin/Verenigd Koninkrijk, nr. 10454/83, 7 juli 1989
Godelli/Italië, nr. 33783/09, 25 september 2012
K.H. e.a./Slowakije, nr. 32881/04, 28 april 2009
Leander/Zweden, nr. 9248/81, 26 maart 1987
M.K./Frankrijk, nr. 19522/09, 18 april 2013
Odièvre/Frankrijk [GK], nr. 42326/98, 13 februari 2003

Afwegen van gegevensbescherming met de vrijheid van meningsuiting en het recht op informatie
Axel Springer AG/Duitsland [Grote kamer], nr. 39954/08, 7 februari 2012
Axen/Duitsland, nr. 53495/09, 19 februari 2015
Couderc en Hachette Filipacchi Associés/Frankrijk [Grote kamer], nr. 40454/07, 10 november 2015
Magyar Helsinki Bizottság/Hongarije [Grote kamer], nr. 18030/11, 8 november 2016
Athanassoglou e.a./Zwitserland, nr. 10737/84, 24 mei 1988
Vereinigung bildender Künstler/Oostenrijk, nr. 68354/01, 25 januari 2007
Von Hannover/Duitsland (nr. 2) [Grote kamer], nrs. 40660/08 en 60641/08, 7 februari 2012
Satakunnan Markkinapörssi Oy en Satamedia Oy/Finland, [Grote kamer], nr. 931/13, 27 juni 2017

Afwegen van gegevensbescherming met de vrijheid van godsdienst
Sinan Işık/Turkije, nr. 21924/05, 2 februari 2010

Uitdagingen in de bescherming van gegevens op internet
K.U.Finland, nr. 2872/02, 2 december 2008

Toestemming van de betrokkene
Elberte/Letland, nr. 61243/08, 13 januari 2015
Sinan Işık/Turkije, nr. 21924/05, 2 februari 2010
Y./Turkije, nr. 648/10, 17 februari 2015

Correspondentie
Amann/Zwitserland [Grote kamer], nr. 27798/95, donderdag 16 februari 2000
Association for European Integration and Human Rights and Ekimdzhiev/Bulgarije, nr. 62540/00, 28 juni 2007
Bernh Larsen Holding AS e.a./Noorwegen, nr. 24117/08, 14 maart 2013
Cemalettin Canli/Turkije, nr. 22427/04, 18 november 2008
D.L./Bulgarije, nr. 7472/14, 19 mei 2016
Dalea/Frankrijk, nr. 964/07, 2 februari 2010
Gaskin/Verenigd Koninkrijk, nr. 10454/83, 7 juli 1989
Haralambie/Roemenië, nr. 21737/03, 27 oktober 2009
Khelili/Zwitserland, nr. 16188/07, 18 oktober 2011
Leander/Zweden, nr. 9248/81, 26 maart 1987
Malone/Verenigd Koninkrijk, nr. 8691/79, 2 augustus 1984
Rotaru/Roemenië [Grote kamer], nr. 28341/95, 4 mei 2000
S. en Marper/Verenigd Koninkrijk [Grote kamer], nrs. 30562/04 en 30566/04, 4 december 2008
Shimovolos/Rusland, nr. 30194/09, 21 juni 2011
Silver e.a./Verenigd Koninkrijk, nrs. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 maart 1983
The Sunday Times/Verenigd Koninkrijk, nr. 6538/74, 26 april 1979

Strafrechtelijke databanken
Aycaguer/Frankrijk, nr. 8806/12, 22 juni 2017
B.B./Frankrijk, nr. 5335/06, 17 december 2009
Brunet/Frankrijk, nr. 21010/10, 18 september 2014
M.K./Frankrijk, nr. 19522/09, 18 april 2013
M.M./Verenigd Koninkrijk, nr. 24029/07, 13 november 2012

Gegevensbeveiliging
Haralambie/Roemenië, nr. 21737/03, 27 oktober 2009
K.H. e.a./Slowakije, nr. 32881/04, 28 april 2009

Dna-databanken
S. en Marper/Verenigd Koninkrijk [Grote kamer], nrs. 30562/04 en 30566/04, 4 december 2008

Gps-gegevens
Uzun/Duitsland, nr. 35623/05, 2 september 2010

Gezondheidsgegevens
Avilkina e.a./Rusland, nr. 1585/09, 6 juni 2013
Biriuk/Litouwen, nr. 23373/03, 25 november 2008
I./Finland, nr. 20511/03, 17 juli 2008
L.H./Letland, nr. 52019/07, 29 april 2014
L.L./Frankrijk, nr. 7508/02, 10 oktober 2006
M.S./Zweden, nr. 20837/92, 27 augustus 1997
Szuluk/Verenigd Koninkrijk, nr. 36936/05, 2 juni 2009
Y./Turkije, nr. 648/10, 17 februari 2015
Z./Finland, nr. 22009/93, 25 februari 1997

Identiteit
Ciubotaru/Moldavië, nr. 27138/04, 27 april 2010
Godelli/Italië, nr. 33783/09, 25 september 2012
Odièvre/Frankrijk [Grote kamer], nr. 42326/98, 13 februari 2003

Informatie met betrekking tot beroepsactiviteiten
G.S.B./Zwitserland, nr. 28601/11, 22 december 2015
M.N. e.a./San Marino, nr 28005/12, 7 juli 2015
Michaud/Frankrijk, nr. 12323/11, 6 december 2012
Niemietz/Duitsland, nr. 13710/88, 16 december 1992

Onderscheppen van communicatie
Amann/Zwitserland [Grote kamer], nr. 27798/95, 16 februari 2000
Brito Ferrinho Bexiga Villa-Nova/Portugal, nr. 69436/10, 1 december 2015
Copland/Verenigd Koninkrijk, nr. 62617/00, 3 april 2007
Halford/Verenigd Koninkrijk, nr. 20605/92, 25 juni 1997
Iordachi e.a./Moldavië, nr. 25198/02, 10 februari 2009

Kopp/Zwitserland, nr. 23224/94, 25 maart 1998
Liberty e.a./Verenigd Koninkrijk, nr. 58243/00, 1 juli 2008
Malone/Verenigd Koninkrijk, nr. 8691/79, 2 augustus 1984
Mustafa Sezgin Tanrıkulu/Turkije, nr. 27473/06, 18 juli 2017
Pruteanu/Roemenië, nr. 30181/05, 3 februari 2015
Szuluk/Verenigd Koninkrijk, nr. 36936/05, 2 juni 2009

Verplichtingen voor plichthouders
B.B./Frankrijk, nr. 5335/06, 17 december 2009
I./Finland, nr. 20511/03, 17 juli 2008
Mosley/Verenigd Koninkrijk, nr. 48009/08, 10 mei 2011

Persoonsgegevens
Amann/Zwitserland [Grote kamer], nr. 27798/95, donderdag 16 februari 2000
Uzun/Duitsland, nr. 35623/05, 2010
Bernh Larsen Holding AS e.a./Noorwegen, nr. 24117/08, 14 maart 2013

Foto's
Sciacca/Italië, nr. 50774/99, 11 januari 2005
Von Hannover/Duitsland, nr. 59320/00, 24 juni 2004

Recht om te worden vergeten
Segerstedt-Wiberg e.a./Zweden, nr. 62332/00, 6 juni 2006
Satakunnan Markkinapörssi Oy en Satamedia Oy/Finland, [Grote kamer], nr. 931/13, 27 juni 2017

Recht van bezwaar
Leander/Zweden, nr. 9248/81, 26 maart 1987
M.S./Zweden, nr. 20837/92, 27 augustus 1997
Mosley/Verenigd Koninkrijk, nr. 48009/08, 10 mei 2011
Rotaru/Roemenië [Grote kamer], nr. 28341/95, 4 mei 2000
Sinan Işık/Turkije, nr. 21924/05, 2 februari 2010

Categorieën gevoelige gegevens
Brunet/Frankrijk, nr. 21010/10, 18 september 2014
I./Finland, nr. 20511/03, 17 juli 2008
Michaud/Frankrijk, nr. 12323/11, 6 december 2012
S. en Marper/Verenigd Koninkrijk [Grote kamer], nrs. 30562/04 en 30566/04, 4 december 2008

Toezicht en handhaving (taken van verschillende actoren, waaronder toezichthoudende autoriteiten)
I./Finland, nr. 20511/03, 17 juli 2008
K.U./Finland, nr. 2872/02, 2 december 2008
Von Hannover/Duitsland, nr. 59320/00, 24 juni 2004
Von Hannover/Duitsland (nr. 2) [Grote kamer], nrs. 40660/08 en 60641/08, 7 februari 2012

Surveillancemethoden
A./Verenigd Koninkrijk, nr. 48539/99, 5 november 2002
Association for European Integration and Human Rights and Ekimdzhiev/Bulgarije, nr. 62540/00, 28 juni 2007
Bărbulescu/Roemenië [Grote kamer], nr. 61496/08, 5 september 2017
D.L./Bulgarije, nr. 7472/14, 19 mei 2016
Dragojević/Kroatië, nr. 68955/11, 15 januari 2015
Karabeyoğlu/Turkije, nr. 30083/10, 7 juni 2016
Klass e.a./Duitsland, nr. 5029/71, 6 september 1978
Rotaru/Roemenië [Grote kamer], nr. 28341/95, 4 mei 2000
Szabó en Vissy/Hongarije, nr. 37138/14, 12 januari 2016
Taylor-Sabori/Verenigd Koninkrijk, nr. 47114/99, 22 oktober 2002
Uzun/Duitsland, nr. 35623/05, 2 september 2010
Versini-Campinchi en Crasnianski/Frankrijk, nr. 49176/11, 16 juni 2016
Vetter/Frankrijk, nr. 59842/00, 31 mei 2005
Vukota-Bojić/Zwitserland, nr. 61838/10, 18 oktober 2016
Roman Zakharov/Rusland [Grote kamer], nr. 47143/06, 4 december 2015

Videobewaking
Köpke/Duitsland, nr. 420/07, 5 oktober 2010
Peck/Verenigd Koninkrijk, nr. 44647/98, 28 januari 2003

Voice samples
Wisse/Frankrijk, nr. 71611/01, 20 december 2005
P.G. en J.H./Verenigd Koninkrijk, nr. 44787/98, 25 september 2001

Geselecteerde jurisprudentie van het Hof van Justitie van de Europese Unie

Jurisprudentie met betrekking tot de richtlijn gegevensbescherming

Zaak C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA 'Rīgas satiksme'*, 4 mei 2017

[Beginsel van de wettige verwerking: gerechtvaardigd belang van een derde partij]

Zaak C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 maart 2017

[Het recht op het wissen van persoonsgegevens; het recht op bezwaar tegen verwerking]

Gevoegde zaken C-203/15 en C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen* en *Secretary of State for the Home Department/Tom Watson e.a.* [Grote kamer], 21 december 2016

[De vertrouwelijkheid van elektronische communicatie; aanbieders van elektronische-communicatiediensten; verplichting met betrekking tot het algemeen en ongedifferentieerd bewaren van verkeers- en locatiegegevens; geen voorafgaand onderzoek door een rechterlijke of onafhankelijke administratieve instantie; Handvest van de grondrechten van de Europese Unie; verenigbaarheid met het Unierecht]

Zaak C-582/14, Patrick Breyer/Bundesrepublik Deutschland, 19 oktober 2016

[Definitie van "persoonsgegevens"; Internetprotocol-adressen; opslag van gegevens door een aanbieder van online mediadiensten; nationale wetgeving die niet toestaat dat rekening wordt gehouden met het gerechtvaardigde belang dat door de verwerkingsverantwoordelijke wordt nagestreefd]

Zaak C-362/14, *Maximillian Schrems/Data Protection Commissioner* [Grote kamer], 6 oktober 2015

[Het beginsel van de wettige verwerking; grondrechten; de nietigheid van het veiligehavenbesluit; de bevoegdheden van de onafhankelijke toezichthoudende autoriteit]

Zaak C-230/14, *Weltimmo s. r. o./Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 oktober 2015

[De bevoegdheden van de nationale toezichthoudende autoriteiten]

Zaak C-201/14, *Smaranda Bara e.a./Casa Națională de Asigurări de Sănătate e.a.*, 1 oktober 2015

[Het recht om te worden geïnformeerd over de verwerking van persoonsgegevens]

Zaak C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 december 2014

[Het concept van "gegevensverwerking" en "verwerkingsverantwoordelijke"]

Zaak C-473/12, *Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert e.a.*, 7 november 2013

[Het recht om te worden geïnformeerd over de verwerking van persoonsgegevens]

Zaak T-462/12 R, *Pilkington Group Ltd/Europese Commissie*, Beschikking van de president van het Gerecht, 11 maart 2013

Zaak C-342/12, *Worten — Equipamentos para o Lar SA/Autoridade para als Condições de Trabalho (ACT)*, 30 mei 2013

[Het Concept "persoonsgegevens"; verslag van de arbeidstijd; beginselen met betrekking tot de kwaliteit van gegevens en criteria voor het rechtmatig maken van de gegevensverwerking; toegang tot de nationale autoriteit die verantwoordelijk is voor het toezicht op de arbeidsomstandigheden; de plicht van de werkgever om het register van de werktijden ter beschikking te stellen, zodat het onmiddellijk kan worden geraadpleegd]

Gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e.a.* en Kärntner Landesregierung e.a. [Grote kamer], 8 april 2014

[Schending van het primaire recht van de EU door de richtlijn gegevensbewaring; rechtmatige verwerking; doelbinding en beperking van de opslag]

Zaak C-288/12, *Europese Commissie/Hongarije* [Grote kamer], 8 april 2014

[Rechtmatigheid van de ontzetting uit zijn ambt van de nationale toezichthouder gegevensbescherming]

Gevoegde zaken C-141/12 en C-372/12, *Y.S./Minister voor Immigratie, Integratie en Asiel* en *Minister voor Immigratie, Integratie en Asiel/M en S*, 17 juli 2014

[Het toepassingsgebied van het recht op toegang van een betrokkene; bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens; het concept van "persoonsgegevens"; gegevens over de aanvrager van een

verblijfsvergunning en een juridische analyse in een administratief document voorafgaand aan het besluit; Handvest van de grondrechten van de Europese Unie]

Zaak C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [Grote kamer], 13 mei 2014

[Verplichtingen van de aanbieders van zoekmachines om af te zien, op verzoek van de betrokkene, van het tonen van persoonsgegevens in de zoekresultaten; toepasbaarheid van de richtlijn gegevensbescherming; begrip "gegevensverwerking"; betekenis van "verwerkingsverantwoordelijken"; het afwegen van gegevensbescherming met de vrijheid van meningsuiting; het recht om te worden vergeten]

Zaak C-614/10, *Europese Commissie/Republiek Oostenrijk* [Grote kamer], 16 oktober 2012

[Onafhankelijkheid van een nationale toezichthoudende autoriteit]

Gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 november 2011

[Correcte tenuitvoerlegging van artikel 7, onder f), van de richtlijn gegevensbescherming — "gerechtvaardigd belang van anderen" — in het nationale recht]

Zaak C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*, 16 februari 2012

[Verplichting van aanbieders van sociale netwerken om onrechtmatig gebruik van muzikale en audiovisuele werken door gebruikers van hun netwerk te voorkomen]

Zaak C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 november 2011

[Informatiemaatschappij; auteursrecht; internet; "peer-to-peer"-software; aanbieders van internetdiensten; installatie van een systeem voor het filtreren van elektronische communicatie teneinde file sharing die een inbreuk maakt op het auteursrecht, te verhinderen; geen algemene verplichting om doorgegeven informatie te controleren]

Zaak C-543/09, *Deutsche Telekom AG/Bondsrepubliek Duitsland*, 5 mei 2011

[Noodzaak van hernieuwde toestemming]

Gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert/Land Hessen* [Grote kamer], 9 november 2010
[Begrip "persoonsgegevens"; Evenredigheid van de wettelijke verplichting om persoonsgegevens van de begunstigden van bepaalde EU-landbouwfondsen te publiceren]

Zaak C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, 7 mei 2009
[Recht op toegang van de betrokkene]

Zaak C-518/07, *Europese Commissie/Bondsrepubliek Duitsland* [Grote kamer], 9 maart 2010
[Onafhankelijkheid van een nationale toezichthoudende autoriteit]

Zaak C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy en Satamedia Oy* [Grote kamer], 16 december 2008
[Begrip "journalistieke activiteiten" in de zin van artikel 9 van de richtlijn gegevensbescherming]

Zaak C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [Grote kamer], 16 december 2008
[Rechtmatigheid van het houden van gegevens over onderdanen van derde landen in een statistisch register]

Zaak C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [Grote kamer], 29 januari 2008
[Begrip "persoonsgegevens"; verplichting van aanbieders van toegang tot internet om de identiteit van gebruikers van KaZaA-programma's voor de uitwisseling van bestanden mee te delen aan de vereniging voor de bescherming van intellectuele eigendomsrechten]

Zaak C-101/01, *Strafzaak tegen Bodil Lindqvist*, 6 november 2003
[Bijzondere categorieën persoonsgegevens]

Gevoegde zaken C-465/00, C-138/01 en C-139/01, *Rechnungshof/Österreichischer Rundfunk e.a.* en *Christa Neukomm en Jospeh Lauermann/Österreichischer Rundfunk*, 20 mei 2003

[Evenredigheid van wettelijke verplichtingen om persoonsgegevens over de salarissen van werknemers van bepaalde categorieën van aan de publieke sector gerelateerde instellingen te publiceren]

Zaak C-434/16, *Peter Nowak/Data Protection Commissioner*, Conclusie van advocaat-generaal Kokott, 20 juli 2017

[Begrip "persoonsgegevens"; toegang tot zijn eigen examentekst; verbeteringen corrector]

Zaak C-291/12, *Michael Schwarz/Stadt Bochum*, 17 oktober 2013

[Verzoek om een prejudiciële beslissing; ruimte van vrijheid, veiligheid en rechtvaardigheid; biometrisch paspoort; vingerafdrukken; rechtsgrondslag; evenredigheid]

Jurisprudentie met betrekking tot Richtlijn (EU) 2016/681

Advies 1/15 van het Hof (Grote Kamer), 26 juli 2017

[Rechtsgrondslag, ontwerpovereenkomst tussen Canada en de Europese Unie betreffende de overdracht en verwerking van persoonsgegevens van passagiers; de verenigbaarheid van de ontwerpovereenkomst met artikel 16 VWEU en de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie]

Jurisprudentie met betrekking tot de verordening gegevensbescherming EU-instellingen

Zaak C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/ Europese Autoriteit voor voedselveiligheid (EFSA), Europese Commissie,* 16 juli 2015

[Toegang tot documenten]

Zaak C-28/08 P, *Europese Commissie/The Bavarian Lager Co. Ltd.* [Grote kamer], 29 juni 2010

[Toegang tot documenten]

Jurisprudentie met betrekking tot Richtlijn 2002/58/EG

Zaak C-536/15, *Tele2 (Netherlands) BV e.a./Autoriteit Consument en Markt (ACM)*, 15 maart 2017

[Beginsel van non-discriminatie, de terbeschikkingstelling van de persoonsgegevens van abonnees met het oog op de verstrekking van openbare telefooninlichtingendiensten en telefoongidsen; toestemming van de abonnee; onderscheid op basis van de lidstaat waar de publiek beschikbare telefooninlichtingendiensten en telefoongidsen worden verstrekt]

Gevoegde zaken C-203/15 en C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen* en *Secretary of State for the Home Department/Tom Watson e.a.* [Grote kamer], 21 december 2016

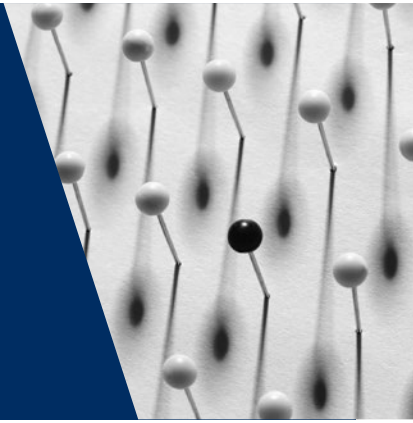
[De vertrouwelijkheid van elektronische communicatie; aanbieders van elektronische-communicatiediensten; verplichting met betrekking tot het algemeen en ongedifferentieerd bewaren van verkeers- en locatiegegevens; geen voorafgaand onderzoek door een rechterlijke of onafhankelijke administratieve instantie; Handvest van de grondrechten van de Europese Unie; verenigbaarheid met het Unierecht]

Zaak C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 november 2011

[Informatiemaatschappij; auteursrecht; internet; "peer-to-peer"-software; aanbieders van internetdiensten; installatie van een systeem voor het filtreren van elektronische communicatie ter verhindering van file sharing die een inbreuk op het auteursrecht vormt; geen algemene verplichting om doorgegeven informatie te controleren]

Zaak C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB/Perfect Communication Sweden AB*, 19 april 2012

[Het auteursrecht en naburige rechten; de verwerking van gegevens door het internet; schending van een uitsluitend recht; luisterboeken ter beschikking gesteld door middel van een FTP-server via internet door internetprovider verstrekt IP-adres; tot internetprovider gericht bevel om naam en adres van gebruiker van IP-adres te verstrekken]



Index

Jurisprudentie van het Hof van Justitie van de Europese Unie

Jurisprudentie van het Europees Hof voor de Rechten van de Mens

Jurisprudentie van nationale rechtbanken

Op internet is zeer veel informatie beschikbaar over het Bureau van de Europese Unie voor de grondrechten. Deze is te vinden op de FRA-website fra.europa.eu.

Nadere informatie over de jurisprudentie van het Europees Hof voor de Rechten van de Mens is beschikbaar op de website van het Hof: echr.coe.int. Het HUDOC-zoekportaal geeft toegang tot de arresten en beschikkingen in het Engels en/of Frans, vertalingen in bijkomende talen, juridische samenvattingen, persmededelingen en andere informatie over de werkzaamheden van het Hof.

Hoe de publicaties van de Raad van Europa verkrijgen

Het Publicatiebureau van de Raad van Europa ("Council of Europe Publishing") produceert werken over alle werkterreinen van de organisatie, waaronder rechten van de mens, rechtswetenschappen, gezondheid, ethiek, sociale aangelegenheden, milieu, onderwijs, cultuur, sport, jeugd en architectonisch erfgoed. Boeken en elektronische publicaties uit de uitgebreide catalogus kunnen online worden besteld (http://book.coe.int).

Een virtuele leeskamer biedt gebruikers de mogelijkheid om kosteloos uittreksels van de belangrijkste recentelijk gepubliceerde werken of de volledige teksten van bepaalde officiële documenten te raadplegen.

Informatie over en de volledige tekst van de verdragen van de Raad van Europa zijn te vinden op de website van het Bureau van de verdragen van de Raad van Europa: http://conventions.coe.int

De EU contacteren

Persoonlijk

Over de gehele Europese Unie zijn er honderden Europe Direct-voorlichtingscentra. Het adres van het dichtstbijzijnde centrum is te vinden op: https://europa.eu/european-union/contact_nl

Per telefoon of e-mail

Europe Direct helpt u antwoord te vinden op uw vragen over de Europese Unie. De dienst is bereikbaar via:

— het gratis nummer: 00 800 6 7 8 9 10 11 (bepaalde operatoren rekenen mogelijk kosten voor deze gesprekken),
— op het volgende telefoonnummer: +32 22999696 of
— per e-mail: https://europa.eu/european-union/contact_nl

Waar vindt u informatie over de EU?

Online

Informatie over de Europese Unie in alle officiële talen van de EU is beschikbaar op de Europa-website op: https://europa.eu/european-union/index_nl

EU-publicaties

U kunt publicaties van de EU downloaden of bestellen bij EU Bookshop op: https://op.europa.eu/nl/publications (sommige zijn gratis, andere niet). Als u meerdere exemplaren van gratis publicaties wenst, neem dan contact op met Europe Direct of uw plaatselijke informatiecentrum (zie https://europa.eu/european-union/contact_nl).

EU-wetgeving en aanverwante documenten

Toegang tot juridische informatie van de EU, waaronder alle EU-wetgeving sinds 1951 in alle officiële talen, krijgt u op EUR-Lex op: http://eur-lex.europa.eu

Open data van de EU

Het opendataportaal van de EU (http://data.europa.eu/euodp/nl) biedt toegang tot datasets uit de EU. Deze gegevens kunnen gratis worden gedownload en hergebruikt, zowel voor commerciële als voor niet-commerciële doeleinden.

doi:10.2811/659087 TK-05-17-225-NL-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

De snelle ontwikkeling van de informatietechnologie heeft de noodzaak voor een degelijke bescherming van persoonsgegevens weer versterkt, het recht dat wordt gewaarborgd door zowel de Europese Unie (EU) als de Raad van Europa (RvE). De bescherming van dit belangrijke recht brengt nieuwe en belangrijke uitdagingen met zich mee, aangezien technologische ontwikkelingen de grenzen van domeinen zoals toezicht, onderschepping van communicatie en gegevensopslag, verlegt. Deze handleiding is bedoeld voor beoefenaars van juridische beroepen die niet gespecialiseerd zijn in gegevensbescherming, om vertrouwd te raken met dit opkomende domein van de wet. In het handboek wordt een overzicht gegeven van de toepasselijke rechtskaders van de EU en de RvE. Daarbij passeert ook de belangrijkste jurisprudentie de revue, met samenvattingen van belangrijke arresten van het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens. Daarnaast worden er hypothetische scenario's voorgesteld die dienen als praktische illustraties van de verschillende vraagstukken die zich in dit steeds veranderende domein kunnen voordoen.

FRA — BUREAU VAN DE EUROPESE UNIE VOOR DE GRONDRECHTEN
Schwarzenbergplatz 11 — 1040 Wenen — Oostenrijk
Tel. +43 158030-0 — Fax +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

EUROPEES HOF VOOR DE RECHTEN VAN DE MENS
RAAD VAN EUROPA
67075 Straatsburg cedex — Frankrijk
Tel. +33 388412018 — Fax +33 388412730
echr.coe.int — publishing@echr.coe.int — twitter.com/ECHR_CEDH

EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING
Wiertzstraat 60 — 1047 Brussel — België
Tel. +32 22831900
edps.europa.eu — edps@edps.europa.eu — twitter.com/EU_EDPS

ISBN 978-92-871-9834-1 (RvE)
ISBN 978-92-9474-296-4 (FRA)

Bureau voor publicaties van de Europese Unie