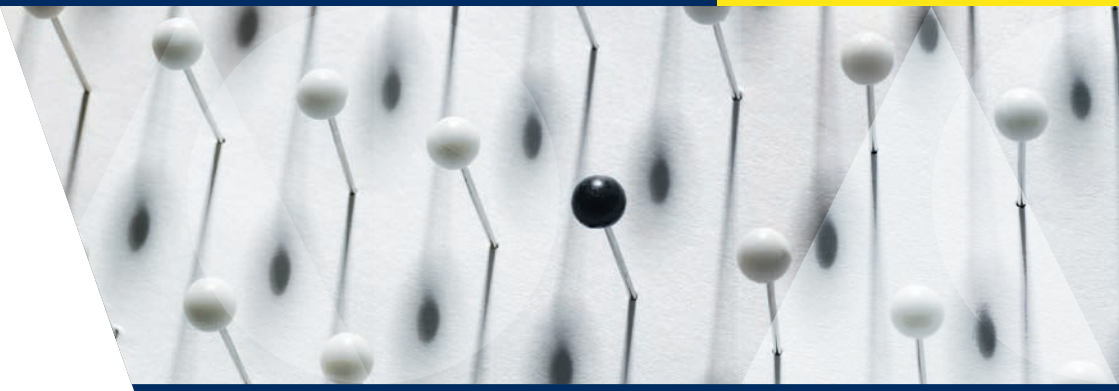
სახელმძღვანელო



მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო

2018 წლის გამოცემა

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

This Handbook is published as part of the Council of Europe Project „Strengthening Personal Data Protection in Georgia“, implemented under the framework of the Council of Europe Action Plan for Georgia 2016-2019.

ეს სახელმძღვანელო დაბეჭდილია ევროპის საბჭოს პროექტის - „პერსონალურ მონაცემთა დაცვის გაძლიერება საქართველოში“ - ფარგლებში, რომელიც საქართველოსთვის ევროპის საბჭოს 2016-2019 წლების სამოქმედო გეგმის ნაწილია.

წინამდებარე სახელმძღვანელოს ტექსტი 2018 წლის აპრილში მომზადდა.

განახლებული ვერსიები სამომავლოდ ხელმისაწვდომი იქნება შემდეგ ვებგვერდებზე: fra.europa.eu (ევროკავშირის ფუნდამენტური უფლებების სააგენტო (FRA)); coe.int/dataprotection (ევროპის საბჭო); echr.coe.int (ადამიანის უფლებათა ევროპული სასამართლო, პრეცედენტული სამართლის განყოფილება); და edps.europa.eu (ევროკავშირის მონაცემთა დაცვის ზედამხედველი).

ფოტოს ავტორი (ყდაზე და სახელმძღვანელოს შიგნით): © iStockphoto

ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018.

ISBN 978-9941-9658-9-0

დაბეჭდილია სს ბეჭდვითი სიტყვის კომბინატში

წინამდებარე სახელმძღვანელო შედგენილია ინგლისურად. სხვა ენებზე თარგმნილი ტექსტის ხარისხზე ევროპის საბჭო (CoE) და ადამიანის უფლებათა ევროპული სასამართლო (ECtHR) პასუხისმგებელნი არ არიან. სახელმძღვანელოში გამოთქმული მოსაზრებები ამ ორგანიზაციებს არაკისრებს რაიმე ვალდებულებას. ნაშრომი მოიცავს მითითებებს სხვადასხვა კომენტარისა და სახელმძღვანელოს შესახებ, რომელთა შინაარსზეც პასუხისმგებლობას არ იღებენ ევროპის საბჭო და ადამიანის უფლებათა ევროპული სასამართლო. ამ გამოცემების შეტანა დამატებით საკითხავი მასალის ჩამონათვალში არ ნიშნავს მათ მხარდაჭერას რაიმე სახით. სხვა სასარგებლო გამოცემათა ჩამონათვალი იხილეთ ადამიანის უფლებათა ევროპული სასამართლოს ბიბლიოთეკის ინტერნეტგვერდებზე: echr.coe.int.

წინამდებარე სახელმძღვანელოს შინაარსი არ გამოხატავს ევროკავშირის მონაცემთა დაცვის ზედამხედველის (EDPS) ოფიციალურ პოზიციას და არ აკისრებს მას რაიმე ვალდებულებას საკუთარი უფლებამოსილებების განხორციელებისას. EDPS ასევე არ არის პასუხისმგებელი სხვა ენებზე თარგმნილი ტექსტის ხარისხზე.

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

მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო

2018 წლის გამოცემა

წინასიტყვაობა

მსოფლიო საზოგადოება სულ უფრო და უფრო მეტად ხდება დამოკიდებული ციფრულ სამყაროზე. ასეთი ცვლილებების ფონზე, ტექნოლოგიური განვითარების ტემპი და პერსონალურ მონაცემთა დამუშავების ფორმები თითოეულ ჩვენგანზე ყოველდღიურად ახდენს გავლენას სხვადასხვა სახით. ცოტა ხნის წინათ გადაიხედა ევროკავშირისა და ევროპის საბჭოს სამართლებრივი ჩარჩო პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა დაცვის შესახებ.

ევროპა მსოფლიოში მონაცემთა დაცვის წინა ხაზზე დგას. ევროკავშირის მონაცემთა დაცვის სტანდარტები ეფუძნება ევროპის საბჭოს 108-ე კონვენციას, ევროკავშირის ინსტრუმენტებს - მათ შორის, მონაცემთა დაცვის ზოგად რეგულაციასა და მონაცემთა დაცვის დირექტივას პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის - ასევე, ადამიანის უფლებათა ევროპული სასამართლოსა და ევროკავშირის მართლმსაჯულების სასამართლოს პრეცედენტულ სამართალს.

ევროკავშირმა და ევროპის საბჭომ გაატარეს მონაცემთა დაცვის ფართო და, ზოგ შემთხვევაში, კომპლექსური ღონისძიებები, რომლებმაც მნიშვნელოვანი გავლენა იქონია ფიზიკურ პირებსა და ბიზნესზე და ფართო სარგებელი მოუტანა მათ. წინამდებარე სახელმძღვანელოს მიზანია ცნობიერების ამაღლება და ცოდნის გაუმჯობესება მონაცემთა დაცვის წესებზე, განსაკუთრებით, იმ პრაქტიკოსი იურისტებისთვის, რომლებიც მონაცემთა დაცვის სპეციალისტები არ არიან, მაგრამ უწევთ ამ საკითხებზე მუშაობა.

სახელმძღვანელო მოამზადა ევროკავშირის ფუნდამენტურ უფლებათა სააგენტომ (FRA), ევროპის საბჭოსა (ადამიანის უფლებათა ევროპული სასამართლოს კანცელარია) და ევროკავშირის მონაცემთა დაცვის ზედამხედველთან თანამშრომლობით. ეს გახლავთ 2014 წლის გამოცემის განახლებული ვერსია, რომელიც ერთიანდება FRA-სა და ევროპის საბჭოს მიერ ერთობლივად გამოქვეყნებული სამართლებრივი სახელმძღვანელოების სერიაში.

ჩვენ მადლობას ვუხდით: ბელგიის, ესტონეთის, საფრანგეთის, საქართველოს, უნგრეთის, ირლანდიის, იტალიის, მონაკოს, შვეიცარიისა და გაერთიანებული სამეფოს მონაცემთა დაცვის ორგანოებს სახელმძღვანელოს სამუშაო ვერსიასთან დაკავშირებული სასარგებლო კომენტარებისთვის; ასევე, ევროკომისიის მონაცემთა დაცვისა თუ მონაცემთა საერთაშორისო გადაცემისა და დაცვის განყოფილებებს და ევროკავშირის მართლმსაჯულების სასამართლოს - სახელმძღვანელოს მომზადებისას მოწოდებული დოკუმენტაციისთვის.

კრისტოს ჯიაკუმოპულოს

ადამიანის უფლებათა და კანონის უზენაესობის მიმართულების გენერალური დირექტორი, ევროპის საბჭო

ჯიოვანი ბუტარელი

ევროკავშირის მონაცემთა დაცვის ზედამხედველი

მაიკლ ო'ფლერთი

ევროკავშირის ფუნდამენტურ უფლებათა სააგენტოს დირექტორი

სარჩევი

აბრევიატურები და აკრონიმები

BCR	სავალდებულო კორპორაციული წესი;
CCTV	ვიდეოთვალთვალის სისტემა;
CETS	ევროპის საბჭოს ხელშეკრულებების სერია;
Charter	ევროკავშირის ფუნდამენტურ უფლებათა ქარტია;
CIS	საბაჟო საინფორმაციო სისტემა;
CJEU	ევროკავშირის მართლმსაჯულების სასამართლო (2009 წლის დეკემბრამდე იგი ცნობილი იყო, როგორც ევროპის მართლმსაჯულების სასამართლო, ECJ);
CoE	ევროპის საბჭო;
108-ე კონვენცია	კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ (ევროპის საბჭო); 108-ე კონვენციის შესწორების ოქმი CETS No. 223 („მოდერნიზებული 108-ე კონვენცია“), მიღებული ევროპის საბჭოს მინისტრთა კომიტეტის მიერ, 128-ე სხდომაზე, რომელიც 2018 წლის 17-18 მაისს გაიმართა დანიაში, ქ. ელსინორში. მასზე მითითება გულისხმობს CETS No. 223 ოქმით შესწორებულ კონვენციას;
CRM	მომხმარებელთან ურთიერთობის მართვა;
C-SIS	შენგენის ცენტრალური საინფორმაციო სისტემა;
DPO	მონაცემთა დაცვის ოფიცერი;
DPA	მონაცემთა დაცვის საზედამხედველო ორგანო;
EAW	დაკავების ევროპული ორდერი;
EDPB	მონაცემთა დაცვის ევროპული საბჭო;
EC	ევროპული თანამეგობრობა;
ECHR	ადამიანის უფლებათა ევროპული კონვენცია;
ECtHR	ადამიანის უფლებათა ევროპული სასამართლო;
EDPS	ევროკავშირის მონაცემთა დაცვის ზედამხედველი;
EEA	ევროპის ეკონომიკური ზონა;

EFSA	ევროპის სურსათის უვნებლობის სააგენტო;
EFTA	თავისუფალი ვაჭრობის ევროპული ასოციაცია;
ENISA	ქსელური და საინფორმაციო უსაფრთხოების ევროპული სააგენტო;
ENU	ევროპოლის შიდასახელმწიფოებრივი ერთეული;
EPPO	ევროკავშირის პროკურატურა;
ESMA	ევროპის ფასიანი ქაღალდებისა და ბაზრების მარეგულირებელი ორგანო;
ETEN	ტრანსევროპული სატელეკომუნიკაციო ქსელები;
EU	ევროკავშირი;
EuroPriSe	პირადი ცხოვრების ხელშეუხებლობის დაცვის ევროპული ხარისხის ბეჭედი;
eu-LISA	ფართომასშტაბიანი ინფორმაციული სისტემების ევროპული კავშირის სააგენტო;
FRA	ევროკავშირის ფუნდამენტური უფლებების სააგენტო;
GDPR	მონაცემთა დაცვის ზოგადი რეგულაცია;
GPS	ადგილმდებარეობის განსაზღვრის გლობალური სისტემა;
ICCPR	საერთაშორისო პაქტი სამოქალაქო და პოლიტიკური უფლებების შესახებ;
ICT	საინფორმაციო და საკომუნიკაციო ტექნოლოგია;
ISP	ინტერნეტმომსახურების მიმწოდებელი;
JSB	საერთო საზედამხედველო ორგანო;
NGO	არასამთავრობო ორგანიზაცია;
N-SIS	შენგენის შიდასახელმწიფოებრივი საინფორმაციო სისტემა;
OECD	ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია;
OJ	ოფიციალური ბეჭდვითი ორგანო;
PIN	პირადი საიდენტიფიკაციო ნომერი;
PNR	მგზავრის პირადი მონაცემები;
SCG	ზედამხედველობის საკოორდინაციო ჯგუფი;

SEPA	ევროთი ანგარიშსწორების საერთო სივრცე;
SIS	შენგენის საინფორმაციო სისტემა;
SWIFT	მსოფლიო ბანკთაშორისი საფინანსო ტელეკომუნიკაციების საზოგადოება;
TEU	ხელშეკრულება ევროკავშირის შესახებ;
TFEU	ხელშეკრულება ევროკავშირის ფუნქციონირების შესახებ;
UDHR	ადამიანის უფლებათა საყოველთაო დეკლარაცია;
UN	გაერთიანებული ერების ორგანიზაცია (გაერო);
VIS	სავიზო საინფორმაციო სისტემა.

როგორ გამოვიყენოთ სახელმძღვანელო

წინამდებარე ნაშრომში წარმოდგენილია ევროკავშირისა და ევროპის საბჭოს სამართლებრივი სტანდარტები მონაცემთა დაცვის შესახებ. სახელმძღვანელო შეიქმნა იმ პროფესიონალთა დასახმარებლად, რომლებიც არ არიან აღნიშნული სფეროს სპეციალისტები. მათ შორის იგულისხმებიან: ადვოკატები, მოსამართლეები და სხვა პრაქტიკოსი იურისტები, სხვადასხვა დაწესებულებაში (მაგ.: არასამთავრობო ორგანიზაციებში) მომუშავე პირები, რომელთაც შეიძლება მოუწიოთ მონაცემთა დაცვის სამართლებრივი საკითხების გადაჭრა.

სახელმძღვანელო ერთგვარი ცნობარია ისეთი დოკუმენტებისთვის, როგორიცაა ევროკავშირის შესაბამისი სამართალი, ადამიანის უფლებათა ევროპული კონვენცია, კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ (108-ე კონვენცია) და ევროპის საბჭოს სხვა ინსტრუმენტები.

თითოეული თავი იწყება ცხრილით, რომელშიც წარმოდგენილია მასში განხილული თემის შესაბამისი სამართლებრივი დებულებები. ცხრილები მოიცავს როგორც ევროპის საბჭოს, ისე ევროკავშირის კანონმდებლობას და ECtHR-ისა და CJEU-ს შესაბამის პრეცედენტულ სამართალს. შემდგომ ერთმანეთის თანმიმდევრობით არის მოცემული ევროპის ორ განსხვავებულ სამართლებრივ სისტემაში მოქმედი შესაბამისი კანონმდებლობა, განსახილველი თემის მიხედვით. ეს მკითხველს საშუალებას აძლევს, დაინახოს განსხვავება და თანხვედრა ამ ორ სისტემას შორის, ასევე, მოიძიოს ძირითადი ინფორმაცია მისთვის საინტერესო საკითხების შესახებ, განსაკუთრებით, თუ მათზე მხოლოდ ევროპის საბჭოს კანონმდებლობა ვრცელდება. აღსანიშნავია, რომ ზოგიერთ თავში, ლაკონიურობის მიზნით, ცხრილში წარმოდგენილი საკითხების რიგითობა უმნიშვნელოდ განსხვავდება განხილული საკითხების რიგითობისგან. სახელმძღვანელო მოკლედ მიმოიხილავს გაეროს სამართლებრივ ჩარჩოსაც.

იმ ქვეყნის პრაქტიკოსებს, რომელიც არ არის ევროკავშირის წევრი, მაგრამ ერთიანდება ევროპის საბჭოში და ხელი მოწერილი აქვს ადამიანის უფლებათა ევროპულ კონვენციასა და 108-ე კონვენციაზე, თავიანთი ქვეყნისთვის რელევანტური ინფორმაციის მოძიება შეუძლიათ პირდაპირ ევროპის საბჭოს ნაწილზე გადასვლით. ამავდროულად, მათ უნდა გაითვალისწინონ, რომ ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის მიღების შემდეგ, ამ გაერთიანების წესები მონაცემთა დაცვის რეგულირების მხრივ ვრცელდება იმ ორგანიზაციებსა და დაწესებულებებზეც, რომლებიც არ არიან რეგისტრირე-

ბულნი ევროკავშირში, მაგრამ ევროკავშირის ტერიტორიაზე მყოფ მონაცემთა სუბიექტებს სთავაზობენ საქონელსა და მომსახურებას, მათ პერსონალურ მონაცემებს ამუშავებენ, ანდა უწევენ მონიტორინგს.

ევროკავშირის წევრ სახელმწიფოებში მომუშავე პრაქტიკოსები ორივე ნაწილს უნდა გაეცნონ, რადგან ასეთ ქვეყნებში ორივე სამართლებრივი სისტემა მოქმედებს სავალდებულო ძალით. აღსანიშნავია, რომ ევროპის საბჭოს და ევროკავშირის მასშტაბით, მონაცემთა დაცვის მარეგულირებელი წესების რეფორმა და მოდერნიზაცია პარალელურად განხორციელდა. კერძოდ, ევროპის საბჭოში 108-ე კონვენციის მოდერნიზების შემდეგ, დოკუმენტი შესწორდა CETS No. 223 ოქმით, ხოლო ევროკავშირმა მიიღო მონაცემთა დაცვის ზოგადი რეგულაცია და დირექტივა 2016/680/EU.

ორივე სამართლებრივ სისტემაში განსაკუთრებული ყურადღება დაეთმო ორი საკანონმდებლო ჩარჩოს თანხვედრასა და თანმიმდევრულობას. ამრიგად, რეფორმებმა გაზარდა ჰარმონიზაციის ხარისხი ევროპის საბჭოსა და ევროკავშირის მონაცემთა დაცვის კანონმდებლობას შორის. ვისაც კონკრეტულ საკითხზე დამატებითი ინფორმაცია ესაჭიროება, სპეციფიკურ თემებთან დაკავშირებული მასალა შეუძლია იხილოს სიაში „დამატებითი საკითხავი“. ინფორმაცია 108-ე კონვენციისა და დამატებითი ოქმის (2001წ.) შესახებ, რომელიც გამოიყენება შესწორების ოქმის ძალაში შესვლამდე, ხელმისაწვდომია სახელმძღვანელოს 2014 წლის გამოცემაში.

CoE-ს კანონმდებლობა წარმოდგენილია გარკვეული საქმეების მიმოხილვით ECtHR-ის პრაქტიკიდან. ეს საქმეები შეირჩა სასამართლოს იმ გადაწყვეტილებებსა და განჩინებებს შორის, რომლებიც შეეხება მონაცემთა დაცვის საკითხებს.

ევროკავშირის შესაბამისი კანონმდებლობა მოიცავს მიღებულ საკანონმდებლო ღონისძიებებს, ხელშეკრულებებსა და ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის დებულებებს, რომლებიც განმარტებულია CJEU-ს პრეცედენტულ სამართალში. ამასთან, წინამდებარე ნაშრომი მიმოიხილავს 29-ე მუხლის სამუშაო ჯგუფის (საკონსულტაციო ორგანო, რომელიც შეიქმნა მონაცემთა დაცვის დირექტივის საფუძველზე და ევროკავშირის წევრ სახელმწიფოებს უწევს ექსპერტულ კონსულტაციას) მიერ მიღებულ სახელმძღვანელო პრინციპებსა და მოსაზრებებს. 2018 წლის 25 მაისიდან ამ ჯგუფს ანაცვლებს მონაცემთა დაცვის ევროპული საბჭო (EDPB). ევროკავშირის კანონმდებლობის განმარტებისათვის მნიშვნელოვანია მისი მონაცემთა დაცვის ზედამხედველის მოსაზრებებიც, რომლებიც ასევე წარმოდგენილია სახელმძღვანელოში.

ნაშრომში აღწერილი ან ციტირებული საქმეები მოიცავს როგორც ECtHR-ის, ისე CJEU-ს პრეცედენტული სამართლის მაგალითებს, ხოლო ბოლოს

წარმოდგენილი სახელმძღვანელო პრინციპები მკითხველებს დაეხმარება სასამართლო გადაწყვეტილებათა ინტერნეტით მოძიებაში. CJEU-ს პრეცედენტული სამართალი უკავშირდება მონაცემთა დაცვის დირექტივას, რომელსაც ამჟამად ძალა აქვს დაკარგული, თუმცა CJEU-ს ინტერპრეტაციები კვლავ ვრცელდება მონაცემთა დაცვის ზოგადი რეგულაციით დადგენილ შესაბამის უფლებებსა და მოვალეობებზე.

ცისფერ გრაფებში წარმოდგენილია ჰიპოთეტური შინაარსის პრაქტიკული ილუსტრაციები, რომლებიც კიდევ უფრო ათვალსაჩინოებს მონაცემთა დაცვის ევროპული წესების გამოყენებას პრაქტიკაში, განსაკუთრებით, თუ არ არსებობს კონკრეტული შემთხვევის შესაბამისი საქმეები ECtHR-ის ან CJEU-ს პრეცედენტულ სამართალში. ნაცრისფერ გრაფებში კი მოცემულია მაგალითები ECtHR-ისა და CJEU-ს მიღმა არსებული წყაროებიდან (მაგ.: 29-ე მუხლის სამუშაო ჯგუფის მოსაზრებები და რეგულაციები).

სახელმძღვანელო იწყება ორი სამართლებრივი სისტემის მნიშვნელობის მოკლე მიმოხილვით, ECHR-ისა და ევროკავშირის სამართლის შესაბამისად (თავი 1). თავები 2-10 მიმოიხილავს შემდეგ საკითხებს:

- მონაცემთა დაცვის ტერმინოლოგია;
- მონაცემთა დაცვის ევროპული სამართლის ძირითადი პრინციპები;
- მონაცემთა დაცვის ევროპული სამართლის წესები;
- დამოუკიდებელი ზედამხედველობა;
- მონაცემთა სუბიექტის უფლებები და მათი დაცვა;
- მონაცემთა გადაცემა საზღვარზე;
- მონაცემთა დაცვა სამართალდამცველ სფეროსა და სისხლისსამართლებრივი მართლმსაჯულების კონტექსტში;
- მონაცემთა დაცვის სხვა ევროპული წესები სპეციფიკურ საკითხებთან დაკავშირებით;
- მონაცემთა დაცვის თანამედროვე გამოწვევები.

1

მონაცემთა დაცვის ევროპული სამართლის კონტექსტი და საფუძველი

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის უფლება		
ევროკავშირის ფუნქციონირების შესახებ ხელშეკრულება, მუხლი 16. ევროკავშირის ქარტია ფუნდამენტური უფლებების შესახებ („ქარტია“), მუხლი 8 („პერსონალურ მონაცემთა დაცვის უფლება“). დირექტივა 95/46/EC პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ („მონაცემთა დაცვის დირექტივა“), OJ 1995 L 281 (ძალაში იყო 2018 წლის მაისამდე). საბჭოს ჩარჩო გადაწყვეტილება 2008/977/JHA სისხლის სამართლის საკითხებში პოლიციისა და სასამართლოს თანამშრომლობის ფარგლებში დამუშავებული პერსონალური მონაცემების დაცვაზე, OJ 2008 L 350 (ძალაში იყო 2018 წლის მაისამდე).		ECHR, მუხლი 8 (პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და მიმოწერის პატივისცემის უფლება). მოდერნიზებული კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ („მოდერნიზებული 108-ე კონვენცია“).

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
რეგულაცია (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ, რომლითაც უქმდება 95/46/EC დირექტივა (მონაცემთა დაცვის ზოგადი რეგულაცია), OJ 2016 L 119.		
დირექტივა (EU) 2016/680 უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნისა და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, რომლითაც უქმდება საბჭოს ჩარჩო გადაწყვეტილება 2008/977/JHA (მონაცემთა დაცვა სამართალდამცველი და სასამართლო ორგანოებისათვის), OJ 2016 L 119.		
დირექტივა 2002/58/EC, ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ (დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ), OJ 2002 L 201.		
რეგულაცია (EC) No. 45/2001 ვროკავშირის ინსტიტუტებისა და ორგანოების მიერ პერსონალური მონაცემების დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ 2001 L 8.		

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის უფლებაზე დაწესებული შეზღუდვები		
ქარტია, მუხლი 52 (1); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 23; CJEU, გაერთიანებული საქმეები C-92/09 და C-93/09, Volker und Markus Schecke GbR და Hartmut Eifert v. Land Hessen *[GC], 2010.*		ECHR, მუხლი 8 (2); მოდერნიზებული 108-ე კონვენცია, მუხლი 11; ECtHR, S. and Marper v. the United Kingdom [GC], Nos. 30562/04 და 30566/04, 2008.
დაბალანსებული უფლებები		
CJEU, გაერთიანებული საქმეები C-92/09 და C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 2010	**ზოგადად**	
CJEU, C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy *[GC], 2008;* *CJEU, C-131/12,* Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 2014.	**გამოხატვის თავისუფლება**	ECtHR, Axel Springer AG v. Germany [GC], No. 39954/08, 2012; ECtHR, Mosley v. the United Kingdom, No. 48009/08, 2011; ECtHR, Bohlen v. Germany, No. 53495/09, 2015.
CJEU, C-28/08 P, European Commission v. The Bavarian Lager Co. Ltd [GC], 2010; CJEU, C-615/13P, ClientEarth, PAN Europe v. EFSA, 2015	**დოკუმენტებთან წვდომა**	ECtHR, *Pruteanu v. Romania,* No. 30181/05, 2015.
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 90	**პროფესიული საიდუმლოება**	
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 91	**რელიგიის ან რწმენის თავისუფლება**	

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
	ხელოვნებისა და მეცნიერების თავისუფლება	ECtHR, Vereinigung bildender Künstler v. Austria, No. 68345/01, 2007
CJEU, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU [GC], 2008	საკუთრების დაცვა	
CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 2014; CJEU, C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 2017.	ეკონომიკური უფლებები	

1.1 პერსონალურ მონაცემთა დაცვის უფლება

ძირითადი საკითხები

- ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის თანახმად, პერსონალურ მონაცემთა დაცვის უფლება ადამიანის პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და მიმოწერის პატივისცემის უფლების ნაწილია.
- დღესდღეობით, ევროპის საბჭოს 108-ე კონვენცია პირველი საერთაშორისო სამართლებრივი ინსტრუმენტია მონაცემთა დაცვის შესახებ, რომელსაც აქვს სავალდებულო ძალა. კონვენციის მოდერნიზაციის პროცესი დასრულდა CETS No. 223 შესწორების ოქმის მიღებით.
- ევროკავშირის კანონმდებლობის თანახმად, მონაცემთა დაცვა აღიარებულია დამოუკიდებელ ფუნდამენტურ უფლებად. მას განამტკიცებს ხელშეკრულება ევროკავშირის ფუნქციონირების შესახებ, კერძოდ, მისი მე-16 მუხლი, და ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლი.

- ევროკავშირის კანონმდებლობაში მონაცემთა დაცვა პირველად მონაცემთა დაცვის დირექტივით დარეგულირდა 1995 წელს.

- სწრაფი ტექნოლოგიური განვითარების გათვალისწინებით, ევროკავშირმა 2016 წელს ახალი კანონმდებლობა მიიღო ციფრულ ეპოქაში მონაცემთა დაცვის წესების ადაპტირებისათვის. 2018 წლის მაისში ძალაში შევიდა მონაცემთა დაცვის ზოგადი რეგულაცია, რომლითაც გაუქმდა მონაცემთა დაცვის დირექტივა.

- მონაცემთა დაცვის ზოგად რეგულაციასთან ერთად, ევროკავშირმა მიიღო კანონმდებლობა სახელმწიფო ორგანოების მიერ მონაცემთა დაცვის დამუშავებაზე სამართლის დასაცავად. დირექტივა (EU) 2016/680 ადგენს მონაცემთა დაცვის წესებსა და პრინციპებს პერსონალურ მონაცემთა დამუშავებაზე, რომლის მიზანია დანაშაულის პრევენცია, გამოძიება, დადგენა, სისხლისსამართლებრივი დევნა, ან სასჯელის აღსრულება.

1.1.1 პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის უფლებები: მოკლე შესავალი

ისინი ერთმანეთს მჭიდროდ უკავშირდება, თუმცა, საქმე გვაქვს ორ სხვადასხვა უფლებასთან: პირადი ცხოვრების ხელშეუხებლობის უფლება, რომელიც ევროპულ სამართალში მოხსენიებულია პირადი ცხოვრების პატივისცემის უფლებად, საერთაშორისო სამართალში წარმოიშვა „ადამიანის უფლებათა საყოველთაო დეკლარაციის“ (UDHR) ფარგლებში (1948 წ.), როგორც ერთ-ერთი ფუნდამენტური და დაცული უფლება. UDHR-ის მიღებიდან მალევე, ეს უფლება აღიარა ევროპამაც, კერძოდ, ადამიანის უფლებათა ევროპულმა კონვენციამ (ECHR), რომელიც 1950 წელს შეიქმნა და ხელმომწერი სახელმწიფოებისათვის სავალდებულო ძალა აქვს. ECHR-ის თანახმად, ყველას აქვს უფლება, პატივი სცენ მის პირად და ოჯახურ ცხოვრებას, საცხოვრებელსა და მიმოწერას. დაუშვებელია ამ უფლების განხორციელებაში საჯარო ხელისუფლების ჩარევა, გარდა ისეთი შემთხვევებისა, როდესაც ასეთი ჩარევა ხორციელდება კანონის შესაბამისად, მნიშვნელოვანი და ლეგიტიმური საჯარო ინტერესების დასაცავად, და აუცილებელია დემოკრატიულ საზოგადოებაში.

UDHR და ECHR მიღებულია კომპიუტერების, ინტერნეტისა და ინფორმაციული საზოგადოების განვითარებაზე გაცილებით ადრე. ამ მოვლენებმა ადამიანებსა და საზოგადოებას მნიშვნელოვანი სარგებელი მოუტანა, გააუმჯობესა ცხოვრების ხარისხი, ეფექტურობა და პროდუქტიულობა, თუმცა, ამავდროულად, ახალი საფრთხეებიც შეუქმნა პირადი ცხოვრების პატივისცემის უფლე-

ბას. პერსონალური ინფორმაციის შეგროვებისა და გამოყენების მარეგულირებელი სპეციფიკური წესების საჭიროებამ წარმოქმნა პირადი ცხოვრების ახალი კონცეფცია, რომელიც სხვადასხვა იურისდიქციაში ცნობილია, როგორც „საინფორმაციო პირადი ცხოვრება“ ან „ინფორმაციული თვითგამორკვევის უფლება“.[1] კონცეფციამ განაპირობა პერსონალურ მონაცემთა დაცვის სპეციალური სამართლებრივი რეგულაციების შემუშავება.

ევროპაში მონაცემთა დაცვა დაიწყო 1970-იან წლებში, როდესაც რამდენიმე სახელმწიფომ მიიღო კანონმდებლობა საჯარო ხელისუფლებისა და მსხვილი კომპანიების მიერ პერსონალური ინფორმაციის დამუშავების გასაკონტროლებლად.[2] შედეგად, ევროპის დონეზე შეიქმნა მონაცემთა დაცვის ინსტრუმენტები[3] და წლების განმავლობაში მონაცემთა დაცვა ცალკე ღირებულებად ჩამოყალიბდა, რომელიც არ განიხილება პირადი ცხოვრების პატივისცემის უფლების ქვეშ. ევროკავშირის სამართლის სისტემაში მონაცემთა დაცვა ფუნდამენტურ უფლებად აღიარებულია პირადი ცხოვრების პატივისცემის უფლებისგან განცალკევებულად. ეს ბადებს კითხვებს ამ ორ უფლებას შორის არსებულ კავშირსა და განსხვავებებზე.

პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის უფლებები მჭიდროდ უკავშირდება ერთმანეთს. ორივე ესწრაფვის მსგავსი ღირებულებების - ადამიანთა დამოუკიდებლობისა და ღირსების დაცვას. შესაბამისად, ეს უფლებები მათ ანიჭებს პერსონალურ სივრცეს, სადაც თავიანთი პიროვნების, აზროვნებისა და შეხედულებების თავისუფლად განვითარება და ფორმირება შეუძლიათ. ამრიგად, ეს უფლებები მნიშვნელოვანი წინაპირობაა სხვა ფუნდამენტურ უფლებათა განხორციელებისთვის, როგო-

1 გერმანიის ფედერალურმა საკონსტიტუციო სასამართლომ განამტკიცა ინფორმაციული თვითგამორკვევის უფლება 1983 წელს მიღებულ გადაწყვეტილებაში საქმეზე *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. სასამართლომ დაადგინა, რომ ასეთი თვითგამორკვევა მომდინარეობს პიროვნების პატივისცემის უფლებიდან, რომელსაც გერმანიის კონსტიტუცია იცავს. ECtHR-მა 2017 წლის გადაწყვეტილებაში დაადგინა, რომ ECHR-ის მე-8 მუხლი „უზრუნველყოფს ინფორმაციული თვითგამორკვევის ფორმის უფლებას.“ იხ. ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, No. 931/13, 27 ივნისი 2017წ., პუნქტი 137.

2 ჰესმენმა (გერმანია) მონაცემთა დაცვის პირველი კანონმდებლობა 1970 წელს მიიღო, რომელიც მხოლოდ ამ ერთეულში მოქმედებდა. 1973 წელს შვედეთმა მიიღო მსოფლიოში პირველი ეროვნული კანონმდებლობა მონაცემთა დაცვის შესახებ. 1980-იანი წლების ბოლოსთვის მონაცემთა დაცვის კანონმდებლობა მიღებული ჰქონდა რამდენიმე ევროპულს სახელმწიფოს (საფრანგეთი, გერმანია, ნიდერლანდები და გაერთიანებული სამეფო).

3 ევროპის საბჭოს კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ (108-ე კონვენცია) მიღებულია 1981 წელს. ევროკავშირმა მონაცემთა დაცვის პირველი ყოვლისმომცველი ინსტრუმენტი 1995 წელს შეიმუშავა: ეს იყო დირექტივა 95/46/EC, რომელიც შეეხება ფიზიკური პირების დაცვას პერსონალურ მონაცემთა დამუშავებისა და თავისუფალი მიმოცვლისას.

რიცაა გამოხატვის თავისუფლება, მშვიდობიანი შეკრებისა და გაერთიანების უფლება, რელიგიის თავისუფლება.

ამ ორი უფლების ფორმულირება და მოქმედების სფერო განსხვავდება. პირადი ცხოვრების პატივისცემის უფლება ზოგადად კრძალავს ჩარევას და ექვემდებარება საჯარო ინტერესის გარკვეულ კრიტერიუმებს, რომლებიც ზოგიერთ შემთხვევაში ამართლებს ჩარევას. პერსონალურ მონაცემთა დაცვა თანამედროვე და აქტუალურ უფლებად მიიჩნევა,[4] რომელიც ქმნის კონტროლისა და დაბალანსების სისტემას პიროვნების დასაცავად პერსონალურ მონაცემთა დამუშავების პროცესში. დამუშავება უნდა აკმაყოფილებდეს ასეთი მონაცემების დაცვის ძირითად კომპონენტებს, კერძოდ, მოთხოვნებს დამოუკიდებელი ზედამხედველობისა და მონაცემთა სუბიექტის უფლებათა პატივისცემის შესახებ.[5]

ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლი არა მხოლოდ განამტკიცებს პერსონალურ მონაცემთა დაცვის უფლებას, არამედ განსაზღვრავს მასთან დაკავშირებულ ძირითად ღირებულებებსაც. ქარტიის თანახმად, პერსონალურ მონაცემთა დამუშავება უნდა იყოს სამართლიანი, ხორციელდებოდეს კონკრეტული მიზნებით, შესაბამისი პირის თანხმობით ან ლეგიტიმური საფუძვლით, რომელსაც ადგენს კანონმდებლობა. ადამიანებს ხელი უნდა მიუწვდებოდეთ თავიანთ პერსონალურ მონაცემებზე და ჰქონდეთ მათი გასწორების შესაძლებლობა, პერსონალურ მონაცემთა დაცვის უფლებასთან შესაბამისობას კი აკონტროლებდეს დამოუკიდებელი ორგანო.

ეს უფლება აქტუალურია პერსონალურ მონაცემთა დამუშავების ნებისმიერი შემთხვევისას. ამრიგად, იგი უფრო ფართოა, ვიდრე პირადი ცხოვრების პატივისცემის უფლება. პერსონალურ მონაცემთა დამუშავების თითოეული ოპერაცია სათანადოდ უნდა იყოს დაცული. ეს ეხება ყველა სახის პერსონალურ მონაცემს და დამუშავებას, პირად ცხოვრებასთან კავშირის ან მასზე გავლენის მიუხედავად. პერსონალური მონაცემების დამუშავება შესაძლოა არღვევდეს პირადი ცხოვრების უფლებასაც, რაც განხილულია ქვემოთ მოყვანილ მაგალითებში. თუმცა, ამ უფლების დარღვევის დემონსტრირება არ არის საჭირო მონაცემთა დაცვის წესების ასამოქმედებლად.

---

4 გენერალური ადვოკატი ელეანორ შარპსტონი ამ საქმეს ორ განსხვავებულ უფლებას უკავშირებდა - პირადი ცხოვრების დაცვის „კლასიკურ“ და მონაცემთა დაცვის „თანამედროვე“ უფლებებს. იხ. CJEU, გაერთიანებული საქმეები C-92/09 და C-93/02, *Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston*, 17 ივნისი, 2010 წ., პუნქტი 71

5 Hustinx, P., EDPS Speeches & Articles, *EU Data Protection Law: the Review oDirective 95/46/EC and the Proposed*, მონაცემთა დაცვის ზოგადი რეგულაცია, 2013 წლის ივლისი.

პირადი ცხოვრების ხელშეუხებლობის უფლება ეხება სიტუაციებს, რომლებიც საფრთხეს უქმნის ადამიანის პირად ინტერესს, ანუ „პირად ცხოვრებას“. წინამდებარე სახელმძღვანელოში ნაჩვენებია, რომ „პირადი ცხოვრების“ კონცეფცია პრეცედენტულ სამართალში საკმაოდ ფართოდ არის განმარტებული და მოიცავს ინტიმურ სიტუაციებს, ასევე, სენსიტიურ, კონფიდენციალურ ან ისეთ ინფორმაციას, რომელმაც შეიძლება ზიანი მიაყენოს პიროვნების აღქმას საზოგადოების მიერ, მათ შორის, ადამიანის პროფესიული ცხოვრებისა და საჯარო ქცევის ასპექტებსაც კი. თუმცა, შეფასება, იყო თუ არა კონკრეტული შემთხვევა ჩარევა „პირად ცხოვრებაში“, დამოკიდებულია მის კონტექსტსა და ფაქტობრივ გარემოებებზე.

მეორე მხრივ, ნებისმიერ ოპერაცია, რომელიც პერსონალურ მონაცემთა დამუშავებას უკავშირდება, შეიძლება მოხვდეს მონაცემთა დამუშავების მარეგულირებელი წესების მოქმედების სფეროში და ამოქმედდეს პერსონალური დაცვის უფლება. მაგალითად, როდესაც დამსაქმებელი უბრალოდ აღრიცხავს ინფორმაციას დასაქმებულთა ვინაობისა და ანაზღაურების შესახებ, ეს პირად ცხოვრებაში ჩარევად ვერ მიიჩნევა, მაგრამ ჩარევის მტკიცება შესაძლებელია, თუ იგი დასაქმებულის პერსონალურ ინფორმაციას მესამე პირს გადასცემს. დამსაქმებელი ნებისმიერ შემთხვევაში უნდა დაემორჩილოს მონაცემთა დაცვის წესებს, ვინაიდან დასაქმებულებზე ინფორმაციის აღრიცხვა მონაცემთა დამუშავებაა.

მაგალითი: *Digital Rights Ireland*-ის საქმეში[6] CJEU-მ იმსჯელა 2006/24/EC დირექტივის საფუძვლიანობაზე პერსონალურ მონაცემთა და პირადი ცხოვრების პატივისცემის ფუნდამენტურ უფლებათა ჭრილში, რომელთაც განამტკიცებს ევროკავშირის ფუნდამენტურ უფლებათა ქარტია. დირექტივა საჯარო ელექტრონული კომუნიკაციებისა და საკომუნიკაციო ქსელების პროვაიდერებს ავალდებულებდა სატელეკომუნიკაციო მონაცემების შენახვას 2 წლამდე ვადით და მათ ხელმისაწვდომობას მძიმე დანაშაულთა პრევენციის, გამოძიებისა და დასჯის მიზნით. ეს ღონისძიება ეხებოდა მეტა, ადგილმდებარეობის განმსაზღვრელ და ისეთ მონაცემებს, რომლებიც საჭიროა გამომწერის ან მომხმარებლის იდენტიფიცირებისთვის და არ უკავშირდებოდა ელექტრონული კომუნიკაციის შინაარსს.

CJEU-მ დაადგინა, რომ დირექტივა ზღუდავდა პერსონალურ მონაცემთა დაცვის ფუნდამენტურ უფლებას, „ვინაიდან იგი ასეთი მონაცემების დამუ-

6 CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი.

შავების შესაძლებლობას იძლევა,“[7] ასევე, პირადი ცხოვრების პატივისცემის უფლებასაც.[8] მთლიანობაში, დირექტივის საფუძველზე შენახული და ხელისუფლების კომპეტენტური ორგანოებისთვის ხელმისაწვდომი მონაცემები იძლევა „ძალიან ზუსტი დასკვნების გაკეთების შესაძლებლობას იმ ადამიანთა პირადი ცხოვრების შესახებ, ვისი მონაცემებიც შენახულია (მათ შორის, ყოველდღიური ჩვევების, მუდმივი ან დროებითი საცხოვრებლის, ყოველდღიური ან სხვა გადაადგილების, აქტივობების, სოციალური კავშირებისა და იმ გარემოს შესახებ, სადაც ხშირად იმყოფებიან“).[9] ზემოაღნიშნული ორი უფლების შეზღუდვა იყო ფართო და განსაკუთრებულად მძიმე.

CJEU-მ 2006/24/EC დირექტივა გაუქმებულად გამოაცხადა. სასამართლოს დასკვნით, მიუხედავად იმისა, რომ პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების უფლებებზე დაწესებული შეზღუდვა ემსახურებოდა ლეგიტიმურ მიზანს, ეს იყო მძიმე შეზღუდვა და არ შემოიფარგლებოდა მხოლოდ მკაცრი საჭიროებით.

1.1.2 საერთაშორისო სამართლებრივი ჩარჩო: გაერო

გაეროს სამართლებრივი ჩარჩო პერსონალურ მონაცემთა დაცვას ფუნდამენტურ უფლებად არ მიიჩნევს, მიუხედავად იმისა, რომ პირადი ცხოვრების დაცვა საერთაშორისო სამართლის სისტემამ დიდი ხნის წინათ აღიარა ფუნდამენტურ უფლებად. UDHR-ის მე-12 მუხლი, რომელიც პირადი და ოჯახური ცხოვრების პატივისცემას შეეხება[10], პირველი საერთაშორისო ინსტრუმენტია, რომლითაც დადგინდა, რომ ადამიანს აქვს უფლება, საკუთარი პირადი სივრცე დაიცვას სხვისი, განსაკუთრებით, სახელმწიფოს ჩარევისგან. UDHR-ს სავალდებულო იურიდიული ძალა არ გააჩნია, თუმცა აქვს ადამიანის უფლებათა საერთაშორისო სამართლის ფუძემდებლური ინსტრუმენტის მნიშვნელოვანი სტატუსი და გავლენა მოახდინა ადამიანის უფლებათა ინსტრუმენტების შექმნაზე ევროპაში. საერთაშორისო პაქტი სამოქალაქო და პოლიტიკური უფლებების შესახებ (ICCPR), რომელიც ძალაში შევიდა 1976 წელს, აცხადებს, რომ „არავინ უნდა დაექვემდებაროს მის პირად და ოჯახურ ცხოვრებაში, საც-

7 *იქვე,* პუნქტი 36.

8 *იქვე,* პუნქტები 32-35.

9 *იქვე,* პუნქტი 27.

10 გაერო (UN), ადამიანის უფლებათა საყოველთაო დეკლარაცია, 1948 წლის 10 დეკემბერი.

ხოვრებლის ან კორესპონდენციის ხელშეუხებლობაში თვითნებურ ან უკანონო ჩარევას ან ღირსებისა და რეპუტაციის უკანონო ხელყოფას“. ICCPR საერთაშორისო ხელშეკრულებაა, რომელიც 169 ხელმომწერ მხარეს ავალდებულებს სამოქალაქო უფლებების - მათ შორის, პირადი ცხოვრების ხელშეუხებლობის - უზრუნველყოფასა და დაცვას.

2013 წლიდან, ახალი ტექნოლოგიების განვითარებასა და ზოგიერთ სახელმწიფოში გამოაშკარავებულ მასობრივ თვალთვალზე („სნოუდენის სკანდალი“) საპასუხოდ, გაერომ პირადი ცხოვრების ხელშეუხებლობის შესახებ მიიღო ორი რეზოლუცია, სახელწოდებით: „პირადი ცხოვრების ხელშეუხებლობის უფლება ციფრულ ეპოქაში“.[11] ეს რეზოლუციები მკაცრად გმობს მასობრივ თვალთვალს და ხაზს უსვამს მის გავლენას პირადი ცხოვრებისა და გამოხატვის თავისუფლების ფუნდამენტურ უფლებებზე, ასევე, ძლიერი და დემოკრატიული სახელმწიფოს ფუნქციონირებაზე. ეს რეზოლუციები შესასრულებლად სავალდებულო არ არის, თუმცა მათ მნიშვნელოვან საერთაშორისო, მაღალი დონის პოლიტიკურ დიალოგს ჩაუყარეს საფუძველი პირადი ცხოვრების ხელშეუხებლობის, ახალი ტექნოლოგიებისა და თვალთვალის შესახებ. სწორედ ამ რეზოლუციებმა განაპირობა სპეციალური მომხსენებლის ინსტიტუტის შექმნა პირადი ცხოვრების ხელშეუხებლობასთან დაკავშირებით, რომლის მანდატიც მოიცავს აღიშნული უფლების ხელშეწყობასა და დაცვას. მომხსენებლის კონკრეტული მოვალეობებია: (1) ინფორმაციის შეგროვება ევროვნულ პრაქტიკასა და გამოცდილებაზე პირადი ცხოვრების ხელშეუხებლობის კუთხით, ასევე, გამოწვევებზე ახალ ტექნოლოგიებთან მიმართებით; (2) საუკეთესო პრაქტიკის გაცვლა-ხელშეწყობა და პოტენციურ დაბრკოლებათა გამოვლენა.

2013-2014 წლებში მიღებული რეზოლუციები მასობრივი თვალთვალის უარყოფით გავლენაზე ამახვილებს ყურადღებას და ხაზს უსვამს სახელმწიფოების პასუხისმგებლობას სადაზვერვო ორგანოების უფლებამოსილებათა შეზღუდვის მხრივ, ხოლო გაეროს ბოლოდროინდელ რეზოლუციებში ასახულია პირადი ცხოვრების ხელშეუხებლობაზე დებატების ძირითადი განვითარება.[12] კერძოდ, 2016 და 2017 წლების რეზოლუციები ადასტურებს სადაზვერვო უწყებათა უფლებამოსილების შეზღუდვის საჭიროებას და გმობს მასობრივ თვალთვალს. ამავდროულად, ამ რეზოლუციებში ცალსახად აღინიშნა, რომ

11 იხ. გაეროს გენერალური ასამბლეა, პირადი ცხოვრების უფლება ციფრულ ეპოქაში, რეზოლუცია A/RES/68/167, New York, 2013 წლის 18 დეკემბერი; და გაეროს გენერალური ასამბლეა, პირადი ცხოვრების უფლება ციფრულ ეპოქაში, შესწორებული რეზოლუციის პროექტი, A/C.3/69/L.26/Rev.1, ნიუ იორკი, 2014 წლის 19 ნოემბერი.

12 გაეროს გენერალური ასამბლეა, პირადი ცხოვრების უფლება ციფრულ ეპოქაში, შესწორებული რეზოლუციის პროექტი, A/C.3/71/L.39/Rev.1, ნიუ იორკი, 2016 წლის 16 ნოემბერი; გაეროს ადამიანის უფლებათა საბჭო, პირადი ცხოვრების უფლება ციფრულ ეპოქაში, A/HRC/34/L.7/Rev.1, 2017 წლის 11 მარტი.

„ბიზნესსაწარმოთა მზარდმა შესაძლებლობამ პერსონალურ მონაცემთა შეგროვების, დამუშავებისა და გამოყენების მხრივ, შეიძლება საფრთხე შეუქმნას ციფრულ ეპოქაში პირადი ცხოვრების ხელშეუხებლობის უფლებით სარგებლობას.“ ამრიგად, გარდა ხელისუფლებისა, რეზოლუციები ყურადღებას ამახვილებს კერძო სექტორის პასუხისმგებლობაზეც ადამიანის უფლებათა დაცვის კუთხით და კომპანიებს მოუწოდებს, მომხმარებლებს გააცნონ ინფორმაცია ასეთი მონაცემების შეგროვების, გამოყენების, გაზიარებისა თუ შენახვის შესახებ და დანერგონ მათი გამჭვირვალედ დამუშავების პოლიტიკა.

1.1.3 ადამიანის უფლებათა ევროპული კონვენცია

ევროპის საბჭო მეორე მსოფლიო ომის შემდეგ შეიქმნა ევროპის სახელმწიფოთა გასაერთიანებლად კანონის უზენაესობის, დემოკრატიის, ადამიანის უფლებებისა და სოციალური განვითარების ხელშეწყობისათვის. ამ მიზნით, ევროპის საბჭომ 1950 წელს მიიღო ადამიანის უფლებათა ევროპული კონვენცია (ECHR), რომელიც ძალაში 1953 წელს შევიდა.

ხელშემკვრელ სახელმწიფოებს აქვთ კონვენციასთან შესაბამისობის საერთაშორისო ვალდებულება. ამ დროისათვის, ევროპის საბჭოს ყველა წევრმა ქვეყანამ საკუთრ კანონმდებლობაში ასახა კონვენცია, ან იურიდიული ძალა მიანიჭა მას, რაც სახელმწიფოებს ავალდებულებს მოქმედებას კონვენციის დებულებათა შესაბამისად. ხელშემკვრელმა მხარეებმა ნებისმიერი საქმიანობის ან უფლებამოსილების განხორციელების პროცესში პატივი უნდა სცენ კონვენციით დაცულ უფლებებს. ეს მოიცავს ეროვნული უსაფრთხოების მიზნით განხორციელებულ ქმედებებსაც. ადამიანის უფლებათა ევროპული სასამართლოს (ECtHR) არაერთი გამორჩეულად მნიშვნელოვანი გადაწყვეტილება ეხება სახელმწიფოს საქმიანობას ისეთ სენსიტიურ სფეროში, როგორიცაა ეროვნული უსაფრთხოების კანონმდებლობა და პრაქტიკა.[13] ამ საქმეებში სასამართლომ უყოყმანოდ დაადგინა, რომ თვალთვალი ადამიანის პირად ცხოვრებაში ჩარევაა.[14]

ხელშემკვრელ მხარეთა მიერ კონვენციით დადგენილი ვალდებულებების შესასრულებლად, 1959 წელს სტრასბურგში (საფრანგეთი) შეიქმნა ადამიანის უფლებათა ევროპული სასამართლო (ECtHR). კონვენციის სავარაუდო დარღვევებზე პიროვნებების, მათი ჯგუფების, არასამთავრობო ორგანიზაციების ან იურიდიული პირების განაცხადები განხილვის გზით, სასამართლო უზრუნველყოფს კონვენციით ნაკისრი ვალდებულებების შესრულებას სახლმ-

13 იხ.მაგ: ECtHR, *Klass and Others v. Germany,* No. 5029/71, 1978 წლის 6 სექტემბერი; ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 2000 წლის 4 მაისი და ECtHR, *Szabó and Vissy v. Hungary,* No. 37138/14, 12 January 2016.

14 *იქვე.*

წიფოთა მიერ. იგი განიხილავს სახელმწიფოთაშორის საქმეებსაც - ევროპის საბჭოს წევრი ერთი ან რამდენიმე ქვეყნის განაცხადს მეორე წევრი ქვეყნის წინააღმდეგ.

2018 წლის მდგომარეობით, ევროპის საბჭო შედგება 47 ხელშემკვრელი სახელმწიფოსგან, რომელთაგან 28 ევროკავშირის წევრია. ევროსასამართლოში განაცხადის შეტანის აუცილებელი წინაპირობა არ არის ხელშემკვრელი სახელმწიფოს მოქალაქეობა, თუმცა, ის სავარაუდო დარღვევები, რომლებზეც განმცხადებელი მიუთითებს, უნდა ექცეოდეს ასეთი სახელმწიფოს იურისდიქციაში.

პერსონალურ მონაცემთა დაცვა მიეკუთვნება ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლით დაცულ უფლებებს. მე-8 მუხლი ადგენს პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და კორესპონდენციის პატივისცემის უფლებას და განსაზღვრავს კონკრეტულ შემთხვევებს, როდესაც დაუშვებელია ამ უფლების შეზღუდვა.[15]

ევროსასამართლოს არაერთი საქმე აქვს განხილული მონაცემთა დაცვის საკითხებზე, მათ შორის, როგორიცაა: კომუნიკაციაზე მიყურადება,[16] თვალთვალის (როგორც კერძო, ისე საჯარო სექტორის წარმომადგენელთა მხრიდან)[17] სხვადასხვა ფორმა და საჯარო უწყებების მიერ პერსონალურ მონაცემთა შენახვისგან დაცვა.[18] პირადი ცხოვრების პატივისცემა არ არის აბსოლუტური უფლება, ვინაიდან მისმა განხორციელებამ შეიძლება დააზიანოს სხვა უფლებები (მაგ.: გამოხატვისა და ინფორმაციაზე წვდომის უფლებები) და პირიქით. ამრიგად, სასამართლო ესწრაფვის ბალანსის დაცვას იმ უფლებებს შორის, რომლებსაც შეეხება კონკრეტული საქმე. მისი განმარტებით, კონვენციის მე-8 მუხლი სახელმწიფოს ავალდებულებს თავშეკავებას ნებისმიერი მოქმედებისგან, რომელმაც შეიძლება დაარღვიოს კონვენციით დაცული უფლება; ასევე, გარკვეული გარემოებებისას, მათ აკისრებს პოზიტიურ ვალდებულებას, პატივი სცენ პირად და ოჯახურ ცხოვრებას.[19] ამ საქმეთა უმრავლესობა დეტალურად არის განხილული შესაბამის თავებში.

---

15 ევროპის საბჭო, *European Convention on Human Rights,* CETS No. 005, 1950.

16 იხ.მაგ: ECtHR, *Malone v. the United Kingdom,* No. 8691/79, 1984 წლის 2 აგვისტო; ECtHR, *Copland v. the United Kingdom,* No. 62617/00, 2007 წლის 3 აპრილი, ან ECtHR, *Mustafa Sezgin Tanrıkulu v. Turkey,* No. 27473/06, 2017 წლის 17 ივლისი.

17 მაგ: ECtHR, *Klass and Others v. Germany,* No. 5029/71, 1978 წლის 6 სექტემბერი; ECtHR, *Uzun v. Germany,* No. 35623/05, 2010 წლის 2 სექტემბერი.

18 მაგ.: ECtHR, *Roman Zakharov v. Russia, No. 47143/06, 2015 4 დეკემბერი; ECtHR, Szabó and Vissy v. Hungary,* No. 37138/14, 2016 12 იანვარი.

19 მაგ.: ECtHR, *I v. Finland,* No. 20511/03, 2008 წლის 17 ივლისი; ECtHR, *K.U. v. Finland,* No. 2872/02, 2008 წლის 2 დეკემბერი.

1.1.4 ევროპის საბჭოს 108-ე კონვენცია

1960-იან წლებში ინფორმაციული ტექნოლოგიების გამოჩენასთან ერთად, გაჩნდა მზარდი მოთხოვნა პერსონალურ მონაცემთა დაცვის დეტალურ წესებზე. 70-იან წლების შუა პერიოდისათვის, ევროპის საბჭოს მინისტრთა კომიტეტმა არაერთი რეზოლუცია მიიღო პერსონალურ მონაცემთა დაცვის შესახებ, რომლებიც ევროპული კონვენციის მე-8 მუხლზე მიუთითებდა.[20] 1981 წელს ხელმოსაწერად გაიხსნა კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ (108-ე კონვენცია)[21]. ეს დოკუმენტი იყო და რჩება სავალდებულო იურიდიული ძალის მქონე ერთადერთ საერთაშორისო ინსტრუმენტად მონაცემთა დაცვის სფეროში.

კონვენცია ვრცელდება ყველა სახის მონაცემთა დამუშავებაზე - როგორც კერძო, ისე საჯარო სექტორის, მათ შორის, მართლმსაჯულებისა და სამართალდამცველი ორგანოების მიერ. იგი ადამიანის უფლებებს იცავს პესონალურ მონაცემთა დამუშავებასთან დაკავშირებული დარღვევებისგან და, ამავდროულად, მიზნად ისახავს მათი საერთაშორისო გადაცემის რეგულირებას. კონვენციით გათვალისწინებული პრინციპები შეეხება მონაცემთა სამართლიან და კანონიერ შეგროვებასა და ავტომატურ დამუშავებას კონკრეტული ლეგიტიმური მიზნებით, რაც ნიშნავს, რომ დაუშვებელია მათი გამოყენება სხვაგვარად, ან შენახვა იმაზე ხანგრძლივად, ვიდრე საჭიროა ამ მიზნების მისაღწევად. დებულებები შეეხება მონაცემთა ხარისხსაც. კერძოდ, ისინი უნდა იყოს ადეკვატური, რელევანტური, ზომიერი (პროპორციული) და ზუსტი.

კონვენცია, გარდა იმისა, რომ უზრუნველყოფს პერსონალურ მონაცემთა დამუშავების გარანტიებისა და უსაფრთხოების ვალდებულებებს, კრძალავს განსაკუთრებული კატეგორიის მონაცემთა (როგორიცაა: პიროვნების რასობრივი კუთვნილება, პოლიტიკური შეხედულებები, ჯანმრთელობის მდგომარეობა, რელიგია, სქესობრივი ცხოვრება და ნასამართლობა) დამუშავებას დაცვის სათანადო სამართლებრივი მექანიზმის გარეშე.

ასევე, იგი იცავს ფიზიკური პირის უფლებას, იცოდეს, თუ რა ინფორმაცია ინახება მასზე და, საჭიროების შემთხვევაში, მოითხოვოს მისი შესწორება. კონვენციით დადგენილი უფლებების შეზღუდვა ნებადართულია მხოლოდ მაშინ,

20 ევროპის საბჭოს მინისტრთა კომიტეტი (1973), რეზოლუცია (73) 22 კერძო სექტორში მონაცემთა ელექტრონული ბანკის პირისპირ ფიზიკურ პირთა პირადი ცხოვრების დაცვის შესახებ, 1973 წლის 26 სექტემბერი; ევროპის საბჭოს მინისტრთა კომიტეტი (1974), რეზოლუცია (74) 29 საჯარო სექტორში მონაცემთა ელექტრონული ბანკის პირისპირ ფიზიკურ პირთა პირადი ცხოვრების დაცვის შესახებ, 1974 წლის 20 სექტემბერი.

21 ევროპის საბჭო, კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ CETS No. 108, 1981.

როცა არსებობს აღმატებული ინტერესები, როგორიცაა სახელმწიფო უსაფრთხოება ან თავდაცვა. ამასთან, კონვენცია ადგენს პერსონალურ მონაცემთა თავისუფალ მიმოცვლას ხელშემკვრელ მხარეებს შორის და გარკვეულ შეზღუდვებს აწესებს მონაცემების გადაცემაზე იმ სახელმწიფოებისთვის, სადაც სამართლებრივი რეგულაციები არ უზრუნველყოფს სათანადო დაცვას.

აღსანიშნავია, რომ 108-ე კონვენციას შესასრულებლად სავალდებულო ძალა აქვს იმ სახელმწიფოებისთვის, რომლებშიც ის რატიფიცირებულია. კონვენცია არ ექვემდებარება ECtHR-ის სასამართლო კონტროლს, თუმცა ამ სასამართლოს პრეცედენტული სამართალი ითვალისწინებს მას ევროპული კონვენციის მე-8 მუხლის კონტექსტში. წლების მანძილზე ECtHR საკუთარ გადაწყვეტილებებში მიუთითებს, რომ პერსონალურ მონაცემთა დაცვა პირადი და ოჯახური ცხოვრების პატივისცემის უფლების (მუხლი 8) მნიშვნელოვანი ნაწილია; ასევე, ხელმძღვანელობს 108-ე კონვენციის პრინციპებით, როდესაც აფასებს სავარაუდო ჩარევას ამ ფუნდამენტურ უფლებაში.[22]

კონვენციით დადგენილი ზოგადი პრინციპებისა და წესების შემდგომი განვითარებისათვის, ევროპის საბჭოს მინისტრთა კომიტეტმა რამდენიმე რეკომენდაცია მიიღო, რომლებსაც არ აქვს სავალდებულო ძალა, თუმცა გავლენა ჰქონდა მონაცემთა დაცვის სამართლის განვითარებაზე ევროპაში. მაგალითად, წლების მანძილზე, ევროპაში არსებული ერთადერთი ინსტრუმენტი, რომელიც მოიცავდა სახელმძღვანელო პრინციპებს სამართალდამცველ სფეროში პერსონალურ მონაცემთა გამოყენების შესახებ, იყო „საპოლიციო რეკომენდაცია“.[23] აღნიშნული რეკომენდაციის პრინციპები (მაგ.: მონაცემთა ფაილების შენახვის საშუალებები და მკაფიო წესები მათზე ხელმისაწვდომობის უფლების მქონე პირთა შესახებ) კიდევ უფრო განვითარდა და აისახა ევროკავშირის შემდგომ კანონმდებლობაში.[24] მოგვიანებით შემუშავებული რეკომენდაციები მოიცავს ციფრული ეპოქის თანმდევ გამოწვევებთან გამკლავებასაც (მაგ.: დასაქმების კონტექსტში მონაცემთა დამუშავება (იხ. თავი 9)).

108-ე კონვენცია რატიფიცირებულია ევროკავშირის ყველა წევრი სახელმწიფოს მიერ. 1999 წელს შემუშავდა მისი შესწორების პროექტი, რომელიც ევროკავშირს საშუალებას აძლევდა, გამხდარიყო კონვენციის მხარე, მაგრამ

22 მაგ: ECtHR, *Z v. Finland,* No. 22009/93, 1997 წლის 25 თებერვალი.

23 ევროპის საბჭო, მინისტრთა კომიტეტი (1987), რეკომენდაცია Rec(87)15 წევრი სახელმწიფოებისათვის პოლიციის სექტორში პერსონალური მონაცემების რეგულაციის შესახებ, სტრასბურგი, 1987 წლის 17 სექტემბერი.

24 რეგულაცია პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ, რომლითაც უქმდება 95/46/EC დირექტივა (მონაცემთა დაცვის ზოგადი რეგულაცია), OJ L 281, 1995 წლის 23 ნოემბერი.

შესწორება ძალაში არ შესულა.[25] 2001 წელს მიიღეს 108-ე კონვენციის დამატებითი ოქმი, რომელიც მოიცავს: დებულებებს მონაცემთა საზღვართაშორის გადაცემაზე - იმ სახელმწიფოებისათვის, რომლებიც კონვენციის მხარეები არ არიან (ე.წ. „მესამე ქვეყნები“); ასევე, სავალდებულო მოთხოვნას შიდასახელმწიფოებრივ დონეზე მონაცემთა დაცვის საზედამხედველო ორგანოს შექმნის შესახებ.[26]

108-ე კონვენციასთან მიერთება შეუძლიათ ევროპის საბჭოს არაწევრ ქვეყნებსაც. კონვენცია გახსნილია მიერთებისთვის და აქვს უნივერსალურ სტანდარტად დამკვიდრების პოტენციალი, რაც გლობალურ დონეზე მონაცემთა დაცვის ხელშეწყობის საფუძველია. დღესდღეობით 108-ე კონვენციის მხარეა 51 ქვეყანა, მათ შორის, ევროპის საბჭოს ყველა წევრი სახელმწიფო (47 ქვეყანა), ურუგვაი (პირველი არაევროპული ქვეყანა, რომელიც კონვენციას მიუერთდა 2013 წლის აგვისტოში), ასევე, მავრიკი, სენეგალი და ტუნისი (რომლებიც კონვენციას 2016 და 2017 წლებში მიუერთდნენ).

ცოტა ხნის წინათ მოხდა კონვენციის მოდერნიზება. 2011 წელს გამართული საჯარო კონსულტაციებით განისაზღვრა პირადი ცხოვრების ხელშეუხებლობის განმტკიცება ციფრულ არენაზე და ისეთი მექანიზმის გაძლიერება, როგორიცაა კონვენციის დანერგვის შეფასება. მოდერნიზების პროცესი ძირითადად ამ ორ ამოცანაზე იყო ორიენტირებული და დასრულდა 108-ე კონვენციის შესწორების ოქმის (CETS No. 223) მიღებით. სამუშაო შესრულდა მონაცემთა დაცვის სხვა საერთაშორისო ინსტრუმენტების, მათ შორის, ევროკავშირის მონაცემთა დაცვის წესების რეფორმასთან ერთად, რომელიც 2012 წელს დაიწყო. ევროპის საბჭოსა და ევროკავშირის კანონმდებლებმა განსაკუთრებული სიფრთხილე გამოიჩინეს, რათა ეს ორი სამართლებრივი ჩარჩო ყოფილიყო ერთმანეთის შესაბამისი და თანმიმდევრული. მოდერნიზების პროცესში შენარჩუნდა კონვენციის ზოგადი ბუნება და მოქნილობა და გაძლიერდა მისი, როგორც მონაცემთა დაცვის სამართლის უნივერსალური ინსტრუმენტის პოტენციალი. იგი განამტკიცებს მთავარ პრინციპებს და მათ სტაბილურობას, ასევე, ადგენს ახალ უფლებებს. ამავდროულად, კონვენცია ზრდის იმ დაწესებულებათა პასუხისმგებლობებს და ანგარიშვალდებულებებს, რომლებიც პერსონალურ მონაცემებს ამუშავებენ. მაგალითად, ფიზიკურ პირს, რომლის მონაცემებიც

25 ევროპის საბჭო, კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, მიღებულია მინისტრთა კომიტეტის მიერ, სტრასბურგი, 1999 წლის 15 ივნისი.

26 ევროპის საბჭო, კონვენციის დამატებითი ოქმი, რომელიც შეეხება ფიზიკური პირების დაცვას პესონალურ მონაცემთა ავტომატური დამუშავებისას, საზედამხედველო ორგანოებსა და მონაცემთა საზღვართშორის მიმოცვლასთან დაკავშირებით, CETS No. 181, 2001. 108-ე კონვენციის მოდერნიზებასთან ერთად, ოქმი აღარ გამოიყენება, რადგან მისი დებულებები განახლდა და ინტეგრირებულია 108-ე მოდერნიზებულ კონვენციაში.

მუშავდება, უფლება აქვს, მიიღოს ინფორმაცია ამ პროცესის დასაბუთებასთან დაკავშირებით და გაასაჩივროს ის. ონლაინ სამყაროში პროფილირების ტექნიკის მზარდი გამოყენების საწინააღმდეგოდ, კონვენცია ადგენს ფიზიკური პირის უფლებას, არ მიიღონ გადაწყვეტილებები მხოლოდ ავტომატური დამუშავების საფუძველზე, მისი მოსაზრებების გაუთვალისწინებლად. ხელშემკვრელ მხარეთა დამოუკიდებელი საზედამხედველო ორგანოების მხრიდან მონაცემთა დაცვის რეგულაციების გაძლიერება მთავარი ფაქტორია კონვენციის პრაქტიკაში დასანერგად. ამდენად, მოდერნიზებული კონვენცია ხაზს უსვამს დამოუკიდებლობის მნიშვნელობას საზედამხედველო ორგანოთა მიერ საკუთარი უფლებამოსილების, ფუნქციებისა და მისიის ეფექტიანად შესრულების პროცესში.

1.1.5 ევროკავშირის მონაცემთა დაცვის სამართალი

ევროკავშირის სამართალი შედგება პირველადი და მეორადი კანონმდებლობისგან. ხელშეკრულება ევროკავშირის შესახებ და ხელშეკრულება ევროკავშირის ფუნქციონირების შესახებ (TFEU) რატიფიცირებულია ყველა წევრი სახელმწიფოს მიერ და ქმნის „ევროკავშირის პირველად კანონმდებლობას.“ რეგულაციები, დირექტივები და გადაწყვეტილებები, რომლებიც ამ ხელშეკრულებათა ფარგლებში მიიღეს გაერთიანების უფლებამოსილმა ინსტიტუტებმა, ქმნის „ევროკავშირის მეორად კანონმდებლობას.“

მონაცემთა დაცვა ევროკავშირის პირველად კანონმდებლობაში

ევროპული თანამეგობრობის თავდაპირველი ხელშეკრულებები არ შეიცავდა რაიმე მითითებას ადამიანის უფლებებსა ან მათ დაცვაზე, იმის გათვალისწინებით, რომ ევროპის ეკონომიკური გაერთიანება ჩამოყალიბდა როგორც ეკონომიკურ ინტეგრაციასა და საერთო ბაზრის შექმნაზე ორიენტირებული რეგიონული ორგანიზაცია. მისი ფუნდამენტური პრინციპი, ევროპული თანამეგობრობის შექმნისა და განვითარების საფუძველი, რომელსაც დღესაც იგივე ძალა აქვს, არის უფლებამოსილებათა მინიჭება (the principle of conferral). ამ პრინციპის თანახმად, ევროკავშირი მოქმედებს მხოლოდ საკუთარი უფლებამოსილების ფარგლებში, რომელიც წევრმა სახელმწიფოებმა მიანიჭეს და ასახულია ევროკავშირის ხელშეკრულებებში. ევროპის საბჭოსგან განსხვავებით, ევროკავშირის ხელშეკრულებები არ მოიცავს მკაფიო მინიშნებას ფუნდამენტურ უფლებებთან დაკავშირებულ უფლებამოსილებებზე.

ვინაიდან ევროკავშირის მართლმსაჯულების სასამართლოში შევიდა საჩივრები ადამიანის უფლებათა სავარაუდო დარღვევებზე იმ სფეროებში, სადაც ვრცელდება ევროკავშირის კანონმდებლობა, სასამართლომ გაითვალისწი-

ნა/შეიმუშავა ხელშეკრულებათა მნიშვნელოვანი განმარტებები. ფიზიკურ პირთა დასაცავად, სასამართლომ ფუნდამენტური უფლებები ევროპული სამართლის ე.წ. ზოგადი პრინციპების ფარგლებში მოაქცია. CJEU-ს მითითებით, ეს პრინციპები ასახავს ადამიანის უფლებათა დაცვის შინაარსს, წარმოდგენილს ეროვნულ კონსტიტუციებსა და ადამიანის უფლებათა ხელშეკრულებებში, განსაკუთრებით, ადამიანის უფლებათა ევროპულ კონვენციაში. CJEU-მ აღნიშნა, რომ უზრუნველყოფს ევროკავშირის სამართლის შესაბამისობას ამ პრინციპებთან.

ევროკავშირმა, აღიარა რა, რომ მის პოლიტიკას შეიძლება გავლენა ჰქონდეს ადამიანის უფლებებზე, ევროკავშირთან მოქალაქეების „დასაახლოებად“, 2000 წელს გამოაცხადა „ფუნდამენტურ უფლებათა ქარტიის“ შექმნის შესახებ. ქარტია მოიცავს ევროპელ მოქალაქეთა სამოქალაქო, პოლიტიკური, ეკონომიკური და სოციალური უფლებების სრულ სპექტრს და ეყრდნობა წევრ სახელმწიფოთა კონსტიტუციურ ტრადიციებსა და ერთიან საერთაშორისო ვალდებულებებს. ამ დოკუმენტით დაცული უფლებები იყოფა 6 კატეგორიად: ღირსება, თავისუფლებები, თანასწორობა, სოლიდარობა, მოქალაქეთა უფლებები და სამართლიანობა.

ქარტია თავდაპირველად მხოლოდ პოლიტიკური დოკუმენტი იყო, თუმცა 2009 წლის 1 დეკემბერს ლისაბონის ხელშეკრულების ამოქმედებით, მიენიჭა სავალდებულო იურიდიული ძალა[27], როგორც ევროკავშირის პირველადი კანონმდებლობის ნაწილს (იხ. TEU-ს მე-6 მუხლის პირველი პუნქტი).[28] მისი დებულებები ევროკავშირის ინსტიტუტებსა და ორგანოებზე ვრცელდება და მათ ავალდებულებს ქარტიაში წარმოდგენილ უფლებათა პატივისცემას საკუთარი მოვალეობების შესრულების პროცესში. ამ დებულებების დაცვა წევრი სახელმწიფოებისთვის სავალდებულოა ევროკავშირის სამართლის დანერგვისას.

ქარტია იცავს არა მხოლოდ პირადი და ოჯახური ცხოვრების (მუხლი 7), არამედ პერსონალურ მონაცემთა დაცვის უფლებასაც (მუხლი 8). ამ უკანასკნელის დაცვას დოკუმენტი ევროკავშირის სამართალში ცალსახად ზრდის ფუნდამენტური უფლების დონემდე. ევროკავშირის ინსტიტუტებმა და ორგანოებმა, ისევე როგორც წევრმა სახელმწიფოებმა, ეს უფლება გარანტირებულად უნდა დაიცვან და პატივი სცენ ევროკავშირის სამართლის პრინციპების დანერგვისას (ქარტიის 51-ე მუხლი). ქარტიის მე-8 მუხლი, რომელიც მონაცემთა დაცვის დირექტივის შექმნიდან რამდენიმე წელიწადში ჩამოყალიბდა, მოიცავს მანამდე არსებულ ევროკავშირის კანონმდებლობას მონაცემთა

27 ევროკავშირი (2012), ფუნდამენტურ უფლებათა ქარტია, OJ 2012 C 326.

28 იხ. შემდეგი დოკუმენტების კონსოლიდირებული ვერსია: ევროპის თანამეგობრობა (2012), ხელშეკრულება ევროკავშირის შესახებ, OJ 2012 C 326; და ევროპის თანამეგობრობა (2012), TFEU, OJ 2012 C 326.

დაცვის შესახებ. შესაბამისად, ქარტია მკაფიოდ მიუთითებს არა მხოლოდ მონაცემთა დაცვის უფლებაზე (მუხლი 8(1)), არამედ, მათი დაცვის ძირითად პრინციპებზეც (მუხლი 8(2)); დაბოლოს, ქარტიის 88(3) მუხლი ადგენს მოთხოვნას დამოუკიდებელი ორგანოს შესახებ, რომელიც გააკონტროლებს ამ პრინციპების განხორციელებას.

ლისაბონის ხელშეკრულების მიღება მნიშვნელოვანი მოვლენაა მონაცემთა დაცვის სამართლის განვითარებაში: მან ქარტიას სამართლებრივად სავალდებულო ინსტრუმენტის სტატუსი მიანიჭა ძირითადი კანონმდებლობის დონეზე და უზრუნველყო პერსონალურ მონაცემთა დაცვის უფლება. ამ უფლებას კონკრეტულად ადგენს TFEU-ს მე-16 მუხლი, კერძოდ, ხელშეკრულების იმ ნაწილში, რომელიც ევროკავშირის ზოგად პრინციპებს ეთმობა. მუხლი ქმნის ახალ სამართლებრივ საფუძველსაც, რომელიც ევროკავშირს აძლევს მონაცემთა დაცვის საკითხებზე კანონების შემუშავების უფლებამოსილებას. ეს მნიშვნელოვანი მოვლენაა, რადგან ევროკავშირის მონაცემთა დაცვის წესები, განსაკუთრებით, მონაცემთა დაცვის დირექტივა, თავდაპირველად ეფუძნებოდა შიდა ბაზრის სამართლებრივ საფუძველს და შიდასახელმწიფოებრივი კანონების დაახლოების საჭიროებას, რათა ხელი არ შეშლოდა ევროკავშირის ფარგლებში მონაცემთა თავისუფალ მოძრაობას. TFEU-ს მე-16 მუხლი ამჟამად ადგენს ცალკე სამართლებრივ საფუძველს მონაცემთა დაცვის დამოუკიდებელი, სრულფასოვანი მიდგომისთვის, რომელიც ფარავს ევროკავშირის უფლებამოსილების ყველა სფეროს, მათ შორის, პოლიციისა და მართლმსაჯულების თანამშრომლობას სისხლის სამართლის საკითხებზე. მუხლი ასევე ადგენს, რომ შესაბამისობას ამ ხელშეკრულების თანახმად მიღებულ მონაცემთა დაცვის წესებთან უნდა აკონტროლებდეს დამოუკიდებელი საზედამხედველო ორგანო. სწორედ მე-16 მუხლი ქმნის სამართლებრივ საფუძველს მონაცემთა დაცვის წესების კომპლექსური რეფორმისათვის (2016), რომელიც მოიცავს მონაცემთა დაცვის ზოგად რეგულაციასა და მონაცემთა დაცვის დირექტივას პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის (იხ. ქვემოთ).

მონაცემთა დაცვის ზოგადი რეგულაცია

1995 წლიდან 2018 წლის მაისამდე, ევროკავშირის მონაცემთა დაცვის მთავარი სამართლებრივი ინსტრუმენტი იყო ევროპის პარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC, რომელიც შეეხებოდა პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვას და ამგვარი მონაცემების თავისუფალ მიმოცვლას (მონაცემთა დაცვის დირექტივა).[29] დირ-

29 ევროპული პარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ 1995 L 281.

ექტივა მიღებულია 1995 წელს. ამ დროისათვის ევროკავშირის რამდენიმე წევრ სახელმწიფოში უკვე მოქმედებდა კანონები მონაცემთა დაცვის შესახებ[30] და საჭირო იყო მათი ჰარმონიზება, რათა უზრუნველეყოთ პერსონალურ მონაცემთა მაღალ დონეზე დაცვა და მათი თავისუფალი გადაცემა სხვადასხვა წევრ სახელმწიფოს შორის. შიდა ბაზარზე საქონლის, კაპიტალის, მომსახურებისა და ადამიანების თავისუფალი გადაადგილება მოითხოვდა მონაცემთა თავისუფალ მოძრაობასაც, რაც ვერ მოხერხდებოდა წევრ ქვეყნებში მონაცემთა დაცვის თანაბრად მაღალი სტანდარტის გარეშე.

დირექტივა ასახავდა მონაცემთა დაცვის პრინციპებს, რომლებსაც აერთიანებდა შიდასახელმწიფოებრივი კანონმდებლობები და 108-ე კონვენცია და, ხშირ შემთხვევაში, განავრცობდა მათ. იგი ეყრდნობოდა 108-ე კონვენციის მე-11 მუხლით განსაზღვრულ შესაძლებლობას დაცვის ინსტრუმენტების გაზრდის შესახებ. კერძოდ, მონაცემთა დაცვის წესებთან შესაბამისობის გასაუმჯობესებლად, დირექტივაში ისეთი ინსტრუმენტის შემოღებამ, როგორიცაა დამოუკიდებელი ზედამხედველობა, მნიშვნელოვანი წვლილი შეიტანა მონაცემთა დაცვის ევროპული სამართლის ეფექტიან დანერგვაში. შედეგად, 2001 წელს ეს მექანიზმი გაითვალისწინეს ევროპის საბჭოს კანონმდებლობაშიც, 108-ე კონვენციის დამატებითი ოქმის საშუალებით, რაც ცხადყოფს ამ ორ ინსტრუმენტს შორის მჭიდრო კავშირსა და პოზიტიურ ურთიერთგავლენას წლების განმავლობაში.

მონაცემთა დაცვის დირექტივამ შექმნა ევროკავშირში მონაცემთა დაცვის დეტალური და სრულფასოვანი სისტემა. თუმცა, ევროკავშირის სამართლებრივი სისტემის შესაბამისად, დირექტივები არ ვრცელდება პირდაპირ, საჭიროა მათი გადატანა წევრ სახელმწიფოთა ეროვნულ კანონმდებლობაში. როგორც მოსალოდნელია, ამ ქვეყნებს აქვთ გარკვეული დისკრეცია/მოქმედების თავისუფლება დირექტივების დებულებათა შიდასახელმწიფოებრივ კანონმდებლობაში გადატანის კუთხით. მიუხედავად იმისა, რომ დირექტივა მიზნად ისახავს სრულ ჰარმონიზაციას[31] (და სრულფასოვან დაცვას), წევრ სახელმწიფოთა ეროვნულ კანონმდებლობაში ის პრაქტიკულად სხვადასხვანაირად აისახა. შედეგად, ევროკავშირში შეიქმნა მონაცემთა დაცვის განსხვავებული

30 ჰესენმა (გერმანია) 1970 წელს მიიღო მსოფლიოში პირველი მონაცემთა დაცვის კანონმდებლობა, რომელიც მხოლოდ ამ ერთეულზე ვრცელდებოდა. შვედეთმა 1973 წელს მიიღო Datalagen;
გერმანიამ 1976 წელს მიიღო *Bundesdatenschutzgestez;* საფრანგეთმა 1977 წელს მიიღო *Loi relatif à l'informatique, aux fichiers et aux libertés*; გაერთიანებულ სამეფოში მონაცემთა დაცვის აქტი მიღებულია 1984 წელს; ნიდერლანდებმა კი Wet Persoonregistraties 1989 წელს მიიღო.

31 CJEU, გაერთიანებული საქმეები C-468/10 და C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 2011 წლის 24 ნოემბერი, პუნქტი 29.

წესები, რომლებიც სხვადასხვაგვარად განიმარტება შიდასახელმწიფოებრივ კანონებში. აღსრულების დონე და სანქციების სიმძიმე ასევე განსხვავდება ამ ქვეყნებში. დაბოლოს, 1990-იანი წლების შუა პერიოდში დირექტივის შემუშავების შედგომ, მნიშვნელოვნი ცვლილებები მოხდა საინფორმაციო ტექნოლოგიაში, რამაც წარმოშვა ევროკავშირის მონაცემთა დაცვის კანონმდებლობის რეფორმის საჭიროება.

რეფორმის პროცესი 2016 წლის აპრილში დასრულდა მონაცემთა დაცვის ზოგადი რეგულაციის მიღებით, ხანგრძლივი და ინტენსიური დებატების შედეგად. დისკუსია ევროკავშირის მონაცემთა დაცვის მარეგულირებელი წესების მოდერნიზებაზე 2009 წლიდან იღებს სათავეს, როდესაც ევროკავშირმა საჯარო კონსულტაცია დაიწყო პერსონალურ მონაცემთა დაცვის ფუნდამენტური უფლების სამართლებრივ ჩარჩოზე. რეგულაციის პროექტი კომისიამ 2012 წლის იანვარში გამოაქვეყნა, რასაც მოჰყვა მოლაპარაკების ხანგრძლივი საკანონმდებლო პროცესი ევროპარლამენტსა და ევროკავშირის საბჭოს შორის. მიღების შემდეგ, მონაცემთა დაცვის ზოგადი რეგულაცია ითვალისწინებდა ორწლიან გარდამავალ პერიოდს, სრულფასოვნად კი ამოქმედდა 2018 წლის 25 მაისს, როდესაც გაუქმდა მონაცემთა დაცვის დირექტივა.

2016 წელს, მონაცემთა დაცვის ზოგადი რეგულაციის მიხედვით, მოხდა ევროკავშირის შესაბამისი კანონმდებლობის მოდერნიზება. შედეგად, კანონმდებლობას მიენიჭა ფუნდამენტურ უფლებათა დაცვის შესაძლებლობა ციფრული ეპოქის ეკონომიკური და სოციალური გამოწვევების კონტექსტში. GDPR ითვალისწინებს და ავითარებს მონაცემთა სუბიექტის ძირითად უფლებებსა და პრინციპებს, რაც მოცემულია მონაცემთა დაცვის დირექტივაში. ამასთან, იგი ადგენს ახალ ვალდებულებებს, რომელთა თანახმადაც ორგანიზაციებმა უნდა დანერგონ მონაცემთა დაცვის სტანდარტები ახალი პროდუქტის ან მომსახურების შექმნისას (by design) და მონაცემთა დაცვა განსაზღვრონ პირველად პარამეტრად (by default); გარკვეულ შემთხვევებში მათ უნდა დანიშნონ მონაცემთა დაცვის ოფიცერი, შეასრულონ მონაცემთა პორტირების ახალი უფლების მოთხოვნები და დაემორჩილონ ანგარიშვალდებულების პრინციპს. ევროკავშირის კანონმდებლობის თანახმად, რეგულაციები ვრცელდება პირდაპირ და ეროვნულ კანონმდებლობაში გადატანას არ საჭიროებს. ამრიგად, მონაცემთა დაცვის ზოგადი რეგულაცია ქმნის მონაცემთა დაცვის ერთიანი წესების კრებულს, რომელიც ევროკავშირის მასშტაბით მოქმედებს. შედეგად, ევროკავშირში ჩამოყალიბდა მონაცემთა დაცვის ერთიანი წესები და სამართლებრივად განჭვრეტადი გარემო, რაც მოქმედებს ეკონომიკური ოპერატორებისა და ფიზიკურ პირების, როგორც „მონაცემთა სუბიექტების“ სასარგებლოდ.

მონაცემთა დაცვის ზოგადი რეგულაცია პირდაპირ ვრცელდება, მაგრამ მასთან სრული შესაბამისობისათვის წევრმა სახელმწიფოებმა უნდა განაახლონ მონაცემთა დაცვის შიდასახელმწიფოებრივი კანონები. ამასთან, კონ-

კრეტულ დებულებებთან დაკავშირებით, წევრ სახელმწიფოებს ენიჭებათ დისკრეცია/მოქმედების თავისუფლება, რეგულაციის პრეამბულის მე-10 პუნქტის შესაბამისად. წინამდებარე სახელმძღვანელოს დიდი ნაწილი ეთმობა ამ რეგულაციით დადგენილ ძირითად წესებსა და პრინციპებს, ასევე მყარ უფლებებს, რომელებსაც იგი ანიჭებს ფიზიკურ პირებს. ეს თემა განხილულია მომდევნო თავებში. რეგულაცია ითვალისწინებს ყოვლისმომცველ წესებს ტერიტორიული მოქმედების სფეროსთან დაკავშირებით. იგი ვრცელდება ევროკავშირში შექმნილ ბიზნესებზე, ასევე, მონაცემთა დამმუშავებლებსა და უფლებამოსილ ორგანოებზე, რომლებიც არ არიან ევროკავშირში დაფუძნებულნი, მაგრამ საქონელსა და მომსახურებას სთავაზობენ ან მონიტორინგს უწევენ ევროკავშირის ტერიტორიაზე არსებულ მონაცემთა სუბიექტებს. ვინაიდან საზღვარგარეთ მოქმედ ტექნოლოგიურ ბიზნესებს ევროპული ბაზრის დიდ წილი უკავია და მილიონობით მომხმარებელი ჰყავს ევროკავშირის ტერიტორიაზე, მნიშვნელოვანია, ევროკავშირის მონაცემთა დაცვის წესები ვრცელდებოდეს აღნიშნულ ორგანიზაციებზეც. ეს უზრუნველყოფს ფიზიკური პირთა დაცვასა და თანაბარ სამოქმედო ველს.

მონაცემთა დაცვა სამართალდამცველ სფეროში - დირექტივა 2016/680

გაუქმებული დირექტივა აწესებდა მონაცემთა დაცვის კომპლექსურ რეჟიმს, რომელიც კიდევ უფრო გაუმჯობესდა ზოგადი რეგულაციის მიღებით. ამის მიუხედავად, დირექტივის მოქმედების სფერო შეზღუდული იყო და მოიცავდა მხოლოდ შიდა ბაზრისა და საჯარო უწყებების აქტივობებს, გარდა სამართალდამცველი ორგანოებისა. შესაბამისად, საჭირო იყო ახალი ინსტრუმენტების მიღება სათანადო სიცხადისა და ბალანსის მისაღწევად მონაცემთა დაცვასა და სხვა ლეგიტიმურ ინტერესებს შორის, ასევე, იმ გამოწვევების დასაძლევად, რომლებიც განსაკუთრებით რელევანტურია გარკვეულ სექტორებში. ეს ეხება წესებს, რომლებიც არეგულირებს პერსონალურ მონაცემთა დამუშავებას სამართალდამცველი ორგანოების მიერ.

ევროკავშირის პირველი სამართლებრივი ინსტრუმენტი, რომელიც აღნიშნულ საკითხს აწესრიგებს, იყო საბჭოს ჩარჩო გადაწყვეტილება 2008/977/JHA - სისხლის სამართლის საკითხებზე პოლიციისა და სასამართლოს თანამშრომლობით დამუშავებულ პერსონალურ მონაცემთა დაცვაზე. ჩარჩო გადაწყვეტილებით დადგენილი წესები ეხება მხოლოდ პოლიციისა და სასამართლოს მონაცემებს, რომლებსაც ცვლიან წევრი სახელმწიფოები. მისი მოქმედების სფერო არ მოიცავს სამართალდამცველი ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებას შიდასახელმწიფოებრივ დონეზე.

ამ ნაკლოვანებას აღმოფხვრის დირექტივა 2016/680 – „უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის და სასჯელის აღსრულების მიზნით პერსონა-

ლური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ“,[32] რომელიც ცნობილია, როგორც „მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის“. მონაცემთა დაცვის ზოგადი რეგულაციის პარალელურად მიღებულმა დირექტივამ გააუქმა ჩარჩო გადაწყვეტილება 2008/977/JHA და შექმნა პერსონალურ მონაცემთა დაცვის კომპლექსური სისტემა სამართალდამცველ კონტექსტში პერსონალურ მონაცემთა დამუშავებისას. ამასთან, იგი ითვალისწინებს საზოგადოებრივ უსაფრთხოებასთან დაკავშირებულ მონაცემთა დამუშავების თავისებურებასაც. ზოგადი რეგულაცია კი ადგენს ზოგად წესებს ფიზიკურ პირთა დასაცავად მათი პერსონალური მონაცემების დამუშავებისას, ასევე, ევროკავშირში ამგვარი მონაცემების თავისუფალი მოძრაობისთვის. ამავდროულად, ის ითვალისწინებს კონკრეტულ წესებს მონაცემთა დაცვისთვის სისხლისსამართლებრივ საკითხებზე და სამართალდამცველ ორგანოებს შორის თანამშრომლობისას. დირექტივა 2016/680 ვრცელდება პერსონალურ მონაცემთა დამუშავებაზე უფლებამოსილი ორგანოს მიერ, რომლის მიზანია სისხლისსამართლებრივი დანაშაულების პრევენცია, გამოძიება, დადგენა, დევნა, ან სასჯელის აღსრულება; ხოლო როდესაც ასეთი ორგანო მონაცემებს ამუშავებს სხვა მიზნებით, მასზე ვრცელდება ზოგადი რეგულაცია. წინამორბედი დოკუმენტისაგან (საბჭოს ჩარჩო გადაწყვეტილება 2008/977/JHA) განსხვავებით, 2016/680 დირექტივის მოქმედების სფერო მოიცავს სამართალდამცველი ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებას შიდასახელმწიფოებრივ დონეზე და არ შემოიფარგლება მათი გაცვლით მხოლოდ წევრ სახელმწიფოებს შორის. ამასთან, დირექტივა მიზნად ისახავს ბალანსის მიღწევას, ერთი მხრივ, ფიზიკურ პირთა უფლებებსა და, მეორე მხრივ, უსაფრთხოებასთან დაკავშირებული დამუშავების კანონიერ მიზნებს შორის.

ამისათვის დირექტივა განამტკიცებს პერსონალურ მონაცემთა დაცვის უფლებას და იმ ძირითად პრინციპებს, რომლებიც უნდა გავრცელდეს მონაცემთა დამუშავებაზე, ზოგადი რეგულაციით გათვალისწინებული წესებისა და პრინციპების ზედმიწევნით დაცვით. ფიზიკურ პირთა უფლებები და მონაცემთა დამმუშავებლის მოვალეობები (მაგ.: მონაცემთა უსაფრთხოება; მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (by design) და მონაცემთა დაცვა პირველად პარამეტრად (by default); ასევე, პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შესახებ შეტყობინება) მონაცემთა დაცვის ზოგად რეგულაციაში წარმოდგენილი უფლებებისა და მოვალეობების მსგავსია. დირექტივა ითვალისწინებს და ცდილობს რეაგირებას იმ მზარდ ტექნოლოგიურ გამოწვევებზე, რომლებმაც

32 ევროპის პარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680, უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ L 119, 2016 წლის 4 მაისი.

შეიძლება განსაკუთრებულად მძიმე შედეგები მოუტანოს ფიზიკურ პირებს (მაგ.: პროფილირების ტექნიკის გამოყენება სამართალდამცველი ორგანოების მიერ). ზოგადად, გადაწყვეტილებები, რომლებიც ეფუძნება მხოლოდ მონაცემთა ავტომატურ დამუშავებას, მათ შორის, პროფილირებას, უნდა აიკრძალოს.[33] ამასთან, ისინი არ უნდა ეფუძნებოდეს განსაკუთრებული კატეგორიის მონაცემებს. ამ პრინციპებთან მიმართებით, დირექტივა ითვალისწინებს გარკვეულ გამონაკლის შემთხვევებს. მონაცემთა ამგვარი დამუშავება არ უნდა იწვევდეს პიროვნების დისკრიმინაციას.[34]

დირექტივა ასევე მოიცავს წესებს მონაცემების დამმუშავებელთა ანგარიშვალდებულების უზრუნველსაყოფად. კერძოდ, მათ უნდა დანიშნონ მონაცემთა დაცვის ოფიცერი, რომელიც: მონიტორინგს გაუწევს შესაბამისობას მონაცემთა დაცვის წესებთან; დაწესებულებასა და მის თანამშრომლებს, რომლებიც მონაცემებს ამუშავებენ, მიაწოდებს ინფორმაციას და გაუწევს კონსულტაციას მათი მოვალეობების შესახებ; ასევე, ითანამშრომლებს შესაბამის საზედამხედველო ორგანოსთან. დღევანდელი მდგომარეობით, პერსონალურ მონაცემთა დამუშავებას სამართალდამცველ და სისხლისსამართლებრივ სექტორებში მეთვალყურეობს დამოუკიდებელი საზედამხედველო ორგანო. მონაცემთა დაცვის ზოგადი სამართლებრივი რეჟიმი და მონაცემთა დაცვის სპეციალური რეჟიმი სამართალდამცველ და სისხლისსამართლებრივ კონტექსტში თანაბრად უნდა ითვალისწინებდეს ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მოთხოვნებს.

სპეციალური რეჟიმი, რომელიც მონაცემთა დაცვის დირექტივის საფუძველზე შეიქმნა სამართალდამცველი და სისხლის სამართლის ორგანოებისთვის, დეტალურად განხილულია მე-8 თავში.

დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ

მონაცემთა დაცვის სპეციალური წესების შექმნა საჭირო იყო ელექტრონული კომუნიკაციის სექტორშიც. ინტერნეტის, ასევე, ფიქსირებული და მობილური ტელეფონების განვითარებასთან ერთად, მნიშვნელოვანი გახდა მომხმარებელთა პირადი ცხოვრების ხელშეუხებლობისა და კონფიდენციალობის უფლების დაცვა. დირექტივა 2002/58/EC[35], რომელიც შეეხება პერსონალურ

33 მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის, მუხლი 11 (1).

34 *იქვე*, მუხლი 11 (2) და (3).

35 ევროპული პარლამენტის და საბჭოს 2002 წლის 12 ივლისის დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ, OJ L 201 (დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ).

მონაცემთა დამუშავებას და პირადი ცხოვრების ხელშეუხებლობის დაცვას ელექტრონული კომუნიკაციების სექტორში (დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ, ანუ e-Privacy დირექტივა), ადგენს წესებს ამ ქსელებში პერსონალურ მონაცემთა უსაფრთხოების, მის დარღვევაზე შეტყობინებისა და კომუნიკაციების კონფიდენციალობის შესახებ.

უსაფრთხოებასთან დაკავშირებით, ელექტრონული კომუნიკაციების ოპერატორებმა უნდა უზრუნველყონ, რომ პერსონალურ მონაცემებზე წვდომა ჰქონდეთ მხოლოდ უფლებამოსილ პირებს და მიიღონ ზომები ამგვარ მონაცემთა განადგურების, დაკარგვის ან შემთხვევით დაზიანების თავიდან ასაცილებლად.[36] განსაკუთრებული რისკი, საზოგადოებრივი კომუნიკაციის ქსელის უსაფრთხოების დარღვევის მხრივ, ოპერატორებმა მომხმარებლებს უნდა შეატყობინონ.[37] თუ გატარებული უსაფრთხოების ზომების მიუხედავად მაინც დაირღვევა მონაცემთა უსაფრთხოება, ოპერატორებმა ეს უნდა აცნობონ უფლებამოსილ ადგილობრივ ორგანოებს, რომელთაც ევალებათ დირექტივის დანერგვა და აღსრულება. ზოგჯერ მათ მოეთხოვებათ ფიზიკური პირების ინფორმირებაც პერსონალურ მონაცემთა უსაფრთხოების დარღვევასთან დაკავშირებით (კერძოდ, როდესაც დარღვევა, სავარაუდოდ, უარყოფით გავლენას მოახდენს მათ პერსონალურ მონაცემებზე ან პირადი ცხოვრების ხელშეუხებლობაზე).[38] კომუნიკაციების კონფიდენციალობა გულისხმობს მოსმენის, მიყურადების, შენახვის, თვალთვალის, ასევე, კომუნიკაციასა და მეტამონაცემებზე მონიტორინგის პრინციპულად აკრძალვას. დირექტივა კრძალავს არასასურველ კომუნიკაციებსაც (ე.წ. spam-ს), გარდა იმ შემთხვევისა, როცა არსებობს მომხმარებლის თანხმობა, და ადგენს წესებს კომპიუტერებსა და მოწყობილობებზე ე.წ. „cookie ჩანაწერების“ (cookies) შენახვასთან მიმართებით. ეს ძირითადი უარყოფითი მოვალეობები მკაფიოდ მიუთითებს, რომ კომუნიკაციების კონფიდენციალობა მნიშვნელოვნად უკავშირდება პირადი ცხოვრების პატივისცემის უფლებას, რომელსაც ითვალისწინებს ქარტიის მე-7 მუხლი, და პერსონალურ მონაცემთა დაცვის უფლებას, გარანტირებულს ქარტიის მე-8 მუხლით.

2017 წლის იანვარში კომისიამ გამოაქვეყნა საკანონმდებლო წინადადება ელექტრონული კომუნიკაციების სფეროში პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის შესახებ, რომელიც ჩაანაცვლებდა დირექტივას პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ (e-Privacy დირექტივა). რეფორმის მიზანია ელექტრონული

36 დირექტივა პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ, მუხლი 4 (1).

37 *იქვე,* მუხლი 4 (2).

38 *იქვე,* მუხლი 4 (3).

კომუნიკაციების მარეგულირებელი წესების ჰარმონიზება მონაცემთა დაცვის ახალ რეჟიმთან, რომელსაც ადგენს მონაცემთა დაცვის ზოგადი რეგულაცია. ეს ახალი რეგულაცია ევროკავშირის მასშტაბით პირდაპირ გავრცელდება. ნებისმიერი პირი ელექტრონულ კომუნიკაციებში ისარგებლებს დაცვის ერთი და იმავე დონით, ხოლო სატელეკომუნიკაციო ოპერატორებს და ბიზნესებს გარანტირებული ექნებათ სამართლებრივი განჭვრეტადობა და ერთიანი, ცხადი წესები ევროკავშირის მასშტაბით. ელექტრონული კომუნიკაციების კონფიდენციალობის შესახებ შემოთავაზებული წესები გავრცელდება ისეთი მომსახურების მიმწოდებელ ახალ მოთამაშეებზეც, რომელიც არ რეგულირდება e-Privacy დირექტივით (იგი ფარავს მხოლოდ ტრადიციული სატელეკომუნიკაციო მომსახურების მიმწოდებლებს). ისეთი სერვისების ზრდასთან ერთად, როგორიცაა Skype, WhatsApp, Facebook Messenger და Viber, შეტყობინების გაგზავნისას ან ზარის განხორციელებისას, ეს OTT (over-the-top) სერვისები მოექცევა რეგულაციის მოქმედების სფეროში და მათზე გავრცელდება მონაცემთა დაცვის, პირადი ცხოვრების ხელშეუხებლობისა და უსაფრთხოების მოთხოვნები. ამ სახელმძღვანელოს გამოქვეყნების დროისათვის, საკანონმდებლო პროცესი ელექტრონულ სივრცეში პირადი ცხოვრების ხელშეუხებლობის დაცვის მარეგულირებელ წესებთან დაკავშირებით ჯერ არ დასრულებულა.

რეგულაცია No. 45/2001

ვინაიდან მონაცემთა დაცვის დირექტივა მხოლოდ ევროკავშირის წევრ სახელმწიფოებზე ვრცელდება, საჭირო იყო დამატებითი სამართლებრივი ინსტრუმენტის შექმნა პერსონალურ მონაცემთა დასაცავად, რომელსაც ამუშავებენ ევროკავშირის ინსტიტუტები და ორგანოები. ამ მიზანს ემსახურება რეგულაცია No. 45/2001 ევროკავშირის ინსტიტუტებისა და ორგანოების მიერ პერსონალური მონაცემების დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ (ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაცია).[39]

ეს რეგულაცია ზედმიწევნით ითვალისწინებს ევროკავშირის მონაცემთა დაცვის ზოგად პრინციპებს და მათ ავრცელებს ევროკავშირის ინსტიტუტებისა და ორგანოების მიერ მონაცემთა დამუშავებაზე საკუთარი ფუნქციების შესრულებისას; ასევე, იგი აფუძნებს დამოუკიდებელ საზედამხედველო ორგანოს - ევროკავშირის მონაცემთა დაცვის ზედამხედველი (EDPS) - რომელიც მონიტორინგს უწევს რეგულაციის დებულებათა გამოყენებას. EDPS-ს ენიჭება საზედამხედველო უფლებამოსილება და მოვალეობა, კერძოდ, მონიტორინ-

39 ევროპის პარლამენტისა და საბჭოს 2000 წლის 18 დეკემბრის რეგულაცია No. 45/2001 ევროკავშირის ინსტიტუტებისა და ორგანოების მიერ პერსონალური მონაცემების დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ 2001 L 8.

გი პერსონალურ მონაცემთა დამუშავებაზე ევროკავშირის ინსტიტუტებსა და ორგანოებში, ასევე, საჩივრების მოსმენა და შესწავლა მონაცემთა დაცვის წესების სავარაუდო დარღვევებზე; იგი კონსულტაციას უწევს ევროკავშირის ინსტიტუტებსა და ორგანოებს ყველა იმ საკითხზე, რომლებიც უკავშირდება პერსონალურ მონაცემთა დაცვას (მაგ.: ახალი კანონპროექტებისა და მონაცემთა დაცვის შიდა მარეგულირებელი წესების შემუშავება).

2017 წლის იანვარში ევროკომისიამ წარმოადგინა ახალი რეგულაციის პროექტი ევროკავშირის ინსტიტუტების მიერ მონაცემთა დამუშავებაზე, რომელიც აუქმებს არსებულ რეგულაციას. რაც შეეხება e-Privacy დირექტივის რეფორმას, No. 45/2001 რეგულაციის რეფორმირება უზრუნველყოფს ამ რეგულაციით დადგენილი წესების მოდერნიზებას, ასევე, შესაბამისობას ზოგადი რეგულაციის საფუძველზე შექმნილ მონაცემთა დაცვის ახალ რეჟიმთან.

ევროკავშირის მართლმსაჯულების სასამართლოს *(CJEU)* როლი

ევროკავშირის მართლმსაჯულების სასამართლოს (CJEU) იურისდიქციაში შედის როგორც იმის დადგენა, რამდენად ასრულებს წევრი სახელმწიფო ევროკავშირის მონაცემთა დაცვის კანონმდებლობით განსაზღვრულ ვალდებულებებს, ასევე ევროკავშირის კანონმდებლობის განმარტება - წევრი სახელმწიფოების მიერ მისი ეფექტიანი და ერთგვაროვანი გამოყენებისათვის. 1995 წელს მონაცემთა დაცვის დირექტივის მიღების შემდგომ დაგროვდა საკმაოდ მოცულობითი პრეცედენტული სამართალი, რომელიც, განმარტავს მონაცემთა დაცვის პრინციპებს, ასევე, ქარტიის მე-8 მუხლით გარანტირებული პერსონალურ მონაცემთა დაცვის უფლების მოქმედების სფეროსა და მნიშვნელობას. მიუხედავად იმისა, რომ დირექტივა ამჟამად გაუქმებულია და ამოქმედდა ახალი სამართლებრივი ინსტრუმენტი (მონაცემთა დაცვის ზოგადი რეგულაცია), მის გაუქმებამდე არსებული პრეცედენტული სამართალი კვლავ რელევანტურია: იგი ძალაში რჩება ევროკავშირის მონაცემთა დაცვის პრინციპების განმარტებასა და გამოყენებასთან მიმართებით, ვინაიდან დირექტივის პრინციპები და კონცეფციები შენარჩუნდა GDPR-ში.

1.2 პერსონალურ მონაცემთა დაცვაზე დაწესებული შეზღუდვები

ძირითადი საკითხები:

- პერსონალურ მონაცემთა დაცვის უფლება არ არის აბსოლუტური; მისი შეზღუდვა ნებადართულია საჯარო ინტერესის საფუძველზე, ან სხვათა უფლებებისა და თავისუფლებების დასაცავად.

- პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის უფლებების შეზღუდვის პირობები წარმოდგენილია ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლსა და ფუნდამენტურ უფლებათა ქარტიის 52-ე მუხლის პირველ პუნქტში. ისინი ვითარდება და განიმარტება ECtHR-ისა და CJEU-ს პრეცედენტული სამართლის საშუალებით.

- ევროპის საბჭოს მონაცემთა დაცვის კანონმდებლობის თანახმად, პერსონალურ მონაცემთა დამუშავება კანონიერი ჩარევაა პირადი ცხოვრების პატივისცემის უფლებაში და ის დაშვებულია, თუ დამუშავება:

  - ხორციელდება კანონის შესაბამისად;

  - კანონიერ მიზანს ემსახურება;

  - პატივს სცემს ფუნდამენტური უფლებებისა და თავისუფლებების არსს;

  - აუცილებელია დემოკრატიულ საზოგადოებაში კანონიერი მიზნის მისაღწევად და მისი პროპორციულია.

- ევროკავშირის სამართლებრივ სისტემაში ქარტიით დაცული ფუნდამენტური უფლებების განხორციელებაზე ვრცელდება მსგავსი შეზღუდვის პირობები. ფუნდამენტურ უფლებაზე, მათ შორის, პერსონალურ მონაცემთა დაცვის უფლებაზე დაწესებული ნებისმიერი შეზღუდვა ჩაითვლება კანონიერად, თუ იგი:

  - გათვალისწინებულია კანონით;

  - პატივს სცემს მონაცემთა დაცვის უფლების ძირითად არსს;

  - აუცილებელია და შეესაბამება პროპორციულობის პრინციპს;

  - ემსახურება ევროკავშირის მიერ აღიარებულ საჯარო ინტერესების მიზნებს, ან საჭიროა სხვათა უფლებებისა და თავისუფლებების დასაცავად.

პერსონალურ მონაცემთა დაცვის ფუნდამენტური უფლება, რომელსაც ადგენს ქარტიის მე-8 მუხლი, არ არის აბსოლუტური და „უნდა განიხილებოდეს საზოგადოებაში მისი ფუნქციის მიხედვით.“[40] ამრიგად, ქარტიის 52-ე მუხლის

40 იხ., მაგ: CJEU, გაერთიანებული საქმეები C-92/09 და C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 2010 წლის 9 ნოემბერი, პუნქტი 48.

პირველი პუნქტი უშვებს მე-7 და მე-8 მუხლებით დაცული უფლებების შეზღუდვას, თუ ის გათვალისწინებულია კანონით, პატივს სცემს ამ უფლებებისა და თავისუფლებების ძირითად არსს, შეესაბამება პროპორციულობის პრინციპს, აუცილებელია და რეალურად პასუხობს ევროკავშირის მიერ აღიარებული საჯარო ინტერესის მიზნებს ან სხვათა უფლებებისა და თავისუფლებების დაცვის საჭიროებას.[41] მსგავსად, ECHR-ის სისტემაში მონაცემთა დაცვა უზრუნველყოფილია მე-8 მუხლით, ხოლო ამ უფლების შეზღუდვა შესაძლებელია საჭიროების შემთხვევაში, კანონიერი მიზნის მისაღწევად. წინამდებარე ნაწილი განიხილავს ECHR-ით დაშვებულ შეზღუდვის პირობებს, განმარტებულს ადამიანის უფლებათა ევროპული სასამართლოს პრეცედენტულ სამართალში, და ქარტიის 52-ე მუხლით გათვალისწინებულ კანონიერი შეზღუდვის პირობებს.

1.2.1 გამართლებული ჩარევის მოთხოვნები ადამიანის უფლებათა ევროპული კონვენციის თანახმად

პერსონალურ მონაცემთა დამუშავება შეიძლება იყოს ჩარევა მონაცემთა სუბიექტის პირადი ცხოვრების პატივისცემის უფლებაში, რომელსაც იცავს ECHR-ის მე-8 მუხლი.[42] როგორც უკვე განიმარტა (იხ. ნაწილები 1.1.1 და 1.1.4), განსხვავებით ევროკავშირის სამართლებრივი სისტემისაგან, ECHR პერსონალურ მონაცემთა დაცვის უფლებას აცხადებს არა დამოუკიდებელ ფუნდამენტურ უფლებად, არამედ პირადი ცხოვრების პატივისცემის ფარგლებში დაცულ უფლებათა ნაწილად. ამრიგად, ნებისმიერი ოპერაცია, რომელიც პერსონალურ მონაცემთა დამუშავებას ითვალისწინებს, შეიძლება მოექცეს ECHR-ის მე-8 მუხლის მოქმედების სფეროში. ამ მუხლის ასამოქმედებლად, პირველ რიგში უნდა განისაზღვროს, მიადგა თუ არა ზიანი პიროვნების პირად ინტერესს ან ცხოვრებას. ECtHR თავის პრეცედენტულ სამართალში „პირადი ცხოვრების“ ცნებას ფართო კონცეფციად მიიჩნევს, რომელიც პროფესიული ცხოვრებისა და საჯარო ქცევის ასპექტებსაც მოიცავს. ევროპულმა სასამართლომ ასევე დაადგინა, რომ პერსონალურ მონაცემთა დაცვა პირადი ცხოვრების პატივისცემის უფლების მნიშვნელოვანი ნაწილია. თუმცა, პირადი ცხოვრების ფართო განმარტების მიუხედავად, მე-8 მუხლით დაცულ უფლებებს არ არღვევს ყველა ტიპის დამუშავება.

თუ ევროპული სასამართლო მიიჩნევს, რომ დამუშავების კონკრეტული ოპერაცია გავლენას ახდენს პირადი ცხოვრების პატივისცემის უფლებაზე, იგი განიხილავს, რამდენად გამართლებულია აღნიშნული ჩარევა. პირადი ცხო-

41 *იქვე,* პუნქტი 50.

42 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 და 30566/04, 2008 წლის 8 დეკემბერი, პუნქტი 67.

ვრების პატივისცემის უფლება არ არის აბსოლუტური - საჭიროა მისი დაბალანსება და დარეგულირება იმ კანონიერ ინტერესებსა და უფლებებთან, რომლებითაც სარგებლობს სხვა პირი (კერძო ინტერესები) ან ფართო საზოგადოება (საჯარო ინტერესები).

ჩარევა გამართლებულია, თუ:

შეესაბამება კანონმდებლობას

ECtHR-ის პრეცედენტული სამართლის თანახმად, ჩარევა კანონის შესაბამისია, თუ ეყრდნობა შიდასახელმწიფოებრივ კანონმდებლობას, რომელიც აკმაყოფილებს გაკრვეულ სტანდარტებს. კერძოდ, კანონი უნდა იყოს „ხელმისაწვდომი შესაბამისი პირებისათვის და შეიძლებოდეს მისი შედეგების განჭვრეტა.“ [43] წესი განჭვრეტადია, თუ „ის ფორმულირებულია საკმარისი სიზუსტით, რათა ნებისმიერ პირს ჰქონდეს საშუალება, საჭიროების შემთხვევაში, შესაბამისი მითითების საფუძველზე, დაარეგულიროს საკუთარი ქცევა.“[44] ამასთან, „ამ მხრივ, კანონმდებლობით დადგენილი სიზუსტის ხარისხი დამოკიდებულია განსახილველ საკითხზე.“ [45]

მაგალითები: საქმეში *Rotaru v. Romania*[46] განმცხადებელი აცხადებდა, რომ დაირღვა მისი პირადი ცხოვრების პატივისცემის უფლება, რადგან რუმინეთის სადაზვერვო სამსახურები ინახავდნენ და იყენებდნენ დოკუმენტს, რომელიც მის პერსონალურ ინფორმაციას შეიცავდა. ECtHR-მა დაადგინა, რომ შიდასახელმწიფოებრივი კანონმდებლობა იძლეოდა იმ ინფორმაციის შემცველი საიდუმლო ფაილების შეგროვების, ჩაწერისა და დაარქივების შესაძლებლობას, რომელიც გავლენას ახდენს ეროვ-

43 ECtHR, *Amann v. Switzerland* [GC], No. 27798/95, 2000 წლის 16 თებერვალი, პუნქტი 50; ასევე, ECtHR, *Kopp v. Switzerland,* No. 23224/94, 1998 წლის 25 მარტი, პუნქტი 55 და ECtHR, *Iordachi and Others v. Moldova,* No. 25198/02, 2009 წლის 10 თებერვალი, პუნქტი 50.

44 ECtHR, *Amann v. Switzerland* [GC], No. 27798/95, 2000 წლის 16 თებერვალი, პუნქტი 56; იხ. ასევე ECtHR, *Malone v. the United Kingdom,* No. 8691/79, 2 August 1984, პუნქტი. 66; ECtHR, *Silver and Others v. the United Kingdom*, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 1983 წლის 25 მარტი, პუნქტი 88.

45 ECtHR, *The Sunday Times v. the United Kingdom,* No. 6538/74, 1979 წლის 26 აპრილი, პუნქტი 49; ასევე, ECtHR, *Silver and Others v. the United Kingdom,* Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 1983 წლის 25 მარტი, პუნქტი 88.

46 ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 2000 წლის 4 მაისი, პუნქტი 57; ასევე, ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* No. 62540/00, 2007 წლის 28 ივნისი; ECtHR, *Shimovolos v. Russia,* No. 30194/09, 2011 წლის 21 ივნისი; და ECtHR, *Vetter v. France,* No. 59842/00, 2005 წლის 31 მაისი.

ნულ უსაფრთხოებაზე, თუმცა იგი არ განსაზღვრავდა რაიმე შეზღუდვას ამ უფლებამოსილებათა განხორციელებაზე, რაც შესაბამის ორგანოს აძლევდა შეხედულებისამებრ მოქმედების საშუალებას. მაგალითად, შიდასახელმწიფოებრივი კანონმდებლობა არ ადგენდა, კონკრეტულად რა სახის ინფორმაცია უნდა დამუშავებულიყო, რომელი კატეგორიის ადამიანების მიმართ გამოიყენებოდა თვალთვალის ზომები, რა პირობებში შეიძლებოდა ასეთი ზომების მიღება და როგორი პროცედურა უნდა დაცულიყო. შესაბამისად, სასამართლომ განმარტა, რომ შიდასახელმწიფოებრივი კანონმდებლობა არ აკმაყოფილებდა ევროპული კონვენციის მე-8 მუხლით განსაზღვრულ განჭვრეტადობის მოთხოვნას და დაადგინა მისი დარღვევა.

საქმეში *Taylor-Sabori v. the United Kingdom*[47] განმცხადებელი იყო პოლიციის თვალთვალის ქვეშ. მისი პეიჯერის „კლონის“ გამოყენებით, პოლიციამ მოიპოვა წვდომა განმცხადებლისთვის გაგზავნილ შეტყობინებებზე. იგი დააპატიმრეს და ბრალად წაუყენეს მონაწილეობა შეთანხმებაში ნარკოტიკული საშუალების მომარაგების შესახებ. სასამართლოზე პროკურატურის მიერ განმცხადებლის წინააღმდეგ წარდგენილ მტკიცებულებათა ნაწილი შედგებოდა პეიჯერით გაგზავნილი შეტყობინებებისგან, რომელიც გაშიფრა პოლიციამ. განმცხადებლის წინააღმდეგ სასამართლო პროცესის მიმდინარეობისას, ბრიტანულ კანონმდებლობაში არ არსებობდა დებულება, რომელიც დაარეგულირებდა პირადი სატელეკომუნიკაციო სისტემის მეშვეობით კომუნიკაციის ფარულ მოსმენას. შესაბამისად, განმცხადებლის უფლებაში ჩარევა არ იყო „კანონის შესაბამისი“. ECtHR-მა დაასკვნა, რომ ეს არღვევდა კონვენციის მე-8 მუხლს.

საქმე Vukota-Bojić v. Switzerland[48] შეეხებოდა იმ ადამიანის ფარულ თვალთვალს კერძო გამომძიებელთა მხრიდან, რომელიც სადაზღვევო ანაზღაურებას ითხოვდა. ECtHR-მა დაადგინა, რომ მართალია, თვალთვალი კერძო სადაზღვევო კომპანიის მითითებით ხორციელდებოდა, მაგრამ კომპანიას სახელმწიფომ მიანიჭა სავალდებულო სამედიცინო დაზღვევიდან გამომდინარე კომპენსაციის გაცემისა და სადაზღვევო პრემიის ამოღების უფლება. შესაბამისად, სახელმწიფო ვერ აირიდებდა კონვენციით ნაკისრ პასუხისმგებლობას საკუთარი ვალდებულებების კერძო ორგანოებისა თუ პირებისათვის დელეგირების გზით. შიდასახელმწიფოებრივმა კანონმდებლობამ საკმარისი დაცვის საშუალებები უნდა უზრუნველყოს, რათა აიცილოს კონვენციის მე-8 მუხლით დაცულ უფლებაში ბოროტად ჩარევა, „კანონთან შესაბამისობის“ საფუძვლით. განსახილველ საქმეში ECtHR-მა დაადგინა კონვენციის მე-8 მუხლის დარღვევა, რადგან შიდასახელმწიფოებრივი კანონმდებლობა საკმარისი სიცხადით არ ადგენდა

47 ECtHR, *Taylor-Sabori v. the United Kingdom,* No. 47114/99, 2002 წლის 22 ოქტომბერი.

48 ECtHR, *Vukota-Bojić v. Switzerland*, No. 61838/10, 2016 წლის 18 ოქტომბერი, პუნქტი 77.

დაზღვეული პირის ფარული თვალთვალის შემთხვევაში იმ სადაზღვევო კომპანიებისათვის მინიჭებული დისკრეციული უფლებამოსილების ფორმას, რომლებიც სადაზღვევო დავებში მოქმედებენ საჯარო ხელისუფლების სახელით.

მოქმედებს კანონიერი მიზნებით

კანონიერი მიზანი შეიძლება იყოს დასახელებულ საჯარო ინტერესებს შორის ერთ-ერთი, ან სხვათა უფლებებისა და თავისუფლებების დაცვა. კონვენციის მე-8 მუხლის მე-2 პუნქტის თანახმად, კანონიერი მიზნები, რომლებიც ამართლებს ჩარევას, მოიცავს შემდეგ საკითხებს: საზოგადოებრივი უსაფრთხოება ან ქვეყნის ეკონომიკური კეთილდღეობა; საზოგადოებრივი წესრიგის დარღვევის ან დანაშაულის თავიდან აცილება; ჯანმრთელობის, ზნეობისა თუ სხვათა უფლებებისა და თავისუფლებების დაცვა.

მაგალითი: საქმეში Peck v. the United Kingdom[49] განმცხადებელმა გადაწყვიტა, თავის მოკვლის მიზნით ქუჩაში ვენები გადაეჭრა. მან არ იცოდა, რომ ამ დროს ვიდეომეთვალყურეობის კამერა უღებდა. პოლიციელებმა, რომლებიც კამერებს უყურებდნენ, იგი გადაარჩინეს, კამერიდან ამოღებული ჩანაწერი კი მედიას გადასცეს. მედიამ ჩანაწერი გამოაქვეყნა ისე, რომ განმცხადებლის სახე არ დაუფარავს. ECtHR-მა განაცხადა, რომ არ არსებობდა სათანადო ან საკმარისი მიზეზი, რომელიც გაამართლებდა ხელისუფლების მიერ ვიდეოჩანაწერის გასაჯაროებას, განმცხადებლის თანხმობის ან მისი ვინაობის დაფარვის გარეშე. სასამართლომ საქმეზე დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

აუცილებელია დემოკრატიულ საზოგადოებაში

ECtHR-ის განმარტებით, „აუცილებლობის ცნება გულისხმობს, რომ ჩარევა შეესაბამება გადაუდებელ სოციალურ საჭიროებას, კერძოდ, კანონიერი მიზნის პროპორციულია.“[50] იმის შეფასებისას, რამდენად აუცილებელია კონკრეტული ღონისძიება გადაუდებელ სოციალურ საჭიროებაზე რეაგირებისათვის, ECtHR განიხილავს ღონისძიების შესაფერისობას, ასევე, შესაბამისობას მისაღწევ მიზანთან. ამ კუთხით, იგი შეისწავლის: არის თუ არა ჩარევის მიზანი იმ პრობლემაზე რეაგირება, რომელიც, ჩაურევლად, ზიანს მოუტანდა საზოგადოებას; რამდენად არსებობს მტკიცებულება, რომ ჩარევა შეამცირებს საზია-

49 ECtHR, *Peck v. the United Kingdom,* No. 44647/98, 2003 წლის 28 იანვარი, პუნქტი 85.

50 ECtHR, *Leander v. Sweden,* No. 9248/81, 1987 წლის 26 მარტი, პუნქტი 58.

ნო შედეგს; და როგორია ფართო საზოგადოების შეხედულება ამ პრობლემის მიმართ[51] (მაგ.: უსაფრთხოების სამსახურების მიერ პერსონალურ მონაცემთა შეგროვება და შენახვა კონკრეტულად იმ ადამიანზე, რომლის კავშირიც ტერორისტულ მოძრაობასთან დადგენილია, მიიჩნევა ჩარევად პირადი ცხოვრების პატივისცემის უფლებაში, თუმცა, ეს ემსახურება სერიოზულ, გადაუდებელ სოციალურ საჭიროებას - ეროვნულ უსაფრთხოებასა და ტერორიზმის წინააღმდეგ ბრძოლას). აუცილებლობის ტესტის მოთხოვნათა დასაკმაყოფილებლად, ჩარევა უნდა იყოს პროპორციული. ECtHR-ის პრეცედენტულ სამართალში პროპორციულობა აუცილებლობის კონცეფციის კონტექსტში ფასდება. ის მოითხოვს, რომ კონვენციით დაცულ უფლებაში ჩარევის მასშტაბი არ იყოს იმაზე მეტი, ვიდრე საჭიროა კანონიერი მიზნის მისაღწევად. პროპორციულობის ტესტთან შესაბამისობის კუთხით გასათვალისწინებელია შემდეგი მნიშვნელოვანი ფაქტორები: ჩარევის მასშტაბი, განსაკუთრებით, იმ ადამიანთა რაოდენობა, რომლებსაც ეხებათ ჩარევა; და დამცავი ან წინასწარი გაფრთხილების (caveats) მექანიზმები, რომლებიც ზღუდავს ჩარევის მასშტაბს ან უარყოფით გავლენას ადამიანის უფლებაზე.[52]

მაგალითები: საქმეში *Khelili v. Switzerland*[53] პოლიციის მიერ ჩატარებული შემოწმებისას განმცხადებელს აღმოაჩნდა სავიზიტო ბარათები შემდეგი წარწერით: „სასიამოვნო, ორმოც წლამდე ასაკის ლამაზი ქალი გაიცნობს მამაკაცს სასმელის დალევის ან დროდადრო გასეირნების მიზნით. ტელეფონის ნომერი [...]“. განმცხადებელი აცხადებდა, რომ პოლიციამ იგი თავის ჩანაწერებში შეიყვანა, როგორც სექსმუშაკი, რასაც თვითონ კატეგორიულად უარყოფდა. იგი ითხოვდა, პოლიციის კომპიუტერული ჩანაწერებიდან წაეშალათ სიტყვა „სექსმუშაკი“. ECtHR-მა დაადგინა, რომ ზოგადად, ადამიანის პერსონალური მონაცემების შენახვა იმ საფუძვლით, რომ შეიძლება სხვა დანაშაული ჩაიდინოს, გარკვეულ გარემოებებში პროპორციულად ითვლება, თუმცა, განმცხადებლის შემთხვევაში, უკანონო პროსტიტუციის შესახებ ბრალდება ზედმეტად ბუნდოვანი და ზოგადი იყო. ეს ბრალდება არ მყარდებოდა რაიმე კონკრეტული ფაქტებით, რადგან განმცხადებელი პროსტიტუციისთვის არასდროს გასამართლებულა. შესაბამისად, ეს ვერ აკმაყოფილებდა „გადაუდებელი სოციალური საჭიროების“ მოთხოვნას კონვენციის მე-8 მუხლის მნიშვნელობის ფარგლებში. სასამართლომ განაცხადა, რომ სამართალდამცვე-

51 29-ე მუხლის მონაცემთა დაცვის სამუშაო ჯგუფი (29-ე მუხლის სამუშაო ჯგუფი) (2014), მოსაზრება სამართალდამცველ სექტორში საჭიროებისა და პროპორციულობის კონცეფციების გამოყენებისა და მონაცემთა დაცვის შესახებ, WP 211, ბრიუსელი, 2014 წლის 27 თებერვალი, გვ. 7–8.

52 *იქვე,* გვ. 9–11.

53 ECtHR, *Khelili v. Switzerland,* No. 16188/07, 2011 წლის 18 ოქტომბერი.

ლი ორგანოების მოვალეობაში შედიოდა განმცხადებელზე შენახული მონაცემების სისწორის დამტკიცება, გაითვალისწინა განმცხადებლის უფლებებში ჩარევის სიმძიმე და დაასკვნა, რომ წლების განმავლობაში სიტყვა „სექსმუშაკის“ შენახვა პოლიციის ფაილებში არ იყო აუცილებელი დემოკრატიულ საზოგადოებაში. შესაბამისად, სასამართლომ საქმეზე დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

საქმეში *S. and Marper v. the United Kingdom*[54] ორი განმცხადებელი სისხლის სამართლის დანაშაულის ბრალდებით დააპატიმრეს. პოლიციამ მათგან თითის ანაბეჭდები და დნმ-ის ნიმუშები აიღო, „პოლიციისა და სისხლის სამართლის მტკიცებულებათა აქტის“ შესაბამისად. ბრალი არ დაუმტკიცდათ: ერთი სასამართლომ უდანაშაულოდ ცნო, ხოლო მეორე განმცხადებლის მიმართ აღძრული სისხლისსამართლებრივი დევნა შეწყდა. მიუხედავად ამისა, მათი ანაბეჭდები, დნმ-ის პროფილები და უჯრედოვანი ნიმუშები დაიტოვეს და შეინახეს პოლიციის მონაცემთა ბაზაში, ხოლო ეროვნული კანონმდებლობის თანახმად, ამ მონაცემების შენახვა შესაძლებელი იყო უვადოდ. მოპასუხე (გაერთიანებული სამეფო) აცხადებდა, რომ მონაცემების შენახვა სამომავლოდ დამნაშავეთა იდენტიფიკაციას უწყობდა ხელს და, შესაბამისად, დანაშაულის პრევენციისა და გამოვლენის კანონიერ მიზნას ემსახურებოდა. სასამართლომ დაადგინა, რომ განმცხადებლის პირადი ცხოვრების პატივისცემის უფლებაში ჩარევა გაუმართლებელი იყო. კერძოდ, მან აღნიშნა, რომ მონაცემთა დაცვის ძირითადი პრინციპების თანახმად, პერსონალური მონაცემების შენახვა უნდა იყოს შეგროვების მიზნის პროპორციული, შენახვის ვადა კი - შეზღუდული. სასამართლოს აზრით, მონაცემთა ბაზის განვრცობა იმგვარად, რომ მოიცვას არა მხოლოდ მსჯავრდებულთა, არამედ იმ ადამიანთა დნმ-ის პროფილებიც, რომლებსაც ბრალი წარედგინათ, მაგრამ არ დაუმტკიცდათ, სავარაუდოდ, ხელს შეუწყობდა გაერთიანებულ სამეფოში დანაშაულის გამოვლენასა და პრევენციას. თუმცა, სასამართლო „გაოცებული იყო [მონაცემთა] შენახვის უფლებამოსილების ბლანკეტურობითა და განურჩევლობით.“ [55]

იმის გათვალისწინებით, რომ უჯრედულ ნიმუშებში ინახება დიდი მოცულობის გენეტიკური და ჯანმრთელობასთან დაკავშირებული ინფორმაცია, განმცხადებლის პირადი ცხოვრების პატივისცემის უფლებაში ჩარევა იყო განსაკუთრებით ინვაზიური. შესაძლებელია დაპატიმრებული ადამიანის თითის ანაბეჭდებისა და ნიმუშების აღება და განუსაზღვრელი პერიოდით შენახვა პოლიციის მონაცემთა ბაზაში, მიუხედავად დანაშაულის

54 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 და 30566/04, 2008 წლის 4 დეკემბერი.

55 *იქვე*, პუნქტი 119.

ბუნებისა და სიმძიმისა (მსუბუქი დანაშაულების შემთხვევაშიც კი, რომელიც არ ისჯება თავისუფლების აღკვეთით). ამასთან, ფიზიკური პირის შესაძლებლობა, მოეთხოვა თავისი მონაცემების წაშლა შესაბამისი ბაზიდან, იყო შეზღუდული. დაბოლოს, ECtHR-მა განსაკუთრებული ყურადღება დაუთმო ფაქტს, რომ ერთ-ერთი განმცხადებელი 11 წლის გახლდათ დაპატიმრებისას. იმ მცირეწლოვნის პერსონალური მონაცემების შენახვა, რომელსაც დანაშაული არ დაუმტკიცდა, შესაძლოა განსაკუთრებით საზიანო იყოს მათი მოწყვლადობის, განვითარებისა და საზოგადოებაში ინტეგრაციის გათვალისწინებით.[56] სასამართლომ ერთხმად დაადგინა, რომ მონაცემთა შენახვა იყო არაპროპორციული ჩარევა პირადი ცხოვრების პატივისცემის უფლებაში, რაც ვერ იქნებოდა აუცილებელი დემოკრატიულ საზოგადოებაში.

საქმეში *Leander v. Sweden*[57] ECtHR-მა დაადგინა, რომ იმ პიროვნებების ფარული შემოწმება, რომლებსაც სურთ თანამდებობის დაკავება ეროვნული უსაფრთხოების სისტემაში, თავისი არსით არ ეწინააღმდეგებოდა აუცილებლობის მოთხოვნას დემოკრატიულ საზოგადოებაში. მონაცემთა სუბიექტის ინტერესების დასაცავად, ეროვნული კანონმდებლობის მიერ განსაზღვრული უსაფრთხოების ზომების საფუძველზე (მაგ.: კონტროლი პარლამენტისა და იუსტიციის კანცლერის მხრიდან), სასამართლომ დაასკვნა, რომ პერსონალის კონტროლის შვედური სისტემა შეესაბამებოდა კონვენციის მე-8 მუხლის მე-2 პუნქტის მოთხოვნებს. მისთვის ხელმისაწვდომი ფართო დისკრეციული უფლებამოსილების გათვალისწინებით, მოპასუხე სახელმწიფოს ჰქონდა უფლება, დაედგინა, რომ განმცხადებლის საქმეში ეროვნული უსაფრთხოების ინტერესები იდგა პირად ინტერესებზე მაღლა. სასამართლომ დაადგინა, რომ კონვენციის მე-8 მუხლი არ დარღვეულა.

1.2.2 კანონიერი შეზღუდვის პირობები ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის შესაბამისად

ქარტიის სტრუქტურა და ტექსტი განსხვავდება ადამიანის უფლებათა ევროპული კონვენციისაგან. ქარტია არ იყენებს აღიარებულ უფლებებში ჩარევის ცნებას, თუმცა, მოიცავს დებულებებს მისი მოქმედების ფარგლებში გათვალისწინებული უფლებებისა და თავისუფლებების შეზღუდვაზე.

52-ე მუხლის პირველი პუნქტის თანახმად, ქარტიით აღიარებული უფლებები-

56 *იქვე,* პუნქტი 124.

57 ECtHR, *Leander v. Sweden,* No. 9248/81, 1987 წლის 26 მარტი, პუნქტები 59 და 67.

სა და თავისუფლებების და, შესაბამისად, პერსონალურ მონაცემთა დაცვის უფლების შეზღუდვა ნებადართულია, თუ იგი:

- გათვალისწინებულია კანონით;
- პატივს სცემს მონაცემთა დაცვის უფლების არსს;
- აუცილებელია და შეესაბამება პროპორციულობის პრინციპს; [58]
- ემსახურება ევროკავშირის მიერ აღიარებულ საჯარო ინტერესის მიზნებს, ან საჭიროა სხვათა უფლებებისა და თავისუფლებების დასაცავად.

ვინაიდან ევროკავშირის სამართლებრივ სისტემაში პერსონალურ მონაცემთა დაცვა განსხვავებული და დამოუკიდებელი ფუნდამენტური უფლებაა, რომელსაც ქარტიის მე-8 მუხლი იცავს, პერსონალურ მონაცემთა დამუშავების ნებისმიერი შემთხვევა მიიჩნევა ამ უფლებაში ჩარევად. არ აქვს არსებითი მნიშვნელობა, რამდენად უკავშირდება პერსონალური მონაცემები ადამიანის პირად ცხოვრებას, განსაკუთრებული კატეგორიის მონაცემია თუ არა, ან ხომ არ შეექმნა რაიმე უხერხულობა მონაცემთა სუბიექტს. ჩარევის კანონიერებისათვის, იგი უნდა აკმაყოფილებდეს ქარტიის 52-ე მუხლის პირველი პუნქტით გათვალისწინებულ ყველა პირობას.

კანონთან შესაბამისობა

პერსონალურ მონაცემთა დაცვის უფლებაზე დაწესებულ შეზღუდვებს კანონი უნდა არეგულირებდეს. ეს მოთხოვნა გულისხმობს, რომ შეზღუდვას უნდა ჰქონდეს სამართლებრივი საფუძველი, რომელიც ხელმისაწვდომია, განჭვრეტადი და საკმარისი სიცხადით ფორმულირებული, რაც ფიზიკურ პირებს აძლევს საკუთარი მოვალეობების გააზრებისა და ქმედებათა დარეგულირების შესაძლებლობას. სამართლებრივი საფუძველი მკაფიოდ უნდა განმარტავდეს შესაბამისი ორგანოს მიერ უფლებამოსილების განხორციელების მასშტაბსა და ფორმას, რაც ფიზიკურ პირებს იცავს თვითნებური ჩარევისგან. ეს განმარტება ჰგავს ECtHR-ის პრეცედენტულ სამართალში გათვალისწინებულ მოთხოვნას „კანონიერი ჩარევის“ შესახებ[59] და არსებობს მოსაზრება, რომ შინაარსი ქარტიაში გამოყენებული ფრაზისა „კანონით გათვალისწინებული“ უნდა ჰგავდეს ECHR-ით მინიჭებულ მნიშვნელობას.[60] ECtHR-ის პრეცედენტუ-

58 იმ ღონისძიებების საჭიროების შეფასება, რომლებიც პერსონალურ მონაცემთა დაცვის ფუნდამენტურ უფლებას ზღუდავს, იხ. EDPS (2017), Necessity Toolkit, ბრიუსელი, 2017 წლის 11 აპრილი.

59 EDPS (2017), *Necessity Toolkit, Brussels,* 2017 წლის 11 აპრილი, გვ. 4; ასევე, იხ. CJEU, სასამართლოს მოსაზრება 1/15 (დიდი პალატა), 2017 წლის 26 ივლისი.

60 CJEU, გაერთიანებული საქმეები C-203/15 და C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, გენერალური ადვოკატის მოსაზრება, 2016 წლის 19 ივლისი, პუნქტი 140.

ლი სამართალი, განსაკუთრებით, „კანონის ხარისხის“ კონცეფცია, რომელიც წლების განმავლობაში ჩამოყალიბდა, რელევანტური საკითხია, რომელიც უნდა გაითვალისწინოს CJEU-მ ქარტიის 52-ე მუხლის პირველი პუნქტის ფარგლებზე მსჯელობისას.[61]

უფლების არსის პატივისცემა

ევროკავშირის სამართლებრივ სისტემაში ქარტიით დაცული ფუნდამენტური უფლების ნებისმიერი შეზღუდვა ამ უფლების არსს უნდა სცემდეს პატივს. კერძოდ, ისეთი ფართო და ინვაზიური შეზღუდვა, რომელიც ფუნდამენტურ უფლებას ძირითად არსს ართმევს, ვერ გამართლდება. თუ ზიანდება უფლების არსი, შეზღუდვა უკანონოდ უნდა ჩაითვალოს. საჭირო არ არის შემდგომი შეფასება, რამდენად ემსახურება იგი საჯარო ინტერესის მიზანს და აკმაყოფილებს თუ არა აუცილებლობისა და პროპორციულობის კრიტერიუმს.

მაგალითები: *Schrems-ის* საქმე[62] შეეხებოდა ფიზიკური პირების დაცვას და მათი პერსონალური მონაცემების მესამე ქვეყნისთვის (ამ შემთხვევაში - აშშ) გადაცემას. შრემსი იყო ავსტრიის მოქალაქე, რომელიც წლების განმავლობაში იყენებდა სოციალურ ქსელს Facebook. მან საჩივარი შეიტანა ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანოში, იმის გამო, რომ მისი პერსონალური მონაცემები Facebook-ის ადგილობრივმა შვილობილმა კომპანიამ გადასცა Facebook Inc.-ს და აშშ-ში მდებარე სერვერებს, სადაც მუშავდება ასეთი მონაცემები. იგი ამტკიცებდა, რომ ამერიკელი „მამხილებლის“ (whisleblower) ედვარდ სნოუდენის 2013 წლის სკანდალის გათვალისწინებით, რომელიც აშშ-ს სადაზვერვო სამსახურების საქმიანობას შეეხებოდა, აშშ-ში არსებული კანონმდებლობა და პრაქტიკა არ ითვალისწინებდა მის ტერიტორიაზე გადაცემული პერსონალური მონაცემების საკმარისად დაცვას. სნოუდენმა გამოააშკარავა, რომ ეროვნული უსაფრთხოების სააგენტო აწარმოებდა ისეთი ფირმების სერვერების პირდაპირ მიყურადებას, როგორიცაა Facebook და, სავარაუდოდ, კითხულობდა მიმოწერასა და პირად მესიჯებს.

მონაცემთა აშშ-სთვის გადაცემა ეფუძნებოდა კომისიის გადაწყვეტილებას შესაბამისობის შესახებ, რომელიც მიღებულია 2000 წელს და იძლევა მონაცემთა გადაცემის ნებართვას ამერიკულ კომპანიებზე, რომლებიც აცხა-

61 CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs compositeurs et éditeurs (SABAM)*, გენერალური ადვოკატის ცრუზ ვილალონის მოსაზრება, 2011 წლის 14 აპრილი, პუნქტი 100.

62 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 5 ოქტომბერი.

დებდნენ, რომ დაიცავდნენ ევროკავშირიდან მიღებულ პერსონალურ მონაცემებს და შეასრულებდნენ ე.წ. „უსაფრთხო ნავსადგომის პრინციპებს“. CJEU-მ საქმის განხილვისას შეისწავლა კომისიის გადაწყვეტილების მართებულობა ქარტიის გათვალისწინებით. სასამართლოს განმარტებით, ევროკავშირში ფუნდამენტური უფლებების დაცვა მოითხოვს, რომ ისინი შეიზღუდოს მხოლოდ მკაცრად აუცილებელი მოცულობით. CJEU-ს განცხადებით, კანონმდებლობა, რომელიც ხელისუფლებას აძლევს ზოგადი წვდომის საშუალებას ელექტრონული კომუნიკაციების შინაარსზე, „აზიანებს პირადი ცხოვრების პატივისცემის ფუნდამენტური უფლების არსს, გარანტირებულს ქარტიის მე-7 მუხლით.“ აღნიშნული უფლება დაკარგავს მნიშვნელობას, თუ აშშ-ს ხელისუფლებას კაზუალური წვდომა ექნება კომუნიკაციებზე, იმ ყოველგვარი ობიექტური გამართლების გარეშე, რომელიც ეფუძნება ეროვნული უსაფრთხოების კონკრეტულ ინტერესებს ან დანაშაულის პრევენციას, კონკრეტულ პირთან მიმართებით და მაშინ, თუ მიყურადების ასეთ პრაქტიკა იარსებებს უფლებამოსილების ბოროტად გამოყენებისგან დაცვის სათანადო მექანიზმების გარეშე. ამასთან, CJEU-მ განაცხადა, რომ „კანონმდებლობა, რომელიც ფიზიკურ პირს არ აძლევს სამართლებრივი დაცვის საშუალებათა გამოყენების შესაძლებლობას - ჰქონდეს ხელმისაწვდომობა მის შესახებ არსებულ პერსონალურ მონაცემებზე, ან მოითხოვოს ასეთი მონაცემების შესწორება ან წაშლა - არ შეესაბამება ეფექტიანი სამართლებრივი დაცვის ფუნდამენტურ უფლებას (ქარტიის 47-ე მუხლი).“ ამრიგად, „უსაფრთხო ნავსადგომის გადაწყვეტილებით“, აშშ ვერ დაიცავდა ფუნდამენტურ უფლებებს იმ დონეზე, რომელიც გარანტირებულია ევროკავშირის დირექტივით, ქარტიასთან ერთობლიობაში. შესაბამისად, CJEU-მ გადაწყვეტილება გამოაცხადა ძალადაკარგულად.[63]

შპს *Digital Rights Ireland-ის* საქმეში[64] CJEU-მ განიხილა 2006/24/EC დირექტივის (მონაცემთა შენახვის დირექტივა) შესაბამისობა ქარტიის მე-7 და მე-8 მუხლებთან. დირექტივა ელექტრონული კომუნიკაციის პროვაიდერებს ავალდებულებდა, შეენახათ გადაადგილებისა და ადგილმდებარეობის განმსაზღვრელი მონაცემები, მინიმუმ, 6 და, მაქსიმუმ, 24 თვის

63 CJEU-ს გადაწყვეტილება კომისიის 520/2000/EC გადაწყვეტილების გაუქმებაზე ეფუძნებოდა სხვა მიზეზებსაც, რომლებიც განხილულია ამ სახელმძღვანელოს სხვა თავებში. აღსანიშნავია, რომ CJEU-ს შეფასებით, გადაწყვეტილება უკანონოდ ზღუდავდა მონაცემთა დაცვის საზედამხედველო ორგანოს ძალაუფლებას. ამასთან, „უსაფრთხო ნავსაყუდელის“ რეჟიმის ფარგლებში, პირს არ მიუწვდება ხელი სამართლებრივი დაცვის საშუალებებზე, თუ ითხოვს მის შესახებ არსებულ პერსონალურ მონაცემებზე წვდომას და/ან მათ შესწორებას/წაშლას. ამრიგად, შეიზღუდა ეფექტიანი სამართლებრივი დაცვის ფუნდამენტური უფლებაც, რომელსაც იცავს ქარტიის 47-ე მუხლი.

64 CJEU, გაერთიანებული საქმეები *C-293/12 და C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი.

განმავლობაში, რაც უფლებამოსილ სახელისუფლებო ორგანოს შესაძლებლობას მისცემდა, ამ მონაცემებზე წვდომა ჰქონოდა მძიმე დანაშაულის პრევენციის, გამოძიების, გამოვლენისა და დამნაშავეთა დასჯის მიზნით. დირექტივა ელექტრონული კომუნიკაციების შინაარსის შენახვის უფლებას არ იძლეოდა. CJEU-მ აღნიშნა, რომ მონაცემები, რომლებიც პროვაიდერებს უნდა შეენახათ დირექტივის შესაბამისად, მოიცავდა შემდეგ საკითხებს: კომუნიკაციის წყარო და დანიშნულების ადგილის მოძებნისა და იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის თარიღი, დრო და ხანგრძლივობა; ინფორმაცია, თუ რა ნომერზე და რა ნომრიდან განხორციელდა ზარი; და IP მისამართი. ეს მონაცემები, „ერთად აღებული, იძლევა ძალიან ზუსტი დასკვნების გაკეთების [შესაძლებლობას] იმ ადამიანთა პირად ცხოვრებაზე, რომელთა მონაცემებიც შეინახეს (მათ შორის, ისეთ დეტალებზე, როგორიცაა ყოველდღიური ჩვევები, მუდმივი ან დროებითი საცხოვრებელი, ყოველდღიური თუ სხვა გადაადგილება, აქტივობები, სოციალური კავშირები და ის სოციალური გარემო, სადაც ხშირად იმყოფებიან.“

ამრიგად, დირექტივის საფუძველზე, პერსონალური მონაცემების შენახვა იყო მძიმე ჩარევა პირადი ცხოვრებისა და მონაცემების დაცვის უფლებაში. თუმცა, CJEU-მ დაადგინა, რომ ეს ჩარევა არსებით უარყოფით გავლენას არ ახდენდა ამ უფლებებზე. კერძოდ, არ ზიანდებოდა პირადი ცხოვრების უფლების არსი, რადგან დირექტივა არ იძლეოდა ელექტრონული კომუნიკაციების შინაარსის მოპოვების შესაძლებლობას. ასევე არ ზიანდებოდა პერსონალურ მონაცემთა დაცვის უფლებაც, რადგან დირექტივა ელექტრონული კომუნიკაციების პროვაიდერებს ავალდებულებდა, რომ გაეთვალისწინებინათ მონაცემთა დაცვისა და უსაფრთხოების გარკვეული პრინციპები და ამ მიზნით გაეტარებინათ სათანადო ტექნიკური და ორგანიზაციული ღონისძიებები.

აუცილებლობა და პროპორციულობა

ქარტიის 52-ე მუხლის პირველი პუნქტის თანახმად, ამ დოკუმენტით აღიარებულ ფუნდამენტურ უფლებებსა და თავისუფლებებზე შეზღუდვების დაწესება შესაძლებელია მხოლოდ აუცილებლობის შემთხვევაში. ამასთან, ის უნდა შეესაბამებოდეს პროპორციულობის პრინციპს.

შეზღუდვა შეიძლება აუცილებელი იყოს, თუ საჯარო ინტერესის მიზნის მისაღწევად საჭიროა ღონისძიებების გატარება. თუმცა, CJEU-ს განმარტებით, საჭიროება გულისხმობს იმასაც, რომ მიღებული ზომა იყოს ყველაზე ნაკლებად ინვაზიური/ჩარევითი, ამ მიზნის მისაღწევ სხვა ღონისძიებებს შორის. პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის უფლებების შეზღუდვებთან მიმართებით, CJEU იყენებს მკაცრი აუცილებლობის ტესტს და

აცხადებს, რომ „[უფლების] შემცირებას და შეზღუდვას უნდა მიმართონ მხოლოდ მაშინ, როდესაც ეს მკაცრად აუცილებელია.“ თუ შეზღუდვა მკაცრად აუცილებლად ჩაითვლება, საჭიროა, შეფასდეს მისი პროპორციულობაც.

პროპორციულობა ნიშნავს, რომ შეზღუდვის შედეგად მიღებული სარგებელი გადაწონის ზიანს, რომელსაც ის აყენებს ფუნდამენტურ უფლებას.[65] პირადი ცხოვრების პატივისცემისა და მონაცემთა დაცვის უფლებების ზიანისა და რისკების შესამცირებლად, მნიშვნელოვანია, შეზღუდვა მოიცავდეს დაცვის სათანადო მექანიზმებს.

მაგალითები: საქმეში *Volker und Markus Schecke*[66] CJEU-მ დაადგინა, რომ პერსონალურ მონაცემთა გამოქვეყნების ვალდებულების დაკისრებით თითოეული ფიზიკური პირის შესახებ, რომელიც კონკრეტული სასოფლო-სამეურნეო ფონდის დახმარების ბენეფიციარი იყო - მიუხედავად იმისა, როდის და როგორი ტიპის დახმარება მიიღო მან, ასევე, რა სიხშირითა და ოდენობით - საბჭომ და კომისიამ გადააჭარბეს პროპორციულობის პრინციპით დაწესებულ ზღვარს. შესაბამისად, CJEU-მ საჭიროდ მიიჩნია, საბჭოს (EC) No. 1290/2005 რეგულაციის გარკვეული დებულებები ძალადაკარგულად გამოეცხადებინა, ხოლო რეგულაცია No. 259/2008 მთლიანად გაეუქმებინა.[67]

საქმეში *Digital Rights Ireland*[68] CJEU-მ დაადგინა, რომ მონაცემთა შენახვის დირექტივის საფუძველზე პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევა არ აზიანებდა მის არსს, ვინაიდან დირექტივამ აკრძალა ელექტრონული კომუნიკაციების შინაარსის შენახვა. თუმცა, სასამართლომ ასევე დაასკვნა, რომ დირექტივა არ შეესაბამებოდა ქარტიის მე-7 და მე-8 მუხლებს და იგი გაუქმებულად გამოაცხადა, ვინაიდან გადაადგილებისა და ადგილმდებარეობის განმსაზღვრელ მონაცემთა შეგროვე-

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

66 CJEU, გაერთიანებული საქმეები C-92/09 და C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 2010 წლის 9 ნოემბერი, პუნქტები 89 და 86

67 საბჭოს 2005 წლის 21 ივნისის რეგულაცია (EC) No. 1290/2005 საერთო სასოფლო სამეურნეო პოლიტიკის დაფინანსებაზე, OJ 2005 L 209; კომისიის 2008 წლის 18 მარტის რეგულაცია (EC) No. 259/2008, რომელიც ადგენს დეტალურ წესებს საბჭოს რეგულაციის (EC) No. 1290/2005 გამოყენებასთან დაკავშირებით, კერძოდ, ინფორმაციის გამოქვეყნებაზე იმ ფონდის ბენეფიციარების შესახებ, რომელიც შექმნილია ევროპული სასოფლო-სამეურნეო საგარანტიო ფონდისა (EAGF) და სოფლის განვითარების ევროპული სასოფლო-სამეურნეო ფონდის (EAFRD) საფუძველზე OJ 2008 L 76.

68 CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი, პუნქტი 39.

ბისა და გაანალიზების შედეგად, შეიძლება შეიქმნას დეტალური სურათი პირის პირადი ცხოვრების შესახებ, რაც მძიმე ჩარევაა მე-7 და მე-8 მუხლებით დაცულ უფლებებში. CJEU-მ გაითვალისწინა, რომ დირექტივა აწესებდა მოთხოვნას ყველა იმ მეტამონაცემის შენახვაზე, რომლებიც უკავშირდება ფიქსირებულ და მობილურ ტელეფონებს, ინტერნეტით სარგებლობას, ელფოსტასა და ინტერნეტტელეფონს - ყველა სახის ელექტრონულ კომუნიკაციას, რომლებსაც ადამიანები ყოველდღიურ ცხოვრებაში საკმაოდ ხშირად იყენებენ. პრაქტიკულად, ეს იყო ჩარევა, რომელიც ევროპის მთლიან მოსახლეობაზე ახდენდა გავლენას. ჩარევის მასშტაბისა და სერიოზულობის გათვალისწინებით, გადაადგილებისა და ადგილმდებარეობის განმსაზღვრელი მონაცემების შენახვა, CJEU-ს განმარტებით, გამართლებულია მხოლოდ მძიმე დანაშაულთან საბრძოლველად. ამასთან, დირექტივა არ ითვალისწინებდა რაიმე ობიექტურ კრიტერიუმს, რომლითაც შეიზღუდებოდა შესაბამისი ადგილობრივი ორგანოების წვდომა შენახულ მონაცემებზე, მკაცრი აუცილებლობის შესაბამისად; არც ცალკეულ არსებით და პროცედურულ დებულებებს შეიცავდა, რომლებიც დაარეგულირებდა ამ ორგანოების წვდომას შენახულ მონაცემებზე და მათ გამოყენებას, რაც არ იყო დამოკიდებული სასამართლოს ან სხვა დამოუკიდებელი ორგანოს მიერ წინასწარ განხილვაზე.

CJEU იმავე დასკვნამდე მივიდა გაერთიანებულ საქმეებში *Tele2 Sverige AB v. Post-och telestryrelsen* და *Secretary of State for the Home Department v. Tom Watson and Others*,[69] რომლებიც შეეხებოდა გადაადგილებისა და ადგილმდებარეობის განმსაზღვრელი მონაცემების შენახვას „ყველა გამომწერსა თუ რეგისტრირებულ მომხმარებელთან და ელექტრონული კომუნიკაციების საშუალებასთან დაკავშირებით, ასევე, მეტამონაცემებს [შენახვას]“, „დიფერენციაციის, შეზღუდვის ან გამონაკლისების გარეშე, მისაღწევი მიზნის შესაბამისად.“[70] ამ საქმეებში მონაცემთა შენახვის წინაპირობა არ გახლდათ პიროვნების პირდაპირი ან ირიბი კავშირი სისხლის სამართლის დანაშაულთან, ან კომუნიკაცია, რომელიც რელევანტური იყო ეროვნული უსაფრთხოებისათვის. შენახულ მონაცემებსა და საზოგადოებრივ უსაფრთხოებას შორის აუცილებელი კავშირის, ასევე, დროის მონაკვეთსა თუ გეოგრაფიულ არეალთან დაკავშირებული შეზღუდვების არარსებობის გათვალისწინებით, CJEU-მ დაასკვნა, რომ შიდასახელმწიფოებრივი კანონმდებლობა აჭარბებდა ზღვარს, რომელიც მკაცრად აუცილებელი იყო მძიმე დანაშაულთან საბრძოლველად.[71]

69 CJEU, გაერთიანებული საქმეები C-203/15 და C-698/15, *Tele 2 Sverige AB v. Post-och telestryrelsen and Secretary of State for the Home Department v. Tom Watson and Others* [GC], 2016 წლის 21 დეკემბერი, პუნქტები 105–106.

70 *იქვე,* პუნქტი 105.

71 *იქვე,* პუნქტი 107.

აუცილებლობის მიმართ ასეთივე მიდგომა აქვს ჩამოყალიბებული ევროკავშირის მონაცემთა დაცვის ზედამხედველს თავის „საჭიროების სახელმძღვანელოში“ (*Necessity Toolkit*).[72] სახელმძღვანელოს მიზანია, შეაფასოს შემოთავაზებული ღონისძიებების შესაბამისობა ევროკავშირის მონაცემთა დაცვის სამართალთან. იგი განკუთვნილია ევროკავშირის პოლიტიკის მესვეურებისა და კანონმდებლებისათვის, რომელთა პასუხისმგებლობაშიც შედის იმ ღონისძიებების მომზადება და კონტროლი, რომლებიც მოიცავს პერსონალურ მონაცემთა დამუშავებას, ასევე, მათი დაცვისა და ქარტიით გათვალისწინებული სხვა უფლებებისა თუ თავისუფლებების შეზღუდვას.

საჯარო ინტერესის სტანდარტი

ქარტიით გათვალისწინებულ უფლებებზე დაწესებული შეზღუდვის გასამართლებლად, ის რეალურად უნდა აკმაყოფილებდეს საჯარო ინტერესის სტანდარტს, რომელიც აღიარებულია ევროკავშირის მიერ, ან სხვათა უფლებებისა და თავისუფლებების დაცვის აუცილებლობას. ამ უკანასკნელთან დაკავშირებით, პერსონალურ მონაცემთა დაცვის უფლება ხშირად ურთიერთქმედებს სხვა ფუნდამენტურ უფლებებთან. 1.3 ნაწილში წარმოდგენილია ამ ურთიერთქმედების დეტალური ანალიზი. რაც შეეხება საზოგადოებრივი ინტერესის სტანდარტს, იგი მოიცავს ევროკავშირის შესახებ ხელშეკრულების მე-3 მუხლით განმტკიცებულ საჯარო ინტერესებს, როგორიცაა: მშვიდობისა და კეთილდღეობის ხელშეწყობა; სოციალური სამართლიანობა და დაცვა; თავისუფალი, უსაფრთხო და სამართლიანი სივრცის შექმნა, სადაც უზრუნველყოფილია თავისუფალი გადაადგილება, იმ სათანადო ღონისძიებებთან ერთად, რომლებიც მიზნად ისახავს დანაშაულის პრევენციას და მასთან ბრძოლას, ასევე, სხვა ამოცანებსა და ინტერესებს, დაცულს ხელშეკრულებათა კონკრეტული დებულებებით.[73] ამ მხრივ, მონაცემთა დაცვის ზოგადი რეგულაცია აკონკრეტებს ქარტიის 52-ე მუხლის პირველ პუნქტს: რეგულაციის 23-ე მუხლის პირველ პუნქტში წარმოდგენილი საჯარო ინტერესთან დაკავშირებული ამოცანები - რომლებიც ამართლებს პიროვნების უფლების შეზღუდვას, თუკი ის ითვალისწინებს პერსონალურ მონაცემთა დაცვის უფლების არსს - აუცილებელი და პროპორციულია. ეროვნული უსაფრთხოება და თავდაცვა, დანაშაულის პრევენცია, ევროკავშირის ან წევრი სახელმწიფოების მნიშვნელოვანი ეკონომიკური და ფინანსური ინტერესების დაცვა, საზოგადოებრივი ჯანდაცვა და სოციალური უსაფრთხოება საზოგადოებრივი ინტერესის მაგალითებია.

მნიშვნელოვანია, საკმარისად განისაზღვროს და განიმარტოს საზოგადოებრივი ინტერესი, რომელსაც დაწესებული შეზღუდვა ემსახურება, ვინაიდან

72 EDPS (2017), *Necessity Toolkit*, ბრიუსელი, 2017 წლის 11 აპრილი.

73 ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის განმარტებები (2007/C 303/02), OJ 2007 No. C 303, გვ. 17–35.

შეზღუდვის აუცილებლობა სწორედ მისი გათვალისწინებით ფასდება. ამ კუთხით, საჭიროა დეტალურად განიმარტოს დაწესებული შეზღუდვის მიზანი და შემოთავაზებული ღონისძიებები.[74] შეზღუდვის მიზანი, აუცილებლობა და პროპორციულობა მჭიდროდ უკავშირდება ერთმანეთს.

მაგალითი: საქმე *Schwarz v. Stadt Bochum*[75] შეეხებოდა პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის უფლებებზე დაწესებულ შეზღუდვას, რომელიც უკავშირდება ანაბეჭდების აღებასა და შენახვას წევრი სახელმწიფოების მიერ პასპორტის გაცემისას.[76] განმცხადებელმა პასპორტისათვის მიმართა ქ. ბოხუმს (გერმანია), თუმცა, უარი განაცხადა თითის ანაბეჭდების აღებაზე. ამის გამო ქ. ბოხუმმა განმცხადებელს უარი უთხრა პასპორტის გაცემაზე, რაც მან გერმანიის სასამართლოში გაასაჩივრა და მოითხოვა, რომ სასამართლოს ქ.ბოხუმისათვის დაევალებინა პასპორტის გაცემა თითის ანაბეჭდების აღების გარეშე. გერმანიის სასამართლომ აღნიშნულ საკითხზე მიმართა CJEU-ს და სთხოვა, შეეფასებინა 2252/2004 რეგულაციის პირველი მუხლის მე-2 პუნქტის დასაბუთებულობა, რომელიც ადგენს სტანდარტებს წევრ სახელმწიფოთა მიერ გაცემული პასპორტებისა და სამოგზაურო დოკუმენტების უსაფრთხოებასა და ბიომეტრიულ მახასიათებლებთან დაკავშირებით.

CJEU-მ აღნიშნა, რომ თითის ანაბეჭდი პერსონალური მონაცემია, რადგან ობიექტურად შეიცავს უნიკალურ ინფორმაციას კონკრეტული პიროვნების შესახებ და ზუსტი იდენტიფიცირების საშუალებას იძლევა, მისი აღება და შენახვა კი პერსონალური მონაცემის დამუშავებაა, რომელსაც არეგულირებს No. 2252/2004 რეგულაციის პირველი მუხლის მე-2 პუნქტი და რომელიც საფრთხეს უქმნის ადამიანის პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის უფლებებს.[77] ამავდროულად, ქარტიის 52-ე მუხლის პირველი პუნქტი იძლევა ამ უფლებებზე გარკვეული შეზღუდვის დაწესების შესაძლებლობას, თუკი ის გათვალისწინებულია კანონმდებლობით, პატივს სცემს ამ უფლებათა ძირითად არსს, შეესაბამება პროპორციულობის პრინციპს, აუცილებელია და რეალურად აკმაყოფილებს ევროკავშირის მიერ აღიარებული საზოგადოებრივი ინტერესის სტანდარტს ან სხვათა უფლებებისა და თავისუფლებების დაცვის საჭიროებას.

ამ საქმეში CJEU-მ პირველ რიგში აღნიშნა, რომ შეზღუდვა, რომელიც უკავშირდება პასპორტის გაცემისას თითის ანაბეჭდების აღებასა და შე-

74 EDPS (2017), *Necessity Toolkit*, 2017 წლის 11 აპრილი, გვ. 4.

75 CJEU, C-291/12, *Michael Schwarz v. Stadt Bochum*, 2013 წლის 17 ოქტომბერი.

76 *იქვე*, პუნქტები 33–36.

77 *იქვე*, პუნქტები 27–30.

ნახვას, განსახილველია კანონთან შესაბამისობის კონტექსტში, რადგან ასეთ ოპერაციებს ითვალისწინებს No. 2252/2004 რეგულაციის პირველი მუხლის მე-2 პუნქტი; მეორე, აღნიშნული რეგულაცია შექმნილია ყალბი პასპორტების გაკეთებისა და თაღლითური გამოყენების თავიდან ასაცილებლად. ამრიგად, პირველი მუხლის მე-2 პუნქტი მიზნად ისახავს ევროკავშირში არალეგალურად შესვლის პრევენციას და, შესაბამისად, ევროკავშირის მიერ აღიარებული საზოგადოებრივი ინტერესის დაცვას; მესამე, CJEU-ს ხელთ არსებული მტკიცებულებით არ დასტურდებოდა, რომ ამ საქმეში აღნიშნულ უფლებებზე დაწესებული შეზღუდვები არ სცემდა პატივს მათ ძირითად არსს (ეს არც განმცხადებელს განუცხადებია); მეოთხე, თითის ანაბეჭდების შენახვა მაღალი სტანდარტებით დაცულ საცავში, როგორც გათვალისწინებულია შესაბამისი დებულებით, კომპლექსურ ტექნოლოგიას საჭიროებს. ამგვარი საცავის არსებობა, სავარაუდოდ, შეამცირებს პასპორტების გაყალბების რისკს და მუშაობას გაუადვილებს ორგანოებს, რომლებსაც ევროკავშირის საზღვარზე პასპორტის ავთენტურობის შემოწმება ევალებათ. იმ ფაქტს, რომ შესაბამისი მეთოდი არ არის ბოლომდე საიმედო, გადამწყვეტი მნიშვნელობა არ აქვს. ამ საშუალებით შეუძლებელია ყველა არაუფლებამოსილი პირის მიღების პრევენცია, თუმცა იგი მნიშვნელოვნად ამცირებს ასეთ შესაძლებლობას, რაც სრულიად საკმარისია. ამის გათვალისწინებით, CJEU-მ დაადგინა, რომ ანაბეჭდების აღება და შენახვა, როგორც ეს მითითებულია No. 2252/2004 რეგულაციის პირველი მუხლის მე-2 პუნქტში, სათანადო ღონისძიებაა ამ რეგულაციის მიზნების შესრულებისა და, შესაბამისად, ევროკავშირში არალეგალურად შესვლის პრევენციისათვის.[78]

CJEU-მ შემდგომ შეაფასა, თუ რამდენად აუცილებელია მონაცემთა ამ ტიპის დამუშავება და მიუთითა, რომ ქმედება გულისხმობდა არაუმეტეს ორი თითის ანაბეჭდის აღებას. ამასთან, როგორც წესი, მისი დანახვა შესაძლებელია სხვებისთვის და, შესაბამისად, არ არის პირადი ხასიათის პროცედურა. იგი არ იწვევს რაიმე განსაკუთრებულ ფიზიკურ ან ფსიქიკურ დისკომფორტს, იმაზე მეტს, ვიდრე ადამიანის სახისათვის სურათის გადაღებაა. თითის ანაბეჭდის აღების ერთადერთი რეალური ალტერნატივა, როგორც ეს საქმის მიმდინარეობისას აღინიშნა, არის თვალის ფერადი გარსის სკანირება. CJEU-ს წინაშე წარმოდგენილი მასალებით არ დასტურდება, რომ ეს უკანასკნელი პროცედურა უფრო ნაკლები ჩარევაა ქარტიის მე-7 და მე-8 მუხლებით დაცულ უფლებებში. რაც შეეხება ამ მეთოდის ეფექტიანობას, გავრცელებული მოსაზრებით, თვალის ფერადი გარსის ამოცნობის ტექნოლოგია არ არის ისე განვითარებული, როგორც თითის ანაბეჭდების დადგენის ტექნიკა; ამასთანავე, ის გაცილებით ძვირი ჯდება, რის გამოც საზოგადოებრივი გამოყენებისათვის ნაკლებად ვარგისია.

78 *იქვე*, პუნქტები 35–45.

შესაბამისად, CJEU-ს წინაშე არ წარდგენილა რაიმე სხვა ღონისძიება, რომელიც საკმარისად ეფექტიანი იქნებოდა პასპორტების თაღლითური გამოყენების პრევენციისათვის და თითის ანაბეჭდების აღებაზე ნაკლებ საფრთხეს შეუქმნიდა ქარტიის მე-7 და მე-8 მუხლებით აღიარებულ უფლებებს.[79]

CJEU-ს განმარტებით, No. 2252/2004 რეგულაციის მე-4 მუხლის მე-3 პუნქტი მკაფიოდ ადგენს, რომ თითის ანაბეჭდების გამოყენება შესაძლებელია მხოლოდ პასპორტის ავთენტურობისა და მფლობელის ვინაობის შესამოწმებლად, ხოლო პირველი მუხლის მე-2 პუნქტი არ ითვალისწინებს თითის ანაბეჭდების შენახვას სხვაგან, გარდა პასპორტისა, რომელიც მხოლოდ მფლობელს ეკუთვნის. ამრიგად, რეგულაცია არ უზრუნველყოფდა სამართლებრივ საფუძველს მის თანახმად შეგროვებულ მონაცემთა ცენტრალიზებული შენახვისა ან გამოყენებისთვის, თუკი ეს მიზნად არ ისახავდა ევროკავშირში არალეგალურად შესვლის პრევენციას.[80] ამის გათვალისწინებით, CJEU-მ დაასკვნა, რომ საქმის განხილვისას არ გამოვლენილა საკითხი, რომელიც გავლენას მოახდენდა No. 2252/2004 რეგულაციის პირველი მუხლის მე-2 პუნქტის საფუძვლიანობაზე.

კავშირი ქარტიასა და ECHR-ს შორის

მიუხედავად განსხვავებული ფორმულირებისა, ქარტიის 52-ე მუხლის პირველი პუნქტით დაცულ უფლებებზე დაწესებული კანონიერი შეზღუდვის პირობები ჰგავს ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის მე-2 პუნქტს, რომელიც შეეხება პირად ცხოვრების პატივისცემის უფლებას. CJEU და ECtHR თავიანთ პრეცედენტულ სამართალში ხშირად მიუთითებენ ერთმანეთის გადაწყვეტილებებზე. ეს ხდება ორ სასამართლოს შორის მუდმივად არსებული დიალოგის ფარგლებში, რომლის მიზანიც არის მონაცემთა დაცვის წესების ჰარმონიული ინტერპრეტაცია. ქარტიის 52-ე მუხლის მე-3 პუნქტის თანახმად, „თუ ქარტიაში გათვალისწინებული უფლებები ემთხვევა ადამიანის უფლებათა ევროპული კონვენციით გარანტირებულ უფლებებს, მათი მნიშვნელობა და ფარგლები იქნება ისეთი, როგორსაც კონვენცია ადგენს.“ ამავდროულად, ქარტიის მე-8 მუხლი პირდაპირ არ შეესაბამება ECHR-ის რომელიმე მუხლს.[81] ქარტიის 52-ე მუხლის მე-3 პუნქტი შეეხება თითოეულ სამართლებრივ სისტემაში დაცულ უფლებათა არსსა და მასშტაბებს და არა

79 CJEU, C-291/12, *Michael Schwarz v. Stadt Bochum,* 2013 წლის 17 ოქტომბერი, პუნქტები 46–53.

80 *იქვე,* პუნქტები 56–61.

81 EDPS (2017), *Necessity Toolkit, Brussels,* 2017 წლის 11 აპრილი, გვ. 6.

მათზე დაწესებული შეზღუდვების პირობებს. თუმცა, ორ სასამართლოს შორის დიალოგისა და თანამშრომლობის ფართო კონტექსტში, CJEU-მ შეიძლება საკუთარ ანალიზში გაითვალისწინოს ECHR-ის მე-8 მუხლში წარმოდგენილი კანონიერი შეზღუდვის კრიტერიუმები, ისე, როგორც განმარტავს ECtHR. შეიძლება მოხდეს პირიქითაც და ECtHR-მა გამოიყენოს ქარტიით დაწესებული კანონიერი შეზღუდვის პირობები. ნებისმიერ შემთხვევაში, გასათვალისწინებელია, რომ ECHR არ შეიცავს ქარტიის მე-8 მუხლის ტოლფას დებულებას, რომელიც მიუთითებს პერსონალურ მონაცემთა დაცვის საკითხებზე, როგორიცაა: მონაცემთა სუბიექტის უფლებები, დამუშავების კანონიერი საფუძვლები და ზედამხედველობა დამოუკიდებელი ორგანოს მხრიდან. ECtHR-ის პრეცედენტულ სამართალში, რომელიც კონვენციის მე-8 მუხლის საფუძველზე ჩამოყალიბდა და 108-ე კონვენციას უკავშირდება, შესაძლებელია ქარტიის მე-8 მუხლის ზოგიერთი კომპონენტის ნახვა.[82] ეს კავშირი ქმნის CJEU-ისა და ECtHR-ის ურთიერთგავლენას მონაცემთა დაცვის საკითხებთან მიმართებით.

1.3 ურთიერთქმედება სხვა უფლებებსა და კანონიერ ინტერესებთან

ძირითადი საკითხები

- მონაცემთა დაცვის უფლება ხშირად ურთიერთქმედებს სხვა უფლებებთან (მაგ: გამოხატვის თავისუფლება და ინფორმაციის მიღებისა და გაცემის უფლება).

- აღნიშნული ურთიერთკავშირი ხშირად არაერთმნიშვნელოვანია: არსებობს სიტუაციები, სადაც პერსონალურ მონაცემთა დაცვის უფლება უპირისპირდება კონკრეტულ უფლებას, თუმცა, ზოგ შემთხვევაში იგი ეფექტიანად უზრუნველყოფს ამავე უფლების პატივისცემას. მაგალითად, გამოხატვის თავისუფლების შემთხვევაში, პროფესიული საიდუმლოება პირადი ცხოვრების პატივისცემის უფლების ნაწილია.

- სხვათა უფლებებისა და თავისუფლებების დაცვის აუცილებლობა ერთერთი კრიტერიუმია, რომელიც გამოიყენება პერსონალურ მონაცემთა დაცვის უფლებაზე დაწესებული კანონიერი შეზღუდვის შესაფასებლად.

- როდესაც სასწორზე დევს სხვადასხვა უფლება, სასამართლოებმა უნდა დააბალანსონ და დაარეგულირონ ისინი.

82 ფუნდამენტურ უფლებათა ევროპულ ქარტიასთან დაკავშირებით (2007/C 303/02), მუხლი 8.

- მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, წევრ სახელმწიფოებს მოეთხოვებათ პერსონალურ მონაცემთა დაცვის უფლების გაწონასწორება გამოხატვისა და ინფორმაციის თავისუფლებასთან.

- წევრმა სახელმწიფოებმა შესაძლოა ეროვნულ კანონმდებლობაში მიიღონ კონკრეტული მარეგულირებელი წესები პერსონალურ მონაცემთა დაცვის უფლების დასაბალანსებლად ოფიციალური დოკუმენტების საჯარო ხელმისაწვდომობისა და პროფესიული საიდუმლოების ვალდებულებებთან.

პერსონალურ მონაცემთა დაცვის უფლება არ არის აბსოლუტური. მისი კანონიერი შეზღუდვის (პირობები ზემოთ დეტალურად არის განხილული) ერთ-ერთი კრიტერიუმი, რომელსაც აღიარებს როგორც ევროპის საბჭოს, ისე ევროკავშირის სამართალი, არის სხვათა უფლებებისა და თავისუფლებების დაცვა. ECtHR-მაც და CJEU-მაც არაერთხელ აღნიშნეს, რომ როდესაც მონაცემთა დაცვა სხვა უფლებებთან ურთიერთქმედებს, საჭიროა მათი დაბალანსება ECHR-ის მე-8 მუხლისა და ქარტიის მე-8 მუხლის გამოყენება-განმარტების პროცესში.[83] ასეთი ბალანსის მიღწევის რამდენიმე მნიშვნელოვანი მაგალითი განხილულია ქვემოთ.

საჭიროების შემთხვევაში, შეიძლება სახელმწიფოებმაც მიიღონ კანონმდებლობა პერსონალურ მონაცემთა დაცვის დასაბალანსებლად სხვა უფლებებთან. ამ მიზნით, მონაცემთა დაცვის ზოგადი რეგულაცია ითვალისწინებს რამდენიმე გამონაკლის სფეროს ეროვნულ დონეზე.

გამოხატვის თავისუფლებასთან დაკავშირებით, GDPR წევრი სახელმწიფოებისაგან მოითხოვს, რომ კანონით „შეუთავსონ ამ რეგულაციით გათვალისწინებული პერსონალურ მონაცემთა დაცვის უფლება გამოხატვისა და ინფორმაციის თავისუფლებას (მათ შორის, პერსონალურ მონაცემთა დამუშავებისას ჟურნალისტური, აკადემიური, სახელოვნებო და ლიტერატურული მიზნებით).“[84] წევრ სახელმწიფოებს შეუძლიათ, მიიღონ კანონები მონაცემთა დაცვის უფლების დასაბალანსებლად ოფიციალური დოკუმენტების საჯარო ხელმისაწვდომობის პრინციპთან, ასევე, პროფესიული საიდუმლოების ვალდებუ-

83 ECtHR, *Von Hannover v. Germany* (No. 2) [GC], Nos. 40660/08 და 60641/08, 2012 წლის 7 თებერვალი; CJEU, გაერთიანებული საქმეები C-468/10 და C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado,* 2011 წლის 24 ნოემბერი, პუნქტი 48; CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 2008 წლის 29 იანვარი, პუნქტი 68.

84 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 85.

ლებებთან, რომელიც დაცულია პირადი ცხოვრების უფლების ერთ-ერთ ფორმად.[85]

1.3.1 გამოხატვის თავისუფლება

ერთ-ერთი უფლება, რომელიც ყველაზე მეტად ურთიერთქმედებს მონაცემთა დაცვის უფლებასთან, არის გამოხატვის თავისუფლება.

გამოხატვის თავისუფლება დაცულია ქარტიის მე-11 მუხლით (გამოხატვისა და ინფორმაციის თავისუფლება) და მოიცავს „პირის თავისუფლებას, ჰქონდეს შეხედულებები, მიიღოს ან გაავრცელოს ინფორმაცია და იდეები საჯარო ხელისუფლების ჩარევის გარეშე, საზღვრების მიუხედავად.“ ინფორმაციის თავისუფლება, როგორც ქარტიის მე-11 მუხლის, ისე კონვენციის მე-10 მუხლის საფუძველზე, იცავს ინფორმაციის არა მხოლოდ გაზიარების, არამედ მიღების უფლებასაც.

გამოხატვის უფლებაზე დაწესებული შეზღუდვები უნდა შეესაბამებოდეს ქარტიის 52-ე მუხლის პირველი პუნქტით დადგენილ კრიტერიუმებს, რომლებიც აღწერილია ზემოთ. ამასთან, მისი მე-11 მუხლი შეესაბამება ECHR-ის მე-10 მუხლს. ქარტიის 52-ე მუხლის მე-3 პუნქტის თანახმად, რაკი ქარტიის უფლებები შეესაბამება ECHR-ით გარანტირებულ უფლებებს, მათი „მნიშვნელობა და ფარგლები უნდა იყოს ისეთი, როგორც ადგენს კონვენცია.“ შეზღუდვები, რომლებიც შესაძლოა კანონის შესაბამისად დაწესდეს ქარტიის მე-11 მუხლით აღიარებულ უფლებაზე, არ უნდა გასცდეს ECHR-ის მე-10 მუხლის მე-2 პუნქტით განსაზღვრულ ფარგლებს. სხვა სიტყვებით, იგი უნდა იყოს კანონით გათვალისწინებული და აუცილებელი დემოკრატიულ საზოგადოებაში „სხვათა უფლებებისა და რეპუტაციის დასაცავად.“ ეს უფლებები განსაკუთრებულად მოიცავს პირადი ცხოვრების პატივისცემასა და პერსონალურ მონაცემთა დაცვას.

პერსონალურ მონაცემთა დაცვასა და გამოხატვის თავისუფლებას შორის ურთიერთობა მოწესრიგებულია მონაცემთა დაცვის ზოგადი რეგულაციის 85-ე მუხლით: „პერსონალურ მონაცემთა დამუშავება და გამოხატვისა და ინფორმაციის თავისუფლება.“ ამ მუხლის თანახმად, წევრი სახელმწიფოები ვალდებულნი არიან, პერსონალურ მონაცემთა დაცვის უფლება შეუთავსონ გამოხატვისა და ინფორმაციის თავისუფლებას. კერძოდ, ჟურნალისტური, აკადემიური, სახელოვნებო ან ლიტერატურული გამოხატვისთვის, საჭიროა გარკვეული გამონაკლისი შემთხვევების დადგენა მონაცემთა დაცვის ზოგადი რეგულაციის კონკრეტულ თავებთან მიმართებით. ეს აუცილებელია პირადი ცხოვრების უფლების დასაბალანსებლად გამოხატვისა და ინფორმაციის თავისუფლებასთან.

85 *იქვე,* მუხლი 86 და 90.

მაგალითები: საქმეში *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*[86] CJEU-ს მიმართეს, რათა განესაზღვრა მონაცემთა დაცვისა და პრესის თავისუფლებას შორის დამოკიდებულება.[87] მას უნდა განეხილა კომპანიის მიერ 1.2 მილიონი ფიზიკური პირის საგადასახადო მონაცემების გავრცელება მოკლე ტექსტური შეტყობინების სერვისით. ეს მონაცემები კანონიერად იყო მოპოვებული ფინეთის საგადასახადო ორგანოდან. ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანომ გამოსცა გადაწყვეტილება, რომელიც კომპანიას ავალდებულებდა, შეეწყვიტა ამ ინფორმაციის გავრცელება. კომპანიამ გადაწყვეტილება ადგილობრივ სასამართლოში გაასაჩივრა, რომელმაც CJEU-სგან მოითხოვა მონაცემთა დაცვის დირექტივის განმარტება. კერძოდ, სასამართლოს უნდა განესაზღვრა, შეიძლებოდა თუ არა მხოლოდ ჟურნალისტური მიზნებით განხორციელებულ ქმედებად ჩათვლილიყო იმ პერსონალურ მონაცემთა დამუშავება, რომლებიც საგადასახადო ორგანოებმა გახადეს ხელმისაწვდომი, რათა მობილური ტელეფონის მომხმარებლებს მიეღოთ სხვა ფიზიკურ პირთა საგადასახადო მონაცემები. მას შემდეგ, რაც დაადგინა, რომ დირექტივის მე-3 მუხლის პირველი პუნქტის თანახმად, კომპანიის საქმიანობა იყო პერსონალური მონაცემების დამუშავება, CJEU-მ გააანალიზა დირექტივის მე-9 მუხლი (პერსონალური მონაცემების დამუშავება და გამოხატვის თავისუფლება). პირველ რიგში, მან აღნიშნა გამოხატვის თავისუფლების მნიშვნელობა ნებისმიერ დემოკრატიულ საზოგადოებაში და ახსნა, რომ ამ თავისუფლებასთან დაკავშირებული ისეთი ცნება, როგორიცაა ჟურნალისტიკა, ფართოდ უნდა განიმარტოს. სასამართლოს თქმით, ორ ფუნდამენტურ უფლებას შორის ბალანსის მისაღწევად, გამონაკლისები და შეზღუდვები მონაცემთა დაცვის უფლებაზე უნდა დაწესდეს მხოლოდ მკაცრად აუცილებელი დოზით. ამ პირობების გათვალისწინებით, სასამართლომ დაადგინა, რომ კომპანიათა ქმედებები იმ დოკუმენტებიდან ამოღებულ მონაცემებთან დაკავშირებით, რომლებიც, ეროვნული კანონმდებლობის თანახმად, საყოველთაო საკუთრებაა, შესაძლებელია „ჟურნალისტურ აქტივობად“ ჩაითვალოს, თუ მათი მიზანია საზოგადოებისათვის ინფორმაციის, მოსაზრებებისა და იდეების მიწოდება (მიუხედავად მათ გადასაცემად გამოყენებული საშუალებისა). სასამართლომ ასევე დაადგინა, რომ აღნიშნული

86 CJEU, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [GC], 2008 16 დეკემბერი, პუნქტები 56, 61 და 62.

87 საქმე შეეხებოდა მონაცემთა დაცვის დირექტივის მე-9 მუხლის განმარტებას, რომელიც ამჟამად ჩანაცვლებულია მონაცემთა დაცვის ზოგადი რეგულაციით და რომლის თანახმადაც „ჟურნალისტური, აკადემიური, სახელოვნებო ან ლიტერატურული გამოხატვის მიზნით მონაცემთა დამუშავებისათვის, წევრმა სახელმწიფოებმა შეიძლება დაუშვან გამონაკლისები და დათქმები ამ, მე-4 და მე-6 თავებთან მიმართებით, თუ ეს აუცილებელია პერსონალურ მონაცემთა დაცვის უფლების შესაბამისობისათვის გამოხატვის თავისუფლებასთან.

ქმედებები არ იზღუდება მხოლოდ მედია აქტივობით და შეიძლება კომერციული მიზნებითაც განხორციელდეს. თუ რომელ მიზანს ემსახურებოდა კონკრეტული შემთხვევა, ეს საკითხი CJEU-მ ეროვნულ სასამართლოს დაუტოვა გასარკვევად.

იგივე საქმე განიხილა ECtHR-მაც, მას შემდეგ, რაც ეროვნულმა სასამართლომ CJEU-სგან მიღებული ინსტრუქციების საფუძველზე გადაწყვიტა, რომ საზედამხედველო ორგანოს მითითება ყველა სახის საგადასახადო ინფორმაციის გასაჯაროების შეწყვეტაზე გამართლებული ჩარევა იყო კომპანიის გამოხატვის თავისუფლებაში. ECtHR-მა აღნიშნულ მიდგომას დაუჭირა მხარი.[88] სასამართლოს გადაწყვეტილებით, ასეთი ჩარევა კომპანიების მიერ ინფორმაციის გაცემის უფლებაში იყო კანონით გათვალისწინებული, კანონიერი მიზნის შესაბამისი და აუცილებელი დემოკრატიულ საზოგადოებაში.

სასამართლომ მიუთითა პრეცედენტული სამართლით დადგენილ კრიტერიუმზე, რომლითაც უნდა იხელმძღვანელოს ხელისუფლებამ და თავად სასამართლომ გამოხატვის თავისუფლების დაბალანსებისას პირადი ცხოვრების პატივისცემის უფლებასთან. თუ სასწორზე დევს პოლიტიკური გამოსვლა, ან დებატები საჯარო ინტერესის საკითხის შესახებ, ინფორმაციის მიღებისა და გაცემის უფლებაზე შეზღუდვის დაწესება შესაძლებელია მხოლოდ ვიწრო მასშტაბით, რადგან საზოგადოებას აქვს აღნიშნული უფლება, „და ის აუცილებელია დემოკრატიულ საზოგადოებაში.“[89] ამავდროულად, ჟურნალისტური სტატიები, რომელთა ერთადერთი მიზანია პირადი ცხოვრების დეტალებზე მკითხველთა გარკვეული წრის ცნობისმოყვარეობის დაკმაყოფილება, ვერ ჩაითვლება წვლილის შეტანად საჯარო ინტერესის საკითხზე დებატებში. მონაცემთა დაცვის წესებთან მიმართებით გამონაკლისის დაშვება ჟურნალისტური მიზნებით ითვალისწინებს მედიის წარმომადგენელთა წვდომას მონაცემთა შეგროვებასა და დამუშავებაზე, რათა შეძლონ პროფესიული მოვალეობების შესრულება. ამრიგად, ნამდვილად არსებობდა საჯარო ინტერესი, რომ განმცხადებელ კომპანიებს ჰქონოდათ დიდი ოდენობით საგადასახადო მონაცემის შეგროვებისა და დამუშავების შესაძლებლობა. ამავდროულად, სასამართლომ დაადგინა, რომ ეს საჯარო ინტერესი არ მოიცავდა დაუმუშავებელი მონაცემების უცვლელად და გაუანალიზებლად გავრცელებას გაზეთების მიერ. საგადასახადო ინფორმაცია, სავარაუდოდ, საზოგადოების დაინტერესებულ წევრებს მისცემდა ფიზიკური პირების კატეგორიზაციის საშუალებას, მათი ეკონომიკური სტატუსიდან გამომდინარე, და დააკ-

88 ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland,* No. 931/13, 2017 წლის 27 ივნისი.

89 *იქვე,* პუნქტი 169.

მაყოფილებდა საზოგადოების ცნობისმოყვარეობას სხვების პირადი ცხოვრების შესახებ. ეს კი ვერ მიიჩნევა წვლილის შეტანად საჯარო ინტერესის საკითხის განხილვაში.

Google Spain[90]-ის საქმეში CJEU-მ იმსჯელა, იყო თუ არა ვალდებული Google, საძიებო სიის შედეგებიდან წაეშალა მოძველებული ინფორმაცია განმცხადებლის ფინანსურ სირთულეებზე. ამ სისტემაში განმცხადებლის სახელის ძიებისას, შედეგებს მოჰყვებოდა ბმულები ძველ საგაზეთო სტატიებზე, სადაც მითითებული იყო განმცხადებლის კავშირი გაკოტრების საქმის წარმოებასთან. განმცხადებლის აზრით, ეს არღვევდა მისი პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის უფლებებს, ვინაიდან წარმოება წლების წინათ დასრულდა და მსგავსი მითითება არარელევანტური იყო.

CJEU-მ პირველ რიგში განმარტა, რომ ინტერნეტის საძიებო სისტემები და ძიების შედეგები, რომლებიც პერსონალურ მონაცემებს აწვდის, პიროვნების დეტალური პროფილის შედგენის საშუალებას იძლევა. ვინაიდან საზოგადოება სულ უფრო და უფრო დამოკიდებული ხდება ციფრულ სამყაროზე, მონაცემთა მაღალ დონეზე დასაცავად, ფუნდამენტურად მნიშვნელოვანია, ისინი იყოს ზუსტი, მათი გამოქვეყნება კი არ სცდებოდეს საჭიროების (ანუ საზოგადოების ინფორმირების) ფარგლებს. „ამ შემთხვევაში, მონაცემთა დამმუშავებელი საკუთარი მოვალეობების, უფლებამოსილებისა და შესაძლებლობების ფარგლებში უნდა აკმაყოფილებდეს [ევროკავშირის სამართლის] მოთხოვნებს მონაცემთა დამუშავებასთან მიმართებით“, რათა დადგენილ სამართლებრივ გარანტიებს ჰქონდეს სრულყოფილი ეფექტი. ეს ნიშნავს, რომ პერსონალურ მონაცემთა წაშლის უფლება, თუკი დამუშავება აღარ არის საჭირო ან მონაცემები მოძველებულია, ვრცელდება ასეთ საძიებო სისტემებზეც, რომლებიც მიიჩნევიან მონაცემთა დამმუშავებლებად და არა უფლებამოსილ პირებად (იხ: პუნქტი 2.3.1).

სასამართლომ იმსჯელა, რამდენად მოეთხოვებოდა Google-ს განმცხადებელთან დაკავშირებული ბმულების წაშლა და დაადგინა, რომ გარკვეულ პირობებში, ადამიანებს აქვთ უფლება, მოითხოვონ თავიანთი პერსონალური მონაცემების წაშლა ინტერნეტსაძიებო სისტემის შედეგებიდან. ამ უფლების გამოყენება შესაძლებელია მაშინ, როდესაც პიროვნებაზე ინფორმაცია არაზუსტი ან შეუსაბამოა, ანდა სცდება დამუშავების მიზნებს. CJEU-მ განაცხადა, რომ წაშლის უფლება არ არის აბსოლუტური. იგი უნდა დაბალანსდეს სხვა უფლებებთან, როგორიცაა ფართო საზოგადოების წვდომა ინტერნეტსა და ინფორმაციაზე. თითოეული მოთ-

90 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014, პუნქტები 81–83.

ხოვნა მონაცემთა წაშლაზე უნდა შეფასდეს ინდივიდუალურად, ბალანსის მიღწევით, ერთი მხრივ, მონაცემთა სუბიექტის პერსონალურ მონაცემთა დაცვის ფუნდამენტურ უფლებასა და პირადი ცხოვრების უფლებას და, მეორე მხრივ, ინტერნეტის ყველა მომხმარებლის კანონიერ ინტერესებს შორის. CJEU-მ განსაზღვრა სახელმძღვანელო მითითებები იმ ფაქტორებზე, რომლებიც გასათვალისწინებელია უფლებათა დაბალანსებისას. ამ მხრივ, განსაკუთრებით მნიშვნელოვანია, რა ტიპის ინფორმაციას ეხება მსჯელობა: თუ ინფორმაცია პირად ცხოვრებას ასახავს და არ არსებობს მისი ხელმისაწვდომობის საჯარო ინტერესი, უპირატესობა ენიჭება მონაცემებისა და პირადი ცხოვრების ხელშეუხებლობის დაცვას. ამავდროულად, თუ მონაცემთა სუბიექტი საჯარო ფიგურაა, ანდა ინფორმაციის თავისებურებიდან გამომდინარე, გამართლებულია საჯარო ხელმისაწვდომობა მასზე, მიზანშეწონილად მიიჩნევა ჩარევა მონაცემთა დაცვისა და პირადი ცხოვრების პატივისცემის ფუნდამენტურ უფლებებში.

სასამართლოს ამ გადაწყვეტილების შემდეგ, 29-ე მუხლის სამუშაო ჯგუფმა მიიღო CJEU-ს გადაწყვეტილების აღსრულების სახელმძღვანელო პრინციპები. ამ პრინციპებში წარმოდგენილია საერთო კრიტერიუმების ჩამონათვალი, რომლებიც საზედამხედველო ორგანოებმა უნდა გამოიყენონ მაშინ, როდესაც განიხილავენ ფიზიკური პირთა მოთხოვნას მონაცემთა წაშლის შესახებ, ასევე, ხსენებული უფლებების დაბალანსებისას.[91]

რაც შეეხება მონაცემთა დაცვის უფლების შეთავსებას გამოხატვის თავისუფლებასთან, ECtHR-ს მიღებული აქვს რამდენიმე გამორჩეულად მნიშვნელოვანი გადაწყვეტილება.

მაგალითები: საქმეში *Axel Springer AG v. Germany*[92] ECtHR-მა დაადგინა, რომ ადგილობრივი სასამართლოს აკრძალვა, რომელიც განმცხადებელ კომპანიას უზღუდავდა სტატიის გამოქვეყნებას ცნობილი მსახიობის დაპატიმრებასა და გასამართლებაზე, არღვევდა ECHR-ის მე-10 მუხლს. სასამართლომ კიდევ ერთხელ განმარტა კრიტერიუმები, რომლებიც უნდა გამოიყენონ გამოხატვისა და პირადი ცხოვრების პატივისცემის უფლებათა დაბალანსებისას, როგორც დადგენილია სასამართლოს პრეცედენტულ სამართალში, კერძოდ:

91 29-ე მუხლის სამუშაო ჯგუფი (2014), სახელმძღვანელო პრინციპები CJEU-ს გადაწყვეტილების იმპლემენტაციისათვის საქმეებზე *Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C-131/12*, WP 225, ბრიუსელი, 2014 წლის 26 ნოემბერი.

92 ECtHR, *Axel Springer AG v. Germany* [GC], No. 39954/08, 2012 წლის 7 თებერვალი, პუნქტები 90 და 91.

- იყო თუ არა კონკრეტული შემთხვევა საზოგადოებრივი ინტერესის საკითხი;
- იყო თუ არა კონკრეტული პიროვნება საჯარო ფიგურა; და
- რა გზით მოიპოვა ინფორმაცია კომპანიამ და რამდენად სარწმუნო გახლდათ ის.

ECHR-მა დაადგინა, რომ მსახიობის დაპატიმრება და გასამართლება საჯაროდ ცნობილი ფაქტი იყო, შესაბამისად, მის მიმართ არსებობდა საჯარო ინტერესი; მსახიობი საკმაოდ ცნობილი გახლდათ საჯარო ფიგურად მიჩნევისათვის; ინფორმაციის წყარო იყო პროკურატურა, ამიტომ მხარეებს მისი სიზუსტე სადავოდ არ გაუხდიათ. შესაბამისად, კომპანიაზე დაწესებული შეზღუდვები გამოქვეყნებასთან მიმართებით არ იყო განმცხადებლის პირადი ცხოვრების ხელშეუხებლობის კანონიერი მიზნის პროპორციული. სასამართლომ საქმეში დაადგინა ECHR-ის მე-10 მუხლის დარღვევა.

საქმე *Coudec and Hachette Filipacchi Associés v. France*[93] შეეხებოდა ქ-ნ კოსტეს ინტერვიუს გამოქვეყნებას ფრანგულ ყოველკვირეულ ჟურნალში, სადაც აცხადებდა, რომ მისი შვილის მამა მონაკოს პრინცი ალბერი იყო. ინტერვიუ აღწერდა ქ-ნ კოსტეს ურთიერთობას პრინცთან, თუ რა რეაქცია ჰქონდა მას ბავშვის დაბადებაზე. სტატიას ახლდა პრინცის ბავშვთან ერთად გადაღებული ფოტოებიც. პრინცმა ალბერმა საგამომცემლო კომპანიას პირადი ცხოვრების დაცვის უფლების დარღვევისთვის უჩივლა. საფრანგეთის სასამართლომ დაადგინა, რომ სტატიის გამოქვეყნებამ პრინც ალბერს გამოუსწორებელი ზიანი მიაყენა და გამომცემელს დააკისრა ზიანის ანაზღაურება, ასევე, ჟურნალის გარეკანზე დეტალური ინფორმაციის გამოქვეყნება გადაწყვეტილების შესახებ.

გამომცემელმა ECtHR-ს მიმართა. განმცხადებელი აცხადებდა, რომ საფრანგეთის სასამართლოს გადაწყვეტილება უსამართლოდ ერეოდა მის გამოხატვის თავისუფლებაში. ECtHR-ს უნდა დაებალანსებინა, ერთი მხრივ, პრინც ალბერის პირადი ცხოვრების პატივისცემის და, მეორე მხრივ, გამომცემლის გამოხატვისა და საზოგადოების ინფორმირებულობის უფლებები; ასევე, გაეთვალისწინებინა ქ-ნ კოსტეს უფლება, თავისი ისტორია საზოგადოებისთვის გაეზიარებინა, და ბავშვის ინტერესი მამა-შვილის ურთიერთობის ოფიციალურად დადგენის მხრივ.

ECtHR-ის დასკვნით, ინტერვიუს გამოქვეყნება გახლდათ პრინცის პირად ცხოვრებაში ჩარევა, რის შემდეგაც მან იმსჯელა ჩარევის აუცილებლო-

93 ECtHR, *Coudec and Hachette Filipacchi Associés v. France* [GC], No. 40454/07, 2015 წლის 10 ნოემბერი.

ბაზე. სასამართლომ მიიჩნია, რომ ინტერვიუ შეეხებოდა საჯარო ფიგურას და საზოგადოებრივი ინტერესის საკითხს: მონაკოს მოქალაქეებს აინტერესებდათ პრინცის შვილის არსებობა, ვინაიდან მემკვიდრეობითი მონარქიის მომავალი „მჭიდროდ უკავშირდება შთამომავლობას“. ამრიგად, საკითხს საზოგადოებრივი მნიშვნელობა ჰქონდა.[94] სასამართლომ ასევე აღნიშნა, რომ ინტერვიუ იყო ქ-ნ კოსტესა და მისი შვილის გამოხატვის თავისუფლების განხორციელება. ეროვნულმა სასამართლოებმა ვერ შეძლეს, სათანადოდ გაეთვალისწინებინათ ECtHR-ის პრეცედენტული სამართლით ჩამოყალიბებული პრინციპები და კრიტერიუმები, რომლებიც შეეხება პირადი ცხოვრების პატივისცემის უფლებისა და გამოხატვის თავისუფლების დაბალანსებას. ევროპულმა სასამართლომ საქმეში დაადგინა კონვენციის მე-10 მუხლის დარღვევა.

ECtHR-ის პრეცედენტულ სამართალში ამ უფლებათა დაბალანსების ერთერთი მნიშვნელოვანი კრიტერიუმია გამოხატვის თავისუფლების წვლილი საზოგადოებრივი ინტერესის საკითხის განხილვაში.

მაგალითები: საქმეში *Mosley v. the United Kingdom*[95] ყოველკვირეულმა ბრიტანულმა გაზეთმა გამოაქვეყნა განმცხადებლის პირადული ფოტოები. განმცხადებელმა, რომელიც ცნობილი ადამიანი იყო, გამომცემლის წინააღმდეგ სამოქალაქო სარჩელი აღძრა და მიიღო კომპენსაცია ზიანის ასანაზღაურებლად. ამის მიუხედავად, მან მაინც მიმართა ევროპულ სასამართლოს პირადი ცხოვრების ხელშეუხებლობის უფლების დარღვევისათვის. საჩივარში იგი მიუთითებდა, რომ ვერ შეძლო ფოტოების გამოქვეყნების აკრძალვა, ვინაიდან გაზეთისთვის არ იყო დადგენილი გამოქვეყნების წინასწარ შეტყობინების ვალდებულება.

ECtHR-მა აღნიშნა, რომ ამგვარი მასალის გავრცელებას, ძირითადად, გასართობი მიზანი ჰქონდა და არა საგანმანათლებლო, თუმცა მასზე უდავოდ ვრცელდებოდა კონვენციის მე-10 მუხლით გათვალისწინებული დაცვა, რომელსაც შეიძლება უპირატესობა მიენიჭოს მე-8 მუხლთან შედარებით (ამ უკანასკნელის თანახმად, ინფორმაცია იყო პირადი და ინტიმური და მისი გავრცელების საზოგადოებრივი ინტერესი არ არსებობდა). ამავდროულად, განსაკუთრებული სიფრთხილით უნდა განიხილოს შეზღუდვები, რომლებიც შეიძლება ცენზურის ფორმით მოქმედებდეს გამოქვეყნებამდე. ECtHR-მა, გაითვალისწინა რა ის „გამყინავი ეფექტი“, რომელიც შეიძლება ჰქონდეს წინასწარი შეტყობინების მოთხოვნას, ასევე, მის

94 *იქვე,* პუნქტები 104–116.

95 ECtHR, *Mosley v. the United Kingdom,* No. 48009/08, 2011 წლის 10 მაისი, პუნქტები 129 და 130.

ეფექტიანობასთან დაკავშირებული ეჭვები და შეფასების ფართო ფარგლები ამ სფეროში, დაასკვნა, რომ წინასწარ შეტყობინების სამართლებრივად სავალდებულო მოთხოვნა მე-8 მუხლით არ იყო გათვალისწინებული. ამრიგად, სასამართლომ დაადგინა, რომ საქმეში კონვენციის მე-8 მუხლი არ დარღვეულა.

საქმეში *Bohlen v. Germany*[96] განმცხადებელმა, ცნობილმა მომღერალმა და პროდიუსერმა, გამოაქვეყნა ავტობიოგრაფიული წიგნი, ხოლო შემდგომში იძულებული გახდა, სასამართლოს გადაწყვეტილებათა საფუძველზე, წიგნიდან ამოეღო გარკვეული მონაკვეთები. ეს ამბავი ადგილობრივი მედიით ფართოდ გაშუქდა, თამბაქოს კომპანიამ კი იუმორისტული სარეკლამო კამპანია წამოიწყო, სადაც მომხდარზე მიუთითებდა და განმცხადებლის სახელი მისი ნებართვის გარეშე გამოიყენა. განმცხადებელი ითხოვდა ზიანის ანაზღაურებას კომპანიის მიერ, მაგრამ უშედეგოდ. იგი აცხადებდა, რომ მის წინააღმდეგ დაირღვა კონვენციის მე-8 მუხლით გათვალისწინებული უფლებები. ECtHR-მა კიდევ ერთხელ გაამახვილა ყურადღება იმ კრიტერიუმზე, რომელიც ერთგვარი სახელმძღვანელოა პირადი ცხოვრების პატივისცემის უფლებისა და გამოხატვის თავისუფლების დასაბალანსებლად და დაადგინა, რომ საქმეში მე-8 მუხლი არ დარღვეულა. განმცხადებელი საჯარო ფიგურა იყო და რეკლამა მიუთითებდა არა მისი პირადი ცხოვრების დეტალებზე, არამედ მოვლენაზე, რომელიც მედიით უკვე გაშუქდა და საჯარო დებატების ნაწილად იქცა. ამასთან, რეკლამა იუმორისტული იყო და არ შეიცავდა რაიმე შეურაცხმყოფელ ან უარყოფით მინიშნებებს განმცხადებლის შესახებ.

საქმეში *Biriuk v. Lithuania*[97] განმცხადებელი ევროსასამართლოში დავობდა, რომ ლიეტუვამ ვერ შეძლო მასზე დაკისრებული მოვალეობების შესრულება პირადი ცხოვრების დაცვის კუთხით: ერთ-ერთი მსხვილი გაზეთის მიერ განმცხადებლის უფლების მძიმე დარღვევის მიუხედავად, მას ეროვნულმა სასამართლოებმა მიზერული ფულადი კომპენსაცია განუსაზღვრეს. ზიანის შეფასებისას, ეროვნულმა სასამართლოებმა გამოიყენეს ეროვნული კანონმდებლობის დებულებები. აღნიშნული დებულებები საზოგადოების ინფორმირებას შეეხება და ადგენს კომპენსაციის დაბალ ზღვარს იმ არამატერიალური ზიანისთვის, რომელიც პირს მიაყენა მედიამ პირადი ცხოვრების ამსახველი ინფორმაციის უკანონო გავრცელებით. საქმე ეხებოდა ლიეტუვას ყველაზე მსხვილი ყოველდღიური გაზეთის მთავარ გვერდზე სტატიის გამოქვეყნებას, რომელშიც გაცხადებული იყო ინფორმაცია განმცხადებლის აივ დადებით სტატუსზე. სტატია აკრიტიკებ-

96 ECtHR, *Bohlen v. Germany,* No. 53495/09, 2015 წლის 19 თებერვალი, პუნქტები 45–60.

97 ECtHR, *Biriuk v. Lithuania,* No. 23373/03, 2008 წლის 25 ნოემბერი.

და განმცხადებლის საქციელს და კითხვის ნიშნის ქვეშ აყენებდა მის მორალურ სტანდარტებს.

ECtHR-მა განმარტა, რომ ადამიანის უფლებათა ევროპული კონვენციის თანახმად, პერსონალური მონაცემების, კერძოდ, სამედიცინო ჩანაწერების დაცვას ფუნდამენტური მნიშვნელობა ენიჭება. ჯანმრთელობის მდგომარეობის კონფიდენციალობა განსაკუთრებით საგულისხმოა, რადგან სამედიცინო მონაცემების (ამ შემთხვევაში, აივ დადებითი სტატუსის) გამჟღავნებამ შესაძლოა მნიშვნელოვანი გავლენა მოახდინოს პიროვნების პირად და ოჯახურ ცხოვრებაზე, ასევე, დასაქმებასა და საზოგადოებაში ინტეგრირებაზე. სასამართლომ განსაკუთრებული მნიშვნელობა მიანიჭა იმ ფაქტს, რომ გაზეთში გამოქვეყნებული სტატიის თანახმად, განმცხადებლის აივ დადებითი სტატუსის ინფორმაციის წყარო გახლდათ საავადმყოფოს სამედიცინო პერსონალი, რაც აშკარად არღვევდა სამედიცინო საიდუმლოების დაცვის ვალდებულებას. ამრიგად, განმცხადებლის პირადი ცხოვრების უფლებაში ჩარევა კანონიერი არ ყოფილა.

სტატია გამოქვეყნდა პრესაში, გამოხატვის თავისუფლება კი ECHR-ის მიერ დაცული ერთ-ერთი ფუნდამენტური უფლებაა. თუმცა, სასამართლომ იმსჯელა, რამდენად ამართლებდა საჯარო ინტერესი ამ ინფორმაციის გამოქვეყნებას და დაადგინა, რომ გამოქვეყნების ძირითადი მიზანი გახლდათ გაზეთის გაყიდვების გაზრდა მკითხველის ცნობისმოყვარეობის დაკმაყოფილების ხარჯზე. ვინაიდან ეს იყო „პრესის თავისუფლების ბოროტად გამოყენების მძიმე შემთხვევა“, ზიანის ანაზღაურებაზე დაწესებული მკაცრი შეზღუდვები და არამატერიალური ეროვნული კანონმდებლობით დადგენილი მინიმალური ზღვარი ზიანის ასანაზღაურებლად ნიშნავდა, რომ ლიეტუვამ ვერ შეძლო საკუთრი პოზიტიური მოვალეობების შესრულება განმცხადებლის პირადი ცხოვრების უფლების დასაცავად. შესაბამისად, ECtHR-მა საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

გამოხატვის თავისუფლება და პერსონალურ მონაცემთა დაცვის უფლება ყოველთვის არ ეწინააღმდეგება ერთმანეთს. არსებობს მაგალითები, თუ როგორ უზრუნველყოფს პეროსნალურ მონაცემთა ეფექტიანი დაცვა გამოხატვის თავისუფლებას.

მაგალითი: CJEU-მ *Tele2 Sverige-ს* საქმეში დაადგინა, რომ ქარტიის მე-7 და მე-8 მუხლებით დაცულ ფუნდამენტურ უფლებებში ჩარევა 2006/24 დირექტივის (მონაცემთა შენახვის დირექტივა) საფუძველზე იყო „ფართომასშტაბიანი და განსაკუთრებით მძიმე [ჩარევა]. ამასთან, ის ფაქტი, რომ მონაცემებს ინახავენ და იყენებენ გამომწერის ან რეგისტრირებული მომხმარებლის ინფორმირების გარეშე, სავარაუდოდ, შესაბამის პირებს

უჩენს განცდას, რომ მათ პირად ცხოვრებას მუდმივად უთვალთვალებენ.“ CJEU-მ ასევე დაადგინა, რომ გადაადგილებისა და ადგილმდებარეობის განმსაზღვრელი მონაცემების განზოგადებულმა შენახვამ შესაძლოა გავლენა მოახდინოს ელექტრონული კომუნიკაციების გამოყენებაზე და, „შესაბამისად, [ელექტრონული კომუნიკაციების] მომხმარებელთა გამოხატვის თავისუფლების რეალიზებაზე, რომელიც გარანტირებულია ქარტიის მე-11 მუხლით.“[98] ამ მხრივ, მონაცემთა დაცვის წესები, მოთხოვნით მკაცრი დაცვის მექანიზმების დაწესებაზე, რომ მონაცემები არ ინახებოდეს განზოგადებულად, საბოლოო ჯამში, ხელს უწყობს გამოხატვის თავისუფლების რეალიზებას.

რაც შეეხება ინფორმაციის მიღებას, რაც გამოხატვის თავისუფლების ნაწილია, სულ უფრო და უფრო ცხადდება მთავრობის გამჭვირვალობის მნიშვნელობა დემოკრატიული საზოგადოების ფუნქციონირებაში. გამჭვირვალობა საჯარო ინტერესის საკითხია და შეიძლება გაამართლოს მონაცემთა დაცვის უფლებაში ჩარევა, თუ ეს აუცილებელი და პროპორციულია 1.2 ნაწილში წარმოდგენილი განმარტების თანახმად. შედეგად, გასული ათწლეულების განმავლობაში, საჯარო ორგანოების ხელთ არსებულ ინფორმაციაზე წვდომა მნიშვნელოვან უფლებად არის აღიარებული ევროკავშირის ნებისმიერი მოქალაქისათვის, ასევე, ფიზიკური თუ იურიდიული პირისთვის, რომელიც ცხოვრობს ან რომელსაც რეგისტრირებული აქვს ოფისი წევრ სახელმწიფოში.

ევროპის საბჭოს კანონმდებლობის თანახმად, შეიძლება მითითება იმ პრინციპებზე, რომლებიც წარმოდგენილია რეკომენდაციაში ოფიციალურ დოკუმენტებზე წვდომის შესახებ (ოფიციალურ დოკუმენტებზე ხელმისაწვდომობის კონვენციის (205-ე კონვენცია) შემქმნელთა ინსპირაციის წყარო).[99]

ევროკავშირის კანონმდებლობის თანახმად, დოკუმენტების ხელმისაწვდომობის უფლებას ადგენს რეგულაცია 1049/2001, რომელიც ითვალისწინებს საჯარო წვდომას ევროპული პარლამენტის, საბჭოსა და კომისიების დოკუმენტებზე (დოკუმენტების ხელმისაწვდომობის რეგულაცია).[100] ქარტიის 42-ე

98 CJEU, გაერთიანებული საქმეები C-203/15 და C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* [GC], 2016 წლის 21 დეკემბერი, პუნქტი 37 და 101; CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი, პუნქტი 28.

99 ევროპის საბჭო, მინისტრთა კომიტეტი (2002), რეკომენდაციები R(81)19 და Rec(2002)2, რომელიც შეეხება ოფიციალურ დოკუმენტებზე წვდომას, 2002 წლის 21 თებერვალი; ევროპის საბჭო, კონვენცია ოფიციალურ დოკუმენტებზე წვდომის შესახებ, CETS No. 205, 2008 წლის 18 ივნისი, კონვენცია ძალაში ჯერ არ შესულა.

100 ევროპის პარლამენტისა და საბჭოს 2001 წლის 30 მაისის რეგულაცია (EC) No. 1049/2001 ევროპის პარლამენტის, საბჭოსა და კომისიის დოკუმენტების წვდომაზე, OJ 2001 L 145;

მუხლი და TFEU-ს მე-15 მუხლის მე-3 პუნქტი ვრცელდება „ევროკავშირის ინსტიტუტების, ორგანოების, ოფისებისა და სააგენტოების დოკუმენტთა“ ხელმისაწვდომობის უფლებაზე, მათი ფორმის მიუხედავად.

ეს უფლება შეიძლება ეწინააღმდეგებოდეს მონაცემთა დაცვის უფლებას, თუ დოკუმენტებზე ხელმისაწვდომობით სხვების პერსონალური მონაცემები გამჟღავნდება. მონაცემთა დაცვის ზოგადი რეგულაციის 86-ე მუხლი ცალსახად ადგენს, რომ საჯარო უწყებებისა და ორგანოების ხელთ არსებულ ოფიციალურ დოკუმენტებში წარმოდგენილი პერსონალური მონაცემები შეიძლება გაამჟღავნოს შესაბამისმა საჯარო უწყებამ და ორგანომ ევროკავშირის[101] ან წევრი სახელმწიფოს კანონმდებლობის შესაბამისად, რათა პერსონალური მონაცემების დაცვა შეუთავსონ ოფიციალურ დოკუმენტებზე წვდომის უფლებას.

ამრიგად, შესაძლოა საჭირო გახდეს საჯარო უწყებების ხელთ არსებულ მონაცემებსა ან ინფორმაციაზე წვდომის დაბალანსება იმ პირთა მონაცემების დაცვის უფლებასთან, რომლებსაც ეხება მოთხოვნილი დოკუმენტები.

მაგალითები: საქმეში *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen*[102] CJEU-მ იმსჯელა ევროკავშირის სასოფლო სამეურნეო სუბსიდიების ბენეფიციართა სახელებისა და მათ მიერ მიღებული თანხის გამოქვეყნების პროპორციულობაზე, ევროკავშირის კანონმდებლობის შესაბამისად. ამ მონაცემების გამოქვეყნების მიზანი იყო გამჭვირვალობის გაუმჯობესება და საჯარო კონტროლის ხელშეწყობა საზოგადოებრივი სახსრების სათანადო გამოყენებაზე ადმინისტრაციის მხრიდან. რამდენიმე ბენეფიციარმა ამ ინფორმაციის გამოქვეყნება გაასაჩივრა.

CJEU-მ განმარტა, რომ მონაცემთა დაცვის უფლება არ არის აბსოლუტური. მისი განაცხადებით, ვებგვერდზე ისეთი მონაცემების გამოქვეყნება, რომლებიც შეიცავდა ევროკავშირის სასოფლო-სამეურნეო დახმარების ორი ფონდის ბენეფიციართა სახელებსა და მათ მიერ მიღებული დაფინანსების ზუსტ ოდენობას, იყო ჩარევა ზოგადად მათ პირად ცხოვრებაში და, კერძოდ, პერსონალურ მონაცემთა დაცვის უფლებაში.

CJEU-მ დაადგინა, რომ ქარტიის მე-7 და მე-8 მუხლებში ჩარევა კანონით იყო გათვალისწინებული და აკმაყოფილებდა ევროკავშირის მიერ აღიარებულ საჯარო ინტერესის სტანდარტს - კერძოდ, საერთო სახსრების გამოყენების გამჭვირვალობას. ამავდროულად, CJEU-მ განმარტა, რომ იმ ფიზიკური პირების სახელების გამოქვეყნება, რომლებიც ევროკავშირის

101 ქარტიის 42-ე მუხლი, TFEU-ს 15(3) მუხლი და რეგულაცია 1049/2009.

102 CJEU, გაერთიანებული საქმეები C-92/09 და C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 2010 წლის 9 ნოემბერი, პუნქტები 47–52, 58, 66–67, 75, 86 და 92.

სასოფლო-სამეურნეო დახმარების ორი ფონდის ბენეფიციარები იყვნენ, ასევე, მათ მიერ მიღებული დახმარების ზუსტი ოდენობის გასაჯაროება არაპროპორციული ღონისძიება გახლდათ და, ქარტიის 52-ე მუხლის პირველი პუნქტის გათვალისწინებით, არ იყო გამართლებული. სასამართლომ აღიარა, რომ დემოკრატიულ საზოგადოებაში მნიშვნელოვანია გადასახადების გადამხდელთა ინფორმირება საზოგადოებრივი სახსრების გამოყენებაზე. ამავდროულად, „გამჭვირვალობას, პერსონალურ მონაცემთა დაცვის უფლებასთან შედარებით, პრიორიტეტი ავტომატურად ვერ მიენიჭებოდა“.[103] შესაბამისად, ევროკავშირის ინსტიტუტებს მოეთხოვებოდათ, ევროკავშირის ინტერესი გამჭვირვალობის მიმართ დაებალანსებინათ შეზღუდვასთან, რომელიც აღნიშნული მონაცემების გამოქვეყნების შედეგად დაწესდა ბენეფიციართა პირადი ცხოვრებისა და მონაცემთა დაცვის უფლებებზე.

CJEU-მ დაადგინა, რომ ევროკავშირის ინსტიტუტებმა ვერ შეძლეს მათი სათანადოდ დაბალანსება, რადგან შესაძლებელი იყო ისეთი ღონისძიებების გათვალისწინება, რომლებიც ნაკლებად დააზიანებდა ფიზიკური პირების ფუნდამენტურ უფლებებს და ეფექტიანად შეუწყობდა ხელს გამჭვირვალობას, რასაც გამოქვეყნება ემსახურებოდა. მაგალითად, ყველა ბენეფიციარის სახელისა და მათ მიერ მიღებული დაფინანსების გამოქვეყნების ნაცვლად, შესაძლებელი იყო გარკვეული განსხვავებების გამოკვეთა შესაბამისი კრიტერიუმების საფუძველზე (მაგ.: დროის მონაკვეთები, როცა ამ პირებმა მიიღეს დახმარება, დახმარების სიხშირე, რაოდენობა და ბუნება).[104] შესაბამისად, CJEU-მ ნაწილობრივ გაუქმებულად გამოაცხადა ევროკავშირის კანონმდებლობა იმ ინფორმაციის გამოქვეყნებასთან მიმართებით, რომელიც ევროპული სასოფლო-სამეურნეო ფონდების ბენეფიციარებს უკავშირდება.

საქმეში *Rechnungshof v. Österreichischer Rundfunk and Others*[105] CJEU-მ იმსჯელა ავსტრიული კანონმდებლობის შესაბამისობაზე ევროკავშირის მონაცემთა დაცვის სამართალთან. კანონმდებლობის თანახმად, სახელმწიფო ორგანოს მოეთხოვება მონაცემთა შეგროვება და გადაცემა შემოსავლის შესახებ, სხვადასხვა საჯარო დაწესებულების თანამშრომელთა ვინაობისა და შემოსავლის გამოსაქვეყნებლად ყოველწლიურ ანგარიშში, რომელიც ხელმისაწვდომია ფართო საზოგადოებისთვის. ზოგიერთმა პირმა უარი განაცხადა მონაცემების მიწოდებაზე, რაც დაასაბუთა მონაცემთა დაცვის არგუმენტით.

103 *იქვე,* პუნქტი 85.

104 *იქვე,* პუნქტი 89.

105 CJEU, C-465/00, C-138/01 და C-139/09, *Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Jospeh Lauermann v. Österreichischer Rundfunk*, 2003 წლის 20 მაისი.

წარმოდგენილი საკითხის შეფასებისას CJEU დაეყრდნო ფუნდამენტურ უფლებათა დაცვას, როგორც ევროკავშირის სამართლის ზოგად პრინციპს, და ECHR-ის მე-8 მუხლს, აღნიშნა რა, რომ ქარტიას იმ დროს სავალდებულოდ შესასრულებელი ძალა არ ჰქონდა. მან დაადგინა, რომ პიროვნების პროფესიული საქმიანობით მიღებულ შემოსავლზე მონაცემების შეგროვება და გადაცემა მესამე პირებისთვის, პირადი ცხოვრების უფლების მოქმედების სფეროში ექცევა და არღვევს მას. ჩარევა გამართლებულია, თუ იგი არის კანონით გათვალისწინებული, კანონიერი მიზნის შესაბამისი და აუცილებელი დემოკრატიულ საზოგადოებაში. CJEU-მ აღნიშნა, რომ ავსტრიის კანონმდებლობა ემსახურებოდა კანონიერ მიზანს, რადგან მის ამოცანა იყო საჯარო მოსამსახურეთა ხელფასების გონივრულ საზღვრებში შენარჩუნება, რაც უკავშირდება ქვეყნის ეკონომიკურ კეთილდღეობას. თუმცა, ავსტრიის ინტერესი საჯარო სახსრების ეფექტიანი გამოყენების მიმართ უნდა დაბალანსებულიყო შესაბამის პირთა პირადი ცხოვრების უფლებაზე დაწესებული შეზღუდვის სიმძიმესთან.

CJEU-მ ეროვნული სასამართლოების უფლებამოსილებაში დატოვა იმის დადგენა, რამდენად აუცილებელი და კანონიერი მიზნის პროპორციული იყო ფიზიკური პირის შემოსავლების გამოქვეყნება, თუმცა ეროვნულ სასამართლოებს მოუწოდა, შეეფასებინათ, შეიძლებოდა თუ არა იმავე მიზნის მიღწევა მსგავსი ეფექტის მქონე სხვა ნაკლებინვაზიური საშუალებით (მაგ.: პერსონალური მონაცემების გადაცემა მხოლოდ ზედამხედველი სახელმწიფო ორგანოსთვის და არა ფართო საზოგადოებისთვის).

ქვემოთ განხილული საქმეები ნათლად ადასტურებს, რომ მონაცემთა დაცვისა და დოკუმენტებზე ხელმისაწვდომობის დაბალანსება თითოეულ შემთხვევაში საჭიროებს დეტალურ ანალიზს და ვერცერთი უფლება ვერ გადაწონის რომელიმე სხვას ავტომატურად. ამ ორი საქმის განხილვისას CJEU-ს ჰქონდა საშუალება, განემარტა პერსონალურ მონაცემთა შემცველ დოკუმენტებზე ხელმისაწვდომობის უფლება.

მაგალითები: საქმეში *European Commission v. Bavarian Lager*[106] CJEU-მ განსაზღვრა მონაცემთა დაცვის ფარგლები ევროკავშირის ინსტიტუტების ხელთ არსებულ დოკუმენტებზე წვდომის კონტექსტში, ასევე, ურთიერთქმედება No. 1049/2001 და No. 45/2001 რეგულაციებს შორის. 1992 წელს დაარსებული Bavarian Lager გერმანული ლუდის იმპორტს ახორციელებს გაერთიანებულ სამეფოში, ძირითადად ლუდხანებისა და ბარებისათვის. თუმცა კომპანია გარკვეულ სირთულეებს გადააწყდა, რადგან ბრიტანული კანონმდებლობა de facto უპირატეს მდგომარეობაში

106 CJEU, C-28/08 *P*, *European Commission v. The Bavarian Lager Co. Ltd.* [GC], 2010 წლის 29 ივნისი.

აყენებდა ადგილობრივ მწარმოებლებს. Bavarian Lager-ის სარჩელზე რეაგირების მიზნით, ევროკომისიამ დაიწყო გაერთიანებული სამეფოს მხრიდან ვალდებულებათა შეუსრულებლობის განხილვა, რის შემდეგაც მას მოუწია სადავო დებულებების შეცვლა და ჰარმონიზება ევროკავშირის კანონმდებლობასთან. ამის შემდეგ, Bavarian Lager-მა კომისიას მიმართა, რათა სხვა დოკუმენტებთან ერთად, წარმოედგინა იმ შეხვედრის ოქმის ასლი, რომელსაც ესწრებოდნენ ევროკომისიის, ბრიტანეთის შესაბამისი უწყებებისა და Confédération des Brasseurs du Marché Commun (CBMC)-ის წარმომადგენლები. ევროკომისია დათანხმდა შეხვედრის გარკვეული დოკუმენტების გამოქვეყნებას, თუმცა ოქმში მითითებული ხუთი პიროვნების სახელი დაფარა, რადგან ორმა ცალსახად უარი განაცხადა თავისი ვინაობის გამხელაზე, დანარჩენ სამს კი ევროკომისია ვერ დაუკავშირდა. 2004 წლის 18 მარტის გადაწყვეტილებით, ევროკომისიამ უარი განაცხადა Bavarian Lager-ის ახალი საჩივრის დაკმაყოფილებაზე, რომელიც შეეხებოდა შეხვედრის ოქმის სრული ვერსიის წარმოდგენას. მიზეზად მიუთითა შესაბამის პირთა პირადი ცხოვრების უფლების დაცვა, რაც გარანტირებული იყო ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაციით.

ვინაიდან კომპანიის მოთხოვნა არ დაკმაყოფილდა, Bavarian Lager-მა სარჩელით მიმართა პირველი ინსტანციის სასამართლოს, რომელმაც გააუქმა ევროკომისიის 2007 წლის 8 ნოემბრის გადაწყვეტილება (საქმე T-194/04, *The Bavarian Lager Co. Ltd v. Commission of the European Communities*) და დაადგინა: ჩამონათვალში მხოლოდ სახელების შეტანა იმ პირებისა, რომლებიც შეხვედრას ესწრებოდნენ, როგორც საკუთარი ორგანიზაციების წარმომადგენლები, არ იყო პირადი ცხოვრების უფლების შეზღუდვა და არ უქმნიდა საფრთხეს ამ ადამიანთა პირად ცხოვრებას.

ევროკომისიის მხრიდან გასაჩივრების შედეგად, CJEU-მ გააუქმა პირველი ინსტანციის სასამართლოს გადაწყვეტილება. მან დაადგინა, რომ რეგულაცია დოკუმენტებზე წვდომის შესახებ განსაზღვრავს „მკაფიო და მტკიცე სისტემას იმ პირთა დასაცავად, რომელთა პერსონალური მონაცემების მიწოდება საზოგადოებისათვის, გარკვეულ შემთხვევებში, შესაძლებელია. CJEU-ს განმარტებით, როდესაც პერსონალური მონაცემების შემცველ დოკუმენტებზე წვდომის მოთხოვნა ეფუძნება დოკუმენტებზე წვდომის რეგულაციას, ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაციის დებულებები ამოქმედდება ერთობლიობაში. CJEU-ს დასკვნით, კომისიას ჰქონდა უფლება, არ დაეკმაყოფილებინა 1996 წლის ოქტომბერში გამართული სხდომის მთლიან ოქმზე ხელმისაწვდომობის მოთხოვნა. შეხვედრის ხუთი მონაწილის თანხმობის არარსებობის პირობებში, კომისიამ საკმარისად დააკმაყოფილა ღიაობის ვალდებულება და გასცა დოკუმენტის ის ვერსია, სადაც შესაბამისი სახელები ამოღებული იყო.

ამასთან, CJEU-ს განმარტებით, „ვინაიდან Bavarian Lager-მა არ წარმოადგინა რაიმე მკაფიო და კანონიერი საფუძველი ან დამაჯერებელი არგუმენტები, რითაც დადასტურდებოდა პერსონალურ მონაცემთა გამჟღავნების აუცილებლობა, კომისიას არ ჰქონდა შესაძლებლობა, ერთმანეთთან შეედარებინა მხარეთა განსხვავებული ინტერესები; ასევე, ემსჯელა, არსებობდა თუ არა რაიმე საფუძველი, რომ მონაცემთა სუბიექტის კანონიერ ინტერესებს ზიანი მიადგებოდა“, ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაციის შესაბამისად.

საქმეში *Client Earth and PAN Europe v. EFSA*[107] CJEU-მ იმსჯელა, რამდენად აუცილებელი იყო ევროპის სურსათის უვნებლობის სააგენტოს (EFSA) უარი კონკრეტული დოკუმენტების ხელმისაწვდომობაზე, მათში მითითებული ადამიანების პირადი ცხოვრებისა და მონაცემთა დაცვის უფლებების დასაცავად. დოკუმენტები შეეხებოდა სახელმძღვანელო ანგარიშის პროექტს, რომელიც EFSA-ს სამუშაო ჯგუფმა გარე ექსპერტებთან ერთად მოამზადა ბაზარზე ნარგავების დაცვის პროდუქტთა განთავსებასთან დაკავშირებით. თავიდან EFSA-მ მომჩივნებს მიაწოდა დოკუმენტების ნაწილი და უარი თქვა სახელმძღვანელო ანგარიშის პროექტის ზოგიერთი სამუშაო ვერსიის მიწოდებაზე. კერძოდ, მან მომჩივნებს წარუდგინა ის პროექტი, რომელიც გარე ექსპერტების ინდივიდუალურ კომენტარებს შეიცავდა. თუმცა, სააგენტომ დოკუმენტიდან ამოშალა მათი სახელები და მიუთითა 45/2001 რეგულაციის მე-4 მუხლის 1 (ბ) პუნქტზე, რომელიც შეეხება პერსონალურ მონაცემთა დამუშავებას ევროკავშირის ინსტიტუტებისა და უწყებების მიერ და გარე ექსპერტთა პირადი ცხოვრების დაცვის საჭიროებას. ევროკავშირის გენერალური სასამართლოს პირველმა ინსტანციამ EFSA-ს გადაწყვეტილება უცვლელი დატოვა.

განმცხადებლების მიერ წარდგენილი საჩივრის საფუძველზე, CJEU-მ გააუქმა პირველი ინსტანციის სასამართლოს გადაწყვეტილება. მან დაასკვნა, რომ კონკრეტულ შემთხვევაში პერსონალური მონაცემების გადაცემა აუცილებელი იყო თითოეული გარე ექსპერტის მიუკერძოებლობის დასადგენად მათი, როგორც მეცნიერების მიერ დავალების შესრულების პროცესში, ასევე, იმის დასადასტურებლად, რომ EFSA-ში გადაწყვეტილებები გამჭვირვალედ მიიღება. CJEU-ს თანახმად, EFSA-ს არ დაუკონკრეტებია, როგორ აზიანებდა მათ კანონიერ ინტერესებს იმ გარე ექსპერტთა ვინაობის გამჟღავნება, რომლებმაც სახელმძღვანელო დოკუმენტის პროექტზე კონკრეტული კომენტარები შეიმუშავეს. ზოგადი არგუმენტი, რომ ეს, სავარაუდოდ, ზიანს მიაყენებდა მათ პირად ცხოვრებას, არ იყო საკმარისი, რადგან თითოეულ კონკრეტულ შემთხვევასთან დაკავშირებით შესაბამისი მტკიცებულება არ წარმოდგენილა.

107 CJEU, C-615/13P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*, 2015 წლის 16 ივლისი.

აღნიშნული გადაწყვეტილებების თანახმად, მონაცემთა დაცვის უფლებაში ჩარევა დოკუმენტებზე წვდომის კონტექსტში საჭიროებს კონკრეტულ და გამართლებულ მიზეზს. დოკუმენტებზე ხელმისაწვდომობის უფლება ავტომატურად ვერ გადაწონის მონაცემთა დაცვის უფლებას.[108]

აღნიშნული მიდგომა მსგავსია ECtHR-ის მიდგომისა პირად ცხოვრებასა და დოკუმენტებზე წვდომასთან დაკავშირებით, რაც ნათლად ჩანს ქვემოთ წარმოდგენილ გადაწყვეტილებებში. *Magyar Helsinki*-ს საქმეში ECtHR-მა დაადგინა, რომ მე-19 მუხლი ფიზიკურ პირებს არ ანიჭებდა უფლებას საჯარო უწყებების ხელთ არსებული მონაცემების წვდომაზე და მთავრობას არ აკისრებდა ასეთი ინფორმაციის ფიზიკური პირისათვის გადაცემის ვალდებულებას. თუმცა, ეს უფლება და მოვალეობა შესაძლოა მომდინარეობდეს შემდეგი გარემოებებიდან: თუ (1) მონაცემის გამჟღავნების ვალდებულებას აწესებს სასამართლოს კანონიერ ძალაში შესული გადაწყვეტილება; და (2) ინფორმაციაზე წვდომა მნიშვნელოვანია პიროვნების გამოხატვის თავისუფლების, კერძოდ, ინფორმაციის მიღებისა და გაცემის თავისუფლების რეალიზებისათვის, ხელმისაწვდომობაზე უარი კი შეზღუდავს აღნიშნულ უფლებას.[109] არის თუ არა ინფორმაციაზე ხელმისაწვდომობა ჩარევა განმცხადებლის გამოხატვის თავისუფლებაში, უნდა შეფასდეს თითოეული საქმის კონკრეტული გარემოებების გათვალისწინებით. ესენია: (i) ინფორმაციის მოთხოვნის მიზანი; (ii) მოთხოვნილი ინფორმაციის ბუნება; (iii) განმცხადებლის როლი; და (iv) არის თუ არა ეს ინფორმაცია მზა და ხელმისაწვდომი.

მაგალითი: საქმეში *Magyar Helsinki Bizottság v. Hungary*[110] განმცხადებელი, რომელიც წარმოადგენდა ადამიანის უფლებათა დამცველ არასამთავრობო ორგანიზაციას, პოლიციისაგან ითხოვდა ინფორმაციას *ex officio* ადვოკატის საქმიანობასთან დაკავშირებით, რათა დაესრულებინა კვლევა უნგრეთში არსებული სახალხო დამცველის სისტემის ფუნქციონირებაზე. პოლიციამ უარი თქვა აღნიშნული ინფორმაციის მიწოდებაზე, იმ მიზეზით, რომ პერსონალურ მონაცემებს შეიცავდა და არ უნდა გამჟღავნებულიყო. ზემოთ განხილული კრიტერიუმების გამოყენებით, ECtHR-მა დაადგინა, რომ ეს იყო ჩარევა მე-10 მუხლით დაცულ უფლებაში. კერძოდ, განმცხადებელს სურდა ინფორმაციის გაცემის უფლების რეალიზება საჯარო ინტერესის საკითხთან დაკავშირებით, რისთვისაც მოითხოვა ინფორმაციაზე წვდომა, ხოლო თავად ინფორმაცია საჭირო იყო განმცხადებლის

108 EDPS-ში დეტალური განხილვებისათვის, იხ. *Public access to documents containing personal data after the Bavarian Lager ruling*, ბრიუსელი, 2011 წლის 24 მარტი.

109 ECtHR, *Magyar Helsinki Bizottság v. Hungary* [GC], No. 18030/11, 2016 წლის 8 ნოემბერი, პუნქტი 148.

110 *იქვე,* პუნქტები 181, 187–200.

გამოხატვის უფლების უზრუნველსაყოფად. სახალხო დამცველების დანიშვნაზე ინფორმაცია საჯარო ინტერესის საკითხი იყო. არ არსებობდა მიზეზი ეჭვის შესატანად, რომ აღნიშნული კვლევა მოიცავდა ინფორმაციას, რომლის საზოგადოებისთვის გადაცემაც სურდა განმცხადებელს, საზოგადოებას კი ჰქონდა ამ ინფორმაციის მიღების უფლება. ამრიგად, სასამართლომ დაადგინა, რომ მოთხოვნილ ინფორმაციაზე წვდომა საჭირო იყო განმცხადებლის მიერ აღნიშნული დავალების შესასრულებლად. და ბოლოს, ინფორმაცია არსებობდა მზა და ხელმისაწვდომი ფორმით.

ECtHR-მა დაასკვნა, რომ უარი ინფორმაციაზე ხელმისაწვდომობის შესახებ, კონკრეტულ შემთხვევაში დააზიანებდა ინფორმაციის მიღების თავისუფლებას. ამ დასკვნამდე სასამართლო მივიდა მას შემდეგ, რაც განიხილა მოთხოვნილი ინფორმაციის კონკრეტული მიზანი და მისი წვლილი მნიშვნელოვან საჯარო დისკუსიაში, ასევე, მოთხოვნილი ინფორმაციის ბუნება, საზოგადოების ინტერესი მის მიმართ და კონკრეტული განმცხადებლის როლი საზოგადოებაში.

სასამართლომ მსჯელობისას აღნიშნა, რომ არასამთავრობო ორგანიზაციის კვლევა შეეხებოდა სასამართლო სისტემის საქმიანობას და სამართლიანი სასამართლოს უფლებას, რომელსაც უაღრესად დიდი მნიშვნელობა ენიჭება ადამიანის უფლებათა ევროპული კონვენციით. ვინაიდან მოთხოვნილი ინფორმაცია არ შეიცავდა მონაცემებს საყოველთაო საკუთრების მიღმა, მონაცემთა სუბიექტების (*ex officio* სახალხო დამცველები) პირადი ცხოვრების უფლებას ზიანი არ მიადგებოდა, თუკი პოლიცია ამ ინფორმაციას მომჩივნებს მიაწვდიდა. მომჩივნების მიერ მოთხოვნილი ინფორმაცია იყო სტატისტიკური და უკავშირდებოდა იმას, თუ რამდენჯერ დაენიშნათ *ex-officio* ადვოკატი სისხლის სამართლის დანაშაულში ბრალდებულ პირებს.

სასამართლოს აზრით, ვინაიდან კვლევა მიზნად ისახავდა წვლილის შეტანას მნიშვნელოვან დისკუსიაში საჯარო ინტერესის საკითხის შესახებ, ნებისმიერი შეზღუდვის დაწესება იმ გამოცემაზე, რომელზეც არასამთავრობო ორგანიზაცია მუშაობდა, მაქსიმალურად უნდა გაკონტროლებულიყო. მოთხოვნილი ინფორმაცია საჯარო ინტერესის საგანი გახლდათ, ხოლო საჯარო ინტერესი მოიცავს „ისეთ საკითხებს, რომლებსაც აქვს პოტენციალი, საკმაო უთანხმოება წარმოშვას მნიშვნელოვან სოციალურ საკითხთან დაკავშირებით, ან პრობლემას, რომელზე ინფორმირების ინტერესიც ექნებოდა საზოგადოებას.“[111] ნათელია, რომ ეს ითვალისწინებს მართლმსაჯულების განხორციელებისა და სამართლიანი სასამართლოს საკითხსაც, რაც განმცხადებლის კვლევის საგანი გახლდათ. წარმოდგე-

111 *იქვე*, პუნქტი 156.

ნილ უფლებათა დაბალანსებითა და პროპორციულობის პრინციპზე დაყრდნობით, ECtHR-მა დაადგინა, რომ ამ საქმეში განმცხადებლის წინააღმდეგ უსამართლოდ დაირღვა ECHR-ის მე-10 მუხლით დაცული უფლება.

1.3.2 პროფესიული საიდუმლოება

ეროვნული კანონმდებლობის თანახმად, გარკვეულ კომუნიკაციაზე შეიძლება გავრცელდეს პროფესიული საიდუმლოს შენახვის ვალდებულება. ეს სპეციალური ეთიკური მოვალეობაა, რომელიც წარმოშობს გარკვეული პროფესიებისა და ფუნქციებისთვის დამახასიათებელ სამართლებრივ ვალდებულებას, დაფუძნებულს რწმენასა და ნდობაზე. ასეთი ფუნქციების შემსრულებელი ფიზიკური პირები და დაწესებულებები ვალდებულნი არიან, არ გათქვან კონფიდენციალური ინფორმაცია, რომელსაც ისინი ეუფლებიან თავიანთი მოვალეობების შესრულებისას. პროფესიული საიდუმლოება განსაკუთრებულად ეხება სამედიცინო პროფესიასა და ადვოკატ-კლიენტის ურთიერთობას, ხოლო არაერთ იურისდიქციაში აღიარებულია ფინანსურ სექტორთან დაკავშირებული პროფესიული საიდუმლოს შენახვის ვალდებულებაც. პროფესიული საიდუმლო არ არის ფუნდამენტური უფლება, თუმცა დაცულია, როგორც პირადი ცხოვრების პატივისცემის უფლების ერთ-ერთი ფორმა. მაგალითად, CJEU-მ დაადგინა, რომ ზოგიერთ საქმეში „პირადი ცხოვრების პატივისცემის ფუნდამენტური უფლების დასაცავად, რაც გარანტირებულია ECHR-ისა და ქარტიის მე-8 მუხლებით, საჭიროა გარკვეული ინფორმაციის გამჟღავნების აკრძალვა, რომელიც კონფიდენციალურად მიიჩნევა.“[112] ECtHR-ის მსჯელობა, არღვევს თუ არა პროფესიულ საიდუმლოებაზე შეზღუდვის დაწესება მის მე-8 მუხლს, წარმოდგენილია ქვემოთ განხილულ მაგალითებში.

მაგალითები: საქმეში *Pruteanu v. Romania*[113] განმცხადებლის, ერთ-ერთი კომერციული კომპანიის ადვოკატს, აეკრძალა საბანკო ტრანზაქციები თაღლითობის ბრალდების გამო. საქმის გამოძიების პროცესში, რუმინულმა სასამართლოებმა პროკურატურას მისცეს ნებართვა, რომ გარკვეული დროის განმავლობაში მოესმინათ და ჩაეწერათ კომპანიის პარტნიორის სატელეფონო საუბრები, მათ შორის, ადვოკატთანაც.

ბატონი პრუტენუ აცხადებდა, რომ მის წინააღმდეგ დაირღვა პირადი ცხოვრებისა და კორესპონდენციის პატივისცემის უფლება. ECtHR-მა მიღებულ გადაწყვეტილებაში ხაზი გაუსვა ადვოკატისა და კლიენტის ურთიერთო-

112 CJEU, Case T-462/12 R, *Pilkington Group Ltd v. European Commission,* Order of the President of the General Court, 2013 წლის 11 მარტი, პუნქტი 44.

113 ECtHR, *Pruteanu v. Romania* No. 30181/05, 2015 წლის 3 თებერვალი.

ბის სტატუსსა და მნიშვნელობას. მათ შორის საუბრების მოსმენა ცალსახად არღვევდა პროფესიულ საიდუმლოებას, რაც ამ ორ ადამიანს შორის ურთიერთობის საფუძველი გახლდათ. ასეთ შემთხვევაში, ადვოკატს შეეძლო სარჩელის შეტანა პირადი ცხოვრებისა და კორესპონდენციის უფლებაში ჩარევის გამოც. სასამართლომ საქმეში დაადგინა ECHR-ის მე-8 მუხლის დარღვევა.

საქმეში *Brito Ferrinho Bexiga Villa-Nova v. Portugal*[114] განმცხადებელი, რომელიც იყო ადვოკატი, უარს აცხადებდა პირადი საბანკო ამონაწერების საგადასახადო ორგანოებისათვის გადაცემაზე იმ მოტივით, რომ ეს არღვევდა პროფესიულ კონფიდენციალობასა და საბანკო საიდუმლოებას. პროკურატურამ საგადასახადო თაღლითობის შესახებ დაწყებულ გამოძიებასთან დაკავშირებით მოითხოვა პროფესიული კონფიდენციალობის გაუქმება. ეროვნულმა სასამართლოებმა გაიზიარეს პროკურატურის პოზიცია, შეაჩერეს კონფიდენციალობისა და საბანკო საიდუმლოების წესები კონკრეტულ შემთხვევასთან დაკავშირებით და დაადგინეს, რომ საჯარო ინტერესი აღემატებოდა განმცხადებლის პირად ინტერესებს.

როდესაც საქმემ ECtHR-მდე მიაღწია, სასამართლომ დაადგინა, რომ განმცხადებლის საბანკო ანგარიშებზე წვდომა იყო ჩარევა მისი პროფესიული კონფიდენციალობის უფლებაში, რაც პირადი ცხოვრების პატივისცემის ფარგლებში ექცევა. ჩარევას ჰქონდა კანონიერი საფუძველი, რამდენადაც იგი სისხლის სამართლის საპროცესო კოდექსს ეფუძნებოდა და ლეგიტიმურ მიზანს ემსახურებოდა. თუმცა, მისი აუცილებლობისა და პროპორციულობის შეფასებისას, ECtHR-მა მიუთითა, რომ საქმისწარმოება კონფიდენციალობის გაუქმების შესახებ განხორციელდა განმცხადებლის მონაწილეობისა ან ინფორმირების გარეშე, რის გამოც მას საკუთარი არგუმენტების წარმოდგენის საშუალება არ ჰქონდა. ამასთან, ეროვნული კანონმდებლობა ითვალისწინებდა ადვოკატთა ასოციაციასთან კონსულტაციას ასეთი წარმოებისას, თუმცა ამ შემთხვევაში ეს არ გაუკეთებიათ. დაბოლოს, განმცხადებელს არ ჰქონდა შესაძლებლობა, რომ ეფექტიანად გაესაჩივრებინა კონფიდენციალობის გაუქმება. მას არც სამართლებრივი დაცვის საშუალებაზე მიუწვდებოდა ხელი, რათა გაესაჩივრებინა ზომა. პროცედურული გარანტიებისა და კონფიდენციალობის გაუქმებაზე ეფექტიანი სასამართლო კონტროლის არარსებობის გამო, ECtHR-მა საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

ხშირად პროფესიულ საიდუმლოებასა და მონაცემთა დაცვას შორის კავშირი არ არის ცალსახა: ერთი მხრივ, მონაცემთა დაცვის წესები და მექანიზმები კა-

114 ECtHR, *Brito Ferrinho Bexiga Villa-Nova v. Portugal,* No. 69436/10, 2015 წლის 1 დეკემბერი.

ნონმდებლობაში შექმნილია პროფესიული საიდუმლოს დაცვის ხელშესაწყობად. მაგალითად, წესები, რომლებიც დამმუშავებლებსა და უფლებამოსილ პირებს უწესებს მოთხოვნას მონაცემთა უსაფრთხოების ზომების დანერგვაზე, მიზნად ისახავს პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალობის დარღვევის პრევენციას; ამასთან, ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია იძლევა ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავების შესაძლებლობას, რაც პერსონალურ მონაცემთა განსაკუთრებულ კატეგორიას განეკუთვნება და უფრო მაღალი დონის დაცვას მოითხოვს. თუმცა, ასეთი დამუშავებაზე ვრცელდება სათანადო და კონკრეტული ღონისძიებები მონაცემთა სუბიექტის უფლებების დასაცავად, კერძოდ, პროფესიული საიდუმლოს ჭრილში.[115]

მეორე მხრივ, პროფესიული საიდუმლოს შენახვის ვალდებულება, რომელიც მონაცემთა დამმუშავებლებსა და უფლებამოსილ პირებს ეკისრებათ გარკვეულ პერსონალურ მონაცემებთან დაკავშირებით, შეიძლება ზღუდავდეს მონაცემთა სუბიექტების უფლებებს, კერძოდ, ინფორმაციის მიღების უფლებას. მონაცემთა დაცვის ზოგადი რეგულაცია შეიცავს ვრცელ ჩამონათვალს, რომელი ინფორმაცია უნდა მიეწოდოს მონაცემთა სუბიექტს, თუ პერსონალური მონაცემები უშუალოდ მისგან არ გროვდება. გამჟღავნების ეს მოთხოვნა არ ვრცელდება, როცა საჭიროა პერსონალურ მონაცემთა კონფიდენციალობის დაცვა პროფესიული საიდუმლოს შენახვის ვალდებულების გამო, რომელსაც აწესებს შიდასახელმწიფოებრივი ან ევროკავშირის კანონმდებლობა.[116]

GDPR ითვალისწინებს წევრი სახელმწიფოების შესაძლებლობას, საკანონმდებლო დონეზე მიიღონ კონკრეტული წესები, რათა შეასრულონ პროფესიული ან სხვა თანაბრად მნიშვნელოვანი საიდუმლოს შენახვის ვალდებულება და მას შეუთავსონ პერსონალურ მონაცემთა დაცვის უფლება.[117]

GDPR-ის თანახმად, წევრ სახელმწიფოებს შეუძლიათ კონკრეტული წესების მიღება საზედამხედველო ორგანოს უფლებამოსილებაზე მონაცემთა დამმუშავებლებსა და უფლებამოსილ პირებთან დაკავშირებით, რომლებსაც აქვთ პროფესიული საიდუმლოების შენახვის ვალდებულება. ეს წესები მიემართება მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის მიერ მონაცემთა დამუშავებისათვის გამოყენებულ აღჭურვილობას, ასევე, დაცულ პერსონალურ მონაცემებზე წვდომას, როდესაც ისინი გროვდება საიდუმლოს შენახვის ვალდებულების მქონე სფეროებში. ამრიგად, საზედამხედველო ორგანოებმა, რომელთაც მონაცემთა დაცვა ევალებათ, პატივი უნდა სცენ პროფესიული საიდუმლოს შენახვის მოვალეობას, რომელსაც მონაცემთა დამმუშავებელებისა

115 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 9 (2) (თ) და 9 (3).

116 *იქვე,* მუხლი 14(5)(დ).

117 *იქვე,* პრეამბულის პუნქტი 164 და მუხლი 90.

და უფლებამოსილი პირებისათვის შესასრულებლად სავალდებულო ძალა აქვს. ამასთან, თვითონ საზედამხედველო ორგანოების წარმომადგენლებსაც ეკისრებათ პროფესიული საიდუმლოს შენახვის პასუხისმგებლობა - თანამდებობაზე ყოფნის პერიოდშიც და უფლებამოსილების ვადის ამოწურვის შემდგომაც. ამ ორგანოების თანამშრომლები, თავიანთი სამსახურებრივი მოვალეობების შესრულებისას, შეიძლება კონფიდენციალურ ინფორმაციას დაეუფლონ. რეგულაციის 54-ე მუხლის მე-2 პუნქტი მკაფიოდ აცხადებს, რომ ასეთ შემთხვევაში, მათ აქვთ პროფესიული საიდუმლოების შენახვის ვალდებულება.

GDPR წევრ სახელმწიფოებს ავალებს, რომ კომისიას შეატყობინონ იმ წესების შესახებ, რომლებიც სახელმწიფომ მიიღო მონაცემთა დაცვის ვალდებულების შესათავსებლად რეგულაციით დადგენილ პროფესიული საიდუმლოს შენახვის ვალდებულებასთან.

1.3.3 რელიგიისა და რწმენის თავისუფლება

რელიგიისა და რწმენის თავისუფლებას იცავს ECHR-ის მე-9 (აზრის, სინდისისა და რელიგიის თავისუფლება) და ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-10 მუხლები. ევროკავშირისა და ევროპის საბჭოს კანონმდებლობით, პერსონალური მონაცემები, რომლებიც რელიგიურ ან ფილოსოფიურ შეხედულებებს ამჟღავნებს, „განსაკუთრებულ კატეგორიას“ მიეკუთვნება, მათ დამუშავებასა და გამოყენებაზე კი ვრცელდება მაღალი დონის დაცვა.

მაგალითი: საქმეში *Sinak Isik v. Turkey*[118] განმცხადებელი იყო ალავიტების რელიგიური თემის წევრი. მის რწმენაზე გავლენას ახდენდა სუფიზმი და სხვა პრეისლამური შეხედულებები. ალევიზმს ზოგიერთი მეცნიერი ცალკე რელიგიურ მიმდინარეობად მიიჩნევს, ზოგი კი - ისლამური რელიგიის ნაწილად. განმცხადებელი აცხადებდა, რომ მისი ნების წინააღმდეგ, პირადობის დამადასტურებელი მოწმობა მის რელიგიად „ისლამს“ მიუთითებდა, ნაცვლად „ალევიზმისა“. ეროვნულმა სასამართლოებმა უარი თქვეს განმცხადებლის მოთხოვნის დაკმაყოფილებაზე პირადობის მოწმობაში „ალევიზმის“ ჩაწერის შესახებ, იმ მიზეზით, რომ ეს სიტყვა ისლამის ქვეჯგუფზე მიუთითებდა და არა ცალკე რელიგიაზე. განმცხადებელმა ადამიანის უფლებათა ევროპულ სასამართლოს მიმართა. იგი განაცხადში აცხადებდა, რომ საკუთარი ნების წინააღმდეგ დაეკისრა რწმენის გამჟღავნების მოთხოვნა, ვინაიდან პირადობის მოწმობაში აღმსარებლობის მითითება სავალდებულო იყო, ეს კი არღვევდა მისი რელიგიისა და სინდისის თავისუფლებას, განსაკუთრებით იმის გათვალისწინებით, რომ მის დოკუმენტში არასწორად იყო აღნიშნული „ისლამი“.

118 ECtHR, *Sinak Isik v. Turkey* No. 21924/05, 2010 წლის 2 თებერვალი.

ECtHR-მა კიდევ ერთხელ ხაზგასმით აღნიშნა, რომ რელიგიის თავისუფლება მოიცავს რელიგიის გაცხადების უფლებას არა მხოლოდ თემში - სხვებთან ერთად, საჯაროდ და იმავე რწმენის მიმდევართა შორის - არამედ ცალკე და განმარტოებითაც. იმ დროისათვის მოქმედი ეროვნული კანონმდებლობა ფიზიკურ პირებს პირადობის დამადასტურებელი ბარათის თან ქონას ავალებდა. ეს დოკუმენტი მფლობელს უნდა წარმოედგინა ნებისმიერი სახელმწიფო ორგანოს ან კერძო დაწესებულების მოთხოვნის საფუძველზე, მოწმობაში კი პიროვნების რელიგიური აღმსარებლობა იყო მითითებული. აღნიშნული ვალდებულება არ ითვალისწინებდა რელიგიის გაცხადების უფლების საპირისპირო ეფექტს, კერძოდ: პიროვნებას უფლება აქვს, არ გაამჟღავნოს საკუთარი რწმენა. მთავრობის მტკიცებით, ეროვნულ კანონმდებლობაში განხორციელდა ცვლილებები, რომლებიც ფიზიკურ პირებს საშუალებას აძლევდა, ცარიელი დაეტოვებინათ გრაფები რელიგიის შესახებ. თუმცა, სასამართლოს აზრით, მხოლოდ ის ფაქტი, რომ პიროვნებამ უნდა მოითხოვოს პირადობის დამადასტურებელი ბარათიდან რელიგიის წაშლა, უკვე ამჟღავნებდა მის დამოკიდებულებას რელიგიის მიმართ. ამასთან, როდესაც პირადობის დამადასტურებელ ბარათზე არის რელიგიის აღმნიშვნელი გრაფა და ის ცარიელი დარჩება, მისი მფლობელი გამორჩეული იქნება მათგან, ვის ბარათზეც აღმსარებლობა მითითებულია. ECtHR-მა დაადგინა, რომ ეროვნული კანონმდებლობა ეწინააღმდეგებოდა კონვენციის მე-9 მუხლს.

ეკლესიის, რელიგიური გაერთიანების ან თემის საქმიანობა წევრთა პერსონალური ინფორმაციის დამუშავებას მოითხოვს, რაც შესაძლებელს ხდის კომუნიკაციასა და აქტივობების ორგანიზებას რელიგიურ ჯგუფში. ამრიგად, ეკლესიები და რელიგიური გაერთიანებები ხშირად ნერგავენ წესებს პერსონალურ მონაცემთა დამუშავების შესახებ. GDPR-ის 91-ე მუხლის თანახმად, ეს წესები შეიძლება კვლავაც მოქმედი იყოს, თუ ყოვლისმომცველია და შეესაბამება რეგულაციას. ამგვარი ეკლესიები და რელიგიური გაერთიანებები შეიძლება იყვნენ საგანგებოდ მათთვის შექმნილი დამოუკიდებელი საზედამხედველო ორგანოს კონტროლქვეშ, იმ პირობით, რომ ეს ორგანო დააკმაყოფილებს რეგულაციით დადგენილ მოთხოვნებს.[119]

რელიგიურ ორგანიზაციას აქვს პერსონალურ მონაცემთა დამუშავების უფლება გარკვეული მიზნებით (მაგ.: რელიგიურ ჯგუფებთან კონტაქტის შესანარჩუნებლად, ან რელიგიურ თუ საქველმოქმედო ღონისძიებებსა და დღესასწაულებზე ინფორმაციის გასავრცელებლად). ზოგიერთ სახელმწიფოში ეკლესიებს მოეთხოვებათ რელიგიური ორგანიზაციის წევრთა რეესტრის წარმოება, კერძოდ, საგადასახადო მიზნებით, ვინაიდან ამან შეიძლება გავლენა იქონიოს პირის მიერ გადასახადების გადახდაზე. ნებისმიერ შემთხვევაში, ევროპული კანონმდებლობის თანახმად, მონაცემები რომლებიც ამჟღავნებს პიროვ-

119 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 91 (2).

ნების რელიგიურ რწმენას, სენსიტიურად მიიჩნევა. შესაბამისად, ეკლესიას გარკვეული ანგარიშვალდებულება უნდა დაეკისროს ასეთი მონაცემების განკარგვისა და დამუშავებისას, განსაკუთრებით იმის გათვალისწინებით, რომ მათ მიერ მოპოვებული ინფორმაცია ხშირად შეეხება ბავშვებს, ხანდაზმულებსა და საზოგადოების სხვა მოწყვლად წევრებს.

1.3.4 ხელოვნებისა და მეცნიერების თავისუფლება

კიდევ ერთი უფლება, რომელიც უნდა დაბალანსდეს პირადი ცხოვრების პატივისცემისა და მონაცემთა დაცვის უფლებებთან, არის ხელოვნებისა და მეცნიერების თავისუფლება, მკაფიოდ დაცული ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-13 მუხლით. ეს უფლება ძირითადად მომდინარეობს აზრისა და გამოხატვის თავისუფლებიდან და უნდა განხორციელდეს ქარტიის პირველი მუხლის (ადამიანური ღირსება) გათვალისწინებით. ECtHR მიიჩნევს, რომ ხელოვნების თავისუფლება დაცულია ადამიანის უფლებათა ევროპული კონვენციის მე-10 მუხლით.[120] შეიძლება ქარტიის მე-13 მუხლით გარანტირებული უფლებაც შეიზღუდოს და ეს განიმარტოს კონვენციის მე-10 მუხლის მე-2 პუნქტის ჭრილში.[121]

მაგალითი: საქმეში *Vereinigung bildender Künstler v. Austria*[122] ავსტრიის სასამართლოებმა განმცხადებელ ასოციაციას აუკრძალეს იმ სურათის გამოფენა, რომელზეც გამოსახული იყო სხვადასხვა საჯარო პირის თავი (ფოტოს სახით), კერძოდ, სექსუალურ კონტექსტში. მათ განმცხადებლის წინააღმდეგ მიმართა ავსტრალიელმა პარლამენტარმა, რომლის ფოტოც გამოყენებული იყო სურათზე, და მოითხოვა მისი გამოფენის აკრძალვა. სასამართლომ პარლამენტარის მოთხოვნა დააკმაყოფილა და შესაბამისი ბრძანება გამოსცა. ECtHR-მა კიდევ ერთხელ ხაზგასმით აღნიშნა, რომ კონვენციის მე-10 მუხლი ეხება იმ იდეების გავრცელებას, რომლებიც შეურაცხმყოფელი, შოკისმომგვრელი ან შემაშფოთებელია სახელმწიფოსთვის, ან მოსახლეობის რომელიმე ჯგუფისთვის. ხელოვნების ნიმუშთა შემქმნელები და გამავრცელებლები ხელს უწყობენ იდეებისა და მოსაზრებების გაცვლას, სახელმწიფო კი ვალდებულია, მათი გამოხატვის თავისუფლება გადაჭარბებულად არ შეზღუდოს. იმის გათვალისწინებით, რომ საქმე ეხებოდა მხოლოდ კოლაჟს, კონკრეტული პიროვნებების თავებით, სხეული კი დახატული იყო არარეალური და გაზვიადებული ფორმით, ის აშკარად არ ისახავდა მიზნად რეალობის გადმოცემას, ან თუნდაც

120 ECtHR, *Müller and Others v. Switzerland,* No. 10737/84, 1988 წლის 24 მაისი.

121 ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის განმარტებები, OJ 2007 C 303.

122 ECtHR, *Vereinigung bildender Künstler v. Austria*, No. 68345/01, 2007 წლის 25 იანვარი, პუნქტები 26 და 34.

მინიშნებას მასზე. ECtHR-მა დამატებით განაცხადა, რომ „ფაქტობრივად, შეუძლებელი გახლდათ ნახატის აღქმა [გამოსახული პირის] პირადი ცხოვრების დეტალების აღწერად, ის უფრო მეტად უკავშირდებოდა [გამოსახული პირის] პოლიტიკურ სტატუსს“, „რომლის გათვალისწინებითაც [გამოსახულ პირს] მეტი მოთმინება უნდა გამოეჩინა კრიტიკის მიმართ.“ განსხვავებული ინტერესების შედარებით, ECtHR-მა დაადგინა, რომ ნახატის გამოფენაზე დაწესებული უვადო აკრძალვა არაპროპორციული იყო და საქმეში დაადგინა კონვენციის მე-10 მუხლის დარღვევა.

მონაცემთა დაცვის ევროპული კანონმდებლობა აცნობიერებს მეცნიერების განსაკუთრებულ მნიშვნელობასაც საზოგადოებისათვის. მონაცემთა დაცვის ზოგადი რეგულაცია და მოდერნიზებული 108-ე კონვენცია პერსონალურ მონაცემთა ხანგრძლივად შენახვის შესაძლებლობას იძლევა, თუ ისინი მუშავდება მხოლოდ და მხოლოდ სამეცნიერო ან ისტორიული კვლევისათვის. ამასთან, დამუშავების კონკრეტული აქტივობის თავდაპირველი მიზნის მიუხედავად, პერსონალური მონაცემების შემდგომი გამოყენება სამეცნიერო კვლევისათვის არ უნდა ითვლებოდეს შეუთავსებელ მიზნად.[123] ამავდროულად, მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დასაცავად, საჭიროა სათანადო მექანიზმების შექმნა ამგვარ დამუშავებასთან დაკავშირებით. ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით შეიძლება ნებადართული იყოს გადახვევა მონაცემთა სუბიექტის უფლებათა დაცვიდან, მაგალითად, როდესაც საქმე ეხება ხელმისაწვდომობის უფლებას, მონაცემთა შესწორებას, დამუშავების შეზღუდვას და პირის უფლებას, უარი განაცხადოს საკუთარი პერსონალური მონაცემების დამუშავებაზე სამეცნიერო, ისტორიული ან სტატისტიკური მიზნებით (ასევე, იხ. ნაწილები 6.1 და 9.4).

1.3.5 ინტელექტუალური საკუთრების დაცვა

ინტელექტუალური საკუთრების უფლებას იცავს ECHR-ის პირველი დამატებითი ოქმის პირველი მუხლი და ქარტიის მე-17 მუხლის პირველი პუნქტი. საკუთრების უფლების ერთ-ერთი მნიშვნელოვანი ასპექტია ინტელექტუალური საკუთრების დაცვა, რომელიც განსაკუთრებით რელევანტურია მონაცემთა დაცვისთვის და ცალსახად არის დადგენილი ამავე მე-17 მუხლის მე-2 პუნქტით. ევროკავშირის სამართლებრივ სისტემაში არსებობს რამდენიმე დირექტივა, რომელთა მიზანია ინტელექტუალური საკუთრების, კერძოდ, საავტორო უფლებების ეფექტიანი დაცვა. ინტელექტუალური საკუთრების უფლება მოიცავს არა მხოლოდ ლიტერატურულ და სახელოვნებო საკუთრებას, არამედ პატენტებს, სავაჭრო ნიშნებსა და მომიჯნავე უფლებებს.

123 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (ბ) და 108-ე მოდერნიზებული კონვენცია, მუხლი 5(4)(ბ).

როგორც CJEU-ს პრეცედენტულმა სამართალმა ცხადყო, საკუთრების ფუნდამენტური უფლების დაცვა უნდა შეესაბამებოდეს სხვა ფუნდამენტურ უფლებებს, კერძოდ, მონაცემთა დაცვის უფლებას.[124] არსებობს საქმეები, სადაც საავტორო უფლებების დამცველი დაწესებულებები ინტერნეტმომსახურების მიმწოდებელთაგან (ISP) ითხოვდნენ, გაემხილათ ონლაინსივრცეში ფაილის გაზიარების პლატფორმის მომხმარებელთა ვინაობა. ეს პლატფორმები ინტერნეტის მომხმარებლებს ხშირად საშუალებას აძლევს, მუსიკალური ფაილები უფასოდ გადმოწეროონ, მიუხედავად იმისა, რომ ეს მასალა დაცულია საავტორო უფლებით.

მაგალითები: საქმე *Promusicae v. Telefónica de España*[125] შეეხებოდა ესპანური ინტერნეტპროვაიდერის Telefónica-ს უარს მუსიკალური პროდიუსერებისა და აუდიოვიზუალური ჩანაწერების გამომცემელთა არაკომერციული ორგანიზაციისათვის Promusicae, კერძოდ, იმ პირთა პერსონალური მონაცემების გამჟღავნებაზე, რომელთაც Telefónica ინტერნეტს აწვდიდა. Promusicae ამ ინფორმაციის გამჟღავნებას ითხოვდა სამოქალაქო სარჩელის აღსაძვრელად იმ პირთა მიმართ, რომლებიც, ორგანიზაციის მტკიცებით, იყენებდნენ ფაილების გაზიარების პროგრამას, ეს კი, თავის მხრივ, უზრუნველყოფდა იმ ფონოგრამებზე წვდომას, რომელთა განკარგვის უფლებაც Promusicae-ს წევრებს ჰქონდათ.

ესპანეთის სასამართლომ ამ საკითხზე მიმართა CJEU-ს და სთხოვა, ევროკავშირის სამართლის შესაბამისად ემსჯელა, უნდა მიეწოდებინა თუ არა პერსონალური მონაცემები სამოქალაქო სარჩელის კონტექსტში, საავტორო უფლებათა ეფექტიანად დასაცავად. იგი მიუთითებდა 2000/31, 2001/29 და 2004/48 დირექტივებზე, ქარტიის მე-17 და 47-ე მუხლის ჭრილში. CJEU-მ დაასკვნა, რომ აღნიშნული სამი დირექტივა, ასევე, დირექტივა 2002/58 (e-Privacy დირექტივა), არ უკრძალავს წევრ სახელმწიფოებს სამოქალაქო დავის პროცესში პერსონალურ მონაცემთა გამჟღავნების ვალდებულების დადგენას, რათა ეფექტიანად იყოს დაცული საავტორო უფლებები.

სასამართლომ აღნიშნა, რომ საქმე ეხებოდა განსხვავებულ ფუნდამენტურ უფლებათა დაცვის ურთიერთშეთავსებას. კერძოდ, ესენია: პირადი ცხოვრების პატივისცემა, საკუთრების დაცვა და ეფექტიანი სამართლებრივი დაცვის საშუალება.

სასამართლომ დაასკვნა, რომ აღნიშნული დირექტივების ეროვნულ კანონმდებლობაში გადატანისას, წევრი სახელმწიფოები ვალდებულნი არი-

124 CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 2008 წლის 29 იანვარი, პუნქტები 62–68.

125 *იქვე*, პუნქტები 54 და 60.

ან, სიფრთხილით გამოიყენონ დირექტივების განმარტება, რომლებიც იძლევა ევროკავშირის სამართლებრივი სისტემით დაცული სხვადასხვა ფუნდამენტური უფლების დაბალანსების საშუალებას. ამასთან, დირექტივების შესაბამისი ღონისძიებების გატარებისას, სახელმწიფო უწყებები და სასამართლოები ვალდებულნი არიან, ეროვნული კანონმდებლობა განმარტონ დირექტივებთან შესაბამისობაში, და არ დაეყრდნონ ისეთ განმარტებებს, რომლებიც ეწინააღმდეგება ფუნდამენტურ უფლებებს ან ევროკავშირის სამართლებრივი სისტემის ზოგად პრინციპებს, როგორიცაა პროპორციულობა.[126]

საქმე *Bonnier Audio AB and Others v. Perfect Communication Sweden AB*[127] შეეხებოდა შესაბამისობას ინტელექტუალური საკუთრებისა და პერსონალურ მონაცემთა დაცვის უფლებებს შორის. განმცხადებლებმა, ხუთმა საგამომცემლო კომპანიამ, რომლებიც ინტელექტუალური საკუთრების უფლებას ფლობდნენ 27 აუდიოწიგნზე, შვედეთის სასამართლოს მიმართეს. საჩივარში ისინი აცხადებდნენ, რომ FTP-ის სერვერმა დაარღვია მათი ინტელექტუალური საკუთრების უფლება (ფაილების გადაცემის პროტოკოლი, რომელიც იძლევა ინტერნეტით ფაილებისა და მონაცემების გაზიარების საშუალებას). განმცხადებლები ითხოვდნენ იმ პირის ვინაობისა და მისამართის გამჟღავნებას ISP-ისგან, რომელიც იყენებდა კონკრეტულ IP მისამართს ფაილების გადასაგზავნად. ინტერნეტმომსახურების მიმწოდებელმა ePhone-მა შესაგებელი წარადგინა, რომელშიც მიუთითებდა 2006/24 დირექტივის (მონაცემთა შენახვის დირექტივა, გაუქმდა 2014 წელს) დარღვევაზე.

შვედეთის სასამართლომ ამ საკითხზე CJEU-ს მიმართა და სთხოვა, ემსჯელა, რამდენად კრძალავს 2006/24 დირექტივა ეროვნული დებულების გამოყენებას 2004/48 დირექტივის („ინტელექტუალური საკუთრების უფლებათა აღსრულება“) მე-8 მუხლის საფუძველზე. ეს მუხლი სასამართლოს საშუალებას აძლევს, ISP-ს მოსთხოვოს საავტორო უფლების მფლობელთათვის ინფორმაციის გადაცემა იმ მომხმარებლებზე, რომელთა IP მისამართიც, სავარაუდოდ, ფიგურირებს დარღვევაში. კითხვა ეფუძნებოდა ვარაუდს, რომ განმცხადებელს წარმოდგენილი ჰქონდა კონკრეტული საავტორო უფლების დარღვევის მკაფიო მტკიცებულება, ხოლო ღონისძიება იყო პროპორციული.

126 *იქვე,* პუნქტები 65 და 68; ასევე, იხ. CJEU, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV,* 2012 წლის 16 თებერვალი.

127 CJEU, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB,* 2012 წლის 19 აპრილი.

CJEU-მ აღნიშნა, რომ დირექტივა არეგულირებდა მხოლოდ და მხოლოდ ელექტრონული კომუნიკაციის პროვაიდერთა მიერ გენერირებული მონაცემების განკარგვა-შენახვას მძიმე დანაშაულის გამოძიების, გამოვლენისა და დამნაშავის დასჯის მიზნით, და მათ გადაცემას უფლებამოსილი სახელმწიფო ორგანოებისათვის. ამრიგად, შიდასახელმწიფოებრივი დებულება, რომელსაც ეროვნულ კანონმდებლობაში გადააქვს 2004/48 (ინტელექტუალური საკუთრების უფლებათა აღსრულების) დირექტივა, სცდება მის ფარგლებს. შესაბამისად, დებულებას კრძალავს დირექტივა.[128]

რაც შეეხება ვინაობის გამჟღავნებასა და IP მისამართის გადაცემას, CJEU-მ განაცხადა, რომ ეს მოქმედება პერსონალურ მონაცემთა დამუშავებაა და 2002/58 დირექტივის მოქმედების ფარგლებში ექცევა. სასამართლომ აღნიშნა ისიც, რომ ხსენებული მონაცემების გადაცემა სამოქალაქო წარმოებისათვის საჭირო იყო საავტორო უფლების მფლობელის სასარგებლოდ, ამ უფლების ეფექტიანად დაცვის მიზნით. ამრიგად, იგი არსებითად ექცეოდა 2004/48 დირექტივის მოქმედების სფეროში.[129]

CJEU-ს დასკვნით, 2002/58 და 2004/48 დირექტივები უნდა განიმარტოს იმგვარად, რომ ძირითად წარმოებაში არ დაბრკოლდეს კონკრეტული ეროვნული კანონმდებლობის მოქმედება, ვინაიდან ის ეროვნულ სასამართლოს (რომელსაც მიმართეს პერსონალურ მონაცემთა გამჟღავნებაზე მითითების გამოცემის მოთხოვნით) საშუალებას აძლევს, დაპირისპირებული ინტერესები შეაფასოს თითოეული საქმის ფაქტობრივ გარემოებებზე დაყრდნობით, და სათანადოდ გაითვალისწინოს პროპორციულობის დაცვის პრინციპი.

1.3.6 მონაცემთა დაცვა და ეკონომიკური ინტერესი

ციფრულ ანუ „დიდი მონაცემების“ (Big Data) ეპოქაში მონაცემები ეკონომიკის „ახალ ნავთობად“ მიიჩნევა, რომელიც ზრდის ინოვაციასა და კრეატიულობას.[130] არაერთმა კომპანიამ საკმაოდ მყარი ბიზნესმოდელები შექმნა მონაცემთა დამუშავების გარშემო, რომელიც ხშირად პერსონალურ მონაცემებსაც ეხება. გარკვეულ კომპანიებს სჯერათ, რომ პერსონალურ მონაცემთა დაცვის კონკრეტული წესები, სავარაუდოდ, ზედმეტად მძიმე ვალდებულებებს ქმნიან პრაქტიკაში, რამაც შეიძლება გავლენა იქონიოს მათ ინტერესებზე. ეს აჩენს კითხვას: რამდენად ამართლებს მონაცემთა დამმუშავებლების, უფლე-

128 *იქვე,* პუნქტები 40-41.

129 *იქვე,* პუნქტები 52–54. ასევე, იხ. CJEU, C-275/06, *Productores de MÚsica de España (Promusicae) v. Telefónica de España SAU* [GC], 2008 წლის 29 იანვარი, პუნქტი 58.

130 იხ. მაგ: *Financial Times* (2016), „Data is the new oil… who’s going to own it?“, 2016 წლის 16 ნოემბერი.

ბამოსილი პირების ან ფართო საზოგადოების ეკონომიკური ინტერესები მონაცემთა დაცვის უფლების შეზღუდვას.

მაგალითი: *Google Spain*[131]-ის საქმეში CJEU-მ დაადგინა, რომ გარკვეულ პირობებში, ფიზიკურ პირებს აქვთ უფლება, საძიებო სისტემებს მოსთხოვონ შედეგების წაშლა თავიანთი ინდექსიდან. CJEU-მ მსჯელობისას მიუთითა, რომ საძიებო სისტემისა და შესაბამისი შედეგების გამოყენებით, შესაძლებელია დეტალური პროფილის შედგენა პიროვნების შესახებ. ამგვარი ინფორმაცია შეიძლება მოიცავდეს კონკრეტული ადამიანის პირადი ცხოვრების ფართო ასპექტს და მისი მოპოვება საძიებო სისტემის გარეშე ადვილი არ იქნებოდა. ამრიგად, ეს, სავარაუდოდ, მძიმე ჩარევაა მონაცემთა სუბიექტის პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის უფლებებში.

CJEU-მ შემდგომ იმსჯელა, თუ რამდენად გამართლებული იყო ჩარევა. რაც შეეხება საძიებო სისტემის ეკონომიკურ ინტერესს მონაცემთა დამუშავებასთან მიმართებით, CJEU-მ აღნიშნა: „ნათელია, რომ [ჩარევა] ვერ გამართლდება მხოლოდ ეკონომიკური ინტერესით, რომელიც აქვს ამგვარი სისტემის ოპერატორს [მონაცემთა] დამუშავებაში“. „როგორც წესი“, ქარტიის მე-7 და მე-8 მუხლებით დაცული ფუნდამენტური უფლებები აღემატება როგორც ეკონომიკურ, ისე საზოგადოების ინტერესს - საძიებო სისტემის საშუალებით მოიპოვოს მონაცემთა სუბიექტის სახელთან დაკავშირებული ინფორმაცია.[132]

ერთ-ერთი ძირითადი ფაქტორი, რომელსაც მონაცემთა დაცვის ევროპული სამართალი ითვალისწინებს, არის ფიზიკური პირებისათვის მეტი კონტროლის მინიჭება თავიანთ პერსონალურ მონაცემებზე. შესაბამისად, ციფრულ ეპოქაში არსებობს განსაკუთრებული დისბალანსი, რომლის ერთ მხარესაც არის იმ ბიზნესორგანიზაციების უფლებამოსილება, რომლებსაც შეუძლიათ დიდი მოცულობით მონაცემებზე წვდომა და მათი დამუშავება, მეორე მხარეს კი - პერსონალურ მონაცემთა მფლობელი ფიზიკური პირების უფლება, აკონტროლონ თავიანთი ინფორმაცია. მონაცემთა დაცვისა და ეკონომიკური ინტერესების შეთავსებისას, CJEU თითოეულ საქმეს განიხილავს ინდივიდუალური მიდგომით. ამის მაგალითია *Manni-ს* საქმეზე მიღებული გადაწყვეტილება, რომელიც შეეხება მესამე მხარის ინტერესებს სააქციო კაპიტალისა და შეზღუდული პასუხისმგებლობის კომპანიებთან დაკავშირებით.

131 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 წლის 13 მაისი.

132 *იქვე,* პუნქტები 81 და 97.

მაგალითი: *Salvatore Manni-ის* საქმე[133] შეეხებოდა პიროვნების პერსონალურ მონაცემთა შეყვანას საჯარო ვაჭრობის რეესტრში. მანიმ ლეჩეს სავაჭრო პალატას მოსთხოვა თავისი პერსონალური მონაცემების წაშლა რეესტრიდან, მას შემდეგ, რაც აღმოაჩინა, რომ პოტენციურ კლიენტებს შეეძლოთ, რეესტრის საშუალებით მიეღოთ მისთვის არასასურველი ინფორმაცია. კერძოდ ის, რომ იგი იყო ადმინისტრატორი კომპანიისა, რომელიც ათ წელზე მეტი ხნის წინათ გაკოტრებულად გამოცხადდა. მანის თქმით, ინფორმაცია მის პოტენციურ კლიენტებს უქმნიდა წინასწარგანწყობას, რომელიც, სავარაუდოდ, უარყოფითად აისახებოდა მის სავაჭრო ინტერესებზე.

CJEU-მ იმსჯელა, აღიარებს თუ არა ევროკავშირის სამართალი წაშლის მოთხოვნის უფლებას მოცემულ შემთხვევაში. სასამართლომ თავის დასკვნაში ერთმანეთს შეუთავსა ევროკავშირის მონაცემთა დაცვის წესები, ბატონი მანის სავაჭრო ინტერესები კომპანიის გაკოტრებაზე ინფორმაციის წაშლასთან მიმართებით და საზოგადოების ინტერესი შესაბამის ინფორმაციაზე წვდომის მხრივ. მან სათანადოდ გაითვალისწინა ფაქტი, რომ საჯარო რეესტრისათვის კომპანიებზე ინფორმაციის გამჟღავნებას განსაზღვრავდა კანონი - კერძოდ, ევროკავშირის დირექტივა, რომლის მიზანია ასეთი ინფორმაციის ხელმისაწვდომობის გამარტივება მესამე პირთათვის. გამჟღავნება მნიშვნელოვანი იყო მესამე მხარის ინტერესების დასაცავად, რომელსაც აქვს კონკრეტულ კომპანიასთან საქმიანი ურთიერთობის სურვილი, ვინაიდან დაცვის ერთადერთი საშუალება, რასაც სააქციო კაპიტალისა და შეზღუდული პასუხისმგებლობის კომპანიები ასეთ პირებს სთავაზობენ, არის მათი აქტივები. შესაბამისად, „ძირითადი დოკუმენტები კომპანიის შესახებ ხელმისაწვდომი უნდა იყოს, რათა მესამე მხარემ შეძლოს გარკვევა მათ შინაარსსა და სხვა სახის ინფორმაციაში კომპანიის შესახებ, განსაკუთრებით, იმ პირებზე, რომლებსაც კომპანიის მოქმედების შეჩერების უფლებამოსილება ენიჭებათ.“[134]

კანონიერი მიზნის გათვალისწინებით, რომელსაც რეესტრი ემსახურება, CJEU-მ დაადგინა, რომ ბატონ მანის არ ჰქონდა უფლება, მოეთხოვა საკუთარი პერსონალური მონაცემების წაშლა: ისეთი საჭიროებები, როგორიცაა მესამე მხარეთა ინტერესის დაცვა სააქციო კაპიტალისა და შეზღუდული პასუხისმგებლობის კომპანიასთან დაკავშირებით, ასევე, სამართლებრივი განჭვრეტადობა, კეთილსინდისიერი ვაჭრობა და, შესაბამისად, შიდა ბაზრის სათანადო ფუნქციონირება, გადაწონიდა განმცხადებლის მონაცემთა დაცვის უფლებებს, გათვალისწინებულს კანონ-

133 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni,* 2017 წლის 9 მარტი.

134 *იქვე,* პუნქტი 49.

მდებლობით. მით უმეტეს იმ ფონზე, რომ პირი, რომელიც ვაჭრობაში მონაწილეობს სააქციო ან შეზღუდული პასუხისმგებლობის კომპანიის საშუალებით, იცნობს მასზე დაკისრებულ ვალდებულებას თავის ვინაობასა და ფუნქციებთან დაკავშირებული ინფორმაციის გამჟღავნების შესახებ.

CJEU-მ დაადგინა, რომ ამ შემთხვევაში არ არსებობდა საფუძველი მონაცემთა წაშლისათვის, თუმცა, ამავდროულად, მან აღიარა დამუშავების შეწყვეტის მოთხოვნის უფლება და აღნიშნა: „გამორიცხული არ არის [...] ისეთი სიტუაციები, სადაც კონკრეტული საქმის ლეგიტიმური და გაცილებით მნიშვნელოვანი მიზეზები, გამონაკლისის სახით და საკმარისი დროის გასვლის შემდეგ [...], ამართლებს რეესტრის პერსონალურ მონაცემებზე წვდომის უფლების მინიჭებას მხოლოდ გარკვეული მხარეებისათვის, რომლებსაც აქვთ ამ ინფორმაციის გაცნობის დადასტურებული და კონკრეტული ინტერესი.“ [135]

CJEU-მ განაცხადა, რომ თითოეულ საქმეში ეროვნულმა სასამართლოებმა ყველა შესაბამისი გარემოების გათვალისწინებით უნდა შეაფასონ ლეგიტიმური და აღმატებული მიზეზების არსებობა, რომლებიც, გამონაკლისის სახით, გაამართლებს მესამე მხარისთვის დაწესებულ შეზღუდვას კომპანიის რეესტრში დაცულ პერსონალურ მონაცემთა წვდომაზე. თუმცა, სასამართლომ განმარტა, რომ ბ-ნი მანის შემთხვევაში მხოლოდ ის ფაქტი, რომ პერსონალური მონაცემების გამჟღავნებამ, სავარაუდოდ, გავლენა მოახდინა მის კლიენტურაზე, არ მიიჩნევა ასეთი მნიშვნელობის მიზეზად. პირის პოტენციურ კლიენტებს აქვთ ლეგიტიმური ინტერესი იმ ინფორმაციის მიმართ, რომელიც შეეხება მისი ყოფილი კომპანიის გაკოტრებას.

ბატონი მანისა და რეესტრში წარმოდგენილ სხვა პირთა პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის ფუნდამენტურ უფლებებში ჩარევა (რომლებიც დაცულია ქარტიის მე-7 და მე-8 მუხლებით) ემსახურებოდა საჯარო ინტერესს და აუცილებელი და პროპორციული იყო დემოკრატიულ საზოგადოებაში.

შესაბამისად, *Salvatore Manni-ის* საქმეში CJEU-მ დაადგინა, რომ მონაცემთა დაცვისა თუ პირადი ცხოვრების პატივისცემის უფლებები არ აღემატებოდა მესამე მხარის ინტერესს - ჰქონოდა წვდომა კომპანიის რეესტრში დაცულ ინფორმაციაზე სააქციო და შეზღუდული პასუხისმგებლობის კომპანიებთან დაკავშირებით.

135 *იქვე,* პუნქტი 60.

2 მონაცემთა დაცვის ტერმინოლოგია

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
პერსონალური მონაცემები		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (1); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (5) და 5 (1) (ე); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 9; CJEU, გაერთიანებული საქმეები C-92/09 და C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 2010; CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 2008; CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011; CJEU, C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland,* 2016; CJEU, გაერთიანებული საქმეები C-141/12 და C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S,* 2014.	**მონაცემთა დაცვის სამართლებრივი განმარტება**	მოდერნიზებული108-ე კონვენცია, მუხლი 2 (ა); ECtHR, *Bernh Larsen Holding AS and Others v. Norway,* No. 24117/08, 2013; ECtHR, Uzun v. Germany No. 35623/05, 2010; ECtHR, *Amann v. Switzerland* [GC], No. 27798/95, 2000.

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist,* 2003	**განსაკუთრებული კატეგორიის პერსონალური მონაცემები**	მოდერნიზებული 108-ე კონვენცია, მუხლი 6 (1)
CJEU, C-434/16, *Peter Nowak v. Data Protection Commissioner,* 2017	**ანონიმიზებული ან ფსევდონიმიზებული პერსონალური მონაცემები**	მოდერნიზებული 108-ეკონვენცია, მუხლი 5 (4) (ე); მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პ.50.
მონაცემთა დამუშავება		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (2); CJEU, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů,* 2014; CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni,* 2017; CJEU, C-101/01, Criminal proceedings against Bodil Lindqvist, 2003; CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014.	**განმარტებები**	მოდერნიზებული 108-ე კონვენცია, მუხლი 2 (დ)
მონაცემთა მომხმარებლები		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (7); CJEU, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů,* 2014; CJEU, C-1318/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014.	**დამმუშავებელი**	მოდერნიზებული 108-ე კონვენცია, მუხლი 2 (დ); რეკომენდაცია პროფილირების შესახებ, მუხლი 1 (ზ)*.

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (8)	**უფლებამოსილი პირი**	108-ე მოდერნიზებული კონვენცია, მუხლი 2 (ვ); რეკომენდაცია პროფილირების შესახებ, მუხლი 1 (თ).
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (9)	**მიმღები**	108-ე მოდერნიზებული კონვენცია, მუხლი 2 (ე)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (10)	**მესამე მხარე/პირი**	
თანხმობა		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 4 (11) და 7; CJEU, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland,* 2011; CJEU, C-536/15, *Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC),* 2017.	**კანონიერი ძალის მქონე თანხმობის განმარტება და წინაპირობები**	108-ე მოდერნიზებული კონვენცია, მუხლი 5 (2); რეკომენდაცია სამედიცინო მონაცემების შესახებ, მუხლი 6, და სხვა შესაბამისი რეკომენდაციები; ECtHR, *Elberte v. Latvia,* No.61243/08, 2015.

2.1 პერსონალური მონაცემები

ძირითადი საკითხები

- მონაცემები პერსონალურია, თუ უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად პირს - „მონაცემთა სუბიექტს“.
- არის თუ არა პირი იდენტიფიცირებადი, ამის დასადგენად მონაცემთა დამმუშავებელმა ან სხვა სუბიექტმა უნდა გაითვალისწინოს ყველა გონივრული საშუალება (მაგ.: პიროვნების გამორჩევა), რომელთა გამოყენებაც შესაძლებელია პიროვნების პირდაპირი ან ირიბი იდენტიფიცირებისათვის.

- ნამდვილობის დადგენა (authentication) - პროცედურა, რომლითაც პირს შეუძლია, დაადასტუროს გარკვეული ვინაობა და/ან უფლებამოსილება გარკვეული ქმედებების განსახორციელებლად.

- არსებობს განსაკუთრებული კატეგორიის, ე.წ. სენსიტიური მონაცემები, წარმოდგენილი მოდერნიზებულ 108-ე კონვენციასა და ევროკავშირის მონაცემთა დაცვის სამართალში, რომლებიც საჭიროებს გაძლიერებულ დაცვას და, შესაბამისად, მკაცრ სამართლებრივ რეჟიმში ექცევა.

- მონაცემები ანონიმურია, თუ აღარ უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად პირს.

- ფსევდონიმიზაცია არის ღონისძიება, რომლის გამოყენებითაც პერსონალური მონაცემები ვეღარ მიეწერება მონაცემთა სუბიექტს, დამატებითი ინფორმაციის გარეშე, რომელიც შენახულია ცალკე. „გასაღები“, რომელიც მონაცემთა სუბიექტის ხელახლა იდენტიფიცირების შესაძლებლობას იძლევა, გამოყოფილად და უსაფრთხოდ უნდა იყოს დაცული. მონაცემები, რომლებმაც ფსევდონიმიზაციის პროცესი გაიარა, პერსონალურ ინფორმაციად რჩება. ევროკავშირის სამართალში არ არსებობს „ფსევდონიმიზებულ მონაცემთა“ კონცეფცია.

- მონაცემთა დაცვის პრინციპები და წესები არ ეხება ანონიმურ ინფორმაციას, მაგრამ ეხება ფსევდონიმიზებულ მონაცემებს.

2.1.1 პერსონალურ მონაცემთა ცნების ძირითადი ასპექტები

ევროკავშირისა და ევროპის საბჭოს კანონმდებლობა „პერსონალურ მონაცემებს“ განმარტავს, როგორც ინფორმაციას იდენტიფიცირებული ან იდენტიფიცირებადი ფიზიკური პირის შესახებ,[136] რომლის ვინაობა ცნობილია, ან შეიძლება დადგინდეს დამატებითი ინფორმაციის საფუძველზე. არის თუ არა პირი იდენტიფიცირებადი, ამის გასარკვევად მონაცემთა დამმუშავებელმა ან სხვა სუბიექტმა უნდა გაითვალისწინოს ყველა გონივრული საშუალება, რომელთა გამოყენებაც შესაძლებელია პირის პირდაპირი ან ირიბი იდენტიფიცირებისათვის (მაგ.: პირის ამოცნობა, რომელიც იძლევა ერთი ადამიანის განსხვავებულად მოპყრობის შესაძლებლობას მეორე ადამიანის მხრიდან).[137]

136 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (1); 108-ე მოდერნიზებული კონვენცია, მუხლი 2 (ა).

137 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 26.

პირს, რომლის პერსონალური მონაცემებიც მუშავდება, „მონაცემთა სუბიექტი“ ეწოდება.

მონაცემთა სუბიექტი

ევროკავშირის კანონმდებლობით, ფიზიკური პირი მონაცემთა დაცვის წესების ერთადერთი ბენეფიციარია[138] და ევროპის მონაცემთა დაცვის სამართალი მხოლოდ ცოცხალ პირებს იცავს.[139] GDPR-ის თანახმად, პერსონალურ მონაცემად მიიჩნევა ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.

ევროპის საბჭოს სამართალი, კერძოდ, მოდერნიზებული 108-ე კონვენცია, ასევე მიუთითებს პიროვნების დაცვაზე პერსონალურ მონაცემთა დამუშავებისას. ამ შემთხვევაშიც, პერსონალური მონაცემი გულისხმობს ნებისმიერ ინფორმაციას იდენტიფიცირებული ან იდენტიფიცირებადი ფიზიკური პირის შესახებ. GDPR-სა და 108-ე მოდერნიზებულ კონვენციაში მითითებული ასეთი პირი მონაცემთა დაცვის სამართალში ცნობილია, როგორც მონაცემთა სუბიექტი.

იურიდიული პირები სარგებლობენ დაცვის გარკვეული დონით. ECtHR-ის პრეცედენტული სამართალი მოიცავს გადაწყვეტილებებს იურიდიულ პირთა საჩივრებზე, რომლებიც ეხება მათი მონაცემების დაცვას სხვა პირის მიერ გამოყენებისგან, ECHR-ის მე-8 მუხლის შესაბამისად. ეს მუხლი ფარავს როგორც პირადი და ოჯახური ცხოვრების, ისე საცხოვრებლისა და კორესპონდენციის პატივისცემის უფლებას. შესაბამისად, სასამართლოს შეუძლია, საქმეები განიხილოს საცხოვრებლისა და კორესპონდენციის პატივისცემის და არა პირადი ცხოვრების უფლების ჭრილში.

> მაგალითი: საქმე *Bernh Larsen Holding AS and Others v. Norway*[140] შეეხებოდა სამი ნორვეგიული კომპანიის საჩივარს საგადასახადო ორგანოს გადაწყვეტილებასთან დაკავშირებით, რომლის მიხედვითაც მათ აუდიტორებისათვის უნდა გადაეცათ იმ სერვერზე განთავსებულ მონაცემთა ასლები, რომლითაც ეს კომპანიები ერთობლივად სარგებლობდნენ.

138 *იქვე,* მუხლი 1.

139 *იქვე,* პრეამბულის პუნქტი 27. ასევე, იხ. 29-ე მუხლის სამუშაო ჯგუფი (2007), მოსაზრება 4/2007 პერსონალური მონაცემების კონცეფციის შესახებ, WP 136, 2007 წლის 20 ივნისი, გვ. 22.

140 ECtHR, *Bernh Larsen Holding AS and Others v. Norway,* No. *24117/08, 2013 წლის 14 მარტი; ასევე, იხ. ECtHR, Liberty and Others v. the United Kingdom,* No. 58243/00, 2008 წლის 1 ივლისი.

ECtHR-მა დაადგინა, რომ ამ მოვალეობის დაკისრება განმცხადებლებზე იყო ჩარევა მათ საცხოვრებლისა და კორესპონდენციის პატივისცემის უფლებაში (მე-8 მუხლი). თუმცა, სასამართლოს განმარტებით, საგადასახადო ორგანოებს ეფექტიანი და სათანადო მექანიზმები ჰქონდათ ჩარევის ბოროტად გამოყენების ასაცილებლად: მათ განმცხადებელი კომპანიები წინასწარ, საკმაო დროით ადრე გააფრთხილეს; კომპანიების წარმომადგენლები ესწრებოდნენ შემოწმებას და ჰქონდათ თავიანთი არგუმენტების ადგილზე წარმოდგენის შესაძლებლობა, მასალები კი განადგურდებოდა საგადასახადო შემოწმების დასრულებისთანავე. ასეთ პირობებში, საჭირო იყო სამართლიანი წონასწორობის მიღწევა საპირისპირო ინტერესებს შორის. კერძოდ, ეფექტიანი შემოწმების საჯარო ინტერესი, საგადასახადო შეფასების მიზნებით, უნდა დაბალანსებულიყო განმცხადებელი კომპანიების „საცხოვრებლისა“ და „კორესპონდენციის“ უფლებასა და მათი თანამშრომლების პირადი ცხოვრების დაცვის ინტერესთან. სასამართლომ დაადგინა, რომ საქმეში კონვენციის მე-8 მუხლი არ დარღვეულა.

მოდერნიზებული 108-ე კონვენციის თანახმად, მონაცემთა დაცვა, ძირითადად, მოიცავს ფიზიკურ პირებს, თუმცა ხელმომწერმა სახელმწიფოებმა ის თავიანთ კანონმდებლობაში შეიძლება გაავრცელონ იურიდიულ პირებზეც (მაგ.: ბიზნესებსა და ასოციაციებზე). ამ კონვენციის განმარტებითი ბარათის თანახმად, ეროვნული კანონმდებლობა შეიძლება იცავდეს იურიდიულ პირთა კანონიერ ინტერესებს, აღნიშნულ აქტორებზე კონვენციის მოქმედების გავრცელებით.[141] ევროკავშირის მონაცემთა დაცვის სამართალი არ მოიცავს მონაცემთა დამუშავებას იურიდიული პირების შესახებ. კერძოდ, იგი არ ეხება იურიდიული პირის სახით შექმნილი საწარმოს სახელს, ფორმასა და საკონტაქტო ინფორმაციას.[142] თუმცა, ელექტრონულ სივრცეში პირადი ცხოვრების დაცვის დირექტივა იცავს კომუნიკაციების კონფიდენციალობას, ასევე, იურიდიული პირის კანონიერ ინტერესებს გამომწერთა და მომხმარებელთა მონაცემების ავტომატური შენახვა-დამუშავების მზარდ შესაძლებლობასთან დაკავშირებით.[143] მსგავსად დირექტივისა, იურიდიული პირების დაცვაზე ასევე ვრცელდება რეგულაცია ელექტრონულ სივრცეში პირადი ცხოვრების დაცვის შესახებ.

141 განმარტებითი ბარათი, 108-ე მოდერნიზებული კონვენცია, პუნქტი 30.

142 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის მე-14 პუნქტი.

143 დირექტივა ელექტრონულ სფეროში პირადი ცხოვრების დაცვის შესახებ, პრეამბულის მე-7 პუნქტი და მუხლი 1 (2).

მაგალითი: საქმეში *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen*[144] CJEU-მ სასოფლო-სამეურნეო დახმარების ბენეფიციართა პერსონალური მონაცემების გამოქვეყნების შესახებ განაცხადა: „ამგვარ იდენტიფიკაციასთან მიმართებით, იურიდიულ პირებს შეუძლიათ, მოითხოვონ ქარტიის მე-7 და მე-8 მუხლებით გათვალისწინებული დაცვა, თუკი იურიდიული პირის ოფიციალური სახელწოდება ერთი ან მეტი ფიზიკური პირის ვინაობას ადგენს. პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით, ქარტიის მე-7 და მე-8 მუხლებით აღიარებული პირადი ცხოვრების პატივისცემის უფლება შეეხება ინფორმაციას იდენტიფიცირებული ან იდენტიფიცირებადი პირის შესახებ [...]“.[145]

დაბალანსა რა ევროკავშირის ინტერესი დახმარების განაწილების გამჭვირვალობასთან დაკავშირებით და იმ ადამიანთა პირადი ცხოვრებისა და მონაცემთა დაცვის უფლებები, რომლებმაც დახმარებით ისარგებლეს, CJEU-მ დაადგინა, რომ ფუნდამენტურ უფლებებში ჩარევა არაპროპორციული იყო. სასამართლომ მიიჩნია, რომ გამჭვირვალობის ამოცანის ეფექტიანად შესრულება შესაძლებელი გახლდათ ისეთი ღონისძიებებითაც, რომლებიც ნაკლებად ხელყოფდა ამ პირთა უფლებებს. თუმცა, დახმარების მიმღებ იურიდიულ პირთა მონაცემების გამოქვეყნებაზე მსჯელობისას, CJEU მივიდა განსხვავებულ დასკვნამდე, რომ გამოქვეყნება არ არღვევდა პროპორციულობის პრინციპს. კერძოდ, სასამართლომ დაადგინა: „პერსონალურ მონაცემთა დაცვის დარღვევის სიმძიმე სხვადასხვანაირად გამოიხატება იურიდიული და ფიზიკური პირებისთვის.“[146] იურიდიულ პირებზე დაწესებული ვალდებულებების ტვირთი უფრო მძიმეა, როდესაც საქმე ეხება მათზე ინფორმაციის გამოქვეყნებას. CJEU-მ დაადგინა, რომ ეროვნული უწყების დავალდებულება, გამოქვეყნებამდე შეესწავლა, რამდენად შეიცავდა თითოეული ბენეფიციარი იურიდიული პირის მონაცემები ინფორმაციას მასთან დაკავშირებულ რომელიმე ფიზიკურ პირზე, ამ ორგანოს დააკისრებდა არაგონივრულ ადმინისტრაციულ ტვირთს. შესაბამისად, კანონმდებლობამ, რომელიც განსაზღვრავდა მოთხოვნას იურიდიულ პირთა მონაცემების ზოგადი გამოქვეყნების შესახებ, სამართლიანი ბალანსი დაადგინა სასწორზე დადებულ საპირისპირო ინტერესებს შორის.

144 CJEU, გაერთიანებული საქმეები C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 2010 წლის 9 ნოემბერი, პუნქტი 53.

145 *იქვე*, პუნქტები 52-53.

146 *იქვე*, პუნქტი 87.

მონაცემთა ბუნება

ნებისმიერი ტიპის მონაცემი შეიძლება პერსონალურ ინფორმაციად ჩაითვალოს, თუ უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად პირს.

მაგალითი: ხელმძღვანელის მიერ დასაქმებულის მუშაობის შეფასება, რომელიც მის პირად საქმეში ინახება, დასაქმებულის პერსონალური მონაცემია. ეს ასეა მაშინაც, თუ შეფასება ნაწილობრივ ან მთლიანად ასახავს ხელმძღვანელის პირად მოსაზრებებს (მაგ.: „დასაქმებული სამსახურში ბოლომდე არ იხარჯება“) და არა ფაქტებს (მაგ.: „დასაქმებული ბოლო 6 თვიდან 5 კვირა სამსახურში არ დადიოდა“).

პერსონალური მონაცემები მოიცავს ინფორმაციას ადამიანის პირადი ცხოვრების, მათ შორის, პროფესიული და საზოგადოებრივი აქტივობების შესახებ.

Amann-ის საქმეში[147] ECtHR-მა „პერსონალური მონაცემები“ იმგვარად განმარტა, რომ არ მოიცავდა მხოლოდ პირადი ცხოვრების სფეროს საკითხებს. ტერმინის მნიშვნელობა მისაღები იყო GDPR-ისთვისაც.

მაგალითები: საქმეში *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen*[148] CJEU-მ განაცხადა: „არ აქვს მნიშვნელობა იმას, რომ გამოქვეყნებული მონაცემები შეეხება პროფესიულ საქმიანობას [...]“; ადამიანის უფლებათა ევროპულმა სასამართლომ კი ამ საკითხთან დაკავშირებით მიუთითა კონვენციის [ECHR] მე-8 მუხლზე და დაადგინა, რომ ტერმინი „პირადი ცხოვრება“ არ უნდა განიმარტოს შეზღუდული ფორმით; ასევე, არ არსებობს რაიმე პრინციპული მიზეზი, რომელიც გაამართლებს [...] პროფესიული აქტივობების გამორიცხვას პირადი ცხოვრების ცნებიდან.“

გაერთიანებულ საქმეებში *YS v. Minister voor Immigratie, Integratie en Asiel* და *Minister voor Immigratie, Integratie en Asiel v. M and S*[149] CJEU-მ განაცხადა, რომ იმიგრაციისა და ნატურალიზაციის სამსახურის

147 იხ. ECtHR, *Amann v. Switzerland,* No. 27798/95, 2000 წლის 16 თებერვალი, პუნქტი 65.

148 CJEU, გაერთიანებული საქმეები C-92/09 და C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 2010 წლის 9 ნოემბერი, პუნქტი 59.

149 CJEU, გაერთიანებული საქმეები C-141/12 და C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S,* 2014 წლის 17 ივლისი, პუნქტი 39.

გადაწყვეტილების პროექტში წარმოდგენილი სამართლებრივი ანალიზი, რომელიც შეეხებოდა განმცხადებელთა ბინადრობის ნებართვას, თავისთავად არ გახლდათ პერსონალური მონაცემი, თუმცა კი შესაძლებელია, გარკვეულ პერსონალურ ინფორმაციას შეიცავდეს.

ECtHR-ის პრეცედენტული სამართალი ევროპული კონვენციის მე-8 მუხლთან დაკავშირებით ადასტურებს, რომ რთულია პირადი და პროფესიული ცხოვრების საკითხების ერთმანეთისაგან გამიჯვნა.[150]

მაგალითი: საქმეში *Bărbulescu v. Romania*[151] განმცხადებელი სამსახურიდან გაათავისუფლეს იმის გამო, რომ სამუშაო საათებში დამსაქმებლის ინტერნეტი შიდა რეგულაციების დარღვევით გამოიყენა. დამსაქმებელი ფარულ მონიტორინგს უწევდა დასაქმებულის კომუნიკაციებს და ჩანაწერები, რომლებიც მოიცავდა მხოლოდ პირადულ მესიჯებს, ეროვნულ დონეზე გამართულ სასამართლო პროცესზე წარმოადგინა. ECtHR-მა, მას შემდეგ, რაც დაადგინა, რომ მე-8 მუხლი ვრცელდებოდა ასეთ მონაცემებზეც, ღია დატოვა კითხვა, თუ რამდენად უჩენდა დამსაქმებლის შემზღუდავი რეგულაციები განმცხადებელს პირადი ცხოვრების დაცვის გონივრულ მოლოდინს; თუმცა, ამავდროულად სასამართლომ დაადგინა, რომ დასაქმებულის ინსტრუქციები პირად სოციალურ ცხოვრებას სამუშაო ადგილზე ბოლომდე ვერ გამორიცხავდა. რაც შეეხება არსებით მხარეს, ხელშემკვრელ სახელმწიფოებს ფართო დისკრეცია ენიჭებათ შესაფასებლად, თუ რამდენად საჭიროა საკანონმდებლო ჩარჩოს შექმნა ისეთი პირობების დარეგულირებისათვის, რომელშიც დამსაქმებელს აქვს სამუშაო ადგილზე დასაქმებულის არაპროფესიული კომუნიკაციის გაკონტროლების უფლება - ელექტრონული თუ სხვა ფორმით. ამავდროულად, სახელმწიფო ორგანოებმა უნდა უზრუნველყონ, რომ დამსაქმებლის მიერ კორესპონდენციასა და სხვა კომუნიკაციაზე მონიტორინგის მიზნით დანერგილ ღონისძიებებს, მიუხედავად მათი მასშტაბისა და ხანგრძლივობისა, თან ახლდეს სათანადო და საკმარისი საშუალებები ბოროტად გამოყენებისგან დასაცავად. უაღრესად მნიშვნელოვანია პროპორციულობა და პროცედურული გარანტიები თვითნებობის წინააღმდეგ. ECtHR-მა გამოავლინა ასეთ პირობებისთვის საგულისხმო რამდენიმე ფაქტორი, მათ შორის, დასაქმებულზე მონიტორინგის ფარგლები და მის პირად ცხოვრებაში შეჭრის ხარისხი. კერძოდ, რა შედეგები ექნება

150 იხ. მაგ: ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 2000 წლის 4 მაისი, პუნქტი 43; ECtHR, *Niemietz v. Germany,* No. 13710/88, 1992 წლის 16 დეკემბერი, პუნქტი 29.

151 ECtHR, *Bărbulescu v. Romania* [GC], No. 61496/08, 2017 წლის 5 სექტემბერი, პუნქტი 121.

ამგვარ ზომას დასაქმებულისთვის და რამდენად უზრუნველყოფილია დაცვის სათანადო საშუალებები. ამასთან, სახელმწიფო ორგანოების ძალისხმევით, დასაქმებულს, რომლის კომუნიკაციებზეც მონიტორინგი ხორციელდება, ხელი უნდა მიუწვდებოდეს სამართლებრივი დაცვის საშუალებაზე შესაბამისი სასამართლო ორგანოს წინაშე, რათა, სულ მცირე, არსებითად დადგინდეს წარმოდგენილი კრიტერიუმების დაცვის საკითხი და სადავო ღონისძიებათა კანონიერება. ამ საქმეში ECtHR-მა დაადგინა მე-9 მუხლის დარღვევა, რადგან სახელმწიფო ორგანოებმა სათანადოდ ვერ დაიცვეს განმცხადებლის პირადი ცხოვრებისა და კორესპონდენციის პატივისცემის უფლება; შედეგად, მათ ვერ შეძლეს ორი საპირისპირო ინტერესის სამართლიანად დაბალანსება.

როგორც ევროკავშირის, ისე ევროპის საბჭოს სამართალში, ინფორმაცია პერსონალურ მონაცემებს შეიცავს, თუ მასში პირი:

- იდენტიფიცირებული, ან იდენტიფიცირებადია;
- არ არის იდენტიფიცირებული, მაგრამ შესაძლებელია ამ ინფორმაციის საფუძველზე მისი გამორჩევა, რაც იძლევა მონაცემთა სუბიექტის დადგენის შესაძლებლობას შემდგომი ძიების მეშვეობით.

ინფორმაციის ორივე სახეობა თანაბრად არის დაცული მონაცემთა დაცვის ევროპულ სამართალში. პიროვნების პირდაპირი ან ირიბი იდენტიფიცირების შესაძლებლობა საჭიროებს მუდმივ შეფასებას, „მონაცემთა დამუშავებისას ხელმისაწვდომი ტექნოლოგიებისა და, ზოგადად, ტექნოლოგიური განვითარების გათვალისწინებით“.[152] ECtHR-მა არაერთხელ აღნიშნა, რომ ადამიანის უფლებათა ევროპული კონვენციით გათვალისწინებული „პერსონალური მონაცემების“ ცნება ჰგავს 108-ე კონვენციაში წარმოდგენილ განსაზღვრებას, განსაკუთრებით, როდესაც საქმე ეხება იდენტიფიცირებულ ან იდენტიფიცირებად პირთა საკითხებს.[153]

GDPR-ის თანახმად, „იდენტიფიცირებადია ფიზიკური პირი, ვისი პირდაპირი ან ირიბი იდენტიფიცირებაც შესაძლებელია ისეთი საშუალებებით, როგორიცაა სახელი, პირადი ნომერი, ინფორმაცია ადგილმდებარეობის შესახებ, ონლაინ იდენტიფიკატორი და ფიზიკური პირის იდენტობისთვის დამახასიათებელი ერთი ან მეტი ფიზიკური, ფსიქოლოგიური, გენეტიკური, გონებრივი, ეკონომიკური, კულტურული ან სოციალური ფაქტორი“.[154] ამრიგად, იდენტი-

152 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის პუნქტი 26.

153 იხ. ECtHR, *Amann v. Switzerland* [GC], No. 27798/95, 2000 წლის 16 თებერვალი, პუნქტი 65.

154 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (1).

ფიკაცია მოითხოვს ელემენტებს, რომლებითაც შესაძლებელია პიროვნების აღწერა დანარჩენებისგან გამორჩეულად, რათა მოხერხდეს მისი, როგორც ინდივიდის ამოცნობა. სახელი და გვარი ამგვარ ელემენტთა ძირითადი მაგალითია, რითაც შესაძლებელია პიროვნების პირდაპირი იდენტიფიცირება. ზოგჯერ შეიძლება სხვა მახასიათებლებსაც ჰქონდეს სახელის მსგავსი ეფექტი და პირდაპირი იდენტიფიცირების საშუალებას იძლეოდეს, მაგალითად: ტელეფონის, სოციალური დაზღვევის ან სატრანსპორტო საშუალების რეგისტრაციის ნომერი. შესაძლებელია სხვა ატრიბუტების გამოყენებაც - როგორიცაა კომპიუტერული ფაილების, „cookie ფაილების“ და ვებტრეფიკის ფარული დაკვირვების ინსტრუმენტები - რომლებითაც ხერხდება ადამიანების გამორჩევა მათი ქცევისა და ჩვევების იდენტიფიცირების გზით. 29-ე მუხლის სამუშაო ჯგუფის მოსაზრებით, „სახელისა და მისამართის გარეშეც შესაძლებელია პიროვნების კატეგორიზაცია სოციალურ-ეკონომიკური, ფსიქოლოგიური, ფილოსოფიური თუ სხვა კრიტერიუმების საფუძველზე და მისთვის გარკვეული გადაწყვეტილებების მიწერა, ვინაიდან პიროვნების საკონტაქტო პუნქტი (კომპიუტერი) აღარ მოითხოვს მისი ვინაობის გამჟღავნებას ვიწრო გაგებით.“[155] პერსონალური მონაცემების განმარტება, როგორც ევროპის საბჭოს, ისე ევროკავშირის კანონმდებლობით, საკმაოდ ფართოა და მოიცავს იდენტიფიკაციის ყველა შესაძლებლობას (შესაბამისად, ყველა დონეს).

მაგალითები: საქმეში *Promusicae v. Telefónica de España*[156] CJEU-მა განაცხადა: „უდავოა, რომ გარკვეულ [ფაილების გაზიარების ინტერნეტ-პლატფორმის] მომხმარებელთა სახელებისა და მისამართების მოთხოვნა Promusicae-ს მიერ გულისხმობს ხელმისაწვდომობას პერსონალურ მონაცემებზე, ანუ ინფორმაციაზე, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს, დირექტივის 2(ა) მუხლში წარმოდგენილი განმარტების შესაბამისად [ამჟამად GDPR-ის მე-4 მუხლის პირველი პუნქტი]. ისეთი ინფორმაციის გადაცემა, რომელიც Promusicae-ს მტკიცებით, შენახულია Telefónica-ს მიერ (რაც, თავის მხრივ, Telefónica-ს სადავო არ გაუხდია), პერსონალური მონაცემების დამუშავებაა.“ [157]

საქმე *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] შეეხებოდა ინტერნეტმომსახურების მიმწო-

155 29-ე მუხლის სამუშაო ჯგუფი, *მოსაზრება 4/2007 პერსონალური მონაცემების კონცეფციის შესახებ*, WP 136, 20 June 2007, გვ. 15.

156 CJEU, C-275/06, *Productores de MÚsica de España (Promusicae) v. Telefónica de España SAU* [GC], 2008 წლის 29 იანვარი, პუნქტი 45.

157 ყოფილი 95/46 დირექტივა, მუხლი 2 (ბ), ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (2).

158 CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 წლის 24 ნოემბერი, პუნქტი 51.

დებელი კომპანიის Scarlet-ის უარს, დაეყენებინა სისტემა იმ ელექტრონული კომუნიკაციების გასაფილტრად, რომლებიც ფაილების გაზიარების კომპიუტერულ პროგრამას იყენებდა. მისი მიზანი იყო ისეთი ფაილების გაზიარების პრევენცია, რომელთა გადაცემაც არღვევს SABAM-ის (კომპანია, რომელიც წარმოადგენს ავტორებს, კომპოზიტორებსა და რედაქტორებს) მიერ დაცულ საავტორო უფლებებს. CJEU-მ დაადგინა, რომ მომხმარებელთა IP მისამართები „დაცული პერსონალური მონაცემებია, რადგან მომხმარებლის ზუსტი იდენტიფიცირების საშუალებას იძლევა.“

ვინაიდან ბევრი სახელი არ არის უნიკალური, პიროვნების ვინაობის დადგენას შეიძლება დასჭირდეს დამატებითი იდენტიფიკატორები სხვა პირთან არევის თავიდან ასაცილებლად. იმ პიროვნების იდენტიფიცირებისათვის, რომელსაც კონკრეტული ინფორმაცია უკავშირდება, ზოგჯერ საჭიროა პირდაპირი და ირიბი მახასიათებლების კომბინირება. ხშირად, ამ მიზნით, იყენებენ დაბადების ადგილსა და თარიღს. ამასთან, ზოგიერთ ქვეყანაში შემოღებულია პერსონალიზებული ნომრები მოქალაქეთა უკეთ გამოსარჩევად. საგადასახადო მონაცემები,[159] ადმინისტრაციულ დოკუმენტში წარმოდგენილი მონაცემები, რომლებიც ბინადრობის ნებართვის განცხადებას უკავშირდება,[160] და საბანკო თუ ფიდუციური (სანდო პირის) ურთიერთობების დოკუმენტები[161] შეიძლება ასევე პერსონალურ მონაცემებს განეკუთვნებოდეს. ბიომეტრიული მონაცემები, როგორიცაა თითის ანაბეჭდები, ციფრული ფოტოები ან თვალის ბადურის სკანირება, ადგილმდებარეობის განმსაზღვრელი მონაცემები და ელექტრონული მახასიათებლები, სულ უფრო და უფრო ხშირად გამოიყენება ტექნოლოგიურ ეპოქაში პიროვნების საიდენტიფიკაციოდ.

მონაცემთა დაცვის ევროპული კანონმდებლობის მოქმედებისთვის, აუცილებელი არ არის მონაცემთა სუბიექტის რეალურად იდენტიფიცირება, საკმარისია, ის იყოს იდენტიფიცირებადი. პიროვნება იდენტიფიცირებადია, თუ არსებობს საკმარისი ელემენტები, რომელთა მეშვეობითაც შესაძლებელია მისი პირდაპირი ან ირიბი იდენტიფიცირება.[162] GDPR-ის პრეამბულის 26-ე პუნქტი ათვლის წეტილად მიიჩნევს იმას, თუ რამდენად ხელმისაწვდომი და მართვადია იდენტიფიცირების არსებული გონივრული საშუალებები ინფორმაციის განჭვრეტადი მომხმარებლებისთვის; ეს მოიცავს იმ მესამე პირების ხელთ არსებულ ინფორმაციას, რომლებიც არიან ინფორმაციის მიმღებნი (იხ. ნაწილი 2.3.2).

159 CJEU, C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others,* 2015 წლის 1 ოქტომბერი.

160 CJEU, *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S,* 2014 წლის 17 ივლისი.

161 ECtHR, *M.N. and Others v. San Marino,* No. 28005/12, 2015 წლის 7 ივლისი.

162 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (1).

მაგალითი: ადგილობრივი ხელისუფლება გადაწყვეტს, შეაგროვოს მონაცემები ქუჩებში გადაჭარბებული სიჩქარით მოძრავ ავტომანქანებზე. ამ მიზნით, იგი ავტომანქანებს უღებს ფოტოებს და ავტომატურად აფიქსირებს დროსა და ადგილს, რათა შემდგომ ეს მონაცემები მიაწოდოს შესაბამის დაწესებულებას, რომელიც სიჩქარის შეზღუდვის დამრღვევებს დააჯარიმებს. მონაცემთა სუბიექტი ამ ქმედებას ასაჩივრებს და აცხადებს, რომ კანონმდებლობის შესაბამისად, ადგილობრივ ხელისუფლებას არ გააჩნია სამართლებრივი საფუძველი ამ მონაცემთა შესაგროვებლად. ადგილობრივი ხელისუფლება პასუხობს, რომ იგი პერსონალურ მონაცემებს არ აგროვებს, რადგან სანომრე ნიშნები ანონიმურია; ასევე, მას არ აქვს ავტოსატრანსპორტო საშუალებათა რეესტრზე წვდომის სამართლებრივი უფლებამოსილება, ავტომანქანის მესაკუთრის ან მძღოლის ვინაობის დასადგენად.

ამგვარი დასაბუთება შეესაბამება GDPR-ის პრეამბულის 26-ე პუნქტს. ვინაიდან მონაცემთა შეგროვების მიზანია დამრღვევთა გამოვლენა და დაჯარიმება, სავარაუდოა, რომ იქნება მათი იდენტიფიცირების მცდელობაც. მართალია, ადგილობრივ ხელისუფლებას არ აქვს წვდომა იდენტიფიცირების საშუალებებზე, მაგრამ იგი მონაცემებს გადასცემს უფლებამოსილ ორგანოს, პოლიციას, რომელსაც ამგვარი შესაძლებლობები ექნება. პრეამბულის 26-ე პუნქტი ცალსახად ვრცელდება ისეთ შემთხვევებზეც, სადაც სავარაუდოა, რომ პიროვნების იდენტიფიცირებას შეეცდება მონაცემთა შემდგომი მიმღები (და არა მხოლოდ მყისიერი მომხმარებელი). პრეამბულის ამავე პუნქტის ჭრილში, ადგილობრივი ხელისუფლების მოქმედება უტოლდება მონაცემთა შეგროვებას იდენტიფიცირებადი პიროვნების შესახებ. შესაბამისად, საჭიროებს სამართლებრივ საფუძველს მონაცემთა დაცვის კანონმდებლობის თანახმად.

იმის დასადგენად, „თუ რამდენად არსებობს გონივრული შესაძლებლობა, რომ გამოყენებული იქნება ფიზიკური პირის იდენტიფიცირების საშუალებები, გასათვალისწინებელია ყველა ობიექტური ფაქტორი, როგორიცაა იდენტიფიკაციისთვის საჭირო დრო, მისი ღირებულება, ასევე, დამუშავების მომენტისათვის არსებული ტექნოლოგიები და ტექნოლოგიური განვითარების დონე.“ [163]

მაგალითი: საქმეში *Breyer v. Bundesrepublik Deutschland*[164] CJEU-მ იმსჯელა მონაცემთა სუბიექტის ირიბი იდენტიფიცირების შესაძლებლობაზე. საქმე შეეხებოდა დინამიკურ IP მისამართებს, რომლებიც ინტერნეტთან

163 *იქვე,* პრეამბულის 26-ე პუნქტი.

164 CJEU, C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland,* 2016 წლის 19 ოქტომბერი, პუნქტი 43.

დაკავშირებისას ყოველ ჯერზე იცვლება. ვებგვერდები, რომლებსაც გერმანიის ფედერალური ინსტიტუტები მართავენ, დინამიკურ IP მისამართებს არეგისტრირებენ და ინახავენ, კიბერთავდასხმების პრევენციისა და, საჭიროების შემთხვევაში, სისხლისსამართლებრივი წარმოების დაწყების მიზნით. ბ-ნი ბრეიერის იდენტიფიცირებისთვის საჭირო დამატებითი ინფორმაცია ჰქონდა მხოლოდ იმ ISP-ს, რომელსაც ის იყენებდა.

CJEU-მ დაადგინა, რომ დინამიკური IP მისამართი, რომელსაც არეგისტრირებს ონლაინ მედიასერვისების მიმწოდებელი პირის ვებგვერდზე შესვლისას და რომელიც პროვაიდერმა გაასაჯაროვა, პერსონალური მონაცემია, სადაც მხოლოდ მესამე პირს - ამ შემთხვევაში ISP-ს - აქვს პიროვნების იდენტიფიცირებისათვის საჭირო დამატებითი მონაცემები.[165] სასამართლომ აღნიშნა: „არ არის აუცილებელი, ყველა ინფორმაცია, რომელიც იძლევა მონაცემთა სუბიექტის იდენტიფიცირების საშუალებას, ერთი პირის ხელში ინახებოდეს“, რომ პერსონალურ მონაცემად ჩაითვალოს. ISP-ის მიერ დარეგისტრირებული დინამიკური IP მისამართის მომხმარებელთა იდენტიფიცირება შეიძლება გარკვეულ სიტუაციებში, მაგალითად კიბერთავდასხმაზე წარმოებული სისხლის სამართლის საქმის ფარგლებში, სხვა პირთა დახმარებით.[166] CJEU-ს განმარტებით, როდესაც პროვაიდერს „სამართლებრივი საშუალება მონაცემთა სუბიექტის იდენტიფიცირების შესაძლებლობას აძლევს - იმ დამატებითი ინფორმაციის გამოყენებით, რომელიც მას დაფიქსირებული აქვს პირის შესახებ - ეს „საშუალება, გონივრული ვარაუდით, გამოყენებული იქნება მონაცემთა სუბიექტის იდენტიფიცირებისთვის“. შესაბამისად, ასეთი ინფორმაცია პერსონალურ მონაცემად ითვლება.

ევროპის საბჭოს კანონმდებლობა იდენტიფიცირებადობას იმავენაირად განმარტავს. 108-ე მოდერნიზებული კონვენციის განმარტებითი ბარათის მიხედვით: „იდენტიფიცირებადობის ცნება მიუთითებს არა მხოლოდ პიროვნების სამოქალაქო ან იურიდიულ იდენტობაზე, არამედ იმაზეც, რაც „ინდივიდუალიზებისა“ და სხვებისგან გამორჩევის შედეგად, მისი განსხვავებული მოპყრობის შესაძლებლობას იძლევა.“ ასეთი „ინდივიდუალიზაცია“ მიიღწევა, მაგალითად, კონკრეტულად ამ პირზე, მოწყობილობასა ან მოწყობილობათა კომბინაციაზე (კომპიუტერი, მობილური ტელეფონი, კამერა, სათამაშო აპარატი და ა.შ.) მითითებით, რომელიც შეიცავს საიდენტიფიკაციო ნომერს, ფსევდონიმს, ბიომეტრიულ, გენეტიკურ ან ადგილმდებარეობის მონაცემებს,

165 ევროპული პარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, მუხლი 2 (ა).

166 CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* 2011 წლის 24 ნოემბერი, პუნქტები 47–48.

IP მისამართს ან სხვა საიდენტიფიკაციო საშუალებებს.[167] პირი არ არის „იდენტიფიცირებადი“, თუ მისი დადგენა საჭიროებს არაგონივრულ დროს, ძალისხმევასა და რესურსებს, მაგალითად, ზედმეტად კომპლექსურ, ხანგრძლივ და ძვირადღირებულ ოპერაციებს. დროის, ძალისხმევისა და რესურსების არაგონივრულობა უნდა შეფასდეს თითოეულ ინდივიდუალურ შემთხვევაში, ისეთი ფაქტორების გათვალისწინებით, როგორიცაა დამუშავების მიზანი, ღირებულება, იდენტიფიცირებით მიღებული სარგებელი, გამოყენებული მაკონტროლებლისა და ტექნოლოგიის ტიპი.“ [168]

რაც შეეხება პერსონალურ მონაცემთა შენახვის ან გამოყენების ფორმას, უნდა აღინიშნოს, რომ ეს არ არის რელევანტური მონაცემთა დაცვის კანონმდებლობის გავრცელების კუთხით. წერილობითი ან ზეპირი კომუნიკაცია შეიძლება შეიცავდეს პერსონალურ მონაცემებსა და გამოსახულებას,[169] მათ შორის, ვიდეოთვალთვალის სისტემის (CCTV)[170] ან აუდიო ჩანაწერს.[171] პერსონალური მონაცემი შეიძლება არსებობდეს როგორც ელექტრონული, ისე ფურცელზე დაწერილი ფორმით. ადამიანის უჯრედული ნიმუშებიც კი, რომელიც შეიცავს დნმ-ს, შეიძლება გახდეს ბიომეტრიული მონაცემების ამოღების წყარო,[172] თუკი მონაცემები უკავშირდება პიროვნების მიერ მემკვიდრეობით მიღებულ ან შეძენილ გენეტიკურ მახასიათებლებს, ან შეიცავს უნიკალურ ინფორმაციას მისი ჯანმრთელობისა თუ ფიზიოლოგიის შესახებ, და ამ პირის ბიოლოგიური ნიმუშის ანალიზის შედეგია.[173]

ანონიმიზაცია

პერსონალურ მონაცემთა შენახვის შეზღუდვის პრინციპით, რომელიც მოცემულია GDPR-სა და მოდერნიზებულ 108-ე კონვენციაში (და ვრცლად არის

167 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 18.

168 *იქვე,* პუნქტი 17.

169 ECtHR, *Von Hannover v. Germany,* No. 59320/00, 2004 წლის 24 ივნისი; ECtHR, *Sciacca v.Italy,* No. 50774/99, 2005 წლის 11 იანვარი; CJEU, C-212/13, *František Ryneš v. Úřad pro ochranu osobnřch Údajů,* 2014 წლის 11 დეკემბერი.

170 ECtHR, *Peck v. the United Kingdom,* No. 44647/98, 2003 წლის 28 იანვარი; ECtHR, *Köpke v. Germany (dec.),* No. 420/07, 2010 წლის 5 ოქტომბერი; EDPS (2010), The EDPS video-surveillance guidelines, 2010 წლის 17 მარტი.

171 ECtHR, *P.G. and J.H. v. the United Kingdom,* No. 44787/98, 2001 წლის 25 სექტემბერი, პუნქტები 59–60; ECtHR, *Wisse v. France,* No. 71611/01, 2005 წლის 20 დეკემბერი (ფრანგულენოვანი ვერსია).

172 იხ. 29-ე მუხლის სამუშაო ჯგუფი (2007), *მოსაზრება 4/2007 პერსონალური მონაცემების კონცეფციის შესახებ,* WP136, 2007 წლის 20 ივნისი, გვ. 9; ევროპის საბჭო, Recommendation No. Rec(2006)4 of the Committee of Ministers to member states on research on biological materials of human origin, 2006 წლის 15 მარტი.

173 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (13).

განხილული მე-3 თავში), მონაცემები „შენახული უნდა იყოს ისეთი ფორმით, რომ მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობას იძლეოდეს მხოლოდ მათი დამუშავების მიზნებისთვის აუცილებელ დროში.“[174] შესაბამისად, მონაცემები უნდა წაიშალოს. თუკი დამმუშავებელს მონაცემების შენახვა სურს მას შემდეგაც, რაც ისინი საჭირო აღარ არის და აღარ ემსახურება თავდაპირველ მიზანს, უნდა მოხდეს მათი ანონიმიზაცია.

ანონიმიზაციის პროცესი გულისხმობს ყველა იმ ელემენტის ამოღებას პერსონალური მონაცემიდან, რომელთა გარეშეც ისინი უკვე აღარ იძლევა იდენტიფიცირების საშუალებას.[175] 29-ე მუხლის სამუშაო ჯგუფი თავის მოსაზრებაში 05/2014 აანალიზებს ანონიმიზაციის სხვადასხვა ტექნიკას.[176] იგი აღიარებს ამ ტექნიკების მნიშვნელობას და, ამავდროულად, ხაზგასმით აღნიშნავს, რომ ზოგიერთი ეს საშუალება შეიძლება არ შეესაბამებოდეს ყველა შემთხვევას. ასეთ ვითარებაში ოპტიმალური გადაწყვეტის მოსაძიებლად, ანონიმიზაციის სათანადო პროცესზე გადაწყვეტილება უნდა მიიღონ თითოეულ კონკრეტულ შემთხვევაში. გამოყენებული ტექნიკის მიუხედავად, საჭიროა იდენტიფიკაციის პრევენცია შეუქცევადი გზით. ამრიგად, მონაცემთა ანონიმიზაციისათვის, ინფორმაციაში არ უნდა დარჩეს არცერთი ელემენტი, რომელიც, გონივრული ძალისხმევის შედეგად, შესაბამისი პირის ხელახალი იდენტიფიცირების შესაძლებლობას იძლევა.[177] ხელახალი იდენტიფიკაციის რისკის შეფასება შესაძლებელია იმ დროის, ძალისხმევისა და რესურსების გათვალისწინებით, „რომლებიც საჭიროა მონაცემთა ბუნებიდან, გამოყენების კონტექსტიდან, ხელახლა იდენტიფიცირების ხელმისაწვდომი ტექნოლოგიებიდან და მათთან დაკავშირებული ხარჯებიდან გამომდინარე“. [178]

წარმატებით ანონიმიზებული ინფორმაცია პერსონალურ მონაცემად აღარ ჩაითვლება და მასზე აღარ გავრცელდება პერსონალურ მონაცემთა დაცვის კანონმდებლობა.

GDPR ადგენს, რომ პირს ან ორგანიზაციას, რომელიც ამუშავებს პერსონალურ მონაცემებს, არ შეიძლება დაეკისროს დამატებითი ინფორმაციის შენახვის, მოპოვებისა და დამუშავების ვალდებულება მონაცემთა სუბიექტის იდენტიფიცირებისათვის, მხოლოდ და მხოლოდ რეგულაციასთან შესაბამისობის

174 *იქვე,* მუხლი 5(1)(ე); 108-ე მოდერნიზებული კონვენცია, მუხლი 5(4)(ე).

175 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის პუნქტი 26.

176 29-ე მუხლის სამუშაო ჯგუფი (2014), მოსაზრება 05/2014 ანონიმიზაციის ტექნიკების შესახებ, WP216, 2014 წლის 10 აპრილი.

177 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის პუნქტი 26.

178 ევროპის საბჭო, 108-ე კონვენციის კომიტეტი (2017), სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, 2017 წლის 23 იანვარი, პუნქტი 6.2.

მიზნით. ამავდროულად, არსებობს მნიშვნელოვანი გამონაკლისი ამ წესიდან: როდესაც მონაცემთა სუბიექტი, მონაცემებზე წვდომის, შესწორების, წაშლისა და დამუშავება-პორტირებაზე უარის თქმის უფლებებით სარგებლობისათვის, დამატებით ინფორმაციას აწვდის დამმუშავებელს და ეს მისი იდენტიფიკაციის შესაძლებლობას იძლევა, მონაცემები, რომლებიც მანამდე ანონიმიზებული იყო, კვლავ პერსონალური ხდება.[179]

ფსევდონიმიზაცია

პერსონალური მონაცემები შეიცავს ისეთ მახასიათებლებს, როგორიცაა სახელი, დაბადების თარიღი, სქესი, მისამართი ან სხვა ელემენტები, რომლებიც იდენტიფიცირების შესაძლებლობას იძლევა. პერსონალური მონაცემების ფსევდონიმიზაციის პროცესი გულისხმობს ამ მახასიათებელთა ჩანაცვლებას ფსევდონიმით.

ევროკავშირის სამართალში ფსევდონიმიზაცია ნიშნავს „პერსონალური მონაცემების იმგვარ დამუშავებას, როდესაც, დამატებითი ინფორმაციის გამოყენების გარეშე, შეუძლებელია მათი დაკავშირება კონკრეტულ მონაცემთა სუბიექტთან, იმ პირობით, რომ ეს დამატებითი ინფორმაცია შენახულია ცალკე, და მონაცემები, ტექნიკური და ორგანიზაციული ზომების მეშვეობით, არ უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.“[180] ანონიმიზებული მონაცემებისაგან განსხვავებით, ფსევდონიმიზებული ინფორმაცია კვლავ პერსონალური მონაცემია. შესაბამისად, მასზე ვრცელდება მონაცემთა დაცვის კანონმდებლობა. მიუხედავად იმისა, რომ ფსევდონიმიზაციას შეუძლია, შეამციროს მონაცემთა სუბიექტების უსაფრთხოების რისკები, იგი კვლავ GDPR-ის მოქმედების სფეროში რჩება.

GDPR აღიარებს, რომ ფსევდონიმიზაციის, როგორც მონაცემთა დაცვის გაძლიერების ღონისძიების, გამოყენება შესაძლებელია სხვადასხვაგვარად. კერძოდ, ის მოხსენიებულია შექმნისა და დამუშავების უსაფრთხოების კონტექსტში.[181] ფსევდონიმიზაცია, როგორც უსაფრთხოების სათანადო ზომა, შეიძლება გამოიყენებოდეს პერსონალურ მონაცემთა დასამუშავებლად თავდაპირველი ამოცანებისგან განსხვავებული მიზნებით. [182]

ფსევდონიმიზაცია კონკრეტულად არ არის მოხსენიებული მოდერნიზებულ 108-ე კონვენციაში, თუმცა, კონვენციის განმარტებითი ბარათი მკაფიოდ

179 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 11.

180 *იქვე,* მუხლი 4 (5).

181 *იქვე,* მუხლი 25 (1).

182 *იქვე,* მუხლი 6 (4).

აცხადებს, რომ „ფსევდონიმის ან ნებისმიერი სხვა სახის ციფრული იდენტიფიკატორის/ციფრული იდენტობის გამოყენება არ იწვევს მონაცემთა ანონიმიზაციას, ვინაიდან მონაცემთა სუბიექტი შეიძლება კვლავ იდენტიფიცირებადი ან ინდივიდუალიზებული იყოს.“[183] მონაცემთა ფსევდონიმიზაციის ერთ-ერთი საშუალებაა მათი დაშიფვრა. ფსევდონიმიზაციის შემდეგ, პიროვნების ვინაობასთან კავშირი იარსებებს იმ ფორმით, რომელიც ერთდროულად მოიცავს როგორც ფსევდონიმის, ისე დაშიფვრის გასაღებს. თუმცა, მათთვის, ვისაც აქვს დაშიფვრის კოდის გამოყენების უფლებამოსილება, ხელახალი იდენტიფიცირება მარტივია. დაშიფვრის კოდი განსაკუთრებით დაცული უნდა იყოს არაუფლებამოსილი პირების მიერ გამოყენებისაგან. შესაბამისად, „ფსევდონიმიზებული მონაცემები [...] მიიჩნევა პერსონალურ მონაცემებად“, რომლებზეც ვრცელდება 108-ე მოდერნიზებული კონვენცია.[184]

ნამდვილობის დადგენა

ნამდვილობის დადგენა არის პროცედურა, რომლითაც პირს შეუძლია, დაადასტუროს გარკვეული ვინაობა ან/და უფლებამოსილება გარკვეული ქმედებების განსახორციელებლად, როგორიცაა დაცულ ტერიტორიაზე შესვლა ან თანხის გამოტანა საბანკო ანგარიშიდან. ნამდვილობა შეიძლება დადგინდეს ისეთი გზებით, როგორიცაა: ბიომეტრიული მონაცემების შედარება (მაგ.: ფოტოსურათის ან პასპორტში თითის ანაბეჭდის შედარება პიროვნების მიერ წარდგენილ მონაცემებთან, თუნდაც საიმიგრაციო კონტროლის დროს);[185] იმ ინფორმაციის მოთხოვნა, რომელიც ეცოდინება მხოლოდ კონკრეტული ვინაობის ან ავტორიზაციის მქონე პირს (მაგ.: პერსონალური საიდენტიფიკაციო ნომერი (PIN) და პაროლი); კონკრეტული გასაღების წარდგენის მოთხოვნა, რომელსაც უნდა ფლობდეს მხოლოდ კონკრეტული ვინაობისა და ავტორიზაციის მქონე პირი (მაგ.: სპეციალური ჩიპიანი ბარათი ან საბანკო სეიფის გასაღები). განსხვავებით პაროლებისა და ჩიპიანი ბარათებისგან, ზოგჯერ, პერსონალურ საიდენტიფიკაციო ნომრებთან ერთად, ინსტრუმენტად გამოიყენება ელექტრონული ხელმოწერები, რაც შესაძლებელს ხდის ელექტრონული კომუნიკაციების პირის ვინაობისა და ავთენტურობის დადგენას.

2.1.2 განსაკუთრებული კატეგორიის პერსონალური მონაცემები

როგორც ევროკავშირის, ისე ევროპის საბჭოს კანონმდებლობის მიხედვით, არსებობს პერსონალურ მონაცემთა განსაკუთრებული კატეგორიები, რომლებიც, თავიანთი ბუნებიდან გამომდინარე, დამუშავებისას შეიძლება რისკებს

183 108-ე მოდერნიზებული კონვენციის განმარტებითი ბარათი, პუნქტი 18.

184 *იქვე.*

185 *იქვე,* პუნქტი 56–57.

შეიცავდეს მონაცემთა სუბიექტებისათვის. შესაბამისად, ისინი საჭიროებს გაძლიერებულ დაცვას. ამგვარ მონაცემებზე ვრცელდება აკრძალვის პრინციპი და მათი დამუშავება კანონის თანახმად ნებადართულია მხოლოდ შეზღუდული რაოდენობით.

108-ე მოდერნიზებული კონვენციის (მუხლი 6) და GDPR-ის (მუხლი 9) ფარგლებში, სენსიტიურ მონაცემებად მიიჩნევა პერსონალური მონაცემები:

- რასისა და ეთნიკური წარმომავლობის შესახებ;
- პოლიტიკური, რელიგიური ან სხვა შეხედულებების შესახებ (ფილოსოფიურის ჩათვლით);
- პროფესიული კავშირის წევრობის შესახებ;
- გენეტიკური და ბიომეტრიული მახასიათებლების შესახებ, რომელთა დამუშავებაც ხდება პროვნების იდენტიფიცირების მიზნით;
- პიროვნების ჯანმრთელობის მდგომარეობის, სქესობრივი ცხოვრების ან სექსუალური ორიენტაციის შესახებ.

მაგალითი: *Bodil Lindqvist-ის*[186] საქმე შეეხებოდა ერთ-ერთ ინტერნეტგვერდზე ადამიანების იდენტიფიცირებას სახელით ან სხვა საშუალებებით, როგორიცაა ტელეფონის ნომერი და ინფორმაცია ჰობის შესახებ. CJEU-მ დაადგინა: „მითითება იმ ფაქტზე, რომ პიროვნებამ დაიზიანა ფეხი და ნახევარ განაკვეთზე მუშაობს სამედიცინო მიზეზების გამო, პერსონალური მონაცემია ჯანმრთელობის შესახებ.“[187]

ნასამართლობასა და დანაშაულის ჩადენასთან დაკავშირებული პერსონალური მონაცემები

მოდერნიზებული 108-ე კონვენცია მოიცავს პერსონალურ მონაცემებს დანაშაულების, სისხლის სამართლის საქმის წარმოებისა და ნასამართლობის შესახებ, ასევე, შესაბამის უსაფრთხოების ზომებს, რომლებიც წარმოდგენილია განსაკუთრებული კატეგორიის მონაცემთა სიაში.[188] ზოგად რეგულაცია-

186 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist,* 2003 წლის 6 ნოემბერი, პუნქტი 51.

187 ყოფილი დირექტივა 95/46/EC, მუხლი 8 (1), ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 9 (1).

188 108-ე მოდერნიზებული კონვენცია, მუხლი 6 (1).

ში (GDPR) ინფორმაცია ნასამართლობისა და დანაშაულის ჩადენის შესახებ, შესაბამის უსაფრთხოების ზომებთან ერთად, წარმოდგენილია განსაკუთრებული კატეგორიის მონაცემთა ჩამონათვალში, თუმცა მას ცალკე მუხლი არეგულირებს. მისი მე-10 მუხლის თანახმად, ასეთი მონაცემები „უნდა დამუშავდეს მხოლოდ ოფიციალური ორგანოს კონტროლქვეშ, ან ევროკავშირისა თუ წევრი სახელმწიფოს კანონის თანახმად, რომელიც უზრუნველყოფს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის სათანადო გარანტიებს.“ კომპლექსური რეესტრები, სადაც დაცულია ინფორმაცია ნასამართლობაზე, ერთი მხრივ, მხოლოდ კონკრეტულმა ოფიციალურმა ორგანოებმა უნდა აწარმოონ.[189] ევროკავშირში პერსონალურ მონაცემთა დაცვას სამართალდამცველი სფეროს კონტექსტში არეგულირებს კონკრეტული სამართლებრივი ინსტრუმენტი - დირექტივა 2016/680/EU.[190] ეს დირექტივა ადგენს უფლებამოსილი ორგანოებისათვის სავალდებულოდ შესასრულებელ კონკრეტულ წესებს მონაცემთა დაცვისათვის, როდესაც ისინი პერსონალურ ინფორმაციას ამუშავებენ კონკრეტულად სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენისა და დამნაშავეთა დასჯის მიზნით (იხ. ნაწილი 8.2.1).

2.2 მონაცემთა დამუშავება

ძირითადი საკითხები

- „მონაცემთა დამუშავება“ გულისხმობს ნებისმიერ ქმედებას პერსონალური მონაცემების მიმართ;
- ტერმინი „დამუშავება“ მოიცავს ავტომატურ და არაავტომატურ დამუშავებას;
- ევროკავშირის კანონმდებლობით, „დამუშავება“ ასევე ეხება არაავტომატურ დამუშავებას სტრუქტურიზებულ ფაილურ სისტემებში.
- ევროპის საბჭოს კანონმდებლობის მიხედვით, შესაძლებელია, „დამუშავების“ ცნება, ეროვნული კანონმდებლობით, ვრცელდებოდეს მონაცემთა არაავტომატურ დამუშავებაზეც.

189 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 10.

190 ევროპის პარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680, უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ L 119.

2.2.1 მონაცემთა დამუშავების კონცეფცია

პერსონალურ მონაცემთა დამუშავების კონცეფცია კომპლექსურია, როგორც ევროკავშირის, ისე ევროპის საბჭოს სამართალში: „პერსონალურ მონაცემთა დამუშავება [...] გულისხმობს ნებისმიერ ქმედებას [...], როგორიცაა, მაგალითად: შეგროვება; აღრიცხვა/ჩაწერა; ორგანიზება; სტრუქტურირება; შენახვა; ადაპტაცია ან შეცვლა; ამოღება; გაცნობა; გამოყენება; გამჟღავნება გადაცემით, გავრცელებით ან სხვაგვარი ხელმისაწვდომობით; დაჯგუფება ან კომბინირება; შეზღუდვა; წაშლა ან განადგურება.“[191] 108-ე მოდერნიზებული კონვენცია ამ ჩამონათვალს ამატებს პერსონალურ მონაცემთა დაცვას.[192]

მაგალითები: *František Ryneš*-ის საქმეში[193] ბატონმა რეინეშმა, სახლში უსაფრთხოების მიზნით დამონტაჟებული CCTV სისტემის გამოყენებით დააფიქსირა იმ ორი ადამიანის გამოსახულება, რომლებმაც ფანჯრები ჩაუმსხვრიეს. CJEU-მ დაადგინა, რომ ვიდეოთვალთვალი, რომელიც მოიცავდა პერსონალურ მონაცემთა ჩაწერა-შენახვას,მონაცემთა ავტომატური დამუშავებაა, რაზეც ვრცელდება ევროკავშირის მონაცემთა დაცვის კანონმდებლობა.

საქმეში *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*[194] ბატონი მანი ითხოვდა თავისი პერსონალური მონაცემების წაშლას სარეიტინგო კომპანიის რეესტრიდან, რომელიც მის სახელს უკავშირებდა უძრავი ქონების ლიკვიდირებულ კომპანიას, რითაც ზიანდებოდა მისი რეპუტაცია. CJEU-მ დაადგინა, რომ „ინფორმაციის ტრანსკრიფციით გადმოცემით, რეესტრში შენახვითა და გადაცემით (მესამე მხარის მოთხოვნის საფუძველზე), რეესტრის შენახვაზე/დაცვაზე პასუხისმგებელი ორგანო „ამუშავებს პერსონალურ მონაცემებს“. შესაბამისად, იგი „დამმუშავებელია“.

მაგალითი: დამსაქმებლები თავიანთ დასაქმებულებზე აგროვებენ და ამუშავებენ მონაცემებს, მათ შორის, ინფორმაციას დასაქმებულთა ანაზღაურების შესახებ. ამ ქმედების კანონიერების სამართლებრივი საფუძველია შრომითი ხელშეკრულება.

191 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (2); ასევე, 108-ე მოდერნიზებული კონვენცია, მუხლი 2 (ბ).

192 108-ე მოდერნიზებული კონვენცია, მუხლი 2 (ბ).

193 CJEU, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů,* 2014 წლის 11 დეკემბერი, პუნქტი 25.

194 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni,* 2017 წლის 9 მარტი, პუნქტი 35.

დამსაქმებლები ვალდებულნი არიან, მონაცემები თავიანთი თანამშრომლების ანაზღაურების შესახებ გადაუგზავნონ საგადასახადო ორგანოებს. მოდერნიზებული 108-ე კონვენციისა და GDPR-ის განმარტებების შესაბამისად, ასეთი გადაგზავნაც მონაცემთა დამუშავებად მიიჩნევა, თუმცა, ამგვარი გამჟღავნების სამართლებრივი საფუძველი შრომითი ხელშეკრულებაა. აუცილებელია, არსებობდეს დამატებითი სამართლებრივი საფუძველი დამუშავების იმ ოპერაციებისათვის, რომლებიც გულისხმობს ანაზღაურების მონაცემთა საგადასახადო ორგანოსათვის გადაგზავნას დამსაქმებლის მიერ. ეს სამართლებრივი საფუძველი, როგორც წესი, მოცემულია შიდასახელმწიფოებრივ საგადასახადო კანონმდებლობაში. ამგვარი დებულებებისა და დამუშავების სხვა კანონიერი საფუძვლების გარეშე, მონაცემთა გადაცემა ჩაითვლება არაკანონიერ დამუშავებად.

2.2.2 მონაცემთა ავტომატური დამუშავება

მოდერნიზებული 108-ე კონვენციითა და GDPR-ით დადგენილი მონაცემთა დაცვა სრულად ვრცელდება მონაცემთა ავტომატურ დამუშავებაზე.

ევროკავშირის სამართალში მონაცემთა ავტომატური დამუშავება გულისხმობს ქმედებებს, რომლებიც ხორციელდება „მონაცემთა მიმართ სრულად ან ნაწილობრივ ავტომატური საშუალებებით.[195] მოდერნიზებული 108-ე კონვენცია შეიცავს ასეთივე განმარტებას.[196] პრაქტიკაში ეს ნიშნავს, რომ პერსონალურ მონაცემთა ნებისმიერი სახის დამუშავებაზე ავტომატური საშუალებებით (მაგ.: პერსონალური კომპიუტერის, მობილური მოწყობილობის ან როუტერის დახმარებით) ვრცელდება როგორც ევროკავშირის, ისე ევროპის საბჭოს მონაცემთა დაცვის წესები.

მაგალითები: *Bodil Lindqvist-ის* საქმე[197] შეეხებოდა ერთ-ერთ ინტერნეტგვერდზე სხვადასხვა ადამიანის იდენტიფიცირებას სახელით ან სხვა საშუალებებით, როგორიცაა ტელეფონის ნომერი და ინფორმაცია ჰობის შესახებ. CJEU-მ დაადგინა: „ვებგვერდის მეშვეობით სხვადასხვა პირონებაზე მითითება და მათი იდენტიფიცირება სახელით ან სხვა საშუალებით (მაგ.: ტელეფონის ნომერი, ან ინფორმაცია მათ სამუშაო პირობებსა თუ გატაცებებზე), 95/46 დირექტივის მე-3 მუხლის პირველი პუნქტის ფარგლებში, არის „პერსონალური მონაცემების დამუშავება მთლიანად ან ნაწილობრივ ავტომატური საშუალებით“.[198]

195 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 2 (1) და 4 (2).

196 108-ე მოდერნიზებული კონვენცია, მუხლი 2(ბ)(გ); 108-ე მოდერნიზებული კონვენციის განმარტებითი ბარათი, პუნქტი 21.

197 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist,* 2003 წლის 6 ნოემბერი, პუნქტი 27.

198 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 2 (1).

საქმეში *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[199] ბატონმა გონზალეზმა მოითხოვა, Google-ის საძიებო სისტემიდან წაეშალათ ან შეეცვალათ კავშირი მის სახელსა და იმ ორ საგაზეთო სტატიას შორის, რომლებიც აანონსებდნენ უძრავი ქონების აუქციონის გამართვას სოციალური უსაფრთხოების დავალიანების ამოსაღებად. CJEU-მ განაცხადა: „ინტერნეტის ავტომატური, მუდმივი და სისტემატური შესწავლის პროცესში, ინტერნეტში გამოქვეყნებული ინფორმაციის მოსაძიებლად, საძიებო სისტემის ოპერატორი „აგროვებს“ მონაცემებს, რომლებსაც შემდგომ „აღადგენს“, „იწერს“ და „ალაგებს“ ინდექსაციის პროგრამების ფრგლებში, „ინახავს“ სერვერებზე და, საჭიროებისას, „ამჟღავნებს“ მას; ასევე, უზრუნველყოფს მასზე „წვდომას“ თავისი მომხმარებლებისათვის, საძიებო შედეგების ჩამონათვალის ფორმით.“[200] CJEU-მ დაასკვნა, რომ ამგვარი ქმედება არის „დამუშავება“, მიუხედავად იმისა, რომ საძიებო სისტემის ოპერატორი იმავე ოპერაციებს ახორციელებს სხვა ტიპის ინფორმაციის მიმართ და ამ უკანასკნელს არ განარჩევს პერსონალური მონაცემებისაგან.“

2.2.3 მონაცემთა არაავტომატური დამუშავება

მონაცემთა არაავტომატური დამუშავება ასევე საჭიროებს მონაცემთა დაცვას.

ევროკავშირის სამართლის თანახმად, მონაცემთა დამუშავება მხოლოდ ავტომატური დამუშავებით არ შემოიფარგლება. შესაბამისად, ამ კანონმდებლობით, მონაცემთა დაცვა ეხება პერსონალური მონაცემების დამუშავებას არაავტომატურ ფაილურ სისტემაში - სპეციალური სტრუქტურის მქონე საქაღალდეში.[201] სტრუქტურიზებული ფაილური სისტემა უზრუნველყოფს პერსონალურ მონაცემთა კატეგორიზაციას და მათზე ხელმისაწვდომობას გარკვეული კრიტერიუმების საფუძველზე. მაგალითად, თუ დამსაქმებელი აწარმოებს საქაღალდეს „დასაქმებულთა შვებულება“, რომელიც შეიცავს დეტალურ ინფორმაციას გასული წლის განმავლობაში თანამშრომელთა შვებულების შესახებ, დალაგებულს ანბანის მიხედვით, ასეთი ფაილი ითვლება არაავტომატურ ფაილურ სისტემად, რომელზეც ვრცელდება ევროკავშირის მონაცემთა დაცვის წესები. ამას რამდენიმე მიზეზი აქვს. კერძოდ:

- ფაილების სტრუქტურიზება შესაძლებელია იმგვარად, რომ მოხერხდეს ინფორმაციის სწრაფად და ადვილად მოძიება;

199 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 წლის 13 მაისი.

200 *იქვე,* პუნქტი 28.

201 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 2 (1).

- პერსონალური მონაცემების შენახვა საქაღალდეებში აიოლებს იმ შეზღუდვების აცილებას, რომლებიც კანონმდებლობით გათვალისწინებულია მონაცემთა ავტომატური დამუშავებისათვის.[202]

ევროკავშირის კანონმდებლობის თანახმად, მონაცემთა ავტომატური დამუშავების განმარტება ითვალისწინებს, რომ ავტომატურ ოპერაციებს შორის შეიძლება საჭირო გახდეს პერსონალური მონაცემების არაავტომატური გამოყენება.[203] მოდერნიზებული 108-ე კონვენციის 2(გ) მუხლის თანახმად, „როდესაც მონაცემები არ მუშავდება ავტომატური საშუალებებით, „მონაცემთა დამუშავება“ ნიშნავს ქმედებას ან ქმედებათა ერთობლიობას პერსონალური მონაცემების მიმართ, რომელიც ხორციელდება მათ სტრუქტურირებულ წყებაზე და ხელმისაწვდომი ან დალაგებულია კონკრეტული კრიტერიუმების შესაბამისად.“

2.3 პერსონალურ მონაცემთა მომხმარებლები

ძირითადი საკითხები

- ნებისმიერი პირი, რომელიც განსაზღვრავს სხვების პერსონალურ მონაცემთა დამუშავების საშუალებებსა და მიზნებს, არის „დამმუშავებელი“, მონაცემთა დაცვის კანონმდებლობის შესაბამისად; თუ ამ გადაწყვეტილებას ერთად რამდენიმე პირი იღებს, მათ „ერთობლივი დამმუშავებლები“ ეწოდებათ;
- „უფლებამოსილი პირი“ არის ფიზიკური ან იურიდიული პირი, რომელიც პერსონალურ მონაცემებს ამუშავებს „დამმუშავებლის“ სახელით;
- უფლებამოსილი პირი დამმუშავებელი ხდება, თუ იგი განსაზღვრავს მონაცემთა დამუშავების საშუალებებსა და მიზნებს;
- ნებისმიერი პირი, რომლისთვისაც მჟღავნდება პერსონალური მონაცემები, არის „მიმღები“;
- „მესამე მხარე“ არის ფიზიკური ან იურიდიული პირი, მონაცემთა სუბიექტის, დამმუშავებლის, უფლებამოსილი პირის ან იმ პირის გარდა, რომელსაც აქვს პერსონალურ მონაცემთა დამუშავების უფლება დამმუშავებლის ან უფლებამოსილი პირის პირდაპირი დავალებით;

202 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის პუნქტი 15.

203 108-ე მოდერნიზებული კონვენცია, მუხლი 2 (ბ)(გ).

- თანხმობა, როგორც პერსონალური მონაცემების დამუშავების სამართლებრივი საფუძველი, უნდა იყოს ნებაყოფლობითი, ინფორმირებული და კონკრეტული, და მკაფიოდ გამოხატავდეს დამუშავებაზე თანხმობის სურვილს, ნათლად დადასტურებულს აქტით.

- განსაკუთრებული კატეგორიის მონაცემთა დამუშავება ნებართვის საფუძველზე, საჭიროებს მკაფიოდ გამოხატულ თანხმობას.

2.3.1 მონაცემთა დამმუშავებლები და უფლებამოსილი პირები

მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ფუნქციის ყველაზე მნიშვნელოვანი შედეგი არის სამართლებრივი პასუხისმგებლობის გავრცელება იმ ვალდებულების შესრულებაზე, რომელიც დადგენილია მონაცემთა დაცვის კანონმდებლობით. კერძო სექტორში ეს „როგორც წესი, ფიზიკური ან იურიდიული პირია, საჯარო სექტორში კი - საჯარო დაწესებულება. მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის მნიშვნელოვანი განსხვავებაა: პირველი გახლავთ იურიდიული ან ფიზიკური პირი, რომელიც განსაზღვრავს დამუშავების მიზნებსა და საშუალებებს, მეორე კი - იურიდიული ან ფიზიკური პირი, რომელიც მონაცემებს ამუშავებს დამმუშავებლის სახელით, მკაცრად განსაზღვრული ინსტრუქციების საფუძველზე. ზოგადად, დამუშავებაზე კონტროლი მონაცემთა დამმუშავებელმა უნდა განახორციელოს, სწორედ მას ეკისრება პასუხისმგებლობა ამ საკითხზე, მათ შორის, სამართლებრივიც. თუმცა, მონაცემთა დაცვის წესების რეფორმასთან ერთად, უფლებამოსილ პირებს დაეკისრათ იმ არაერთი მოთხოვნის შესრულების ვალდებულება, რომლებიც მონაცემთა დამმუშავებლებზე ვრცელდება. მაგალითად, GDPR-ის თანახმად, უფლებამოსილი პირი ვალდებულია, აღრიცხოს დამუშავებასთან დაკავშირებული ყველა ქმედება, რითაც დაადასტურებს რეგულაციით დაწესებული ვალდებულებების შესრულებას.[204] მას ასევე მოეთხოვება სათანადო ტექნიკური და ორგანიზაციული ღონისძიებების გატარება დამუშავების უსაფრთხოების უზრუნველსაყოფად[205]: მონაცემთა დაცვის ოფიცრის დანიშვნა გარკვეულ სიტუაციებში[206] და მონაცემთა უსაფრთხოების ნებისმიერი დარღვევის შეტყობინება დამმუშავებლისათვის.[207]

204 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 30 (2).

205 *იქვე,* მუხლი 32.

206 *იქვე,* მუხლი 37.

207 *იქვე,* მუხლი 33 (2).

თუ რამდენად შეუძლია პირს დამუშავების მიზნისა და საშუალებების განსაზღვრა, დამოკიდებულია კონკრეტული შემთხვევის ფაქტობრივ ელემენტებსა ან გარემოებებზე. GDPR-ის თანახმად, უფლებამოსილი პირი შეიძლება იყოს ფიზიკური პირი, იურიდიული პირი ან ნებისმიერი ორგანო. თუმცა, 29-ე მუხლის სამუშაო ჯგუფმა ხაზგასმით აღნიშნა, რომ ადამიანების მიერ საკუთარი უფლებების განსახორციელებლად უფრო სტაბილური დაწესებულების უზრუნველყოფისათვის, „მონაცემთა დამმუშავებლად უპირატესად უნდა განიხილებოდეს თავად კომპანია ან ორგანო, ნაცვლად კონკრეტული პირისა ამ კომპანიასა ან ორგანოში.“ [208] მაგალითად, მედიკოსებისთვის სამედიცინო პრეპარატების მიყიდვის შემთხვევაში, მედიკოსთა სადისტრიბუციო სიის შედგენისა და წარმოებისას მონაცემთა დამმუშავებელი არის უშუალოდ კომპანია და არა მისი გაყიდვების მენეჯერი, რომელიც რეალურად იყენებს და აწარმოებს ამ სიას.

მაგალითი: როდესაც კომპანია Sunshine-ის მარკეტინგის განყოფილება გეგმავს მონაცემთა დამუშავებას მარკეტინგული კვლევებისათვის, დამმუშავებელი არის კომპანია და არა მარკეტინგის განყოფილება, რადგან ამ უკანასკნელს არ გააჩნია დამოუკიდებელი სტატუსი.

ევროკავშირისა და ევროპის საბჭოს კანონმდებლობის თანახმად, მონაცემთა დამმუშავებელი შეიძლება იყოს ფიზიკური პირი. თუმცა, როდესაც მონაცემები მუშავდება ცალსახად პირადი ან საოჯახო საქმიანობის ფარგლებში, კერძო პირზე არ ვრცელდება GDPR-ითა და მოდერნიზებული 108-ე კონვენციით გათვალისწინებული წესები და ის მონაცემთა დამმუშავებლად არ მიიჩნევა.[209] პირზე, რომელიც აწარმოებს პირად მიმოწერას, ან პერსონალურ დღიურს, სადაც აღწერს მეგობრებსა და კოლეგებთან დაკავშირებულ მოვლენებსა თუ ოჯახის წევრთა ჯანმრთელობის მდგომარეობას, შეიძლება არ გავრცელდეს მონაცემთა დაცვის წესები, რადგან ეს მონაცემები, სავარაუდოდ, მხოლოდ პირად ან საოჯახო საქმიანობას შეეხება. GDPR დამატებით განმარტავს, რომ პირადი და საოჯახო საქმიანობა შეიძლება მოიცავდეს სოციალურ ქსელებში აქტიურობასა და ინტერნეტაქტივობასაც.[210] მეორე მხრივ, მონაცემთა დაცვის წესები სრულად ვრცელდება მონაცემთა დამმუშავებლებსა და უფლებამოსილ პირებზე, რომლებიც ქმნიან პერსონალურ მონაცემთა დამუშავების საშუალებებს პირადი ან საოჯახო საქმიანობისათვის (მაგ.: სოციალური ქსელი/პლატფორმა).[211]

208 29-ე მუხლის სამუშაო ჯგუფი (2010), მოსაზრება 1/2010 „უფლებამოსილი პირისა“ და „დამმუშავებლის“ კონცეფციების შესახებ, WP 169, ბრიუსელი, 2010 წლის 16 თებერვალი.

209 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის პუნქტი 18 და მუხლი 2 (2) (გ); 108-ე მოდერნიზებული კონვენცია, მუხლი 3 (2).

210 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის პუნქტი 18.

211 *იქვე*, პრეამბულის პუნქტი 18; 108-ე მოდერნიზებული კონვენციის განმარტებითი ბარათი, პუნქტი 29.

მოქალაქეთა წვდომა ინტერნეტზე, ასევე, ელექტრონული კომერციული პლატფორმების, სოციალური ქსელებისა და ბლოგების გამოყენება საკუთარ თავსა ან სხვებზე პერსონალური ინფორმაციის გასაზიარებლად, სულ უფრო და უფრო ართულებს მონაცემთა დამუშავების გარჩევას პირადი და არაპირადი საქმიანობის ფარგლებში.[212] საქმიანობის პირად ან საოჯახო ბუნებას განსაზღვრავს არსებული გარემოებები.[213] პროფესიული ან კომერციული ასპექტების შემცველი აქტივობა კი საოჯახო საქმიანობად ვერ ჩაითვლება და მასზე ვერ გავრცელდება შესაბამისი საგამონაკლისო წესი.[214] ამრიგად, თუ მონაცემთა დამუშავების მასშტაბი და სიხშირე მიანიშნებს პროფესიულ ან სრულგანაკვეთურ საქმიანობაზე, ფიზიკური პირი შეიძლება ჩაითვალოს მონაცემთა დამმუშავებლად. დამუშავების პროფესიული და კომერციული ბუნების გარდა, კიდევ ერთი გასათვალისწინებელი ფაქტორია პერსონალური მონაცემების ხელმისაწვდომობა ფართო საზოგადოებისათვის, პიროვნების პირადი სფეროს გარეთ. მონაცემთა დაცვის დირექტივის საფუძველზე შექმნილი პრეცედენტული სამართლის თანახმად, მონაცემთა დაცვის კანონმდებლობა ვრცელდება იმ შემთხვევაზეც, როდესაც ფიზიკური პირი ინტერნეტის მოხმარებისას საჯარო ვებგვერდზე გამოაქვეყნებს ინფორმაციას სხვების შესახებ. CJEU-ს ასეთ ფაქტებთან დაკავშირებული საქმე ჯერ არ განუხილავს GDPR-ის საფუძველზე. აღნიშნული რეგულაცია უფრო მეტ ინსტრუქციებს ითვალისწინებს ისეთ თემებთან დაკავშირებით, რომლებზეც არ ვრცელდება მონაცემთა დაცვის კანონმდებლობა და რომლებიც „საოჯახო გამონაკლისის“ ფარგლებში ექცევა (მაგ.: სოციალური მედიის გამოყენება პირადი მიზნებით).

მაგალითი: *Bodil Lindqvist*-ის საქმე[215] შეეხებოდა ერთ-ერთ ინტერნეტგვერდზე სხვადასხვა ადამიანის იდენტიფიცირებას ისეთი საშუალებებით, როგორიცაა სახელი, ტელეფონის ნომერი და ინფორმაცია ჰობის შესახებ. CJEU-მ დაადგინა, რომ „ვებგვერდის მეშვეობით სხვადასხვა პიროვნებაზე მითითება და მათი იდენტიფიცირება სახელით ან სხვა საშუალებით [...], მონაცემთა დაცვის დირექტივის მე-3 მუხლის 1 პუნქტის ფარგლებში, არის „პერსონალური მონაცემების დამუშავება მთლიანად ან ნაწილობრივ ავტომატური საშუალებით“.[216]

212 იხ. 29-ე მუხლის სამუშაო ჯგუფის განცხადება მონაცემთა დაცვის რეფორმის პაკეტის შესახებ გამართულ დისკუსიებზე (2013), დანართი 2: წინადადებები და შესწორებები პირად ან ოჯახურ საქმიანობასთან დაკავშირებული საგამონაკლისო შემთხვევების თაობაზე, 2013 წლის 27 თებერვალი;

213 108-ე მოდერნიზებული კონვენციის განმარტებითი ბარათი, პუნქტი 28.

214 იხ. მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულის პუნქტი 18 და 108-ე მოდერნიზებული კონვენციის განმარტებითი ბარათი, პუნქტი 27.

215 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist,* 2003 წლის 6 ნოემბერი.

216 *იქვე,* პუნქტი 27; ყოფილი 95/46/EC დირექტივა, მუხლი 3 (1), ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 2(1);

> მონაცემთა ასეთი დამუშავება არ ხდება ცალსახად პირადი ან ოჯახური საქმიანობის შემთხვევაში, რომელზეც არ ვრცელდება ევროკავშირის მონაცემთა დაცვის წესები: ეს გამონაკლისი „უნდა განიმარტოს მხოლოდ იმ საქმიანობასთან მიმართებით, რომელიც ხორციელდება პიროვნების პირადი ან ოჯახური ცხოვრების ფარგლებში. ნათელია, რომ ეს არ ეხება პერსონალურ მონაცემთა დამუშავებას ინტერნეტში გამოქვეყნებისას, იმ მიზნით, რომ ისინი ადამიანთა განუსაზღვრელი რაოდენობისათვის იყოს ხელმისაწვდომი.“ [217]

CJEU-ს თანახმად, გარკვეულ შემთხვევებში, ევროკავშირის მონაცემთა დაცვის კანონმდებლობა შეიძლება ვრცელდებოდეს უსაფრთხოების მიზნით დაყენებული კამერის ჩანაწერებზეც.

> მაგალითი: *František Ryneš*-ის საქმეში[218] ბატონმა რეინეშმა უსაფრთხოების მიზნით სახლში დამონტაჟებული CCTV სისტემის გამოყენებით დააფიქსირა იმ ორი ადამიანის გამოსახულება, რომლებმაც ფანჯრები ჩაუმსხვრიეს. ვიდეოჩანაწერი შემდგომ გადაეცა პოლიციას და წარდგენილი იყო სასამართლო პროცესზე. CJEU-მ დაადგინა: „ვინაიდან ვიდეოთვალთვალი [...] მოიცავს (თუნდაც ნაწილობრივ) საჯარო სივრცეს და, შესაბამისად, მონაცემთა დამუშავება პიროვნების პირადი სივრციდან გარეთ არის მიმართული, იგი ვერ ჩაითვლება ცალსახად „პირად ან ოჯახურ საქმიანობად [...].“[219]

მონაცემთა დამმუშავებელი

ევროკავშირის სამართალში მონაცემთა დამმუშავებელი არის პირი, რომელიც „დამოუკიდებლად ან სხვებთან ერთად განსაზღვრავს პერსონალურ მონაცემთა დამუშავების მიზნებსა და საშუალებებს.“[220] დამმუშავებლის გადაწყვეტილება ადგენს, თუ რატომ და როგორ უნდა დამუშავდეს მონაცემები.

ევროპის საბჭოს სამართალში მოდერნიზებული 108-ე კონვენცია „დამმუშავებელს“ განსაზღვრავს შემდეგნაირად: „ფიზიკური ან იურიდიული პირი, საჯარო უწყება, მომსახურების სააგენტო ან ორგანო, რომელსაც, დამოუკიდებ-

---

217 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist,* 2003 წლის 6 ნოემბერი, პუნქტი 47.

218 CJEU, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů,* 2014 წლის 11 დეკემბერი, პუნქტი 33.

219 ყოფილი 95/46/EC დირექტივა, მუხლი 3 (2), მეორე აბზაცი, ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 2(2)(გ).

220 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (7).

ლად ან სხვებთან ერთად, აქვს გადაწყვეტილების მიღების უფლებამოსილება მონაცემთა დამუშავების კუთხით.“[221] ეს უფლებამოსილება შეეხება დამუშავების მიზნებსა და საშუალებებს, დასამუშავებელ მონაცემთა კატეგორიებსა და მონაცემებზე ხელმისაწვდომობას.[222] კანონმდებლობიდან მომდინარეობს ეს უფლებამოსილება თუ ფაქტობრივი გარემოებებიდან, უნდა განისაზღვროს თითოეულ კონკრეტულ შემთხვევაში.[223]

მაგალითი: *Google Spain-ის*[224] საქმეში განმცხადებელი, ესპანეთის მოქალაქე, მოითხოვდა Google-იდან ძველი საგაზეთო სტატიის ამოღებას მისი ფინანსური წარსულის შესახებ.

CJEU-მ იმსჯელა, იყო თუ არა საძიებო სისტემის ოპერატორი Google მონაცემთა „დამმუშავებელი“, მონაცემთა დაცვის დირექტივის 2(დ) მუხლის თანახმად.[225] CJEU-მ გაითვალისწინა „დამმუშავებლის“ ფართო განსაზღვრება „მონაცემთა სუბიექტების ეფექტიანად და სრულად დაცვისათვის“[226] და დაადგინა, რომ საძიებო სისტემის ოპერატორი განსაზღვრავდა საქმიანობის მიზნებსა და საშუალებებს და უზრუნველყოფდა ვებსაიტების გამომცემელთა მიერ ინტერნეტგვერდებზე ატვირთული მონაცემების ხელმისაწვდომობას ნებისმიერი მომხმარებლისათვის, რომელიც ძიებას ახორციელებს მონაცემთა სუბიექტის სახელით.[227] შესაბამისად, CJEU-მ დაადგინა, რომ Google შეიძლება „დამმუშავებლად“ ჩაითვალოს.[228]

თუ დამმუშავებელი რეგისტრირებულია ევროკავშირის ფარგლებს გარეთ, ამ კომპანიას მოეთხოვება ევროკავშირში წარმომადგენლის დანიშვნა, წერილობითი ფორმით.[229] GDPR-ში ხაზგასმით არის აღნიშნული, რომ „წარმომადგენელი უნდა დაინიშნოს ერთ-ერთ წევრ სახელმწიფოში, სადაც იმყოფება

221 მოდერნიზებული 108-ე კონვენცია, მუხლი 2 (დ).

222 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 22.

223 *იქვე.*

224 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 წლის 13 მაისი.

225 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (7); CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 წლის 13 მაისი, პუნქტი 21.

226 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 წლის 13 მაისი, პუნქტი 34.

227 *იქვე,* პუნქტები 35–40.

228 *იქვე,* პუნქტი 41.

229 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 27 (1);

მონაცემთა ის სუბიექტი, რომლის პერსონალური მონაცემებიც მუშავდება სერვისების ან პროდუქტების შესათავაზებლად, ან ვის ქცევასაც აკვირდებიან.“ [230] სხვა შემთხვევაში, შესაძლებელია სამართლებრივი მექანიზმების ინიცირება თავად დამმუშავებლის ან უფლებამოსილი პირის მიმართ.[231]

ერთობლივი დამუშავება

GDPR-ის თანახმად, თუ ორი ან მეტი დამმუშავებელი ერთობლივად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, ისინი ერთობლივ დამმუშავებლად მიიჩნევიან. ეს ნიშნავს, რომ აღნიშნულ პირებს შეუძლიათ, ერთობლივად მიიღონ გადაწყვეტილება მონაცემთა დამუშავების შესახებ, საერთო მიზნის მისაღწევად.[232] მოდერნიზებული 108-ე კონვენციის განმარტებით ბარათში აღნიშნულია, რომ **ევროპის საბჭოს** სამართლებრივი ჩარჩო უშვებს რამდენიმე დამმუშავებლის ანუ ერთობლივი დამმუშავებლების არსებობას. [233]

29-ე მუხლის სამუშაო ჯგუფის თანახმად, ერთობლივ დამუშავებას შეიძლება ჰქონდეს სხვადასხვა ფორმა, სხვადასხვა დამმუშავებლის მონაწილეობა ამ საქმიანობაში კი იყოს არათანაბარი.[234] ამგვარი მოქნილობა იძლევა მონაცემთა დამუშავების სულ უფრო და უფრო კომპლექსურ რეალობაზე მორგების საშუალებას.[235] ამრიგად, რეგულაციით გათვალისწინებულ მოთხოვნებთან შესაბამისობისათვის, დამმუშავებლებმა სპეციალურ შეთანხმებაში უნდა განსაზღვრონ თავიანთი ვალდებულებები.[236]

ერთობლივი დამუშავება განაპირობებს ერთობლივ პასუხისმგებლობას ამ საქმიანობაზე.[237] **ევროკავშირის სამართლის** ფარგლებში ეს ნიშნავს, რომ ერთობლივი დამუშავებისას გამოწვეული მთლიანი ზიანისათვის პასუხი შეიძლება თითოეულ დამმუშავებელს დაეკისროს, რათა მონაცემთა სუბიექტმა ეფექტიანი კომპენსაცია მიიღოს. [238]

---

230 *იქვე,* მუხლი 27 (3);

231 *იქვე,* მუხლი 27 (5).

232 *იქვე,* მუხლი 4 (7) და მუხლი 26.

233 მოდერნიზებული 108-ე კონვენცია, მუხლი 2 (დ); მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 22.

234 29-ე მუხლის სამუშაო ჯგუფი (2010), მოსაზრება 1/2010 „მონაცემთა დამმუშავებლისა“ და „უფლებამოსილი პირის“კონცეფციების შესახებ, WP 169, ბრიუსელი, 16 თებერვალი, 2010, გვ. 19.

235 *იქვე.*

236 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 79.

237 *იქვე,* პუნქტი 21.

238 *იქვე,* მუხლი 82 (4).

მაგალითი: ერთობლივი დამუშავების მაგალითია რამდენიმე საკრედიტო კომპანიის მიერ მონაცემთა ბაზის ერთობლივად წარმოება იმ მომხმარებლების შესახებ, რომლებიც თავიანთ ვალდებულებებს არ ასრულებენ. ამ შემთხვევაში, როდესაც პირი ერთობლივ დამმუშავებელთაგან ერთ-ერთს (ბანკს) მიმართავს კრედიტის მისაღებად, ბანკი მონაცემთა ბაზაში ამოწმებს მომხმარებელს, ინფორმირებული გადაწყვეტილების მისაღებად მის გადახდისუნარიანობაზე.

კანონმდებლობაში ცალსახად არ არის დადგენილი, რამდენად საჭიროა ერთობლივი მიზნის არსებობა ერთობლივი დამუშავებისას, ან საკმარისია თუ არა მიზნების მხოლოდ ნაწილობრივი თანხვედრა. ჯერჯერობით, ევროპულ დონეზე არ არსებობს შესაბამისი პრეცედენტული სამართალი. 29-ე მუხლის სამუშაო ჯგუფი თავის მოსაზრებაში (2010 წ.) აღნიშნავს, რომ ერთობლივ დამმუშავებლებს მიზნები და დამუშავების საშუალებები შეიძლება მთლიანად ან ნაწილობრივ ჰქონდეთ საერთო.[239] საერთო მიზნები და დამუშავების საშუალებები ნიშნავს მჭიდრო კავშირს სხვადასხვა აქტორს შორის; თუ აქტორების მიზნები და დამუშავების საშუალებები ნაწილობრივ ემთხვევა ერთმანეთს, მათ შორის შედარებით ნაკლები კავშირია.

29-ე მუხლის სამუშაო ჯგუფი მხარს უჭერს ერთობლივი დამუშავების უფრო ფართო განმარტებას. ამგვარი მოქნილობა იძლევა მონაცემთა დამუშავების სულ უფრო და უფრო კომპლექსურ რეალობაზე მორგების საშუალებას.[240] სამუშაო ჯგუფის ამ პოზიციას ასახავს SWIFT-ის (მსოფლიო ბანკთაშორისი საფინანსო ტელეკომუნიკაციების საზოგადოება) საქმე.

მაგალითი: ე.წ. *SWIFT-ის* საქმეში ევროპულმა საბანკო ინსტიტუტებმა თავდაპირველად SWIFT დაიქირავეს, როგორც დამმუშავებელი, საბანკო ტრანზაქციების პროცესში მონაცემთა გადასაცემად. SWIFT-მა ეს მონაცემები, რომლებიც აშშ-ში მდებარე კომპიუტერულ სერვერზე ინახებოდა, აშშ-ს სახაზინო დეპარტამენტს გაუზიარა - ისე, რომ დამქირავებლებისგან (ევროპული საბანკო ინსტიტუტებისგან) პირდაპირი მითითება არ მიუღია. 29-ე მუხლის სამუშაო ჯგუფმა იმსჯელა შექმნილი სიტუაციის კანონიერებაზე და დაადგინა, რომ SWIFT და მისი დამქირავებელი ევროპული საბანკო ინსტიტუტები იყვნენ ერთობლივი დამმუშავებლები, რომელთაც ევროპელი მომხმარებლების წინაშე ეკისრებოდათ პასუხისმგებლობა მათი მონაცემების აშშ-ს მთავრობისთვის გამჟღავნების გამო.[241]

239 29-ე მუხლის სამუშაო ჯგუფი (2010), მოსაზრება 1/2010 „მონაცემთა დამმუშავებელისა“ და „უფლებამოსილი პირის“ კონცეფციების შესახებ, WP 169, ბრიუსელი, 2010 წლის 16 თებერვალი, გვ. 19.

240 *იქვე.*

241 29-ე მუხლის სამუშაო ჯგუფი (2006), მოსაზრება 10/2006 მსოფლიო ბანკთაშორისი საფინანსო ტელეკომუნიკაციების საზოგადოების (SWIFT) მიერ პერსონალური მონაცემების დამუშავების შესახებ, WP 128, ბრიუსელი, 2006 წლის 22 ნოემბერი.

უფლებამოსილი პირი

ევროკავშირის სამართალში უფლებამოსილი პირია ის, ვინც პერსონალურ მონაცემებს ამუშავებს დამმუშავებლის სახელით.[242] უფლებამოსილი პირის საქმიანობა შეიძლება შემოიფარგლებოდეს კონკრეტული დავალებით/კონტექსტით, ან იყოს საკმაოდ ვრცელი და კომპლექსური.

ევროპის საბჭოს სამართალში უფლებამოსილი პირის მნიშვნელობა ევროკავშირის სამართლის მსგავსია.[243]

უფლებამოსილი პირები, გარდა იმისა, რომ სხვებისთვის ამუშავებენ მონაცემებს, მონაცემთა სრულფასოვანი დამმუშავებლებიც არიან, ისეთი მიზნებისთვის, როგორიცაა კადრების ადმინისტრირება, გაყიდვები და მომხმარებლები.

მაგალითი: კომპანია, სახელწოდებით Everready სხვა კომპანიებისთვის ამუშავებს მონაცემებს ადამიანური რესურსების ადმინისტრირების მიზნით. ამ ფუნქციის ფარგლებში იგი უფლებამოსილი პირია, თუმცა, როდესაც საკუთარი თანამშრომლების მონაცემებს ამუშავებს, იგი გახლავთ დამმუშავებელი, რაც განიხილება მისი, როგორც დამსაქმებლის მოვალეობათა ჭრილში.

კავშირი მონაცემთა დამმუშავებლებსა და უფლებამოსილ პირებს შორის

ნათელია, რომ მონაცემთა დამმუშავებელი განსაზღვრავს დამუშავების მიზნებსა და საშუალებებს. GDPR-ში ნათლად არის განსაზღვრული, რომ უფლებამოსილ პირს მხოლოდ მონაცემთა დამმუშავებლის მითითების საფუძველზე შეუძლია პერსონალურ მონაცემთა დამუშავება, თუ ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით სხვა რამ არ არის დადგენილი.[244] მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის კონტრაქტი მათი ურთიერთობის აუცილებელი ელემენტია და, ამასთანავე, სამართლებრივი მოთხოვნაც.[245]

მაგალითი: კომპანია Sunshine-ის დირექტორი გადაწყვეტს, რომ მონაცემები თავისი მომხმარებლების შესახებ მართოს Cloudy-მ - მონა-

242 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (8).

243 მოდერნიზებული 108-ე კონვენცია, მუხლი 2 (ვ).

244 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 29.

245 *იქვე,* მუხლი 28 (3).

ცემთა „ღრუბლის“ საშუალებით შენახვის სპეციალისტმა. Sunshine რჩება მონაცემთა დამმუშავებლად, ხოლო Cloudy Company - უფლებამოსილ პირად, ვინაიდან, კონტრაქტის შესაბამისად, Cloudy-ს მხოლოდ Sunshine-ის მომხმარებელთა მონაცემების გამოყენების უფლება აქვს, ამ უკანასკნელის მიერ განსაზღვრული მიზნებით.

თუ დამუშავების საშუალებათა განსაზღვრა დელეგირებულია უფლებამოსილ პირზე, მონაცემთა დამმუშავებელს უნდა შეეძლოს ამ პირის გადაწყვეტილებათა სათანადო კონტროლი დამუშავების საშუალებებთან დაკავშირებით. ზოგადად, პასუხისმგებლობა კვლავ მონაცემთა დამმუშავებელს ეკისრება, რომელმაც უფლებამოსილ პირს უნდა გაუწიოს ზედამხედველობა, რათა მისი გადაწყვეტილებები შეესაბამებოდეს მონაცემთა დაცვის კანონმდებლობასა და მონაცემთა დამმუშავებლის მითითებებს.

ამასთან, თუ უფლებამოსილი პირი არ ითვალისწინებს მონაცემთა დამმუშავებლის მიერ დადგენილ პირობებს, ის გახდება დამმუშავებელი, სულ მცირე, იმ ფარგლებში, რომლითაც დაირღვა დამმუშავებლის ინსტრუქციები. შედეგად, უფლებამოსილი პირი იქნება კანონის შესაბამისად მოქმედი მონაცემთა დამმუშავებელი, ხოლო თავდაპირველ დამმუშავებელს მოუწევს, განმარტოს, თუ როგორ შეძლო აღნიშნულმა პირმა საკუთარი უფლებამოსილების დარღვევა.[246] მართლაც, 29-ე მუხლის სამუშაო ჯგუფი ასეთ შემთხვევებს ერთობლივ დამუშავებად განიხილავს, ვინაიდან ეს მონაცემთა სუბიექტის ინტერესების საუკეთესოდ დაცვას განაპირობებს.[247]

შეიძლება არსებობდეს პრობლემები პასუხისმგებლობის განაწილებასთან დაკავშირებით, თუკი მონაცემთა დამმუშავებელი მცირე საწარმოა, ხოლო უფლებამოსილი პირი - დიდი ზომის კომპანია, რომელსაც აქვს ძალაუფლება, მონაცემთა დამმუშავებელს უკარნახოს დამუშავების პირობები. ასეთ ვითარებაში, 29-ე მუხლის სამუშაო ჯგუფი აცხადებს, რომ პასუხისმგებელობის სტანდარტი არ უნდა შემცირდეს ეკონომიკური დისბალანსის საფუძველზე, მონაცემთა დამმუშავებლის კონცეფციის განმარტება კი უნდა შენარჩუნდეს.[248]

246 *იქვე,* მუხლი 82 (2).

247 29-ე მუხლის სამუშაო ჯგუფი (2010), *მოსაზრება 1/2010 „მონაცემთა დამმუშავებელისა“ და „უფლებამოსილი პირის“ კონცეფციების შესახებ*, WP 169, ბრიუსელი, 2010 წლის 16 თებერვალი, გვ. 25; 29-ე მუხლის სამუშაო ჯგუფი (2006), მოსაზრება 10/2006 მსოფლიო ბანკთაშორისი საფინანსო ტელეკომუნიკაციების საზოგადოების (SWIFT) მიერ პერსონალური მონაცემების დამუშავების შესახებ, WP 128, ბრიუსელი, 2006 წლის 22 ნოემბერი.

248 29-ე მუხლის სამუშაო ჯგუფი (2010), *მოსაზრება 1/2010 „მონაცემთა დამმუშავებელისა“ და „უფლებამოსილი პირის“ კონცეფციების შესახებ,* WP 169, ბრიუსელი, 2010 წლის 16 თებერვალი, გვ. 26.

მკაფიო და გამჭვირვალე პროცესის უზრუნველსაყოფად, მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ურთიერთობის დეტალები წერილობით კონტრაქტში უნდა გაიწეროს.[249] კერძოდ, კონტრაქტი უნდა მოიცავდეს დამუშავების არსს, ბუნებას, მიზანსა და ხანგრძლივობას, ასევე, პერსონალური მონაცემების ტიპსა და მონაცემთა სუბიექტების კატეგორიებს. იგი უნდა ადგენდეს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის უფლება-მოვალეობებს, როგორიცაა მოთხოვნები კონფიდენციალობასა და უსაფრთხოებასთან დაკავშირებით. ასეთი კონტრაქტის არარსებობა არღვევს მონაცემთა დამმუშავებლის ვალდებულებას, წარმოადგინოს წერილობითი დოკუმენტი საერთო პასუხისმგებლობების შესახებ, და ექვემდებარება სანქციის დაწესებას. თუ ზიანი გამოწვეულია იმით, რომ მონაცემთა დამმუშავებელი მოქმედებს კანონიერი ინსტრუქციების ფარგლებს გარეთ, ან არ ასრულებს ამ ინსტრუქციებს, პასუხისმგებლობა შეიძლება დაეკისროს არა მხოლოდ მონაცემთა დამმუშავებელს, არამედ უფლებამოსილ პირსაც.[250] უფლებამოსილმა პირმა მონაცემებთან დაკავშირებულ ყველა სახის მოქმედებაზე ჩანაწერები უნდა აწარმოოს მონაცემთა დამმუშავებლის სახელით.[251] ეს ჩანაწერები მოთხოვნისთანავე წარედგინება საზედამხედველო ორგანოს, რადგან მონაცემთა დამმუშავებელიც და უფლებამოსილი პირიც ვალდებულნი არიან, საქმიანობის პროცესში ითანამშრომლონ ამ ორგანოსთან.[252] მათ ასევე ევალებათ, დაემორჩილონ დამტკიცებულ ქცევის კოდექსსა თუ სერტიფიცირების მექანიზმს, რაც დაადასტურებს შესაბამისობას GDPR-ის მოთხოვნებთან.[253]

უფლებამოსილ პირს შეუძლია გარკვეული დავალებების დელეგირება სხვა უფლებამოსილ პირზე, რაც სამართლებრივად ნებადართულია, თუ მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის მოქმედებს სათანადო სახელშეკრულებო პირობები (მათ შორის, რამდენად საჭიროა დამმუშავებლის ავტორიზაცია ყოველ ჯერზე, და ხომ არ კმარა მხოლოდ ინფორმირება). GDPR-ის თანახმად, როცა მეორე უფლებამოსილი პირი ვერ შეასრულებს მონაცემთა დაცვის ვალდებულებებს, სრული პასუხისმგებლობა ეკისრება პირველ უფლებამოსილ პირს. [254]

ევროპის საბჭოს სამართალში სრულად გამოიყენება მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ის განმარტება, რომელიც წარმოდგენილია ზემოთ. [255]

249 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 28 (3) და (9).

250 *იქვე,* მუხლი 82 (2).

251 *იქვე,* მუხლი 30 (2).

252 *იქვე,* მუხლი 30 (4) და 31.

253 *იქვე,* მუხლი 28 (5) და 42 (4).

254 *იქვე,* მუხლი 28 (4).

255 იხ. მოდერნიზებული 108-ე კონვენცია, მუხლი 2 (ბ)(ვ); რეკომენდაცია პროფილირების შესახებ, მუხლი 1.

2.3.2 მონაცემთა მიმღები და მესამე მხარე/პირი

ამ ორი კატეგორიის პირებსა თუ დაწესებულებებს შორის განსხვავება, რომელიც შემოღებულია მონაცემთა დაცვის დირექტივით, ძირითადად ეხება მათ ურთიერთობას მონაცემთა დამმუშავებელთან და, შესაბამისად, უფლებამოსილებას, ჰქონდეთ წვდომა მონაცემთა დამმუშავებლის ხელთ არსებულ პერსონალურ მონაცემებზე.

„მესამე მხარე/პირი“ განსხვავდება მონაცემთა დამმუშავებლისა და უფლებამოსილი პირისგან. GDPR-ის თანახმად, ეს „არის ფიზიკური ან იურიდიული პირი, საჯარო უწყება, დაწესებულება ან სხვა პირი, მონაცემთა სუბიექტის, დამმუშავებლის, უფლებამოსილი ან იმ პირის გარდა, რომელსაც აქვს პერსონალური მონაცემების დამუშავების უფლებამოსილება დამმუშავებლის ან უფლებამოსილი პირის პირდაპირი დავალებით.“ ეს ნიშნავს, რომ იმ ორგანიზაციის თანამშრომელი, რომელიც არ არის მონაცემთა დამმუშავებელი - მაშინაც კი, თუ იმავე ჯგუფს ან კომპანიას ეკუთვნის - „მესამე პირად“ ჩაითვლება. მეორე მხრივ, იმ ბანკის ფილიალი, რომელიც მომხმარებელთა ანგარიშებს ამუშავებს ცენტრალური ფილიალის პირდაპირი უფლებამოსილების ფარგლებში, „მესამე პირად“ არ მიიჩნევა. [256]

„მიმღები“ ფართო ცნებაა და მხოლოდ „მესამე პირს“ არ მოიცავს. GDPR-ის მე-4 მუხლის მე-9 პუნქტის თანახმად, მონაცემთა მიმღები „გულისხმობს ფიზიკურ ან იურიდიულ პირს, საჯარო დაწესებულებას, სააგენტოს ან სხვა უწყებას, რომელსაც გადაეცემა პერსონალური მონაცემები, მიუხედავად იმისა, მესამე პირია თუ არა.“ მონაცემთა მიმღები შეიძლება იყოს პირი, რომელიც არ არის დაკავშირებული მონაცემთა დამმუშავებელსა ან უფლებამოსილ პირთან (შესაბამისად, იგი მესამე პირად ჩაითვლება), ან პირიქით, უკავშირდება მათ (მაგ.: იმავე კომპანიის ან უწყების სხვა განყოფილების წარმომადგენელი).

მიმღებსა და მესამე მხარეს შორის განსხვავება მნიშვნელოვანია მხოლოდ მონაცემთა კანონიერი გადაცემის პირობებიდან გამომდინარე. მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის თანამშრომელი შეიძლება იყოს პერსონალურ მონაცემთა მიმღები, რომელზეც დამატებითი სამართლებრივი მოთხოვნები არ ვრცელდება, თუკი ის ჩართულია დამმუშავებლის ან უფლებამოსილი პირის მიერ წარმოებულ მონაცემთა დამუშავების ოპერაციებში. ამავდროულად, მესამე პირს, რომელიც არ არის დაკავშირებული მონაცემთა დამმუშავებელსა ან უფლებამოსილ პირთან, არ აქვს მათ მიერ დამუშავებული მონაცემების გამოყენების უფლება, თუ კონკრეტულ საქმეში არ არსებობს სპეციფიკური სამართლებრივი საფუძვლები.

256 29-ე მუხლის სამუშაო ჯგუფი (2010), *მოსაზრება 1/2010 „მონაცემთა დამმუშავებელისა“ და „უფლებამოსილი პირის“ კონცეფციების შესახებ,* WP 169, ბრიუსელი, 2010 წლის 16 თებერვალი, გვ. 31.

მაგალითი: მონაცემთა დამმუშავებლის თანამშრომელი, რომელიც პერსონალურ მონაცემებს იყენებს დამსაქმებლის მიერ მინიჭებულ უფლებამოვალეობათა ფარგლებში, მონაცემთა მიმღებია, თუმცა არ არის მესამე პირი, რადგან იგი მონაცემებს დამმუშავებლის სახელით და მითითებით იყენებს. მაგალითად, თუ დამსაქმებელი ადამიანური რესურსების დეპარტამენტს გადასცემს საკუთარი თანამშრომლების პერსონალურ მონაცემებს მათი მუშაობის შესაფასებლად, ამ დეპარტამენტის თანამშრომლები პერსონალური მონაცემების მიმღებნი იქნებიან, რადგან მათ ეს მონაცემები გაუმჟღავნეს მონაცემთა დამმუშავებლისთვის განხორციელებული საქმიანობის პროცესში.

ამავდროულად, თუ ორგანიზაცია თავისი დასაქმებულებზე ინფორმაციას გადასცემს ტრენინგების კომპანიას, რომელიც მათ გამოიყენებს შესაფერისი ტრენინგპროგრამების შესადგენად, ეს კომპანია მესამე პირად ჩაითვლება. კერძოდ, ტრენინგკომპანიას არ აქვს პერსონალურ მონაცემთა დამუშავებისათვის საჭირო ლეგიტიმაცია ან ავტორიზაცია (ადამიანური რესურსების დეპარტამენტისგან განსხვავებით, რომელიც მონაცემთა დამმუშავებელთან არის დაკავშირებული). სხვა სიტყვებით რომ ვთქვათ, მათ ინფორმაცია არ მიუღიათ მონაცემთა დამმუშავებელ კომპანიაში დასაქმების პროცესში.

2.4 თანხმობა

ძირითადი საკითხები

- თანხმობა, როგორც პერსონალურ მონაცემთა დამუშავების სამართლებრივი საფუძველი, უნდა იყოს ნებაყოფლობითი, ინფორმირებული და კონკრეტული და მკაფიოდ გამოხატავდეს დამუშავებაზე თანხმობის სურვილს.

- განსაკუთრებული კატეგორიის მონაცემთა დამუშავება საჭიროებს მკაფიოდ გამოხატულ თანხმობას.

მე-4 თავში დეტალურად არის განხილული, რომ თანხმობა მონაცემთა დამუშავების 6 კანონიერი საფუძვლიდან ერთ-ერთია და ნიშნავს „მონაცემთა სუბიექტის სურვილის ნებაყოფილობით, კონკრეტულ და ინფორმირებულ გამოხატულებას.“ [257]

257 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (11); ასევე, მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (2).

ევროკავშირის კანონმდებლობა ადგენს რამდენიმე ელემენტს, რომელთა საფუძველზეც თანხმობა დასაბუთებული/მოქმედია, რაც მიზნად ისახავს იმის დადასტურებას, რომ მონაცემთა სუბიექტს ნამდვილად სურდა დათანხმება თავისი მონაცემების გარკვეული სახით გამოყენებაზე: [258]

- თანხმობა უნდა იყოს მკაფიოდ გამოხატული (მაგ.: განცხადებით) და დგინდებოდეს მონაცემთა სუბიექტის ნებაყოფლობითი, კონკრეტული და ინფორმირებული სურვილი მის მონაცემების დამუშავების შესახებ.

- მონაცემთა სუბიექტი უფლებამოსილია, ნებისმიერ დროს გამოითხოვოს თანხმობა.

- წერილობითი განცხადების კონტექსტში, რომელიც სხვა საკითხებსაც მოიცავს (მაგ.: „მომსახურების პირობებს“), თანხმობაზე მოთხოვნა უნდა იყოს მკაფიო, მარტივი ენით დაწერილი, გასაგები და ადვილად ხელმისაწვდომი, თანხმობა კი ნათლად იყოს გამოყოფილი სხვა საკითხებისგან; თუ ეს განაცხადი არღვევს GDPR-ს, მას არ ექნება შესასრულებლად სავალდებულო ძალა.

მონაცემთა დაცვის კანონმდებლობის კონტექსტში, თანხმობა მოქმედია მხოლოდ მაშინ, თუ შესრულდება ყველა ზემოაღნიშნული მოთხოვნა. მონაცემთა დამმუშავებლის პასუხისმგებლობაში შედის იმის დადასტურება, რომ მონაცემთა სუბიექტმა გამოხატა თანხმობა მისი მონაცემების დამუშავებაზე.[259] იურიდიული ძალის მქონე თანხმობის ელემენტები უფრო დეტალურად განხილულია 4.1.1 ნაწილში, რომელიც შეეხება პერსონალურ მონაცემთა დამუშავების კანონიერ საფუძვლებს.

108-ე კონვენცია არ განმარტავს თანხმობის ცნებას. ამ საკითხის დარეგულირებას კონვენცია ტოვებს შიდასახელმწიფოებრივი კანონმდებლობის ფარგლებში. თუმცა, **ევროპის საბჭოს სამართალში** კანონიერი ძალის მქონე თანხმობის ელემენტები შეესაბამება ზემოთ განხილულ ელემენტებს.[260]

სამოქალაქო სამართლის მიხედვით, თანხმობასთან დაკავშირებული დამატებითი მოთხოვნები, როგორიცაა პირის ქმედუნარიანობა, ბუნებრივია, ვრცელდება მონაცემთა დაცვის სფეროზეც, ვინაიდან ეს მოთხოვნები ძირითადი სამართლებრივი წინაპირობებია. სამართლებრივი ძალის არმქონე თანხმობა ქმედუუნარო პირებისგან ნიშნავს სამართლებრივი საფუძვლის არარსებობას

258 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 7.

259 *იქვე*, მუხლი 7 (1).

260 მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (2); მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტები 42–45.

მათი მონაცემების დამუშავებისათვის. რაც შეეხება არასრულწლოვანთა ქმედუნარიანობას ხელშეკრულების გაფორმების მხრივ, GDPR ადგენს, რომ დირექტივით გათვალისწინებული ასაკობრივი ცენზი კანონიერი ძალის მქონე თანხმობის მოსაპოვებლად გავლენას არ ახდენს წევრ სახელმწიფოთა სახელშეკრულებო სამართალზე.[261]

თანხმობა უნდა გადმოიცეს ნათლად, ისე, რომ არ წარმოშვას რაიმე ეჭვი მონაცემთა სუბიექტის განზრახვასთან დაკავშირებით.[262] როდესაც საქმე ეხება განსაკუთრებული კატეგორიის მონაცემთა დამუშავებას, თანხმობა უნდა გამოიხატოს მკაფიოდ, ზეპირი ან წერილობითი ფორმით.[263] წერილობითი თანხმობის მიცემა შესაძლებელია ელექტრონულადაც.[264] **ევროკავშირისა და ევროპის საბჭოს სამართლის ფარგლებში,** პერსონალური მონაცემების დამუშავებაზე თანხმობა უნდა გამოიხატოს განცხადებით ან ნათელი და აქტიური ქმედებით.[265] ამრიგად, დუმილი, წინასწარ მონიშნული გრაფები, წინასწარ შევსებული ფორმები ან უმოქმედობა ვერ წარმოშობს თანხმობას.[266]

261 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 8 (3).

262 *იქვე,* მუხლი 6(1)(ა) და 9(2)(ა).

263 *იქვე,* პრეამბულა, პუნქტი 32.

264 *იქვე.*

265 *იქვე,* მუხლი 4 (11); მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 42.

266 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 32; მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 42.

3

მონაცემთა დაცვის ევროპული სამართლის მთავარი პრინციპები

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (ა)	**კანონიერების პრინციპი**	მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (3)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (ა)	**სამართლიანობის პრინციპი**	მოდერნიზებული 108-ე კონვენცია, მუხლი (4) (ა); ECtHR, *K.H. and Others v. Slovakia,* No. 32881/04, 2009.
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (ა); CJEU, C-201/14, *Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others,* 2015.	**გამჭვირვალობის პრინციპი**	მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (ა) და მუხლი 8; ECtHR, *Haralambie v. Romania,* No. 21737/03, 2009.
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (ბ)	**მიზნის შეზღუდვის პრინციპი**	მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (ბ)

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (გ); CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland and Kärntner Landesregierung and Others* [GC], 2014.	**მონაცემთა მინიმიზაციის პრინციპი**	მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (გ)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (დ); CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 2009.	**მონაცემთა სიზუსტის პრინციპი**	მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (დ)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (ე); CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland and Kärntner Landesregierung and Others* [GC], 2014.	**შენახვის ვადის შეზღუდვის პრინციპი**	მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (ე); ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 და 30566/04, 2008.
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 5 (1) (ვ) და 32	**მონაცემთა უსაფრთხოების (დაცულობისა და კონფიდენციალობის) პრინციპი**	მოდერნიზებული 108-ე კონვენცია, მუხლი 7
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (2)	**ანგარიშვალდებულების პრინციპი**	მოდერნიზებული 108-ე კონვენცია, მუხლი 10

მონაცემთა დაცვის ზოგადი რეგულაცია ადგენს პერსონალურ მონაცემთა დამუშავების ძირითად პრინციპებს. ესენია:

- კანონიერება, სამართლიანობა და გამჭვირვალობა;
- მიზნის შეზღუდვა;

- მონაცემთა მინიმიზაცია;
- მონაცემთა სიზუსტე;
- შენახვის ვადის შეზღუდვა;
- მონაცემთა უსაფრთხოება და კონფიდენციალობა.

ეს პრინციპები იმ დეტალური დებულებების საფუძველია, რომლებიც წარმოდგენილია რეგულაციის მომდევნო მუხლებში და შეიცავს მოდერნიზებული 108-ე კონვენციის მე-5, მე-7, მე-8 და მე-10 მუხლებიც. მონაცემთა დაცვის ნებისმიერი კანონმდებლობა ევროპის საბჭოსა და ევროკავშირის დონეზე ამ პრინციპებს უნდა აკმაყოფილებდეს. სწორედ მათ უნდა ითვალისწინებდნენ ამ კანონმდებლობის განმარტების დროსაც. ევროკავშირის სამართალში მონაცემთა დამუშავების პრინციპებზე შეზღუდვის დაწესება ნებადართულია მხოლოდ მაშინ, როცა ეს შეზღუდვა შეესაბამება 12-22 მუხლებში წარმოდგენილ უფლება-მოვალეობებს და ითვალისწინებს ფუნდამენტური უფლებებისა და თავისუფლებების არსს. ასეთ შეზღუდვებსა და გამონაკლის შემთხვევებს შეიძლება ადგენდეს ევროპული და შიდასახელმწიფოებრივი კანონმდებლობა.[267] ისინი უნდა იყოს კანონმდებლობით გათვალისწინებული, კანონიერი მიზნის შესაბამისი და აუცილებელი და პროპორციული დემოკრატიულ საზოგადოებაში.[268] აუცილებელია სამივე პირობის დაკმაყოფილება.

3.1 დამუშავების კანონიერების, სამართლიანობისა და გამჭვირვალობის პრინციპები

ძირითადი საკითხები

- კანონიერების, სამართლიანობისა და გამჭვირვალობის პრინციპები ვრცელდება მონაცემთა ნებისმიერი სახის დამუშავებაზე.
- GDPR-ის თანახმად, მონაცემთა დამუშავება კანონიერია, თუ არსებობს:
  - მონაცემთა სუბიექტის თანხმობა;
  - ხელშეკრულების დადების საჭიროება;

267 მოდერნიზებული 108-ე კონვენცია, მუხლი 11 (1); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 23 (1).

268 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 23 (1).

- სამართლებრივი ვალდებულება;
- მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დაცვის საჭიროება;
- საჯარო ინტერესში შემავალი ამოცანების შესრულების საჭიროება;
- მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დაცვის საჭიროება, გარდა იმ შემთხვევისა, როდესაც მონაცემთა სუბიექტის უფლებები და ინტერესები აღემატება მათ.

- პერსონალური მონაცემები უნდა დამუშავდეს სამართლიანად.
  - მონაცემთა სუბიექტი ინფორმირებული უნდა იყოს რისკების შესახებ, რათა დამუშავებას არ მოჰყვეს გაუთვალისწინებელი უარყოფითი შედეგები.
- პერსონალური მონაცემები უნდა დამუშავდეს გამჭვირვალედ.
  - მონაცემთა დამუშავებამდე, დამმუშავებელმა მონაცემთა სუბიექტს უნდა შეატყობინოს დამუშავების მიზანი, დამმუშავებლის ვინაობა და მისამართი, სხვა დეტალებთან ერთად.
  - ინფორმაცია მონაცემთა დამუშავების შესახებ წარმოდგენილი უნდა იყოს გასაგები და მარტივი ენით, რათა მონაცემთა სუბიექტმა ადვილად გაიაზროს შესაბამისი წესები, რისკები, უსაფრთხოების ზომები და უფლებები.
  - მონაცემთა სუბიექტს აქვს მათ მონაცემებზე წვდომის უფლება, დამუშავების ადგილის მიუხედავად.

3.1.1 დამუშავების კანონიერება

ევროკავშირისა და ევროპის საბჭოს მონაცემთა დაცვის კანონმდებლობა ადგენს პერსონალურ მონაცემთა დამუშავების კანონიერების მოთხოვნას.[269] კანონიერი დამუშავება საჭიროებს მონაცემთა სუბიექტის თანხმობას ან მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული სხვა კანონიერი საფუძ-

269 მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (3); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5(1)(ა).

ვლის არსებობას.[270] GDPR-ის მე-6 მუხლის პირველი პუნქტი მოიცავს დამუშავების 5 კანონიერ საფუძველს, თანხმობასთან ერთად. კერძოდ, როდესაც პერსონალური მონაცემების დამუშავება საჭიროა შემდეგი მიზნებით: ხელშეკრულების პირობების შესრულება; საჯარო უფლებამოსილების ფარგლებში დაკისრებული მოვალეობის შესრულება; სამართლებრივი ვალდებულების შესრულება; მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დაცვა; და მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დაცვა.

ეს საკითხები დეტალურად განხილულია 4.1. თავში.

3.1.2 დამუშავების სამართლიანობა

კანონიერების გარდა, ევროკავშირისა და ევროპის საბჭოს მონაცემთა დაცვის კანონმდებლობა მოითხოვს პერსონალურ მონაცემთა სამართლიან დამუშავებასაც.[271] სამართლიანი დამუშავების პრინციპი, ძირითადად, აწესრიგებს ურთიერთობას მონაცემთა დამმუშავებელსა და მონაცემთა სუბიექტს შორის.

დამმუშავებელმა მონაცემთა სუბიექტებსა და ფართო საზოგადოებას უნდა შეატყობინოს, რომ მონაცემებს ამუშავებს კანონიერად და გამჭვირვალედ. მან უნდა შეძლოს დადასტურება, რომ დამუშავებასთან დაკავშირებული საქმიანობა შეესაბამება GDPR-ს. დამუშავება არ უნდა განხორციელდეს საიდუმლოდ, ხოლო მონაცემთა სუბიექტებს უნდა ჰქონდეთ ინფორმაცია რისკების შესახებ. ამასთან, მონაცემთა დამმუშავებელმა შეძლებისდაგვარად სწრაფად უნდა შეასრულოს მონაცემთა სუბიექტის სურვილები, განსაკუთრებით, თუ ამ უკანასკნელის თანხმობა ქმნის მონაცემთა დაცვის სამართლებრივ საფუძველს.

მაგალითი: საქმეში *K.H. and Others v. Slovakia*[272] განმცხადებლებს - ბოშური წარმოშობის ქალებს - აღმოსავლეთ სლოვაკეთში მდებარე ორ საავადმყოფოში გაუწიეს სამედიცინო მომსახურება ორსულობისა და მშობიარობის დროს. ამის შემდეგ, მიუხედავად არაერთი მცდელობისა, ვერცერთმა მათგანმა ვერ შეძლო დაორსულება. ეროვნულმა სასამართლოებმა საავადმყოფოებს მოსთხოვეს, განმცხადებლებისა და მათი წარმომადგენლებისათვის დაერთოთ ნება, გაცნობოდნენ სამედიცინო ჩა-

270 ევროკავშირის ფუნდამენტურ უფლებათა ქარტია, მუხლი 8 (2); მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 40 და მუხლები 6–9; მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (2); მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 41.

271 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (ა); მოდერნიზებული 108-ე კონვენცია, მუხლი 5(4)(ა).

272 ECtHR, *K.H. and Others v. Slovakia,* No. 32881/04, 2009 წლის 28 აპრილი.

ნაწერებს და გაეკეთებინათ წერილობითი ამონაწერები, თუმცა მათ არ დააკმაყოფილეს მოთხოვნა დოკუმენტების ასლის გადაღებაზე. მიზეზად დაასახელეს დოკუმენტების ბოროტად გამოყენების საფრთხე. ECHR-ის მე-8 მუხლი სახელმწიფოებს უდგენს პოზიტიურ ვალდებულებას, რომელიც მოიცავს მონაცემთა სუბიექტის ხელმისაწვდომობას თავისი მონაცემების ასლებზე. სახელმწიფომ უნდა განსაზღვროს პერსონალურ მონაცემთა ფაილების ასლად გადაღების პირობები ან, მყარი მიზეზების არსებობისას, მონაცემთა სუბიექტს უარი უთხრას ამაზე. განმცხადებლების შემთხვევაში, ეროვნული სასამართლოები ასლების გადაღებაზე უარს ამართლებდნენ შესაბამისი ინფორმაციის ბოროტად გამოყენებისგან დაცვით. თუმცა, ECtHR-მა ვერ დაინახა, როგორ გამოიყენებდნენ ბოროტად განმცხადებლები მათ შესახებ ინფორმაციას, თუკი ექნებოდათ წვდომა მთლიან სამედიცინო მასალებზე. ამასთან, ბოროტად გამოყენების პრევენცია შესაძლებელია სხვა საშუალებებით, რომლებიც არ გულისხმობს ასლის გადაღებაზე უარის თქმას (მაგ.: იმ პირთა წრის დავიწროება, რომლებსაც აღნიშნულ მასალებზე წვდომის უფლება აქვთ). სახელმწიფომ საკმარისად მყარი მიზეზებით ვერ დაასაბუთა თავისი უარი, განმცხადებლებს ჰქონოდათ წვდომა მათი ჯანმრთელობის შესახებ ინფორმაციაზე. სასამართლომ საქმეში დაადგინა მე-8 მუხლის დარღვევა.

ინტერნეტმომსახურებასთან მიმართებით, მონაცემთა დამუშავების სისტემის მახასიათებლები მონაცემთა სუბიექტებს საშუალებას უნდა აძლევდეს, იცოდნენ, რა ემართება მათ მონაცემებს. ნებისმიერ შემთხვევაში, სამართლიანობის პრინციპი სცდება გამჭვირვალობის ვალდებულებებს და, შეიძლება ითქვას, უკავშირდება პერსონალურ მონაცემთა ეთიკური პრინციპებით დამუშავებას.

მაგალითი: უნივერსიტეტის კვლევითი დეპარტამენტი ატარებს ექსპერიმენტს, რომელიც აანალიზებს 50 სუბიექტის განწყობის ცვლილებას. მონაწილეებს მოეთხოვებათ, თავიანთი აზრები ნებისმიერ დროს საათობრივად აღრიცხონ ელექტრონულ ფაილებში. პროექტში მონაწილეობას და უნივერსიტეტის მიერ მონაცემთა ამგვარ კონკრეტულ გამოყენებას დათანხმდა 50 პირი. მოგვიანებით, კვლევის დეპარტამენტმა აღმოაჩინა, რომ აზრების ელექტრონულად აღრიცხვის შედეგად მიღებული მონაცემები კიდევ ერთ პროექტსაც გამოადგება, რომელიც ფიკუსირებულია ფსიქიკურ ჯანმრთელობაზე და სხვა ჯგუფის კოორდინაციით ხორციელდება. ვინაიდან მიზნები იყო ურთიერთშესაბამისი, უნივერსიტეტს, როგორც მონაცემთა დამმუშავებელს, შეეძლო, იგივე მონაცემები სხვა ჯგუფის სამუშაოსთვის ისე გამოეყენებინა, რომ არ გადაედგა დამატებითი ნაბიჯები მონაცემთა დამუშავების კანონიერებისათვის, თუმცა მან მაინც აცნობა სუბიექტების ამის შესახებ და ხელახლა სთხოვა ნებართვა. ამრიგად, უნივერსიტეტი მოიქცა კვლევის ეთიკის კოდექსისა და სამართლიანი დამუშავების პრინციპების შესაბამისად.

3.1.3 დამუშავების გამჭვირვალობა

ევროკავშირისა და ევროპის საბჭოს მონაცემთა დაცვის სამართალი მოითხოვს, რომ პერსონალური მონაცემები „მონაცემთა სუბიექტთან მიმართებით გამჭვირვალედ“ დამუშავდეს. [273]

ეს პრინციპი ადგენს მონაცემთა დამმუშავებლის ვალდებულებას, მიიღოს სათანადო ზომები მონაცემთა სუბიექტების (მომხმარებლებისა თუ კლიენტების) ინფორმირებისათვის მათი მონაცემების გამოყენებაზე. [274] გამჭვირვალობა გულისხმობს ინფორმაციას, რომელსაც მონაცემთა სუბიექტები იღებენ მონაცემთა დამუშავების დაწყებამდე.[275] ეს ინფორმაცია მზა ფორმით უნდა იყოს ხელმისაწვდომი მონაცემთა სუბიექტებისათვის, დამუშავების პროცესში.[276] გამჭვირვალობა შესაძლოა მოიცავდეს იმ ინფორმაციასაც, რომელსაც მონაცემთა სუბიექტები იღებენ საკუთარ მონაცემებზე წვდომის მოთხოვნის საფუძველზე.[277]

მაგალითი: საქმეში *Haralambie v. Romania*[278] განმცხადებლის მოთხოვნა მის შესახებ საიდუმლო სამსახურის ხელთ არსებული ინფორმაციის ხელმისაწვდომობაზე მხოლოდ 5 წლის შემდეგ დააკმაყოფილეს. ECtHR-მა კიდევ ერთხელ ხაზგასმით აღნიშნა, რომ პირებს, რომლებიც საჯარო უწყებების ხელთ არსებული პერსონალური ფაილების (პირადი საქმის) სუბიექტები არიან, აქვთ ამ ფაილებზე წვდომის სასიცოცხლო ინტერესი და ხელისუფლებას ევალებოდა შესაბამისი ეფექტიანი პროცედურის უზრუნველყოფა. ECtHR-მა მიიჩნია, რომ არც გადაცემული ფაილების რაოდენობა და არც არქივის სისტემაში არსებული ხარვეზები არ ამართლებდა განმცხადებლის მოთხოვნის დაკმაყოფილებას 5 წლის შემდეგ. ხელისუფლებამ განმცხადებელი ვერ უზრუნველყო ეფექტიანი პროცედურით - გონივრულ ვადაში მიეღო წვდომა თავის პერსონალურ ფაილებზე. სასამართლომ საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

დამუშავების ოპერაციები მონაცემთა სუბიექტს უნდა განემარტოს მარტივი ფორმით, რათა შეძლონ გაგება, თუ რა მოსდის მათ მონაცემებს. ეს ნიშნავს,

273 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5(1)(ა); მოდერნიზებული 108-ე კონვენცია, მუხლები 5(4)(ა) და 8.

274 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 12.

275 *იქვე,* მუხლები 13 და 14.

276 29-ე მუხლის სამუშაო ჯგუფი, მოსაზრება 2/2017 სამსახურში მონაცემთა დამუშავების შესახებ, გვ. 23;

277 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 15.

278 ECtHR, *Haralambie v. Romania,* No. 21737/03, 2009 წლის 27 ოქტომბერი.

რომ მონაცემთა სუბიექტმა პერსონალური მონაცემების შეგროვებისას უნდა იცოდეს მათი დამუშავების კონკრეტული მიზანი.[279] დამუშავების გამჭვირვალობა საჭიროებს მარტივი და გასაგები ენის გამოყენებას.[280] შესაბამის პირებს ნათელი წარმოდგენა უნდა ჰქონდეთ პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული რისკების, წესების, უსაფრთხოების ზომებისა და უფლებების შესახებ.[281]

ევროპის საბჭოს კანონმდებლობა ასევე განმარტავს, რომ გარკვეული ინფორმაცია დამმუშავებელმა სავალდებულოდ და პროაქტიულად უნდა წარუდგინოს მონაცემთა სუბიექტებს. კერძოდ, შესაბამის ფორმატში უნდა იყოს მითითებული (ვებგვერდის ან პერსონალური მოწყობილობის ტექნოლოგიური ინსტრუმენტების საშუალებით) მონაცემთა დამმუშავებლის (ან თანადამმუშავებლების) სახელი და მისამართი, დამუშავების სამართლებრივი საფუძველი და მიზნები, დამუშავებული მონაცემების კატეგორიები, მიმღებები და უფლებებით სარგებლობის გზები. მთავარია, ეს ინფორმაცია მონაცემთა სუბიექტს სამართლიანად და ეფექტიანად წარედგინოს. წარდგენილი ინფორმაცია უნდა იყოს ადვილად ხელმისაწვდომი, გარკვევით შედგენილი, გასაგები და მონაცემთა სუბიექტის საჭიროებებზე მორგებული (მაგ.: საჭიროების შემთხვევაში, გამოიყენონ ბავშვისთვის გასაგები ენა). ასევე, წარმოდგენილი უნდა იყოს ნებისმიერი დამატებითი ინფორმაცია, რომელიც ესაჭიროება ან ეხმარება მონაცემთა სამართლიან დამუშავებას, მაგალითად: შენახვის ვადა, ინფორმაცია დამუშავების ლოგიკური საფუძვლის ან სხვა მხარისა თუ არამხარისათვის მონაცემთა გადაცემის შესახებ (მათ შორის, რამდენად იცავს არამხარე მონაცემებს), ან დამმუშავებლის მიერ განხორციელებული ღონისძიებები მონაცემთა სათანადოდ დაცვისთვის).[282]

მონაცემებზე წვდომის უფლების შესაბამისად, [283] მონაცემთა სუბიექტს ენიჭება უფლება, დამმუშავებლისგან მოითხოვოს დასტური მისი მონაცემების დამუშავების შესახებ, ხოლო დადასტურების შემთხვევაში მიიღოს ინფორმაცია დამუშავებულ მონაცემთა კატეგორიებზე. [284] ამასთან, ინფორმაციის მიღების უფლების თანახმად,[285] იმ პირებმა, ვისი მონაცემებიც მუშავდება, მონაცემთა დამმუშავებლისა თუ უფლებამოსილი პირისაგან დამუშავების დაწყებამდე და პროაქტიულად უნდა მიიღონ ინფორმაცია ამ პროცედურის მიზნების, ხანგრძლივობისა და საშუალებების შესახებ, სხვა დეტალებთან ერთად.

279 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 39.

280 *იქვე.*

281 *იქვე.*

282 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 68.

283 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 15.

284 მოდერნიზებული 108-ე კონვენცია, მუხლები 8 და 9 (1) (ბ).

285 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 13 და 14.

მაგალითი: საქმეში *Smaranda Bara and Others v. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)*[286] რუმინეთის ეროვნულმა საგადასახადო ორგანომ თვითდასაქმებულ პირთა შემოსავლების საგადასახადო მონაცემები გადასცა ჯანმრთელობის დაზღვევის ეროვნულ ფონდს, რის საფუძველზეც განისაზღვრა ჯანმრთელობის დაზღვევის გადასახადის ოდენობა. CJEU-მ იმსჯელა, უნდა ეცნობებინათ თუ არა მონაცემთა სუბიექტებისთვის დამმუშავებლის ვინაობა და მონაცემთა გადაცემის მიზანი მანამდე, სანამ მათ დაამუშავებდა ჯანმრთელობის დაზღვევის ეროვნული ფონდი. CJEU-მ დაადგინა: როდესაც წევრი სახელმწიფოს ერთი საჯარო ადმინისტრაციული ორგანო პერსონალურ მონაცემებს მეორე ასეთ უწყებას გადასცემს შემდგომი დამუშავებისთვის, საჭიროა მონაცემთა სუბიექტების ინფორმირება ამის შესახებ.

გარკვეულ სიტუაციებში, მონაცემთა სუბიექტების ინფორმირების ვალდებულებასთან დაკავშირებით, დაშვებულია გამონაკლისები. ამას დეტალურად მიმოიხილავს ნაწილი 6.1, რომელიც მონაცემთა სუბიექტების უფლებებს ეხება.

3.2 მიზნის შეზღუდვის პრინციპი

ძირითადი საკითხები

- მონაცემთა დამუშავების მიზანი ნათლად უნდა განისაზღვროს დამუშავების დაწყებამდე.
- დაუშვებელია მონაცემთა შემდგომი დამუშავება იმგვარად, რომ არ შეესაბამებოდეს დამუშავების თავდაპირველ მიზანს. თუმცა, ამ კუთხით მონაცემთა დაცვის ზოგადი რეგულაცია ითვალისწინებს გარკვეულ გამონაკლის შემთხვევებს, საჯარო ან სამეცნიერო/ისტორიული კვლევის ინტერესებიდან, ანდა სტატისტიკური მიზნებიდან გამომდინარე.
- მიზნის შეზღუდვის პრინციპის არსი ის არის, რომ პერსონალური მონაცემები დამუშავდეს კონკრეტული, კარგად განსაზღვრული მიზნით და მხოლოდ თავდაპირველი მიზნის შესაბამისი დამატებითი, კონკრეტული ამოცანებით.

286 CJEU, C-201/14, *Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others,* 2015 წლის 1 ოქტომბერი, პუნქტები 28–46.

მიზნის შეზღუდვა მონაცემთა დაცვის ევროპულ სამართალში ერთ-ერთი ფუნდამენტური პრინციპია. იგი მჭიდროდ უკავშირდება გამჭვირვალობას, განჭვრეტადობას და მომხმარებლის მხრიდან კონტროლს: თუ დამუშავების მიზანი საკმარისად კონკრეტული და მკაფიოა, შესაბამის პირებს ექმნებათ წარმოდგენა, თუ რას უნდა ელოდონ; ამასთან, უმჯობესდება გამჭვირვალობისა და სამართლებრივი განჭვრეტადობის დონე. მეორე მხრივ, მიზნების მკაფიოდ განსაზღვრა მნიშვნელოვანია იმისათვისაც, რომ მონაცემთა სუბიექტებმა შეძლონ თავიანთი უფლებების ეფექტიანად განხორციელება (მაგ.: როგორიცაა დამუშავების შეწყვეტის მოთხოვნა).[287]

მიზნის შეზღუდვის პრინციპი მოითხოვს პერსონალური მონაცემების დამუშავებას კონკრეტული, კარგად განსაზღვრული მიზნებით და მხოლოდ თავდაპირველი მიზნის შესაბამისი დამატებითი ამოცანებით.[288] ამრიგად, პერსონალურ მონაცემთა დამუშავება განუსაზღვრელი და/ან შეუზღუდავი ვადით არის კანონდარღვევა. კანონს ასევე არღვევს პერსონალურ მონაცემთა დამუშავება კონკრეტული მიზნის გარეშე, მხოლოდ იმ გათვლით, რომ ეს მონაცემები შესაძლოა სასარგებლო აღმოჩნდეს მომავალში. დამუშავების კანონიერება დამოკიდებულია მის მიზანზე, რომელიც უნდა იყოს მკაფიო, კონკრეტული და კანონის შესაბამისი.

მონაცემთა დამუშავების ნებისმიერ ახალ მიზანს, რომელიც თავდაპირველ ამოცანას არ შეესაბამება, უნდა ჰქონდეს სამართლებრივი საფუძველი. იგი ვერ დაეყრდნობა იმ ფაქტს, რომ მონაცემთა მიღება-დამუშავება თავდაპირველად მოხდა სხვა კანონიერი მიზნის საფუძველზე. კანონიერი დამუშავება, თავის მხრივ, შემოიფარგლება მხოლოდ საწყისი მიზნით და ნებისმიერი ახალი ამოცანა საჭიროებს ცალკე სამართლებრივ საფუძველს. მაგალითად, პერსონალურ მონაცემთა მესამე პირისათვის გამჟღავნება ახალი მიზნებით გულდასმით უნდა განიხილონ, რადგან ასეთი გამჟღავნება შეიძლება საჭიროებდეს დამატებით სამართლებრივ საფუძველს, რომელიც მონაცემთა შეგროვების საფუძვლისგან განსხვავდება.

მაგალითი: ავიაკომპანია მგზავრებისგან აგროვებს მონაცემებს, ადგილების დაჯავშნისა და რეისების სათანადოდ ოპერირების მიზნით. ამისათვის, ავიაკომპანიას ესაჭიროება შემდეგი ინფორმაცია: მგზავრის ადგილის ნომერი, ინფორმაცია ფიზიკური შეზღუდვის შესახებ (მაგ.: სავარძლის საჭიროება), ან საკვებთან დაკავშირებული საჭიროებები („ქოშერი“ ან „ჰალალი“). თუ ავიაკომპანიას სთხოვენ, რომ მგზავრთა პირა-

287 29-ე მუხლის სამუშაო ჯგუფი (2013), *Opinion 3/2013 on purpose limitation,* WP 203, 2013 წლის 2 აპრილი.

288 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5(1)(ბ).

დი მონაცემები (PNR) დაშვების პუნქტში გადასცეს საიმიგრაციო უწყებას, მათ გამოიყენებენ იმიგრაციის კონტროლის მიზნებითაც, რაც მონაცემთა შეგროვების თავდაპირველი ამოცანისგან განსხვავდება. შესაბამისად, ამ მონაცემთა გადაცემა საიმიგრაციო უწყებისთვის საჭიროებს ახალ და დამოუკიდებელ სამართლებრივ საფუძველს.

კონკრეტული მიზნის მასშტაბებისა და შეზღუდვების განხილვისას, მოდერნიზებული 108-ე კონვენცია და მონაცემთა დაცვის ზოგადი რეგულაცია ეყრდნობა თავსებადობის კონცეფციას: მონაცემთა გამოყენება თავსებადი მიზნებისთვის დაშვებულია თავდაპირველ სამართლებრივ საფუძველზე მითითებით. შესაბამისად, მონაცემთა შემდგომი დამუშავება დაუშვებელია მონაცემთა სუბიექტისათვის მოულოდნელი და შეუსაბამო ფორმით.[289] მონაცემთა შემდგომი დამუშავების თავდაპირველ მიზანთან თავსებადობის შესაფასებლად, დამმუშავებელმა უნდა გაითვალისწინოს გარკვეული საკითხები, მათ შორის:

- „ნებისმიერი კავშირი თავდაპირველ და შემდგომი დამუშავების მიზნებს შორის;
- პერსონალურ მონაცემთა შეგროვების კონტექსტი, კერძოდ, მონაცემთა სუბიექტების გონივრული მოლოდინები მონაცემთა შემდგომ გამოყენებასთან დაკავშირებით, რომელიც ეფუძნება მათ ურთიერთობას დამმუშავებელთან;
- პერსონალურ მონაცემთა ბუნება;
- მონაცემთა შემდგომი დამუშავების შესაძლო შედეგები;
- უსაფრთხოების შესაბამისი ზომების არსებობა დამუშავების საწყისი და შემდგომი ოპერაციების დროს“ [290] (მაგ.: დაშიფვრა ან ფსევდონიმიზაცია).

მაგალითი: კომპანია Sunshine-მა მომხმარებლებზე მონაცემები მოიპოვა მათთან ურთიერთობების მართვის (CRM) პროცესში. შემდგომ, ეს მონაცემები გადასცა კომპანია Moonlight-ს, რომელიც პირდაპირ მარკეტინგს ეწევა. ამ უკანასკნელს სურს მონაცემების გამოყენება მესამე კომპანიების მარკეტინგული მიზნებისთვის. Sunshine-ის მიერ მონაცემთა სხვა კომპანიებისთვის გადაცემა მარკეტინგული მიზნებით არის მონაცემთა გამოყენება ახალი ამოცანისთვის, რაც შეუთავსებელია Sunshine-ის მიერ მონაცემთა შეგროვების თავდაპირველ მიზანთან (CRM). ამრიგად,

289 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 49.

290 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლები 50 და 6 (4); მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 49.

Moonlight-ისათვის მონაცემთა კანონიერი გადაცემა საჭიროებს ახალ სამართლებრივ საფუძველს.

მეორე მხრივ, Sunshine-ის მიერ CRM მონაცემთა გამოყენება მარკეტინგული მიზნებით - მომხმარებლებისთვის საკუთარ პროდუქტებზე შეტყობინებათა გასაგზავნად - როგორც წესი, თავსებადი მიზანია.

მონაცემთა დაცვის ზოგადი რეგულაციისა და მოდერნიზებული 108-ე კონვენციის თანახმად, „მონაცემთა შემდგომი დამუშავება საჯარო ინტერესისათვის დაარქივების, სამეცნიერო/ისტორიული კვლევის ან სტატისტიკური მიზნებით,“ *a priori* ჩაითვლება თავსებადად თავდაპირველ მიზანთან.[291] ამავდროულად, პერსონალურ მონაცემთა შედგომი დამუშავებისათვის უნდა დაინერგოს უსაფრთხოების სათანადო ზომები, როგორიცაა მონაცემთა ანონიმიზაცია, დაშიფვრა ან ფსევდონიმიზაცია.[292] მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, „როცა მონაცემთა სუბიექტი ეთანხმება დამუშავებას ან დამუშავება ეფუძნება ევროკავშირისა თუ წევრი სახელმწიფოს კანონს, რომელიც საჯარო ინტერესის შესაბამისი მნიშვნელოვანი მიზნების დაცვის მექანიზმია დემოკრატიულ საზოგადოებაში, დამმუშავებელს უნდა შეეძლოს პერსონალურ მონაცემთა დამუშავება მიზნების შესაბამისობის გაუთვალისწინებლად.“[293] შემდგომი დამუშავებისას, საჭიროა მონაცემთა სუბიექტის ინფორმირება დამუშავების მიზნებსა და მის უფლებებზე, როგორიცაა მონაცემთა დამუშავების შეწყვეტის მოთხოვნა. [294]

მაგალითი: კომპანია Sunshine-მა შეაგროვა და CRM-ში შეინახა საკუთარი კლიენტების მონაცემები. მათი შემდგომი გამოყენება კლიენტთა მსყიდველობითი ქცევის სტატისტიკური ანალიზის მიზნით, კომპანიისთვის ნებადართულია, ვინაიდან სტატისტიკა თავსებადი მიზანია. დამატებითი სამართლებრივი საფუძველი, როგორიცაა მონაცემთა სუბიექტების თანხმობა, საჭირო არ არის. თუმცა, პერსონალურ მონაცემთა სტატისტიკური მიზნებით დასამუშავებლად, კომპანიამ უნდა დანერგოს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დაცვის სათანადო მექანიზმები. Sunshine-ის მიერ განსახორციელებელი ტექნიკური და ორგანიზაციული ღონისძიებები შეიძლება მოიცავდეს ფსევდონიმიზაციას.

291 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (b); მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (ბ); ასეთი ეროვნული კანონმდებლობის მაგალითია ავსტრიის მონაცემთა დაცვის აქტი *(Datenschutzgesetz)*, Federal Law Gazette I No. 165/1999, პუნქტი 46.

292 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (4); მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (ბ); მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 50.

293 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 50.

294 *იქვე.*

3.3 მონაცემთა მინიმიზაციის პრინციპი

ძირითადი საკითხები

- მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც საჭიროა ლეგიტიმური მიზნის მისაღწევად.
- პერსონალურ მონაცემები უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, როდესაც დამუშავების მიზნის მიღწევა, გონივრულობის ფარგლებში, შეუძლებელია სხვა საშუალებებით.
- მონაცემთა დამუშავება არ უნდა იყოს არაპროპორციული ჩარევა კონკრეტულ ინტერესებში, უფლებებსა და თავისუფლებებში.

უნდა დამუშავდეს მხოლოდ ისეთი მონაცემები, რომლებიც „შესაბამისი და რელევანტურია, მოცულობა კი არ აჭარბებდეს მიზანს, რისთვისაც ისინი შეგროვდა და/ან დამუშავდა.“ [295] დამუშავებისთვის შერჩეულ მონაცემთა კატეგორიები საჭირო უნდა იყოს დამუშავების ოპერაციების გაცხადებული მიზნის მისაღწევად, ხოლო დამმუშავებელი მკაცრად შეიზღუდოს მხოლოდ იმ მონაცემთა შეგროვებით, რომლებიც პირდაპირ შეესაბამება კონკრეტულ მიზანს.

მაგალითი: საქმეში *Digital Rights Ireland* case[296] CJEU-მ იმსჯელა მონაცემთა შენახვის დირექტივის კანონიერებაზე. დირექტივა მიზნად ისახავდა შიდასახელმწიფოებრივი დებულებების ჰარმონიზებას ისეთი პერსონალური მონაცემების შენახვასთან დაკავშირებით, რომლებიც მოპოვებული და დამუშავებულია საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო სერვისების ან ქსელების საშუალებით და ითვალისწინებს მათ გადაცემას უფლებამოსილი უწყებისთვის, კერძოდ, ორგანიზებულ დანაშაულსა და ტერორიზმთან საბრძოლველად. მართალია, ეს მიზანი ნამდვილად აკმაყოფილებს საჯარო ინტერესის ამოცანას, მაგრამ სასამართლომ პრობლემურად მიიჩნია ის, რომ დირექტივა განზოგადებულად მოიცავდა „ყველა პირსა და ელექტრონული კომუნიკაციის საშუალებას, ასევე, გადაადგილების განმსაზღვრელ მონაცემებს, ყოველგვარი განსხვავების, შეზღუდვისა თუ გამონაკლისის გარეშე, მძიმე დანაშაულთან ბრძოლის მიზნის გათვალისწინებით.“[297]

295 მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (გ); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (გ).

296 CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი.

297 *იქვე,* პუნქტები 44 და 57.

ამასთან, პირადი ცხოვრების დაცვის გასაუმჯობესებელი სპეციალური ტექნოლოგიის გამოყენება შესაძლებელს ხდის, რომ ზოგჯერ პერსონალური მონაცემები საერთოდ არ გამოიყენონ, ან გამოიყენონ მხოლოდ ის ზომები, რომლებიც ამცირებს მათი დაკავშირების შესაძლებლობას მონაცემთა სუბიექტთან (მაგ.: ფსევდონიმიზაცია). შედეგად, ვიღებთ პრობლემის გადაჭრის გზას, რომელიც პირად ცხოვრებას არ ზღუდავს. ეს განსაკუთრებით საჭიროა მონაცემთა დაცვის ფართომასშტაბიან სისტემებში.

მაგალითი: ქალაქის მერია საზოგადოებრივი ტრანსპორტის რეგულარულ მომხმარებლებს გარკვეული საფასურის სანაცვლოდ სთავაზობს ჩიპიან ბარათებს. ბარათი შეიცავს მომხმარებლის სახელს, როგორც წერილობითი (მის ზედაპირზე), ისე ელექტრონული (ჩიპში) ფორმით. ავტობუსით ან ტრამვაით მგზავრობისას მომხმარებელმა ბარათი წამკითხველ მოწყობილობას უნდა მიუახლოოს. შედეგად, წაკითხული მონაცემები ელექტრონულად გადამოწმდება სამგზავრო ბარათის მფლობელთა სახელებისა და გვარების ბაზაში.

ამ შემთხვევაში ოპტიმალურად არ არის დაცული მონაცემთა მინიმიზაციის პრინციპი. კერძოდ, შემოწმება იმისა, დაიშვება თუ არა კონკრეტული პირი სატრანსპორტო საშუალებაში, შესაძლებელია ბარათის ჩიპში მოთავსებული პერსონალური მონაცემების სპეციალურ ბაზასთან შედარების გარეშე. მაგალითად, ამისთვის საკმარისია, ბარათის ჩიპი შეიცავდეს სპეციალურ ელექტრონულ გამოსახულებას, როგორიცაა შტრიხკოდი, რომელიც, წამკითხველ მოწყობილობასთან მიახლოების შემდეგ, დაადასტურებს, ბარათი მოქმედია თუ არა. ასეთ სისტემაში არ აღირიცხება, თუ ვინ და როდის იყენებს კონკრეტულ სატრანსპორტო საშუალებას. ეს იქნება ოპტიმალური გადაწყვეტა მინიმიზაციის პრინციპის გათვალისწინებით, რომელიც ადგენს მონაცემთა შეგროვების მინიმიზაციის ვალდებულებას.

მოდერნიზებული 108-ე კონვენციის მე-5 მუხლის პირველი პუნქტი შეიცავს მოთხოვნას პროპორციულობის შესახებ. კერძოდ, პერსონალურ მონაცემთა დამუშავება უნდა იყოს იმ ლეგიტიმური მიზნის პროპორციული, რომელსაც ემსახურება დამუშავება. მონაცემთა დამუშავების ყველა ეტაპზე უნდა არსებობდეს სამართლიანი წონასწორობა ყველა შესაბამის ინტერესს შორის. ეს ნიშნავს, რომ „პერსონალური მონაცემები, რომლებიც შესაბამისი და რელევანტურია, მაგრამ მოიცავს არაპროპორციულ ჩარევას სასწორზე დადებულ ფუნდამენტურ უფლებებსა და თავისუფლებებში, გადაჭარბებულად უნდა ჩაითვალოს.“ [298]

298 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 52; მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (გ).

3.4 მონაცემთა სიზუსტის პრინციპი

ძირითადი საკითხები

- მონაცემთა დამმუშავებელი ვალდებულია, მონაცემთა სიზუსტის პრინციპი დანერგოს დამუშავების ყველა ოპერაციაში.
- არაზუსტი მონაცემები უნდა წაიშალოს, ან დაუყოვნებლივ გასწორდეს.
- შესაძლებელია, საჭირო გახდეს მონაცემთა რეგულარული შემოწმება და განახლება, სიზუსტის დასაცავად.

მონაცემთა დამმუშავებელმა, რომელიც პერსონალურ მონაცემებს ინახავს, არ უნდა გამოიყენოს ინფორმაცია იმ ნაბიჯების გადადგმამდე, რომლებიც გონივრული სიცხადით უზრუნველყოფს მონაცემთა სიზუსტესა და განახლებას. [299]

მონაცემთა სიზუსტის უზრუნველყოფის მოვალეობა უნდა აღვიქვათ მონაცემთა დამუშავების მიზნის კონტექსტში.

მაგალითი: *Rijkeboer*-ის[300] საქმეში CJEU-მ განიხილა ნიდერლანდების სამეფოს მოქალაქის მიმართვა ქ. ამსტერდამის ადგილობრივი ადმინისტრაციიდან ინფორმაციის მიღების თაობაზე. კერძოდ, იგი ითხოვდა იმ პირთა ვინაობის გამხელას, რომელთაც ადგილობრივმა ხელისუფლებამ გასული ორი წლის მანძილზე გადასცა მის შესახებ არსებული ჩანაწერები. განმცხადებელი ითხოვდა ინფორმაციას გადაცემული მონაცემების შინაარსზეც. CJEU-მ განაცხადა, რომ „პირადი ცხოვრების უფლება გულისხმობს მონაცემთა სუბიექტის უფლებას, დარწმუნდეს, რომ მის პერსონალური მონაცემები მუშავდება ზუსტად და კანონის შესაბამისად. კერძოდ, მონაცემთა სუბიექტს შეუძლია იცოდეს, რომ მის შესახებ არსებული ძირითადი მონაცემები სწორია და გადაეცა ავტორიზებულ [მონაცემთა] მიმღებს.“ CJEU-მ მიუთითა მონაცემთა დაცვის დირექტივის პრეამბულაზე, სადაც აღნიშნულია, რომ მონაცემთა სუბიექტს უნდა ჰქონდეს მის პერსონალურ მონაცემებზე წვდომის უფლება, რათა შეძლოს ამ მონაცემთა სიზუსტის შემოწმება. [301]

299 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (ფ); მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (ფ).

300 CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 2009 წლის 7 მაისი.

301 დირექტივა 95/46/EC, პრეამბულა, მუხლი 41.

ზოგ შემთხვევაში, კანონმდებლობა კრძალავს შენახული მონაცემების განახლებას, რადგან შენახვის მიზანი, ძირითადად, არის მოვლენათა დოკუმენტირება, ისტორიული „მომენტალური კადრების“ (snapshot) სახით.

მაგალითი: დაუშვებელია ოპერაციის შესახებ სამედიცინო ჩანაწერში ცვლილების შეტანა ანუ „განახლება“, იმ შემთხვევაშიც კი, თუ თავდაპირველად მითითებული შედეგები შემდგომ არასწორი აღმოჩნდება. ასეთ ვითარებაში, ჩანაწერში შესაძლებელია მხოლოდ შენიშვნების შეტანა, რომლებიც მკაფიოდ უნდა იყოს მონიშნული, როგორც მოგვიანებით შეტანილი ინფორმაცია.

მეორე მხრივ, ზოგიერთ სიტუაციაში არსებობს მონაცემთა განახლებისა და სიზუსტის შემოწმების აბსოლუტური საჭიროება, იმ პოტენციური ზიანის გამო, რომელიც შეიძლება არაზუსტმა მონაცემებმა მოუტანოს მონაცემთა სუბიექტს.

მაგალითი: თუ პირს სურს საკრედიტო ხელშეკრულების გაფორმება საბანკო დაწესებულებასთან, ბანკი, როგორც წესი, ამოწმებს პერსპექტიული კლიენტის გადახდისუნარიანობას. ამ მიზნით, არსებობს სპეციალური მონაცემთა ბაზა, რომელიც შეიცავს მონაცემებს ფიზიკური პირის საკრედიტო ისტორიის შესახებ. თუ ამ მონაცემთა ბაზაში მითითებულია არასწორი ან მოძველებული მონაცემები კონკრეტული პირის შესახებ, ამან შეიძლება უარყოფითი შედეგები მოუტანოს მას. ასეთი მონაცემთა ბაზის დამმუშავებელმა განსაკუთრებული ძალისხმევა უნდა გაწიოს სიზუსტის პრინციპის დასაცავად.

3.5 შენახვის ვადის შეზღუდვის პრინციპი

ძირითადი საკითხები

- შენახვის ვადის შეზღუდვის პრინციპი გულისხმობს, რომ პერსონალური მონაცემები უნდა წაიშალოს, ან მოხდეს მათი ანონიმიზაცია, როგორც კი აღარ იქნება საჭირო იმ მიზნებისთვის, რომლებისთვისაც შეგროვდა.

GDPR-ის მე-5 მუხლის 1(ე) და მოდერნიზებული 108-ე კონვენციის მე-5 მუხლის 4(ე) პუნქტების თანახმად, პერსონალური მონაცემები „უნდა შეინახონ ისეთი ფორმით, რომელიც იძლევა მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობას არაუმეტეს იმ დროით, რომელიც აუცილებელია

მონაცემთა დამუშავების მიზნებისთვის.“ შესაბამისად, აღნიშნული მიზნების მიღწევისთანავე საჭიროა მონაცემთა წაშლა ან ანონიმიზება. ამისათვის „მონაცემთა დამმუშავებელმა უნდა განსაზღვროს ვადა, რომლის გასვლის შემდეგაც მონაცემები წაიშლება ან პერიოდულად გადაიხედება“, რათა ისინი არ შეინახონ იმაზე მეტი დროით, ვიდრე საჭიროა.[302]

S. and Marper-ის საქმეში ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ ევროპის საბჭოს შესაბამისი ინსტრუმენტების ძირითადი პრინციპები, ხელშემკვრელ მხარეთა კანონმდებლობა და პრაქტიკა მოითხოვდა მონაცემთა შენახვას შეგროვების მიზნის პროპორციულად და შეზღუდული ვადით, განსაკუთრებით, პოლიციის სექტორში.[303]

> მაგალითი: საქმეში *S. and Marper*[304] ECtHR-მა დაადგინა, რომ განმცხადებელთა თითის ანაბეჭდების, უჯრედული ნიმუშებისა და დნმ-ის პროფილების განუსაზღვრელი ვადით შენახვა იყო არაპროპორციული და არასაჭირო დემოკრატიულ საზოგადოებაში, იმის გათვალისწინებით, რომ ორივე განმცხადებლის მიმართ სისხლისსამართლებრივი დევნა აღარ გაგრძელდა - ერთი გამართლდა, ხოლო მეორის მიმართ წარმოებული საქმე შეწყდა.

პერსონალურ მონაცემთა შენახვის ვადაზე დაწესებული შეზღუდვა ეხება მხოლოდ იმ ფორმით შენახულ მონაცემებს, რომელიც იძლევა მონაცემთა სუბიექტების იდენტიფიკაციის საშუალებას. ამრიგად, იმ მონაცემთა კანონიერი შენახვა, რომელიც საჭირო აღარ არის, მიიღწევა მონაცემთა ანონიმიზაციით.

მონაცემთა დაარქივება საჯარო ინტერესის, ასევე, სამეცნიერო/ისტორიული ან სტატისტიკური მიზნებით, შესაძლებელია უფრო ხანგრძლივადაც, თუკი ამ მონაცემებს გამოიყენებენ მხოლოდ დასახელებული მიზნებისთვის.[305] სათანადო ტექნიკური და ორგანიზაციული ღონისძიებები უნდა გატარდეს პერსონალურ მონაცემთა მიმდინარე შენახვისა და გამოყენებისთვის, რათა დაცული იყოს მონაცემთა სუბიექტების უფლებები და თავისუფლებები.

მოდერნიზებული 108-ე კონვენცია ითვალისწინებს გარკვეულ გამონაკლის შემთხვევებსაც შენახვის ვადის შეზღუდვასთან დაკავშირებით. კერძოდ, გა-

---

302 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 39.

303 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 და 30566/04, 2008 წლის 4 დეკემბერი; ასევე, ECtHR, *M.M. v. the United Kingdom,* No. 24029/07, 2012 წლის 13 ნოემბერი.

304 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 და 30566/04, 2008 წლის 4 დეკემბერი.

305 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (ე); მოდერნიზებული 108-ე კონვენცია, მუხლები 5 (4) (ბ) და 11 (2).

მონაკლისი უნდა იყოს კანონმდებლობით გათვალისწინებული, გარკვეული კანონიერი მიზნების მისაღწევად საჭირო და პროპორციული, და მოიცავდეს ფუნდამენტურ უფლებებსა და თავისუფლებებს.[306] კანონიერი მიზნებია: ეროვნული უსაფრთხოების დაცვა, სისხლის სამართლის დანაშაულების გამოძიება და დამნაშავეთა დასჯა, სისხლის სამართლით გათვალისწინებული სასჯელის აღსრულება, მონაცემთა სუბიექტის დაცვა, სხვათა ფუნდამენტური უფლებებისა და თავისუფლებების პატივისცემა და სხვა.

მაგალითი: საქმეში *Digital Rights Ireland*[307] CJEU-მ იმსჯელა მონაცემთა შენახვის დირექტივის კანონიერებაზე. დირექტივა მიზნად ისახავდა შიდასახელმწიფოებრივი დებულებების ჰარმონიზებას ისეთი პერსონალური მონაცემების შენახვასთან დაკავშირებით, რომლებიც მოპოვებული და დამუშავებულია საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო სერვისების ან ქსელების საშუალებით და შეიძლება გადაეცეს უფლებამოსილ უწყებას ორგანიზებულ დანაშაულსა და ტერორიზმთან ბრძოლის მიზნებით. მონაცემთა დაცვის დირექტივა ადგენდა მონაცემთა შენახვას, „სულ მცირე, 6 თვის [ვადით], ისე, რომ არ განარჩევდა ამავე დირექტივის მე-5 მუხლით გათვალისწინებულ მონაცემთა კატეგორიებს იმის მიხედვით, თუ რამდენად გამოსადეგი იყო დასახული მიზნის მისაღწევად ან რომელ პირებს მიემართებოდა.“ [308] CJEU შეეხო მონაცემთა შენახვის დირექტივაში ობიექტურ კრიტერიუმთა არარსებობასაც, რომელთა საფუძველზეც უნდა განისაზღვროს მონაცემთა შენახვის ზუსტი პერიოდი - მინიმალური 6 თვიდან მაქსიმალურ 24 თვემდე - რაც ზღუდავს ამ პერიოდს მკაცრად საჭირო ვადით.[309]

3.6 მონაცემთა უსაფრთხოების პრინციპი

ძირითადი საკითხები

- პერსონალურ მონაცემთა უსაფრთხოებასა და კონფიდენციალობას უდიდესი მნიშვნელობა ენიჭება მონაცემთა სუბიექტებზე უარყოფითი გავლენის თავიდან ასაცილებლად.

306 მოდერნიზებული 108-ე კონვენცია, მუხლი 11.1; მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტები 91–98.

307 CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი.

308 *იქვე,* პუნქტი 63.

309 *იქვე,* პუნქტი 64.

- უსაფრთხოების ზომები შეიძლება იყოს ტექნიკური და/ან ორგანიზაციული.
- ფსევდონიმიზაცია არის პროცესი, რომელსაც შეუძლია პერსონალური მონაცემების დაცვა.
- უსაფრთხოების ზომის შესაბამისობა უნდა განისაზღვროს თითოეულ შემთხვევაში და რეგულარულად გადაიხედოს.

მონაცემთა უსაფრთხოების პრინციპი მოითხოვს სათანადო ტექნიკური ან ორგანიზაციული ღონისძიებების გატარებას პერსონალურ მონაცემთა დამუშავების პროცესში, რათა ისინი დაცული იყოს შემთხვევითი, არაავტორიზებული ან უკანონო წვდომის, გამოყენების, შეცვლის, გამჟღავნების, განადგურების ან დაზიანებისაგან. [310] GDPR-ის თანახმად, მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა ეს ღონისძიებები უნდა გაატარონ ისეთი საკითხების გათვალისწინებით, როგორიცაა „უახლესი ტექნოლოგიები, განხორციელების ხარჯები, დამუშავების ბუნება, მოცულობა, კონტექსტი და მიზნები, ასევე, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების სავარაუდო რისკები“.[311] საქმის კონკრეტული გარემოებებიდან გამომდინარე, სათანადო ტექნიკური და ორგანიზაციული ზომები შეიძლება მოიცავდეს პერსონალურ მონაცემთა ფსევდონიმიზაციასა და დაშიფვრას და/ან ღონისძიებათა ეფექტიანობის რეგულარულ ტესტირებასა და შეფასებას მონაცემთა დამუშავების უსაფრთხოებისათვის. [312]

როგორც ეს 2.1.1 ნაწილშია განმარტებული, მონაცემთა ფსევდონიმიზაცია გულისხმობს პერსონალურ მონაცემებში იმ მახასიათებელთა ჩანაცვლებას ფსევდონიმით, რომლებიც მონაცემთა სუბიექტის იდენტიფიცირების საშუალებას იძლევა, და მათ შენახვას ცალკე, ტექნიკური ან ორგანიზაციული ზომების მეშვეობით. ფსევდონიმიზაციის პროცესი განსხვავდება ანონიმიზაციისგან, სადაც პირის იდენტიფიცირებისათვის საჭირო ნებისმიერ ინფორმაციასთან კავშირი გაწყვეტილია.

მაგალითი: წინადადება - „ჩარლზ სპენსერი, დაბადებული 1967 წლის 3 აპრილს, არის ოთხი შვილის, ორი გოგოს და ორი ბიჭის მამა“ - შეიძლება შემდეგნაირად იყოს ფსევდონიმიზებული:

„ჩ.ს. 1967 არის ოთხი შვილის, ორი გოგოს და ორი ბიჭის მამა“; ან

310 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლები 39 და 5(1) (ვ); მოდერნიზებული 108-ე კონვენცია, მუხლი 7.

311 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 32 (1).

312 *იქვე.*

„324 არის ოთხი შვილის, ორი გოგოს და ორი ბიჭის მამა“; ან

„YESz320I არის ოთხი შვილის, ორი გოგოს და ორი ბიჭის მამა.“

მომხმარებელი, რომელსაც ფსევდონიმიზებულ მონაცემებზე აქვს წვდომა, ვერ შეძლებს „ჩარლზ სპენსერი, დაბადებული 1967 წლის 3 აპრილს“, დაუკავშიროს 324-ს ან YESz3201-ს. შესაბამისად, ასეთი მონაცემები დაცულია ბოროტად გამოყენებისგან.

თუმცა, პირველი მაგალითი ნაკლებად უსაფრთხოა. თუ ჩარლზ სპენსერი პატარა სოფელში ცხოვრობს, მის ვინაობას შეიძლება ადვილად მიხვდნენ წინადადებიდან „ჩ.ს. 1967 არის ოთხი შვილის, ორი გოგოს და ორი ბიჭის მამა“. ფსევდონიმიზაციის მეთოდმა შეიძლება გავლენა მოახდინოს მონაცემთა დაცვის ეფექტიანობაზე.

პიროვნების ვინაობის გასაიდუმლოების მიზნით, ხშირად მიმართავენ მახასიათებელთა დაშიფვრას, ან მათ ცალკე ინახავენ. ეს განსაკუთრებით სასარგებლო მეთოდია, თუ მონაცემთა დამმუშავებლებს სურთ, დარწმუნდნენ, რომ ერთსა და იმავე მონაცემთა სუბიექტებზე მუშაობენ, მაგრამ არ ესაჭიროებათ ან არ შეუძლიათ, მოითხოვონ მონაცემთა სუბიექტების რეალური ვინაობა (მაგ.: მკვლევარი შეისწავლის დაავადების მიმდინარეობას პაციენტებში, რომელთა ვინაობაც მხოლოდ იმ საავადმყოფოსთვის არის ცნობილი, სადაც მათ მკურნალობენ და საიდანაც მკვლევარები ფსევდონიმიზებულ სამედიცინო ისტორიებს იღებენ). ამრიგად, ფსევდონიმიზაცია იმ ტექნოლოგიის მნიშვნელოვანი ინსტრუმენტია, რომელიც პირადი ცხოვრების ხელშეუხებლობის დასაცავად გამოიყენება. იგი არსებით როლს ასრულებს მონაცემთა დაცვის სტანდარტების გათვალისწინებაში ახალი პროდუქტის ან მომსახურების შექმნისას (privacy by design). ეს გულისხმობს მონაცემთა დაცვის დანერგვას მათი დამუშავების სისტემებში.

GDPR-ის 25-ე მუხლი, რომელიც შეეხება მონაცემთა დაცვის სტანდარტების გათვალისწინებას ახალი პროდუქტის ან მომსახურების შექმნისას, ცალსახად მიუთითებს ფსევდონიმიზაციაზე, როგორც შესაბამისი ტექნიკური და ორგანიზაციული ღონისძიების მაგალითზე, რომელიც მონაცემთა დამმუშავებელმა უნდა გაატაროს დაცვის პრინციპების შესრულებისა და საჭირო მექანიზმების ინტეგრირებისათვის.

დამტკიცებული ქცევის კოდექსის დაცვა ან სერტიფიცირების მექანიზმის გამოყენება ხელს შეუწყობს დამუშავების უსაფრთხოების მოთხოვნის შესრულებას.[313] მგზავრთა პირადი მონაცემების (PNR) დამუშავებაზე მონაცემთა

313 *იქვე*, მუხლი 32 (3).

დაცვის გავლენის შესახებ ევროპის საბჭოს მოსაზრებაში წარმოდგენილია უსაფრთხოების სათანადო ზომების სხვა მაგალითები, რომლებიც გამოიყენება პერსონალურ მონაცემთა დასაცავად PNR სისტემებში. ესენია: მონაცემთა უსაფრთხო ფიზიკურ გარემოში შენახვა; წვდომის შეზღუდვა მონაცემთა ბაზაში შესვლის მრავალდონიანი სისტემის გამოყენებით; და მონაცემთა გადაცემის დაცვა მყარი კრიპტოგრაფიით. [314]

მაგალითი: სოციალური ქსელები და ელფოსტის პროვაიდერები მომხმარებლებს სთავაზობენ მონაცემთა დამატებითი უსაფრთხოების გამოყენებას, ნამდვილობის დადგენის (authentification) ორდონიანი მექანიზმის მეშვეობით. ამასთან, პირად გვერდზე შესასვლელად მომხმარებლებს პაროლთან ერთად სჭირდებათ მეორე ავტორიზაციის გავლაც. ეს შეიძლება იყოს უსაფრთხოების კოდის შეყვანა, რომელიც პირად გვერდთან დაკავშირებულ მობილური ტელეფონის ნომერზე ეგზავნებათ. ამრიგად, ორეტაპიანი ვერიფიკაცია პერსონალურ ინფორმაციას უკეთ იცავს არაავტორიზებული წვდომისაგან (მაგ.: ჰაკერული შეღწევის გზით).

მოდერნიზებული 108-ე კონვენციის განმარტებით ბარათში წარმოდგენილია დაცვის სათანადო მექანიზმების სხვა მაგალითები, როგორიცაა პროფესიული საიდუმლოების დაცვის ვალდებულების დანერგვა ან ტექნიკური უსაფრთხოების კვალიფიციური ზომების მიღება (მაგ.: მონაცემთა დაშიფვრა).[315] უსაფრთხოების კონკრეტული ზომის დანერგვისას, მონაცემთა დამმუშავებელმა ან უფლებამოსილმა პირმა უნდა გაითვალისწინოს რამდენიმე ელემენტი, როგორიცაა დამუშავებული პერსონალური მონაცემების ბუნება და მოცულობა, მონაცემთა დამუშავების შესაძლო უარყოფითი გავლენა მონაცემთა სუბიექტებზე, და მონაცემთა შეზღუდული წვდომის საჭიროება. [316] უსაფრთხოების სათანადო ზომების დანერგვის პროცესში გასათვალისწინებელია მონაცემთა უსაფრთხოების თანამედროვე მეთოდები და ტექნოლოგიებიც. ასეთი ზომების ღირებულება უნდა იყოს შესაძლო რისკების სერიოზულობისა და ალბათობის პროპორციული. უსაფრთხოების ზომების საჭიროებისამებრ განახლებისათვის, აუცილებელია მათი რეგულარული გადახედვა.[317]

მოდერნიზებული 108-ე კონვენციაც და GDPR-იც მონაცემთა დამმუშავებელს უწესებს მოთხოვნას, რომ უფლებამოსილ საზედამხედველო ორგანოს შეა-

314 ევროპის საბჭო, 108-ე კონვენციის კომიტეტის მოსაზრება, მგზავრთა პირადი მონაცემების დამუშავების გავლენა მონაცემთა დაცვაზე, T-PD(2016)18rev, 2016 წლის 19 აგვისტო, გვ. 9.

315 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 56.

316 *იქვე,* პუნქტი 62.

317 *იქვე,* პუნქტი 63.

ტყობინოს მონაცემთა უსაფრთხოების ისეთი დარღვევის შესახებ, რომელმაც შეიძლება შელახოს ფიზიკურ პირთა უფლებები და თავისუფლებები.[318] შეტყობინების ვალდებულება დაწესებულია მონაცემთა სუბიექტთან დაკავშირებითაც, თუკი პერსონალურ მონაცემთა უსაფრთხოების დარღვევა, სავარაუდოდ, მაღალ რისკს შეუქმნის მის უფლებებსა და თავისუფლებებს.[319] ამ ტიპის კომუნიკაცია უნდა განხორციელდეს გასაგები და მარტივი ენით.[320] პერსონალურ მონაცემთა დარღვევის შესახებ უფლებამოსილმა პირმა დაუყოვნებლივ უნდა შეატყობინოს მონაცემთა დამმუშავებელს.[321] ამ მხრივ, დაშვებულია გამონაკლისი შემთხვევებიც. მაგალითად: მონაცემთა დამმუშავებელი არ არის ვალდებული, საზედამხედველო ორგანოს შეატყობინოს მონაცემთა უსაფრთხოების დარღვევა, თუ „ნაკლებ სავარაუდოა, რომ ის შელახავს ფიზიკურ პირთა უფლებებსა და თავისუფლებებს.“[322] მონაცემთა სუბიექტთან მიმართებით, შეტყობინების ვალდებულება არ დგება იმ შემთხვევაში, თუ გატარებული უსაფრთხოების ზომების შედეგად პერსონალური მონაცემები მიუწვდომელი/გაუგებარია ნებისმიერი არაუფლებამოსილი პირისათვის, ან სათანადო დამატებითი ზომები, დიდი ალბათობით, გამორიცხავს სუბიექტის უფლებებისა და თავისუფლებების შელახვის მაღალ რისკს.[323] თუ მონაცემთა სუბიექტისათვის უსაფრთხოების დარღვევაზე ინფორმაციის მიწოდება არაპროპორციულ ძალისხმევას მოითხოვს დამმუშავებლის მხრიდან, ინფორმაცია უნდა გავრცელდეს საჯაროდ, ან მსგავსი ფორმით, რომლითაც „მონაცემთა ყველა სუბიექტი ინფორმაციას თანაბრად ეფექტიანად მიიღებს.“[324]

3.7 ანგარიშვალდებულების პრინციპი

ძირითადი საკითხები

- ანგარიშვალდებულება მოითხოვს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის მიერ იმ ზომების აქტიურად და მუდმივად გატარებას, რომლებიც ხელს შეუწყობს და განამტკიცებს მონაცემთა დაცვას დამუშავების პროცესში.

318 მოდერნიზებული 108-ე კონვენცია, მუხლი 7 (2); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 33 (1).

319 მოდერნიზებული 108-ე კონვენცია, მუხლი 7 (2); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 34 (1).

320 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 34 (2).

321 *იქვე,* მუხლი 33(1).

322 *იქვე,* მუხლი 32(1).

323 *იქვე,* მუხლი 34 (3)(ა)(ბ).

324 *იქვე,* მუხლი 34 (3)(გ).

- მონაცემთა დამმუშავებელი და უფლებამოსილი პირი პასუხისმგებელნი არიან დამუშავების ოპერაციების შესაბამისობაზე მონაცემთა დაცვის კანონმდებლობასა და საკუთარ ვალდებულებებთან.

- დამმუშავებელმა, მონაცემთა სუბიექტის, საზოგადოებისა და საზედამხედველო ორგანოების წინაშე, ნებისმიერ დროს უნდა შეძლოს მონაცემთა დაცვის დებულებებთან შესაბამისობის დადასტურება. უფლებამოსილმა პირმა უნდა შეასრულოს სხვა გარკვეული ვალდებულებებიც, რომლებიც მკაცრად უკავშირდება ანგარიშვალდებულებას (მაგ.: დამუშავების ოპერაციების აღრიცხვა და მონაცემთა დაცვის ოფიცრის დანიშვნა).

GDPR და მოდერნიზებული 108-ე კონვენცია ადგენს, რომ მონაცემთა დამმუშავებელი პასუხისმგებელია შესაბამისობაზე წინამდებარე თავში აღწერილ მონაცემთა დამუშავების პრინციპებთან.[325] ამ მიზნით, მან სათანადო ტექნიკური და ორგანიზაციული ზომები უნდა გაატაროს.[326] GDPR-ის მე-5 მუხლის მე-2 პუნქტში წარმოდგენილი ანგარიშვალდებულების პრინციპის დაცვა პირდაპირ მხოლოდ მონაცემთა დამმუშავებელს მიემართება, თუმცა ანგარიშვალდებულება მოეთხოვებათ უფლებამოსილ პირებსაც, იმის გათვალისწინებით, რომ მათ გარკვეული ვალდებულებები უნდა შეასრულონ და ანგარიშვალდებულებასთან მჭიდროდ არიან დაკავშირებულნი.

ევროკავშირისა და ევროპის საბჭოს მონაცემთა დაცვის კანონმდებლობა ასევე განსაზღვრავს, რომ მონაცემთა დამმუშავებელი პასუხისმგებელია შესაბამისობაზე 3.1-3.6 ნაწილებში[327] განხილულ მონაცემთა დაცვის პრინციპებთან. 29-ე მუხლის სამუშაო ჯგუფის თანახმად, „პროცედურებისა და მექანიზმების ტიპები დამოკიდებულია დამუშავებით წარმოქმნილ რისკებსა და მონაცემთა ბუნებაზე.“[328]

მონაცემთა დამმუშავებელს მოთხოვნებთან შესაბამისობის მიღწევა შეუძლია სხვადასხვა გზით, კერძოდ:

- დამუშავების ოპერაციების აღრიცხვა და მათი ხელმისაწვდომობა საზედამხედველო ორგანოს მოთხოვნის საფუძველზე;[329]

325 *იქვე*, მუხლი 5 (2); მოდერნიზებული 108-ე კონვენცია, მუხლი 10 (1).

326 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 24.

327 *იქვე*, მუხლი 5 (2); მოდერნიზებული 108-ე კონვენცია, მუხლი 10 (1).

328 29-ე მუხლის სამუშაო ჯგუფი, მოსაზრება 3/2010 ანგარიშვალდებულების პრინციპის შესახებ, WP 173, ბრიუსელი, 2010 წლის 13 ივლისი, პუნქტი 12.

329 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 30.

- გარკვეულ სიტუაციებში, მონაცემთა დაცვის ოფიცრის დანიშვნა, რომელიც ჩართული იქნება პერსონალურ მონაცემთა დაცვის ყველა საკითხში; [330]

- მონაცემთა დაცვის რისკების შეფასება სხვადასხვა ტიპის დამუშავებისათვის, რომლებიც, სავარაუდოდ, საფრთხეს შეუქმნის ფიზიკურ პირთა უფლებებსა და თავისუფლებებს; [331]

- მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (by design) და მონაცემთა დაცვა პირველად პარამეტრად (by default); [332]

- მონაცემთა სუბიექტების უფლებათა განსახორციელებელი საშუალებებისა და პროცედურების დანერგვა; [333]

- დამტკიცებული ქცევის კოდექსისა და სერტიფიცირების მექანიზმების შესრულება. [334]

მართალია, GDPR-ის მე-5 მუხლის მე-2 პუნქტით გათვალისწინებული ანგარიშვალდებულების პრინციპი პირდაპირ არ მიემართება უფლებამოსილ პირს, მაგრამ არსებობს დებულებები, რომლებიც უკავშირდება ანგარიშვალდებულებას და გარკვეულ ვალდებულებებს უდგენს ამ პირს (მაგ.: დამუშავების აქტივობათა აღრიცხვა და მონაცემთა დაცვის ოფიცრის დანიშვნა ნებისმიერი დამუშავებისთვის, რომელიც ამას მოითხოვს).[335] უფლებამოსილმა პირმა უნდა გატაროს მონაცემთა უსაფრთხოების დასაცავად საჭირო ყველა ზომა.[336] იურიდიულად სავალდებულო კონტრაქტი მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის უნდა ადგენდეს უფლებამოსილი პირის ვალდებულებას, დახმარება გაუწიოს დამმუშავებელს გარკვეული მოთხოვნების შესრულებაში (მაგ.: მონაცემთა დაცვის რისკების შეფასება ან, პერსონალურ მონაცემთა უსაფრთხოების დარღვევის აღმოჩენის შემთხვევაში, მონაცემთა დამმუშავებლისათვის შეტყობინება). [337]

---

330 *იქვე,* მუხლები 37–39.

331 *იქვე,* მუხლი 35; მოდერნიზებული 108-ე კონვენცია, მუხლი 10 (2).

332 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 25; მოდერნიზებული 108-ე კონვენცია, მუხლები 10 (2) და (3).

333 *იქვე,* მუხლები 12 და 24.

334 *იქვე,* მუხლები 40 და 42.

335 *იქვე,* მუხლები 5 (2), 30 და 37.

336 *იქვე,* მუხლი 28 (3) (გ).

337 *იქვე,* მუხლი 28 (3) (დ).

ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციამ (OECD) 2013 წელს დაამტკიცა პირადი ცხოვრების ხელშეუხებლობის დაცვის სახელმძღვანელო პრინციპები, სადაც ხაზგასმით არის აღნიშნული, რომ დამმუშავებელი მნიშვნელოვან როლს ასრულებს მონაცემთა დაცვაში. ეს სახელმძღვანელო პრინციპები მოიცავს ანგარიშვალდებულებასაც, ვინაიდან ადგენს, რომ „მონაცემთა დამმუშავებელი ანგარიშვალდებულია, მიიღოს ზომები, რომლებიც აამოქმედებს ზემოაღნიშნულ [მატერიალურ] პრინციპებს.“ [338]

მაგალითი: 2002/58/EC დირექტივაში 2009 წელს შეტანილი შესწორება[339] იმ კანონმდებლობის მაგალითია, სადაც ანგარიშვალდებულების პრინციპი ხაზგასმით არის აღნიშნული. დირექტივის მე-4 მუხლი (შესწორებული ფორმა) ადგენს „უსაფრთხოების პოლიტიკის დანერგვის ვალდებულებას პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით.“ ამრიგად, დირექტივაში უსაფრთხოების დებულებებთან მიმართებით, კანონმდებელმა გადაწყვიტა, რომ საჭირო იყო მკაფიო მოთხოვნის დაწესება შესაბამისი პოლიტიკის შემუშავებასა და დანეგრვაზე.

29-ე მუხლის სამუშაო ჯგუფის მოსაზრებით, [340] ანგარიშვალდებულების არსი განისაზღვრება მონაცემთა დამმუშავებლის მოვალეობით:

- გაატაროს ღონისძიებები, რომლებიც, ჩვეულებრივ პირობებში, უზრუნველყოფს მონაცემთა დაცვის წესების შესრულებას დამუშავების ოპერაციების კონტექსტში; და

- მზად იქონიოს დოკუმენტაცია, რომელიც მონაცემთა სუბიექტებსა და საზედამხედველო ორგანოებს დაუდასტურებს, რომ გატარდა ღონისძიებები მონაცემთა დაცვის წესების შესასრულებლად.

ამრიგად, ანგარიშვალდებულების პრინციპი მონაცემთა დამმუშავებელს ავალდებულებს შესაბამისი წესების შესრულების აქტიურად წარმოჩენას, ნაცვლად იმისა, რომ უბრალოდ დაელოდოს ხარვეზზე მითითებას მონაცემთა სუბიექტების ან საზემდახედველო ორგანოს მხრიდან.

---

338 OECD (2013), სახელმძღვანელო პრინციპები პირადი ცხოვრების დაცვისა და პერსონალურ მონაცემთა საერთაშორისო გადაცემის მართვის შესახებ, მუხლი 14.

339 ევროპული პარლამენტისა და საბჭოს 2009 წლის 25 ნოემბერის დირექტივა 2009/136/EC, რომლითაც შესწორდა დირექტივა 2002/22/EC უნივერსალური მომსახურებებისა და ელექტრონულ საკომუნიკაციო ქსელებსა და მომსახურებებთან დაკავშირებით მომხმარებელთა უფლებების შესახებ; დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ; რეგულაცია (EC) No. 2006/2004, რომელიც შეეხება მომხმარებელთა დაცვის კანონმდებლობის აღსრულებაზე პასუხისმგებელ ეროვნულ უწყებებს შორის თანამშრომლობას, OJ 2009 L 337, გვ. 11.

340 29-ე მუხლის სამუშაო ჯგუფი, მოსაზრება 3/2010 ანგარიშვალდებულების პრინციპის შესახებ, WP 173, ბრიუსელი, 2010 წლის 13 ივლისი.

4

მონაცემთა დაცვის ევროპული სამართლის წესები

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა კანონიერი დამუშავების წესები		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6(1)(ა); CJEU, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 2011; CJEU, C-536/15, *Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*, 2017.	**თანხმობა**	რეკომენდაცია პროფილირების შესახებ, მუხლები 3.4 (ბ) და 3.6; მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (2).
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (1) (ბ)	**(წინა) სახელშეკრულებო ურთიერთობები**	რეკომენდაცია პროფილირების შესახებ, მუხლი 3.4 (ბ)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (1) (გ)	**მონაცემთა დამმუშავებლის სამართლებრივი ვალდებულებები**	რეკომენდაცია პროფილირების შესახებ, მუხლი 3.4 (ა)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (1) (დ)	**მონაცემთა სუბიექტის სასიცოცხლო ინტერესები**	რეკომენდაცია პროფილირების შესახებ, მუხლი 3.4 (ბ)

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (1) (ე); CJEU, C-524/06, *Huber v. Bundesrepublik Deutschland* [GC], 2008.	**საჯარო ინტერესი და კანონით მინიჭებული უფლებამოსილების განხორციელება**	რეკომენდაცია პროფილირების შესახებ, მუხლი 3.4 (ბ)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (1) (ვ); CJEU, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'*, 2017; CJEU, გაერთიანებული საქმეები C-468/10 და C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 2011.	**სხვათა ლეგიტიმური ინტერესები**	რეკომენდაცია პროფილირების შესახებ, მუხლი 3.4 (ბ); ECtHR, *Y v. Turkey*, No. 648/10, 2015.
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (4)	**გამონაკლისი მიზნის შეზღუდვის პრინციპიდან: შემდგომი დამუშავება სხვა მიზნებით**	მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (ბ)
სენსიტიურ მონაცემთა კანონიერი დამუშავების წესები		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 9 (1)	**დამუშავების ზოგადი აკრძალვა**	მოდერნიზებული 108-ე კონვენცია, მუხლი 6
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 9 (2)	**გამონაკლისები დამუშავების ზოგადი აკრძალვიდან**	მოდერნიზებული 108-ე კონვენცია, მუხლი 6

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მოდერნიზებული 108-ე კონვენცია		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 32	**უსაფრთხო დამუშავების ვალდებულება**	მოდერნიზებული 108-ე კონვენცია, მუხლი 7 (1)
		ECtHR, *I v. Finland,* No. 20511/03, 2008
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 32 (1) (ბ)	**კონფიდენციალობის დაცვის ვალდებულება**	მოდერნიზებული 108-ე კონვენცია, მუხლი 7 (1)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 34; დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ, მუხლი 4 (2).	**შეტყობინება მონაცემთა უსაფრთხოების დარღვევის შესახებ**	მოდერნიზებული 108-ე კონვენცია, მუხლი 7 (2)
ანგარიშვალდებულებისა და შესაბამისობის ხელშეწყობის წესები		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 12, 13 და 14	**გამჭვირვალობა**	მოდერნიზებული 108-ე კონვენცია, მუხლი 8
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 37, 38 და 39	**მონაცემთა დაცვის ოფიცრები**	მოდერნიზებული 108-ე კონვენცია, მუხლი 10 (1)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 30	**მონაცემთა დამუშავების აქტივობების აღრიცხვა**	
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლიები 35 და 36	**მონაცემთა დაცვის რისკების შეფასება და წინასწარი კონსულტაცია**	მოდერნიზებული 108-ე კონვენცია, მუხლი 10 (2);

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 33 და 34	**შეტყობინება მონაცემთა უსაფრთხოების დარღვევის შესახებ**	მოდერნიზებული 108-ე კონვენცია, მუხლი 7(2)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 40 და 41	**ქცევის კოდექსი**	
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 42 და 43	**სერტიფიცირება**	
მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (data protection by design) და მონაცემთა დაცვა პირველად პარამეტრად (data protection by default)		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 25 (1) (ა)	**მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (data protection by design)**	მოდერნიზებული 108-ე კონვენცია, მუხლი 10 (2)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 25 (1) (ბ)	**მონაცემთა დაცვა პირველად პარამეტრად (data protection by default)**	მოდერნიზებული 108-ე კონვენცია, მუხლი 10 (3)

აუცილებელია, პრინციპები იყოს ზოგადი. მათი გამოყენება კონკრეტულ სიტუაციებში გარკვეულ თავისუფლებას ქმნის ინტერპრეტაციისა და საშუალებათა შერჩევის მხრივ. **ევროპის საბჭოს სამართლის** მიხედვით, ასეთი თავისუფლების ფარგლების/ზღვრის განსაზღვრა შიდასახელმწიფოებრივ კანონმდებლობაში დამოკიდებულია მოდერნიზებული 108-ე კონვენციის მხარეებზე, ხოლო **ევროკავშირის სამართალში** ამ მხრივ განსხვავებული სიტუაციაა: კერძოდ, შიდა ბაზარზე მონაცემთა დასაცავად განისაზღვრა უფრო დეტალური წესების შექმნის საჭიროება ევროკავშირის დონეზე, რათა მომხდარიყო წევრი სახელმწიფოების მონაცემთა დაცვის ეროვნულ კანონმდებლობათა ჰარმონიზება. მონაცემთა დაცვის ზოგადი რეგულაცია, მე-5 მუხლის პრინციპების ფარგლებში, ადგენს დეტალური წესების ახალ დონეს, რომელიც პირდაპირ ვრცელდება სამართლის ეროვნულ სისტემაზე. შესაბამისად, ქვემოთ წარმოდგენილი ინფორმაცია ევროპულ დონეზე მონაცემთა დაცვის დეტალური წესების შესახებ ძირითადად შეეხება ევროკავშირის სამართალს.

4.1 კანონიერი დამუშავების წესები

ძირითადი საკითხები

- პერსონალურ მონაცემთა კანონიერი დამუშავება უნდა აკმყოფილებდეს შემდეგ კრიტერიუმებს:
  - ხორციელდებოდეს მონაცემთა სუბიექტის თანხმობის საფუძველზე;
  - ითვალისწინებდეს სახელშეკრულებო ურთიერთობა;
  - საჭირო იყოს მონაცემთა დამმუშავებლის სამართლებრივი ვალდებულების შესასრულებლად;
  - მოითხოვდეს მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესები;
  - აუცილებელი იყოს საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად;
  - განაპირობებდეს მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესები, მხოლოდ იმ შემთხვევაში, თუ ამ ინტერესებს არ გადაწონის მონაცემთა სუბიექტის ინტერესები ან ფუნდამენტური უფლებები.

განსაკუთრებული კატეგორიის პერსონალური მონაცემების კანონიერ დამუშავებაზე ვრცელდება სპეციალური, უფრო მკაცრი რეჟიმი.

4.1.1 მონაცემთა დამუშავების კანონიერი საფუძვლები

მონაცემთა დაცვის ზოგადი რეგულაციის მე-2 თავი („პრინციპები“) ადგენს, რომ პერსონალურ მონაცემთა დამუშავება, პირველ რიგში, უნდა აკმაყოფილებდეს იმ პრინციპებს, რომლებიც უკავშირდება მონაცემთა ხარისხს და წარმოდგენილია რეგულაციის მე-5 მუხლში. ერთ-ერთი პრინციპის თანახმად, პერსონალური მონაცემები „უნდა დამუშავდეს კანონიერად, სამართლიანად და გამჭვირვალედ.“ ამასთან, არაგანსაკუთრებული კატეგორიის პერსონალურ

მონაცემთა კანონიერი დამუშავება უნდა აკმაყოფილებდეს მე-6[341] მუხლში წარმოდგენილ რომელიმე საფუძველს, განსაკუთრებული კატეგორიის (ანუ სენსიტიურ) მონაცემთა დამუშავება კი - მე-9 მუხლის საფუძვლებს. მოდერნიზებული 108-ე კონვენციის მე-2 მუხლის თანახმად, რომელიც ითვალისწინებს „პერსონალურ მონაცემთა დაცვის ძირითად პრინციპებს“, კანონიერი დამუშავება უნდა იყოს „დასახული კანონიერი მიზნის პროპორციული.“

იმ კანონიერი საფუძვლების მიუხედავად, რომლებსაც დამმუშავებელი ეყრდნობა პერსონალურ მონაცემთა დამუშავების ოპერაციის ინიცირებისთვის, მან ასევე უნდა გამოიყენოს მონაცემთა დაცვის ზოგადი სამართლებრივი რეჟიმით გათვალისწინებული დაცვის მექანიზმებიც.

თანხმობა

ევროპის საბჭოს სამართალში თანხმობაზე მიუთითებს მოდერნიზებული 108-ე კონვენციის 5(2) მუხლი; ასევე, ECtHR-ის პრეცედენტული სამართალი და ევროპის საბჭოს რამდენიმე რეკომენდაცია.[342] ევროკავშირის სამართალში თანხმობა, როგორც მონაცემთა კანონიერი დამუშავების საფუძველი, მკაცრად არის დადგენილი GDPR-ის მე-6 მუხლით. მასზე მკაფიოდ მიუთითებს ქარტიის მე-8 მუხლიც. კანონიერი თანხმობის მახასიათებლები განმარტებულია რეგულაციის მე-4 მუხლში, ასეთი თანხმობის მოპოვების პირობები კი დეტალურად არის წარმოდგენილი მე-7 მუხლში; რაც შეეხება არასრულწლოვნისგან თანხმობის მიღების სპეციალურ წესებს საინფორმაციო საზოგადოების მომსახურებასთან დაკავშირებით, მათ ადგენს რეგულაციის მე-8 მუხლი.

2.4 ნაწილში განმარტებულია, რომ თანხმობა არის სურვილის ნებაყოფილობითი, კონკრეტული, ინფორმირებული და მკაფიო გამოხატულება, გადმოცემული განცხადებით ან ნათელი და აქტიური ქმედებით, რომლითაც შესაბამისი პირი აცხადებს თანხმობას თავისი პერსონალური მონაცემების დამუშავებაზე. მას უფლება აქვს, თანხმობა უკან გამოითხოვოს ნებისმიერ დროს. მონაცემთა დამმუშავებელი ვალდებულია, თანხმობა აღრიცხოს იმ ფორმით, რომ შეიძლებოდეს მისი შემოწმება.

341 CJEU, გაერთიანებული საქმეები C-465/00, C-138/01 და C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Jospeh Lauermann v. Österreichischer Rundfunk,* 2003 წლის 20 მაისი, პუნქტი 65; CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 2008 წლის 16 დეკემბერი, პუნქტი 48; CJEU, გაერთიანებული საქმეები C-468/10 და C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado,* 2011 წლის 24 ნოემბერი, პუნქტი 26.

342 იხ: ევროპის საბჭოს მინისტრთა კომიტეტის რეკომენდაცია CM/Rec(2010)13 წევრი სახელმწიფოებისთვის, პროფილირების კონტექსტში პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირთა დაცვის შესახებ, 2010 წლის 23 ნოემბერი, მუხლი 3.4 (ბ).

ნებაყოფლობითი/თავისუფალი თანხმობა

მოდერნიზებული 108-ე კონვენციის ფარგლებში, მონაცემთა სუბიექტის თანხმობა უნდა „იყოს გამიზნული არჩევანის ნებაყოფლობითი გამოხატულება.“ [343] თანხმობა ნებაყოფლობითია, როცა „მონაცემთა სუბიექტს აქვს რეალური არჩევანის შესაძლებლობა და არ არსებობს მოტყუების, დაშინების, იძულების ან მნიშვნელოვანი უარყოფითი შედეგების საფრთხე, თუკი უარს იტყვის მის გაცემაზე.“ [344] ამ კუთხით, **ევროკავშირის სამართალში** აღნიშნულია, რომ თანხმობა არ მიიჩნევა ნებაყოფლობითად, თუ „მონაცემთა სუბიექტს არ აქვს რეალური და თავისუფალი არჩევანის საშუალება, არ შეუძლია უარის თქმა ან თანხმობის გამოთხოვა ისე, რომ არ გახდეს მისთვის საზიანო.“ [345] GDPR-ში ხაზგასმით არის აღნიშნული, რომ „თანხმობის ნებაყოფლობითობის შეფასებისას განსაკუთრებული ყურადღება უნდა დაეთმოს *inter alia* იმას, თუ რამდენად აუცილებელი იყო მონაცემების დამუშავება ამ ხელშეკრულების შესრულებისა ან მომსახურების მიწოდებისათვის.“[346] მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათის თანახმად, „დაუშვებელია მონაცემთა სუბიექტზე (ეკონომიკური ან სხვა ტიპის) არასათანადო გავლენა ან ზეწოლა, პირდაპირ ან ირიბად, თანხმობა კი არ უნდა ჩაითვალოს ნებაყოფლობითად, თუ მონაცემთა სუბიექტს არ აქვს რეალური არჩევანის საშუალება, არ შეუძლია თანხმობაზე უარის თქმა, ანდა მისი გამოთხოვა ისე, რომ არ გახდეს საზიანო.“ [347]

მაგალითი: სახელმწიფო A-ს ზოგიერთმა მუნიციპალიტეტმა გადაწყვიტა ჩიპიანი ბინადრობის ბარათების შექმნა. ეს ბარათები სავალდებულო არ არის, თუმცა, ვინც არ ფლობს, ხელი არ მიუწვდება რიგ მნიშვნელოვან ადმინისტრაციულ მომსახურებებზე (მაგ.: მუნიციპალური გადასახადების ინტერნეტით გადახდა; საჩივრების ელექტრონულად წარდგენა, რაც იძლევა საშუალებას, შესაბამისმა სახელმწიფო უწყებამ საჩივარს 3 დღის ვადაში გასცეს პასუხი; მომსახურების რიგში დგომის გარეშე მიღება; მუნიციპალური საკონცერტო დარბაზის ბილეთების ფასდაკლებით შეძენა; შესასვლელში განთავსებული სკანერებით სარგებლობა).

ამ მაგალითში მუნიციპალიტეტების მიერ პერსონალურ მონაცემთა დამუშავება არ ეფუძნება თანხმობას. ქალაქის მოსახლეობაზე, სულ მცირე,

343 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 42.

344 29-ე მუხლის სამუშაო ჯგუფი (2011), მოსაზრება 15/2011 თანხმობის ცნების შესახებ, WP 187, ბრიუსელი, 2011 წლის 13 ივლისი, გვ.12.

345 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 42.

346 *იქვე,* მუხლი 7(4).

347 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 42.

ირიბი ზეწოლა ხორციელდება, რომ აიღონ ელექტრონული ბარათები და დათანხმდნენ მონაცემთა დამუშავებას. შესაბამისად, თანხმობა არ არის ნებაყოფლობითი. მუნიციპალიტეტების მიერ ელექტრონული ბარათების სისტემის შექმნა უნდა ეფუძნებოდეს კანონიერ საფუძველს, რომელიც გაამართლებს მონაცემთა დამუშავებას. მაგალითად, მათ შეიძლება განუმარტონ, რომ დამუშავება საჭიროა საჯარო ინტერესის გარკვეული ამოცანების შესასრულებლად, რაც GDPR-ის მე-6 მუხლის 1 (ე) პუნქტის თანახმად, ქმნის დამუშავების კანონიერ საფუძველს. [348]

ნებაყოფლობითი თანხმობა ეჭვქვეშ დგება, როდესაც, გარკვეული სუბორდინაციის მიხედვით, მონაცემთა დამმუშავებელსა (თანხმობის მიმღები) და მონაცემთა სუბიექტს (თანხმობის გამცემი) შორის მნიშვნელოვანი ეკონომიკური ან სხვა სახის დისბალანსია. [349] ამის ტიპური მაგალითია დამსაქმებლის მიერ პერსონალურ მონაცემთა დამუშავება დასაქმებულთან ურთიერთობის კონტექსტში. 29-ე მუხლის სამუშაო ჯგუფის თანახმად, დასაქმებულსა და დამსაქმებელს შორის ურთიერთობის გათვალისწინებით, „დასაქმებულებს თითქმის არასდროს აქვთ შესაძლებლობა, გამოხატონ ნებაყოფლობითი თანხმობა, და უარი თქვან ან უკან გამოითხოვონ ის. ძალაუფლების დისბალანსის გამო, დასაქმებულებს ნებაყოფლობითი თანხმობის გამოხატვა მხოლოდ გამონაკლის შემთხვევებში შეუძლიათ, როდესაც შეთავაზებაზე დათანხმება ან უარის თქმა არ იწვევს რაიმე შედეგს.“ [350]

მაგალითი: ერთ-ერთი მსხვილი კომპანია აპირებს საკუთარი თანამშრომლების ცნობარის შექმნას, სადაც წარმოდგენილი იქნება მათი სახელი, ინფორმაცია სამსახურებრივი ფუნქციების შესახებ და სამსახურებრივი მისამართები. ცნობარი იქმნება მხოლოდ და მხოლოდ კომპანიის შიდა კომუნიკაციის გასაუმჯობესებლად. კადრების განყოფილების ხელმძღვანელმა წარმოადგინა წინადადება ცნობარში თანამშრომელთა ფოტოების შეტანის შესახებ, რაც გააიოლებს შეხვედრებზე კოლეგების იდენტიფიცირებას. დასაქმებულთა წარმომადგენლების მოთხოვნით, სურათები ცნობარში უნდა შეიტანონ მხოლოდ დასაქმებულთა ნებართვის საფუძველზე.

348 29-ე მუხლის სამუშაო ჯგუფი (2011), მოსაზრება 15/2011 თანხმობის ცნების შესახებ, WP187, ბრიუსელი, 2011 წლის 13 ივლისი, გვ. 16. იმ საქმეების მაგალითები, სადაც მონაცემთა დამუშავება არ/ვერ დაეფუძნება თანხმობას, მაგრამ საჭიროებს განსხვავებულ სამართლებრივ საფუძველს დამუშავების ლეგიტიმიზაციისათვის, გვ: 14 და 17.

349 ასევე, იხ. 29-ე მუხლის სამუშაო ჯგუფი (2001), მოსაზრება 8/2001 დასაქმების კონტექსტში პერსონალური მონაცემების დამუშავების შესახებ, WP 48, ბრიუსელი, 2001 წლის 13 სექტემბერი; 29-ე მუხლის სამუშაო ჯგუფი (2005), სამუშაო დოკუმენტი 1995 წლის 24 ოქტომბერის 95/46/EC დირექტივის 26-ე მუხლის პირველი პუნქტის საერთო განმარტების შესახებ, ბრიუსელი, 2005 წლის 25 ნოემბერი; 29-ე მუხლის სამუშაო ჯგუფი (2017), მოსაზრება 2/2017 სამსახურში მონაცემთა დამუშავების შესახებ, WP 249, ბრიუსელი, 2017 წლის 8 ივნისი.

350 29-ე მუხლის სამუშაო ჯგუფი, *მოსაზრება 2/2017 სამსახურში მონაცემთა დამუშავების შესახებ, WP 249, ბრიუსელი,* 2017 წლის 8 ივნისი.

ასეთ ვითარებაში, დასაქმებულის თანხმობა უნდა ჩაითვალოს სამართლებრივ საფუძვლად ცნობარში ფოტოების დამუშავებისთვის, ვინაიდან, შეგვიძლია ვივარაუდოთ, რომ საკუთარი ფოტოს გამოქვეყნებაზე უარი დასაქმებულს უარყოფით შედეგს არ მოუტანს.

მაგალითი: კომპანია A აპირებს შეხვედრის გამართვას 3 დასაქმებულსა და კომპანია B-ს დირექტორებს შორის, ერთ-ერთ პროექტზე სამომავლო თანამშრომლობის განსახილველად. შეხვედრა გაიმართება კომპანია B-ის ოფისში. ამ უკანასკნელმა კომპანია A-ს მოსთხოვა შეხვედრის მონაწილეთა სახელები, ავტობიოგრაფიები (CV) და ფოტოები. კომპანია B აცხადებს, რომ მას სახელები და ფოტოები სჭირდება უსაფრთხოების მიზნებით, რათა დაცვის თანამშრომლებმა შეძლონ შენობაში შემომსვლელთა ვინაობის დადგენა, ხოლო ბიოგრაფიები სჭირდებათ დირექტორებს, შეხვედრისთვის უკეთ მოსამზადებლად. ასეთ შემთხვევაში, კომპანია A-ს მიერ საკუთარი თანამშრომლების პერსონალური მონაცემების გადაცემა ვერ იქნება თანხმობაზე დაფუძნებული. თანხმობა ვერ ჩაითვლება ნებაყოფლობითად, თუ ივარაუდება, რომ დასაქმებულს უარყოფით შედეგს მოუტანს შეთავაზებაზე უარი (მაგ.: შესაძლოა, ისინი კომპანიამ სხვა კოლეგით ჩაანაცვლოს არა მხოლოდ შეხვედრაზე, არამედ კომპანია B-სთან თანამშრომლობის და, ზოგადად, პროექტში მონაწილეობის თვალსაზრისითაც). ამრიგად, დამუშავებას უნდა ჰქონდეს სხვა კანონიერი საფუძველი.

ეს არ ნიშნავს, რომ თანხმობას ვერ ექნება კანონიერი ძალა (არ იქნება ვალიდური) იმ შემთხვევაში, თუ უარს რაიმე უარყოფითი შედეგის მოტანა შეუძლია. მაგალითად, როცა სუპერმარკეტის მომხმარებელთა უარი ბარათის აღებაზე ნიშნავს მხოლოდ იმას, რომ ისინი ვერ შეძლებენ გარკვეული პროდუქტების ფასდაკლებით შეძენას, თანხმობა ჩაითვლება დასაბუთებულ სამართლებრივ საფუძვლად იმ პირთა პერსონალური მონაცემების დამუშავებისთვის, რომლებიც დათანხმდნენ ასეთი ბარათის აღებას. კომპანიასა და მომხმარებელს შორის სუბორდინაცია არ არსებობს, ხოლო უარის შედეგები არ გახლავთ იმდენად მძიმე, რომ მონაცემთა სუბიექტს თავისუფალი არჩევანის საშუალება არ მისცეს (თუ დავუშვებთ, რომ ფასდაკლება მცირეა და არჩევანზე გავლენას არ მოახდენს).

თუმცა, როცა საქონლისა და მომსახურების შეძენა შესაძლებელია მხოლოდ მონაცემთა დამმუშავებლის ან მესამე პირისათვის გარკვეულ პერსონალურ მონაცემთა გამჟღავნების შემთხვევაში, მონაცემთა სუბიექტის თანხმობა გამჟღავნებაზე, რომელიც არ არის საჭირო ხელშეკრულების გასაფორმებლად, ვერ ჩაითვლება ნებაყოფლობით გადაწყვეტილებად - და, შესაბამისად, კანონიერი ძალის მქონე თანხმობად - მონაცემთა დაცვის კანონმდებლო-

ბის მიხედვით.[351] GDPR მკაცრად კრძალავს საქონლისა და მომსახურების მჭიდროდ დაკავშირებას პერსონალურ მონაცემთა დამუშავებაზე თანხმობასთან.[352]

მაგალითი: მგზავრების თანხმობა, რომ ავიაკომპანიამ მგზავრთა პირადი მონაცემები (ე.ი. მათ ვინაობა, კვებითი შეზღუდვები თუ ჯანმრთელობის მდგომარეობა) უცხო ქვეყნის საიმიგრაციო სამსახურს გადასცეს, ვერ ჩაითვლება კანონიერი ძალის მქონედ მონაცემთა დაცვის კანონმდებლობის შესაბამისად, რადგან მგზავრებს სხვა არჩევანი არ აქვთ ამ ქვეყნის მოსანახულებლად. მონაცემთა ამგვარი გადაცემის კანონიერებისთვის საჭიროა სხვა სამართლებრივი საფუძველი - სავარაუდოდ, კონკრეტული კანონმდებლობა.

ინფორმირებული თანხმობა

მონაცემთა სუბიექტს გადაწყვეტილების მიღებამდე საკმარისი ინფორმაცია უნდა ჰქონდეს. ინფორმირებული თანხმობა ძირითადად მოიცავს იმ საკითხის ზუსტ და მარტივ აღწერას, რომელზეც იგი მოითხოვება. 29-ე მუხლის სამუშაო ჯგუფი განმარტავს, რომ თანხმობა უნდა ეფუძნებოდეს იმ ფაქტებისა და შედეგების გაცნობა-გააზრებას, რომლებსაც გამოიწვევს მონაცემთა სუბიექტის თანხმობა მონაცემთა დამუშავებაზე. ამრიგად, „შესაბამის პირს მკაფიო და გასაგები ფორმით უნდა მიეწოდოს ზუსტი და სრული ინფორმაცია ყველა საჭირო საკითხზე [...], როგორიცაა დამუშავებული მონაცემების ბუნება, მათი შესაძლო მიმღებები და მონაცემთა სუბიექტების უფლებები.“ [353] ინფორმირებული თანხმობისთვის, შესაბამის პირს უნდა ეცნობოს დამუშავებაზე უარის თქმის შედეგებიც.

ინფორმირებული თანხმობის მნიშვნელობის გათვალისწინებით, GDPR და მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი მოიცავს ამ ცნების განმარტებას. GDPR-ის შესავალ ნაწილში აღნიშნულია: ინფორმირებული თანხმობა ნიშნავს, რომ „მონაცემთა სუბიექტისთვის ცნობილი უნდა იყოს, სულ მცირე, დამმუშავებლის ვინაობა და დამუშავების მიზანი.“ [354]

351 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 7(4).

352 *იქვე.*

353 29-ე მუხლის სამუშაო ჯგუფი (2007), სამუშაო დოკუმენტი ჯანდაცვის ელექტრონულ ჩანაწერებში ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების შესახებ, WP 131, ბრიუსელი, 2007 წლის 15 თებერვალი.

354 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 42.

როდესაც გამონაკლის შემთხვევებში მონაცემთა საერთაშორისო გადაცემის საფუძველს ქმნის თანხმობა, მისი კანონიერებისთვის, დამმუშავებელმა მონაცემთა სუბიექტს უნდა შეატყობინოს გადაცემასთან დაკავშირებული რისკები, შესაბამისობაზე გადაწყვეტილებისა და სათანადო დაცვის ზომების არარსებობის გამო. [355]

მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი ადგენს მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდების ვალდებულებას გადაწყვეტილების შედეგებზე. კერძოდ, ამ ინფორმაციაში იგულისხმება „თანხმობის მნიშვნელობა და ფარგლები.“ [356]

ინფორმაციის ხარისხი ასევე საგულისხმოა და ნიშნავს, რომ მისი ენა მორგებული უნდა იყოს შესაძლო მიმღებებზე. ინფორმაცია უნდა მიეწოდოს ჟარგონების გარეშე, მკაფიოდ და მარტივი ენით, რომლის გაგებაც მომხმარებელს არ გაუჭირდება; [357] ასევე, ის ადვილად ხელმისაწვდომი უნდა იყოს მონაცემთა სუბიექტისათვის, ზეპირი ან წერილობითი ფორმით. მნიშვნელოვანი ელემენტებია ინფორმაციის ნათლად და თვალსაჩინოდ წარმოდგენაც. ონლაინ სივრცეში ეფექტიანი გადაწყვეტის ნიმუშია რამდენიმედონიანი შეტყობინება. ასეთი შეტყობინება მონაცემთა სუბიექტს საშუალებას აძლევს, თვითონ აირჩიოს ინფორმაციის მოკლე (ლაკონიური) ან უფრო ვრცელი ვერსია.

კონკრეტული თანხმობა

იმისათვის, რომ თანხმობას ჰქონდეს კანონიერი ძალა, უნდა მიემართებოდეს კონკრეტული დამუშავების მიზანს, რომელიც ნათლად და მკაფიოდ არის აღწერილი. ეს მჭიდროდ უკავშირდება თანხმობის მიზანზე მონაცემთა სუბიექტისათვის მიწოდებული ინფორმაციის ხარისხს. ასეთ კონტექსტში მისი გონივრული მოლოდინები შესაბამისია. შესაძლოა, მონაცემთა სუბიექტს ხელმეორედ ეთხოვოს თანხმობა, თუკი საჭირო გახდება დამუშავების ოპერაციების დამატება ან შეცვლა, რისი განჭვრეტაც, გონივრულობის ფარგლებში, შეუძლებელი იქნებოდა თავდაპირველი თანხმობის გაცემისას. როდესაც დამუშავება რამდენიმე მიზანს ემსახურება, თანხმობა უნდა გაიცეს თითოეულთან დაკავშირებით. [358]

355 *იქვე,* მუხლი 49(1)(ა).

356 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 42.

357 29-ე მუხლის სამუშაო ჯგუფი (2011), მოსაზრება 15/2011 თანხმობის განმარტების შესახებ, WP187, ბრიუსელი, 2011 წლის 13 ივლისი, გვ.19.

358 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 32.

მაგალითები: საქმეში *Deutsche Telekom AG*[359] CJEU-ს უნდა დაედგინა, სჭირდებოდა თუ არა ტელეკომუნიკაციების პროვაიდერს აბონენტთა პერსონალური მონაცემების ცნობარში გამოსაქვეყნებლად განახლებული თანხმობა მონაცემთა სუბიექტებისგან,[360] რამდენადაც თავდაპირველი თანხმობის გაცემისას მონაცემთა მიმღებნი არ იყვნენ დასახელებულნი.

სასამართლომ დაადგინა, რომ პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების დირექტივის მე-12 მუხლის თანახმად, მონაცემთა გადაცემამდე განახლებული თანხმობის მიღება არ იყო საჭირო. მონაცემთა სუბიექტებს მოცემულ პირობებში თანხმობის გამოხატვა შეეძლოთ მხოლოდ დამუშავების მიზანთან დაკავშირებით (მათი მონაცემების გამოქვეყნება). შესაბამისად, მათ არ შეეძლოთ იმ კონკრეტული ცნობარის არჩევა, სადაც შეიძლება გამოექვეყნებინათ მათი მონაცემები.

სასამართლომ ხაზგასმით აღნიშნა: „პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების დირექტივის მე-12 მუხლის კონტექსტუალური და სისტემური განმარტებიდან გამომდინარე, 12(2) მუხლის საფუძველზე გაცემული თანხმობა უკავშირდება საჯარო ცნობარში პერსონალურ მონაცემთა გამოქვეყნების მიზანს და არა ცნობარის კონკრეტული გამომცემის ვინაობას.“[361] ამასთან, „აბონენტებისთვის უარყოფითი შედეგის მოტანა შეუძლია პერსონალურ მონაცემთა საჯარო ცნობარში გამოქვეყნებას“ [362] და არა ცნობარის გამომცემლის ვინაობას.

საქმეში *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV v. Autoriteit Consument en Markt (AMC)*[363] ერთ-ერთი ბელგიური კომპანია ითხოვდა, რომ საცნობარო სამსახურებსა და იმ კომპანიებს, რომლებიც ნიდერლანდებში სატელეფონო ნომრებს ანაწილებენ, მისთვის უზრუნველეყოთ წვდომა აბონენტთა მონაცემებზე. ბელგიური კომპანია მიუთითებდა უნივერსალური სერვისების დირექტივით გათვალისწინე-

359 CJEU, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland,* 2011 წლის 5 მაისი. იხ. განსაკუთრებით, პუნქტები 53 და 54.

360 ევროპარლამენტისა და საბჭოს 2002/58/EC დირექტივა ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ OJ 2002 L 201 (დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ).

361 CJEU, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland,* 2011 წლის 5 მაისი, პუნქტი 61.

362 *იქვე,* პუნქტი 62.

363 CJEU, C-536/15, *Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC),* 2017 წლის 15 მარტი.

ბულ მოვალეობაზე.[364] კერძოდ, ამ დირექტივის თანახმად, კომპანიები, რომლებიც ანაწილებენ სატელეფონო ნომრებს, ვალდებულნი არიან, ეს ნომრები, მოთხოვნის შემთხვევაში, მიაწოდონ ცნობარის გამომცემელს, მომხმარებლის თანხმობის საფუძველზე. ჰოლანდიური კომპანიები უარს აცხადებდნენ აღნიშნული მონაცემების მიწოდებაზე - იმ მოტივით, რომ სხვა წევრ სახელმწიფოში შექმნილი დაწესებულებისთვის მონაცემების მიწოდება არ მოეთხოვებოდათ. კერძოდ, მათი არგუმენტი იყო ის, რომ მომხმარებლებმა თანხმობა გასცეს თავიანთი ნომრების ჰოლანდიურ (და არა სხვა ქვეყნის) ცნობარში გამოქვეყნებაზე. CJEU-მ დაადგინა, რომ უნივერსალური სერვისების დირექტივა ვრცელდება ცნობარის ნებისმიერ გამომცემელზე, მიუხედავად იმისა, რომელ წევრ სახელმწიფოშია შექმნილი; სასამართლომ ასევე განმარტა, რომ აბონენტთა განახლებული თანხმობის გარეშე იმავე მონაცემების გადაცემა სხვა დაწესებულებისათვის, რომელიც საჯარო ცნობარის გამოცემას აპირებს, მნიშვნელოვნად არ შელახავდა პერსონალურ მონაცემთა დაცვის უფლებას.[365] ამრიგად, სატელეფონო ნომრების გამანაწილებელი კომპანია არ არის ვალდებული, რომ თანხმობის მოთხოვნაში, რომლის ადრესატიც კონკრეტული აბონენტია, მიუთითოს, რომელ წევრ სახელმწიფოში გაიგზავნება მასზე ინფორმაცია. [366]

მკაფიო თანხმობა

ყველა თანხმობა უნდა იყოს მკაფიო;[367] კერძოდ, გამოირიცხოს ყოველგვარი გონივრული ეჭვი, რამდენად სურდა მონაცემთა სუბიექტს, გამოეხატა თანხმობა საკუთარი მონაცემების დამუშავებაზე. მაგალითად, მონაცემთა სუბიექტის მხრიდან უმოქმედობა არ აღნიშნავს მკაფიო თანხმობას.

ეს ეხება ისეთ შემთხვევას, როდესაც, მაგალითად, თანხმობის მიღებისათვის, დამმუშავებელი, კონფიდენციალობის პოლიტიკის (privacy policy) მიხედვით, მონაცემთა სუბიექტს უგზავნის შეტყობინებას: „ჩვენი სერვისების გამოყენებით, თქვენ ეთანხმებით პერსონალურ მონაცემთა დამუშავებას.“ ამ შემთხვე-

364 2002 წლის 7 მარტის ევროპარლამენტისა და საბჭოს 2002/22/EC დირექტივა უნივერსალურ მომსახურებებსა და ელექტრონულ საკომუნიკაციო ქსელებსა და მომსახურებებთან დაკავშირებით მომხმარებელთა უფლებების შესახებ (დირექტივა უნივერსალური მომსახურების შესახებ), OJ 2002 L 108, გვ.51, რომელიც შესწორდა ევროპარლამენტისა და საბჭოს 2009/136/EC დირექტივით (უნივერსალური მომსახურების დირექტივა), OJ 2009 L 337, გვ. 11.

365 CJEU, C-536/15, *Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC),* 2017 წლის 15 მარტი, პუნქტი 36.

366 *იქვე,* პუნქტები 40-41.

367 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (11).

ვაში მონაცემთა დამმუშავებელმა უნდა უზრუნველყოს, რომ მომხმარებელი ასეთ განაცხადს დაეთანხმება ინდივიდუალურად და არაავტომატურად.

თუ თანხმობა გაიცემა წერილობითი ფორმით, კონტრაქტის ფარგლებში, პერსონალურ მონაცემთა დამუშავებაზე თანხმობა ცალკე უნდა განისაზღვროს და, ნებისმიერ შემთხვევაში, „არსებობდეს უსაფრთხოების ზომები, რომლებიც უზრუნველყოფს თანხმობის გაცემას და მისი მასშტაბის გაცნობიერებას მონაცემთა სუბიექტის მხრიდან.“ [368]

თანხმობის მოთხოვნა ბავშვების შემთხვევაში

GDPR ბავშვებისათვის განსაკუთრებულ დაცვას ითვალისწინებს საინფორმაციო საზოგადოების მომსახურების კონტექსტში, ვინაიდან „მათთვის შეიძლება ნაკლებად იყოს ცნობილი რისკები, შედეგები, დაცვის მექანიზმები და უფლებები, რომლებიც უკავშირდება პერსონალური მონაცემების დამუშავებას.“ [369] შესაბამისად, **ევროკავშირის სამართალში**, როდესაც საინფორმაციო საზოგადოების მომსახურების მიმწოდებელი ამუშავებს 16 წლამდე პირთა პერსონალურ მონაცემებს თანხმობის საფუძველზე, ასეთი დამუშავება კანონიერად ჩაითვლება „მხოლოდ იმ შემთხვევაში, თუ თანხმობა გაცემულია/დამუშავება ნებადართულია მშობლის უფლების მქონე პირის მიერ.“ [370] შესაძლოა, წევრმა სახელმწიფოებმა ეროვნულ კანონმდებლობაში უფრო მცირე ასაკი დაადგინონ, თუმცა, არა 13 წელზე ნაკლები. [371] მშობლის უფლების მქონე პირის თანხმობა არ არის საჭირო „ბავშვებისთვის პრევენციული ან საკონსულტაციო მომსახურების პირდაპირ შეთავაზების შემთხვევაში.“ [372] დამუშავების კონტექსტში, ბავშვებისთვის განკუთვნილი ნებისმიერი ინფორმაცია გადმოცემული უნდა იყოს ნათლად, მარტივი და ბავშვისთვის გასაგები ენით.[373]

თანხმობის ნებისმიერ დროს გამოთხოვის უფლება

GDRP აწესებს თანხმობის ნებისმიერ დროს გამოთხოვის ზოგად უფლებას.[374] მონაცემთა სუბიექტს ეს უფლება უნდა განემარტოს თანხმობის გაცემამდე,

368 *იქვე,* პრეამბულა, მუხლი 42.

369 *იქვე,* პრეამბულა, მუხლი 38.

370 *იქვე,* მუხლი 8 (1), პირველი აბზაცი. საინფორმაციო საზოგადოებრივი სერვისების განმარტება წარმოდგენილია მონაცემთა დაცვის ზოგადი რეგულაციის მე-4 მუხლის 25-ე პუნქტში.

371 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 8 (1), მეორე აბზაცი.

372 *იქვე,* პრეამბულა, მუხლი 38.

373 *იქვე,* პრეამბულა, მუხლი 58. ასევე, მოდერნიზებული 108-ე კონვენცია, მუხლი 15(2)(ე). მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტები 68 და 125;

374 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 7(3); მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 45.

მისი რეალიზება კი შეეძლოს ნებისმიერ დროს და საკუთარი შეხედულებისამებრ. მონაცემთა სუბიექტი არ არის ვალდებული, ახსნას, თუ რატომ გამოითხოვა თანხმობა. გამოთხოვამ არ უნდა გამოიწვიოს რაიმე უარყოფითი შედეგი, გარდა იმ სარგებლის შეწყვეტისა, რომელიც უკავშირდებოდა მონაცემთა გამოყენებას სუბიექტის მიერ გამოხატული თანხმობის საფუძველზე; ასევე, გამოთხოვა ისეთივე მარტივი უნდა იყოს, როგორც გაცემა.[375] თანხმობა ნებაყოფლობითად არ ჩაითვლება, თუ მონაცემთა სუბიექტს არ აქვს მისი გამოთხოვის შესაძლებლობა რაიმე ზიანის გარეშე, ან გამოთხოვა არ არის ისეთივე ადვილი, როგორც მისი გამოხატვა.[376]

მაგალითი: კლიენტმა თანხმობა განაცხადა სარეკლამო მასალების ფოსტით მიღების შესახებ - იმ მისამართზე, რომელიც მონაცემთა დამმუშავებელს გადასცა. თანხმობის გამოთხოვის შემთხვევაში, მონაცემთა დამმუშავებელმა დაუყოვნებლივ უნდა შეწყვიტოს სარეკლამო მასალების ფოსტით გაგზავნა ამ კლიენტის მისამართზე და ამას არ უნდა მოჰყვეს რაიმე უარყოფითი/საჯარიმო შედეგი (მაგ.: კლიენტისთვის გადასახადის დაკისრება). ამავდროულად, თანხმობის გამოთხოვა ხდება სამომავლოდ და მას არ აქვს უკუძალა. პერიოდი, რომლის განმავლობაშიც კლიენტის პერსონალური მონაცემები მუშავდებოდა მისი თანხმობის საფუძველზე, იყო კანონიერი. თანხმობის გამოთხოვა იწვევს ამ მონაცემთა სამომავლო დამუშავების პრევენციას, გარდა იმ შემთხვევისა, თუ დამუშავება ხორციელდება მონაცემთა წაშლის უფლების შესაბამისად.[377]

ხელშეკრულების შესრულების აუცილებლობა

ევროკავშირის სამართალში GDPR-ის მე-6 მუხლის 1(ბ) პუნქტში წარმოდგენილია კანონიერი დამუშავების კიდევ ერთი საფუძველი - კერძოდ, მონაცემთა დამუშავება, როდესაც ეს „აუცილებელია მონაცემთა სუბიექტის მიერ დადებული ხელშეკრულების შესასრულებლად.“ აღნიშნული დებულება ფარავს წინასახელშეკრულებო ურთიერთობასაც - მაგალითად, როდესაც მხარე აპირებს ხელშეკრულების დადებას, მაგრამ ჯერ არ დაუდია, რადგან არ დასრულებულა გარკვეული შემოწმება. როცა მხარეს ამ მიზნით სურს მონაცემთა დამუშავება, დამუშავება იქნება კანონიერი, თუ ეს აუცილებელია „სუბიექტის თხოვნით გარკვეული ზომების მისაღებად, ხელშეკრულების დადებამდე.“[378]

375 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 7 (3).

376 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 42; მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 42.

377 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 17(1)(ბ).

378 *იქვე*, მუხლი 6(1)(ბ).

მონაცემთა დამუშავების ცნება, როგორც „კანონით გათვალისწინებული საფუძველი“, წარმოდგენილი მოდერნიზებული 108-ე კონვენციის მე-5 მუხლის მე-2 პუნქტში, მოიცავს „მონაცემთა დამუშავებას იმ ხელშეკრულების შესასრულებლად (ან წინასახელშეკრულებო ზომების მისაღებად), რომლის მხარეც არის მონაცემთა სუბიექტი.“ [379]

მონაცემთა დამმუშავებლის სამართლებრივი ვალდებულებები

ევროკავშირის სამართალში მონაცემთა კანონიერი დამუშავების კიდევ ერთი საფუძველია „დამუშავების აუცილებლობა დამმუშავებელზე დაკისრებული სამართლებრივი ვალდებულების შესასრულებლად“ (GDPR, მე-6 მუხლის 1(გ) პუნქტი). აღნიშნული დებულება მოიცავს მონაცემთა დამმუშავებელს როგორც კერძო, ისე საჯარო სექტორში; საჯარო სექტორში მონაცემთა დამმუშავებლის სამართლებრივი ვალდებულებები შეიძლება მოხვდეს რეგულაციის მე-6 მუხლის 1 (ე) პუნქტის მოქმედების სფეროში. გარკვეულ სიტუაციებში, კანონმდებლობა დამმუშავებელს, რომელიც კერძო სექტორს წარმოადგენს, ავალდებულებს მონაცემების დამუშავებას კონკრეტული მონაცემთა სუბიექტების შესახებ. მაგალითად, დამსაქმებლებმა დასაქმებულთა მონაცემები უნდა დაამუშაონ სოციალური უსაფრთხოებისა თუ საგადასახადო მიზნებით, ხოლო ბიზნესებმა თავიანთი კლიენტების პერსონალური მონაცემები უნდა დაამუშაონ საგადასახადო ამოცანებით.

შესაძლოა, სამართლებრივი ვალდებულება გამომდინარეობდეს ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობიდან, რომელიც საფუძვლად უდევს დამუშავების ერთ ან რამდენიმე ოპერაციას. სწორედ კანონმა უნდა განსაზღვროს დამუშავების მიზანი, მონაცემთა დამმუშავებლის მახასიათებლები, დასამუშავებელი პერსონალური მონაცემების ტიპი, უწყებები, რომელთათვისაც შესაძლებელია მონაცემების გადაცემა, მიზნის შეზღუდვა, შენახვის ვადა და კანონიერი და სამართლიანი დამუშავებისათვის საჭირო სხვა ზომები.[380] ნებისმიერი კანონმდებლობა, რომელიც პერსონალურ მონაცემთა დამუშავების საფუძველია, უნდა შეესაბამებოდეს ქარტიის მე-7 და მე-8 მუხლებსა და ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლს.

მონაცემთა დამმუშავებელზე კანონმდებლობით დაკისრებული ვალდებულება დამუშავების კანონიერი საფუძველია **ევროპის საბჭოს** სამართალ-

379 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 46; ევროპის საბჭო, მინისტრთა კომიტეტი (2010), მინისტრთა კომიტეტის რეკომენდაცია CM/Rec(2010)13 წევრი სახელმწიფოებისთვის, პროფილირების კონტექსტში პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირთა დაცვის შესახებ, 2010 წლის 23 ნოემბერი, მუხლი 3.4 (ბ).

380 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 45.

შიც. [381] როგორც უკვე აღინიშნა, ასეთი ვალდებულებები, დაკისრებული იმ დამმუშავებელზე, რომელიც კერძო სექტორს წარმოადგენს, სხვათა კანონიერი ინტერესების ერთ-ერთი კონკრეტული შემთხვევაა, ECHR-ის მე-8 მუხლის მე-2 პუნქტის თანახმად. შესაბამისად, დამსაქმებლის მიერ დასაქმებულთა მონაცემების დამუშავება მიღებულია ევროპის საბჭოს სამართალშიც.

მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესები

ევროკავშირის სამართალში GDPR-ის მე-6 მუხლის 1(დ) პუნქტის თანახმად, მონაცემთა დამუშავება კანონიერია, თუ ეს „აუცილებელია მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დასაცავად.“ ამ კანონიერი საფუძვლის გამოყენება შესაძლებელია მხოლოდ იმ შემთხვევაში, თუ დამუშავება „ცალსახად ვერ მოხდება სხვა სამართლებრივი საფუძვლით.“ [382] ზოგჯერ, ასეთი დამუშავება შესაძლოა დაეფუძნოს როგორც საჯარო ინტერესებს, ისე მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესებს (მაგ.: ეპიდემიებისა და მათ განვითარებაზე მონიტორინგის, ან ჰუმანიტარული კრიზისის შემთხვევაში).

ევროპის საბჭოს სამართალში მონაცემთა სუბიექტის სასიცოცხლო ინტერესები არ არის ნახსენები ECHR-ის მე-8 მუხლში, თუმცა, ისინი ნაგულისხმევია მოდერნიზებული 108-ე კონვენციის მე-5 მუხლის მე-2 პუნქტში, კერძოდ, „კანონიერი საფუძვლის“ ცნებით, რომელიც უკავშირდება პერსონალურ მონაცემთა დამუშავების კანონიერებას. [383]

საჯარო ინტერესი და ოფიციალური უფლებამოსილების განხორციელება

ვინაიდან საზოგადოებრივ საქმეთა ორგანიზება შესაძლებელია სხვადასხვა გზით, GDPR-ის მე-6 მუხლის 1(ე) პუნქტის თანახმად, „პერსონალურ მონაცემთა დამუშავება კანონიერია, თუ ეს „აუცილებელია საჯარო ინტერესის სფეროში შემავალი ამოცანების ან მონაცემთა დამმუშავებლისთვის მინიჭებული ოფიციალური უფლებამოსილების შესასრულებლად [...]“.[384]

---

381 ევროპის საბჭო, მინისტრთა კომიტეტი (2010), მინისტრთა კომიტეტის რეკომენდაცია CM/Rec(2010)13 წევრი სახელმწიფოებისთვის, პროფილირების კონტექსტში პერსონალური მონაცემების ავტომატურ დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ, 2010 წლის 23 ნოემბერი, მუხლი 3.4 (ა).

382 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 46.

383 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 46.

384 იხ: მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 45.

მაგალითი: საქმეში *Huber v. Bundesrepublik Deutschland*[385] გერმანიაში მცხოვრები ავსტრიის მოქალაქე, ბ-ნი ჰუბნერი, მიგრაციისა და ლტოლვილთა ფედერალური სამსახურისგან მოითხოვდა თავისი მონაცემების წაშლას „უცხოელთა ცენტრალური რეესტრიდან“ (AZR). ეს რეესტრი შეიცავს პერსონალურ მონაცემებს ევროკავშირის არაგერმანელი მოქალაქეების შესახებ, რომლებიც გერმანიაში ცხოვრობენ სამ თვეზე მეტხანს, და გამოიყენება სტატისტიკური მიზნებით, ასევე, სასამართლო ორგანოების მიერ - დანაშაულებრივი ან საზოგადოებრივი უსაფრთხოებისათვის სარისკო ქმედებების გამოსაძიებლად და გასახსნელად. CJEU-ს უნდა ემსჯელა, თუ რამდენად შეესაბამება პერსონალურ მონაცემთა დამუშავება AZR-ის მსგავს რეესტრში (რომელზეც სხვა საჯარო უწყებებსაც მიუწვდებათ ხელი) ევროკავშირის კანონმდებლობის მოთხოვნებს, იმის გათვალისწინებით, რომ გერმანიის მოქალაქეებისათვის ასეთი რეესტრი არ არსებობს.

CJEU-მ დაადგინა, რომ 95/46 დირექტივის 7(ე) მუხლის თანახმად,[386] პერსონალურ მონაცემთა დამუშავება კანონიერად მიიჩნევა, თუ ეს აუცილებელია საჯარო ინტერესის სფეროში შემავალი ამოცანების ან მონაცემთა დამმუშავებლისათვის მინიჭებული ოფიციალური უფლებამოსილების შესასრულებლად.

CJEU-ს განმარტებით, „ყველა წევრ სახელმწიფოში დაცვის თანაბარი დონის უზრუნველსაყოფად, 95/46 დირექტივის 7(ე) მუხლში მითითებულ აუცილებლობის კონცეფციას[387] […] ვერ ექნება წევრ სახელმწიფოებს შორის განსხვავებული შინაარსი. ამგვარად, განსახილველ საკითხს დამოუკიდებელი მნიშვნელობა აქვს თანამეგობრობის სამართალში და უნდა განიმარტოს აღნიშნული დირექტივის ამოცანასთან სრულ შესაბამისობაში, მისი 1(1) მუხლის თანახმად.“ [388]

CJEU-მ აღნიშნა, რომ ევროკავშირის მოქალაქის გადაადგილების თავისუფლება იმ წევრი სახელმწიფოს ტერიტორიაზე, რომლის მოქალაქეც არ არის, არ გახლავთ უპირობო. მასზე შეიძლება გავრცელდეს გარკვეული შეზღუდვები და პირობები, რომლებსაც აწესებს ევროპული თანამეგობრობის შექმნის ხელშეკრულება და ამ ხელშეკრულების ასამოქმედე-

385 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 2008 წლის 16 დეკემბერი.

386 ყოფილი მონაცემთა დაცვის დირექტივა, მუხლი 7 (ე), ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6(1)(ე).

387 *იქვე.*

388 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 2008 წლის 16 დეკემბერი, პუნქტი 52.

ბელი ზომები. ამრიგად, თუ წევრი სახელმწიფოს მიერ AZR-ის მსგავსი რეესტრის გამოყენება არსებითად კანონიერია, ბინადრობის უფლების კანონმდებლობის გამოყენებაზე პასუხისმგებელი ორგანოების მხარდასაჭერად, ასეთი რეესტრი უნდა შეიცავდეს მხოლოდ იმ ინფორმაციას, რომელიც აუცილებელია კონკრეტული მიზნისთვის. CJEU-მ დაასკვნა, რომ პერსონალურ მონაცემთა დამუშავების ამგვარი სისტემა ევროკავშირის კანონმდებლობის შესაბამისია, თუ იგი შეიცავს მხოლოდ შესაბამისი კანონმდებლობის გამოყენებისთვის აუცილებელ ინფორმაციას, რეესტრის ცენტრალიზებული სისტემა კი კანონმდებლობის გამოყენებას უფრო ეფექტიანს ხდის. ეროვნულმა სასამართლომ უნდა დაადგინოს, რამდენად აკმაყოფილებს აღნიშნულ პირობებს მოცემული შემთხვევა. თუ არ აკმაყოფილებს, AZR-ის მსგავს რეესტრში პერსონალურ მონაცემთა შენახვა და დამუშავება სტატისტიკური მიზნებისთვის ვერცერთი მიზეზით ვერ ჩაითვლება აუცილებლად 95/46 დირექტივის 7(ე) მუხლის[389] ფარგლებში.[390]

და ბოლოს, რაც შეეხება რეესტრში დაცული მონაცემების გამოყენებას დანაშაულთან ბრძოლის მიზნით, CJEU-მ დაადგინა, რომ ეს ამოცანა „აუცილებლად მოიცავს სისხლის სამართლისა თუ სხვა დანაშაულებთან დაკავშირებული სასჯელის აღსრულებას, მიუხედავად დამნაშავეთა წარმომავლობისა.“ რეესტრი არ შეიცავს პერსონალურ მონაცემებს გერმანიის მოქალაქეების შესახებ და ასეთი განსხვავებული მოპყრობა დისკრიმინაციაა, რომელსაც კრძალავს TFEU-ს მე-18 მუხლი. CJEU-ს განმარტებით, აღნიშნული დებულება კრძალავს „დანაშაულთან ბრძოლის მიზნით, წევრი სახელმწიფოს მიერ პერსონალურ მონაცემთა დამუშავების ისეთი სისტემის დანერგვას, რომელიც განკუთვნილია ევროკავშირის კონკრეტული მოქალაქეებისთვის, კერძოდ, ვინც არ არის ამ ქვეყნის მოქალაქე.“ [391]

უწყებების მიერ პერსონალურ მონაცემთა გამოყენება საჯარო სფეროში მოქმედების დროს ასევე ექცევა ECHR-ის მე-8 და, საჭიროების შემთხვევაში, მოდერნიზებული კონვენციის 5(2) მუხლებში. [392]

389 ყოფილი მონაცემთა დაცვის დირექტივა, მუხლი 7 (ე), ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6(1)(ე).

390 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 2008 წლის 16 დეკემბერი, პუნქტები 54, 58–59 და 66–68.

391 *იქვე,* პუნქტები 78 და 81.

392 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტები 46 და 47.

მონაცემთა დამმუშავებლის ან მესამე მხარის/პირის კანონიერი ინტერესები

ევროკავშირის სამართალში კანონიერი ინტერესები მხოლოდ მონაცემთა სუბიექტს არ აქვს. GDPR-ის მე-6 მუხლის 1(ვ) პუნქტის თანახმად, მონაცემთა დამუშავება კანონიერია, როცა ეს „აუცილებელია მონაცემთა დამმუშავებლის ან იმ მესამე პირ(ებ)ის კანონიერი ინტერესების დასაცავად [თუ საქმე არ ეხება საჯარო ხელისუფლებას, საკუთარი ამოცანების შესრულების პროცესში], რომლებსაც ისინი გადაეცემა, გარდა იმ შემთხვევისა, როდესაც აღნიშნულ ინტერესებს გადაწონის მონაცემთა სუბიექტის ინტერესები, ფუნდამენტური უფლებები და თავისუფლებები, რომლებიც მოითხოვს მონაცემთა დაცვას [...]“.[393]

კანონიერი ინტერესების არსებობა თითოეულ შემთხვევაში ყურადღებით უნდა შეფასდეს.[394] მონაცემთა დამმუშავებლის კანონიერი ინტერესების გამოვლენის შემთხვევაში, საჭიროა მათი დაბალნსება მონაცემთა სუბიექტის ინტერესებთან, ასევე, ფუნდამენტურ უფლებებსა და თავისუფლებებთან.[395] ასეთი შეფასებისას გასათვალისწინებელია მონაცემთა სუბიექტის გონივრული მოლოდინები, რათა დადგინდეს, აღემატება თუ არა მისი ინტერესები და ფუნდამენტური უფლებები მონაცემთა დამმუშავებლის კანონიერ ინტერესებს.[396] თუ ასეა, მაშინ მონაცემთა დამმუშავებელს შეუძლია უსაფრთხოების ზომების მიღება და გამოყენება მონაცემთა სუბიექტის უფლებებზე გავლენის მინიმუმამდე შესამცირებლად (მაგ.: მონაცემთა ფსევდონიმიზაცია) და „ბალანსის“ შესაცვლელად მანამდე, სანამ არ შეძლებს დამუშავების კანონიერ საფუძველზე დაყრდნობას. მოსაზრებაში მონაცემთა დამმუშავებლის კანონიერი ინტერესების ცნების შესახებ 29-ე მუხლის სამუშაო ჯგუფმა ხაზგასმით აღნიშნა ანგარიშვალდებულებისა და გამჭვირვალობის მნიშვნელოვანი როლი და მონაცემთა სუბიექტის უფლება, მოითხოვოს საკუთარი მონაცემების დამუშავების შეწყვეტა, წვდომა, შეცვლა, წაშლა ან გადაცემა, ერთი მხრივ, დამმუშავებლის კანონიერ ინტერესებს და, მეორე მხრივ, მონაცემთა სუბიექტის ინტერესებსა თუ ფუნდამენტურ უფლებებს შორის ბალანსის მიღწევისას.[397]

393 95/46 დირექტივასთან შედარებით, მონაცემთა დაცვის ზოგადი რეგულაციაში წარმოდგენილია უფრო მეტი მაგალითი შემთხვევებისა, რომლებიც ლეგიტიმურ ინტერესად მიიჩნევა.

394 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 47.

395 29-ე მუხლის სამუშაო ჯგუფი (2014), მოსაზრება 06/2014 მონაცემთა დამმუშავებლის ლეგიტიმური ინტერესების ცნების შესახებ, 95/46/EC დირექტივის მე-7 მუხლის თანახმად, 2014 წლის 4 აპრილი.

396 *იქვე.*

397 *იქვე.*

GDPR-ის პრეამბულაში წარმოდგენილია რამდენიმე მაგალითი მონაცემთა დამმუშავებლის კანონიერი ინტერესების შესახებ. მაგალითად, მონაცემთა დამუშავება მონაცემთა სუბიექტის თანხმობის გარეშე ნებადართულია, თუ ეს ხდება პირდაპირი მარკეტინგული მიზნებით, ან „მკაცრად აუცილებელია თაღლითობის თავიდან ასაცილებლად.“ [398]

CJEU-ს პრეცედენტული სამართალი უფრო დეტალურ განმარტებებს შეიცავს ტესტებზე, რომლებითაც კანონიერი ინტერესი დგინდება.

მაგალითი: საქმე *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] შეეხებოდა რიგის სატრანსპორტო კომპანიის ტროლეიბუსის დაზიანებას მგზავრის მიერ ტაქსის კარის მოულოდნელად გაღების შედეგად. კომპანიას სურდა სარჩელის აღძვრა მგზავრის წინააღმდეგ, თუმცა, პოლიციამ მას მხოლოდ მგზავრის სახელი და გვარი მიაწოდა, პირადი ნომრისა და მისამართის შეტყობინებაზე კი უარი განაცხადა, იმ მოტივით, რომ მონაცემთა დაცვის ეროვნული კანონმდებლობის თანახმად, ამ ინფორმაციის გამჟღავნება აკრძალული იყო.

CJEU-ს ლატვიის სასამართლომ მიმართა თხოვნით, მიეღო წინასწარი განჩინება და დაედგინა, ითვალისწინებდა თუ არა ევროკავშირის მონაცემთა დაცვის კანონმდებლობა იმ პერსონალურ მონაცემთა გამჟღავნების ვალდებულებას, რომლებიც საჭიროა სამოქალაქო საქმის აღსაძვრელად ადმინისტრაციული დანაშაულის სავარაუდო ჩამდენის წინააღმდეგ.[400]

CJEU-მ განმარტა, რომ ევროკავშირის მონაცემთა დაცვის კანონმდებლობა ითვალისწინებს შესაძლებლობას - და არა ვალდებულებას - მესამე მხარისათვის მონაცემთა გადაცემის შესახებ, თუკი ეს მის კანონიერ ინტერესებს ემსახურება.[401] CJEU-მ განსაზღვრა 3 კუმულაციური პირობა, რომლებიც უნდა დაკმაყოფილდეს პერსონალურ მონაცემთა „კანონიერი ინტერესების“ საფუძველზე და კანონიერად დამუშავების შემთხვევაში.[402] პირველ რიგში, მესამე პირს, რომელსაც გადაეცემა მონაცემები, კანონიერი ინტერესი უნდა ჰქონდეს. მოცემულ შემთხვევაში, პერსონალურ მონაცემთა მოთხოვნა იმ პირის წინააღმდეგ სარჩელის აღსაძვრელად,

398 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 47.

399 CJEU, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'*, 2017 წლის 4 მაისი.

400 *იქვე,* პუნქტი 23.

401 *იქვე,* პუნქტი 26.

402 *იქვე,* პუნქტები 28–34.

რომლის ქმედებამაც გამოიწვია მატერიალური ზიანი, მესამე მხარის კანონიერი ინტერესია; მეორე, პერსონალურ მონაცემთა დამუშავება აუცილებელი უნდა იყოს დასახული კანონიერი მიზნების მისაღწევად. მოცემულ შემთხვევაში, ისეთი პერსონალური მონაცემები, როგორიცაა მისამართი და/ან პირადი ნომერი, მკაცრად აუცილებელია შესაბამისი პირის იდენტიფიცირებისათვის; მესამე, მონაცემთა სუბიექტის უფლებები და თავისუფლებები არ უნდა აღემატებოდეს მონაცემთა დამმუშავებლის ან მესამე მხარის კანონიერ ინტერესებს. ისინი უნდა დაბალანსდეს ინდივიდუალურად, თითოეულ კონკრეტულ შემთხვევაში, და ისეთი ელემენტების გათვალისწინებით, როგორიცაა მონაცემთა სუბიექტის უფლებების დარღვევის სიმძიმე ან, გარკვეულ შემთხვევებში, მისი ასაკიც კი. თუმცა, CJEU-ს დასკვნით, კონკრეტულ საქმეში ინფორმაციის გამჟღავნებაზე უარს არ ამართლებდა მხოლოდ ის ფაქტი, რომ მონაცემთა სუბიექტი არასრულწლოვანი იყო.

ASNEF and FECEMD -ის საქმეში CJEU-მ იმსჯელა მონაცემთა „კანონიერი ინტერესების“ საფუძველზე დამუშავების შესახებ, რაც იმ დროისათვის მონაცემთა დაცვის დირექტივის 7(ვ) მუხლით იყო გათვალისწინებული.[403]

მაგალითი: საქმეში *ASNEF and FECEMD*[404] CJEU-მ განმარტა, რომ ეროვნულ კანონმდებლობაში დირექტივის 7(ვ) მუხლში წარმოდგენილ პირობებთან დაკავშირებით დამატებითი პირობების დაწესება დაუშვებელია.[405] საქმე შეეხებოდა ესპანეთის მონაცემთა დაცვის კანონმდებლობას, რომლის ერთ-ერთი დებულების თანახმად, კერძო პირს პერსონალური მონაცემების კანონიერი ინტერესის საფუძველზე დამუშავების უფლება აქვს მხოლოდ იმ შემთხვევაში, თუ ეს ინფორმაცია გამოქვეყნებულია საჯარო წყაროებში.

CJEU-მ პირველ რიგში აღნიშნა, რომ 95/46 დირექტივის[406] მიზანია, პერსონალური მონაცემების დამუშავებასთან მიმართებით, ყველა წევრ სახელმწიფოში თანაბრად იყოს დაცული ფიზიკურ პირთა უფლებები და თავისუფლებები. ამ სფეროში შესაბამისი შიდასახელმწიფოებრივი კანო-

403 ყოფილი მონაცემთა დაცვის დირექტივა, მუხლი 7 (ვ), ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (1) (ვ).

404 CJEU, გაერთიანებული საქმეები C-468/10 და C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado,* 2011 წლის 24 ნოემბერი.

405 ყოფილი მონაცემთა დაცვის დირექტივა, მუხლი 7 (ვ), ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6(1)(ვ).

406 ყოფილი მონაცემთა დაცვის დირექტივა, ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია.

ნმდებლობების ჰარმონიზება არ უნდა აქვეითებდეს დადგენილ სტანდარტს, პირიქით, ის მიზნად უნდა ისახავდეს დაცვის დონის გაზრდას ევროკავშირში.[407] შესაბამისად, CJEU-მ დაადგინა: „ყველა წევრ სახელმწიფოში დაცვის თანაბარი დონის უზრუნველსაყოფად, 95/46[408] დირექტივის მე-7 მუხლი ითვალისწინებს ამომწურავ და შემზღუდავ ჩამონათვალს იმ შემთხვევებისა, რომლებშიც პერსონალურ მონაცემთა დამუშავება შეიძლება კანონიერად ჩაითვალოს.“ ამასთან, „დაუშვებელია წევრი სახელმწიფოების მიერ პერსონალურ მონაცემთა დამუშავების კანონიერებასთან დაკავშირებით 95/46 დირექტივის მე-7 მუხლში[409] ახალი პრინციპების დამატება ან დამატებითი მოთხოვნების დაწესება, რაც ნიშნავს ცვლილების შეტანას [მე-7 მუხლში] წარმოდგენილი 6 პრინციპიდან რომელიმეს მოქმედების ფარგლებში.“ [410] CJEU-მ აღიარა, რომ დირექტივის 7(ვ) მუხლით განსაზღვრული ბალანსის მისაღწევად, შეიძლება იმ ფაქტის გათვალისწინებაც, რომ დამუშავების შედეგად მონაცემთა სუბიექტის ფუნდამენტური უფლებების დარღვევის სიმძიმე შეიძლება განსხვავდებოდეს. ეს დამოკიდებულია იმაზე, განთავსდა თუ არა შესაბამისი მონაცემები საჯარო წყაროებში.“

თუმცა, დირექტივის 7(ვ) მუხლი „წევრ სახელმწიფოებს არ აძლევს გარკვეული კატეგორიის პერსონალურ მონაცემთა დამუშავების კატეგორიული და ზოგადი გამორიცხვის საშუალებას, თითოეულ საქმეში დაპირისპირებული უფლებებისა და ინტერესების ერთმანეთთან გაწონასწორების შესაძლებლობის გარეშე.

ზემოაღნიშნულის გათვალისწინებით, CJEU-მ დაასკვნა, რომ დირექტივის 7(ვ) მუხლი[411] უნდა განიმარტოს შემდეგნაირად: მონაცემთა სუბიექტის თანხმობის არარსებობის პირობებში - ასევე, პერსონალურ მონაცემთა დამუშავების დასაშვებად დამმუშავებლის ან იმ მესამე მხარის კანონიერი ინტერესის საფუძველზე, რომელსაც ეს მონაცემები გადაეცემა - დირექტივა, შიდასახელმწიფოებრივი წესებით, არ იძლევა საშუალებას,

407 CJEU, გაერთიანებული საქმეები C-468/10 და C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado,* 2011 წლის 24 ნოემბერი, პუნქტი 28; მონაცემთა დაცვის დირექტივა, პრეამბულა, მუხლები 8 და 10.

408 ყოფილი მონაცემთა დაცვის დირექტივა, მუხლი 7, ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (1) (ვ).

409 ყოფილი მონაცემთა დაცვის დირექტივა, მუხლი 7, ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6.

410 *იქვე.*

411 ყოფილი მონაცემთა დაცვის დირექტივა, მუხლი 7 (ვ), ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (1) (ვ).

> რომ დაწესდეს მონაცემთა სუბიექტის ფუნდამენტური უფლებებისა და თავისუფლებების პატივისცემის ან მონაცემთა საჯარო წყაროებში გამოქვეყნების მოთხოვნა, რითაც კატეგორიულად და ზოგადი ფორმით გამორიცხება ისეთი მონაცემების ნებისმიერი სახით დამუშავება, რომლებიც ღია წყაროებში არ არის განთავსებული.[412]

პერსონალური მონაცემების „კანონიერი ინტერესების“ საფუძველზე დამუშავებისას, შესაბამის პირს ენიჭება უფლება, ნებისმიერ დროს მოითხოვოს მონაცემთა დამუშავების შეწყვეტა, იმ საფუძვლის მითითებით, რომელიც კონკრეტულ სიტუაციას შეესაბამება, GDPR-ის 21-ე მუხლის პირველი პუნქტის თანახმად. მონაცემთა დამმუშავებელი ვალდებულია, შეწყვიტოს დამუშავება, თუკი არ არსებობს მყარი საფუძველი დამუშავების გასაგრძელებლად.

რაც შეეხება ევროპის საბჭოს სამართალს, იმავე ფორმულირებას შეიცავს მოდერნიზებული 108-ე კონვენცია[413] და ევროპის საბჭოს რეკომენდაციები. ევროპის საბჭოს რეკომენდაცია პროფილირების შესახებ პროფილირების მიზნებისთვის მონაცემთა დამუშავებას კანონიერად მიიჩნევს, თუ ეს აუცილებელია სხვათა კანონიერი ინტერესების დასაცავად, „გარდა იმ შემთხვევისა, როდესაც ასეთ ინტერესებზე მაღლა დგას მონაცემთა სუბიექტების ფუნდამენტური უფლებები და თავისუფლებები.“[414] ამასთან, ECHR-ის მე-8 მუხლის მე-2 პუნქტში სხვათა უფლებებისა და თავისუფლებების დაცვა გათვალისწინებულია, როგორც კანონიერი საფუძველი მონაცემთა დაცვის უფლების შესაზღუდად.

> მაგალითი: საქმეში *Y v. Turkey*[415] განმცხადებელს ჰქონდა აივ დადებითი სტატუსი. ვინაიდან საავადმყოფოში მიყვანისას იგი უგონოდ იყო, კლინიკის პერსონალს სასწრაფო დახმარების ექიმებმა დაუდასტურეს პაციენტის აივ დადებითი სტატუსი. განმცხადებელი ECtHR-ის წინაშე აცხადებდა, რომ ამ ინფორმაციის გამჟღავნებით დაირღვა მისი პირდი ცხოვრების პატივისცემის უფლება. თუმცა, საავადმყოფოს პერსონალის უსაფრთხოების დაცვის საჭიროების გათვალისწინებით, სასამართლომ ამ ინფორმაციის გაზიარება განმცხადებლის უფლებების დარღვევად არ მიიჩნია.

412 CJEU, გაერთიანებული საქმეები C-468/10 და C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado,* 2011 წლის 24 ნოემბერი, პუნქტები 40, 44 და 48–49.

413 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 46.

414 ევროპის საბჭო, მინისტრთა კომიტეტი (2010), მინისტრთა კომიტეტის რეკომენდაცია CM/Rec(2010)13 წევრი სახელმწიფოებისთვის, პროფილირების კონტექსტში პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ, 2010 წლის 23 ნოემბერი, მუხლი 3.4 (ბ) (რეკომენდაცია პროფილირების შესახებ).

415 ECtHR, *Y v. Turkey,* No. 648/10, 2015 წლის 17 თებერვალი.

4.1.2 განსაკუთრებული კატეგორიის მონაცემთა დამუშავება

ევროპის საბჭოს კანონმდებლობა სათანადო დაცვის ზომების განსაზღვრას განსაკუთრებული კატეგორიის მონაცემთა გამოყენებისათვის ეროვნულ კანონმდებლობას ანდობს. ასეთ შემთხვევაში, დაცული უნდა იყოს მოდერნიზებული 108-ე კონვენციის პირობები - კერძოდ, კანონმდებლობის მიერ გათვალისწინებული უსაფრთხოების სათანადო ზომები შეესაბამებოდეს კონვენციის სხვა დებულებებს. რაც შეეხება ევროკავშირის სამართალს, GDPR-ის მე-9 მუხლი დეტალურ რეჟიმს განსაზღვრავს განსაკუთრებული კატეგორიის (ე.წ. „სენსიტიურ“) მონაცემთა დასამუშავებლად. ასეთი მონაცემები ამჟღავნებს პირის რასობრივ ან ეთნიკურ წარმომავლობას, პოლიტიკურ შეხედულებებს, რელიგიურ ან ფილოსოფიურ მრწამსს, პროფესიული კავშირის წევრობას. განსაკუთრებულ კატეგორიას განეკუთვნება: გენეტიკური და ბიომეტრიული მონაცემები, რომელთა მიზანია ფიზიკური პირის უნიკალური იდენტიფიცირება; ასევე, ჯანმრთელობასთან, პირის სქესობრივ ცხოვრებასა ან სექსუალურ ორიენტაციასთან დაკავშირებული ინფორმაცია. ზოგადად, განსაკუთრებული კატეგორიის მონაცემების დამუშავება აკრძალულია.[416]

თუმცა, არსებობს გამონაკლისი შემთხვევების ამომწურავი ჩამონათვალი, რომელიც წარმოდგენილია რეგულაციის მე-9 მუხლის მე-2 პუნქტში. ჩამონათვალი ითვალისწინებს განსაკუთრებული კატეგორიის მონაცემთა დამუშავების კანონიერ საფუძვლებს და მოიცავს სიტუაციებს, როდესაც:

- არსებობს მონაცემთა სუბიექტის მკაფიო თანხმობა დამუშავებაზე;
- მონაცემებს ამუშავებს არაკომერციული ორგანიზაცია, კერძოდ, კანონიერი საქმიანობისას პოლიტიკური, ფილოსოფიური, რელიგიური ან პროფესიული კავშირის მიზნებით და იმ პირობით, რომ დამუშავება ეხება მხოლოდ მის მოქმედ ან ყოფილ წევრებს, რომელთაც მუდმივი კავშირი აქვთ ორგანიზაციასთან, მისი ამოცანებიდან გამომდინარე;
- დამუშავება მოიცავს ისეთ მონაცემებს, რომლებიც თვითონ სუბიექტმა საჯაროდ გამოაქვეყნა;
- დამუშავება აუცილებელია შემდეგი მიზნებისთვის:
    - დამმუშავებლის ან მონაცემთა სუბიექტის მოვალეობებისა და კონკრეტული უფლებების განხორციელება, დასაქმების, სოციალური უსაფრთხოების ან სოციალური დაცვის კონტექსტში;

416 ყოფილი მონაცემთა დაცვის დირექტივა, მუხლი 7 (ვ); ამჟამად მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 9 (1).

- მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დაცვა (როდესაც მონაცემთა სუბიექტს არ შეუძლია თანხმობის გაცემა);

- სამართლებრივი მოთხოვნის დადგენა, შესრულება ან დაცვა; ანდა სასამართლო საქმისწარმოება;

- პრევენციული მედიცინა ან შრომითი უსაფრთხოების დაცვა: დასაქმებულის სამუშაო შესაძლებლობათა შეფასება; სამედიცინო დიაგნოზის დასმა; ჯანდაცვა ან სოციალური დაცვა; ასევე, აღნიშნული სფეროსა და შესაბამისი მომსახურების მართვა ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობისა თუ სამედიცინო სფეროს სპეციალისტთან დადებული ხელშეკრულების საფუძველზე“;

- საჯარო ინტერესებისათვის არქივირება, სამეცნიერო/ისტორიული კვლევა ან სტატისტიკის წარმოება;

- საჯარო ინტერესი საზოგადოებრივი ჯანდაცვის სფეროში;

- მნიშვნელოვანი საჯარო ინტერესი.

ამრიგად, განსაკუთრებული კატეგორიის მონაცემთა დასამუშავებლად მონაცემთა სუბიექტთან არსებული სახელშეკრულებო ურთიერთობა არ არის მათი კანონიერი დამუშავების სამართლებრივი საფუძველი, თუ არ ჩავთვლით ჯანდაცვის სფეროს სპეციალისტთან დადებულ ხელშეკრულებას, რომელშიც გათვალისწინებულია პროფესიული საიდუმლოს დაცვის ვალდებულება.[417]

მონაცემთა სუბიექტის მკაფიო თანხმობა

ევროკავშირის კანონმდებლობაში მონაცემთა კანონიერი დამუშავების უპირველესი პირობა - როგორც განსაკუთრებული კატეგორიის, ისე სხვა მონაცემებისათვის - არის მონაცემთა სუბიექტის თანხმობა. განსაკუთრებული კატეგორიის მონაცემების შემთხვევაში, ასეთი თანხმობა უნდა იყოს მკაფიო. ამავდროულად, ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობა შეიძლება ადგენდეს, რომ განსაკუთრებული კატეგორიის მონაცემთა დამუშავების აკრძალვას მონაცემთა სუბიექტი ვერ შეეწინააღმდეგება[418] (მაგ.: როდესაც დამუშავება მონაცემთა სუბიექტს უჩვეულო საფრთხეს უქმნის).

417 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 9 (2)(თ)(ი).

418 *იქვე*, მუხლი 9(2)(ა).

დასაქმების ან სოციალური უსაფრთხოებისა და დაცვის კანონმდებლობა

ევროკავშირის კანონმდებლობით, მე-9 მუხლის პირველი პუნქტით გათვალისწინებული აკრძალვის გაუქმება შესაძლებელია მონაცემთა სუბიექტისა თუ დამმუშავებლის მოვალეობათა ან უფლებათა განსახორციელებლად დასაქმებისა და სოციალური უსაფრთხოების სფეროში. ამავდროულად, დამუშავების უფლებას უნდა იძლეოდეს როგორც ევროკავშირის, ისე ეროვნული კანონმდებლობა, ან მის საფუძველზე დადებული კოლექტიური შეთანხმება, რომელიც ითვალისწინებს უსაფრთხოების სათანადო ზომებს მონაცემთა სუბიექტის ფუნდამენტური უფლებებისა და ინტერესების დასაცავად. [419] ორგანიზაციაში დაცული ჩანაწერები დასაქმებულთა შესახებ შეიძლება შეიცავდეს განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს, GDPR-ით, ასევე, შესაბამისი ეროვნული კანონმდებლობით გათვალისწინებულ შემთხვევებში. განსაკუთრებული კატეგორიის მონაცემების მაგალითებია პროფკავშირის წევრობა ან ინფორმაცია ჯანმრთელობის მდგომარეობის შესახებ.

მონაცემთა სუბიექტის სასიცოცხლო ინტერესები

ევროკავშირის კანონმდებლობით, განსაკუთრებული კატეგორიის მონაცემები, სხვა ტიპის მონაცემთა მსგავსად, შეიძლება დამუშავდეს მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების გამო.[420] პერსონალური მონაცემების დამუშავება შესაძლებელია სხვა პირის სასიცოცხლო ინტერესის საფუძველზე, თუ „დამუშავება ცალსახად ვერ მოხდება სხვა სამართლებრივი საფუძვლით.“[421] ზოგ შემთხვევაში, შესაძლოა, პერსონალურ მონაცემთა დამუშავება იცავდეს როგორც ცალკეული პირის, ისე საჯარო ინტერესებს (მაგ.: როდესაც დამუშავება ხდება ჰუმანიტარული მიზნებით). [422]

ამ საფუძვლით განსაკუთრებული კატეგორიის მონაცემთა კანონიერად დამუშავებისთვის, აუცილებელია, ვერ ხერხდებოდეს თანხმობის მოთხოვნა მონაცემთა სუბიექტისათვის (მაგ.: როცა იგი უგონო მდგომარეობაშია, ადგილზე არ იმყოფება, ან მიუწვდომელია. სხვა სიტყვებით რომ ვთქვათ, პირს ფიზიკური ან სამართლებრივი ქმედუუნარობის გამო არ შეუძლია თანხმობის გაცემა).

419 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 9(2)(ბ).

420 *იქვე*, მუხლი 9(2)(გ).

421 *იქვე*, პრეამბულა, მუხლი 46.

422 *იქვე*.

საქველმოქმედო ან არაკომერციული ორგანიზაციები

პერსონალურ მონაცემთა დამუშავება ნებადართულია ფონდების, ასოციაციების ან სხვა არაკომერციული ორგანიზაციების კანონიერი საქმიანობის ფარგლებშიც, რომლებსაც პოლიტიკური, ფილოსოფიური, რელიგიური ან პროფესიული კავშირის მიზნები აქვთ. ამავდროულად, დამუშავება უნდა ეხებოდეს მხოლოდ და მხოლოდ ამ ორგანიზაციის მოქმედ ან ყოფილ წევრებს, ან ვისაც მასთან რეგულარული კონტაქტი აქვს.[423] ასეთი ორგანიზაციების მიერ განსაკუთრებული კატეგორიის მონაცემების გამჟღავნება მონაცემთა სუბიექტის თანხმობის გარეშე დაუშვებელია.

მონაცემთა სუბიექტის მიერ ცალსახად საჯაროდ გამოქვეყნებული მონაცემები

GDPR-ის 9(ე) მუხლის თანახმად, დამუშავება არ იკრძალება, თუ იგი ეხება მონაცემთა სუბიექტის მიერ ცალსახად საჯაროდ გამოქვეყნებულ პერსონალურ მონაცემებს. რეგულაცია არ განმარტავს „მონაცემთა სუბიექტის მიერ ცალსახად საჯაროდ გამოქვეყნებულ მონაცემებს“, ვინაიდან ეს გამონაკლისია განსაკუთრებული კატეგორიის მონაცემთა დამუშავებაზე დაწესებული აკრძალვიდან, თუმცა მისი შინაარსი უნდა გავიგოთ, როგორც მონაცემთა სუბიექტის მიერ საკუთარი მონაცემების განზრახ გამოქვეყნება საჯაროდ. ამრიგად, თუ ტელევიზიით გადაიცემა სათვალთვალო კამერიდან ამოღებული ვიდეოჩანაწერი, სადაც ჩანს, როგორ დაშავდა მეხანძე შენობის ევაკუაციისას, ეს ვერ ჩაითვლება მეხანძრის მიერ ცალსახად საჯაროდ გამოქვეყნებულ მონაცემებად. მეორე მხრივ, თუ მეხანძრე გადაწყვეტს, რომ ინციდენტის შესახებ ინფორმაცია, ვიდეომასალა და ფოტოები განათავსოს საჯარო ვებგვერდზე, ეს მისი მხრიდან იქნება წინასწარგანზრახული, ნათლად გამოხატული მოქმედება პერსონალურ მონაცემთა საჯაროდ გამოსაქვეყნებლად. უნდა აღინიშნოს, რომ მონაცემთა გამოქვეყნება არის არა თანხმობა, არამედ ნებართვა განსაკუთრებული კატეგორიის მონაცემთა დამუშავების შესახებ.

დამუშავებული პერსონალური მონაცემების გამოქვეყნება მონაცემთა სუბიექტის მიერ დამმუშავებელს არ ათავისუფლებს მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული ვალდებულებებისგან (მაგ.: მიზნის შეზღუდვის პრინციპი კვლავ ვრცელდება პერსონალურ მონაცემებზე, მიუხედავად იმისა, რომ ეს მონაცემები საჯაროდ ხელმისაწვდომია). [424]

423 *იქვე*, მუხლი 9 (2) (დ).

424 29-ე მუხლის სამუშაო ჯგუფი (2013), *Opinion 3/13 on purpose limitation*, WP 203, ბრიუსელი, 2013 წლის 2 აპრილი, გვ.14.

სამართლებრივი მოთხოვნები

GDPR-ის თანახმად,[425] განსაკუთრებული კატეგორიის მონაცემთა დამუშავება ნებადართულია, თუ ეს აუცილებელია სამართლებრივი მოთხოვნების დასადგენად, შესასრულებლად ან დასაცავად სასამართლო საქმისწარმოების დროს, ან ადმინისტრაციული პროცედურისა თუ დავის არასასამართლო გზით მოგვარებისას.[426] ასეთ შემთხვევაში, დამუშავება რელევანტური უნდა იყოს კონკრეტული სამართლებრივი მოთხოვნის შესრულებისა თუ დაცვისთვის და მას ითხოვდეს სამართლებრივი დავის ერთ-ერთი მხარე.

საკუთარი ფუნქციების განხორციელების პროცესში, სასამართლოს აქვს განსაკუთრებული კატეგორიის მონაცემთა დამუშავების უფლება სამართლებრივი დავის გადაწყვეტის კონტექსტში.[427] ამ ტიპის მონაცემთა მაგალითებია: გენეტიკური ინფორმაცია მამობის ან დედობის დადგენისას; და ჯანმრთელობის მდგომარეობა, როდესაც მტკიცებულებათა ნაწილი ეხება მსხვერპლისთვის მიყენებული ზიანის დეტალებს.

მნიშვნელოვანი საჯარო ინტერესი

GDPR-ის მე-9 მუხლის 2(ზ) პუნქტის თანახმად, წევრ სახელმწიფოებს უფლება აქვთ, დაადგინონ დამატებითი გარემოებები, სადაც დაშვებულია განსაკუთრებული კატეგორიის მონაცემთა დამუშავება, თუკი:

- ეს აუცილებელია მნიშვნელოვანი საჯარო ინტერესიდან გამომდინარე;
- გათვალისწინებულია ევროპული ან ეროვნული კანონმდებლობით;
- ევროპული ან ეროვნული კანონმდებლობა პროპორციულია, პატივს სცემს მონაცემთა დაცვის უფლებას და ითვალისწინებს სათანადო და კონკრეტულ ღონისძიებებს მონაცემთა სუბიექტის ფუნდამენტური უფლებებისა და ინტერესების დასაცავად.[428]

ამის თვალსაჩინო მაგალითია ჯანდაცვის ელექტრონული ფაილური სისტემა. ასეთ სისტემაში ნებადართულია ჯანდაცვის სფეროს პროფესიონალთა მიერ პაციენტის მკურნალობის პროცესში შეგროვებულ მონაცემებზე უფრო ფართო (როგორც წესი, ქვეყნის მასშტაბით) წვდომა ჯანდაცვის სხვა პროვაიდერისათვის, რომელიც იმავე პაციენტს ემსახურება.

425 *იქვე*, მუხლი 9 (2) (ვ).

426 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 52.

427 *იქვე*.

428 *იქვე*, მუხლი 9(2)(ზ).

29-ე სამუშაო ჯგუფის დასკვნით, ასეთი სისტემების შექმნა შეუძლებელი იყო არსებული საკანონმდებლო წესების პირობებში, რომელიც მიემართება პაციენტების მონაცემთა დამუშავებას.[429] თუმცა, ჯანდაცვის ელექტრონული ფაილური სისტემების შექმნა შესაძლებელია, თუ ისინი ეფუძნება „მნიშვნელოვან საჯარო ინტერესს.“[430] ეს მოითხოვს მკაფიო სამართლებრივ საფუძველს, რაც ასევე მოიცავს დაცვის აუცილებელ მექანიზმებს სისტემის უსაფრთხო მართვის უზრუნველსაყოფად.[431]

განსაკუთრებული კატეგორიის მონაცემთა დამუშავების სხვა საფუძვლები

GDPR-ის თანახმად, განსაკუთრებული კატეგორიის მონაცემთა დამუშავება შესაძლებელია, თუ ის აუცილებელია შემდეგი მიზნებიდან გამომდინარე:[432]

- პრევენციული ან ოკუპაციური მედიცინა, ანდა შრომითი უსაფრთხოების დაცვა; დასაქმებულის სამუშაო შესაძლებლობათა შეფასება; სამედიცინო დიაგნოზის დასმა; ჯანდაცვა ან სოციალური დაცვა; ასევე, აღნიშნული სფეროსა და შესაბამისი მომსახურების მართვა ევროკავშირის ან მისი წევრი სახელმწიფოს კანონმდებლობის, ან სამედიცინო სფეროს სპეციალისტთან დადებული ხელშეკრულების საფუძველზე;

- საზოგადოებრივ ჯანმრთელობასთან დაკავშირებული საჯარო ინტერესი, როგორიცაა, მაგალითად: დაცვა ჯანმრთელობის სერიოზული საერთაშორისო საფრთხეებისგან; მაღალხარისხიანი და უსაფრთხო ჯანდაცვის მომსახურების, სამედიცინო პროდუქტებისა და მოწყობილობების უზრუნველყოფა ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობის საფუძველზე, რომელშიც გათვალისწინებულია სათანადო ზომები მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დასაცავად;

- არქივირება, სამეცნიერო/ისტორიული კვლევა ან სტატისტიკის წარმოება ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობის შესაბამისად. იგი უნდა იყოს დასახული მიზნის პროპორციული, პატივს სცემდეს მონაცემთა დაცვის უფლებას და ითვალისწინებდეს სათანადო და კონ-

429 29-ე მუხლის სამუშაო ჯგუფი (2007), სამუშაო დოკუმენტი ჯანდაცვის ელექტრონულ ჩანაწერებში ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების შესახებ, WP 131, ბრიუსელი, 2007 წლის 15 თებერვალი; ასევე, მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 9 (3).

430 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 9 (2) (ზ).

431 29-ე მუხლის სამუშაო ჯგუფი (2007), სამუშაო დოკუმენტი ჯანდაცვის ელექტრონულ ჩანაწერებში ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების შესახებ, WP 131, ბრიუსელი, 2007 წლის 15 თებერვალი.

432 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 9 (2) (თ)(ი)(კ).

კრეტულ ზომებს მონაცემთა სუბიექტის ფუნდამენტური უფლებებისა და ინტერესების დასაცავად.

ეროვნული კანონმდებლობით გათვალისწინებული დამატებითი პირობები

GDPR-ის თანახმად, წევრ სახელმწიფოებს უფლება აქვთ, შემოიღონ ან შეინარჩუნონ დამატებითი პირობები, მათ შორის, შეზღუდვები გენეტიკურ, ბიომეტრიულ ან ჯანმრთელობასთან დაკავშირებულ მონაცემთა დამუშავებაზე.[433]

4.2 დამუშავების უსაფრთხოების წესები

ძირითადი საკითხები

- დამუშავების უსაფრთხოების წესები მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს ავალდებულებს შესაბამისი ტექნიკური და ორგანიზაციული ზომების დანერგვას დამუშავების პროცესში ნებისმიერი უნებართვო ჩარევის პრევენციისათვის;
- მონაცემთა უსაფრთხოების აუცილებელი დონე განისაზღვრება შემდეგი ფაქტორებით:
- ბაზარზე ხელმისწვდომი უსაფრთხოების ზომები ნებისმიერი ტიპის დამუშავებისთვის;
- ხარჯები;
- საფრთხე, რომელსაც დამუშავება უქმნის მონაცემთა სუბიექტების ფუნდამენტურ უფლებებსა და თავისუფლებებს.
- პერსონალური მონაცემების კონფიდენციალობა იმ ზოგადი პრინციპის ნაწილია, რომელსაც აღიარებს მონაცემთა დაცვის ზოგადი რეგულაცია.

როგორც **ევროკავშირის, ისე ევროპის საბჭოს სამართალში,** დამმუშავებელს, პერსონალურ მონაცემთა დამუშავების პროცესში, ეკისრება გამჭვირვალობისა და ანგარიშვალდებულების ზოგადი ვალდებულება, კერძოდ, მონაცემთა უსაფრთხოების დარღვევებთან დაკავშირებით. ასეთ შემთხვევაში, მონაცემთა დამმუშავებელი ვალდებულია, უსაფრთხოების დარღვევის შე-

433 *იქვე*, მუხლები 9(2)(თ) და 9 (4).

სახებ შეატყობინოს საზედამხედველო ორგანოებს, გარდა იმ შემთხვევისა, როცა ნაკლებია რისკი, რომ ეს დარღვევა შელახავს ფიზიკურ პირთა უფლებებსა და თავისუფლებებს. აუცილებელია მონაცემთა სუბიექტის ინფორმირებაც პერსონალურ მონაცემთა უსაფრთხოების დარღვევაზე, თუკი სავარაუდოა, რომ დარღვევა მნიშვნელოვან საფრთხეს შეუქმნის ფიზიკურ პირთა უფლებებსა და თავისუფლებებს.

4.2.1 მონაცემთა უსაფრთხოების ელემენტები

ევროკავშირის კანონმდებლობის შესაბამისი დებულებების თანახმად:

> *„უახლესი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ბუნების, მოცულობის, კონტექსტისა და მიზნების, ასევე, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისათვის სავარაუდო საფრთხეების გათვალისწინებით, მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა უნდა მიიღონ რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები უსაფრთხოების უზრუნველსაყოფად […].“*[434]

ეს ზომები მოიცავს შემდეგ ასპექტებს:

- პერსონალურ მონაცემთა ფსევდონიმიზაცია და დაშიფვრა; [435]
- დამუშავების სისტემებისა და სერვისების მუდმივი კონფიდენციალობა, ხელშეუხებლობა, ხელმისაწვდომობა და მოქნილობა; [436]
- ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში, პერსონალურ მონაცემთა წვდომისა და ხელმისაწვდომობის დროული აღდგენა;[437]
- დამუშავების უსაფრთხოების ტექნიკურ და ორგანიზაციულ საშუალებათა ეფექტიანობის რეგულარული შემოწმება და შეფასება.[438]

434 *იქვე*, მუხლი 32 (1).

435 *იქვე*, მუხლი 32 (1) (ა).

436 *იქვე*, მუხლი 32 (1) (ბ).

437 *იქვე*, მუხლი 32 (1) (გ).

438 *იქვე*, მუხლი 32 (1) (დ).

ევროპის საბჭოს კანონმდებლობა შეიცავს მსგავს დებულებას:

> *„თითოეულმა მხარემ უნდა უზრუნველყოს, რომ მონაცემთა დამმუშავებელი და, საჭიროების შემთხვევაში, უფლებამოსილი პირი, მიიღებენ უსაფრთხოების სათანადო ზომებს ისეთი რისკების აღმოსაფხვრელად, როგორიცაა შემთხვევითი ან არასანქცირებული წვდომა პერსონალურ მონაცემებზე, მათი განადგურება, დაკარგვა, გამოყენება, შეცვლა ან გამჟღავნება.“* [439]

ევროკავშირისა და ევროპის საბჭოს სამართალში მონაცემთა უსაფრთხოების დარღვევა, რამაც შესაძლოა გავლენა იქონიოს ფიზიკური პირის უფლებებსა და თავისუფლებებზე, დამმუშავებელს ავალდებულებს დარღვევის შეტყობინებას საზედამხედველო ორგანოსთვის (იხ. ნაწილი 4.2.3).

ხშირად, ასევე არსებობს ინდუსტრიული, ეროვნული ან საერთაშორისო სტანდარტები, რომლებიც მონაცემთა უსაფრთხო დამუშავებისთვის შეიქმნა, მაგალითად: პირადი ცხოვრების ევროპული ხარისხის ბეჭედი (EuroPriSe), ევროკავშირის ტრანსევროპული სატელეკომუნიკაციო ქსელის (eTEN) პროექტი, რომელიც იკვლევს პროდუქტების, განსაკუთრებით, პროგრამული უზრუნველყოფის სერტიფიცირების შესაძლებლობებს, რათა ხელი შეუწყოს ევროკავშირის მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობას; ქსელისა და ინფორმაციული უსაფრთხოების ევროპული სააგენტო (ENSISA) შეიქმნა ევროკავშირის, წევრი ქვეყნებისა და ბიზნესგაერთიანებების მიერ. მისი მიზანია ქსელისა და ინფორმაციის უსაფრთხოების პრობლემათა პრევენცია, გამოვლენა და მათზე რეაგირების გაუმჯობესება.[440] ENSIA რეგულარულად აქვეყნებს უსაფრთხოების მხრივ არსებული რისკების ანალიზს, ასევე, რჩევებს მათთან გასამკლავებლად.[441]

მონაცემთა უსაფრთხოება არ მიიღწევა მხოლოდ სათანადო აღჭურვილობის - ტექნოლოგიური და პროგრამული უზრუნველყოფის - დანერგვით, იგი ასევე საჭიროებს შესაბამის შიდა ორგანიზაციულ წესებს. ასეთი შიდა წესები, საუკეთესო შემთხვევაში, უნდა ითვალისწინებდეს ქვემოთ ჩამოთვლილ საკითხებს:

- ყველა თანამშრომლისათვის ინფორმაციის რეგულარული მიწოდება მო-

439 მოდერნიზებული 108-ე კონვენცია, მუხლი 7 (1).

440 ევროპის პარლამენტის და საბჭოს 2013 წლის 21 მაისის რეგულაცია (EC) No. 526/2013, რომელიც შეეხება ევროკავშირის ქსელისა და ინფორმაციის უსაფრთხოების სააგენტოს (ENISA) და აუქმებს (EC) No. 460/2004 რეგულაციას, OJ 2013 L 165.

441 მაგ.: ENISA, (2016), კიბერუსაფრთხოება და „სმარტ“ მანქანების მდგრადობა. კარგი პრაქტიკა და რეკომენდაციები; ENISA (2016), მობილური გადახდებისა და ციფრული საფულეების უსაფრთხოება.

ნაცემთა უსაფრთხოების წესებისა და მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული ვალდებულებების, განსაკუთრებით, კონფიდენციალობის პირობების შესახებ;

- მონაცემთა დამუშავების საკითხებში პასუხისმგებლობის მკაფიო გადანაწილება და უფლებამოსილებათა ნათლად ჩამოყალიბება, განსაკუთრებით, როცა მიიღება გადაწყვეტილება პერსონალურ მონაცემთა დამუშავებაზე, ასევე, მესამე პირების ან მონაცემთა სუბიექტისათვის გადაცემაზე;

- პერსონალურ მონაცემთა გამოყენება მხოლოდ უფლებამოსილ პირთა მიერ დადგენილი ინსტრუქციების ან ზოგადი წესების შესაბამისად;

- დაცვა მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის ადგილმდებარეობასა და ტექნიკურ თუ პროგრამულ უზრუნველყოფაზე წვდომისაგან (მათ შორის, წვდომის ნებართვის შემოწმება);

- პერსონალურ მონაცემებზე წვდომის ნებართვის გაცემა მხოლოდ უფლებამოსილი პირის მიერ და შესაბამისი დოკუმენტაციის საფუძველზე;

- ელექტრონული საშუალებებით პერსონალურ მონაცემებზე წვდომის ავტომატიზებული წესები (პროტოკოლი) და შიდა საზედამხედველო ორგანოს მიერ მათი რეგულარული შემოწმება (შესაბამისად, მოთხოვნა დამუშავების ყველა აქტივობის აღრიცხვის შესახებ);

- მონაცემთა ავტომატიზებული წვდომის გარდა, სხვა ფორმების საგულდაგულოდ დოკუმენტირებაც, მონაცემთა გაცემის უკანონო ფორმათა არარსებობის საჩვენებლად.

თანამშრომელთათვის მონაცემთა დაცვის სათანადო ტრენინგებისა და განათლების მიწოდება უსაფრთხოების ეფექტიანი ზომების მნიშვნელოვანი ნაწილია. უნდა დაინერგოს ნამდვილობის დადასტურების პროცედურებიც, რათა შესაბამისი ზომები მხოლოდ ფურცელზე არ არსებობდეს და ეფექტიანად დაინერგოს პრაქტიკაშიც (მაგ.: შიდა და გარე აუდიტი).

მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის მიერ უსაფრთხოების გასაუმჯობესებლად მიღებული ზომები მოიცავს შემდეგ ინსტრუმენტებს: პერსონალურ მონაცემთა დაცვაზე პასუხისმგებელი პირები, დასაქმებულთა ტრენინგი უსაფრთხოების საკითხებზე, რეგულარული აუდიტი, ტესტები სისტემის შეღწევადობის შესახებ და ხარისხის ბეჭდები.

მაგალითი: საქმეში *I v. Finland*[442] განმცხადებელმა ვერ შეძლო დაედასტურებინა უკანონო წვდომა ჩანაწერზე მისი ჯანმრთელობის მდგომარეო-

442 ECtHR, *I v. Finland,* No. 20511/03, 2008 წლის 17 ივლისი.

ბის შესახებ, კერძოდ, იმ ჰოსპიტალის თანამშრომელთა მხრიდან, სადაც ის მუშაობდა. შესაბამისად, მისი საჩივარი მონაცემთა დაცვის უფლების დარღვევასთან დაკავშირებით ეროვნულმა სასამართლოებმა უარყვეს. ECtHR-მა დაადგინა კონვენციის მე-8 მუხლის დარღვევა, ვინაიდან ჯანმრთელობის მდგომარეობის შესახებ ჰოსპიტალის ფაილური რეესტრის სისტემა „არ იძლეოდა პაციენტთა შესახებ ჩანაწერების გამოყენების რეტროაქტიულად დადგენის საშუალებას: იგი ავლენდა წვდომის მხოლოდ ბოლო ხუთ ფაქტს და ეს ინფორმაცია იშლებოდა ფაილის არქივში დაბრუნებისთანავე.“ სასამართლომ გადამწყვეტად მიიჩნია ის, რომ ჰოსპიტალში არსებული ჩანაწერთა სისტემა არ შეესაბამებოდა ეროვნული კანონმდებლობის მოთხოვნებს, რაც ეროვნულმა სასამართლოებმა ჯეროვნად არ შეაფასეს.

ევროკავშირში მოქმედებს დირექტივა ქსელისა და ინფორმაციული უსაფრთხოების შესახებ (NIS დირექტივა), [443] რომელიც ევროკავშირის მასშტაბით მოქმედი პირველი ინსტრუმენტია კიბერუსაფრთხოების კუთხით. დირექტივის მიზანია, ერთი მხრივ, კიბერუსაფრთხოების გაუმჯობესება ეროვნულ დონეზე, ხოლო მეორე მხრივ, ევროკავშირის ფარგლებში თანამშრომლობის დონის გაღრმავება. იგი ვალდებულებებს უწესებს ძირითადი სერვისების ოპერატორებსა (მათ შორის, ენერგეტიკის, ჯანდაცვის, საბანკო, სატრანსპორტო, ციფრული ინფრასტრუქტურისა და ა.შ. სექტორებში) და ციფრული სერვისების მიმწოდებლებს, რათა მართონ რისკები, უზრუნველყონ თავიანთი ქსელისა და საინფორმაციო სისტემების უსაფრთხოება და ინციდენტები შეატყობინონ შესაბამის პირებს.

სამომავლო ხედვები

2017 წლის სექტემბერში ევროპულმა კომისიამ წარმოადგინა რეგულაციის პროექტი, რომელიც მიზნად ისახავდა ENISA-ს მანდატის რეფორმირებას, მისი ახალი უფლებამოსილებებისა და მოვალეობების გათვალისწინებით, NIS-ის დირექტივის შესაბამისად. შემოთავაზებული რეგულაციის მიზანია, განავითაროს ENISA-ს მოვალეობები და განამტკიცოს მისი, როგორც „ევროკავშირის კიბერუსაფრთხოების ეკოსისტემაში ათვლის წერტილის“ როლი.[444] შემოთავაზებული რეგულაცია არ გამორიცხავს GDPR-ის პრინციპებს

443 ევროპული პარლამენტის და საბჭოს 2016 წლის 6 ივლისის დირექტივა (EU) 2016/1148, რომელიც შეეხება ევროკავშირში ქსელისა და საინფორმაციო სისტემების მაღალი დონის უსაფრთხოებას, OJ 2016 L 194.

444 ევროპარლამენტისა და საბჭოს წინადადება ENISA-ს, „კიბერუსაფრთხოების სააგენტოს“ რეგულაციის შესახებ და რეგულაცია (EU) 526/2013, რომელიც აუქმებს მას; ასევე, საინფორმაციო და საკომუნიკაციო ტექნოლოგიის კიბერუსაფრთხოების სერტიფიცირების (კიბერუსაფრთხოების აქტის) შესახებ, COM(2017)477, 2017 წლის 13 სექტემბერი, გვ. 6.

და ევროპული კიბერუსაფრთხოების სერტიფიცირების სქემის აუცილებელი ელემენტების განმარტებით განამტკიცებს პერსონალურ მონაცემთა უსაფრთხოებას. პარალელურად, 2017 წლის სექტემბერში, ევროპულმა კომისიამ წარმოადგინა დამნერგავი რეგულაცია. დოკუმენტი მოიცავს იმ ელემენტებს, რომლებიც ციფრული მომსახურების მიმწოდებლებმა უნდა გაითვალისწინონ თავიანთი ქსელისა და საინფორმაციო სისტემების უსაფრთხოებისათვის, როგორც ამას მოითხოვს NIS-ის დირექტივის 16(8) მუხლი. ამ ორი რეგულაციის პროექტი სწორედ წინამდებარე სახელმძღვანელოზე მუშაობისას განიხილებოდა.

4.2.2 კონფიდენციალობა

ევროკავშირის კანონმდებლობაში GDPR პერსონალურ მონაცემთა კონფიდენციალობას ზოგადი პრინციპის ნაწილად მიიჩნევს.[445] საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს მოეთხოვებათ კონფიდენციალობისა და მომსახურების უსაფრთხოების დაცვა. [446]

მაგალითი: სადაზღვევო კომპანიის თანამშრომელს სამსახურში ტელეფონით უკავშირდება პირი, რომელიც კლიენტად ეცნობა და თავისი სადაზღვევო ხელშეკრულების შესახებ ინფორმაციას სთხოვს.

კლიენტთა მონაცემების კონფიდენციალობის ვალდებულებიდან გამომდინარე, სადაზღვევო კომპანიის თანამშრომელმა, პერსონალური მონაცემების გაცემამდე, მინიმალური ზომები მაინც უნდა მიიღოს. ეს შეიძლება მოიცავდეს კლიენტთან ხელმეორედ დაკავშირებას მის ფაილში მითითებულ ტელეფონის ნომერზე.

მე-5 მუხლის 1(ვ) პუნქტის თანახმად, პერსონალური მონაცემები უნდა დამუშავდეს იმგვარად, რომ სათანადო ტექნიკური ან ორგანიზაციული ზომების მეშვეობით, უზრუნველყონ მათი უსაფრთხოება. მონაცემები დაცული უნდა იყოს უკანონო და არაუფლებამოსილი პირების მხრიდან დამუშავების, დაკარგვის, განადგურების ან დაზიანებისგან („უსაფრთხოება და კონფიდენციალობა“).

32-ე მუხლის თანახმად, მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა უნდა მიიღონ სავარაუდო რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები, უსაფრთხოების მაღალი დონის უზრუნველსაყოფად. ეს ზომები მოიცავს შემდეგ ასპექტებს: მონაცემთა ფსევდონიმიზაცია და დაშიფვ-

445 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5(1)(ვ).

446 დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ, მუხლი 5 (1).

რა; დამუშავების მუდმივი კონფიდენციალობა, ხელშეუხებლობა, ხელმისაწვდომობა და მოქნილობა; შესაბამისი ზომების ეფექტიანობის შეფასება და შემოწმება; ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში, დამუშავების პროცესის დროული აღდგენა. ამასთან, დამტკიცებულ ქცევის კოდექსსა ან სერტიფიცირების დამტკიცებულ მექანიზმთან შესაბამისობა შესაძლოა გამოყენებულ იყოს მთლიანობისა და კონფიდენციალობის პრინციპის დაცვის სადემონსტრაციოდ. GDPR-ის 28-ე მუხლის თანახმად, მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის არსებული სავალდებულო ძალის მქონე კონტრაქტი უნდა ითვალისწინებდეს უფლებამოსილი პირის პასუხისმგებლობას, უზრუნველყოს კონფიდენციალობის ან კანონით განსაზღვრული შესაბამისი ვალდებულებების შესრულება დამუშავებაზე პასუხისმგებელ პირთა მხრიდან.

კონფიდენციალობის ვალდებულება არ ვრცელდება, თუ მონაცემებს მოიპოვებს კერძო პირი, და არა მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის თანამშრომელი. ასეთ დროს GDPR-ის 32-ე და 28-ე მუხლები არ მოქმედებს, რადგან კერძო პირთა მიერ პერსონალური მონაცემების გამოყენება მთლიანად სცდება რეგულაციის მოქმედების სფეროს, თუკი ის ხვდება ე.წ. ოჯახური გამონაკლისის ფარგლებში.[447] ოჯახური გამონაკლისი გულისხმობს პერსონალური მონაცემების გამოყენებას „ფიზიკური პირის მიერ, ცალსახად პირადი ან ოჯახური საქმიანობის ფარგლებში.“[448] *Bodil Lindqvist-ის* საქმეში[449] CJEU-ს მიერ მიღებული გადაწყვეტილების თანახმად, ეს გამონაკლისი ვიწროდ უნდა განიმარტოს, განსაკუთრებით, მონაცემთა გამჟღავნების კუთხით. კერძოდ, ე.წ. ოჯახური გამონაკლისი არ ვრცელდება: პერსონალურ მონაცემთა გამოქვეყნებაზე ინტერნეტში, როდესაც მონაცემების მიმღებთა რაოდენობა შეუზღუდავია; და მონაცემთა დამუშავებაზე, რომელსაც აქვს პროფესიული ან კომერციული ასპექტები (უფრო დეტალური ინფორმაციისათვის იხ. ნაწილები 2.1.2, 2.2.2 და 2.3.1).

კონფიდენციალობის კიდევ ერთი ასპექტია „კომუნიკაციების კონფიდენციალობა“, რომელიც სპეციალური ნორმით (*lex specialis*) რეგულირდება. ელექტრონულ სივრცეში პირადი ცხოვრების შესახებ დირექტივით გათვალისწინებული სპეციალური წესები, რომლებიც მიზნად ისახავს ელექტრონული კომუნიკაციების კონფიდენციალობას, წევრ სახელმწიფოებს ავალდებულებს, რომ ნებისმიერ პირს, გარდა მომხმარებლებისა, აუკრძალონ კომუნიკაციებისა და მასთან დაკავშირებული მეტამონაცემების მოსმენა, მიყურადება, შენახვა ან სხვა სახის წვდომა თუ მონიტორინგი, მომხმარებელთა

447 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 2(2)(გ).

448 *იქვე.*

449 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist,* 2003 წლის 6 ნოემბერი.

თანხმობის გარეშე.[450] ეროვნული კანონმდებლობა შესაძლოა უშვებდეს გარკვეულ გამონაკლისებს მხოლოდ და მხოლოდ ეროვნული უსაფრთხოების, თავდაცვის, ასევე, დანაშაულის პრევენციისა და გამოვლენის მიზნებით, თუკი ასეთი ზომები აუცილებელია და დასახული მიზნის პროპორციული.[451] ელექტრონულ სივრცეში პირადი ცხოვრების რეგულაცია იმავე წესებს ითვალისწინებს, თუმცა, სამართლებრივი აქტის მოქმედების სფეროს გაფართოების შედეგად, იგი გავრცელდება არა მხოლოდ საჯაროდ ხელმისაწვდომ ელექტრონულ კომუნიკაციებზე, არამედ OTT (over-the-top) სერვისებზეც (მაგ.: მობილური აპლიკაციები).

ევროპის საბჭოს სამართალში კონფიდენციალობის ვალდებულებას მოიცავს მონაცემთა უსაფრთხოების ცნება, რომელსაც განსაზღვრავს მოდერნიზებული 108-ე კონვენციის მე-7 მუხლის პირველი პუნქტი.

უფლებამოსილი პირების შემთხვევაში კონფიდენციალობის დაცვა ნიშნავს, რომ მათ ეკრძალებათ მონაცემთა გამჟღავნება მესამე პირების ან სხვა მიმღებებისთვის, შესაბამისი ნებართვის გარეშე; მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის თანამშრომლებისათვის კი ეს ცნება გულისხმობს პერსონალური მონაცემების გამოყენებას მხოლოდ უფლებამოსილი ხელმძღვანელი პირების ინსტრუქციათა შესაბამისად.

კონფიდენციალობა გათვალისწინებული უნდა იყოს მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის გაფორმებულ ნებისმიერ ხელშეკრულებაშიც. ამასთან, მონაცემთა დამმუშავებლებსა და უფლებამოსილ პირებს ეკისრებათ სპეციალური ზომების მიღების ვალდებულება, მათი თანამშრომლების მხრიდან კონფიდენციალობის სამართლებრივი მოთხოვნის შესასრულებლად. როგორც წესი, ეს ეყრდნობა დამსაქმებელსა და დასაქმებულს შორის არსებულ ხელშეკრულებაში განსაზღვრულ კონფიდენციალობის პირობებს.

ევროკავშირის არაერთ წევრ სახელმწიფოში და 108-ე კონვენციის ხელმომწერ ქვეყნებში კონფიდენციალობის პროფესიული მოვალეობის დარღვევა სისხლის სამართლის წესით ისჯება.

450 დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ, მუხლი 5(1).

451 *იქვე*, მუხლი 15(1).

4.2.3 შეტყობინება პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შესახებ

ასეთი დარღვევა გულისხმობს გადაცემული, შენახული ან სხვაგვარად დამუშავებული პერსონალური მონაცემების შემთხვევით ან უკანონო განადგურებას, დაკარგვას, შეცვლას, უკანონო გამჟღავნებას ან არასანქცირებულ წვდომას.[452] ახალი ტექნოლოგიები, როგორიცაა დაშიფვრა, მეტ შესაძლებლობას ქმნის დამუშავების უსაფრთხოების მხრივ, თუმცა, მონაცემთა უსაფრთხოების დარღვევა კვლავ გავრცელებულ ფენომენად რჩება. მისი მიზეზი შეიძლება იყოს ორგანიზაციაში მომუშავე ადამიანთა უნებლიე შეცდომები, ასევე, გარე საფრთხეები, როგორიცაა ჰაკერული და კიბერდანაშაულებრივი ორგანიზაციები.

მონაცემთა უსაფრთხოების დარღვევას შეიძლება ძალიან უარყოფითი გავლენა ჰქონდეს იმ პირთა პირადი ცხოვრებისა და მონაცემთა დაცვის უფლებაზე, რომელთაც უსაფრთხოების დარღვევის შედეგად დაკარგეს კონტროლი საკუთარ პერსონალურ მონაცემებზე. უსაფრთხოების დარღვევამ შეიძლება გამოიწვიოს პერსონალურ მონაცემთა მითვისება (identity theft) ან გაყალბება, ფინანსური დანაკარგი ან მატერიალური ზიანი, პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალობის დარღვევა და მონაცემთა სუბიექტის რეპუტაციის შელახვა. 29-ე მუხლის სამუშაო ჯგუფის სახელმძღვანელო პრინციპებში, რომლებიც შეეხება შეტყობინებას პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შესახებ, 2016/679 რეგულაციის თანახმად, განმარტებულია, რომ დარღვევამ შეიძლება გამოიწვიოს სამი სახის შედეგი: პერსონალური მონაცემების გამჟღავნება, დაკარგვა და/ან შეცვლა.[453] უსაფრთხოებისათვის საჭირო ზომების მიღებასთან ერთად, როგორც ეს 4.2 ნაწილშია განმარტებული, ასევე მნიშვნელოვანია დამმუშავებლის სათანადო და დროული რეაგირება მონაცემთა უსაფრთხოების დარღვევის შემთხვევაში.

ორგანოები და პირები, რომლებიც ზედამხედველობას ახორციელებენ, ხშირად არ ფლობენ ინფორმაციას მონაცემთა უსაფრთხოების დარღვევაზე, რაც ფიზიკურ პირებს ხელს უშლის გარკვეული ნაბიჯების გადადგმაში დარღვევის უარყოფითი შედეგებისგან თავდაცვის მხრივ. ფიზიკურ პირთა უფლებების განსამტკიცებლად და იმ უარყოფითი გავლენის შესამცირებლად, რომელსაც

452 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (12); ასევე, იხ. 29-ე მუხლის სამუშაო ჯგუფი (2017), სახელმძღვანელო პრინციპები პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შეტყობინებაზე 2016/679 რეგულაციის თანახმად, WP250, 2017 წლის 3 ოქტომბერი, გვ. 8.

453 29-ე მუხლის სამუშაო ჯგუფი (2017), სახელმძღვანელო პრინციპები პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შეტყობინებაზე 2016/679 რეგულაციის თანახმად, WP250, 2017 წლის 3 ოქტომბერი, გვ. 6.

იწვევს მონაცემთა უსაფრთხოების დარღვევა, ევროკავშირი და ევროპის საბჭო მონაცემთა დამმუშავებელს უწესებს შეტყობინების ვალდებულებას გარკვეულ გარემოებებში.

ევროპის საბჭოს მოდერნიზებული 108-ე კონვენციის თანახმად, ხელშემკვრელმა მხარეებმა მონაცემთა დამმუშავებლებს უნდა დააკისრონ ვალდებულება, რომ უსაფრთხოების დარღვევისას, სულ მცირე, „დაუყოვნებლივ“ გაუგზავნონ შეტყობინება კომპეტენტურ საზედამხედველო ორგანოს, თუკი ამ ფაქტმა შეიძლება მნიშვნელოვნად შელახოს მონაცემთა სუბიექტის უფლებები.[454]

ევროკავშირის კანონმდებლობა დეტალურ რეჟიმს ადგენს შეტყობინების შინაარსისა და გაგზავნის ვადების რეგულირებისათვის.[455] კერძოდ, მონაცემთა დამმუშავებელმა საზედამხედველო ორგანოს გარკვეული დარღვევები უნდა აცნობოს დაუყოვნებლივ, თუ შესაძლებელია, შეტყობიდან არაუგვიანეს 72 საათში. სხვა შემთხვევაში მას თან უნდა დაერთოს განმარტება დაყოვნების მიზეზებზე. ასეთი მოთხოვნა დამმუშავებელზე არ ვრცელდება, თუ იგი შეძლებს დადასტურებას, რომ მონაცემთა უსაფრთხოების დარღვევა, სავარაუდოდ, არ შეუქმნის საფრთხეს შესაბამის პირთა უფლებებსა და თავისუფლებებს.

რეგულაცია ითვალისწინებს იმ მინიმალურ ინფორმაციას, რომელსაც შეტყობინება უნდა შეიცავდეს, რათა საზედამხედველო ორგანომ შეძლოს საჭირო ქმედების განხორციელება.[456] კერძოდ: მონაცემთა უსაფრთხოების დარღვევის ბუნება; მონაცემთა სუბიექტების კატეგორიები და რაოდენობა; დარღვევის მოსალოდნელი შედეგები; მონაცემთა დამმუშავებლის მიერ მიღებული ზომები დარღვევის აღმოსაფხვრელად ან მისი შედეგების შესამცირებლად. ამასთან, შეტყობინებაში მითითებული უნდა იყოს მონაცემთა დაცვის ოფიცრის ან სხვა საკონტაქტო პირის ვინაობა, საკონტაქტო მონაცემებთან ერთად, რათა კომპეტენტურმა საზედამხედველო ორგანომ შეძლოს დამატებითი ინფორმაციის მიღება (საჭიროების შემთხვევაში).

თუ სავარაუდოა, რომ მონაცემთა უსაფრთხოების დარღვევა მნიშვნელოვან საფრთხეს შეუქმნის ფიზიკურ პირთა უფლებებსა და თავისუფლებებს, დამმუშავებელმა დაუყოვნებლივ უნდა შეატყობინოს მის შესახებ შესაბამის პირებს (მონაცემთა სუბიექტებს).[457] მონაცემთა სუბიექტებისთვის განკუთვნილი ინფორმაცია უნდა ჩამოყალიბდეს წერილობით, გასაგებ და მარტივ ენაზე, და

454 მოდერნიზებული 108-ე კონვენცია, მუხლი 7 (2); მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტები 64-66.

455 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 33 და 34.

456 *იქვე*, მუხლი 33 (3).

457 *იქვე*, მუხლი 34.

მოიცავდეს იმავე ცნობებს, რასაც საზედამხედველო ორგანოებისთვის წარსადგენი შეტყობინება. გამონაკლის შემთხვევებში, დამმუშავებელი თავისუფლდება შეტყობინების ვალდებულებისგან (მაგ.: როცა მას გატარებული აქვს სათანადო ტექნიკური და ორგანიზაციული ზომები, მათ შორის, იმ მონაცემებთან დაკავშირებით, რომლებსაც შეეხო დარღვევა და რომლებიც, ამ ზომების (მაგ.: დაშიფვრა) შედეგად, მიუწვდომელია ნებისმიერი არაუფლებამოსილი პირისთვის); დამმუშავებლი დარღვევის შემდგომაც განახორციელებს ქმედებას, რომელიც, დიდი ალბათობით, გამორიცხავს მაღალ რისკებს მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებთან მიმართებით. და ბოლოს, თუ შეტყობინება არაპროპორციულ ძალისხმევას მოითხოვს დამმუშავებლის მხრიდან, მონაცემთა სუბიექტების ინფორმირება დარღვევის შესახებ ნებადართულია სხვა საშუალებებითაც (მაგ.: საჯარო კომუნიკაცია ან მსგავსი გზები). [458]

მონაცემთა უსაფრთხოების დარღვევის საზედამხედველო ორგანოებისა და მონაცემთა სუბიექტებისთვის შეტყობინების ვალდებულება ეკისრება მონაცემთა დამმუშავებელს. თუმცა, უსაფრთხოება შეიძლება დაირღვეს როგორც მონაცემთა დამმუშავებლის, ისე უფლებამოსილი პირის შემთხვევაში. ამის გამო, დარღვევის შეტყობინების ვალდებულება უნდა ვრცელდებოდეს უფლებამოსილ პირზეც და ასეთი შემთხვევა დაუყოვნებლივ შეატყობინოს დამმუშავებელს.[459] ეს უკანასკნელი, თავის მხრივ, ვალდებულია, დარღვევა აცნობოს საზედამხედველო ორგანოებსა და მონაცემთა სუბიექტებს, ზემოაღნიშნული წესებითა და ვადებით.

4.3 წესები ანგარიშვალდებულებისა და შესაბამისობის ხელშეწყობისთვის

ძირითადი საკითხები

- პერსონალურ მონაცემთა დამუშავების პროცესში ანგარიშვალდებულების უზრუნველსაყოფად, მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ვალდებულნი არიან, აწარმოონ ჩანაწერები საკუთარი მოვალეობების ფარგლებში შესრულებულ სამუშაოზე და, მოთხოვნის შემთხვევაში, გადასცენ საზედამხედველო ორგანოებს.

- შესაბამისობის ხელშესაწყობად, მონაცემთა დაცვის ზოგადი რეგულაცია ითვალისწინებს რამდენიმე ინსტრუმენტს:

458 *იქვე*, მუხლი 34(3)(გ).

459 *იქვე*, მუხლი 33 (2).

- მონაცემთა დაცვის ოფიცრის დანიშვნა გარკვეულ სიტუაციებში;
- როდესაც სავარაუდოა, რომ კონკრეტული ტიპის დამუშავება სერიოზულ საფრთხეს შეუქმნის ფიზიკურ პირთა უფლებებსა და თავისუფლებებს, დამმუშავებელს დაევალოს მონაცემთა დაცვის რისკების შეფასება;
- წინასწარი კონსულტაციის გავლა შესაბამის საზედამხედველო ორგანოსთან, თუკი მონაცემთა დაცვის რისკების შეფასების თანახმად, დამუშავება შექმნის შეუქცევად საფრთხეებს, რომელთა აღმოფხვრაც შეუძლებელია;
- მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ქცევის კოდექსის შექმნა, რომელიც დეტალურად მიმოიხილავს რეგულაციის გამოყენებას დამუშავების სხვადასხვა სფეროში;
- სერტიფიცირების მექანიზმები, მონაცემთა დაცვის ბეჭდები და ნიშნები.

- ევროპის საბჭოს კანონმდებლობა მსგავს ინსტრუმენტებს ითვლისწინებს მოდერნიზებულ 108-ე კონვენციასთან შესაბამისობის მხრივაც.

ანგარიშვალდებულების პრინციპი განსაკუთრებით მნიშვნელოვანია ევროპაში მონაცემთა დაცვის წესების აღსრულებისათვის. დამმუშავებელი პასუხისმგებელია მონაცემთა დაცვის წესებთან შესაბამისობაზე და უნდა შეძლოს დადასტურება, რომ უზრუნველყოფს მას. ანგარიშვალდებულება მხოლოდ დარღვევის შემდგომ არ უნდა გააქტიურდეს, მონაცემთა დამმუშავებელს ეკისრება პროაქტიული ვალდებულება, რომ მონაცემთა მართვის შესაბამისი პრინციპები დაიცვას დამუშავების ყველა ეტაპზე. მონაცემთა დაცვის ეროვნული კანონმდებლობა დამმუშავებელს ავალდებულებს სათანადო ტექნიკური და ორგანიზაციული ზომების შემუშავებას, რათა შეძლოს დადასტურება, რომ დამუშავება ხორციელდება კანონის შესაბამისად. ესენია: მონაცემთა დაცვის ოფიცრების დანიშვნა, დამუშავებასთან დაკავშირებული ჩანაწერებისა და დოკუმენტაციის შენახვა და მონაცემთა დაცვის რისკების შეფასება.

4.3.1 მონაცემთა დაცვის ოფიცრები

მონაცემთა დაცვის ოფიცერი (DPO) არის პირი, რომელიც დამმუშავებელ ორგანიზაციას აწვდის რჩევებს მონაცემთა დაცვის წესებთან შესაბამისობაზე. ის „ანგარიშვალდებულების ქვაკუთხდია“, ვინაიდან ხელს უწყობს შესაბამისობას და, ამავდროულად, მოქმედებს, როგორც შუამავალი საზედამხედველო ორგანოებს, მონაცემთა სუბიექტებსა და დამნიშნავ ორგანიზაციას შორის.

ევროპის საბჭოს სამართალში მოდერნიზებული 108-ე კონვენცია ანგარიშვალდებულების ზოგად პასუხისმგებლობას აკისრებს მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს. კერძოდ, მათ მოეთხოვებათ ყველა შესაბამისი ზომის მიღება, რათა შეასრულონ კონვენციით გათვალისწინებული მონაცემთა დაცვის წესები და შეძლონ დამტკიცება, რომ მათ კონტროლქვეშ მონაცემთა დამუშავება შეესაბამება კონვენციის დებულებებს. მიუხედავად იმისა, რომ კონვენცია არ აკონკრეტებს ზომებს, რომლებიც მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა უნდა მიიღონ, მის განმარტებით ბარათში აღნიშნულია, რომ მონაცემთა დაცვის ოფიცრის დანიშვნა ერთ-ერთი შესაძლო ღონისძიებაა შესაბამისობის დასადასტურებლად. მონაცემთა დაცვის ოფიცერი უზრუნველყოფილი უნდა იყოს ყველა საშუალებით, რომლებიც აუცილებელია მისი მანდატის განსახორციელებლად.[460]

ევროპის საბჭოს კანონმდებლობისგან განსხვავებით, ევროკავშირში მონაცემთა დაცვის ოფიცერი ყოველთვის მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის შეხედულებისამებრ არ ინიშნება, გარკვეულ პირობებში ეს აუცილებლობაა. GDPR-ის თანახმად, მონაცემთა დაცვის ოფიცერს წამყვანი როლი აქვს მართვის ახალ სისტემაში. რეგულაცია დეტალურ დებულებებს შეიცავს ოფიცრის დანიშვნასთან, თანამდებობასთან, მოვალეობასა და ამოცანებთან დაკავშირებით.[461]

GDPR-ის თანახმად, მონაცემთა დაცვის ოფიცრის დანიშვნა სავალდებულოა 3 შემთხვევაში: როდესაც მონაცემებს ამუშავებს სახელმწიფო უწყება ან ორგანო; მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის ძირითადი საქმიანობა მოიცავს მონაცემთა სუბიექტების რეგულარულ და სისტემატურ მონიტორინგს ფართო მასშტაბებით; მათი ძირითადი საქმიანობაა განსაკუთრებული კატეგორიის მონაცემთა ფართომასშტაბიანი დამუშავება ან პირის ნასამართლობასა და სისხლის სამართლის დანაშაულთან დაკავშირებული მონაცემების დამუშავება.[462] მიუხედავად იმისა, რომ ტერმინები, როგორიცაა „ფართომასშტაბიანი სისტემატური მონიტორინგი“ და „ძირითადი საქმიანობა,“ რეგულაციაში არ არის განმარტებული, 29-ე მუხლის სამუშაო ჯგუფმა გამოსცა სახელმძღვანელო პრინციპები მათი ინტერპრეტაციის შესახებ. [463]

მაგალითი: სოციალური მედიაკომპანიები და საძიებო სისტემები არიან ისეთი კატეგორიის დამმუშავებლები, რომლებიც დამუშავების პროცესში

460 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 87.

461 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 37–39.

462 *იქვე*, მუხლი 37 (1).

463 29-ე მუხლის სამუშაო ჯგუფი (2017), სახელმძღვანელო პრინციპები მონაცემთა დაცვის ოფიცრების შესახებ, (‘DPOs’), WP 243 rev.01, ბოლოს გადაიხედა და დამტკიცდა 2017 წლის 5 აპრილს.

ახორციელებენ მონაცემთა სუბიექტების ფართომასშტაბიან, რეგულარულ და სისტემატურ მონიტორინგს. ასეთი კომპანიების ბიზნესმოდელი ეფუძნება დიდი მოცულობის პერსონალურ მონაცემთა დამუშავებას. ისინი დიდ შემოსავალს იღებენ მიზნობრივი სარეკლამო მომსახურების შეთავაზებით, ასევე იმით, რომ კომპანიებს თავიანთ ვებგვერდებზე რეკლამების განთავსების შესაძლებლობას აძლევენ. მიზნობრივი რეკლამა გულისხმობს რეკლამის განთავსებას დემოგრაფიის, ასევე, მომხმარებელთა მსყიდველობითი ისტორიისა და ქცევის საფუძველზე, რაც საჭიროებს სისტემატურ მონიტორინგს მონაცემთა სუბიექტების ონლაინჩვევებსა და ქცევაზე.

მაგალითი: საავადმყოფო და სადაზღვევო კომპანია იმ დამმუშავებელთა ტიპური მაგალითებია, რომელთა საქმიანობაც მოიცავს განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა ფართომასშტაბიან დამუშავებას. მონაცემები, რომლებიც ამჟღავნებს ინფორმაციას ფიზიკური პირის ჯანმრთელობის შესახებ, განსაკუთრებული კატეგორიის მონაცემებად მიიჩნევა, როგორც ევროპის საბჭოს, ისე ევროკავშირის კანონმდებლობით. ამრიგად, ამ ტიპის მონაცემები გაძლიერებულ დაცვას საჭიროებს. ევროკავშირის კანონმდებლობა განსაკუთრებული კატეგორიის მონაცემებად აღიარებს გენეტიკურ და ბიომეტრიულ ინფორმაციას.

რაც შეეხება ასეთი მონაცემების ფართომასშტაბიან დამუშავებას სამედიცინო დაწესებულებებისა და სადაზღვევო კომპანიების მიერ, GDPR-ის თანახმად, მათ მოეთხოვებათ მონაცემთა დაცვის ოფიცრის დანიშვნა.

ამასთან, GDPR-ის 37-ე მუხლის მე-4 პუნქტის თანახმად, პირველ პუნქტში მითითებული შემთხვევების გარდა, მონაცემთა დამმუშავებელმა, უფლებამოსილმა პირმა ან ასოციაციებმა - ანდა სხვა უწყებებმა, რომლებიც დამმუშავებელთა ან უფლებამოსილ პირთა გარკვეულ კატეგორიებს წარმოადგენენ - მონაცემთა დაცვის ოფიცერი შეიძლება დანიშნონ ნებაყოფლობით, ან ევროკავშირისა თუ მისი წევრი სახელმწიფოს კანონმდებლობის მიხედვით.

მონაცემთა დაცვის ოფიცრის დანიშვნა ყველა დანარჩენ ორგანიზაციებს კანონით არ მოეთხოვებათ. თუმცა, GDPR-ის მიხედვით, მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს მისი დანიშვნა ნებაყოფლობით შეუძლიათ. ამასთან, რეგულაცია წევრ სახელმწიფოებს აძლევს შესაძლებლობას, რომ მონაცემთა დაცვის ოფიცრის დანიშვნა სხვა კატეგორიის ორგანიზაციებისთვისაც სავალდებულო გახდეს.[464]

დამმუშავებელმა, მას შემდეგ, რაც დანიშნავს მონაცემთა დაცვის ოფიცერს, უნდა უზრუნველყოს „მისი სათანადო და დროული ჩართულობა პერსონალურ

464 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 37(3)(4).

მონაცემთა დაცვასთან დაკავშირებულ ყველა საკითხში.“[465] მაგალითად, მონაცემთა დაცვის ოფიცერი უნდა მონაწილეობდეს რჩევების მიცემაში რისკების შეფასების შესახებ, ასევე, დამუშავებასთან დაკავშირებული ჩანაწერების წარმოებაში. მონაცემთა დაცვის ოფიცრის მიერ მასზე დაკისრებულ მოვალეობათა ეფექტიანად შესრულებისათვის, დამმუშავებელი და უფლებამოსილი პირი ვალდებულნი არიან, იგი უზრუნველყონ აუცილებელი (მათ შორის, ფინანსური) რესურსებით, ინფრასტრუქტურითა და მოწყობილობით. დამატებითი მოთხოვნები ეხება საკმარისი დროის გამოყოფას ფუნქციების შესასრულებლად, ასევე, განგრძობით ტრენინგებს ექსპერტული ცოდნის გასაღრმავებლად და განახლებული ინფორმაციის მისაღებად მონაცემთა დაცვის კანონმდებლობაში განხორციელებულ ცვლილებებზე. [466]

GDPR გარკვეულ მოთხოვნებს აწესებს მონაცემთა დაცვის ოფიცრის დამოუკიდებლობისთვისაც. კერძოდ, დამმუშავებელმა და უფლებამოსილმა პირმა უნდა უზრუნველყონ, რომ მონაცემთა დაცვასთან დაკავშირებული მოვალეობების შესრულებისას, დაცვის ოფიცერმა არ მიიღოს რაიმე ინსტრუქციები კომპანიიდან, მათ შორის, უმაღლესი რგოლის ხელმძღვანელობისგან. ამასთან, დაუშვებელია ოფიცრის სამსახურიდან დათხოვნა ან რაიმე ფორმით დასჯა საკუთარი მოვალეობების შესრულების გამო.[467] მაგალითისათვის განვიხილოთ ასეთი შემთხვევა: მონაცემთა დაცვის ოფიცერი დამმუშავებელს ან უფლებამოსილ პირს ურჩევს რისკების შეფასებას, რადგან ვარაუდობს, რომ მონაცემთა დამუშავება მნიშვნელოვან საფრთხეს შეუქმნის მონაცემთა სუბიექტებს. კომპანია ოფიცრის მოსაზრებას არ ეთანხმება და მიაჩნია, რომ მისი პოზიცია საფუძველს მოკლებულია. საბოლოოდ, კომპანია გადაწყვეტს, არ შეაფასოს რისკები. მას შეუძლია, არ გაითვალისწინოს მონაცემთა დაცვის ოფიცრის რჩევა, მაგრამ უფლება არ აქვს, ამის გამო ოფიცერი სამსახურიდან გაათავისუფლოს, ან დასაჯოს/დააჯარიმოს.

და ბოლოს, მონაცემთა დაცვის ოფიცრის ამოცანები და მოვალეობები დეტალურად არის წარმოდგენილი GDPR-ის 39-ე მუხლში, მათ შორისაა: კანონმდებლობით დადგენილი ვალდებულებების გაცნობა და რჩევების მიცემა კომპანიებისა და თანამშრომლებისთვის, რომლებიც მონაცემებს ამუშავებენ; და მონიტორინგი ევროკავშირის ან წევრი სახელმწიფოების კანონმდებლობით დადგენილი შესაბამისი წესების შესრულებაზე, რაც შეიძლება განხორციელდეს აუდიტითა და მონაცემთა დამუშავებაში ჩართული თანამშრომლების ტრენინგის საშუალებით. მონაცემთა დაცვის ოფიცერმა უნდა ითანამშრომლოს საზედამხედველო ორგანოსთანაც. ამ შემთხვევაში მან მთავარი საკო-

465 *იქვე*, მუხლი 38 (1).

466 29-ე მუხლის სამუშაო ჯგუფი (2017), სახელმძღვანელო პრინციპები მონაცემთა დაცვის ოფიცრების შესახებ, (‘DPOs’), WP 243 rev.01, ბოლოს გადაიხედა და დამტკიცდა 2017 წლის 5 აპრილს, პუნქტი 3.1.

467 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 38(2)(3).

ნტაქტო პირის ფუნქცია უნდა შეასრულოს მონაცემთა დამუშავების ისეთ საკითხებზე, როგორიცაა, მაგალითად, მონაცემთა უსაფრთხოების დარღვევა.

რაც შეეხება ევროკავშირის ინსტიტუტებისა და ორგანოების ხელთ არსებულ მონაცემებს, 45/2001 რეგულაციის თანახმად, თითოეულმა ინსტიტუტმა და ორგანომ უნდა დანიშნოს მონაცემთა დაცვის ოფიცერი. მას ევალება: კონტროლი რეგულაციის დებულებათა სწორად გამოყენებაზე ევროკავშირის ინსტიტუტებისა და ორგანოების მიერ; მონაცემთა სუბიექტისა და დამმუშავებლის ინფორმირება მათ უფლებებსა და მოვალეობებზე;[468] პასუხის გაცემა EDPS-ის მოთხოვნებზე და, საჭიროების შემთხვევაში, მასთან თანამშრომლობა. GDPR-ის მსგავსად, 45/2001 რეგულაცია შეიცავს დებულებებს მონაცემთა დაცვის ოფიცრის დამოუკიდებლობაზე მოვალეობათა შესრულების პროცესში, ასევე, ვალდებულებას მისი საჭირო თანამშრომლებითა და რესურსებით უზრუნველყოფის შესახებ.[469] ევროკავშირის ინსტიტუტი ან ორგანო (ან მათი რომელიმე დეპარტამენტი), დამუშავების ნებისმიერი ოპერაციის განხორციელებამდე, ვალდებულია, მონაცემთა დაცვის ოფიცერს გაუგზავნოს შესაბამისი შეტყობინება. მათ უნდა აწარმოონ იმ ოპერაციების რეესტრიც, რომელთა შესახებაც აცნობეს მონაცემთა დაცვის ოფიცერს.[470]

4.3.2 დამუშავების საქმიანობის აღრიცხვა

შესაბამისობის დასადასტურებლად და ანგარიშვალდებულების გამო, კომპანიებს ხშირად კანონმდებლობით ეკისრებათ თავიანთი საქმიანობის დოკუმენტირება და აღრიცხვა. ამის მნიშვნელოვანი მაგალითია საგადასახადო კანონმდებლობა და აუდიტი, რომელიც ყველა კომპანიას ავალდებულებს ვრცელი დოკუმენტაციისა და ჩანაწერების წარმოებას. სამართლის სხვა სფეროებში, კერძოდ, მონაცემთა დაცვის სამართალში, იმავე მოთხოვნების დადგენა მნიშვნელოვანია, რადგან ჩანაწერების წარმოება არსებითად უწყობს ხელს მონაცემთა დაცვის წესებთან შესაბამისობას. **ევროკავშირის კანონმდებლობით,** მონაცემთა დამმუშავებელი ან მისი წარმომადგენელი ვალდებულია, აღრიცხოს მისი უფლებამოსილების ფარგლებში განხორციელებული ნებისმიერი დამუშავება.[471] ამ ვალდებულების მიზანია, საჭიროების შემთხვევაში, საზედამხედველო ორგანომ მიიღოს დამუშავების კანონიერების დასადგენად საჭირო დოკუმენტები.

468 იხ. (EC) No. 45/2001 რეგულაციის მუხლი 24 (1), სადაც წარმოდგენილია მონაცემთა დაცვის ოფიცერთა ფუნქციების სრული ჩამონათვალი.

469 რეგულაცია (EC) No. 45/2001, მუხლი 24(6)(7).

470 *იქვე*, მუხლები 25 და 26.

471 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 30.

ჩანაწერები უნდა შეიცავდეს შემდეგ ინფორმაციას:

- მონაცემთა დამმუშავებლის, ერთობლივი დამმუშავებლის, დამმუშავებლის წარმომადგენლის, ან მონაცემთა დაცვის ოფიცრის სახელი და საკონტაქტო ინფორმაცია;
- დამუშავების მიზნები;
- მონაცემთა სუბიექტის და პერსონალურ მონაცემთა კატეგორიები;
- მონაცემთა მიმღების კატეგორიები, ვისთვისაც გამჟღავნდა/გამჟღავნდება პერსონალური მონაცემები;
- ინფორმაცია მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციისთვის მონაცემთა გადაცემის შესახებ;
- თუ შესაძლებელია, სხვადასხვა კატეგორიის პერსონალურ მონაცემთა წაშლის ვადები; ასევე, დამუშავების უსაფრთხოებისთვის შემუშავებული ტექნიკური და ორგანიზაციული ზომების ზოგადი აღწერილობა. [472]

GDPR-ით გათვალისწინებული ვალდებულება დამუშავების აქტივობათა აღრიცხვის შესახებ ვრცელდება არა მხოლოდ მონაცემთა დამმუშავებელზე, არამედ უფლებამოსილ პირზეც. ეს მნიშვნელოვანი პროგრესია, ვინაიდან, რეგულაციის მიღებამდე, მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის დადებული ხელშეკრულება, ძირითადად, ითვალისწინებდა უფლებამოსილი პირის მოვალეობებს. ამჟამად კანონმდებლობა პირდაპირ განსაზღვრავს დამმუშავებლის მოვალეობასაც ჩანაწერების წარმოებასთან დაკავშირებით.

აღნიშნულ ვალდებულებასთან დაკავშირებით, GDPR-ით დაშვებულია გამონაკლისიც. აღრიცხვის ვალდებულება არ ვრცელდება საწარმოსა ან ორგანიზაციაზე (მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი), სადაც დასაქმებულია 250-ზე ნაკლები ადამიანი, გარდა იმ შემთხვევებისა, როდესაც: ამ კომპანიის მიერ მონაცემთა დამუშავებამ შეიძლება საფრთხე შეუქმნას მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებს; საქმე ეხება რეგულარულ (და არა პერიოდულ) დამუშავებას; ან კომპანია ამუშავებს მე-9 მუხლის პირველი პუნქტით დადგენილ განსაკუთრებული კატეგორიის მონაცემებს, მათ შორის, მე-10 მუხლით განსაზღვრულ ნასამართლობასა და სისხლისსამართლებრივ დანაშაულებთან დაკავშირებით.

დამუშავების შესახებ ჩანაწერების წარმოება მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს საშუალებას მისცემს, რომ დაადასტურონ რეგულაციას-

472 *იქვე*, მუხლი 30(1).

თან შესაბამისობა. ამასთან, საზედამხედველო ორგანოები შეძლებენ დამუშავების კანონიერების კონტროლს. თუ საზედამხედველო ორგანო მოითხოვს ამ ჩანაწერებზე წვდომას, მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ვალდებულნი არიან, ითანამშრომლონ მასთან და წარუდგინონ ჩანაწერები.

4.3.3 მონაცემთა დაცვის რისკების შეფასება და წინასწარი კონსულტაცია

დამუშავების ოპერაციები მათთვის დამახასიათებელ საფრთხეს უქმნის ფიზიკურ პირთა უფლებებს. შესაძლოა, პერსონალური მონაცემები დაიკარგოს, გადაეცეს არაუფლებამოსილ მხარეებს, ან უკანონოდ დამუშავდეს. ბუნებრივია, რისკები განსხვავდება და დამოკიდებულია დამუშავების ბუნებასა და მასშტაბზე. ფართომასშტაბიანი ოპერაციები, რომლებიც, მაგალითად, განსაკუთრებული კატეგორიის მონაცემთა დამუშავებას ითვალისწინებს, უფრო მაღალ რისკებს წარმოქმნის მონაცემთა სუბიექტებისათვის, ვიდრე საკუთარი თანამშრომლების მისამართებისა და პირადი ტელეფონის ნომრების დამუშავება მცირე კომპანიის მიერ.

ახალი ტექნოლოგიების განვითარებასთან ერთად, დამუშავება სულ უფრო და უფრო კომპლექსური ხდება. ამის გამო, მონაცემთა დამმუშავებელი ვალდებულია, რისკებზე რეაგირების მიზნით, ოპერაციის დაწყებამდე შეაფასოს დამუშავების შესაძლო გავლენა. ეს ორგანიზაციას უქმნის რისკების სათანადოდ გამოვლენის, მათზე რეაგირებისა და მათი შემცირების საშუალებას, რაც მნიშვნელოვნად ზღუდავს უარყოფით ზეგავლენას ფიზიკურ პირებზე.

მონაცემთა დაცვის რისკების შეფასებას ითვალისწინებს როგორც ევროპის საბჭოს, ისე ევროკავშირის კანონმდებლობა. ევროპის საბჭოს საკანონმდებლო ჩარჩოში, მოდერნიზებული 108-ე კონვენციის მე-10 მუხლის მე-2 პუნქტის თანახმად, ხელშემკვრელ მხარეებს მოეთხოვებათ, რომ მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა შეაფასონ შესაძლო რისკები, რომლებსაც მონაცემთა დამუშავება უქმნის მონაცემთა სუბიექტის უფლებებსა და ფუნდამენტურ თავისუფლებებს. ასეთი შეფასება დამუშავების დაწყებამდე უნდა განხორციელდეს, ხოლო შეფასების შემდეგ შემუშავდეს ისეთი მოდელი, რომლითაც შესაძლებელი იქნება დამუშავებასთან დაკავშირებული რისკების პრევენცია ან მინიმუმამდე შემცირება.

ევროკავშირის კანონმდებლობა იმავე, ოღონდ უფრო დეტალურ ვალდებულებას აკისრებს მონაცემთა დამმუშავებელს GDPR-ის მოქმედების ფარგლებში. კერძოდ, რეგულაციის 35-ე მუხლის თანახმად, თუ შესაძლებელია, რომ დამუშავებამ სერიოზული საფრთხე შეუქმნას ფიზიკურ პირთა უფლებებსა და თავისუფლებებს, მონაცემთა დამმუშავებელმა უნდა შეაფასოს დაგეგმილი დამუშავების რისკები. რეგულაცია არ განმარტავს, როგორ უნდა შეფასდეს

ეს რისკები, თუმცა, მიუთითებს მათზე.[473] კერძოდ, რეგულაციის თანახმად, რისკების შეფასება განსაკუთრებით მნიშვნელოვანია, როდესაც:

- პერსონალური მონაცემები მუშავდება ფიზიკურ პირებთან დაკავშირებული გადაწყვეტილებების მისაღებად, ინდივიდთა პიროვნული ასპექტების სისტემატური და ფართომასშტაბიანი შეფასების შედეგად (პროფილირება);

- მუშავდება განსაკუთრებული კატეგორიის მონაცემები ან საქმე ეხება პერსონალურ მონაცემთა ფართომასშტაბიან დამუშავებას, ნასამართლობასა ან სისხლის სამართლის დანაშაულთან დაკავშირებით;

- დამუშავება მოიცავს საჯარო სივრცის ფართომასშტაბიან, სისტემატურ მონიტორინგს.

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ უნდა შექმნას და გამოაქვეყნოს დამუშავების აქტივობათა სია, რომლებიც შეიძლება შეფასდეს რისკების მხრივ. შესაძლებელია, განისაზღვროს ის მოქმედებებიც, რომლებზეც ასეთი ვალდებულება არ ვრცელდება. [474]

თუ რისკების შეფასება აუცილებელია, მონაცემთა დამმუშავებელს ევალება, შეაფასოს დამუშავების აუცილებლობა და პროპორციულობა, ასევე, ფიზიკურ პირთა უფლებების შელახვის საფრთხეები. რისკების შეფასება უნდა მოიცავდეს უსაფრთხოების ღონისძიებათა დაგეგმვას გამოვლენილ საფრთხეებზე რეაგირების მიზნით. ჩამონათვალის განსაზღვრისას, წევრ სახელმწიფოთა საზედამხედველო ორგანოებს მოეთხოვებათ ერთმანეთსა და ევროკავშირის მონაცემთა დაცვის საბჭოსთან თანამშრომლობა. თანამშრომლობის მიზანია ევროკავშირის მასშტაბით თანმიმდევრული მიდგომის არსებობა იმ ოპერაციებთან დაკავშირებით, რომლებიც რისკების შეფასებას საჭიროებს, მონაცემთა დამმუშავებლებზე კი ერთი და იგივე მოთხოვნები ვრცელდება, მიუხედავად ადგილმდებარეობისა.

თუ რისკების შეფასების შემდეგ გამოვლინდება ფიზიკურ პირთა უფლებების შელახვის საფრთხე და მის აღმოსაფხვრელად სათანადო ღონისძიება ჯერ არ შემუშავებულა, მონაცემთა დამმუშავებელი ვალდებულია, ოპერაციის დაწყებამდე კონსულტაცია გაიაროს შესაბამის საზედამხედველო ორგანოსთან. [475]

---

473 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 75.

474 *იქვე*, მუხლები 35 (4) და (5).

475 იქვე, მუხლი 36 (1); 29-ე მუხლის სამუშაო ჯგუფი (2017), 2016/679 რეგულაციის მიზნებისთვის, მონაცემთა დაცვის რისკების შეფასებისა (DPIA) და მონაცემთა დამუშავებით გამოწვეული შესაძლო მაღალი რისკის განსაზღვრის სახელმძღვანელო პრინციპები, WP 248 rev.01, ბიუსელი, 2017 წლის 4 ოქტომბერი.

29-ე მუხლის სამუშაო ჯგუფმა გამოაქვეყნა მონაცემთა დაცვის რისკების შეფასების სახელმძღვანელო პრინციპები, ასევე, როგორ უნდა განისაზღვროს მონაცემთა დამუშავების მაღალი რისკები.[476] იმის დასადგენად, საჭიროა თუ არა მონაცემთა დაცვის რისკების შეფასება კონკრეტულ შემთხვევაში, სამუშაო ჯგუფმა შეიმუშავა 9 კრიტერიუმი:[477] (1) შეფასება ანუ ქულების მინიჭება; (2) ისეთი გადაწყვეტილებების ავტომატური მიღება, რომლებიც ფიზიკური პირისთვის იწვევს სამართლებრივ შედეგებს, ან მსგავს მნიშვნელოვან გავლენას; (3) სისტემატური მონიტორინგი; (4) განსაკუთრებული კატეგორიის მონაცემები; (5) მონაცემთა ფართომასშტაბიანი დამუშავება; (6) მონაცემები, რომლებიც დაწყვილდა ან კომბინირებულია; (7) ინფორმაცია მონაცემთა მოწყვლადი სუბიექტების შესახებ; (8) ინოვაციური გამოყენება ან ტექნოლოგიური თუ ორგანიზაციული გადაჭრის გზების დანერგვა; (9) როდესაც დამუშავება „მონაცემთა სუბიექტებს არ აძლევს უფლებით სარგებლობის ან მომსახურებისა თუ ხელშეკრულების გამოყენების შესაძლებლობას“. 29-ე მუხლის სამუშაო ჯგუფის მიერ დადგენილი საერთო წესის თანახმად, დამუშავების ოპერაციები, რომლებიც ორზე ნაკლებ კრიტერიუმს აკმაყოფილებს, ქმნის საფრთხის დაბალ დონეს და არ საჭიროებს მონაცემთა დაცვის რისკების შეფასებას, ხოლო ორი ან მეტი კრიტერიუმის დაკმაყოფილების შემთხვევაში, ასეთი შეფასება საჭიროა. თუ მონაცემთა დაცვის რისკების შეფასების აუცილებლობა ბუნდოვანია, 29-ე მუხლის სამუშაო ჯგუფის რეკომენდაციით, შეფასება მაინც უნდა ჩატარდეს, ვინაიდან ის „სასარგებლო ინსტრუმენტია, რომელიც მონაცემთა დამმუშავებელს ეხმარება მონაცემთა დაცვის კანონმდებლობის დაცვაში.“[478] მონაცემთა დამუშავების ახალი ტექნოლოგიის დანერგვისას, მონაცემთა დაცვის რისკების შეფასება აუცილებელია.[479]

4.3.4 ქცევის კოდექსები

ქცევის კოდექსები გამოიყენება ინდუსტრიის სხვადასხვა სექტორში, ამ სფეროებში GDPR-ის გამოყენების აღწერისა და დეტალურად განსაზღვრის მიზნით. პერსონალურ მონაცემთა დამმუშავებლებისა და უფლებამოსილი პირებისთვის ასეთი კოდექსის შექმნა მნიშვნელოვნად გააუმჯობესებს ევროკავშირის მონაცემთა დაცვის წესებთან შესაბამისობას და მათ დანერგვას. კონკრეტული სექტორის წევრთა ექსპერტული ცოდნა და გამოცდილება ხელს შე-

476 29-ე მუხლის სამუშაო ჯგუფი (2017), 2016/679 რეგულაციის მიზნებისთვის, მონაცემთა დაცვის რისკების შეფასებისა (DPIA) და მონაცემთა დამუშავებით გამოწვეული შესაძლო მაღალი რისკის განსაზღვრის სახელმძღვანელო პრინციპები, WP 248 rev.01, ბიუსელი, 2017 წლის 4 ოქტომბერი.

477 *იქვე*, გვ. 9–11.

478 *იქვე*, გვ. 9.

479 *იქვე*.

უწყობს გადაჭრის პრაქტიკული და, შესაბამისად, ადვილად შესასრულებელი გზების იდენტიფიცირებას. GDPR აღიარებს, რომ ასეთ კოდექსებს მნიშვნელოვანი როლი აქვთ მონაცემთა დაცვის კანონმდებლობის ეფექტიან გამოყენებაში. იგი წევრ სახელმწიფოებს, საზედამხედველო ორგანოებს, კომისიასა და ევროკავშირის მონაცემთა დაცვის საბჭოს მოუწოდებს, წაახალისონ ქცევის კოდექსის შემუშავება, რათა ხელი შეუწყონ რეგულაციის სათანადოდ დანერგვას ევროკავშირში.[480] კოდექსი შესაძლოა დეტალურად აღწერდეს კონკრეტულ სექტორში რეგულაციის გამოყენებას, მათ შორის, ისეთ საკითხებს, როგორიცაა პერსონალურ მონაცემთა შეგროვება, მონაცემთა სუბიექტებისა და საზოგადოების ინფორმირება და მონაცემთა სუბიექტის მიერ უფლებებით სარგებლობა.

იმისათვის, რომ ქცევის კოდექსი შეესაბამებოდეს GDPR-ით დადგენილ წესებს, დამტკიცებამდე უნდა წარედგინოს კომპეტენტურ საზედამხედველო ორგანოს. ეს უწყება თავის მოსაზრებას ჩამოაყალიბებს კოდექსის რეგულაციასთან შესაბამისობის შესახებ და, თუ დაადგენს, რომ კოდექსი ითვალისწინებს დაცვის სათანადო მექანიზმებს, ამტკიცებს მას.[481] საზედამხედველო ორგანომ უნდა იზრუნოს დამტკიცებული ქცევის კოდექსისა და იმ კრიტერიუმების გამოქვეყნებაზე, რომელთა საფუძველზეც ის დამტკიცდა. როდესაც ქცევის კოდექსის პროექტი შეეხება მონაცემთა დამუშავებას რამდენიმე წევრ სახელმწიფოში, კომპეტენტურმა საზედამხედველო ორგანომ, დამტკიცებამდე, შესწორებამდე ან ვადის გაგრძელებამდე, ის უნდა წარუდგინოს ევროკავშირის მონაცემთა დაცვის საბჭოს. ეს უკანასკნელი გააცნობს თავის მოსაზრებას კოდექსის GDPR-თან შესაბამისობის შესახებ. შეიძლება კომისიამ დამნერგავი აქტით მიიღოს გადაწყვეტილება, რომ დამტკიცებული ქცევის კოდექსი ძალაშია ევროკავშირის მასშტაბით.

ქცევის კოდექსის მოთხოვნათა დაცვა მნიშვნელოვან სარგებელს მოუტანს როგორც მონაცემთა სუბიექტს, ისე დამმუშავებელსა და უფლებამოსილ პირს. კოდექსი ადგენს დეტალურ ინსტრუქციებს, რომელთა საფუძველზეც საკანონმდებლო მოთხოვნები კონკრეტულ სექტორს მოერგება და უმჯობესდება დამუშავების გამჭვირვალობა. კოდექსის მოთხოვნათა შესრულებით, მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ადასტურებენ ევროკავშირის კანონმდებლობასთან შესაბამისობას. ეს მათ საზოგადოების თვალში წარმოაჩენს ისეთ ორგანიზაციებად, რომლებიც თავიანთი საქმიანობისას პატივს სცემენ და პრიორიტეტად განსაზღვრავენ მონაცემთა დაცვას. ქცევის დამტკიცებული კოდექსი, შესასრულებლად სავალდებულო და აღსრულებად ვალდებულებებთან ერთად, შესაძლებელია დაცვის სათანადო მექანიზმების სახით გამოიყენონ მონაცემთა მესამე ქვეყნისთვის გადაცემისას. იმისათვის, რომ ორ-

480 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 40 (1).

481 *იქვე*, მუხლი 40 (5).

განიზაციამ, რომელიც ქცევის კოდექსს იცავს, რეალურად შეასრულოს მისი მოთხოვნები, შესაძლებელია სპეციალური (საზედამხედველო ორგანოს მიერ აკრედიტებული) უწყების შექმნა, რომელიც მონიტორინგს გაუწევს ამ პროცესს. აღნიშნულ უწყებას კი, მასზე დაკისრებული ამოცანების შესასრულებლად, უნდა ჰქონდეს დადასტურებული ექსპერტული ცოდნა და გამოცდილება ქცევის კოდექსით დარეგულირებულ საკითხებზე, ასევე, გამჭვირვალე პროცედურები და სტრუქტურა, რომლებიც მისცემს კოდექსის დარღვევაზე შესული საჩივრების განხილვის საშუალებას.[482]

ევროპის საბჭოს სამართალში მოდერნიზებული 108-ე კონვენცია ადგენს, რომ მონაცემთა დაცვის დონე, რომელიც გარანტირებულია ეროვნული კანონმდებლობით, შეიძლება ეფექტიანად განმტკიცდეს ნებაყოფლობითი მარეგულირებელი მექანიზმებით, როგორიცაა კარგი პრაქტიკის ან პროფესიული ქცევის კოდექსები. თუმცა, კონვენციის თანახმად, ესენი მხოლოდ ნებაყოფლობითი მექანიზმებია - იგი არ ადგენს ასეთი მექანიზმების შემოღების სამართლებრივ ვალდებულებას და ამ საკითხზე მხოლოდ რეკომენდაციით შემოიფარგლება. აღნიშნული მექანიზმები, ცალკე აღებული, არ კმარა კონვენციასთან სრული შესაბამისობისათვის. [483]

4.3.5 სერტიფიცირება

ქცევის კოდექსთან ერთად, სერტიფიცირების მექანიზმები, ასევე, მონაცემთა დაცვის ბეჭდები და ნიშნები, კიდევ ერთი საშუალებაა, რითაც მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შეუძლიათ GDPR-თან შესაბამისობის დადასტურება. ამ მიზნით, რეგულაცია ითვალისწინებს სერტიფიცირების ნებაყოფლობით სისტემას, რაც გულისხმობს გარკვეული უწყებების ან საზედამხედველო ორგანოების მიერ სერტიფიკატების გაცემას. მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი, რომელიც სერტიფიცირების მექანიზმის დაცვას გადაწყვეტს, უფრო მეტ სანდოობასა და სახელს მოიპოვებს, რადგან სერტიფიკატები, ბეჭდები და ნიშნები მონაცემთა სუბიექტებს საშუალებას აძლევს, სწრაფად შეაფასონ ორგანიზაციის მიერ მონაცემთა დაცვის დონე დამუშავების პროცესში. ამავდროულად, მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის მიერ ასეთი სერტიფიკატის ფლობა არ ამცირებს მათ მოვალეობებსა და პასუხისმგებლობებს, დაემორჩილონ რეგულაციის ყველა მოთხოვნას.

482 *იქვე*, მუხლი 41(1)(2).

483 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 33.

4.4 მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (by design) და მონაცემთა დაცვა პირველად პარამეტრად (by default)

მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (data protection by design)

ევროკავშირის სამართალში მონაცემთა დამმუშავებელს ეკისრება საჭირო ზომების შემოღება მონაცემთა დაცვის პრინციპების ეფექტიანად განხორციელებისა და დაცვის აუცილებელი მექანიზმების ინტეგრირებისათვის, რეგულაციის მოთხოვნათა შესაბამისად და მონაცემთა სუბიექტების უფლებების დასაცავად.[484] აღნიშნული ზომების დანერგვა შესაძლებელია როგორც დამუშავებასთან მიმართებით, ისე მისი საშუალებების განსაზღვრისას. ამ პროცესში მონაცემთა დამმუშავებელმა უნდა გაითვალისწინოს ტექნიკის ბოლოდროინდელი მიღწევები, განხორციელების ხარჯები, პერსონალურ მონაცემთა დამუშავების ბუნება, მოცულობა და მიზანი, ასევე, მონაცემთა სუბიექტის უფლებათა დარღვევის რისკები და მათი სიმძიმე.[485]

ევროპის საბჭოს კანონმდებლობით, მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ვალდებულნი არიან, პერსონალურ მონაცემთა დამუშავების დაწყებამდე შეაფასონ დამუშავების გავლენა მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებზე. ამასთან, მათ ევალებათ მონაცემთა დამუშავების ისეთი სისტემის შექმნა, რომელიც აღმოფხვრის ან შეამცირებს აღნიშნული უფლებებისა და თავისუფლებების შელახვის საფრთხეს; ასევე, ტექნიკური და ორგანიზაციული ზომების გატარება, რომლებიც ითვალისწინებს პერსონალურ მონაცემთა დაცვის უფლებისთვის შექმნილ რისკებს მონაცემთა დამუშავების ყველა ეტაპზე.[486]

---

484 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 25 (1).

485 იხ: 29-ე მუხლის სამუშაო ჯგუფი (2017), 2016/679 რეგულაციის მიზნებისთვის, მონაცემთა დაცვის რისკების შეფასების (DPIA) და მონაცემთა დამუშავებით გამოწვეული შესაძლო მაღალი რისკის განსაზღვრის სახელმძღვანელო პრინციპები, WP 248 rev.01, ბიუსელი, 2017 წლის 4 ოქტომბერი. ასევე, იხ. ENISA (2015), პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას - პოლიტიკიდან საინჟინრო მეცნიერებამდე, 2015 წლის 12 იანვარი.

486 მოდერნიზებული 108-ე კონვენცია, მუხლი 10 (2)(3), მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 89.

მონაცემთა დაცვა პირველად პარამეტრად (data protection by default)

ევროკავშირის კანონმდებლობა მონაცემთა დამმუშავებელს ავალდებულებს ისეთი ზომების გატარებას, რომ დამუშავდეს მხოლოდ კონკრეტული მიზნისთვის აუცილებელი მონაცემები. ეს ვალდებულება ვრცელდება შეგროვებულ მონაცემთა რაოდენობაზე, დამუშავების მასშტაბებზე, შენახვის ვადებსა და წვდომაზე. [487] მაგალითად, აღნიშნული ზომების მეშვეობით, დამმუშავებლის მხოლოდ გარკვეულ თანამშრომლებს (და არა ყველას) უნდა ჰქონდეთ წვდომა მონაცემთა სუბიექტების პერსონალურ მონაცემებზე. დამატებითი ინსტრუქციები წარმოდგენილია EDPS-ის მიერ შემუშავებულ სახელმძღვანელოში აუცილებელი ზომების შესახებ.[488]

ევროპის საბჭოს კანონმდებლობით, მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს მოეთხოვებათ ისეთი ტექნიკური და ორგანიზაციული ზომების გატარება და დანერგვა, რომლებიც ითვალისწინებს პერსონალურ მონაცემთა დაცვისთვის შექმნილ საფრთხეებს მონაცემთა დამუშავების ყველა ეტაპზე.[489]

2016 წელს ENISA-მ გამოაქვეყნა ანგარიში პირადი ცხოვრების ხელშეუხებლობის ინსტრუმენტებისა და სერვისების ხელმისაწვდომობაზე.[490] შეფასებაში, სხვა საკითხებთან ერთად, წარმოდგენილია იმ კრიტერიუმებისა და პარამეტრების ინდექსი, რომლებიც პირადი ცხოვრების დაცვის ეფექტიანი თუ არაეფექტიანი პრაქტიკის ინდიკატორებად მიიჩნევა. ზოგიერთი კრიტერიუმი პირდაპირ უკავშირდება GDPR-ის დებულებებს (მაგ:. ფსევდონიმიზაციისა და სერტიფიცირების დამტკიცებული მექანიზმების გამოყენება), ხოლო სხვა კრიტერიუმები ითვალისწინებს ინოვაციურ ინიციატივებს ისეთი პრინციპების დასაცავად, როგორიცაა მონაცემთა დაცვის სტანდარტების გათვალისწინება პროდუქტის ან მომსახურების შექმნისას (privacy by design) და მონაცემთა დაცვა პირველად პარამეტრად (privacy by default). მაგალითად, გამოყენებადობის კრიტერიუმი პირდაპირ არ უკავშირდება პირადი ცხოვრების ხელშეუხებლობას, თუმცა აუმჯობესებს პირადი ცხოვრების დაცვას, რადგან მისი ინსტრუმენტებისა თუ მომსახურების ფართო ათვისების შესაძლებლობას იძლევა. მართლაც, პირადი ცხოვრების დაცვის ინსტრუმენტები, რომელთა

487 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 25 (2).

488 ევროკავშირის მონაცემთა დაცვის ზედამხედველი (EDPS), (2017), სახელმძღვანელო აუცილებელი ზომების შესახებ, ბრიუსელი, 2017 წლის 11 აპრილი.

489 მოდერნიზებული 108-ე კონვენცია, მუხლი 10 (3), მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 89.

490 ENISA, PET კონტროლის მატრიცა: სისტემური მიდგომა პირადი ცხოვრების ონლაინ და მობილური ინსტრუმენტების შესაფასებლად, 2016 წლის 20 დეკემბერი.

პრაქტიკაში განხორციელებაც რთულია, შეიძლება ფართო საზოგადოებაში გამოყენების ძალზე დაბალი მაჩვენებლით ხასიათდებოდეს, მაშინაც კი, როცა დაცვის მყარ გარანტიებს იძლევა. ამასთან, უაღრესად მნიშვნელოვანია კრიტერიუმი, რომელიც განსაზღვრავს პირადი ცხოვრების ხელშეუხებლობის დაცვის ინსტრუმენტის სიმწიფესა (maturity) და სტაბილურობას. ეს ნიშნავს, რომ ინსტრუმენტი დროთა განმავლობაში ევოლუციას განიცდის და პასუხობს პირადი ცხოვრების ხელშეუხებლობასთან დაკავშირებულ როგორც ძველ, ისე ახალ გამოწვევებს. პირადი ცხოვრების დაცვის სხვა ტექნოლოგიები (მაგ.: უსაფრთხო კომუნიკაციების კონტექსტში) მოიცავს შემდეგ ასპექტებს: გამჭოლი (end-to-end) დაშიფვრა (შეტყობინების წაკითხვა შეუძლიათ მხოლოდ იმ პირებს, რომლებიც ერთმანეთს ესაუბრებიან); კლიენტსა და სერვერს შორის არსებული საკომუნიკაციო არხის დაშიფვრა (client-server encryption); ნამდვილობის დადგენა (კომუნიკაციის მხარეთა ვინაობის ვერიფიკაცია); და ანონიმური კომუნიკაცია (მესამე პირს არ შეუძლია კომუნიკაციის მხარეთა იდენტიფიცირება).

5
დამოუკიდებელი ზედამხედველობა

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
ქარტია, მუხლი 8 (3); ევროკავშირის ფუნქციონირების შესახებ ხელშეკრულება, მუხლი 16 (2); მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 51–59; CJEU, C-518/07, *European Commission v. Federal Republic of Germany* [GC], 2010; CJEU, C-614/10, *European Commission v. Republic of Austria* [GC], 2012; CJEU, C-288/12, *European Commission v. Hungary* [GC], 2014; CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015.	**საზედამხედველო ორგანოები**	მოდერნიზებული 108-ე კონვენცია, მუხლი 15
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 60–67	**თანამშრომლობა საზედამხედველო ორგანოებს შორის**	მოდერნიზებული 108-ე კონვენცია, მუხლები 16–21
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 68–76	**ევროკავშირის მონაცემთა დაცვის საბჭო**	

ძირითადი საკითხები

- დამოუკიდებელი ზედამხედველობა მონაცემთა დაცვის ევროპული კანონმდებლობის ძირითადი კომპონენტია, გათვალისწინებული ქარტიის მე-8 მუხლის მე-3 პუნქტით;
- მონაცემთა ეფექტიანად დაცვისათვის, საჭიროა დამოუკიდებელი საზედამხედველო ორგანოს შექმნა ეროვნული კანონმდებლობის საფუძველზე.
- საზედამხედველო ორგანო უნდა მოქმედებდეს სრული დმოუკიდებლობით, რაც გარანტირებული იქნება სადამფუძნებლო კანონით და აისახება საზედამხედველო ორგანოს სპეციალურ ორგანიზაციულ სტრუქტურაში.
- საზედამხედველო ორგანოს აქვს კონკრეტული უფლებამოსილებები და ამოცანები, მათ შორის:
  - შიდასახელმწიფოებრივ დონეზე მონაცემთა დაცვის კონტროლი და ხელშეწყობა;
  - კონსულტაცია მონაცემთა სუბიექტებისა და დამმუშავებლებისათვის, ასევე, ხელისუფლებისა და მთლიანად საზოგადოებისათვის;
  - საჩივრების/განცხადებების განხილვა და მონაცემთა სუბიექტის დახმარება მონაცემთა დაცვის უფლების შესაძლო დარღვევებისას;
  - დამმუშავებლებისა და უფლებამოსილი პირების ზედამხედველობა.
- საზედამხედველო ორგანოებს, საჭიროების შემთხვევაში, აქვთ ჩარევის უფლებამოსილებაც, კერძოდ:
  - მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის გაფრთხილება, საყვედურის გამოცხადება ან დაჯარიმება;
  - მონაცემთა შესწორებაზე, დაბლოკვასა ან წაშლაზე ბრძანების გაცემა;
  - მონაცემთა დამუშავების აკრძალვა ან ადმინისტრაციული ჯარიმის დაკისრება;
  - საქმის სასამართლოსთვის გადაცემა.
- ხშირად პერსონალურ მონაცემთა დამუშავებაში მონაწილეობენ სხვადასხვა სახელმწიფოში მყოფი მონაცემთა დამმუშავებლები, უფლებამოსილი პირები და მონაცემთა სუბიექტები. შესაბამისად, საზედამხედველო ორ-

განოებს მოეთხოვებათ საერთაშორისო საკითხებზე თანამშრომლობა, რაც უზრუნველყოფს ფიზიკურ პირთა ეფექტიან დაცვას ევროპაში.

- ევროკავშირში მონაცემთა დაცვის ზოგადი რეგულაცია ადგენს „ერთი ფანჯრის პრინციპს“ მონაცემთა დამუშავების საერთაშორისო შემთხვევებისთვის. ზოგიერთი კომპანია ახორციელებს საერთაშორისო დამუშავებას, რადგან მონაცემები მუშავდება სხვადასხვა წევრ სახელმწიფოში მდებარე დაწესებულებათა საქმიანობის კონტექსტში, ან ეს პროცესი მნიშვნელოვან გავლენას ახდენს რამდენიმე წევრ ქვეყანაში მცხოვრებ მონაცემთა სუბიექტებზე. ასეთი მექანიზმის ფარგლებში, კომპანიებს მხოლოდ ერთ ეროვნულ საზედამხედველო ორგანოსთან მოუწევთ ურთიერთობა.

- თანამშრომლობისა და თანმიმდევრულობის მექანიზმი ხელს უწყობს კონკრეტულ საქმეში მონაწილე საზედამხედველო ორგანოთა კოორდინირებული მიდგომის დანერგვას. ძირითადი ან ერთი დაწესებულების წამყვანი საზედამხედველო ორგანო კონსულტაციას გადის და გადაწყვეტილების პროექტს წარუდგენს სხვა შესაბამის საზედამხედველო ორგანოებს.

- 29-ე მუხლის სამუშაო ჯგუფის მსგავსად, ევროკავშირის მონაცემთა დაცვის საბჭოს შემადგენლობაში იქნებიან თითოეული წევრი სახელმწიფოს საზედამხედველო ორგანო და ევროპის მონაცემთა დაცვის ზედამხედველი (EDPS).

- ევროკავშირის მონაცემთა დაცვის საბჭოს მიზნებია: რეგულაციის სწორად დანერგვაზე კონტროლი, კომისიისთვის კონსულტაციის გაწევა შესაბამის საკითხებზე, და მოსაზრებების, სახელმძღვანელო პრინციპების ან საუკეთესო პრაქტიკის მაგალითების მომზადება სხვადასხვა საკითხზე.

- ძირითადი განსხვავება ის არის, რომ 95/46/EC დირექტივის თანახმად, ევროკავშირის მონაცემთა დაცვის საბჭოს აქვს არა მხოლოდ მოსაზრებების, არამედ სავალდებულო ძალის მქონე გადაწყვეტილებათა გამოცემის უფლებაც. ეს ეხება იმ საქმეებს, სადაც: „ერთი ფანჯრის პრინციპის“ ფარგლებში საზედამხედველო ორგანომ რელევანტური და საფუძვლიანი მოთხოვნა დააყენა; არსებობს განსხვავებული მოსაზრებები, რომელი საზედამხედველო ორგანო უნდა იყოს წამყვანი; და ბოლოს, კომპეტენტურ საზედამხედველო ორგანოს არ მოუთხოვია ან არ ასრულებს EDPB-ის მოსაზრებას. ევროკავშირის მონაცემთა დაცვის საბჭოს მთავარი მიზანია ყველა წევრ სახელმწიფოში რეგულაციის თანმიმდევრული გამოყენება.

დამოუკიდებელი ზედამხედველობა მონაცემთა დაცვის ევროპული კანონმდებლობის მნიშვნელოვანი კომპონენტია. როგორც ევროკავშირის, ისე

ევროპის საბჭოს კანონმდებლობის მიხედვით, პერსონალურ მონაცემთა დამუშავების კონტექსტში ფიზიკურ პირთა უფლებებისა და თავისუფლებების დასაცავად, დამოუკიდებელი საზედამხედველო ორგანოს არსებობა აუცილებელია. ვინაიდან მონაცემთა დამუშავება ფართოდ გავრცელებული ფენომენია და მისი აღქმა სულ უფრო და უფრო რთულდება ფიზიკური პირებისათვის, საზედამხედველო ორგანოები ციფრული ეპოქის დამკვირვებლები (watchdogs) არიან. ევროკავშირში დამოუკიდებელი საზედამხედველო ორგანოების არსებობა პერსონალურ მონაცემთა დაცვის უფლების ერთ-ერთ ყველაზე მნიშვნელოვან ელემენტად მიიჩნევა. მას, ძირითადად, ევროკავშირის კანონმდებლობა ითვალისწინებს. ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლის მე-3 პუნქტისა და TFEU-ს მე-16 მუხლის მე-2 პუნქტის თანახმად, პერსონალური მონაცემების დაცვა ფუნდამენტური უფლებაა, ხოლო მონაცემთა დაცვის წესების შესრულებას უნდა აკონტროლებდეს დამოუკიდებელი ორგანო.

მონაცემთა დაცვის კანონმდებლობის შესრულების კუთხით, დამოუკიდებელი საზედამხედველო ორგანოს მნიშვნელობა აღიარებულია პრეცედენტულ სამართალშიც.

მაგალითი: *Schrems*-ის საქმეში[491] CJEU-მ, ევროკავშირისა და აშშ-ს შორის დაცვის საშუალებათა შეთანხმების (Safe Harbour Agreement) საფუძველზე, განიხილა აშშ-სთვის პერსონალური მონაცემების გადაცემის შესაბამისობა ევროკავშირის მონაცემთა დაცვის სამართალთან. საქმე ეხებოდა აშშ-ს ეროვნული უსაფრთხოების სააგენტოს მასობრივ თვალთვალს, რაც ედვარდ სნოუდენის სკანდალმა გამოააშკარავა. აშშ-სთვის პერსონალური მონაცემების გადაცემა ეფუძნებოდა ევროპული კომისიის მიერ 2000 წელს მიღებულ გადაწყვეტილებას, რომელიც ითვალისწინებდა დაცვის საშუალებათა (Safe Harbour) სქემის ფარგლებში თვითსერტიფიცირებული ამერიკული ორგანიზაციებისათვის მონაცემთა გადაცემას ევროკავშირიდან. დაცვის საშუალებათა (Safe Harbour) ამ სქემით პერსონალური მონაცემები სათანადო დონეზე იყო დაცული. განმცხადებელი, სნოუდენის სკანდალის გათვალისწინებით, კითხვის ნიშნის ქვეშ აყენებდა მონაცემთა გადაცემის კანონიერებას, თუმცა, მისი საჩივარი ირლანდიის საზედამხედველო ორგანომ წარმოებაში არ მიიღო. მოტივი გახლდათ კომისიის გადაწყვეტილება აშშ-ს მონაცემთა დაცვის რეჟიმის ადეკვატურობაზე, რაც ასახულია დაცვის საშუალებათა პრინციპებში („გადაწყვეტილება დაცვის საშუალებების შესახებ“ - Safe Harbour Decision), რომელიც მას საჩივრის განხილვის საშუალებას არ აძლევდა.

491 CJEU, C-362/14, *Maximilliam Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი.

თუმცა, CJEU-მ დაადგინა, რომ კომისიის გადაწყვეტილება იძლეოდა ნებართვას მონაცემთა გადაცემაზე იმ მესამე ქვეყნებისთვის, სადაც მონაცემები სათანადო დონეზე იყო დაცული, თუმცა ის არ აუქმებდა ან აკნინებდა ეროვნულ საზედამხედველო ორგანოთა უფლებამოსილებას. CJEU-მ განმარტა, რომ ამ უწყებების უფლებამოსილებას, მონიტორინგი გაუწიონ მონაცემთა დაცვის შესაბამისობას ევროკავშირის წესებთან, განსაზღვრავს ევროკავშირის ძირითადი სამართალი, კერძოდ, ქარტიის მე-8 მუხლის მე-3 პუნქტი და TFEU-ს მე-16 მუხლის მე-2 პუნქტი. „ამრიგად, დამოუკიდებელი საზედამხედველო ორგანოს შექმნა [...] აუცილებელი კომპონენტია ფიზიკურ პირთა დასაცავად პერსონალურ მონაცემთა დამუშავებისას.“[492]

CJEU-მ გადაწყვიტა, რომ იმ შემთხვევაშიც, როდესაც პერსონალურ მონაცემთა გადაცემის საფუძველია კომისიის გადაწყვეტილება შესაბამისობაზე, ეროვნულ საზედამხედველო ორგანოში საჩივრის შეტანისას, უწყება ვალდებულია, გულმოდგინედ განიხილოს ის. საზედამხედველო ორგანომ შეიძლება უარი თქვას საჩივრის დაკმაყოფილებაზე უსაფუძვლობის გამო. ასეთ შემთხვევაში CJEU-მ ხაზგასმით აღნიშნა, რომ ეფექტიანი სამართლებრივი მისაგებლის უფლება ითვალისწინებს გადაწყვეტილების ეროვნულ სასამართლოში გასაჩივრების შესაძლებლობას შესაბამისი პირისათვის. შესაძლოა სასამართლომ, თავის მხრივ, საქმე გადასცეს CJEU-ს და ითხოვოს წინასწარი განჩინების მიღება კომისიის გადაწყვეტილების (შესაბამისობის შესახებ) იურიდიულ ძალასთან დაკავშირებით. თუ საზედამხედველო ორგანო მიიჩნევს, რომ საჩივარი საფუძვლიანია, მან უნდა შეძლოს სამართალწარმოებაში ჩართვა და საქმის ეროვნულ სასამართლოში აღძვრა. ეროვნულ სასამართლოებს უფლება აქვთ, საქმე გადასცენ CJEU-ს, ვინაიდან იგი ერთადერთი ორგანოა, რომელსაც აქვს გადაწყვეტილების მიღების უფლებამოსილება კომისიის გადაწყვეტილების იურიდიულ ძალასთან დაკავშირებით.[493]

CJEU-მ განიხილა ამ გადაწყვეტილების (Safe Harbour Decision) იურიდიული ძალის საკითხი, რათა დაედგინა, შეესაბამებოდა თუ არა მონაცემთა გადაცემის სისტემა ევროკავშირის მონაცემთა დაცვის წესებს. მან დაადგინა, რომ გადაწყვეტილების მე-3 მუხლი ზღუდავდა ეროვნული საზედამხედველო ორგანოების უფლებამოსილებას (მინიჭებულს მონაცემთა დაცვის რეგულაციის საფუძველზე), გაეტარებინათ პრევენციული ზომები, თუკი აშშ-ში პერსონალურ მონაცემთა დაცვის დონე არ იქნებოდა სათანადო. CJEU-მ, გაითვალისწინა რა დამოუკიდებელი საზედამხედველო ორგანოების მნიშვნელობა მონაცემთა დაცვის კანონმდებლობასთან

492 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი, პუნქტი 41.

493 *იქვე*, პუნქტები 53–66.

შესაბამისობის კუთხით, დაადგინა, რომ მონაცემთა დაცვის დირექტივის თანახმად, ქარტიის ჭრილში, კომისიას არ ჰქონდა დამოუკიდებელი საზედამხედველო ორგანოს უფლებამოსილების ამ გზით შეზღუდვის უფლება. ეს იყო ერთ-ერთი მიზეზი, რის გამოც CJEU-მ გადაწყვეტილება დაცვის საშუალებების შესახებ (Safe Harbour Decision) ძალადაკარგულად გამოაცხადა.

ამრიგად, ევროპული კანონმდებლობა აწესებს დამოუკიდებელი ზედამხედველობის მოთხოვნას, როგორც მნიშვნელოვან მექანიზმს მონაცემთა ეფექტიანად დაცვისათვის. პირადი ცხოვრების ხელშეუხებლობის უფლების შეზღუდვისას, დამოუკიდებელი საზედამხედველო ორგანო მონაცემთა სუბიექტისთვის პირველი საკონტაქტო პირია. [494] როგორც ევროკავშირის, ისე ევროპის საბჭოს კანონმდებლობის თანახმად, საზედამხედველო ორგანოს შექმნა სავალდებულოა. ორივე სამართლებრივი ჩარჩო ითვალისწინებს ამ ორგანოს უფლება-მოვალეობათა ჩამონათვალს, რომელიც GDPR-ში წარმოდგენილი სიის მსგავსია. ამგვარად, შეიძლება ითქვას, რომ საზედამხედველო ორგანოები ფუნქციონირებენ ერთნაირად, როგორც ევროკავშირის, ისე ევროპის საბჭოს კანონმდებლობის მიხედვით. [495]

5.1 დამოუკიდებლობა

ევროკავშირისა და ევროპის საბჭოს სამართალი საზედამხედველო ორგანოებს ავალდებულებს სრული დამოუკიდებლობით მოქმედებას თავიანთი ფუნქციებისა და უფლებამოსილებების განხორციელებისას.[496] საზედამხედველო ორგანოს, ასევე, მისი წევრებისა და თანამშრომლების დამოუკიდებლობას პირდაპირი და ირიბი გარე გავლენებისგან, ფუნდამენტური მნიშვნელობა აქვს მონაცემთა დაცვის საკითხებზე ობიექტური გადაწყვეტილების მიღებისათვის. საზედამხედველო ორგანოს საფუძველში ჩადებული კანონმდებლობა უნდა შეიცავდეს დებულებებს, რომლებიც კონკრეტულად დამოუკიდებლობას უზრუნველყოფს. მეტიც, უწყების ორგანიზაციული სტრუქტურა სწორედ დამოუკიდებლობას უნდა წარმოაჩენდეს. 2010 წელს CJEU-მ პირველად იმსჯელა საზედამხედველო ორგანოების დამოუკიდებლობის მასშტაბებზე.[497] ქვემოთ წარმოდგენილი მაგალითებით ნათელია, თუ როგორ განმარტავს ეს სასამართლო „სრულ დამოუკიდებლობას.“

494 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 13 (2) (დ).

495 *იქვე*, მუხლი 51; მოდერნიზებული 108-ე კონვენცია, მუხლი 15.

496 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 52 (1); მოდერნიზებული 108-ე კონვენცია, მუხლი 15(5).

497 FRA (2010), ფუნდამენტური უფლებები: გამოწვევები და მიღწევები 2010 წელს, ყოველწლიური ანგარიში, 2010, გვ. 59; FRA (2010), მონაცემთა დაცვა ევროკავშირში: მონაცემთა დაცვის ეროვნული უწყების როლი, 2010 წლის მაისი.

მაგალითები: *European Commission v. Federal Republic of Germany*[498] ევროპულმა კომისიამ CJEU-ს მიმართა თხოვნით, რათა დაედგინა, რომ გერმანიამ მონაცემთა დაცვაზე პასუხისმგებელი ორგანოებისათვის „სრული დამოუკიდებლობის“ მოთხოვნა და მასზე დაკისრებული ვალდებულებები ვერ შეასრულა მონაცემთა დაცვის დირექტივის 28-ე მუხლის პირველი პუნქტის შესაბამისად. კომისიის აზრით, ის, რომ გერმანიამ საზედამხედველო ორგანოები, რომლებიც სხვადასხვა ფედერალურ ერთეულში *(Länder)* პერსონალურ მონაცემთა დამუშავებას აკონტროლებდნენ, სახელმწიფო კონტროლქვეშ მოაქცია, ეწინააღმდეგებოდა დამოუკიდებლობის მოთხოვნას მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის მიზნით.

CJEU-მ ხაზგასმით აღნიშნა, რომ ცნება „სრული დამოუკიდებლობით“ უნდა განიმარტოს [28-ე მუხლის პირველი პუნქტის] ფორმულირების, ასევე, ევროკავშირის მონაცემთა დაცვის კანონმდებლობის მიზნებისა და სტრუქტურის საფუძველზე.[499] CJEU-მ ხაზი გაუსვა, რომ საზედამხედველო ორგანოები პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული უფლებების „დამცველები“ არიან. ამრიგად, მათი შექმნა წევრ სახელმწიფოში მიჩნეულია „ფიზიკურ პირთა დაცვის მნიშვნელოვან კომპონენტად პერსონალურ მონაცემთა დამუშავებისას.“[500] CJEU-ს დასკვნით, „მოვალეობების შესრულებისას, საზედამხედველო ორგანოები ობიექტურად და მიუკერძოებლად უნდა მოქმედებდნენ. საამისოდ ისინი თავისუფალნი უნდა იყვნენ ნებისმიერი გარე ზემოქმედებისგან, მათ შორის, სახელმწიფო ორგანოთა პირდაპირი ან არაპირდაპირი გავლენისგან.“ [501]

სასამართლომ ასევე დაადგინა, რომ „სრული დამოუკიდებლობა“ უნდა განიმარტოს EDPS-ის დამოუკიდებლობიდან გამომდინარე, რაც განსაზღვრულია ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაციით. ამ რეგულაციის თანახმად, დამოუკიდებლობის კონცეფცია გულისხმობს, რომ EDPS-მა არ მოითხოვოს/მიიღოს ინსტრუქციები რომელიმე პირისგან.

შესაბამისად, CJEU-მ დაადგინა, რომ საზედამხედველო ორგანოები გერმანიაში - სახელმწიფო ორგანოების მხრიდან კონტროლის გამო - არ იყვნენ სრულად დამოუკიდებელნი ევროკავშირის მონაცემთა დაცვის კანონმდებლობის მიხედვით.

498 CJEU, C-518/07, *European Commission v. Federal Republic of Germany* [GC], 2010 წლის 9 მარტი, პუნქტი 27.

499 *იქვე*, პუნქტები 17 და 29.

500 *იქვე*, პუნქტი 23.

501 *იქვე*, პუნქტი 25.

საქმეში *European Commission v. Republic of Austria*[502] CJEU-მ იმავე პრობლემებს გაუსვა ხაზი, ამჯერად ავსტრიის მონაცემთა დაცვის საზედამხედველო ორგანოს (მონაცემთა დაცვის კომისია, DSK) გარკვეული წევრებისა და თანამშრომლების დამოუკიდებლობასთან მიმართებით. სასამართლომ განმარტა: ის ფაქტი, რომ ფედერალური კანცელარია საზედამხედველო ორგანოს უზრუნველყოფდა სამუშაო ძალით, ევროკავშირის მონაცემთა დაცვის კანონმდებლობით გათვალისწინებულ დამოუკიდებლობის მოთხოვნას ასუსტებდა. CJEU-მ ასევე დაადგინა, რომ კანცელარიის უფლება, ნებისმიერ დროს ყოფილიყო ინფორმირებული DSK-ის საქმიანობის შესახებ, უგულებელყოფდა საზედამხედველო ორგანოს სრული დამოუკიდებლობის მოთხოვნას.

საქმეში *European Commission v. Hungary*[503] სასამართლომ აკრძალა შიდასახელმწიფოებრივ დონეზე არსებული მსგავსი პრაქტიკა, რომელიც საზედამხედველო ორგანოს სამუშაო ძალის დამოუკიდებლობაზე ახდენდა გავლენას. მან აღნიშნა: „მოთხოვნა [...], რომ თითოეულმა საზედამხედველო ორგანომ შეძლოს მასზე დაკისრებულ მოვალეობათა სრული დამოუკიდებლობით შესრულება, მოიცავს შესაბამისი წევრი სახელმწიფოს ვალდებულებას, ამ უწყებას მისცეს უფლებამოსილების ვადის სრულ ამოწურვამდე მუშაობის საშუალება.“ CJEU-მ ასევე დაადგინა, რომ „პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს უფლებამოსილების ვადის ნაადრევი შეწყვეტით, უნგრეთმა ვერ შეასრულა 95/46/EC დირექტივით გათვალისწინებული ვალდებულებები [...]“.

„სრული დამოუკიდებლობის“ ცნება და კრიტერიუმები მკაფიოდ არის განმარტებული GDPR-ში, რომელიც შეიცავს CJEU-ს ამ გადაწყვეტილებებში დადგენილ პრინციპებს. რეგულაციის თანახმად, სრული დამოუკიდებლობა საზედამხედველო ორგანოს მიერ საკუთარი ფუნქციებისა და უფლებამოსილებების განხორციელებისას გულისხმობს, რომ:[504]

- თითოეული საზედამხედველო ორგანოს წევრები უნდა იყვნენ თავისუფალნი პირდაპირი თუ ირიბი ჩარევისგან და არ მოითხოვონ/მიიღონ მითითებები გარეშე პირთაგან;

- თითოეული საზედამხედველო ორგანოს წევრებმა, ინტერესთა კონფლიქტის თავიდან აცილების მიზნით, თავი შეიკავონ ნებისმიერი ქმედებისგან, რომელიც არ შეესაბამება მათ ვალდებულებებს;

502 CJEU, C-614/10, *European Commission v. Republic of Austria* [GC], 2012 წლის 16 ოქტომბერი პუნქტები 59 და 63.

503 CJEU, C-288/12, *European Commission v. Hungary* [GC], 2014 წლის 8 აპრილი, პუნქტები 50 და 67.

504 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 69.

- წევრმა სახელმწიფოებმა საზედამხედველო ორგანო უზრუნველყონ ადამიანური, ტექნიკური და ფინანსური რესურსებით, ასევე, შენობითა და ინფრასტრუქტურით - საკუთარი ფუნქციებისა და უფლებამოსილებების ეფექტიანად განხორციელებისათვის;

- წევრმა სახელმწიფოებმა უზრუნველყონ, რომ საზედამხედველო ორგანომ თვითონ შეარჩიოს საკუთარი თანამშრომლების შემადგენლობა;

- თითოეულმა წევრმა სახელმწიფომ საზედამხედველო ორგანოს ფინანსური კონტროლი იმგვარად განახორციელოს, რომ არ შეიზღუდოს მისი დამოუკიდებლობა. საზედამხედველო ორგანოს უნდა ჰქონდეს ცალკე წლიური ბიუჯეტი, რომელიც იქნება საჯარო და უზრუნველყოფს მის სათანადო ფუნქციონირებას.

საზედამხედველო ორგანოების დამოუკიდებლობა მნიშვნელოვან მოთხოვნად მიიჩნევა ევროპის საბჭოს სამართალშიც. მოდერნიზებული 108-ე კონვენციის თანახმად, საზედამხედველო ორგანოები ვალდებულნი არიან, „სრული დამოუკიდებლობითა და მიუკერძოებლობით იმოქმედონ მათზე დაკისრებული ფუნქციებისა და უფლებამოსილებების განხორციელებისას“, ინსტრუქციების მოთხოვნისა თუ მიღების გარეშე. [505] ამრიგად, კონვენციის თანახმად, ეს ორგანოები ვერ შეძლებენ ფიზიკურ პირთა უფლებებისა და თავისუფლებების დაცვას მონაცემთა დამუშავებასთან დაკავშირებით, თუკი თავიანთ ფუნქციებს სრული დამოუკიდებლობით არ შეასრულებენ. მოდერნიზებული 108-ე კონვენცია ითვალისწინებს დამოუკიდებლობის დაცვისთვის მნიშვნელოვან არაერთ ელემენტს, როგორიცაა: საზედამხედველო ორგანოთა შესაძლებლობა, თვითონ შეარჩიონ საკუთარი თანამშრომლები და გადაწყვეტილება მიიღონ გარე ზეგავლენების გარეშე; ასევე, მათი ფუნქციების განხორციელების ხანგრძლივობასთან დაკავშირებული ფაქტორები და ფუნქციების შეწყვეტის პირობები.[506]

5.2 კომპეტენცია და უფლებამოსილება

ევროკავშირის კანონმდებლობაში GDPR ითვალისწინებს საზედამხედველო ორგანოთა კომპეტენციებსა და ორგანიზაციულ სტრუქტურას და ადგენს მოთხოვნას, რომ ისინი იყვნენ კომპეტენტურნი და ჰქონდეთ რეგულაციით გათვალისწინებული ფუნქციების შესასრულებლად საჭირო უფლებამოსილება.

505 მოდერნიზებული 108-ე კონვენცია, მუხლი 15(5).

506 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი.

საზედამხედველო ორგანო ეროვნულ კანონმდებლობაში ძირითადი უწყებაა, რომელიც უზრუნველყოფს შესაბამისობას ევროკავშირის მონაცემთა დაცვის კანონმდებლობასთან. მას აქვს არაერთი მოვალეობა და უფლებამოსილება, რომლებიც სცდება პროაქტიული და პრევენციული ზედამხედველობის ფარგლებს. ამ მოვალეობათა შესასრულებლად, საზედამხედველო ორგანოს უნდა ჰქონდეს სათანადო უფლებამოსილებები გამოძიების, დარღვევის გამოსწორებისა თუ კონსულტაციის გაცემის მხრივ, რომლებიც წარმოდგენილია GDPR-ის 57-ე და 58-ე მუხლებში, კერძოდ: [507]

- კონსულტაცია გაუწიოს მონაცემთა სუბიექტებსა და დამმუშავებლებს მონაცემთა დაცვის ყველა საკითხზე;
- დაამტკიცოს სტანდარტული სახელშეკრულებო პირობები, სავალდებულო ძალის მქონე კორპორატიული წესები, ან ადმინისტრაციული შეთანხმებები;
- გამოიძიოს დამუშავების ოპერაციები და, საჭიროების შემთხვევაში, ჩაერიოს კიდეც;
- მოითხოვოს ინფორმაცია, რომელიც საჭიროა მონაცემთა დამმუშავებლის საქმიანობაზე ზედამხედველობისთვის;
- მონაცემთა დამმუშავებელს გამოუცხადოს გაფრთხილება ან საყვედური და გასცეს ბრძანება, რომ პერსონალურ მონაცემთა უსაფრთხოების დარღვევა ეცნობოთ მონაცემთა სუბიექტებს;
- გასცეს მონაცემთა შესწორების, დაბლოკვის, წაშლის ან განადგურების ბრძანება;
- დააწესოს დროებითი ან საბოლოო აკრძალვა მონაცემთა დამუშავებაზე, ან შესაბამის პირს დააკისროს ადმინისტრაციული ჯარიმა;
- საქმე განსახილველად გადასცეს სასამართლოს.

ამ ფუნქციების განსახორციელებლად, საზედამხედველო ორგანოს ხელი უნდა მიუწვდებოდეს ყველა პერსონალურ მონაცემსა და ინფორმაციაზე, რომელიც საჭიროა მოკვლევის ჩასატარებლად, აგრეთვე, ნებისმიერ შენობაზე, სადაც მონაცემთა დამმუშავებელი რელევანტურ ინფორმაციას ინახავს. CJEU-ს თანახმად, საზედამხედველო ორგანოს უფლებამოსილებები უნდა განიმარტოს ფართოდ, რაც უზრუნველყოფს მონაცემთა დაცვის სრულ ეფექტიანობას ევროკავშირში.

507 მონაცემთა დაცვის ზოგადი რეგულაცია, 57-ე და 58-ე მუხლები; ასევე, 108-ე კონვენცია, დამატებითი ოქმი, მუხლი 1.

მაგალითი: *Schrems*-ის საქმეში[508] CJEU-მ, ევროკავშირსა და აშშ-ს შორის დაცვის საშუალებათა შეთანხმების (Safe Harbour Agreement) საფუძველზე, განიხილა აშშ-სთვის პერსონალური მონაცემების გადაცემის შესაბამისობა ევროკავშირის მონაცემთა დაცვის სამართალთან. საქმე ეხებოდა მასობრივ თვალთვალს აშშ-ს ეროვნული უსაფრთხოების სააგენტოს მხრიდან, რაც ედვარდ სნოუდენის სკანდალმა გამოააშკარავა. CJEU-მ განმარტა, რომ ეროვნულ საზედამხედველო ორგანოებს, როგორც მონაცემთა დამუშავების დამოუკიდებელ მონიტორებს, აქვთ პერსონალურ მონაცემთა მესამე ქვეყნისთვის გადაცემის პრევენციის უფლება (მიუხედავად გადაწყვეტილებისა შესაბამისობის შესახებ), თუკი არსებობს გონივრული მტკიცებულება, რომ მესამე ქვეყანაში სათანადო დაცვა აღარ არის გარანტირებული.[509]

თითოეულ საზედამხედველო ორგანოს აქვს სათანადო კომპეტენცია საგამოძიებო უფლებამოსილების განხორციელებისა და ჩარევისათვის საკუთარი იურისდიქციის ფარგლებში. თუმცა, ვინაიდან მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის აქტივობები ხშირად კვეთს საზღვარს, თვითონ დამუშავება კი გავლენას ახდენს რამდენიმე წევრ სახელმწიფოში მყოფ მონაცემთა სუბიექტებზე, აქტუალური ხდება კომპეტენციათა გადანაწილება სხვადასხვა საზედამხედველო ორგანოს შორის. CJEU-მ ამ საკითხზე *Weltimmo*-ს საქმეში იმსჯელა.

მაგალითი: *Weltimmo-ს* საქმეში[510] CJEU-მ იმსჯელა ეროვნული საზედამხედველო ორგანოების კომპეტენციებზე, მათი იურისდიქციის გარეთ შექმნილ ორგანიზაციებთან დაკავშირებით. Weltimmo სლოვაკეთში რეგისტრირებული კომპანიაა, რომელიც უნგრეთში არსებული უძრავი ქონების ყიდვა-გაყიდვის ვებგვერდს მართავს. რეკლამის დამკვეთებმა უნგრეთის მონაცემთა დაცვის საზედამხედველო ორგანოში შეიტანეს საჩივარი მონაცემთა დაცვის შიდასახელმწიფოებრივი კანონმდებლობის დარღვევაზე, რის შედეგადაც საზედამხედველო ორგანომ Weltimmo-ს ჯარიმა დააკისრა. კომპანიამ ჯარიმა გაასაჩივრა ეროვნულ სასამართლოში, რომელმაც CJEU-ს მიმართა და სთხოვა დადგენა, აძლევდა თუ არა ევროკავშირის მონაცემთა დაცვის დირექტივა წევრი სახელმწიფოს საზედამხედველო ორგანოს მონაცემთა დაცვის ეროვნული კანონმდებლობის გამოყენების უფლებას იმ კომპანიასთან მიმართებით, რომელიც სხვა წევრ ქვეყანაში იყო დარეგისტრირებული.

508 CJEU, C-362/14, *Maximilliam Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი.

509 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი, პუნქტები 26–36 და 40–41.

510 CJEU, C-230/14, *Weltimmo s.r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 2015 წლის 1 ოქტომბერი.

CJEU-მ განმარტა, რომ მონაცემთა დაცვის დირექტივის მე-4 მუხლის 1 (ა) პუნქტი წევრ სახელმწიფოს აძლევს უფლებას, მონაცემთა დაცვის საკუთარი კანონმდებლობა გამოიყენოს სხვა წევრ სახელმწიფოში რეგისტრირებული დამმუშავებლის მიმართ, თუკი ის „შესაბამისი წევრი სახელმწიფოს ტერიტორიაზე სტაბილურად ორგანიზებული დაწესებულების მეშვეობით, რეალურად ეწევა თუნდაც მინიმალურ ეფექტიან საქმიანობას მონაცემთა დამუშავების კუთხით.“ CJEU-მ აღნიშნა, რომ მის ხელთ არსებულ ინფორმაციაზე დაყრდნობით, Weltimmo-ს საქმიანობა უნგრეთში რეალური და ეფექტიანი გახლდათ, რადგან კომპანიის წარმომადგენელი ამ ქვეყანაში სლოვაკეთის კომპანიათა რეესტრში უნგრული მისამართით იყო დარეგისტრირებული; ასევე, მას უნგრეთში ჰქონდა საბანკო ანგარიში და საფოსტო ყუთი და უნგრულ ენაზე დაწერილ აქტივობებს ახორციელებდა. ეს ინფორმაცია მიუთითებდა დაწესებულების რეალურად არსებობაზე, რის გამოც Weltimmo-ს აქტივობებზე ვრცელდებოდა უნგრეთის მონაცემთა დაცვის კანონმდებლობა და საზედამხედველო ორგანოს იურისდიქცია. თუმცა, CJEU-მ ეროვნულ სასამართლოს მიანდო ამ ინფორმაციის გადამოწმება, კერძოდ:

თუ ეროვნული სასამართლო დაადგენდა, რომ Weltimmo-ს უნგრეთში ჰქონდა დაწესებულება, უნგრეთის საზედამხედველო ორგანოს ექნებოდა ჯარიმის დაკისრების უფლებამოსილება; სასამართლოს მიერ საპირისპირო გადაწყვეტილების მიღების შემთხვევაში, კომპანიაზე გავრცელდებოდა იმ წევრი სახელმწიფოს კანონმდებლობა, სადაც კომპანია რეგისტრირებული იყო. ვინაიდან საზედამხედველო ორგანოების უფლებამოსილება უნდა განხორციელდეს სხვა წევრი სახელმწიფოების ტერიტორიულ სუვერენიტეტთან შესაბამისობაში, ამ საქმეში უნგრეთის საზედამხედველო ორგანოს არ ჰქონდა ჯარიმის დაკისრების უფლება. თუმცა, რაკი მონაცემთა დაცვის დირექტივა ითვალისწინებდა საზედამხედველო ორგანოებს შორის თანამშრომლობის ვალდებულებას, უნგრეთის საზედამხედველო ორგანოს შეეძლო, სლოვაკეთის ასეთივე ორგანოსთვის ეთხოვა აღნიშნული საკითხის გარკვევა, სლოვაკეთის კანონმდებლობის დარღვევის დადგენა და მისივე სამართლით გათვალისწინებული სანქციების დაკისრება.

GDPR-ის მიღებით, დეტალური წესები დაინერგა საერთაშორისო საქმეებში საზედამხედველო ორგანოების უფლებამოსილებასთან დაკავშირებით. რეგულაცია ადგენს „ერთი ფანჯრის პრინციპს“ და მოიცავს დებულებებს, რომლებიც სავალდებულოს ხდის სხვადასხვა საზედამხედველო ორგანოს შორის თანამშრომლობას. საერთაშორისო საქმეებზე ეფექტიანი თანამშრომლობისთვის, GDPR ადგენს წამყვანი საზედამხედველო ორგანოს შექმნის ვალდებულებას, მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის ძირითადი

ან ერთადერთი ადგილსამყოფელის მიხედვით.[511] წამყვანი საზედამხედველო ორგანო, რომელიც საერთაშორისო საქმეებზე მუშაობს, მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ერთადერთი მარეგულირებელია საერთაშორისო დამუშავების პროცესში და კოორდინაციას უწევს სხვა საზედამხედველო ორგანოებთან თანამშრომლობას, კონსენსუსის მისაღწევად. თანამშრომლობა მოიცავს ინფორმაციის გაცვლას, ურთიერთდახმარებას მონიტორინგისა და გამოძიების პროცესში, ასევე, შესასრულებლად სავალდებულო გადაწყვეტილებათა მიღებას.[512]

ევროპის საბჭოს კანონმდებლობაში საზედამხედველო ორგანოთა კომპეტენციები და უფლებამოსილებები წარმოდგენილია მოდერნიზებული 108-ე კონვენციის მე-15 მუხლში და შეესაბამება მათთვის ევროკავშირის კანონმდებლობით მინიჭებულ უფლებამოსილებებს, როგორიცაა: გამოძიება და ჩარევა; ადმინისტრაციული სანქციის დაწესება გადაწყვეტილებათა გამოცემისა და კონვენციის დებულებათა დარღვევის შემთხვევაში; სასამართლო საქმისწარმოების დაწყება. ზოგადად, დამოუკიდებელ საზედამხედველო ორგანოებს აქვთ შემდეგი უფლებამოსილებებიც: რეაგირება მონაცემთა სუბიექტების მოთხოვნებსა და საჩივრებზე; საზოგადოების ცნობიერების ამაღლება მონაცემთა დაცვის კანონმდებლობის შესახებ; კონსულტაციის გაწევა მათთვის, ვინც ეროვნულ დონეზე იღებს გადაწყვეტილებას იმ საკანონმდებლო ან ადმინისტრაციულ ზომებზე, რომლებიც ითვალისწინებს პერსონალურ მონაცემთა დამუშავებას.

5.3 თანამშრომლობა

GDPR ადგენს ზოგად ჩარჩოს საზედამხედველო ორგანოებს შორის თანამშრომლობის შესახებ და ამ მხრივ ითვალისწინებს კონკრეტულ წესებს მონაცემთა დამუშავების საერთაშორისო აქტივობებთან მიმართებით.

GDPR-ის თანახმად, საზედამხედველო ორგანოებს ეკისრებათ ურთიერთდახმარებისა და რელევანტური ინფორმაციის გაცვლის ვალდებულება, რათა რეგულაცია თანმიმდევრულად განხორციელდეს და დაინერგოს.[513] ეს ეხება მოთხოვნის მიმღებ საზედამხედველო ორგანოს, რომელიც ატარებს კონსულტაციებს, ინსპექტირებასა და გამოძიებას. საზედამხედველო ორგანოებს აქვთ ერთობლივი საქმიანობის უფლებაც (მაგ.: ერთობლივი გამოძიება და აღსრულების ერთობლივი ზომების გატარება, რაშიც მონაწილეობენ წევრ სა-

511 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 56(1).

512 *იქვე*, მუხლი 60.

513 *იქვე*, მუხლები 61(1)-(3) და 62 (1).

ხელმწიფოთა საზედამხედველო ორგანოების წარმომადგენლები და თანამშრომლები). [514]

ევროკავშირში მონაცემთა დამმუშავებლები და უფლებამოსილი პირები სულ უფრო და უფრო ხშირად საქმიანობენ ტრანსნაციონალურ დონეზე. შესაბამისად, საჭიროა მჭიდრო თანამშრომლობა წევრ სახელმწიფოთა კომპეტენტურ საზედამხედველო ორგანოებს შორის, რათა პერსონალური მონაცემები დამუშავდეს GDPR-ის მოთხოვნათა შესაბამისად. რეგულაციის „ერთი ფანჯრის პრინციპის“ თანახმად, თუ მონაცემთა დამმუშავებელს ან უფლებამოსილ პირს დაწესებულებები აქვს რამდენიმე წევრ სახელმწიფოში, ან ეკუთვნის ერთი დაწესებულება, მაგრამ მისი საქმიანობა მნიშვნელოვან გავლენას ახდენს მონაცემთა სუბიექტებზე სხვადასხვა წევრ სახელმწიფოში, მის საერთაშორისო საქმიანობაზე ზედამხედველი წამყვანი ორგანო იქნება უწყება, რომელიც მდებარეობს ძირითად ან ერთადერთ ადგილას. წამყვან ორგანოებს აქვთ უფლება, მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის წინააღმდეგ განახორციელონ აღსრულების ღონისძიება. „ერთი ფანჯრის პრინციპის“ მიზანია, ხელი შეუწყოს ევროკავშირის მონაცემთა დაცვის კანონმდებლობის ერთნაირ გამოყენებასა და ჰარმონიზებას სხვადასხვა წევრ სახელმწიფოში. იგი მოქმედებს საწარმოების სასარგებლოდაც, რომლებსაც მხოლოდ ერთ წამყვან საზედამხედველო ორგანოსთან დასჭირდებათ ურთიერთობა. ეს აუმჯობესებს სამართლებრივ განჭვრეტადობას საწარმოებისთვის, ხოლო პრაქტიკაში ნიშნავს გადაწყვეტილებათა უფრო სწრაფად მიღებას, ასევე, იმას, რომ საწარმოები არ დარჩებიან პირისპირ სხვადასხვა საზედამხედველო ორგანოსთან, რომლებიც ურთიერთსაწინააღმდეგო მოთხოვნებს უწესებენ.

წამყვანი ორგანოს იდენტიფიცირება გულისხმობს ევროკავშირში კონკრეტული საწარმოს ძირითადი დაწესებულების ადგილმდებარეობის განსაზღვრას. GDPR განმარტავს ტერმინს „ძირითადი დაწესებულება“. ამასთან, 29-ე მუხლის სამუშაო ჯგუფმა გამოსცა სახელმძღვანელო პრინციპები მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის წამყვანი საზედამხედველო ორგანოს განსაზღვრაზე, რომელიც მოიცავს ძირითადი დაწესებულების იდენტიფიცირების კრიტერიუმებს.[515]

ევროკავშირის მასშტაბით მონაცემთა მაღალ დონეზე დასაცავად, წამყვანი საზედამხედველო ორგანო დამოუკიდებლად არ მოქმედებს. კონსენსუსისა და თანმიმდევრულობის მისაღწევად, იგი ვალდებულია, სხვა საზედამხედველო

514 *იქვე*, მუხლი 62 (1).

515 29-ე მუხლის სამუშაო ჯგუფი (2016), მონაცემთა დამმუშავებლის ან უფლებამოსილი პირისთვის წამყვანი საზედამხედველო ორგანოს იდენტიფიცირების სახელმძღვანელო პრინციპები, WP 244, ბრიუსელი, 2016 წლის 13 დეკემბერი, გადაიხედა 2017 წლის 5 აპრილს.

ორგანოებთანაც ითანამშრომლოს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის მიერ გადაწყვეტილებათა მიღებისას. ეს მოიცავს ინფორმაციის გაცვლას, ურთიერთდახმარებას, ერთობლივ გამოძიებასა და მონიტორინგს.[516] ურთიერთდახმარების პროცესში საზედამხედველო ორგანოები სიფრთხილით უნდა მოეკიდონ სხვა ასეთივე ორგანოების მიერ მოთხოვნილ ინფორმაციას და გაატარონ საზედამხედველო ღონისძიებები, როგორიცაა, მაგალითად, წინასწარი ავტორიზაცია და კონსულტაცია მონაცემთა დამმუშავებელთან მის საქმიანობაზე, ასევე, ინსპექტირება ან გამოძიება. სხვა წევრ სახელმწიფოში არსებულ საზედამხედველო ორგანოს დახმარება უნდა გაეწიოს მოთხოვნის შემთხვევაში, ზედმეტი დაყოვნების გარეშე და მოთხოვნიდან არა უგვიანეს ერთი თვის განმავლობაში.[517]

თუ მონაცემთა დამმუშავებელს ფილიალები სხვადასხვა წევრ სახელმწიფოში აქვს, საზედამხედველო ორგანოებს უფლება აქვთ, ჩაატარონ ერთობლივი ოპერაციები, მათ შორის, გამოძიება და აღსრულების ღონისძიებები, რაშიც მონაწილეობენ სხვა წევრი სახელმწიფოს საზედამხედველო ორგანოს თანამშრომლები.[518]

სხვადასხვა საზედამხედველო ორგანოს შორის თანამშრომლობა ევროპის საბჭოს კანონმდებლობის მნიშვნელოვანი მოთხოვნაც არის. მოდერნიზებული 108-ე კონვენციის თანახმად, ამ ორგანოებმა ერთმანეთთან უნდა ითანამშრომლონ თავიანთი ფუნქციების შესასრულებლად საჭირო ფარგლებში[519] (მაგ.: ერთმანეთისათვის რელევანტური და სასარგებლო ინფორმაციის მიწოდება, გამოძიების კოორდინირება და ერთობლივი ქმედებების განხორციელება[520]).

5.4 ევროკავშირის მონაცემთა დაცვის საბჭო

წინამდებარე თავში უკვე განვიხილეთ დამოუკიდებელი საზედამხედველო ორგანოების მნიშვნელობა და ის ძირითადი უფლებამოსილებები, რომლებიც მათ ენიჭებათ მონაცემთა დაცვის ევროპული კანონმდებლობით. EDPB ერთერთ მნიშვნელოვან როლს ასრულებს მონაცემთა დაცვის წესების ეფექტიანად და თანმიმდევრულად დანერგვაში ევროკავშირის მასშტაბით.

516 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 60 (1)-(3).

517 *იქვე*, მუხლი 61(1)(2).

518 *იქვე*, მუხლი 62 (1).

519 მოდერნიზებული 108-ე კონვენცია, მუხლები 16 და 17.

520 *იქვე*, მუხლი 12-bis (7).

GDPR-ის თანახმად, EDPB შექმნილია როგორც ევროკავშირის ორგანო და სამართლის სუბიექტი.[521] საბჭო 29-ე მუხლის სამუშაო ჯგუფის სამართალმემკვიდრეა.[522] ეს უკანასკნელი კი მონაცემთა დაცვის დირექტივის საფუძველზე შეიქმნა შემდეგი მიზნებით: კომისიისათვის კონსულტაციის გაწევა ევროკავშირის ნებისმიერ ღონისძიებაზე, რომელიც გავლენას ახდენს ფიზიკურ პირთა უფლებებზე პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების ხელშეუხებლობის კუთხით; დირექტივის ერთგვაროვანი დანერგვის ხელშეწყობა; და კომისიისთვის ექსპერტული მოსაზრების მიწოდება მონაცემთა დაცვის საკითხებზე. 29-ე მუხლის სამუშაო ჯგუფი შედგებოდა ევროკავშირის წევრი სახელმწიფოების საზედამხედველო ორგანოების, ასევე, კომისიისა და EDPS-ის წარმომადგენლებისგან.

სამუშაო ჯგუფის მსგავსად, საბჭოს შემადგენლობაში არიან: თითოეული წევრი სახელმწიფოს საზედამხედველო ორგანოს ხელმძღვანელი, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, ან მათი წარმომადგენლები.[523] EDPS სარგებლობს თანაბარი ხმის უფლებით, გარდა დავების გადაწყვეტის შემთხვევებისა. ასეთ საქმეებში EDPS-ს ხმის მიცემა შეუძლია მხოლოდ იმ პრინციპებსა და წესებზე გადაწყვეტილებათა მიღებისას, რომლებიც შეეხება ევროკავშირის ინსტიტუტებს და შეესაბამება GDPR-ით გათვალისწინებულ პრინციპებსა და წესებს. კომისიას უფლება აქვს, მონაწილეობა მიიღოს საბჭოს შეხვედრებსა და საქმიანობაში, ხმის მიცემის უფლების გარეშე.[524] საბჭო წევრებიდან ირჩევს თავმჯდომარეს (რომელიც წარმოადგენს საბჭოს) და თავმჯდომარის ორ მოადგილეს, უბრალო უმრავლესობით და 5-წლიანი ვადით. ამასთან, EDPB-ს აქვს სამდივნოც, რომელსაც უზრუნველყოფს EDPS. იგი ანალიტიკურ, ადმინისტრაციულ და ლოგისტიკურ მხარდაჭერას უწევს საბჭოს. [525]

EDPB-ს ფუნქციები დეტალურად არის აღწერილი GDPR-ის 64-ე, 65-ე და 70-ე მუხლებში და მოიცავს კომპლექსურ ფუნქციებს, რომელთა დაყოფაც შეიძლება 3 ძირითად კატეგორიად:

521 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 68.

522 95/46/EC დირექტივის თანახმად, 29-ე მუხლის სამუშაო ჯგუფს კომისიისთვის კონსულტაცია უნდა გაეწია ნებისმიერ ღონისძიებაზე, რომელიც გავლენას ახდენს ფიზიკურ პირთა უფლებებზე პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის კუთხით. მისი მიზანი იყო კომისიისათვის ექსპერტული მოსაზრების მიწოდება დირექტივის ერთნაირი გამოყენების ხელშეწყობისა და მონაცემთა დაცვის საკითხებზე. 29-ე მუხლის სამუშაო ჯგუფი შედგებოდა ევროკავშირის წევრ სახელმწიფოთა საზედამხედველო ორგანოების, ასევე, კომისიისა და EDPS-ის წარმომადგენლებისაგან.

523 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 68 (3).

524 *იქვე*, მუხლი 68(4)(5).

525 *იქვე*, მუხლები 73 და 75.

- **თანმიმდევრულობა:** EDPB-ს იურიდიულად სავალდებულო ძალის მქონე გადაწყვეტილებათა მიღების უფლება აქვს 3 შემთხვევაში, კერძოდ, როდესაც: (1) საქმე ეხება საზედამხედველო ორგანოს მართებულ ან დასაბუთებულ საწინააღმდეგო პროცედურას/უარს „ერთი ფანჯრის პრინციპთან“ დაკავშირებით; (2) არსებობს ურთიერთსაწინააღმდეგო მოსაზრებები, თუ რომელი საზედამხედველო ორგანოა წამყვანი; (3) კომპეტენტური საზედამხედველო უწყება არ ითხოვს/არ იზიარებს EDPB-ის მოსაზრებას.[526] EDPB-ს ძირითადი პასუხისმგებლობაა GDPR-ის თანმიმდევრულად დანერგვა ევროკავშირის მასშტაბით. იგი მნიშვნელოვან როლს ასრულებს თანმიმდევრობის მექანიზმში, როგორც ეს განხილულია 5.5 ნაწილში.

- **კონსულტაცია:** EDPB კონსულტაციას უწევს კომისიას ევროკავშირში პესონალურ მონაცემთა დაცვის ნებისმიერ საკითხზე, მათ შორის: რეგულაციაში ცვლილების შეტანა; ევროკავშირის იმ კანონმდებლობის გადახედვა, რომელიც მონაცემთა დამუშავებას შეეხება და, შესაძლოა, ეწინააღმდეგებოდეს ევროკავშირის მონაცემთა დაცვის წესებს; კომისიის მიერ შესაბამისობაზე გადაწყვეტილებების მიღება, რაც იძლევა პერსონალურ მონაცემთა გადაცემის შესაძლებლობას მესამე ქვეყნისთვის ან საერთაშორისო ორგანიზაციისათვის.

- **ხელმძღვანელობა/კონსულტაცია:** რეგულაციის თანმიმდევრულად დანერგვისათვის, საბჭო შეიმუშავებს სახელმძღვანელო პრინციპებს, რეკომენდაციებსა და საუკეთესო პრაქტიკასაც, ასევე, ხელს უწყობს თანამშრომლობასა და ცოდნის გაზიარებას საზედამხედველო ორგანოთა შორის. იგი ვალდებულია, რომ მონაცემთა დამმუშავებლებისა თუ უფლებამოსილი პირების ასოციაციები წაახალისოს ქცევის კოდექსების, მონაცემთა დაცვის სერტიფიცირების მექანიზმებისა და ბეჭდების შესაქმნელად.

EDPB-ის გადაწყვეტილებათა გასაჩივრება შესაძლებელია CJEU-ს წინაშე.

5.5 GDPR-ის თანმიმდევრულობის მექანიზმი

წევრ სახელმწიფოებში რეგულაციის თანმიმდევრულად დანერგვისთვის, GDPR ითვალისწინებს თანმიმდევრულობის მექანიზმს. ამ მექანიზმის ფარგლებში, საზედამხედველო ორგანოები თანამშრომლობენ ერთმანეთთან და, საჭიროების შემთხვევაში, კომისიასთანაც. თანმიმდევრულობის მექანიზმი გამოიყენება 2 შემთხვევაში: პირველი - EDPB-ს მოსაზრებებთან მიმართებით, როდესაც კომპეტენტური საზედამხედველო ორგანო აპირებს ხელშეკ-

526 *იქვე*, მუხლი 65.

რულების სტანდარტული პირობების შემუშავებას ან ღონისძიების გატარებას იმ აქტივობათა განსაზღვრისათვის, რომლებიც მოითხოვს მონაცემთა დაცვის რისკების შეფასებას (DPIA); მეორე მოიცავს EDPB-ს გადაწყვეტილებებს, რომელთა შესრულებაც საზედამხედველო ორგანოებისათვის სავალდებულოა „ერთი ფანჯრის პრინციპის“ შემთხვევებში, როცა საზედამხედველო ორგანო არ ითხოვს/არ იზიარებს EDPB-ს მოსაზრებას.

6

მონაცემთა სუბიექტის უფლებები და მათი რეალიზება

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
ინფორმაციის მიღების უფლება		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 12; CJEU, C-473/12, *Institut professionnel des agents immobiliers (IPI) v. Englebert*, 2013; CJEU, C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, 2015.	**ინფორმაციის გამჭვირვალობა**	მოდერნიზებული 108-ე კონვენცია, მუხლი 8
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 13(1)(2) და 14(1)(2)	**ინფორმაციის შინაარსი**	მოდერნიზებული 108-ე კონვენცია, მუხლი 8 (1)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 13 (1) და 14 (3)	**ინფორმაციის მიწოდების ვადები**	მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1) (ბ)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 12 (1), (5) და (7)	**ინფორმაციის მიწოდების საშუალებები**	მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1) (ბ)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები: 13(2) (დ), 14(2)(ე), 77, 78 და 79	**საჩივრის/ განცხადების შეტანის უფლება**	მოდერნიზებული 108-ე კონვენცია, მუხლი 9(1) (ვ)

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემებზე წვდომის უფლება		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 15 (1); CJEU, *C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer,* 2009; CJEU, გაერთიანებული საქმეები C-141/12 და C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S,* 2014; CJEU, C-434/16, *Peter Nowak v. Data Protection Commissioner,* 2017.	**საკუთარ მონაცემებზე წვდომის უფლება**	მოდერნიზებული 108-ე კონვენცია, მუხლი 9(1) (ბ); ECtHR, *Leander v. Sweden,* No. 9248/81, 1987.
მონაცემთა გასწორების უფლება		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 16	**მცდარი/არაზუსტი პერსონალური მონაცემების შესწორება**	მოდერნიზებული 108-ე კონვენცია, მუხლი 9(1) (ე); ECtHR, *Cemalettin Canli v. Turkey,* No. 22427/04, 2008; ECtHR, *Ciubotaru v. Moldova,* No. 27138/04, 2010.
მონაცემთა წაშლის უფლება		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 17 (1);	**პერსონალური მონაცემების წაშლა**	მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1) (ე); ECtHR, *Segerstedt-Wiberg and Others v. Sweden,* No. 62332/00, 2006.
CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014;	**„დავიწყების” უფლება**	

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni,* 2017.		
მონაცემთა დაბლოკვის უფლება		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 18 (1)	**პერსონალურ მონაცემთა დაბლოკვის უფლება**	
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 19	**შეტყობინების ვალდებულება**	
მონაცემთა პორტირების (გადატანის) უფლება		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 20	**მონაცემთა პორტირების უფლება**	
მონაცემთა დამუშავების შეწყვეტის მოთხოვნის უფლება		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 21 (1); CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni,* 2017.	**მონაცემთა დამუშავების შეწყვეტის მოთხოვნის უფლება მონაცემთა სუბიექტის ინდივიდუალური გარემოებებიდან გამომდინარე**	რეკომენდაცია პროფილირების შესახებ, მუხლი 5.3; მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1) (დ).
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 21 (2)	**მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 21 (5)**	რეკომენდაცია პირდაპირი მარკეტინგის შესახებ, მუხლი 4 (1)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 21 (5)	**მონაცემთა ავტომატური საშუალებით დამუშავების შეწყვეტის მოთხოვნა**	

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებისა და პროფილირების უფლება		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 22	**ავტომატიზებული გადაწყვეტილების მიღებისა და პროფილირების უფლებები**	
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 21	**უფლება, მოითხოვოს ავტომატიზებული გადაწყვეტილების მიღების შეწყვეტა**	
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 13(2)(ვ)	**მნიშვნელოვანი/ არსებითი განმარტების მიღების უფლება**	
უფლების აღდგენის/დაცვის საშუალებები, პასუხისმგებლობა, სანქციები და კომპენსაცია		
ქარტია, მუხლი 47; CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015; მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 77–84.	**მონაცემთა დაცვის ეროვნული კანონმდებლობის დარღვევა**	ECHR, მუხლი 13 (მხოლოდ ევროპის საბჭოს წევრი სახელმწიფოებისათვის); მოდერნიზებული 108-ე კონვენცია, მუხლები: 9(1)(ვ), 12, 15, 16-21; ECtHR, *K.U. v. Finland,* No. 2872/02, 2008; ECtHR, *Biriuk v. Lithuania,* No. 23373/03, 2008.
EU Institutions Data Protection Regulation, მუხლები 34 და 49; CJEU, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd* [GC], 2010.	**ევროკავშირის კანონმდებლობის დარღვევა მისი ინსტიტუტებისა და ორგანოების მიერ**	

ზოგადად, სამართლებრივი წესების, კერძოდ, მონაცემთა სუბიექტის უფლებების ეფექტიანობა მნიშვნელოვანწილად დამოკიდებულია მათი აღსრულებისათვის საჭირო სათანადო მექანიზმების არსებობაზე. ციფრულ ეპოქაში

მონაცემთა დამუშავება ფართოდ არის გავრცელებული, ხოლო ფიზიკურ პირებისათვის სულ უფრო და უფრო რთულდება მისი მნიშვნელობის გააზრება. მონაცემთა სუბიექტებისა და დამმუშავებლების უფლებამოსილებათა შორის დისბალანსის შესამცირებლად, ფიზიკურ პირებს გარკვეული უფლებები ენიჭებათ, რათა მეტად შეძლონ თავიანთი პერსონალური მონაცემების დამუშავების კონტროლი. საკუთარ მონაცემებზე წვდომისა და მათი შესწორების უფლებები დაცულია ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლის მეორე პუნქტით. ეს დოკუმენტი ევროკავშირის ძირითად კანონმდებლობას ქმნის და მის სამართლებრივ სისტემაში ფუნდამენტური მნიშვნელობა ენიჭება. ევროკავშირის მეორადი კანონმდებლობა, კერძოდ, მონაცემთა დაცვის ზოგადი რეგულაცია, ითვალისწინებს თანმიმდევრულ საკანონმდებლო ჩარჩოს, რომელიც მონაცემთა სუბიექტებს აძლიერებს და გარკვეულ უფლებებს ანიჭებს დამმუშავებლებთან მიმართებით. წვდომისა და გასწორების გარდა, GDPR არაერთ სხვა უფლებასაც აღიარებს, როგორიცაა მონაცემების წაშლა („დავიწყება“), მათი დამუშავების შეწყვეტა და დაბლოკვა, ავტომატიზებული გადაწყვეტილებების მიღება და პროფილირება. მოდერნიზებული 108-ე კონვენცია ითვალისწინებს დაცვის მსგავს მექანიზმებს, რათა მონაცემთა სუბიექტებმა შეძლონ თავიანთი მონაცემების ეფექტიანი კონტროლი. მე-9 მუხლში წარმოდგენილია პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული უფლებები, რომლებიც ფიზიკურ პირებს ენიჭებათ. ხელშემკვრელმა სახელმწიფოებმა, თავიანთი იურისდიქციის ფარგლებში, ამ უფლებებზე წვდომა უნდა უზრუნველყონ მონაცემთა თითოეული სუბიექტისთვის, ეფექტიან სამართლებრივ და პრაქტიკულ საშუალებებთან ერთად, რომლებიც მათ საკუთარი უფლებებით სარგებლობის შესაძლებლობას მისცემს.

ფიზიკურ პირთა უფლებებით აღჭურვის გარდა, მნიშვნელოვანია ისეთი მექანიზმების შექმნაც, რომლებიც მონაცემთა სუბიექტებს საშუალებას მისცემს, გაასაჩივრონ თავიანთი უფლებების დარღვევა, ან მოითხოვონ მონაცემთა დამმუშავებლის პასუხისგებაში მიცემა და კომპენსაცია. ეფექტიანი სამართლებრივი დაცვის უფლება, გარანტირებული ECHR-ითა და ქარტიით, მოითხოვს, რომ სამართლებრივი დაცვის საშუალებები ხელმისაწვდომი იყოს ნებისმიერი პირისთვის.

6.1 მონაცემთა სუბიექტების უფლებები

ძირითადი საკითხები

- მონაცემთა თითოეულ სუბიექტს აქვს უფლება, ნებისმიერი დამმუშავებლისგან მოითხოვოს ინფორმაცია მისი მონაცემების დამუშავების შესახებ, რაც განეკუთვნება შეზღუდულ გამონაკლის შემთხვევებს.

- მონაცემთა სუბიექტებს უნდა ჰქონდეთ შემდეგი უფლებები:
  - შეეძლოთ საკუთარ მონაცემებზე წვდომა და კონკრეტული ინფორმაციის მიღება დამუშავების შესახებ;
  - მოითხოვონ თავიანთი მონაცემების შესწორება მონაცემთა დამმუშავებლის მიერ, თუკი ისინი არაზუსტია;
  - მონაცემთა დამმუშავებელს მოსთხოვონ თავიანთი მონაცემების წაშლა, თუ იგი ამ მონაცემებს უკანონოდ ამუშავებს;
  - მოითხოვონ დამუშავების დროებით დაბლოკვა;
  - გარკვეულ პირობებში, მოითხოვონ თავიანთი მონაცემების გადატანა (პორტირება) სხვა დამმუშავებელთან.
- ამასთან, მონაცემთა სუბიექტებს უნდა ჰქონდეთ უფლება, მოითხოვონ მონაცემთა დამუშავების შეწყვეტა:
  - თავიანთი ინდივიდუალური გარემოებებიდან გამომდინარე;
  - თუ მონაცემები გამოიყენება პირდაპირი მარკეტინგის მიზნებით.
- მონაცემთა სუბიექტებს უფლება აქვთ, მათზე არ მიიღონ მხოლოდ ავტომატიზებული გადაწყვეტილებები - მათ შორის, პროფილირებით - რომლებსაც სამართლებრივი ან სხვა სახის მნიშვნელოვანი შედეგები ექნება ამ პირებისთვის. მათ ასევე, უფლება აქვთ:
  - მოითხოვონ გადაწყვეტილების მიღების პროცესში ადამიანური რესურსის ჩართვა მონაცემთა დამმუშავებლის მიერ;
  - გამოხატონ თავიანთი მოსაზრება და გაასაჩივრონ ავტომატიზებული დამუშავების საფუძველზე მიღებული გადაწყვეტილება.

6.1.1 ინფორმაციის მიღების უფლება

ევროპის საბჭოსა და ევროკავშირის კანონმდებლობით, დამმუშავებლებს ეკისრებათ ვალდებულება, რომ პერსონალური მონაცემების შეგროვებისას მონაცემთა სუბიექტს მიაწოდონ ინფორმაცია დაგეგმილი დამუშავების შესახებ. ეს ვალდებულება დამმუშავებელმა პროაქტიულად უნდა შეასრულოს, მიუხედავად იმისა, მონაცემთა სუბიექტი გამოავლენს თუ არა ინტერესს ამ ინფორმაციის მიმართ.

ევროპის საბჭოს კანონმდებლობაში, მოდერნიზებული 108-ე კონვენციის მე-8 მუხლის თანახმად, ხელშემკვრელი სახელმწიფოები ვალდებულნი არიან, უზრუნველყონ, რომ დამმუშავებელმა მონაცემთა სუბიექტებს აცნობოს თავისი ვინაობა და მუდმივი მისამართი, დამუშავების სამართლებრივი საფუძველი და მიზანი, დამუშავებულ პერსონალურ მონაცემთა კატეგორიები, მათი მიმღებები (ასეთის არსებობის შემთხვევაში) და მე-9 მუხლით გათვალისწინებულ უფლებათა (მონაცემთა წვდომა, შესწორება და სამართლებრივი დაცვა) რეალიზების გზები; ასევე, ნებისმიერი დამატებითი ინფორმაცია, რომელიც საჭიროდ ჩაითვლება პერსონალურ მონაცემთა სამართლიანი და გამჭვირვალე დამუშავებისთვის. მოდერნიზებული 108-ე კონვენციის განმარტებით ბარათში აღნიშნულია, რომ მონაცემთა სუბიექტებისათვის მიწოდებული ინფორმაცია „უნდა იყოს ადვილად ხელმისაწვდომი, გარკვევით შედგენილი, გასაგები და მონაცემთა სუბიექტებზე მორგებული.“[527]

ევროკავშირის კანონმდებლობის თანახმად, გამჭვირვალობის პრინციპი მოითხოვს, რომ ზოგადად, დამუშავებული პერსონალური მონაცემები გამჭვირვალე იყოს ფიზიკური პირებისთვის. მათ უფლება აქვთ, იცოდნენ ისიც, თუ რომელი პერსონალური მონაცემები გროვდება და როგორ, ასევე, რისთვის გამოიყენება ისინი ან რა სახით მუშავდება. ამ პირებს უნდა მიეწოდოთ ინფორმაცია რისკებზე, დაცვის მექანიზმებსა და დამუშავებასთან დაკავშირებულ უფლებებზე. [528] GDPR-ის მე-12 მუხლი მონაცემთა დამმუშავებლისთვის ფართო და ყოვლისმომცველ მოვალეობებს განსაზღვრავს ინფორმაციის გამჭვირვალობისა და/ან მონაცემთა სუბიექტების ინფორმირების კუთხით, თუ როგორ შეუძლიათ სარგებლობა საკუთარი უფლებებით.[529] ინფორმაცია უნდა იყოს მოკლე, გამჭვირვალე, გასაგები, იოლად აღსაქმელი და მარტივი ენით შედგენილი. მონაცემთა სუბიექტებს ის უნდა მიეწოდოთ წერილობითი ფორმით, საჭიროების შემთხვევაში, ელექტრონულად. ინფორმაციის მიწოდება შესაძლებელია ზეპირი ფორმითაც, მონაცემთა სუბიექტის მოთხოვნის საფუძველზე, ასევე, თუ მისი ვინაობა დადასტურდება. ინფორმაცია უნდა მიეწოდოს ზედმეტი დაყოვნების ან ხარჯების გარეშე.[530]

GDPR-ის მე-13 და მე-14 მუხლები შეეხება მონაცემთა სუბიექტების ინფორმირებას მონაცემთა შეგროვებისას როგორც უშუალოდ მათგან, ისე სხვა შემთხვევებში.

527 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 68.

528 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, მუხლი 39.

529 *იქვე*, მუხლები 13 და 14; მოდერნიზებული 108-ე კონვენცია, მუხლი 8(1)(ბ).

530 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 12 (5); მოდერნიზებული 108-ე კონვენცია, მუხლი 9(1)(ბ).

ევროკავშირის კანონმდებლობით გათვალისწინებული ინფორმაციის მიღების უფლების მასშტაბები, ასევე, მასზე დაწესებული შეზღუდვები, განმარტებულია CJEU-ს პრეცედენტულ სამართალში.

მაგალითი: საქმეში *Institut professionnel des agents immobiliers (IPI) v. Englebert*[531] CJEU-ს ეთხოვა 95/46 დირექტივის მე-13 მუხლის პირველი პუნქტის განმარტება. ეს მუხლი წევრ სახელმწიფოებს საშუალებას აძლევს, თვითონ გადაწყვიტონ საკანონმდებლო ღონისძიებათა გატარება ინფორმაციის მიღების უფლების შესაზღუდად, თუკი ეს აუცილებელია სხვათა უფლებებისა და თავისუფლებების დასაცავად, დანაშაულის ან რეგულირებად პროფესიათა ეთიკის დარღვევის ასაცილებლად და გამოძიებისათვის. IPI ბელგიაში უძრავი ქონების აგენტთა პროფესიული ორგანოა, რომლის პასუხისმგებლობაშიც შედის უძრავი ქონების აგენტის პროფესიის შესაბამისობა სათანადო პრაქტიკასთან. IPI-მ ეროვნულ სასამართლოს მიმართა თხოვნით, რომ დაედგინა პროფესიული წესების დარღვევა მოპასუხეთა მიერ და მიეღო გადაწყვეტილება, რომლის მიხედვითაც მოპასუხეებს უნდა შეეწყვიტათ უძრავ ქონებასთან დაკავშირებული სხვადასხვა საქმიანობა. მოთხოვნა ეფუძნებოდა IPI-ს მიერ დაქირავებული კერძო დეტექტივების მიერ წარმოდგენილ მტკიცებულებებს.

ეროვნული სასამართლო ეჭვქვეშ აყენებდა ამ მტკიცებულებებს, ვინაიდან ვარაუდობდა, რომ ბელგიის მონაცემთა დაცვის კანონმდებლობის დარღვევით იყო მოპოვებული. კერძოდ, ამ კანონმდებლობის თანახმად, ინფორმაციის შეგროვებამდე მონაცემთა სუბიექტებს უნდა ეცნობოთ მათი პერსონალური მონაცემების დამუშავების შესახებ.

CJEU-მ განმარტა, რომ მე-13 მუხლის პირველი პუნქტის შესაბამისად, წევრ სახელმწიფოებს „შეუძლიათ“, მაგრამ არ აქვთ ვალდებულება, რომ ეროვნულ კანონმდებლობაში გაითვალისწინონ გამონაკლისები დამუშავებაზე მონაცემთა სუბიექტების ინფორმირებასთან დაკავშირებით. ამ დებულების თანახმად, ფიზიკურ პირთა უფლებების შეზღუდვა დასაშვებია ისეთი მიზეზებით, როგორიცაა დანაშაულის ან ეთიკის დარღვევის პრევენცია, გამოძიება, გამოვლენა და სასჯელის აღსრულება. IPI-ის მსგავს ორგანოსა და კერძო დეტექტივებს, რომლებიც მისი სახელით მოქმედებენ, შეუძლიათ ამ დებულებაზე დაყრდნობა, თუმცა, როცა წევრ სახელმწიფოს ასეთი გამონაკლისი არ აქვს გათვალისწინებული, აუცილებელია მონაცემთა სუბიექტების ინფორმირება.

531 CJEU, C-473/12, *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and Others,* 2013 წლის 7 ნოემბერი.

მაგალითი: საქმეში *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*[532] CJEU-მ განმარტა, რამდენად იძლევა ევროკავშირის კანონმდებლობა უფლებას, რომ ეროვნულმა საჯარო ადმინისტრაციულმა ორგანომ მონაცემები სხვა ასეთივე ორგანოს გადასცეს შემდგომი დამუშავებისთვის, მონაცემთა სუბიექტების წინასწარი ინფორმირების გარეშე. განსახილველ შემთხვევაში, ეროვნული ადმინისტრაციის სააგენტომ წინასწარ არ აცნობა განმცხადებლებს მათი მონაცემების გადაცემა ეროვნული ჯანდაცვის სადაზღვევო ფონდისთვის.

CJEU-მ განმარტა: ევროკავშირის კანონმდებლობით დაწესებული მოთხოვნა, რომ მონაცემთა სუბიექტები ინფორმირებულნი იყვნენ პერსონალური მონაცემების დამუშავების შესახებ, „განსაკუთრებით მნიშვნელოვანია, ვინაიდან ეს გავლენას ახდენს მათ უფლებებზე, როგორიცაა დამუშავებულ მონაცემებზე წვდომა და შესწორება [...], ასევე, მოთხოვნა მონაცემთა დამუშავების შეწყვეტის შესახებ.“ სამართლიანი დამუშავების პრინციპის თანახმად, აუცილებელია, მონაცემთა სუბიექტებს ეცნობოთ მათი მონაცემების სხვა საჯარო ორგანოსთვის გადაცემა, შემდგომი დამუშავების მიზნით. 95/46 დირექტივის მე-13 მუხლის პირველი პუნქტის თანახმად, წევრ სახელმწიფოებს შეუძლიათ შეზღუდვის დაწესება ინფორმაციის მიწოდების უფლებაზე, თუკი ეს აუცილებელია მნიშვნელოვანი ეკონომიკური მიზნისათვის (მაგ.: საგადასახადო საკითხების გადასაჭრელად), თუმცა, ასეთი შეზღუდვა საკანონმდებლო ღონისძიებით უნდა დაწესდეს. ვინაიდან გადასაცემი მონაცემების განმარტება და გადაცემის პირობები გათვალისწინებული იყო არა საკანონმდებლო ღონისძიებით, არამედ ორ საჯარო უწყებას შორის გაფორმებული ოქმით, ეს შემთხვევა ვერ აკმაყოფილებდა ევროკავშირის კანონმდებლობით დადგენილ საგამონაკლისო პირობებს. შესაბამისად, განმცხადებლებისთვის წინასწარ უნდა ეცნობებინათ მათი მონაცემების გადაცემა ეროვნული ჯანდაცვის სადაზღვევო ფონდისთვის და შემდგომი დამუშავება.

ინფორმაციის შინაარსი

მოდერნიზებული 108-ე კონვენციის მე-8 მუხლის პირველი პუნქტის თანახმად, დამმუშავებელი ვალდებულია, მონაცემთა სუბიექტს მიაწოდოს ნებისმიერი ინფორმაცია, რომელიც უზრუნველყოფს მონაცემთა სამართლიან და გამჭვირვალე დამუშავებას, მათ შორის:

- მონაცემთა დამმუშავებლის ვინაობა, მუდმივი საცხოვრებელი ან რეგისტრაციის ადგილი;

532 CJEU, C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others,* 2015 წლის 1 ოქტომბერი.

- დაგეგმილი დამუშავების სამართლებრივი საფუძველი და მიზნები;
- დამუშავებული პერსონალური მონაცემების კატეგორიები;
- მონაცემთა მიმღები ან მიმღებთა კატეგორიები, ასეთის არსებობის შემთხვევაში;
- მონაცემთა სუბიექტების მიერ უფლებებით სარგებლობის გზები.

GDPR-ის თანახმად, როდესაც დამმუშავებელი პერსონალურ ინფორმაციას აგროვებს უშუალოდ მონაცემთა სუბიექტისგან, ვალდებულია, მიღების მომენტში მას მიაწოდოს შემდეგი ინფორმაცია:[533]

- დამმუშავებლისა და პერსონალურ მონაცემთა დაცვის ოფიცრის (ასეთის არსებობის შემთხვევაში) ვინაობა და საკონტაქტო ინფორმაცია;
- მონაცემთა დამუშავების მიზნები და სამართლებრივი საფუძველი (კონტრაქტი ან სამართლებრივი ვალდებულება);
- მონაცემთა დამმუშავებლის კანონიერი ინტერესები, თუ დამუშავების საფუძველი ეს ინტერესებია;
- მონაცემთა მიმღების ვინაობა ან მიმღებთა კატეგორიები (ასეთის არსებობის შემთხვევაში);
- გადაეცემა თუ არა მონაცემები მესამე ქვეყანას ან საერთაშორისო ორგანიზაციას, ასევე, რამდენად ეფუძნება ეს შესაბამისობის გადაწყვეტილებასა და უსაფრთხოების სათანადო ზომებს;
- მონაცემთა შენახვის ვადა, ან, თუ ეს შეუძლებელია, ვადის განსაზღვრის კრიტერიუმები;
- მონაცემთა სუბიექტების უფლებები დამუშავების კუთხით, მათ შორის, როგორიცაა მოთხოვნა მონაცემთა წვდომის, გასწორების, დაბლოკვის, წაშლის, განადგურების ან დამუშავების შეწყვეტის შესახებ;
- თუ პერსონალური მონაცემების მიწოდებას ითვალისწინებს კანონი ან კონტრაქტი, რამდენად ვალდებულია მონაცემთა სუბიექტი, რომ წარმოადგინოს თავისი პერსონალური ინფორმაცია; ასევე, როგორი იქნება ამ ვალდებულების შეუსრულებლობის შედეგები;

533 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 13 (1).

- თუ გადაწყვეტილება არ მიიღება ავტომატიზებულად, მათ შორის, პროფილირებით;
- საზედამხედველო ორგანოსთვის საჩივრით მიმართვის უფლება;
- თანხმობის გამოთხოვის უფლება.

გადაწყვეტილების ავტომატიზებულად მიღების, მათ შორის, პროფილირების შემთხვევაში, დამმუშავებელი ვალდებულია, მონაცემთა სუბიექტებს მიაწოდოს მნიშვნელოვანი/არსებითი ინფორმაცია გამოყენებულ ლოგიკაზე/კრიტერიუმებზე, მათ საჭიროებასა და მონაცემთა სუბიექტისათვის შესაძლო შედეგებზე.

თუ ინფორმაცია არ გროვდება უშუალოდ მონაცემთა სუბიექტისაგან, დამმუშავებელი ვალდებულია, ფიზიკურ პირს შეატყობინოს პერსონალური მონაცემების წყარო. ასეთ შემთხვევაში, დამმუშავებელი ვალდებულია, მონაცემთა სუბიექტს აცნობოს გადაწყვეტილების ავტომატიზებულად მიღების, მათ შორის, პროფილირების შესახებ.[534] და ბოლოს, თუ დამმუშავებელი გეგმავს მონაცემთა შემდგომ დამუშავებას თავდაპირველი მიზნისგან განსხვავებული ამოცანებით, მიზნის შეზღუდვისა და გამჭვირვალობის პრინციპების თანახმად, იგი ვალდებულია, დამუშავების დაწყებამდე აცნობოს სუბიექტს ამის შესახებ. როცა იცვლება მონაცემთა დამუშავების მიზანი, ან მას ემატება სხვა ამოცანები, დამმუშავებელმა მონაცემთა სუბიექტისგან უნდა მიიღოს განახლებული თანხმობა.

ინფორმაციის მიწოდების ვადები

GDPR განასხვავებს ორ სცენარს და მონაცემთა დამმუშავებლის მიერ მონაცემთა სუბიექტის ინფორმირების ორ ვადას:

- თუ პერსონალური მონაცემები გროვდება უშუალოდ მონაცემთა სუბიექტისაგან, დამმუშავებელი ვალდებულია, მას მიაწოდოს შესაბამისი ინფორმაცია და განუმარტოს GDPR-ით გათვალისწინებული უფლებები მონაცემთა მოპოვებისას.[535]

  როდესაც მონაცემთა დამმუშავებელი გეგმავს მონაცემთა შემდგომ დამუშავებას განსხვავებული მიზნისთვის, იგი ვალდებულია, შესაბამისი ინფორმაცია სუბიექტს მიაწოდოს შემდგომი დამუშავების დაწყებამდე.

534 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 13 (2) და 14 (2) (ვ).

535 *იქვე,* მუხლი 13 (1)(2), შესავალი ნაწილი, სადაც რეგულაცია მიუთითებს ინფორმაციის მიწოდებაზე „პერსონალური მონაცემების მიღებისას“.

- თუ მონაცემები უშუალოდ მონაცემთა სუბიექტისგან არ გროვდება, დამმუშავებელი ვალდებულია, ინფორმაცია დამუშავების შესახებ მიაწოდოს „მონაცემთა შეგროვებიდან გონივრულ ვადაში, არაუგვიანეს ერთ თვეში“, ან მონაცემების მესამე პირისთვის გადაცემამდე.[536]

მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათის თანახმად, თუ დამუშავების დაწყებისას მონაცემთა სუბიექტების ინფორმირება შეუძლებელია, ამის გაკეთება დასაშვებია მოგვიანებითაც (მაგ.: როდესაც მონაცემთა დამმუშავებელი მონაცემთა სუბიექტს რაიმე მიზეზის გამო დაუკავშირდება).[537]

ინფორმაციის მიწოდების გზები

როგორც ევროპის საბჭოს, ისე ევროკავშირის კანონმდებლობით, დამმუშავებელმა მონაცემთა სუბიექტს უნდა მიაწოდოს მოკლე, გამჭვირვალე, გასაგები და ადვილად ხელმისაწვდომი ინფორმაცია, წერილობით ან სხვა ფორმით, მათ შორის, ელექტრონულად, და მკაფიო, მარტივი ენით. ინფორმაციის ცხადი და გასაგები ფორმით მისაწოდებლად, დამმუშავებელს შეუძლია სტანდარტიზებული სიმბოლოების გამოყენება[538] (მაგ.: მონაცემთა უსაფრთხო შეგროვება და/ან დაშიფვრა შეიძლება გამოისახოს ბოქლომის სიმბოლოს მეშვეობით). მონაცემთა სუბიექტებს შეუძლიათ, მოითხოვონ ინფორმაციის ზეპირი ფორმით მიღება. ინფორმირება უნდა იყოს უფასო, გარდა იმ შემთხვევისა, როცა მონაცემთა სუბიექტის მოთხოვნები აშკარად დაუსაბუთებელი ან გადაჭარბებულია (მაგ.: განმეორებითი მოთხოვნები).[539] მიწოდებული ინფორმაციის ადვილად ხელმისაწვდომობას უაღრესად დიდი მნიშვნელობა აქვს მონაცემთა სუბიექტის მიერ ევროკავშირის მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული უფლებებით სარგებლობისათვის.

სამართლიანი დამუშავების პრინციპის თანახმად, ინფორმაცია ადრესატს უნდა გადაეცეს ადვილად გასაგები და მასზე მორგებული ენით. მონაცემთა სუბიექტის ინფორმირების ენა და ტიპი განსხვავდება და დამოკიდებულია სამიზნე აუდიტორიაზე (მაგ.: ზრდასრული ადამიანია, ბავშვი, ფართო საზოგადოება თუ აკადემიური ექსპერტი). ეს საკითხი განხილულია 29-ე სამუშაო ჯგუფის მოსაზრებაში ინფორმაციის დაბალანსებულად მიწოდების თაობაზე.

536 *იქვე,* მუხლები 13 (3) და 14 (3); ასევე, იხ: მითითება გონივრულ ინტერვალებსა და ინფორმაციის ზედმეტი დაყოვნების გარეშე მიწოდებაზე, რომელსაც ითვალისწინებს მოდერნიზებული 108-ე კონვენცია, მუხლი 8 (1) (ბ).

537 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 70.

538 ევროკომისია უფლებამოსილია, მიიღოს დელეგირებული აქტები სტანდარტიზებული სიმბოლოებით გადმოცემული ინფორმაციისა და ამ სიმბოლოების მიწოდების პროცედურის დასადგენად. იხ: მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 12 (8).

539 *იქვე,* მუხლი 12 (1)(5)(7) და მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1) (ბ).

მოსაზრება ყურადღებას ამახვილებს ე.წ. „მრავალდონიან შეტყობინებაზე“,[540] რომელიც მონაცემთა სუბიექტს საშუალებას აძლევს, თვითონ გადაწყვიტოს, რამდენად დეტალური ინფორმაციის მიღება სურს. ამავდროულად, ინფორმაციის ასეთი ფორმით წარდგენა მონაცემთა დამმუშავებელს არ ათავისუფლებს GDPR-ის მე-13 და მე-14 მუხლებით გათვალისწინებული მოვალეობებისგან. იგი ვალდებულია, მონაცემთა სუბიექტს მიაწოდოს ყველა სახის ინფორმაცია.

ინფორმაციის მიწოდების ერთ-ერთი ყველაზე ეფექტიანი გზა გახლავთ სათანადო ინფორმაციის (მაგ.: ვებგვერდის ე.წ. კონფიდენციალობის პოლიტიკის (privacy policy)) განთავსება მონაცემთა დამმუშავებლის მთავარ გვერდზე (home page). თუმცა, კომპანიისა თუ სახელმწიფო ორგანოს საინფორმაციო პოლიტიკა უნდა ითვალისწინებდეს, რომ მოსახლეობის მნიშვნელოვანი ნაწილი ინტერნეტს არ მოიხმარს.

ვებგვერდზე განთავსებული განაცხადი კონფიდენციალობის შესახებ შეიძლება გამოიყურებოდეს შემდეგნაირად:

ვინ ვართ ჩვენ?

„მონაცემთა დამმუშავებელი“ არის Bed and Breakfast C&U, რომელიც დაარსდა [მისამართი: xxx], ტელეფონი: xxx; ფაქსი: xxx; ელფოსტა: info@c&u.com; მონაცემთა დაცვის ოფიცრის საკონტაქტო მონაცემები: [xxx].

პერსონალურ მონაცემთა დამუშავებაზე ინფორმირება ჩვენი სასტუმროს მომსახურებისა და წესების ნაწილია.

რა სახის ინფორმაციას ვაგროვებთ თქვენგან?

ჩვენ ვაგროვებთ შემდეგი სახის პერსონალურ ინფორმაციას: სახელი, საფოსტო მისამართი, ტელეფონის ნომერი, ელფოსტა, სასტუმროში დარჩენის შესახებ ინფორმაცია, საკრედიტო და სადებეტო ბარათების ნომრები და ჩვენს ვებგვერდთან დასაკავშირებლად გამოყენებული IP მისამართები ან დომენური სახელები (domain names).

რატომ ვაგროვებთ თქვენს მონაცემებს?

ამ მონაცემებს ვამუშავებთ თქვენი თანხმობის საფუძველზე, ჯავშნების განსახორციელებლად, რათა გავაფორმოთ და შევასრულოთ ჩვენ მიერ

540 29-ე მუხლის სამუშაო ჯგუფი (2004), მოსაზრება 10/2004 ინფორმაციის მიწოდების ჰარმონიზების გაუმჯობესებაზე, WP 100, ბრიუსელი, 2004 წლის 25 ნოემბერი.

შემოთავაზებულ სერვისებთან დაკავშირებული კონტრაქტები, ასევე, კანონმდებლობით დაკისრებული მოვალეობები (მაგ.: „ადგილობრივი მოსაკრებლების შესახებ აქტის“ თანახმად, ვალდებულნი ვართ, შევაგროვოთ პერსონალური მონაცემები ტურისტებზე დაწესებული გადასახადის (city tax) დასაფარად).

როგორ ვამუშავებთ თქვენს მონაცემებს?

ამ მონაცემებს ვინახავთ 3 თვის ვადით. მათზე არ ვრცელდება გადაწყვეტილების ავტომატიზებულად მიღების პროცედურები.

ჩვენი კომპანია Bed and Breakfast C&U იცავს უსაფრთხოების მკაცრ პროცედურებს, რათა თავიდან ავიცილოთ თქვენი პერსონალური ინფორმაციის დაზიანება, განადგურება, მესამე პირისთვის უნებართვოდ გადაცემა ან არასანქცირებული წვდომა. კომპიუტერები, რომელზეც ინახება ეს ინფორმაცია, განთავსებულია უსაფრთხო გარემოში და მათზე წვდომა გამკაცრებულია. უსაფრთხოებისათვის ვიყენებთ დამცავ ზღუდეებს (firewalls) და სხვა ზომებს ელექტრონული წვდომის შესაზღუდად. მონაცემთა მესამე პირისათვის გადაცემის აუცილებლობის შემთხვევაში, მათგან ვითხოვთ უსაფრთხოების იმავე ზომებს.

შეგროვებული და აღრიცხული მონაცემები ჩვენს ოფისებში ინახება და მათზე წვდომის უფლება აქვთ მხოლოდ იმ პირებს, რომელთაც ეს ინფორმაცია სჭირდებათ ხელშეკრულებით გათვალისწინებული ვალდებულებების შესასრულებლად. თუ გვჭირდება ინფორმაცია თქვენი იდენტიფიცირებისათვის, ამის შესახებ პირდაპირ და ნათლად გეკითხებით. ინფორმაციის გამჟღავნებამდე შესაძლოა გთხოვოთ უსაფრთხოების შემოწმების (security check) გავლა. პერსონალური ინფორმაციის განახლება შეგიძლიათ ნებისმიერ დროს, ჩვენთან პირდაპირ კავშირის გზით.

რა უფლებები გენიჭებათ?

თქვენ გაქვთ უფლება, მოითხოვოთ საკუთარ პერსონალურ მონაცემებზე წვდომა, მონაცემთა ასლის მიღება, მათი წაშლა და გასწორება, ასევე, სხვა მონაცემთა დამმუშავებელთან გადატანა (პორტირება).

მოთხოვნების გამოგზავნა შეგიძლიათ ელფოსტით, მისამართზე: info@c&u.com. ვალდებულნი ვართ, თხოვნაზე პასუხი გაგცეთ ერთი თვის ვადაში. თუ ეს რთულია ან ერთდროულად ბევრ მოთხოვნას ვიღებთ, პასუხის გასაცემად, შეიძლება 2 თვე დაგვჭირდეს, რის შესახებაც შეგატყობინებთ.

თქვენს პერსონალურ მონაცემებზე წვდომა

თქვენ გაქვთ უფლება: მოთხოვნისთანავე გქონდეთ საკუთარ პერსონალურ მონაცემებზე წვდომა; მიიღოთ ინფორმაცია მონაცემთა დამუშავების მიზნებზე; მოითხოვოთ მონაცემთა წაშლა ან გასწორება; არ დაექვემდებაროთ ცალსახა და ავტომატიზებულ გადაწყვეტილებას, თქვენი მოსაზრების გაუთვალისწინებლად. მოთხოვნების გამოგზავნა შეგიძლიათ ელფოსტით, მისამართზე: info@c&u.com. ასევე, შეგიძლიათ, მოითხოვოთ დამუშავების შეწყვეტა, გამოითხოვოთ თანხმობა, შეიტანოთ საჩივარი ეროვნულ საზედამხედველო ორგანოში, თუკი მიიჩნევთ, რომ მონაცემები კანონის დარღვევით მუშავდება, და მოითხოვოთ უკანონო დამუშავებით მიყენებული ზიანის ანაზღაურება.

საჩივრის შეტანის უფლება

GDPR-ის თანახმად, პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შემთხვევაში, დამმუშავებელი ვალდებულია, მონაცემთა სუბიექტებს აცნობოს ეროვნული და ევროკავშირის კანონმდებლობით გათვალისწინებული აღსრულების მექანიზმების შესახებ; ასევე, განუმარტოს უფლება, რომ ამ ფაქტზე საჩივრის შეტანა შეუძლიათ საზედამხედველო ორგანოსა და, საჭიროების შემთხვევაში, სასამართლოში.[541] ამავდროულად, ევროპის საბჭოს კანონმდებლობა ითვალისწინებს მონაცემთა სუბიექტების უფლებას, მიიღონ ინფორმაცია თავიანთი უფლებებით სარგებლობის საშუალებებზე, როგორიცაა ქმედითი სამართლებრივი მისაგებელი, გათვალისწინებული მე-8 მუხლის 1 (ვ) პუნქტით.

გამონაკლისები შეტყობინების ვალდებულებასთან დაკავშირებით

GDPR ითვალისწინებს გამონაკლის შემთხვევებს შეტყობინების ვალდებულებასთან დაკავშირებით, კერძოდ, მე-13 მუხლის მე-4 პუნქტისა და მე-14 მუხლის მე-5 პუნქტის თანახმად, ინფორმაციის მიწოდება არ არის სავალდებულო, თუ მონაცემთა სუბიექტი უკვე ფლობს ყველა სათანადო ინფორმაციას.[542] ამასთან, როცა პერსონალური მონაცემები არ გროვდება მონაცემთა სუბიექტისგან, შეტყობინების ვალდებულება არ ვრცელდება ისეთ შემთხვევებზე, როდესაც ინფორმაციის მიწოდება შეუძლებელია, ან უკავშირდება არაპროპორციულად დიდ ძალისხმევას (მაგ.: პერსონალური მონაცემები მუშავდება

541 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 13 (2) (დ) და 14 (2) (ე); მოდერნიზებული 108-ე კონვენცია, მუხლი 8 (1) (ვ).

542 *იქვე*, მუხლი 13 (4) და 14 (5) (ა).

საჯარო ინტერესის ფარგლებში მონაცემთა არქივირების, სამეცნიერო/ისტორიული კვლევის, ან სტატისტიკური მიზნებით).[543]

ამასთან, GDPR-ის თანახმად, წევრი სახელმწიფოები გარკვეული დისკრეციით (მოქმედების თავისუფლებით) სარგებლობენ რეგულაციით გათვალისწინებულ მოვალეობებსა და უფლებებზე შეზღუდვების დაწესებისას, თუ ეს აუცილებელი და პროპორციული ღონისძიებაა დემოკრატიულ საზოგადოებაში (მაგ.: ეროვნული და საზოგადოებრივი უსაფრთხოების დაცვა; სასამართლო გამოძიება; ეკონომიკური, ფინანსური, ან კერძო ინტერესების (თუ მათი მნიშვნელობა აღემატება მონაცემთა დაცვის ინტერესებს) დაცვა.[544]

ნებისმიერი გამონაკლისი ან შეზღუდვა უნდა იყოს აუცილებელი დემოკრატიულ საზოგადოებაში და დასახული მიზნის პროპორციული. გამონაკლის შემთხვევებში (მაგ.: სამედიცინო მიზეზების გამო), შეიძლება მონაცემთა სუბიექტის დაცვა საჭიროებდეს გამჭვირვალობის შეზღუდვას. ეს განსაკუთრებულად ეხება შეზღუდვის დაწესებას მონაცემთა თითოეული სუბიექტის წვდომის უფლებაზე. [545] ამავდროულად, მინიმალური დაცვის სახით, ეროვნული კანონმდებლობა პატივს უნდა სცემდეს ევროკავშირის კანონმდებლობით დაცული უფლებებისა და თავისუფლებების ძირითად არსს,[546] კერძოდ: შეიცავდეს დებულებებს, სადაც დაკონკრეტდება დამუშავების მიზნები, დამუშავებულ პერსონალურ მონაცემთა კატეგორიები, უსაფრთხოების ზომები და სხვა საპროცედურო მოთხოვნები.[547]

როდესაც მონაცემები გროვდება საჯარო ინტერესში შემავალი სამეცნიერო/ისტორიული კვლევის ან სტატისტიკური მიზნებით, ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობა შეიძლება ითვალისწინებდეს გამონაკლისებს ინფორმაციის მიწოდების ვალდებულებასთან დაკავშირებით, თუკი ამ უფლების განხორციელებით შეუძლებელი ხდება ან სერიოზულად რთულდება კონკრეტული მიზნების მიღწევა.[548]

მსგავსი შეზღუდვები არსებობს ევროპის საბჭოს კანონმდებლობაშიც: მოდერნიზებული 108-ე კონვენციის მე-9 მუხლით დაცული მონაცემთა სუბიექტის უფლებები შეიძლება შეიზღუდოს მე-11 მუხლით მკაცრად განსაზღვრულ პირობებში. ამასთან, კონვენციის მე-8 მუხლის მე-2 პუნქტის თანახმად, მონაცემთა დამმუშავებელზე დაკისრებული გამჭვირვალობის მოვალეობა არ ვრცელდება იმ შემთხვევებზე, როდესაც მონაცემთა სუბიექტი უკვე ფლობს შესაბამის ინფორმაციას.

543 *იქვე,* მუხლი 14 (5) (ბ)–(ე).

544 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 23 (14).

545 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 15.

546 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 23 (1).

547 *იქვე,* მუხლი 23 (2).

548 *იქვე,* მუხლი 89 (2) (3).

ფიზიკური პირის წვდომის უფლება საკუთარ მონაცემებზე

ევროპის საბჭოს კანონმდებლობაში საკუთარ მონაცემებზე წვდომის უფლებას მკაფიოდ აღიარებს მოდერნიზებული 108-ე კონვენციის მე-9 მუხლი. კერძოდ, თითოეულ ფიზიკურ პირს აქვს უფლება, მოთხოვნისთანავე მიიღოს ინფორმაცია საკუთარი პერსონალური მონაცემების დამუშავებაზე. ეს ინფორმაცია მონაცემთა სუბიექტს უნდა გადაეცეს იოლად აღსაქმელი ფორმით. წვდომის უფლება აღიარებულია ECtHR-ის პრეცედენტული სამართლითაც. კერძოდ, მან არაერთ საქმეზე დაადგინა, რომ ფიზიკურ პირს აქვს საკუთარ პერსონალურ მონაცემებზე წვდომის უფლება, რომელიც მომდინარეობს პირადი ცხოვრების პატივისცემის აუცილებლობიდან.[549] ამავდროულად, გარკვეულ ვითარებაში, შეიძლება შეიზღუდოს წვდომა საჯარო და კერძო ორგანიზაციების მიერ შენახულ პერსონალურ მონაცემებზე.[550]

ევროკავშირის კანონმდებლობაში პერსონალურ მონაცემებზე წვდომის უფლება მკაფიოდ აღიარებულია GDPR-ის მე-15 მუხლით და მიიჩნევა ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლის მე-2 პუნქტით გარანტირებული მონაცემთა დაცვის ფუნდამენტური უფლების ერთ-ერთ ელემენტად.[551] ფიზიკური პირის უფლება, ჰქონდეს წვდომა საკუთარ პერსონალურ მონაცემებზე, ევროპის მონაცემთა დაცვის კანონმდებლობის ძირითადი კომპონენტია.[552]

GDPR-ის თანახმად, მონაცემთა თითოეულ სუბიექტს ენიჭება წვდომის უფლება თავის პერსონალურ მონაცემებსა და დამუშავების შესახებ ინფორმაციაზე, რომელიც დამმუშავებელმა უნდა მიაწოდოს.[553] კერძოდ, მონაცემთა თითოეულ სუბიექტს აქვს უფლება, დამმუშავებლისგან მოითხოვოს დასტური თავისი მონაცემების დამუშავების შესახებ და ეცნობოს:

- დამუშავების მიზნები;

---

549 ECtHR, *Gaskin v. the United Kingdom,* No. 10454/83, 1989 წლის 7 ივლისი; ECtHR, *Odièvre v. France* [GC], No. 42326/98, 2003 წლის 3 თებერვალი; ECtHR, *K.H. and Others v. Slovakia,* No. 32881/04, 2009 წლის 28 აპრილი; ECtHR, *Godelli v. Italy,* No. 33783/09, 2012 წლის 25 სექტემბერი.

550 ECtHR, *Leander v. Sweden,* No. 9248/81, 1987 წლის 26 მარტი.

551 ასევე, იხ. CJEU, გაერთიანებული საქმეები: C-141/12 და C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* და *Minister voor Immigratie, Integratie en Asiel v. M and S,* 2014 წლის 17 ივლისი; CJEU, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission,* 2015 წლის 16 ივლისი.

552 CJEU, გაერთიანებული საქმეები: C-141/12 და C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S,* 2014 წლის 17 ივლისი.

553 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 15 (1).

- დამუშავებულ მონაცემთა კატეგორიები;
- მონაცემთა მიმღების ვინაობა, ან კატეგორია;
- მონაცემთა შენახვის ვადა. თუ ეს შეუძლებელია, ვადის განსაზღვრის კრიტერიუმები;
- მონაცემთა სუბიექტის უფლება, რომ შეუძლია მოითხოვოს მის შესახებ არსებული მონაცემების გასწორება, წაშლა ან დაბლოკვა;
- საზედამხედველო ორგანოში საჩივრის შეტანის უფლება;
- თუ მონაცემები არ გროვდება უშუალოდ მონაცემთა სუბიექტისგან, ნებისმიერი ხელმისაწვდომი ინფორმაცია მათი შეგროვების წყაროზე;
- ავტომატიზებული გადაწყვეტილებების შემთხვევაში, ინფორმაცია მონაცემთა ავტომატური დამუშავებისას გამოყენებული ლოგიკის/კრიტერიუმების შესახებ.

დამმუშავებელი ვალდებულია, მონაცემთა სუბიექტს მიაწოდოს დამუშავებული პერსონალური მონაცემების ასლი და ნებისმიერი ინფორმაცია გადასცეს იოლად აღსაქმელი ფორმით. ეს ნიშნავს, რომ მან უნდა გააგებინოს მონაცემთა სუბიექტს მიწოდებული ინფორმაციის მნიშვნელობა (მაგ.: წვდომის მოთხოვნაზე პასუხად, ტექნიკური აბრევიატურების, კოდირებული ტერმინების ან აკრომინების მიწოდება, როგორც წესი, უკმარია, თუკი ამ ტერმინების მნიშვნელობა არ არის განმარტებული; ავტომატიზებულ გადაწყვეტილებათა მიღების, მათ შორის, პროფილირების დროს, უნდა განიმარტოს გამოყენებული ზოგადი ლოგიკა, როგორიცაა მონაცემთა სუბიექტის შეფასების კრიტერიუმები. ევროპის საბჭოს კანონმდებლობა იმავე მოთხოვნებს ითვალისწინებს.[554]

მაგალითი: საკუთარ პერსონალურ მონაცემებზე წვდომის შემთხვევაში, მონაცემთა სუბიექტი შეძლებს მათი სიზუსტის შეაფასებას. შესაბამისად, აუცილებელია მისი ინფორმირება იოლად აღსაქმელი ფორმით, არა მხოლოდ დამუშავებულ პერსონალურ მონაცემებზე, არამედ იმ კატეგორიებზეც, რომელთა ფარგლებშიც მუშავდება ისინი (მაგ.: სახელი, IP მისამართი, ადგილმდებარეობა, საკრედიტო ბარათის ნომერი და ა.შ.)

როდესაც მონაცემები არ გროვდება პირდაპირ მონაცემთა სუბიექტისგან, წყაროზე ინფორმაცია (თუკი ასეთი არსებობს) უნდა გაიგზავნოს წვდომის მოთხოვნის საპასუხოდ. ეს უნდა გავიგოთ სამართლიანობის, გამჭვირვალობისა და ანგარიშვალდებულების პრინციპის კონტექსტში. მონაცემთა დამმუ-

554 იხ. მოდერნიზებული 108-ე კონვენცია, მუხლი 8 (1) (გ).

შავებელმა არ უნდა გაანადგუროს ინფორმაცია მონაცემთა წყაროს შესახებ მისი გამჟღავნების ვალდებულებისგან გასათავისუფლებლად - გარდა იმ შემთხვევისა, როდესაც მონაცემები წაიშლებოდა წვდომაზე მოთხოვნის მიღების მიუხედავად - და მაინც უნდა დაემორჩილოს ზოგადი „ანგარიშვალდებულების“ მოთხოვნას.

CJEU-ს პრეცედენტული სამართლის თანახმად, დაუშვებელია პერსონალურ მონაცემებზე წვდომის გადაჭარბებულად შეზღუდვა გარკვეული ვადების დაწესებით. მონაცემთა სუბიექტს გონივრული შესაძლებლობა უნდა მიეცეს, რომ მიიღოს ინფორმაცია წარსულში განხორციელებულ დამუშავების ოპერაციებზე.

მაგალითი: *Rijkeboer*-ის საქმეში[555] CJEU-ს უნდა ემსჯელა, შეიძლება თუ არა, რომ ფიზიკური პირის წვდომა პერსონალურ მონაცემთა მიმღებებზე, მათ კატეგორიებსა და მონაცემთა შინაარსზე შეიზღუდოს მოთხოვნამდე ერთწლიანი პერიოდით.

იმის დასადგენად, თუ რამდენად იძლევა ევროკავშირის კანონმდებლობა ამგვარი შეზღუდვის დაწესების შესაძლებლობას, სასამართლომ გადაწყვიტა, განემარტა მე-12 მუხლი, დირექტივის მიზნებიდან გამომდინარე. პირველ რიგში, მან განაცხადა: წვდომა აუცილებელია იმისათვის, რომ ფიზიკურმა პირმა შეძლოს ისეთი უფლებებით სარგებლობა, როგორიცაა: მონაცემთა გასწორება, წაშლა ან დაბლოკვა, ან ამის შეტყობინება იმ მესამე პირებისთვის, რომლებსაც გადაეცათ მონაცემები; ასევე, მონაცემთა დამუშავების შეწყვეტა, საჩივრის შეტანა და ზიანის ანაზღაურების მოთხოვნა.[556] მონაცემთა სუბიექტებისათვის მინიჭებული უფლების პრაქტიკული ეფექტის მისაღებად, CJEU-მ დაადგინა, რომ „უფლება აუცილებლად უნდა უკავშირდებოდეს წარსულს. წინააღმდეგ შემთხვევაში, მონაცემთა სუბიექტი ეფექტიანად ვერ შეძლებს უკანონოდ ან არასწორად მიჩნეული ინფორმაციის გასწორებას, წაშლას ან დაბლოკვას, ანდა სარჩელის შეტანასა და ზიანის ანაზღაურებას.“

6.1.2 მონაცემთა გასწორების უფლება

ევროკავშირისა და ევროპის საბჭოს კანონმდებლობათა შესაბამისად, მონაცემთა სუბიექტებს ენიჭებათ უფლება, მოითხოვონ თავიანთი პერსონალური მონაცემების გასწორება. მათი სიზუსტე აუცილებელია მონაცემთა სუბიექტების პერსონალური ინფორმაციის მაღალ დონეზე დასაცავად.[557]

555 CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 2009 წლის 7 მაისი.

556 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები: 15 (1) (გ) (ვ), 16, 17 (2) და 21; ასევე, თავი VIII.

557 *იქვე*, მუხლი 16; პრეამბულა, პუნქტი 65; მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1) (ე).

მაგალითი: საქმეში *Ciubotaru v. Moldova*[558] განმცხადებელმა ვერ შეძლო სახელმწიფო რეესტრში მისი ეთნიკური წარმომავლობის შესახებ ჩანაწერი - „მოლდოველი“ - შეეცვლა „რუმინელით“. რეესტრის განცხადებით, მან ვერ დაასაბუთა საკუთარი მოთხოვნა. EctHR-მა დასაშვებად მიიჩნია ფიზიკური პირის ეთნიკური წარმომავლობის რეგისტრაციისათვის ობიექტური მტკიცებულებების მოთხოვნა სახელმწიფოების მხრიდან, ხოლო თუ პირის მოთხოვნა სუბიექტურ და დაუსაბუთებელ გარემოებებს ეფუძნებოდა, ხელისუფლებას ჰქონდა მასზე უარის თქმის უფლება. განმცხადებლის მოთხოვნა არ ეყრდნობოდა მხოლოდ სუბიექტურ ვარაუდებს, მან შეძლო, წარმოედგინა ობიექტურად დადასტურებული კავშირები რუმინულ ეთნიკურ ჯგუფებთან (მაგ.: ენა, სახელი, ემპათია/კავშირი და სხვა). თუმცა, შიდასახელმწიფოებრივი კანონმდებლობით, განმცხადებელს მოეთხოვებოდა მტკიცებულების წარდგენა, რომ მისი მშობლები რუმინულ ეთნიკურ ჯგუფს მიეკუთვნებოდნენ. მოლდოვაში არსებული ისტორიული რეალობის გათვალისწინებით, ამ მოთხოვნამ დაუძლეველი ბარიერი წარმოშვა ისეთი ეთნიკური წარმომავლობის დასარეგისტრირებლად, რომელიც განსხვავდებოდა მის მშობლებთან მიმართებით საბჭოთა ხელისუფლების მიერ გაკეთებული ჩანაწერისგან. მიუხედავად ობიექტური მტკიცებულებისა, განმცხადებელს მოთხოვნის განხილვაზე უარი უთხრეს. შესაბამისად, სახელმწიფომ ვერ შეძლო, შეესრულებინა მასზე დაკისრებული პოზიტიური ვალდებულება, რომელიც გულისხმობს განმცხადებლის პირადი ცხოვრების პატივისცემის უფლების ეფექტიანად დაცვას. სასამართლომ საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

გარკვეულ შემთხვევებში, საკმარისია, მონაცემთა სუბიექტმა უბრალოდ მოითხოვოს, მაგალითად, სახელის მართლწერაში დაშვებული შეცდომის გასწორება, ან მისამართისა თუ ტელეფონის ნომრის შეცვლა. ევროკავშირისა და ევროპის საბჭოს კანონმდებლობების თანახმად, აუცილებელია მცდარი პერსონალური მონაცემების გასწორება ყოველგვარი ზედმეტი დაყოვნების გარეშე.[559] თუ ასეთი მოთხოვნა უკავშირდება სამართლებრივი მნიშვნელობის საკითხებს, როგორიცაა მონაცემთა სუბიექტის სამართლებრივი იდენტობა ან სამართლებრივი დოკუმენტების მისაღებად სწორი საცხოვრებელი ადგილის მითითება, გასწორების მოთხოვნა შეიძლება არ იყოს საკმარისი. ასეთ შემთხვევებში, მონაცემთა დამმუშავებელს უფლება აქვს, მოითხოვოს შესაძლო უზუსტობის დამადასტურებელი მტკიცებულება. ამგვარი მოთხოვნა არ უნდა აკისრებდეს მონაცემთა სუბიექტს მტკიცების არაგონივრულ ტვირთს ან აფერხებდეს მისი მონაცემების გასწორების შესაძლებლობას. EctHR-მა არაერთ საქმეში დაადგინა ECHR-ის მე-8 მუხლის დარღვევა იმის გამო, რომ განმ-

558 ECtHR, *Ciubotaru v. Moldova,* No. 27138/04, 2010 წლის 27 აპრილი, პუნქტები 51 და 59.

559 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 16; მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1).

ცხადებლებმა ვერ შეძლეს, სადავო გაეხადათ მათ შესახებ საიდუმლო რეესტრებში არსებული მონაცემების სისწორე. [560]

> მაგალითი: საქმეში *Canli v. Turkey*[561] ECtHR-მა დაადგინა კონვენციის მე-8 მუხლის დარღვევა პოლიციის მიერ შედგენილ დოკუმენტში არსებული უზუსტობის გამო.
>
> კრიმინალური ორგანიზაციების შესაძლო წევრობისთვის განმცხადებლის წინააღმდეგ ორჯერ აღიძრა სისხლის სამართლის საქმე, თუმცა ორივე შემთხვევაში ის დამნაშავედ არ ცნეს. როდესაც იგი მესამედ დააპატიმრეს და ბრალი წაუყენეს სხვა დანაშაულზე, პოლიციამ სასამართლოს წარუდგინა დოკუმენტი „ინფორმაცია სხვა დანაშაულების შესახებ“, რომლის მიხედვითაც განმცხადებელი ორი კრიმინალური ორგანიზაციის წევრი იყო. განმცხადებლის მოთხოვნა ამ დოკუმენტსა და პოლიციის ჩანაწერებში შესწორების შეტანაზე წარუმატებელი აღმოჩნდა. ECtHR-მა დაადგინა, რომ პოლიციის მიერ შედგენილ დოკუმენტში მითითებული ინფორმაცია კონვენციის მე-8 მუხლის მოქმედების სფეროში ხვდებოდა, რადგან სისტემატურად შეგროვებული საჯარო ინფორმაცია, რომელიც ინახება საჯარო უწყებათა ფაილებში, შესაძლოა, ექცეოდეს „პირადი ცხოვრების“ ფარგლებში. ამასთან, პოლიციის მიერ შედგენილ დოკუმენტში შეცდომა იყო, ხოლო მისი წარდგენა სისხლის სამართლის სასამართლოსთვის არ შეესაბამებოდა ეროვნულ კანონმდებლობას. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

საჯარო უწყების წინააღმდეგ სამოქალაქო საქმისწარმოების ან პროცესის დროს, მონაცემთა სუბიექტს აქვს უფლება, მოითხოვოს მის პირად ფაილზე ჩანაწერის ან შენიშვნის გაკეთება, რომ მონაცემების სიზუსტე დავის საგანია, ოფიციალური გადაწყვეტილება კი ჯერ არ გამოუტანიათ.[562] ამ დროის განმავლობაში, დამმუშავებელმა ეს მონაცემები მესამე პირს არ უნდა წარუდგინოს ზუსტ/სწორ ინფორმაციად, რომელიც არ ექვემდებარება გასწორებას.

6.1.3 მონაცემთა წაშლის („დავიწყების“) უფლება

მონაცემთა სუბიექტებისათვის თავიანთი მონაცემების წაშლის მოთხოვნის უფლების მინიჭება განსაკუთრებით მნიშვნელოვანია მონაცემთა დაცვის პრინციპების, კერძოდ, მინიმიზაციის ეფექტიანი გამოყენებისთვის (პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცი-

560 ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 2000 წლის 4 მაისი.

561 ECtHR, *Cemalettin Canli v. Turkey,* No. 22427/04, 2008 წლის 18 ნოემბერი, პუნქტები 33 და 42–43. ECtHR, *Dalea v. France,* No. 964/07, 2010 წლის 2 თებერვალი.

562 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 18, პრეამბულა 67.

ლებელია დამუშავების მიზნების მისაღწევად). შესაბამისად, წაშლის უფლება დაცულია როგორც ევროპის საბჭოს, ისე ევროკავშირის სამართლებრივი ინსტრუმენტებით.[563]

მაგალითები: საქმეში *Segerstedt-Wiberg and Others v. Sweden*[564] განმცხადებლები, რომლებიც გარკვეულ ლიბერალურ და კომუნისტურ პოლიტიკურ პარტიებთან იყვნენ დაკავშირებულნი, ეჭვობდნენ, რომ მათზე ინფორმაცია პოლიციის ჩანაწერებში იყო შეტანილი და ითხოვდნენ წაშლას. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ ამ შემთხვევაში, მონაცემთა შენახვას ჰქონდა სამართლებრივი საფუძველი და ემსახურებოდა კანონიერ მიზანს. თუმცა, ზოგიერთ განმცხადებელთან მიმართებით, სასამართლომ დაადგინა, რომ მონაცემების შემდგომი შენახვა იყო არაპროპორციული ჩარევა მათ პირად ცხოვრებაში. მაგალითად, ერთ-ერთ მათგანზე სახელმწიფო ორგანოები ინახავდნენ ინფორმაციას, რომ 1969 წელს გამართული დემონსტრაციის დროს, სავარაუდოდ, მხარი დაუჭირა პოლიციის წინააღმდეგ მიმართულ ძალადობრივ ქმედებას. EctHR-ის დასკვნით, ეს ინფორმაცია, თავისი ისტორიული ბუნებიდან გამომდინარე, არ ემსახურებოდა ეროვნული უსაფრთხოების მიზანს. სასამართლომ 5 განმცხადებლიდან 4-ის შემთხვევაში დაადგინა კონვენციის მე-8 მუხლის დარღვევა, ვინაიდან მათ მიერ ჩადენილი სავარაუდო ქმედებებიდან საკმაო დრო გავიდა და ამ მონაცემების შენახვა საფუძველს იყო მოკლებული.

საქმეში *Brunet v. France*[565] განმცხადებელი ასაჩივრებდა პოლიციის მონაცემთა ბაზაში მათი პერსონალური ინფორმაციის შენახვას. ეს ბაზა მოიცავდა ინფორმაციას მსჯავრდებულ, ბრალდებულ და დაზარალებულ პირებზე. მიუხედავად იმისა, რომ განმცხადებლის წინააღმდეგ სისხლის-სამართლებრივი წარმოება შეწყდა, დეტალური ინფორმაცია მასზე კვლავ ინახებოდა მონაცემთა ბაზაში. ევროპულმა სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა. მან გაითვალისწინა, რომ პრაქტიკაში არ არსებობდა განმცხადებლის შესახებ ბაზაში შეტანილი პერსონალური მონაცემების წაშლის შესაძლებლობა; ასევე ისიც, თუ რა ტიპის მონაცემები ინახებოდა ბაზაში, და დაასკვნა, რომ ეს არღვევდა განმცხადებლის პირადი ცხოვრების უფლებას, ვინაიდან შეიცავდა დეტალურ ინფორმაციას მის ვინაობასა და პიროვნებაზე. სასამართლომ ასევე დაადგინა, რომ ბაზაში პერსონალური ჩანაწერების შენახვის ვადა - 20 წელი - იყო ზედმეტად ხანგრძლივი, განსაკუთრებით იმის გათვალისწინებით, რომ განმცხადებელს ბრალი არცერთმა სასამართლომ არ დაუმტკიცა.

563 *იქვე,* მუხლი 17.

564 ECtHR, *Segerstedt-Wiberg and Others v. Sweden,* No. 62332/00, 2006 წლის 6 ივნისი, პუნქტები 89 და 90; ასევე, იხ: ECtHR, *M.K. v. France,* No. 19522/09, 2013 წლის 18 აპრილი.

565 ECtHR, *Brunet v. France,* No. 21010/10, 2014 წლის 18 სექტემბერი.

მოდერნიზებული 108-ე კონვენცია ცალსახად აღიარებს, რომ თითოეულ პირს უფლება აქვს, მოითხოვოს არაზუსტი, მცდარი ან უკანონოდ დამუშავებული მონაცემების წაშლა. [566]

ევროკავშირის სამართალში GDPR-ის მე-17 მუხლი მონაცემთა სუბიექტებს საშუალებას აძლევს, მოითხოვონ მონაცემების წაშლა. კერძოდ, დაუყოვნებლივ წაშლის უფლება მოქმედებს, როცა:

- მონაცემები აღარ არის საჭირო იმ მიზნისთვის, რომლისთვისაც შეგროვდა ან დამუშავდა;
- მონაცემთა სუბიექტი გამოითხოვს თანხმობას, დამუშავების სხვა სამართლებრივი საფუძველი კი აღარ არსებობს;
- მონაცემთა სუბიექტი მოითხოვს თავისი მონაცემების დამუშავების შეწყვეტას, დამუშავების სხვა კანონიერი საფუძველი კი აღარ არსებობს;
- მონაცემების დამუშავება უკანონოა;
- მონაცემები უნდა წაიშალოს ევროკავშირის ან წევრი სახელმწიფოს საკანონმდებლო მოთხოვნის შესასრულებლად, რომელსაც დამმუშავებლისთვის სავალდებულო ძალა აქვს;
- მონაცემები შეგროვდა არასრულწლოვნებისთვის GDPR-ის მე-8 მუხლით გათვალისწინებული ელექტრონული მომსახურების შესათავაზებლად.[567]

მტკიცების ტვირთი მონაცემთა დამუშავების კანონიერების შესახებ ეკისრებათ დამმუშავებლებს, რადგან სწორედ ისინი არიან პასუხისმგებელნი ამ პროცესის კანონიერებაზე.[568] ანგარიშვალდებულების პრინციპის თანახმად, მონაცემთა დამმუშავებელი ვალდებულია, ნებისმიერ დროს დაადასტუროს მონაცემთა დამუშავების მყარი სამართლებრივი საფუძვლის არსებობა. წინააღმდეგ შემთხვევაში, დამუშავება უნდა შეწყდეს.[569] GDPR განსაზღვრავს გამონაკლისებს „დავიწყების“ უფლებასთან დაკავშირებით, მათ შორის, როდესაც პერსონალური მონაცემების დამუშავება აუცილებელია შემდეგი მიზნებისთვის:

- გამოხატვისა და ინფორმაციის თავისუფლებით სარგებლობა;

566 მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1) (ე).

567 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 17 (1).

568 *იქვე.*

569 *იქვე,* მუხლი 5 (2).

- ევროკავშირის ან წევრი სახელმწიფოს კანონით გათვალისწინებული დამუშავების სამართლებრივი ვალდებულების ან საჯარო ინტერესის სფეროში შემავალი ამოცანის შესრულება, ანდა მონაცემთა დამმუშავებლისათვის კანონით მინიჭებული უფლებამოსილების განხორციელება;
- საჯარო ინტერესი საზოგადოებრივი ჯანდაცვის სფეროში;
- საჯარო ინტერესებში შემავალი არქივირება, სამეცნიერო/ისტორიული კვლევა ან სტატისტიკის წარმოება;
- სამართლებრივი მოთხოვნის დადგენა, შესრულება ან დაცვა.[570]

CJEU-მ განამტკიცა წაშლის უფლების მნიშვნელობა მონაცემთა მაღალ დონეზე დასაცავად.

მაგალითი: საქმეში *Google Spain*[571] CJEU-ს უნდა გადაეწყვიტა, მოეთხოვებოდა თუ არა Google-ს საძიებო შედეგებიდან მოძველებული ინფორმაციის წაშლა განმცხადებლის ფინანსურ პრობლემებზე. სხვა საკითხებთან ერთად, Google აცხადებდა, რომ იგი არ იყო პასუხისმგებელი, ვინაიდან საძიებო სისტემა აჩვენებდა მხოლოდ გამომცემლის ვებგვერდის ჰიპერბმულს, სადაც განთავსებული იყო შესაბამისი ინფორმაცია, კერძოდ, საგაზეთო სტატია განმცხადებლის გადახდისუუნარობაზე.[572] Google აცხადებდა, რომ განმცხადებელს მოძველებული ინფორმაციის წაშლა უნდა მოეთხოვა ვებგვერდის ჰოსტისთვის, და არა Google-ისათვის, რადგან ეს უკანასკნელი მხოლოდ ორიგინალი გვერდის ბმულს აწვდიდა. CJEU-ს დასკვნით, Google, ვებინფორმაციისა და ვებგვერდების მოძიების პროცესში, ასევე, საძიებო შედეგების დასადებად შინაარსის ინდექსაციისას, არის მონაცემთა დამმუშავებელი, რომელზეც ვრცელდება ევროკავშირის კანონმდებლობით გათვალისწინებული პასუხისმგებლობები და მოვალეობები.

570 *იქვე,* მუხლი 17 (3).

571 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 წლის 13 მაისი, პუნქტები 55–58.

572 Google ასევე ეწინააღმდეგებოდა ევროკავშირის მონაცემთა დაცვის წესების გამოყენებას იმის გამო, რომ Google Inc. შექმნილია აშშ-ში და პერსონალური მონაცემები აშშ-ში დამუშავდა. მეორე არგუმენტთან დაკავშირებით, Google აცხადებდა, რომ საძიებო სისტემა ვერ ჩაითვლება „მონაცემთა დამმუშავებლად“ ძიების შედეგებში წარმოდგენილ მონაცემებთან დაკავშირებით, რადგან იგი არ ფლობს ინფორმაციას ამ მონაცემებზე და არ აკონტროლებს მათ.
CJEU-მ ორივე არგუმენტი უსაფუძვლოდ მიიჩნია და დაადგინა, რომ საქმეზე ვრცელდებოდა დირექტივა 95/46/EC. სასამართლომ საქმეში განიხილა უფლებები, რომლებსაც დირექტივა უზრუნველყოფს - კერძოდ, პერსონალურ მონაცემთა წაშლის უფლება.

CJEU-მ განმარტა, რომ ინტერნეტსაძიებო სისტემებსა და ძიების შედეგებს, რომლებიც პერსონალურ მონაცემებს წარადგენს, პიროვნების დეტალური პროფილის შედგენა შეუძლია.[573] საძიებო სისტემათა შედეგების სიაში წარმოდგენილი ინფორმაცია ფართოდ ვრცელდება. მისი პოტენციური სერიოზულობიდან გამომდინარე, ჩარევა ვერ გამართლდება მხოლოდ საძიებო სისტემის ოპერატორის ეკონომიკური ინტერესებით. საჭიროა სამართლიანი ბალანსის დაცვა ინტერნეტის მომხმარებელთა ინფორმაციაზე წვდომის ლეგიტიმურ ინტერესსა და მონაცემთა სუბიექტის ფუნდამენტურ უფლებებს შორის, რომლებიც დაცულია ქარტიის (Charter) მე-7 და მე-8 მუხლებით. საზოგადოებაში სულ უფრო და უფრო მეტი მნიშვნელობა ენიჭება ციფრულ სამყაროს. შესაბამისად, ფიზიკურ პირთა მონაცემების მაღალ დონეზე დასაცავად, ფუნდამენტური მნიშვნელობა აქვს მათ სიზუსტეს და მხოლოდ აუცილებელი მოცულობით დამუშავებას (მაგ.: საზოგადოების ინფორმირება). „მონაცემთა დამმუშავებელმა საკუთარი მოვალეობების, უფლებამოსილებისა და შესაძლებლობების ფარგლებში უნდა უზრუნველყოს, რომ დამუშავება აკმაყოფილებდეს“ ევროკავშირის კანონმდებლობას, დადგენილი სამართლებრივი გარანტიები კი სრულად მოქმედებდეს.[574] ეს ნიშნავს, რომ პერსონალური მონაცემების წაშლის უფლება, როცა ისინი მოძველებულია ან საჭირო აღარ არის, ეხება მონაცემთა დამმუშავებელსაც, რომელიც ამ ინფორმაციას ხეალხლა აწარმოებს.[575]

რაც შეეხება განმცხადებელთან დაკავშირებული ბმულების წაშლას Google-ის მიერ, CJEU-მ დაადგინა, რომ გარკვეულ პირობებში ფიზიკურ პირებს უფლება აქვთ, მოითხოვონ პერსონალური მონაცემების წაშლა. ამ უფლების გამოყენება შესაძლებელია, როცა ინფორმაცია არაზუსტი, არაადეკვატური, არარელევანტური ან გადაჭარბებულია მონაცემთა დამუშავების მიზნებისთვის. CJEU-ს განმარტებით, აღნიშნული უფლება არ არის აბსოლუტური და საჭიროა მისი შეთავსება სხვა უფლებებსა და ინტერესებთან, კერძოდ, როგორიცაა საზოგადოების წვდომა გარკვეულ ინფორმაციაზე. წაშლის მოთხოვნა უნდა შეფასდეს თითოეულ შემთხვევაში და დაბალანსდეს პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის ფუნდამენტური უფლება და ინტერნეტმომხმარებელთა

573 *იქვე,* პუნქტები 36, 38, 80–81 და 97.

574 *იქვე,* პუნქტები 81–83.

575 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 წლის 13 მაისი, პუნქტი 88. ასევე, იხ. 29-ე მუხლის სამუშაო ჯგუფი (2014), სახელმძღვანელო პრინციპები CJEU-ს გადაწყვეტილების იმპლემენტაციისათვის საქმეებზე *„Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González„* C-131/12 WP 225, ბრიუსელი, 2014 წლის 26 ნოემბერი; მინისტრთა კომიტეტის რეკომენდაცია წევრი სახელმწიფოებისთვის CM/Rec 2012(3) საძიებო სისტემებთან დაკავშირებით ადამიანის უფლებათა დაცვის შესახებ, 2012 წლის 4 აპრილი.

- მათ შორის გამომცემელთა - კანონიერი ინტერესები. CJEU-მ მიმოიხილა ასეთ დროს, გასათვალისწინებელი ფაქტორები, რომელთა შორის განსაკუთრებულად მნიშვნელოვნად მიიჩნია ის, თუ რა ტიპის ინფორმაციას შეეხება საქმე. როცა ინფორმაცია უკავშირდება პირად ცხოვრებას და არ არსებობს საჯარო ინტერესი ამ ინფორმაციის ხელმისაწვდომობასთან დაკავშირებით, მონაცემთა დაცვა და პირადი ცხოვრების ხელშეუხებლობა გადაწონის ფართო საზოგადოების ინფორმაციაზე წვდომის უფლებას. მეორე მხრივ, თუ მონაცემთა სუბიექტი საზოგადო მოღვაწეა, ან ინფორმაციის ბუნება ამართლებს მის მისაწვდომობას ფართო საზოგადოებისათვის, ამ უკანასკნელის უპირატესი ინტერესი გაამართლებს ჩარევას მონაცემთა სუბიექტის პირადი ცხოვრებისა და მონაცემთა დაცვის ფუნდამენტურ უფლებებში.

აღნიშნული გადაწყვეტილების შემდგომ, 29-ე მუხლის სამუშაო ჯგუფმა, CJEU-ს გადაწყვეტილების დასანერგად, მიიღო სახელმძღვანელო პრინციპები,[576] სადაც წარმოდგენილია საერთო კრიტერიუმები საზედამხედველო ორგანოებისთვის. ეს კრიტერიუმები მოიცავს წაშლის მოთხოვნების განხილვას, წაშლის უფლების განმარტებას და უფლებათა დაბალანსებას. სახელმძღვანელო პრინციპებში ხაზგასმულია, რომ შეფასება უნდა ჩატარდეს თითოეულ შემთხვევაში. „დავიწყების“ უფლება არ არის აბსოლუტური. შესაბამისად, წაშლის მოთხოვნებთან დაკავშირებული გადაწყვეტილებები განსხვავდება და დამოკიდებულია მოცემული საქმის გარემოებებზე. ამის ნათელი დასტურია CJEU-ს მიერ Google-ის შემდგომ განხილულ საქმეებზე გამოტანილი გადაწყვეტილებები.

მაგალითი: საქმეში *Camera di Commercio di Lecce v. Manni*[577] CJEU-მ იმსჯელა, ჰქონდა თუ არა ფიზიკურ პირს უფლება, მოეთხოვა კომპანიების საჯარო რეესტრში გამოქვეყნებული პერსონალური მონაცემების წაშლა კომპანიის გაუქმების შემდეგ. ბ-ნმა მანიმ ლეჩეს სავაჭრო პალატას რეესტრიდან თავისი პერსონალური მონაცემების წაშლა მოსთხოვა მას შემდეგ, რაც აღმოაჩინა, რომ პოტენციურ კლიენტებს ამ გზით შეეძლოთ მისთვის არასასურველი ინფორმაციის მიიღება: კერძოდ იმის, რომ ბ-ნი მანი გახლდათ ადმინისტრატორი ერთ-ერთი კომპანიისა, რომელიც ათ წელზე მეტი ხნის წინათ გაკოტრებულად გამოცხადდა. განმცხადებელი მიიჩნევდა, რომ ეს ინფორმაცია მის პოტენციურ კლიენტებს აფრთხობდა.

576 29-ე მუხლის სამუშაო ჯგუფი (2014), სახელმძღვანელო პრინციპები CJEU-ს გადაწყვეტილების იმპლემენტაციისათვის საქმეებზე „*Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*„ C-131/12, 2014 წლის 26 ნოემბერი.

577 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017 წლის 9 მარტი.

განმცხადებლის პერსონალურ მონაცემთა დაცვისა და ფართო საზოგადოების ინფორმაციაზე წვდომის უფლებათა შესათავსებლად, სასამართლომ პირველ რიგში განიხილა საჯარო რეესტრის მიზანი. მან აღნიშნა, რომ ასეთი მონაცემების გამოქვეყნება კანონით იყო გათვალისწინებული, კერძოდ, ევროკავშირის დირექტივით, რომელიც მიზნად ისახავს კომპანიის შესახებ ინფორმაციის ხელმისაწვდომობას მესამე პირებისთვის. ამრიგად, მესამე პირებს უნდა შეეძლოთ, გაეცნონ კომპანიის ძირითად დოკუმენტებსა და სხვა ინფორმაციას, „განსაკუთრებით იმ პირებზე, რომლებსაც კომპანიის საქმიანობის შეჩერების უფლებამოსილება აქვთ.“ ევროკავშირის წევრ სახელმწიფოებს შორის ინტენსიური ვაჭრობის გათვალისწინებით, ამ ინფორმაციის გამოქვეყნების მიზანი გახლდათ სამართლებრივი განჭვრეტადობაც, რომლის უზრუნველყოფა შესაძლებელია მესამე პირების წვდომით ყველა რელევანტურ ინფორმაციაზე ევროკავშირში არსებული კომპანიების შესახებ.

CJEU-მ დამატებით აღნიშნა, რომ კომპანიის უფლებები და სამართლებრივი მოვალეობები არსებობს გაუქმებიდან გარკვეული ხნის შემდეგაც. მის დაშლასთან დაკავშირებული დავები შეიძლება დროში გაიწელოს, მენეჯერებსა და ლიკვიდატორებთან დაკავშირებული კითხვები კი წარმოიშვას მას მერეც, რაც კომპანია შეწყვეტს არსებობას. CJEU-მ დაადგინა, რომ სხვადასხვა შესაძლო სცენარისა და თითოეულ სახლმწიფოში მოქმედი განსხვავებული ვადების გათვალისწინებით, „როგორც ჩანს, ამჟამად, შეუძლებელია კომპანიის ლიკვიდაციის შემდგომ მოქმედი ერთი საერთო ვადის განსაზღვრა, რომლის გასვლის შემდეგაც, რეესტრში შესაბამისი მონაცემების შეტანა და გამჟღავნება საჭირო აღარ იქნება.“ CJEU-მ, გაითვალისწინა რა გამჟღავნების კანონიერი მიზანი, ასევე იმ ვადის განსაზღვრის სირთულეები, რომლის გასვლის შემდგომაც შესაძლებელი იქნება რეესტრიდან პერსონალური მონაცემების წაშლა მესამე მხარის ინტერესების დაზარალების გარეშე, დაადგინა, რომ ევროკავშირის მონაცემთა დაცვის წესები ბ-ნი მანის შემთხვევაში არ მოიცავს პერსონალურ მონაცემთა წაშლის უფლებას.

თუ დამმუშავებელს მოსთხოვენ გასაჯაროებული პერსონალური მონაცემების წაშლას, იგი ვალდებულია, გადადგას გონივრული ნაბიჯები, რათა ეს მოთხოვნა შეატყობინოს იმავე მონაცემების სხვა დამმუშავებელს. მონაცემთა დამმუშავებლის საქმიანობა უნდა ითვალისწინებდეს არსებულ ტექნოლოგიებსა და მათთან დაკავშირებულ ხარჯებს.[578]

578 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 17 (2); პრეამბულა, პუნქტი 66.

6.1.4 მონაცემთა დაბლოკვის უფლება

GDPR-ის მე-18 მუხლის თანახმად, მონაცემთა სუბიექტებს ენიჭებათ უფლება, დროებით შეუზღუდონ დამმუშავებელს თავიანთი პერსონალური მონაცემების დამუშავება, კერძოდ, მოითხოვონ მათი დაბლოკვა, თუკი:

- სადავოდ მიაჩნიათ მონაცემთა სიზუსტე;
- მონაცემთა დამუშავება უკანონოა და, წაშლის ნაცვლად, ითხოვენ მათ დაბლოკვას;
- მონაცემები საჭიროა სამართლებრივი მოთხოვნის შესასრულებლად ან დასაცავად;
- განიხილება საკითხი, რამდენად აღემატება დამმუშავებლის კანონიერი ინტერესები მონაცემთა სუბიექტის ინტერესებს, გადაწყვეტილება კი ჯერ არ მიღებულა.[579]

პერსონალურ მონაცემთა დამუშავების შეზღუდვის მეთოდები შესაძლოა მოიცავდეს შერჩეული მონაცემების დროებით გადატანას დამუშავების სხვა სისტემაში, მათზე წვდომის გაუქმებას სხვა მომხმარებლებისთვის, ან გამოქვეყნებული მონაცემების წაშლას.[580] დამმუშავებელი ვალდებულია, მონაცემთა სუბიექტს წინასწარ შეატყობინოს მონაცემთა განბლოკვა.[581]

პერსონალურ მონაცემთა გასწორებაზე, წაშლაზე ან დამუშავების შეზღუდვაზე შეტყობინების ვალდებულება

დამმუშავებელი ვალდებულია, პერსონალური მონაცემების გასწორება, წაშლა ან დამუშავების შეზღუდვა აცნობოს თითოეულ მიმღებს, რომელსაც იგი გადასცემს მონაცემებს. ამავდროულად, აღნიშნული მოვალეობის შესრულება დამმუშავებელს არ უნდა აკისრებდეს არაპროპორციულ ტვირთს.[582] თუ მონაცემთა სუბიექტი მოითხოვს ინფორმაციას მონაცემთა მიმღების შესახებ, დამმუშავებელი ვალდებულია, მიაწოდოს ის.[583]

579 *იქვე,* მუხლი 18 (1).

580 *იქვე,* პრეამბულა, პუნქტი 67.

581 *იქვე,* მუხლი 18 (3).

582 *იქვე,* მუხლი 19.

583 *იქვე.*

6.1.5 მონაცემთა პორტირების (გადატანის) უფლება

GDPR-ის თანახმად, მონაცემთა სუბიექტებს ენიჭებათ მონაცემთა პორტირების უფლება, თუკი დამმუშავებლისათვის მიწოდებული პერსონალური მონაცემები მუშავდება ავტომატიზებული საშუალებით, თანხმობის საფუძველზე, ან პერსონალური მონაცემების დამუშავება აუცილებელია სახელშეკრულებო ვალდებულების შესასრულებლად და ხორციელდება ავტომატური საშუალებით. ეს ნიშნავს, რომ მონაცემთა გადატანის უფლება არ ვრცელდება ისეთ სიტუაციებზე, როდესაც დამუშავება ეფუძნება სხვა რომელიმე სამართლებრივ საფუძველს, გარდა თანხმობისა და ხელშეკრულებისა.[584]

პორტირების უფლება გულისხმობს მონაცემთა სუბიექტის უფლებას, მოითხოვოს მონაცემების პირდაპირ გადაცემა ერთი დამმუშავებლისაგან მეორისათვის, თუ ეს ტექნიკურად შესაძლებელია.[585] ამის ხელშესაწყობად, დამმუშავებელი ვალდებულია, შექმნას თავსებადი ფორმატები, რომლებიც იძლევა პორტირების საშუალებას.[586] GDPR-ის თანახმად, ეს ფორმატები უნდა იყოს სტრუქტურირებული, გამოიყენებოდეს ჩვეულებრივ და იკითხებოდეს ელექტრონულად, რაც ხელს შეუწყობს თავსებადობას.[587] ეს უკანასკნელი ზოგადად განისაზღვრება, როგორც მონაცემთა გაცვლისა და გაზიარების შესაძლებლობა საინფორმაციო სისტემების ფარგლებში.[588] გარკვეული ფორმატების გამოყენების მიზანია თავსებადობა, თუმცა, GDPR არ ითვალისწინებს რეკომენდაციებს რაიმე კონკრეტული ფორმატის გამოყენებაზე - ისინი შეიძლება სექტორების მიხედვით განსხვავდებოდეს.[589]

29-ე მუხლის სამუშაო ჯგუფის სახელმძღვანელო პრინციპების თანახმად, მონაცემთა პორტირების (გადატანის) უფლება „ხელს უწყობს მომხმარებლის არჩევანს, მომხმარებლის მხრიდან კონტროლსა და მის გაძლიერებას“, რისი მიზანიც არის მონაცემთა სუბიექტისთვის საკუთარი მონაცემების გაკონტროლების შესაძლებლობის მიცემა.[590] სახელმძღვანელო პრინციპები ითვალისწინებს მონაცემთა პორტირების 5 ძირითად ელემენტს, კერძოდ:

---

584 *იქვე,* პრეამბულა, პუნქტი 68 და მუხლი 20 (1).

585 *იქვე,* მუხლი 20 (2).

586 *იქვე,* პრეამბულა, პუნქტი 68 და მუხლი 20 (1).

587 *იქვე,* პრეამბულა, პუნქტი 68.

588 ევროკომისიის მიმართვა საზღვრებისა და უსაფრთხოებისათვის უფრო ძლიერი და ჭკვიანი საინფორმაციო სისტემების შესახებ, COM(2016) 205 საბოლოო, 2016 წლის 2 აპრილი.

589 29-ე მუხლის სამუშაო ჯგუფი (2016), სახელმძღვანელო პრინციპები მონაცემთა პორტატულობის შესახებ, WP 242, 2016 წლის 13 დეკემბერი, გადაიხედა 2017 წლის 5 აპრილს, გვ. 13.

590 *იქვე.*

- მონაცემთა სუბიექტის უფლება, მიიღოს საკუთარი პერსონალური მონაცემები, რომლებიც დამუშავდა სტრუქტურირებულ, ჩვეულებრივად გამოყენებულ და თავსებად ფორმატში, ელექტრონულად წაკითხვის შესაძლებლობით;

- ერთი დამმუშავებლიდან მეორესთვის პერსონალურ მონაცემთა დაუბრკოლებლად გადაცემის უფლება, თუ ეს ტექნიკურად შესაძლებელია;

- მონაცემთა დამმუშავებლის რეჟიმი - როდესაც დამმუშავებელი პორტირების მოთხოვნას პასუხობს, მონაცემთა სუბიექტის ინსტრუქციათა შესაბამისად იქცევა. ეს ნიშნავს, რომ იგი არ არის პასუხისმგებელი მონაცემთა მიმღების შესაბამისობაზე მონაცემთა დაცვის კანონმდებლობასთან, ვინაიდან მონაცემთა სუბიექტი წყვეტს, რომელ დამმუშავებელთან მოხდება მონაცემების პორტირება;

- მონაცემთა პორტირების უფლების განხორციელება ისე, რომ არ დაზიანდეს სხვა უფლება, როგორც გათვალისწინებულია GDPR-ით განსაზღვრული ნებისმიერი სხვა უფლების შემთხვევაში.

6.1.6 მონაცემთა დამუშავების შეწყვეტის უფლება

მონაცემთა სუბიექტს აქვს უფლება, მოითხოვოს მონაცემთა დამუშავების შეწყვეტა, ინდივიდუალური გარემოებებიდან გამომდინარე. კერძოდ, ეს ეხება მონაცემებს, რომლებიც მუშავდება პირდაპირი მარკეტინგის მიზნებით. ამ უფლების განხორციელება შესაძლებელია ავტომატიზებული საშუალებებით.

მონაცემთა დამუშავების შეწყვეტის უფლება პირის ინდივიდუალური გარემოებებიდან გამომდინარე

მონაცემთა სუბიექტების უფლება, მოითხოვონ მონაცემთა დამუშავების შეწყვეტა, ზოგადი არ არის.[591] GDPR-ის 21-ე მუხლის პირველი პუნქტის თანახმად, თუკი დამუშავების სამართლებრივი საფუძველია საჯარო ინტერესში შემავალი ამოცანების შესრულება ან დამმუშავებლის კანონიერი ინტერესები, მათ ამის მოთხოვნა შეუძლიათ თავიანთი ინდივიდუალური გარემოებებიდან გამომდინარე.[592] დამუშავების შეწყვეტის მოთხოვნის უფლება ვრცელდება

591 ასევე, იხ. ECtHR, *M.S. v. Sweden,* No. 20837/92, 1997 წლის 27 აგვისტო (სამედიცინო მონაცემები გადაეცა თანხმობისა და გასაჩივრების შესაძლებლობის გარეშე); ECtHR, *Leander v. Sweden,* No. 9248/81, 1987 წლის 26 მარტი; ECtHR, *Mosley v. the United Kingdom,* No. 48009/08, 2011 წლის 10 მაისი.

592 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 69; მუხლი 6 (1) (ე) და (ვ).

პროფილირებასთან დაკავშირებულ საქმიანობაზე. იგივე უფლება აღიარებულია მოდერნიზებული 108-ე კონვენციითაც.[593]

მონაცემთა დამუშავების შეწყვეტა პირის ინდივიდუალური გარემოებებიდან გამომდინარე, მიზნად ისახავს სწორ ბალანსს სუბიექტის მონაცემთა დაცვის უფლებებსა და სხვათა ლეგიტიმურ უფლებებს შორის, მონაცემთა დამუშავების პროცესში, თუმცა, CJEU-მ განმარტა, რომ მონაცემთა სუბიექტის უფლებები, „როგორც წესი“, დამმუშავებლის ეკონომიკურ ინტერესებზე მაღლა დგას, რაც დამოკიდებულია „ინფორმაციის ბუნებასა და სენსიტიურობაზე მონაცემთა სუბიექტის პირადი ცხოვრების კონტექსტში, ასევე, საზოგადოების ინტერესზე ამ ინფორმაციის წვდომის მხრივ.“[594] GDPR-ის თანახმად, მტკიცების ტვირთი ეკისრება მონაცემთა დამმუშავებელს, რომელმაც მყარი საფუძვლები უნდა წარმოადგინოს დამუშავების გასაგრძელებლად.[595] GDPR-ის მსგავსად, მოდერნიზებული 108-ე კონვენციაც ადგენს, რომ მონაცემთა დამუშავების ლეგიტიმური საფუძვლების ჩვენება (რომლებიც გადაწონის მონაცემთა სუბიექტის მოთხოვნას დამუშავების შეწყვეტაზე) აუცილებელია თითოეულ კონკრეტულ შემთხვევაში.[596]

მაგალითი: *Manni*-ის საქმეში[597] CJEU-მ დაადგინა, რომ იმ კანონიერი მიზნის გათვალისწინებით, რომელსაც რეესტრი ემსახურება (კერძოდ, მესამე პირთა ინტერესების დაცვა და სამართლებრივი განჭვრეტადობა), ბატონ მანის არ ჰქონდა უფლება, მოეთხოვა საკუთარი პერსონალური მონაცემების წაშლა. ამავდროულად, სასამართლომ აღიარა დამუშავების შეწყვეტის მოთხოვნის უფლება და აღნიშნა: „გამორიცხული არ არის [...] ისეთი სიტუაციები, სადაც კონკრეტული საქმის ლეგიტიმური და გაცილებით მნიშვნელოვანი მიზეზები, გამონაკლისის სახით და საკმარისი დროის გასვლის შემდეგ [...], ამართლებს რეესტრის პერსონალურ მონაცემებზე წვდომის უფლების მინიჭებას მხოლოდ გარკვეული მხარეებისთვის, რომლებსაც აქვთ ამ ინფორმაციის გაცნობის დადასტურებული და კონკრეტული ინტერესი.

593 მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1) (დ); რეკომენდაცია პროფილირების შესახებ, მუხლი 5 (3).

594 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 წლის 13 მაისი, პუნქტი 81.

595 მოდერნიზებული 108-ე კონვენცია, მუხლი 98 (1) (დ), რომლის მიხედვითაც მონაცემთა სუბიექტს უფლება აქვს, მოითხოვოს დამუშავების შეწყვეტა, გარდა იმ შემთხვევისა, როცა „დამუშავებელი წარადგენს ლეგიტიმურ საფუძვლებს, რომლებიც აღემატება მონაცემთა სუბიექტის ინტერესებს ან უფლებებსა და ფუნდამენტურ თავისუფლებებს.“

596 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 78.

597 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni,* 2017 წლის 9 მარტი, პუნქტები 47 და 60.

CJEU-მ განაცხადა, რომ თითოეულ საქმეში ეროვნულმა სასამართლოებმა ყველა შესაბამისი გარემოების გათვალისწინებით უნდა შეაფასონ ლეგიტიმური და აღმატებული მიზეზების არსებობა, რომლებიც, გამონაკლისის სახით, გაამართლებს მესამე მხარისთვის დაწესებულ შეზღუდვას კომპანიის რეესტრში დაცულ პერსონალურ მონაცემთა წვდომაზე. თუმცა, სასამართლომ განმარტა, რომ ბ-ნი მანის შემთხვევაში მხოლოდ ის ფაქტი, რომ პერსონალური მონაცემების გამჟღავნებამ, სავარაუდოდ, გავლენა მოახდინა მის კლიენტურაზე, არ მიიჩნევა ასეთი მნიშვნელობის მიზეზად. პირის პოტენციურ კლიენტებს აქვთ ლეგიტიმური ინტერესი იმ ინფორმაციის მიმართ, რომელიც შეეხება მისი ყოფილი კომპანიის გაკოტრებას.

თუ მონაცემთა დამუშავების შეწყვეტის მოთხოვნა განხორციელდება წარმატებით, დამმუშავებელი ვეღარ შეძლებს მათ დამუშავებას. თუმცა, მოთხოვნის შესრულებამდე მონაცემები ლეგიტიმურობას არ კარგავს.

პირდაპირი მარკეტინგის მიზნებით მონაცემთა დამუშავების შეწყვეტის უფლება

GDPR-ის 21-ე მუხლის მე-2 პუნქტი ითვალისწინებს მოთხოვნას პირდაპირი მარკეტინგის მიზნებით პერსონალურ მონაცემთა გამოყენების შეწყვეტაზე, რითაც განმარტავს ელექტრონულ სივრცეში პირადი ცხოვრების დაცვის დირექტივის მე-13 მუხლს. ამ უფლებას ითვალისწინებს მოდერნიზებული 108-ე კონვენციაც და ევროპის საბჭოს რეკომენდაციაც პირდაპირი მარკეტინგის შესახებ.[598] კონვენციის განმარტებითი ბარათის თანახმად, პირდაპირი მარკეტინგის მიზნებისთვის მონაცემთა დამუშავების შეწყვეტა განაპირობებს შესაბამისი პერსონალური მონაცემების წაშლას ან ამოღებას.[599]

მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს მოითხოვოს თავისი პერსონალური მონაცემების პირდაპირი მრკეტინგისთვის გამოყენების შეწყვეტა უსასყიდლოდ. მონაცემთა სუბიექტს ეს უფლება უნდა განემარტოს ნათლად და ნებისმიერი სხვა ინფორმაციისგან განცალკევებულად.

მონაცემთა ავტომატური საშუალებებით დამუშავების შეწყვეტის უფლება

თუ პერსონალური მონაცემები გამოიყენება ან მუშავდება საინფორმაციო სა-

598 ევროპის საბჭოს მინისტრთა კომიტეტი (1985), რეკომენდაცია Rec(85)20 წევრი სახელმწიფოებისთვის პირდაპირი მარკეტინგის მიზნებით გამოყენებული პერსონალური მონაცემების დაცვის შესახებ, 1985 წლის 25 ოქტომბერი, მუხლი 4 (1).

599 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 79.

ზოგადოებრივი სერვისებისათვის, მონაცემთა სუბიექტს უფლება აქვს, მოითხოვოს მათი ავტომატური საშუალებებით დამუშავების შეწყვეტა.

საინფორმაციო საზოგადოებრივი სერვისები გულისხმობს ნებისმიერ მომსახურებას, რომელიც, როგორც წესი, მიეწოდება გარკვეული ანაზღაურების საფუძველზე, დისტანციურად, ელექტრონული საშუალებებითა და მომსახურების მიმღების ინდივიდუალური მოთხოვნით.[600]

დამმუშავებელი, რომელიც მონაცემთა სუბიექტებს სთავაზობს საინფორმაციო საზოგადოებრივ სერვისებს, ვალდებულია, გაატაროს სათანადო ტექნიკური ღონისძიებები და პროცედურები, რათა მათ მისცეს საშუალება, ეფექტიანად ისარგებლონ მონაცემთა ავტომატური საშუალებებით დამუშავების შეწყვეტის უფლებით.[601] ეს შეიძლება მოიცავდეს, „cookie“ ფაილების დაბლოკვას ვებგვერდზე, ან ინტერნეტძიებაზე (Internet browsing) მონიტორინგის ფუნქციის გათიშვას.

მონაცემთა სამეცნიერო/ისტორიული კვლევის ან სტატისტიკური მიზნებით დამუშავების შეწყვეტა

ევროკავშირის კანონმდებლობით, პერსონალურ მონაცემთა დამუშავება სამეცნიერო კვლევებისთვის უნდა განიმარტოს ფართოდ და მოიცავდეს ისეთ საკითხებს, როგორიცაა ტექნოლოგიების განვითარება და მათი დემონსტრირება, ფუნდამენტური ან გამოყენებითი და კერძო წყაროებიდან დაფინანსებული კვლევები.[602] ისტორიული კვლევა მოიცავს გენეოლოგიური მიზნებით ჩატარებულ კვლევასაც, თუმცა გასათვალისწინებელია, რომ რეგულაცია არ ვრცელდება გარდაცვლილებზე.[603] სტატისტიკური მიზნები გულისხმობს პერსონალური მონაცემების შეგროვებისა და დამუშავების ნებისმიერ ოპერაციას, რომლებიც საჭიროა სტატისტიკური გამოკითხვის ან შედეგების მისაღებად.[604] ამ შემთხვევაშიც, მონაცემთა სუბიექტს უფლება აქვს, ინდივიდუალური გარემოებებიდან გამომდინარე, მოითხოვოს თავისი მონაცემების დამუშავების შეწყვეტა.[605] ერთადერთი გამონაკლისია საჯარო ინტერესებით განპირობებული აუცილებელი დამუშავება. თუმცა, წაშლის უფლება არ ეხება ისეთ შემთხვე-

600 დირექტივა 98/34/EC, რომელიც შესწორდა 98/48/EC დირექტივით და ადგენს პროცედურას ტექნიკური სტანდარტებისა და რეგულაციების სფეროში ინფორმაციის მიწოდებისთვის, მუხლი 1 (2).

601 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 21 (5).

602 *იქვე*, პრეამბულა, პუნქტი 159.

603 *იქვე*, პრეამბულა, პუნქტი 160.

604 *იქვე*, პრეამბულა, პუნქტი 162.

605 *იქვე*, მუხლი 21 (6).

ვებს, როდესაც დამუშავება აუცილებელია (საჯარო ინტერესის გამო ან მის გარეშე) სამეცნიერო /ისტორიული კვლევების ან სტატისტიკური მიზნებით.[606]

GDPR ითვალისწინებს ბალანსის მიღწევას სამეცნიერო/ისტორიული ან სტატისტიკური კვლევის მოთხოვნებსა და მონაცემთა სუბიექტების უფლებებს შორის. ამ მხრივ, 89-ე მუხლი ადგენს უსაფრთხოების ზომებსა და გამონაკლის შემთხვევებს. შესაბამისად, ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობები შეიძლება ითვალისწინებს მონაცემთა დამუშავების მოთხოვნასთან დაკავშირებულ გამონაკლისებს, თუ ამ უფლებით სარგებლობა ხელს უშლის კვლევის კონკრეტული მიზნების მიღწევას და ამგვარი გამონაკლისების დაშვება აუცილებელია.

ევროპის საბჭოს კანონმდებლობით, მოდერნიზებული 108-ე კონვენციის მე-9 მუხლის მე-2 პუნქტი ადგენს, რომ მონაცემთა დამუშავების შეწყვეტის მოთხოვნაზე შეზღუდვის დაწესებას კანონმდებლობა შეიძლება ითვალისწინებდეს მაშინ, როდესაც დამუშავება ემსახურება საჯარო ინტერესს, სამეცნიერო/ისტორიული კვლევის ან სტატისტიკურ მიზნებს და არ არსებობს მონაცემთა სუბიექტების უფლებებისა და ფუნდამენტური თავისუფლებების დარღვევის გაცნობიერებული რისკი.

ამავდროულად, განმარტებითი ბარათი (პუნქტი 41) აღიარებს მონაცემთა სუბიექტის შესაძლებლობას, თანხმობა გასცეს კვლევის მხოლოდ გარკვეულ მიმართულებებსა ან ნაწილზე, როცა კვლევის მიზანი ამის საშუალებას იძლევა, და მოითხოვოს მონაცემთა დამუშავების შეწყვეტა, თუკი მიაჩნია, რომ ეს ზედმეტად ზღუდავს მის უფლებებსა და თავისუფლებებს, კანონიერი საფუძვლის გარეშე.

სხვა სიტყვებით რომ ვთქვათ, ასეთი დამუშავება *a priori* ჩაითვლება შესაბამისად, თუკი არსებობს დაცვის სხვა გარანტიები, ხოლო დამუშავების ოპერაციები გამორიცხავს კონკრეტულ პირთან დაკავშირებული გადაწყვეტილებების ან ზომების მისაღებად მოპოვებული ინფორმაციის გამოყენებას რაიმე სახით.

6.1.7 ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღება, მათ შორის, პროფილირებით

ავტომატიზებული გადაწყვეტილებები მიიღება იმ პერსონალური მონაცემების გამოყენებით, რომლებიც დამუშავებულია მხოლოდ ავტომატური საშუალებებით, ადამიანური რესურსების ჩაურთველად. ევროკავშირის კანონმდებლო-

606 *იქვე,* მუხლი 17 (3) (დ).

ბის თანახმად, მონაცემთა სუბიექტები არ უნდა დაექვემდებარონ ავტომატიზებულ გადაწყვეტილებებს, რომლებსაც შეიძლება ჰქონდეს სამართლებრივი ან მსგავსი მნიშვნელოვანი შედეგი. თუ ასეთ გადაწყვეტილებას არსებითი გავლენა ექნება პიროვნების ცხოვრებაზე, რადგან უკავშირდება, მაგალითად, გადახდისუნარიანობას, ელექტრონულად დაქირავებას, სამუშაოს შესრულებას ან ქცევისა თუ სანდოობის ანალიზს, საჭიროა სპეციალური დაცვა ამ შედეგების თავიდან ასაცილებლად. ავტომატიზებული გადაწყვეტილება მოიცავს პროფილირებას - პერსონალურ მონაცემთა ნებისმიერ ავტომატურ დამუშავებას ფიზიკური პირის გარკვეული პიროვნული მახასიათებლების შესაფასებლად, კერძოდ, მუშაობის, ეკონომიკური მდგომარეობის, ჯანმრთელობის, პერსონალური მიდრეკილებების, ინტერესების, სანდოობის, ქცევის, ადგილმდებარეობის ან გადაადგილების ასპექტთა“ ავტომატური შეფასების ნებისმიერ ფორმას.[607]

მაგალითი: მომავალი მომხმარებლის გადახდისუნარიანობის შესაფასებლად, საკრედიტო ისტორიების ბიურო აგროვებს გარკვეულ მონაცემებს, როგორიცაა ინფორმაცია მომხმარებლის საკრედიტო და სამომსახურებო/კომუნალური ანგარიშების შესახებ, მომხმარებლის ძველი მისამართები და ინფორმაცია საჯარო წყაროებიდან (მაგ.: საარჩევნო სია და საჯარო ინფორმაცია, მათ შორის, სასამართლო გადაწყვეტილებები; ინფორმაცია გაკოტრებისა თუ გადახდისუუნარობის შესახებ). შემდგომ, ეს პერსონალური მონაცემები შეჰყავთ სპეციალურ ალგორითმში, რომელიც მომხმარებელს ანიჭებს გადახდისუნარიანობის შესაბამის ქულას.

29-ე მუხლის სამუშაო ჯგუფის თანახმად, მონაცემთა სუბიექტის უფლება, არ დაექვემდებაროს მხოლოდ ავტომატიზებული დამუშავებით მიღებულ გადაწყვეტილებებს, რომლებსაც შეიძლება ჰქონდეს გარკვეული სამართლებრივი შედეგები ან მნიშვნელოვანი გავლენა მონაცემთა სუბიექტზე, უტოლდება ზოგად აკრძალვას და არ საჭიროებს პროაქტიულ გასაჩივრებას მონაცემთა სუბიექტის მიერ.[608]

მიუხედავად ამისა, GDPR-ის თანახმად, გადაწყვეტილების ავტომატიზებულად მიღება, რომელიც წარმოშობს სამართლებრივ ან სხვა მნიშვნელოვან შედეგებს მონაცემთა სუბიექტისათვის, დასაშვებია, თუ: ეს აუცილებელია მონაცემთა სუბიექტსა და დამმუშავებელს შორის ხელშეკრულების გასაფორმებლად/შესასრულებლად, ან ეფუძნება მონაცემთა სუბიექტის მკაფიო თანხმობას; ასევე, ცალსახად ნებადართულია კანონით, ხოლო მონაცემთა სუბიექტის

607 *იქვე,* პრეამბულა, პუნქტი 71, მუხლები 4 (4) და 22.

608 29-ე მუხლის სამუშაო ჯგუფი, სახელმძღვანელო პრინციპები ინდივიდუალური გადაწყვეტილებების ავტომატური საშუალებებით მიღებისა და პროფილირების შესახებ, 2016/679 რეგულაციის მიზნებისთვის, WP 251, 2017 წლის 3 ოქტომბერი, გვ. 15.

უფლებები, თავისუფლებები და ლეგიტიმური ინტერესები სათანადოდ არის დაცული.[609]

GDPR-ის თანახმად, შეტყობინების ვალდებულება, რომელიც მონაცემთა დამმუშავებელს ეკისრება პერსონალურ მონაცემთა შეგროვებისას, მოიცავს მონაცემთა სუბიექტის ინფორმირებას გადაწყვეტილების ავტომატიზებულად მიღების, მათ შორის, პროფილირების შესახებაც.[610] დამუშავებულ პერსონალურ მონაცემებზე წვდომის უფლება ძალაში რჩება.[611] დამმუშავებელმა მონაცემთა სუბიექტს უნდა შეატყობინოს არა მხოლოდ დაგეგმილი პროფილირება, არამედ მნიშვნელოვანი/არსებითი ინფორმაციაც გამოყენებულ ლოგიკაზე/კრიტერიუმებზე, მათ საჭიროებასა და მონაცემთა სუბიექტისთვის შესაძლო შედეგებზე.[612] მაგალითად, სადაზღვევო კომპანია, რომელიც გადაწყვეტილებებს ავტომატიზებულად იღებს, ვალდებულია, მონაცემთა სუბიექტებს მიაწოდოს ზოგადი ინფორმაცია, თუ როგორ მუშაობს ალგორითმი და რა ფაქტორებს იყენებს იგი სადაზღვევო პრემიის გამოსაანგარიშებლად. მსგავსად, „წვდომის უფლებით“ სარგებლობისას, მონაცემთა სუბიექტს შეუძლია, დამმუშავებლისაგან მოითხოვოს ინფორმაცია ავტომატიზებულ გადაწყვეტილებებზე, ასევე, მნიშვნელოვანი/არსებითი ინფორმაცია გამოყენებულ ლოგიკაზე/კრიტერიუმებზე.[613]

მონაცემთა სუბიექტისთვის მიწოდებული ინფორმაცია მიზნად ისახავს გამჭვირვალობას, რაც მას საშუალებას აძლევს, განაცხადოს ინფორმირებული თანხმობა, ან მოითხოვოს ადამიანური რესურსის ჩართვა. დამმუშავებელს მოეთხოვება სათანადო ღონისძიებების გატარება მონაცემთა სუბიექტის უფლებების, თავისუფლებებისა და კანონიერი ინტერესების დასაცავად. აღნიშნული მოიცავს, სულ მცირე, იმ შესაძლებლობას, რომ მონაცემთა სუბიექტმა მოითხოვოს ადამიანური რესურსის ჩართვა გადაწყვეტილების მიღების პროცესში, გამოთქვას საკუთარი მოსაზრება და გაასაჩივროს პერსონალურ მონაცემთა ავტომატური დამუშავებით მიღებული გადაწყვეტილება.[614]

29-ე მუხლის სამუშაო ჯგუფმა დაადგინა გადაწყვეტილების ავტომატური საშუალებებით მიღების დამატებითი სახელმძღვანელო პრინციპები, GDPR-ის შესაბამისად.[615]

---

609 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 22 (2).

610 *იქვე,* მუხლი 12.

611 *იქვე,* მუხლი 15.

612 *იქვე,* მუხლი 13 (2) (ვ).

613 *იქვე,* მუხლი 15 (1) (თ).

614 *იქვე,* მუხლი 22 (3).

615 29-ე მუხლის სამუშაო ჯგუფი (2017), სახელმძღვანელო პრინციპები ინდივიდუალური გადაწყვეტილებების ავტომატური საშუალებებით მიღებისა და პროფილირების შესახებ, 2016/679 რეგულაციის მიზნებისთვის, WP 251, 2017 წლის 3 ოქტომბერი.

ევროპის საბჭოს კანონმდებლობის თანახმად, ფიზიკურ პირს უფლება აქვს, არ დაექვემდებაროს გადაწყვეტილებას, რომელიც მნიშვნელოვან გავლენას ახდენს მასზე და მიღებულია მხოლოდ ავტომატური დამუშავებით, პირის მოსაზრებების გაუთვალისწინებლად.[616] ასეთ შემთხვევაში მონაცემთა სუბიექტის მოსაზრებების გათვალისწინების მოთხოვნა ნიშნავს მისთვის გასაჩივრების შესაძლებლობის მიცემას. მონაცემთა სუბიექტს ასევე უნდა შეეძლოს, სადავო გახადოს იმ პერსონალური მონაცემების სიზუსტე, რომლებითაც დამუშავებელი სარგებლობს და გაასაჩივროს მის მიმართ გამოყენებული რომელიმე პროფილის რელევანტურობა.[617] ამავდროულად, აღნიშნული უფლებით სარგებლობას ფიზიკური პირი ვერ შეძლებს, თუ გადაწყვეტილების ავტომატიზებულად მიღება ნებადართულია იმ კანონმდებლობით, რომელიც ვრცელდება მონაცემთა სუბიექტზე და ადგენს სათანადო ღონისძიებებს მისი უფლებების, თავისუფლებებისა და კანონიერი ინტერესების დასაცავად. ამასთან, მონაცემთა სუბიექტს აქვს უფლება, მოთხოვნისთანავე მიიღოს ინფორმაცია მონაცემთა დამუშავების მიზეზებზე.[618] მოდერნიზებული 108-ე კონვენციის განმარტებით ბარათში წარმოდგენილია საკრედიტო ქულების მინიჭების მაგალითი. ფიზიკურ პირებს უფლება აქვთ, იცოდნენ არა მხოლოდ დადებითი ან უარყოფითი შეფასებები მათ შესახებ, არამედ ის ლოგიკა/კრიტერიუმებიც, რაზე დაყრდნობითაც დამუშავდა მათი პერსონალური მონაცემები და მიღებულია შესაბამისი გადაწყვეტილება. „ამ ელემენტების აღქმა ხელს უწყობს სხვა აუცილებელი უსაფრთხოების ზომების ეფექტიან გამოყენებას, როგორიცაა მონაცემთა დამუშავების შეწყვეტის მოთხოვნა და უფლებამოსილ ორგანოში საჩივრის შეტანის უფლება.“ [619]

რეკომენდაცია პროფილირების შესახებ, მიუხედავად იმისა, რომ სავალდებულოდ შესასრულებელი არ არის, ითვალისწინებს პროფილირების კონტექსტში პერსონალურ მონაცემთა შეგროვებისა და დამუშავების კრიტერიუმებს.[620] მისი დებულებების თანახმად, აუცილებელია, პროფილირების კონტექსტში განხორციელებული დამუშავება იყოს სამართლიანი, კანონიერი, პროპორციული და კონკრეტული კანონიერი მიზნის შესაბამისი. იგი მოიცავს დებულებებს იმ ინფორმაციაზეც, რომელიც დამმუშავებელმა უნდა მიაწოდოს მონაცემთა სუბიექტებს. რეკომენდაციაში ასევე წარმოდგენილია მონაცემთა ხარისხის პრინციპი, რომელიც დამმუშავებლებს ავალდებულებს მონაცემებისა და ალგორითმის პერიოდულ შეფასებას, ასევე, ზომების მიღებას მო-

616 მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1) (ა).

617 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 75.

618 მოდერნიზებული 108-ე კონვენცია, მუხლი 9 (1) (გ).

619 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 77.

620 ევროპის საბჭოს მინისტრთა კომიტეტის რეკომენდაცია CM/Rec(2010)13 წევრი სახელმწიფოებისთვის, პროფილირების კონტექსტში პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ, მუხლი 5 (5).

ნაცემებში არსებული უზუსტობების გასასწორებლად და პროფილირებასთან დაკავშირებული რისკებისა თუ შეცდომების შესამცირებლად.

6.2 უფლების აღდგენის/დაცვის საშუალებები, პასუხისმგებლობა, სანქციები და კომპენსაცია

ძირითადი საკითხები

- მოდერნიზებული 108-ე კონვენციის თანახმად, ხელშემკვრელ სახელმწიფოთა ეროვნული კანონმდებლობები უნდა ითვალისწინებდეს დაცვის სათანადო საშუალებებს, ასევე, სანქციებს მონაცემთა დაცვის უფლების დარღვევის წინააღმდეგ.

- ევროკავშირის შემთხვევაში, მონაცემთა სუბიექტების უფლების დარღვევისას GDPR ადგენს მისი აღდგენის/დაცვის საშუალებებს. იგი ასევე ითვალისწინებს სანქციებს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის წინააღმდეგ, თუ მათი ქმედებები რეგულაციის დებულებებს არ შეესაბამება, და ანესებს მიყენებული ზიანის აღიარებისა და კომპენსაციის მოთხოვნის უფლებას:

  - მონაცემთა სუბიექტებს შეუძლიათ, საზედამხედველო ორგანოში შეიტანონ საჩივარი რეგულაციის სავარაუდო დარღვევის შემთხვევებზე. მათ ენიჭებათ ეფექტიანი სამართლებრივი დაცვისა და კომპენსაციის უფლებებიც;

  - სამართლებრივი დაცვის უფლებით ეფექტიანად სარგებლობისას, ფიზიკური პირები შეიძლება იყვნენ არასამთავრობო ორგანიზაციები, რომლებიც მონაცემთა დაცვის სფეროში მუშაობენ;

  - მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი პასუხისმგებელია იმ ნებისმიერ მატერიალურ ან მორალურ ზიანზე, რომელიც ფიზიკურმა პირმა დარღვევის შედეგად განიცადა;

  - საზედამხედველო ორგანოებს უფლება აქვთ, რეგულაციის დამრღვევებს დააკისრონ ადმინისტრაციული ჯარიმა, მაქსიმუმ 20,000,000 ევრო ან, საწარმოს/კომპანიის შემთხვევაში, მთლიანი წლიური ბრუნვის 4% (რომელიც უფრო მეტია).

- მონაცემთა სუბიექტებს უფლება აქვთ, მონაცემთა დაცვის დარღვევებზე,

უკიდურესი საშუალების სახით და გარკვეული პირობების არსებობისას, მიმართონ ადამიანის უფლებათა ევროპულ სასამართლოს.

- ნებისმიერ ფიზიკურ ან იურიდიულ პირს აქვს უფლება, მიმართოს CJEU-ს მონაცემთა დაცვის ევროპული საბჭოს მიერ მიღებული გადაწყვეტილებების გასაუქმებლად (გარკვეული პირობების არსებობის შემთხვევაში, რომლებიც გათვალისწინებულია ხელშეკრულებებით).

სამართლებრივი ინსტრუმენტების მიღება არ კმარა ევროპაში პერსონალურ მონაცემთა დასაცავად. მონაცემთა დაცვის წესების ეფექტიანობისთვის, საჭიროა ისეთი გარანტიების შექმნა, რომლებიც ფიზიკურ პირებს საშუალებას მისცემს, შეეწინააღმდეგონ უფლებების დარღვევას და მოითხოვონ განცდილი ზიანის ანაზღაურება. მნიშვნელოვანია ისიც, რომ საზედამხედველო ორგანოებს ჰქონდეთ ეფექტიანი, აღმკვეთი და დარღვევის პროპორციული სანქციების დაწესების შესაძლებლობა.

მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული უფლებებით სარგებლობა შეუძლიათ იმ პირებს, რომელთა უფლებებიც დევს სასწორზე (მაგ.: მონაცემთა სუბიექტი). ამავდროულად, სხვა პირებს - რომლებიც ეროვნული კანონმდებლობით განსაზღვრულ გარკვეულ პირობებს აკმაყოფილებენ - უფლება აქვთ, დაიცვან მონაცემთა სუბიექტების ინტერესები. კერძოდ, არაერთი ეროვნული კანონმდებლობის თანახმად, ბავშვებსა და ინტელექტუალური შეზღუდვის მქონე პირებს მათი მეურვეები უნდა წარმოადგენდნენ. [621] ევროკავშირის მონაცემთა დაცვის კანონმდებლობის შესაბამისად, ასოციაციას, რომელსაც აქვს მონაცემთა უფლებების დაცვის კანონიერი მიზანი, შეუძლია მონაცემთა სუბიექტის ინტერესები დაიცვას საზედამხედველო ორგანოს წინაშე, ან სასამართლოში.[622]

6.2.1 საზედამხედველო ორგანოში საჩივრის შეტანის უფლება

ევროპის საბჭოსა და ევროკავშირის კანონმდებლობით, ფიზიკურ პირებს ენიჭებათ კომპეტენტურ საზედამხედველო ორგანოში განცხადებისა და საჩივრების შეტანის უფლება, თუკი მიიჩნევენ, რომ მათი პერსონალური მონაცემების დამუშავება არ იყო კანონის შესაბამისი.

621 FRA (2015), ევროპული სამართლის სახელმძღვანელო ბავშვთა უფლებებზე, ლუქსემბურგი, Publications Office; FRA (2013), ინტელექტუალური შეზღუდვის მქონე და ფსიქიკური ჯანმრთელობის პრობლემების პირთა ქმედუნარიანობა, ლუქსემბურგი, Publications Office.

622 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 80.

მოდერნიზებული 108-ე კონვენცია აღიარებს მონაცემთა სუბიექტის უფლებას, კონვენციით გათვალისწინებული უფლებებით სარგებლობისას დაიხმაროს საზედამხედველო ორგანო, მისი წარმომავლობისა და საცხოვრებელი ადგილის მიუხედავად.[623] დახმარების თხოვნის უარყოფა შეიძლება მხოლოდ განსაკუთრებულ შემთხვევებში, მონაცემთა სუბიექტს კი არ უნდა დაეკისროს დახმარებასთან დაკავშირებული ხარჯებისა და მოსაკრებლების დაფარვა.[624]

იმავე დებულებებს შეიცავს ევროკავშირის სამართლებრივი სისტემაც. GDPR-ის თანახმად, საზედამხედველო ორგანოებმა უნდა მიიღონ ზომები, რომლებიც ხელს შეუწყობს საჩივრების წარდგენას (მაგ.: საჩივრის ელექტრონული ფორმა).[625] მონაცემთა სუბიექტს უფლება აქვს, წევრი სახელმწიფოს საზედამხედველო ორგანოში შეიტანოს საჩივარი, მისი მუდმივი საცხოვრებლის, სამსახურის ან სავარაუდო დარღვევის ადგილის მიხედვით.[626] საჩივრები უნდა განხილონ/გამოიძიონ, საზედამხედველო ორგანომ კი შესაბამის პირს შეატყობინოს მის მოთხოვნასთან დაკავშირებული წარმოების შედეგები.[627]

ევროკავშირის ინსტიტუტებისა თუ ორგანოების მიერ ჩადენილ სავარაუდო დარღვევებზე ფიზიკურ პირებს შეუძლიათ მიმართონ ევროკავშირის მონაცემთა დაცვის ზედამხედველს. [628] თუ ეს უკანასკნელი 6 თვის ვადაში არ უპასუხებს მათ, საჩივარი უარყოფილად უნდა ჩაითვალოს. ზედამხედველის გადაწყვეტილების გასაჩივრება შესაძლებელია CJEU-ში, (EC) No. 45/2001 რეგულაციის თანახმად, რომელიც ევროკავშირის ინსტიტუტებსა და ორგანოებს აკისრებს მონაცემთა დაცვის წესებთან შესაბამისობის ვალდებულებას.

აუცილებელია, არსებობდეს ეროვნული საზედამხედველო ორგანოს გადაწყვეტილების სასამართლოში გასაჩივრების შესაძლებლობა. ეს ეხება როგორც მონაცემთა სუბიექტს, ისე დამმუშავებელსა და უფლებამოსილ პირს, რომელიც საზედამხედველო ორგანოში მიმდინარე წარმოების მხარეა.

მაგალითი: 2017 წლის სექტემბერში ესპანეთის საზედამხედველო ორგანომ მონაცემთა დაცვის რამდენიმე რეგულაციის დარღვევისთვის დაა-

623 მოდერნიზებული 108-ე კონვენცია, მუხლი 18.

624 *იქვე,* მუხლი 16–17.

625 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 57 (2).

626 *იქვე,* მუხლი 77 (1).

627 *იქვე,* მუხლი 77 (2).

628 ევროპული პარლამენტისა და საბჭოს 2000 წლის 18 დეკემბრის რეგულაცია (EC) No. 45/2001 ევროკავშირის ინსტიტუტებისა და ორგანოების მიერ პერსონალური მონაცემების დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ 2001 L 8.

ჯარიმა Facebook. კერძოდ, ჯარიმის დაკისრების საფუძველი იყო კომპანიის მიერ განსაკუთრებული კატეგორიის პერსონალური მონაცემების შეგროვება, შენახვა და დამუშავება სარეკლამო მიზნებით და მონაცემთა სუბიექტის ნებართვის გარეშე. გადაწყვეტილება ეფუძნებოდა გამოძიებას, რომელიც საზედამხედველო ორგანოს ინიციატივით ჩატარდა.

6.2.2 უფლება სამართლებრივი დაცვის ეფექტიან საშუალებაზე

საზედამხედველო ორგანოში საჩივრის შეტანის გარდა, ფიზიკურ პირებს უნდა ჰქონდეთ უფლება ეფექტიანი სამართლებრივი დაცვის საშუალებასა და საქმის სასამართლოში წარდგენაზე. აქედან პირველ უფლებას იცავს ევროპული სამართლებრივი ტრადიცია და აღიარებულია ფუნდამენტურ უფლებად, როგორც Charter-ის 47-ე მუხლის, ისე ECHR-ის მე-13 მუხლის შესაბამისად.[629]

ევროკავშირის კანონმდებლობაში მონაცემთა სუბიექტების სამართლებრივი დაცვის ეფექტიანი საშუალების მნიშვნელობა მათი უფლებების დარღვევის შემთხვევაში, ნათლად ჩანს GDPR-ის დებულებებითაც (რომლებიც აღნიშნულ უფლებას ადგენს საზედამხედველო ორგანოების, მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის წინააღმდეგ) და CJEU-ს პრეცედენტულ სამართალშიც.

მაგალითი: *Schrems*-ის საქმეში[630] CJEU-მ „გადაწყვეტილება დაცვის საშუალებათა ადეკვატურობის შესახებ“ (Safe Harbour Adequacy Decision) ძალადაკარგულად გამოაცხადა. ეს გადაწყვეტილება იძლეოდა ევროკავშირიდან მონაცემთა გადაცემის საშუალებას დაცვის საშუალებათა სქემის (Safe Harbour scheme) საფუძველზე თვითსერტიფიცირებული ამერიკული ორგანიზაციებისათვის. სასამართლომ დაადგინა, რომ სქემას რამდენიმე ნაკლი ჰქონდა, რაც ზღუდავდა ევროკავშირის მოქალაქეთა ფუნდამენტურ უფლებებს პირადი ცხოვრების ხელშეუხებლობასა და პერსონალური მონაცემების დაცვაზე, ასევე, სამართლებრივი დაცვის ეფექტიან საშუალებაზე.

პირადი ცხოვრებისა მონაცემთა დაცვის უფლებების დარღვევასთან დაკავშირებით, CJEU-მ ხაზგასმით აღნიშნა, რომ აშშ-ის კანონმდებლობა გარკვეულ საჯარო უწყებებს აძლევს საშუალებას, ჰქონდეთ წვდომა

629 იხ: ECtHR, *Karabeyoğlu v. Turkey, No. 30083/10*, 2016 წლის 7 ივნისი; *ECtHR, Mustafa Sezgin Tanrıkulu v. Turkey,* No. 27473/06, 2017 წლის 18 ივლისი.

630 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 16 ოქტომბერი.

ევროკავშირის წევრი სახელმწიფოებიდან გადაცემულ პერსონალურ მონაცემებზე და დაამუშაონ ისინი იმ ფორმით, რომელიც არ შეესაბამება მონაცემთა გადაცემის თავდაპირველ მიზანს და სცდება ეროვნული უსაფრთხოების დაცვის მკაცრი აუცილებლობისა და პროპორციულობის ფარგლებს. სამართლებრივი დაცვის ეფექტიანი საშუალების უფლებასთან მიმართებით, სასამართლომ აღნიშნა, რომ მონაცემთა სუბიექტებს არ ჰქონდათ უფლებების აღდგენის/დაცვის ადმინისტრაციული ან სამართლებრივი საშუალება, რაც მათ მისცემდა შესაძლებლობას, მოეთხოვათ მონაცემებზე წვდომა, მათი გასწორება ან წაშლა. CJEU-მ დაასკვნა, რომ კანონმდებლობა, რომელიც არ ითვალისწინებს უფლების აღდგენის/დაცვის მოთხოვნას პერსონალურ მონაცემებზე წვდომის, გასწორებისა თუ წაშლის გზით, „არ სცემს პატივს სამართლებრივი დაცვის ეფექტიან საშუალებაზე წვდომის ფუნდამენტურ უფლებას, დაცულს ქარტიის 47-ე მუხლით.“ მან ხაზგასმით აღნიშნა, რომ ისეთი სამართლებრივი დაცვის საშუალება, რომელიც უზრუნველყოფს შესაბამისობას სამართლებრივ წესებთან, კანონის უზენაესობის განუყოფელი ნაწილია.

ფიზიკურ პირს, მონაცემთა დამმუშავებელს ან უფლებამოსილ პირს, რომელსაც სურს, გაასაჩივროს საზედამხედველო ორგანოს სამართლებრივად სავალდებულო ძალის მქონე გადაწყვეტილება, შეუძლია, მიმართოს სასამართლოს.[631] დაუშვებელია ტერმინ „გადაწყვეტილების“ ისე ფართოდ განმარტება, რომ მოიცავდეს საზედამხედველო ორგანოს მიერ გამოძიების, სანქციის დაკისრებისა და ავტორიზაციის უფლებამოსილების განხორციელებას, ასევე, გადაწყვეტილებას საჩივრის უარყოფასა თუ დაუშვებლად ცნობაზე. ამასთან, ფიზიკური პირი, მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი ვალდებულია, მიმართოს იმ წევრი სახელმწიფოს სასამართლოს, სადაც საზედამხედველო ორგანოა შექმნილი.[632] სასამართლოსთვის მიმართვის უფლება არ ვრცელდება საზედამხედველო ორგანოს არასავალდებულო ღონისძიებებზე - (მაგ.: მოსაზრებები ან კონსულტაცია).[633]

თუ მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი დაარღვევს მონაცემთა სუბიექტის უფლებას, ამ უკანასკნელს ენიჭება სასამართლოში სარჩელის შეტანის უფლება.[634] მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის წინააღმდეგ აღძრულ საქმესთან დაკავშირებით განსაკუთრებით მნიშვნელოვანია, ფიზიკურ პირს ჰქონდეს არჩევანის საშუალება, თუ სად შეიტანოს სარჩელი. მას სარჩელის შეტანა შეუძლია იმ წევრი სახელმწიფოს სასამარ-

631 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 78.

632 *იქვე*, მუხლი 78 (3).

633 *იქვე*, პრეამბულა, პუნქტი 143.

634 *იქვე*, მუხლი 79.

თლოში, სადაც შექმნილია მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი, ანდა ცხოვრობს მონაცემთა სუბიექტი.[635] მეორე შესაძლებლობა მნიშვნელოვნად უწყობს ხელს ფიზიკურ პირთა უფლებების განხორციელებას და საშუალებას იძლევა, საჩივარი შეიტანონ იმ სახელმწიფოში, სადაც ცხოვრობენ, და იურისდიქციაში, რომელსაც კარგად იცნობენ. ასეთი საჩივრის შეტანაზე გეოგრაფიული შეზღუდვის დაწესებამ შეიძლება სხვა წევრ სახელმწიფოში მცხოვრებ სუბიექტს გადააფიქრებინოს სარჩელის შეტანა, რადგან ამ მიზნით მას მოუწევს სამგზავრო და დამატებითი ხარჯების გაღება; ამასთან, წარმოება ჩატარდება უცხო ენაზე და უცხო იურისდიქციაში. გამონაკლისი დაშვებულია მხოლოდ მაშინ, როდესაც მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი საჯარო უწყებაა, ხოლო მონაცემები მუშავდება ამ უწყებათა საჯარო უფლებამოსილების განხორციელების ფარგლებში. ასეთ შემთხვევაში, საჩივრის განხილვა შეუძლიათ მხოლოდ იმ სახელმწიფოს სასამართლოებს, სადაც საჯარო უწყება მდებარეობს.[636]

ზოგადად, მონაცემთა დაცვის წესების დარღვევასთან დაკავშირებულ საჩივარზე გადაწყვეტილებას იღებს წევრი სახელმწიფო. თუმცა, გარკვეულ შემთხვევებში საჩივრის შეტანა შესაძლებელია ევროკავშირის მართლმსაჯულების სასამართლოში. ეს ხდება ორ შემთხვევაში:

(1) როდესაც მონაცემთა სუბიექტი, მონაცემთა დამმუშავებელი, უფლებამოსილი პირი ან საზედამხედველო ორგანო EDPB-ის გადაწყვეტილების გაუქმებას ითხოვს. აღნიშნულ საჩივარზე ვრცელდება TFEU-ს 263-ე მუხლის პირობები, კერძოდ: საჩივრის დასაშვებობისთვის შესაბამისმა პირებმა და დაწესებულებებმა უნდა აჩვენონ, რომ საბჭოს გადაწყვეტილება მათ პირდაპირ და ინდივიდუალურად ეხება;

(2) საქმე ეხება პერსონალურ მონაცემთა უკანონო დამუშავებას ევროკავშირის ინსტიტუტებისა თუ ორგანოების მიერ. როცა მონაცემთა დაცვის კანონმდებლობას არღვევენ ევროკავშირის ინსტიტუტები, მონაცემთა სუბიექტებს უფლება აქვთ, საჩივარი პირდაპირ ევროკავშირის გენერალურ სასამართლოში აღძრან (გენერალური სასამართლო CJEU-ს შემადგენელი ნაწილია). გენერალური სასამართლო არის პირველი ინსტანციის სასამართლო, რომელიც განიხილავს ევროკავშირის კანონმდებლობის დარღვევას მისი ინსტიტუტების მიერ. ამრიგად, EDPS-ის - როგორც ევროკავშირის ინსტიტუტის - წინააღმდეგ საჩივრების შეტანა შესაძლებელია გენერალურ სასამართლოშიც.[637]

635 *იქვე,* მუხლი 79 (2).

636 *იქვე.*

637 რეგულაცია (EC) No. 45/2001, მუხლი 32 (3).

მაგალითი: *Bavarian Lager*[638]-ის საქმეში კომპანიამ ევროპულ კომისიას მიმართა განცხადებით კომისიის მიერ გამართული შეხვედრების ჩანაწერთა მიწოდებაზე, ვინაიდან ეს შეხვედრები, სავარაუდოდ, უკავშირდებოდა კომპანიისათვის რელევანტურ სამართლებრივ საკითხებს. კომისიამ კომპანიის განცხადება არ დააკმაყოფილა იმ მიზეზით, რომ მონაცემთა დაცვის ინტერესები აღემატებოდა კომპანიის ინტერესებს.[639] Bavarian Lager-მა, ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაციის 32-ე მუხლის თანახმად, პირველი ინსტანციის სასამართლოს (გენერალური სასამართლოს წინამორბედი) მიმართა საჩივრით. სასამართლომ საკუთარი გადაწყვეტილებით (საქმეზე T194/04, *The Bavarian Lager Co. Ltd v. Commission of the European Communities*) გააუქმა კომისიის გადაწყვეტილება, რომლითაც განმცხადებელს უარი ეთქვა მონაცემების მიწოდებაზე. ევროპულმა კომისიამ ის CJEU-ში გაასაჩივრა.

CJEU-მ (დიდმა პალატამ) მიიღო გადაწყვეტილება, რომლითაც გააუქმა პირველი ინსტანციის სასამართლოს გადაწყვეტილება და მხარი დაუჭირა ევროპული კომისიის უარს მონაცემთა მიწოდებაზე, შეხვედრის მონაწილეთა პერსონალური მონაცემების დაცვის მოტივით. CJEU-ს დასკვნით, კომისიამ მიიღო სწორი გადაწყვეტილება - მან უარი განაცხადა ინფორმაციის გამჟღავნებაზე, იმის გათვალისწინებით, რომ მონაწილეებს თავიანთი პერსონალური მონაცემების გამჟღავნებაზე თანხმობა არ ჰქონდათ გაცემული. ამასთან, Bavarian Lager-მა ვერ წარმოადგინა საკმარისი მტკიცებულება, რომ მოთხოვნილი ინფორმაცია მისთვის აუცილებელი იყო.

და ბოლოს, მონაცემთა სუბიექტებს, დამმუშავებლებსა თუ უფლებამოსილ პირებს უფლება აქვთ, ეროვნულ დონეზე სამართალწარმოების პროცესში სასამართლოს მიმართონ თხოვნით, რომ CJEU-სგან მოითხოვონ ევროკავშირის ინსტიტუტების, ორგანოების, ოფისებისა თუ სააგენტოების მიერ გამოცემული აქტების ან მათი საფუძვლიანობის განმარტება. ასეთ განმარტებას წინასწარი განჩინება ეწოდება. ეს არ არის პირდაპირი სამართლებრივი დაცვის საშუალება განმცხადებლისთვის, თუმცა, ეროვნულ სასამართლოებს ევროკავშირის კანონმდებლობის სწორი ინტერპრეტაციის საშუალებას აძლევს. სწორედ წინასწარი განჩინების მექანიზმის წყალობით მოხვდა ევროკავშირის მართლმსაჯულების სასამართლოში ისეთი მნიშვნელოვანი საქმეები, როგორიცაა *Digital Rights Ireland* and Kärntner Landesregierung and Others[640]

638 CJEU, C-28/08 P, *European Commission v. The Bavarian Lager Co.* Ltd [GC], 2010.

639 ანალიზისა და არგუმენტებისათვის, იხ., EDPS (2011), Bavarian Lager-ის საქმეში მიღებული გადაწყვეტილების შემდგომ, საჯარო წვდომა დოკუმენტებზე, რომლებიც პერსონალურ მონაცემებს შეიცავს, ბრიუსელი, EDPS.

640 CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი.

და *Maximilian Schrems v. Data protection*[641], რომლებმაც მნიშვნელოვანი გავლენა იქონიეს ევროკავშირის მონაცემთა დაცვის კანონმდებლობის ჩამოყალიბებაზე.

მაგალითები: გაერთიანებული საქმე *Digital Rights Ireland* and *Kärntner Landesregierung and Others*[642] CJEU-ს წარუდგინეს ირლანდიის უზენაესმა სასამართლომ და ავსტრიის საკონსტიტუციო სასამართლომ. იგი მიემართებოდა 2006/24/EC დირექტივის (მონაცემთა შენახვის დირექტივა) შესაბამისობას ევროკავშირის მონაცემთა დაცვის კანონმდებლობასთან. ავსტრიის საკონსტიტუციო სასამართლოს მიერ CJEU-სთვის დასმული კითხვები შეეხებოდა დირექტივის მე-3 და მე-9 მუხლების კანონიერებას, ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-7, მე-9 და მე-11 მუხლების გათვალისწინებით. ეს მოიცავდა ავსტრიის ტელეკომუნიკაციების ფედერალური კანონის გარკვეულ დებულებათა (რომლითაც მონაცემთა შენახვის დირექტივა გადავიდა ეროვნულ კანონმდებლობაში) შესაბამისობას მონაცემთა დაცვის დირექტივასა და ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაციასთან.

საქმეში *Kärntner Landesregierung and Others* ბატონი სეტლინჯერი, საკონსტიტუციო სასამართლოში მიმდინარე წარმოების ერთ-ერთი მხარე (განმცხადებელი), აცხადებდა, რომ როგორც სამსახურებრივი, ისე პირადი ცხოვრების მიზნებისთვის იყენებდა ტელეფონს, ინტერნეტსა და ელფოსტას. შედეგად, იგი ინფორმაციას იღებდა და გადასცემდა საჯარო ტელეკომუნიკაციის ქსელების გავლით. ტელეკომუნიკაციების შესახებ ავსტრიის აქტის (2003 წ.) თანახმად, სატელეკომუნიკაციო პროვაიდერს, რომელსაც იყენებდა მოასრჩელე, სამართლებრივად ეკისრებოდა მონაცემთა შეგროვებისა და შენახვის ვალდებულება მომხმარებელთა მიერ ქსელის გამოყენების შესახებ. ბ-ნი სეტლინჯერი მიიჩნევდა, რომ ამ ვალდებულების ფარგლებში, მისი პერსონალური მონაცემების შეგროვება და შენახვა არ იყო აუცილებელი ქსელის საშუალებით ინფორმაციის მიღებისა და გაგზავნის ტექნიკური მიზნებისათვის. მისი მტკიცებით, ეს არც ანგარიშსწორებისთვის გახლდათ საჭირო. ბ-ნი სეტლინჯერი აცხადებდა, რომ იმ პერსონალური მონაცემების გამოყენებაზე, რომელთა შეგროვება და შენახვაც ეფუძნებოდა ავსტრიის ტელეკომუნიკაციების აქტს, თანხმობა არ ჰქონდა გაცემული.

ამის გამო, ბ-ნმა სეტლინჯერმა ავსტრიის საკონსტიტუციო სასამართლოში შეიტანა საჩივარი, რომელშიც აცხადებდა, რომ სატელეკომუნიკაციო

641 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი.

642 CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი.

პროვაიდერის კანონით გათვალისწინებული ვალდებულებები არღვევდა მის უფლებებს, დაცულს ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლით. ვინაიდან ავსტრიის შესაბამისი კანონმდებლობა ევროკავშირის კანონმდებლობას (კერძოდ, მონაცემთა შენახვის დირექტივას) ამკვიდრებდა, ქვეყნის საკონსტიტუციო სასამართლომ საქმე გადასცა CJEU-ს, რათა განეხილა დირექტივის შესაბამისობა პირადი ცხოვრებისა და მონაცემთა დაცვის უფლებებთან, რომლებიც გარანტირებულია ევროკავშირის ფუნდამენტურ უფლებათა ქარტიით.

საქმეზე იმსჯელა CJEU-ს დიდმა პალატამ, რის შედეგადაც გააუქმა ევროკავშირის მონაცემთა დაცვის დირექტივა. მან დაადგინა, რომ დირექტივა ითვალისწინებდა განსაკუთრებით მძიმე ჩარევას პირადი ცხოვრებისა და პერსონალური მონაცემების დაცვის ფუნდამენტურ უფლებებში, რაც არ იყო შეზღუდული მკაცრი აუცილებლობით. დირექტივა კანონიერ მიზანს ემსახურებოდა, რადგან ქვეყნის ხელისუფლებას აძლევდა დამატებით შესაძლებლობას მძიმე დანაშაულების გამოსაძიებლად და დამნაშავეთა დასასჯელად, ეს კი ფასეული ინსტრუმენტია სისხლის სამართლის საქმის გამოძიების პროცესში. ამავდროულად, CJEU-მ განაცხადა, რომ ფუნდამენტურ უფლებებზე დაწესებული შეზღუდვების გამოყენება შეიძლება მხოლოდ იმ შემთხვევაში, როცა ეს მკაცრად აუცილებელია. შეზღუდვებით სარგებლობას თან უნდა ახლდეს მკაფიო და ზუსტი წესები მათი მოქმედების სფეროსთან დაკავშირებით და ფიზიკური პირებისათვის გათვალისწინებული დაცვის გარანტიები.

CJEU-ს თანახმად, დირექტივამ ვერ დააკმაყოფილა აუცილებლობის სტანდარტი. კერძოდ, პირველ რიგში, იგი არ განსაზღვრავდა მკაფიო და ზუსტ წესებს, რომლებიც შეზღუდავდა უფლებებში ჩარევის ფარგლებს; ასევე, არ ადგენდა მოთხოვნას შენახულ მონაცემებსა და მძიმე დანაშაულს შორის კავშირის არსებობაზე. მისი მოქმედება ვრცელდებოდა ყველა ელექტრონული კომუნიკაციის საშუალების მომხმარებელთა ნებისმიერ მეტამონაცემზე. ამრიგად, დირექტივა, ფაქტობრივად, ერეოდა ევროკავშირის მთლიანი მოსახლეობის პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის უფლებებში, რაც შესაძლოა ჩაითვალოს არაპროპორციულად. დირექტივა არ ითვალისწინებდა პირობებს პერსონალურ მონაცემებზე წვდომის შესაზღუდად, წვდომაზე კი არ ვრცელდებოდა ისეთი პროცედურული პირობები, როგორიცაა ადმინისტრაციული ორგანოს ან სასამართლოს ნებართვის მოთხოვნა. და ბოლოს, დირექტივა არ განსაზღვრავდა მკაფიო მექანიზმებს შენახულ მონაცემთა დასაცავად. ამრიგად, ვერ უზრუნველყოფდა მონაცემთა ეფექტიან დაცვას ბოროტად გამოყენების, უკანონო წვდომისა თუ მოხმარებისგან.[643]

643 CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი, პუნქტი 69.

ზოგადად, CJEU ვალდებულია, უპასუხოს მიმართვას. მას არ აქვს უფლება, უარი თქვას წინასწარი განჩინების გამოტანაზე - იმ მიზეზით, რომ რეაგირება არ იქნება რელევანტური ან დროული თავდაპირველ საქმესთან მიმართებით. ამავდროულად, სასამართლოს აქვს უარის თქმის უფლება, თუ კონკრეტული საკითხი მისი უფლებამოსილების სფეროში არ ხვდება.[644] CJEU გადაწყვეტილებას იღებს მხოლოდ შემოსული მიმართვის შემადგენელ ელემენტებზე, თავდაპირველი საქმე კი ეროვნული სასამართლოს უფლებამოსილებაში რჩება.[645]

ევროპის საბჭოს კანონმდებლობით, ხელშემკვრელ მხარეებს ეკისრებათ სათანადო სამართლებრივი თუ არასამართლებრივი დაცვის საშუალებების შექმნა მოდერნიზებული 108-ე კონვენციის დებულებათა დარღვევებთან მიმართებით.[646] შიდასახელმწიფოებრივი დაცვის საშუალებათა ამოწურვის შემთხვევაში, პირს აქვს უფლება, ადამიანის უფლებათა ევროპულ სასამართლოს მიმართოს ევროპული კონვენციის ხელშემკვრელი მხარის წინააღმდეგ, პერსონალურ მონაცემთა დაცვის იმ სავარაუდო დარღვევებზე, რომლებიც კონვენციის მე-8 მუხლს ეწინააღმდეგება. ევროპულ სასამართლოში შეტანილი განაცხადი უნდა აკმაყოფილებდეს დასაშვებობის კრიტერიუმსაც (კონვენცია, მუხლები 34-35).[647]

მიუხედავად იმისა, რომ ადამიანის უფლებათა ევროპულ სასამართლოში განაცხადის შეტანა შესაძლებელია მხოლოდ ხელშემკვრელი მხარის წინააღმდეგ, საჩივარი შეიძლება ირიბად ეხებოდეს კერძო პირის ქმედებებს ან უმოქმედობასაც, თუ ხელშემკვრელი მხარე არ შეასრულებს კონვენციით დაკისრებულ პოზიტიურ ვალდებულებებს და ვერ ქმნის მონაცემთა დაცვის უფლების სათანადო გარანტიებს ეროვნულ კანონმდებლობაში.

მაგალითები: საქმეში *K.U. v. Finland*[648] განმცხადებელი (მცირეწლოვანი) აცხადებდა, რომ ინტერნეტგვერდმა მის შესახებ გამოაქვეყნა სქესობრივი ხასიათის რეკლამა. სერვისპროვაიდერი უარს აცხადებდა იმ პირის ვინაობის გამჟღავნებაზე, რომელმაც ეს გააკეთა და საფუძვლად მიუთითებდა ფინეთის კანონმდებლობით გათვალისწინებულ კონფიდენციალობის ვალდებულებებს. განმცხადებელი აცხადებდა, რომ ეროვნული კანონმდებლობა ვერ იცავდა იმ კერძო პირის ქმედებებისგან, რომელმაც მის შესახებ ინტერნეტში დანაშაულებრივი მონაცემები გამოაქვეყნა. ECtHR-

644 CJEU, C-244/80, *Pasquale Foglia v. Mariella Novello (No. 2), 16 December 1981; CJEU, C-467/04, Criminal Proceedings against Gasparini and Others,* 2006 წლის 28 სექტემბერი.

645 CJEU, C-438/05, *International Transport Workers› Federation, Finnish Seamen›s Union v. Viking Line ABP, OÜ Viking Line Eesti* [GC], 2007 წლის 11 დეკემბერი, პუნქტი 85.

646 მოდერნიზებული 108-ე კონვენცია, მუხლი 12.

647 ECHR, მუხლი 34–37.

648 ECtHR, *K.U. v. Finland,* No. 2872/02, 2008 წლის 2 დეკემბერი.

მა დაადგინა, რომ ხელშემკვრელ სახელმწიფოს ეკისრება არა მხოლოდ პირად ცხოვრებაში თვითნებური ჩარევისგან თავშეკავება, არამედ ის პოზიტიური ვალდებულებებიც, რომლებიც მოიცავს „ზომების მიღებას პირადი ცხოვრების პატივისცემის უფლების დასაცავად, მათ შორის, ფიზიკურ პირებს შორის ურთიერთობის სფეროში.“ განმცხადებლის შემთხვევაში, მისი პრაქტიკული და ეფექტიანი დაცვა მოითხოვდა სათანადო ნაბიჯების გადადგმას დამნაშავის იდენტიფიცირებისა და დასჯისათვის. თუმცა, სახელმწიფომ ვერ შეძლო ამის უზრუნველყოფა, რის გამოც სასამართლომ საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

საქმეში *Köpke v. Germany*[649] განმცხადებელზე, რომელიც სამსახურში ქურდობაში იყო ეჭვმიტანილი, ხორციელდებოდა ვიდეოთვალთვალი. ECtHR-ის განმარტებით, „არაფერი მიუთითებდა იმაზე, რომ ეროვნულმა ხელისუფლებამ ვერ შეძლო თავისუფალი შეფასების ფარგლებში დაებალანსებინა, ერთი მხრივ, განმცხადებლის პირადი ცხოვრების პატივისცემის უფლება, რომელსაც იცავს მე-8 მუხლი, მეორე მხრივ კი მისი დამსაქმებლის საკუთრების უფლება და საზოგადოების ინტერესი მართლმსაჯულების აღსრულების მიმართ.“ შესაბამისად, სასამართლომ საჩივარი დაუშვებლად ცნო.

თუ ევროპული სასამართლო დაადგენს, რომ ხელშემკვრელმა სახელმწიფომ დაარღვია ევროპული კონვენციით დაცული რომელიმე უფლება, სახელმწიფო ვალდებულია, აღასრულოს სასამართლოს გადაწყვეტილება (კონვენციის 46-ე მუხლი). აღსრულების ღონისძიებებმა, პირველ რიგში, უნდა აღმოფხვრას დარღვევა და მაქსიმალურად აღადგინოს/გამოასწოროს მოსარჩელის უფლება. გადაწყვეტილების აღსრულება შეიძლება საჭიროებდეს ზოგად ღონისძიებებსაც სასამართლოს მიერ დადგენილი დარღვევის მსგავსი შემთხვევების თავიდან ასაცილებლად (მაგ.: საკანონმდებლო ცვლილებები, პრეცედენტული სამართალი თუ სხვა ზომები).

თუ ECtHR დაადგენს კონვენციის დარღვევას, 41-ე მუხლის თანახმად, სასამართლო, ხელშემკვრელი სახელმწიფოს ხარჯზე, განმცხადებელს უზრუნველყოფს „სამართლიანი დაკმაყოფილებით.“

წარმომადგენლობის უფლებამოსილების მინიჭება არაკომერციული იურიდიული პირის, ორგანიზაციისა თუ ასოციაციისათვის

GDPR ფიზიკურ პირს საშუალებას აძლევს, საზედამხედველო ორგანოში საჩივრის შეტანის ან სასამართლოსთვის მიმართვის შემთხვევაში, წარმომადგენლობის უფლებამოსილება მიანიჭოს არაკომერციულ იურიდიულ პირს,

649 ECtHR, *Köpke v. Germany (dec.)*, No. 420/07, 2010 წლის 5 ოქტომბერი.

ორგანიზაციასა თუ ასოციაციას.[650] ასეთ დაწესებულებას უნდა ჰქონდეს საჯარო ინტერესის შესაბამისი კანონიერი მიზნები და მუშაობდეს მონაცემთა დაცვის სფეროში. მას უფლება აქვს, შეიტანოს საჩივარი და ისარგებლოს სამართლებრივი დაცვის ეფექტიანი საშუალებით, როგორც მონაცემთა სუბიექტმა. რეგულაცია წევრ სახელმწიფოებს აძლევს შესაძლებლობას, ეროვნული კანონმდებლობის საფუძველზე გადაწყვიტონ, რამდენად შეძლებს ასეთი დაწესებულება საჩივრის შეტანას მონაცემთა სუბიექტის სახელით, თუკი მონაცემთა სუბიექტს ეს მისთვის არ დაუვალებია.

წარმომადგენლობის უფლება ფიზიკურ პირებს საშუალებას აძლევს, ისარგებლონ ასეთი არაკომერციული დაწესებულებების ექსპერტული ცოდნითა და გამოცდილებით, ასევე, ორგანიზაციული და ფინანსური შესაძლებლობით, რაც მნიშვნელოვნად დაეხმარება მათ უფლებების განხორციელებაში. GDPR ჩამოთვლილ დაწესებულებებს საშუალებას აძლევს, მონაცემთა სუბიექტების სახელით შეიტანონ კოლექტიური საჩივრები, რაც დადებითად აისახება სასამართლო სისტემის ფუნქციონირებასა და ეფექტიანობაზე, რადგან ერთი და იგივე სასარჩელო მოთხოვნები ჯგუფდება და განიხილება ერთად.

6.2.3 პასუხისმგებლობა და კომპენსაციის უფლება

უფლება სამართლებრივი დაცვის ეფექტიან საშუალებაზე იძლევა კომპენსაციის მოთხოვნის შესაძლებლობას ზიანისათვის, რომელიც გამოწვეულია პერსონალურ მონაცემთა კანონდარღვევით დამუშავების შედეგად. მონაცემთა დამმუშავებლისა თუ უფლებამოსილი პირის პასუხისმგებლობას არაკანონიერ დამუშავებასთან დაკავშირებით ნათლად აღიარებს GDPR.[651] კერძოდ, რეგულაცია ფიზიკურ პირებს საშუალებას აძლევს, კომპენსაცია მოითხოვონ მონაცემთა დამმუშავებლისა ან უფლებამოსილი პირისგან, როგორც მატერიალური, ისე მორალური ზიანისთვის. რეგულაციის პრეამბულაში აღნიშნულია: „ზიანი უნდა განიმარტოს ზოგადად მართლმსაჯულების სასამართლოს გადაწყვეტილებათა საფუძველზე და სრულად ასახავდეს ამ რეგულაციის მიზნებს.“ [652] მონაცემთა დამმუშავებელს ეკისრება პასუხისმგებლობა, შესაძლოა, კომპენსაციის გადახდაც, თუკი არ შეასრულებს რეგულაციით გათვალისწინებულ ვალდებულებებს. უფლებამოსილი პირი დამუშავებით გამოწვეულ ზიანზე პასუხისმგებელია მაშინ, როცა არ შეასრულებს რეგულაციაში კონკრეტულად მისთვის განსაზღვრულ მოვალეობებს, ანდა იმოქმედებს მონაცემთა დამმუშავებლის კანონიერი ინსტრუქციების ფარგლებს გარეთ ან საწინააღმდეგოდ. თუ მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი სრულად

650 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 80.

651 *იქვე,* მუხლი 82.

652 *იქვე,* პრეამბულა, პუნქტი 146.

აანაზღაურებს ზიანს, მას შეუძლია, პროცესში ჩართულ სხვა დამმუშავებლებსა და უფლებამოსილ პირებს მოსთხოვოს კომპენსაციის ის ნაწილი, რომელიც შეესაბამება მათ წილ პასუხისმგებლობას მიყენებულ ზიანზე.[653] ამავდროულად, პასუხისმგებლობისგან გათავისუფლების პირობები საკმაოდ მკაცრია. ასეთ შემთხვევაში, უნდა წარმოადგინონ მტკიცებულება, რომ მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი არ არის რამე ფორმით პასუხისმგებელი ზიანის გამომწვევ მოვლენებზე.

კომპენსაცია უნდა იყოს „სრული და ეფექტიანი“ მიყენებულ ზიანთან მიმართებით. თუ ის გამოიწვია რამდენიმე დამმუშავებლის ან უფლებამოსილი პირის ერთობლივმა მოქმედებამ, თითოეულ მათგანს უნდა დაეკისროს პასუხისმგებლობა მთლიან ზიანზე. ამ წესის მიზანია მონაცემთა სუბიექტისათვის ეფექტიანი კომპენსაციის გაცემა და პროცესში მონაწილე მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის მიერ კოორდინირებული მიდგომის დანერგვა შესაბამისი სამართლებრივი ნორმების დაცვისადმი.

მაგალითი: მონაცემთა სუბიექტებს არ მოეთხოვებათ საჩივრის შეტანა და კომპენსაციის მოთხოვნა მიყენებულ ზიანზე პასუხისმგებელ ყველა დაწესებულებასთან მიმართებით, რადგან ეს ძვირადღირებული და ხანგრძლივი პროცესი იქნება. საკმარისია საჩივრის შეტანა მხოლოდ ერთ-ერთი თანადამმუშავებლის წინააღმდეგ, რომელსაც შემდეგ პასუხისმგებლობა დაეკისრება მთლიან ზიანზე. ასეთ შემთხვევაში, მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი, რომელიც მიყენებულ ზიანს აანაზღაურებს, გადახდილი თანხის ამოღებას შეძლებს იმ სხვა დაწესებულებებისგან, რომლებიც მონაწილეობდნენ დამუშავებაში და პასუხისმგებელნი არიან დარღვევაზე. მოთხოვნილი თანხა უნდა იყოს ამ პასუხისმგებლობის პროპორციული. აღნიშნული პროცესი თანადამმუშავებლებსა და უფლებამოსილ პირებს შორის წარიმართება მას შემდეგ, რაც მონაცემთა სუბიექტი მიიღებს კომპენსაციას. ეს ნიშნავს, რომ მონაცემთა სუბიექტი ამ პროცესში არ მონაწილეობს.

ევროპის საბჭოს კანონმდებლობაში მოდერნიზებული 108-ე კონვენციის მე-12 მუხლი ხელშემკვრელ სახელმწიფოებს ავალდებულებს უფლების აღდგენის/დაცვის სათანადო საშუალებათა შექმნას იმ ეროვნული კანონმდებლობის დარღვევასთან დაკავშირებით, რომლითაც სრულდება კონვენციის მოთხოვნები. კონვენციის განმარტებითი ბარათის თანახმად, ეს საშუალებები შეიძლება მოიცავდეს საჩივრის შეტანის შესაძლებლობას გადაწყვეტილების ან პრაქტიკის წინააღმდეგ. ამასთან, ხელმისაწვდომი უნდა იყოს არასამარ-

653 *იქვე*, მუხლი 82 (2) და (5).

თლებრივი დაცვის საშუალებებიც.[654] მათი მარეგულირებელი მოდალობებისა და წესების, ასევე, შესაბამისი პროცედურების განსაზღვრა დამოკიდებულია თითოეული ხელშემკვრელი სახელმწიფოს დისკრეციაზე (შეხედულებებზე). ხელშემკვრელმა მხარეებმა და ეროვნულმა სასამართლოებმა ასევე უნდა გაითვალისწინონ, რომ დამუშავების შედეგად მიყენებული მატერიალური და მორალური ზიანის ანაზღაურებისთვის მნიშვნელოვანია, არსებობდეს ფინანსური კომპენსაციის მარგულირებელი დებულებები და კოლექტიური საჩივრის შეტანის შესაძლებლობა.[655]

6.2.4 სანქციები

ევროპის საბჭოს კანონმდებლობაში, მოდერნიზებული 108-ე კონვენციის მე-12 მუხლის თანახმად, თითოეული ხელშემკვრელი სახელმწიფო უნდა ადგენდეს სათანადო სანქციებსა და დაცვის საშუალებებს იმ კანონმდებლობის დარღვევაზე, რომელიც ააქტიურებს კონვენციით გათვალისწინებულ მონაცემთა დაცვის ძირითად პრინციპებს. კონვენცია არ მოიცავს/ადგენს გარკვეულ სანქციებს. იგი აცხადებს, რომ სამართლებრივი (სისხლისსამართლებრივი, ადმინისტრაციული ან სამოქალაქო) და არასამართლებრივი სანქციები უნდა განსაზღვროს თითოეულმა ხელშემკვრელმა მხარემ, თავის შეხედულებაზე დაყრდნობით. კონვენციის განმარტებითი ბარათის თანახმად, სანქციები უნდა იყოს ეფექტიანი, პროპორციული და აღმკვეთი.[656] ხელშემკვრელმა სახელმწიფოებმა სწორედ ეს პრინციპი უნდა გაითვალისწინონ სამართლის ეროვნულ სისტემაში სანქციების ბუნებისა და სიმკაცრის განსაზღვრისას.

ევროკავშირის კანონმდებლობაში GDPR-ის 83-ე მუხლი წევრი სახელმწიფოების საზედამხედველო ორგანოებს აძლევს ადმინისტრაციული ჯარიმის დაკისრების უფლებამოსილებას რეგულაციის დარღვევის შემთხვევებში. ეს მუხლი ითვალისწინებს ჯარიმის დონესა და მაქსიმალურ ოდენობას, ასევე გარემოებებს, რომლებიც სახელმწიფო ორგანოებმა უნდა გაითვალისწინონ მისი დაკისრებისას. ამრიგად, სანქციების რეჟიმი ევროკავშირის მასშტაბით ჰარმონიზებულია.

GDPR ჯარიმებთან მიმართებით მოიცავს მრავალდონიან მიდგომას. საზედამხედველო ორგანოებს აქვთ უფლება, რეგულაციის დამრღვევს დააკისრონ ადმინისტრაციული ჯარიმა, მაქსიმუმ, 20,000,000 ევრო ან, საწარმოს/კომპანიის შემთხვევაში, მთლიანი წლიური საერთაშორისო ბრუნვის 4% (რომელიც უფრო მეტია). დარღვევები, რომლებზეც ასეთი სახის ჯარიმა ვრცელდება, მო-

654 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 100.

655 *იქვე.*

656 *იქვე.*

იცავს დამუშავების ძირითადი პრინციპების, თანხმობის პირობების, მონაცემთა სუბიექტების უფლებებისა და რეგულაციის იმ დებულებების დარღვევას, რომლებიც არეგულირებს პერსონალურ მონაცემთა გადაცემას მესამე ქვეყნებისთვის. სხვა სახის დარღვევებზე საზედამხედველო ორგანოს უფლება აქვს, დამრღვევს დააკისროს 10,000,000 ევრომდე ჯარიმა ან, საწარმოს/კომპანიის შემთხვევაში, მთლიანი წლიური საერთაშორისო ბრუნვის 2% (რომელიც უფრო მეტია).

ჯარიმის ტიპისა და ოდენობის განსაზღვრისას, საზედამხედველო ორგანოებმა უნდა გაითვალისწინონ არაერთი ფაქტორი[657] (მაგ.: დარღვევის სახე, სიმძიმე და ხანგრძლივობა; მონაცემთა კატეგორიები, რომლებსაც შეეხება დარღვევა და მისი განზრახ ან გაუფრთხილებლობით ჩადენა; დამმუშავებლისა და უფლებამოსილი პირის მიერ მიღებული ზომები მონაცემთა სუბიექტებისათვის მიყენებული ზიანის შესამცირებლად). საზედამხედველო ორგანოების გადაწყვეტილება უნდა ეყრდნობოდეს ისეთ მნიშვნელოვან ფაქტორებსაც, როგორიცაა საზედამხედველო ორგანოსთან თანამშრომლობის ხარისხი დარღვევის შემდეგ; როგორ შეიტყო საზედამხედველო ორგანომ დარღვევის შესახებ (დამუშავებაზე პასუხისმგებელი უწყებისგან თუ მონაცემთა სუბიექტისგან, რომლის უფლებებიც დაირღვა) და სხვა.[658]

ადმინისტრაციული ჯარიმის დაკისრებასთან ერთად, საზედამხედველო ორგანოებს აქვთ სხვადასხვა ღონისძიების გატარების უფლებამოსილება დარღვევის გამოსასწორებლად. ეს დეტალურად არის წარმოდგენილი რეგულაციის 58-ე მუხლში და ითვალისწინებს შემდეგ ზომებს: მონაცემთა დამმუშავებლისა და უფლებამოსილი პირისთვის მითითების მიცემა; გაფრთხილებისა თუ საყვედურის გამოცხადება; დამუშავების დროებით ან სამუდამოდ აკრძალვა.

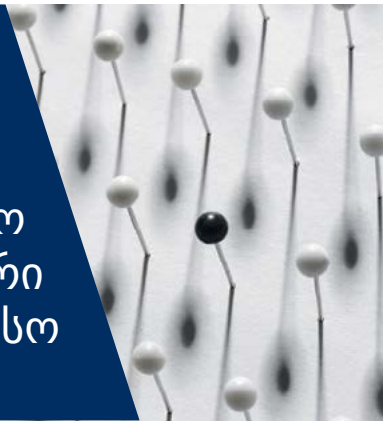
რაც შეეხება ევროკავშირის კანონმდებლობის დარღვევას მისი ინსტიტუტებისა თუ ორგანოების მიერ, მონაცემთა დაცვის რეგულაციის სპეციალური ფარგლების გამო, სანქციებს შეიძლება ჰქონდეს დისციპლინური პასუხისმგებლობის სახე. 49-ე მუხლის თანახმად, „წინამდებარე რეგულაციით განსაზღვრული ვალდებულებების შეუსრულებლობის გამო (განზრახ ან გაუფრთხილებლობით), ევროკომისიის წევრ ან სხვა წარმომადგენელს დაეკისრება დისციპლინური პასუხისმგებლობა [...].“

657 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 83 (2).

658 29-ე მუხლის სამუშაო ჯგუფი(2017), სახელმძღვანელო პრინციპები 2016/679 რეგულაციის მიზნებისთვის ადმინისტრაციული ჯარიმების გამოყენებისა და შემუშავების შესახებ, WP 253, 2017 წლის 3 ოქტომბერი.

7

მონაცემთა საერთაშორისო გადაცემა და პერსონალური მონაცემების საერთაშორისო მიმოცვლა



ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
პერსონალური მონაცემების გადაცემა		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 44	**კონცეფცია**	მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (1) (2)
პერსონალური მონაცემების თავისუფალი მიმოცვლა		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 1 (3) და პრეამბულის მუხლი 170	**ევროკავშირის წევრ სახელმწიფოებს შორის**	
	მოდერნიზებული 108-ე კონვენციის ხელშემკვრელ მხარეებს შორის	მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (1)
პერსონალური მონაცემების გადაცემა მესამე ქვეყნებისთვის ან საერთაშორისო ორგანიზაციებისთვის		
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 45; C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015.	**შესაბამისობის გადაწყვეტილება/ მესამე ქვეყნები ან საერთაშორისო ორგანიზაციები, სადაც დაცვის სათანადო დონეა**	მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (2)

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 46 (1) და 46 (2)	**დაცვის სათანადო გარანტიები, მათ შორის, მონაცემთა სუბიექტების მიერ გამოსაყენებელი უფლებები და სამართლებრივი დაცვის საშუალებები, უზრუნველყოფილი ხელშეკრულების სტანდარტული პირობებით, სავალდებულო კორპორაციული წესებით, ქცევის კოდექსებითა და სერტიფიცირების მექანიზმებით**	მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (2) (3) (5)(6)
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 46 (3)	**ხელშეკრულების პირობები და დებულებები, რომლებიც წარმოდგენილია საჯარო უწყებებს შორის გაფორმებულ ადმინისტრაციულ შეთანხმებებში და დამტკიცებულია უფლებამოსილი საზედამხედველო ორგანოს მიერ**	
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 46 (5)	**ავტორიზაცია 95/46 დირექტივის საფუძველზე**	
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 47	**შესასრულებლად სავალდებულო კორპორაციული წესები**	
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 49	**გამონაკლისები კონკრეტული გარემოებების შემთხვევაში**	მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (4)
მაგალითები: ევროკავშირი-აშშ-ის PNR შეთანხმება; ევროკავშირი-აშშ-ის SWIFT შეთანხმება.	**საერთაშორისო შეთანხმებები**	მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (3) (ა)

ევროკავშირის კანონმდებლობაში მონაცემთა დაცვის ზოგადი რეგულაცია ითვალისწინებს მონაცემთა თავისუფალ მიმოცვლას გაერთიანების ფარგლებში. თუმცა ასევე, შეიცავს კონკრეტულ მოთხოვნებს მონაცემების გადაცემაზე ევროკავშირის გარეთ, მესამე ქვეყნებისა და საერთაშორისო ორგანიზაციებისათვის. რეგულაცია აღიარებს ასეთი გადაცემის მნიშვნელობას, განსაკუთრებით, საერთაშორისო ვაჭრობისა და თანამშრომლობის გათვალისწინებით, თუმცა აღნიშნავს მომეტებულ რისკსაც პერსონალური მონაცემების მიმართ. შესაბამისად, რეგულაცია მიზნად ისახავს მესამე ქვეყნებისთვის გადაცემული პერსონალური მონაცემების ისეთივე დონეზე დაცვას, როგორიც მოქმედებს ევროკავშირში.[659] ევროპის საბჭოს სამართალში აღიარებულია მონაცემთა საერთაშორისო მიმოცვლის დამნერგავი წესების მნიშვნელობაც, მხარეებს შორის მონაცემთა თავისუფალი მიმოცვლისა და კონკრეტული წესების საფუძველზე. ეს წესები არეგულირებს მონაცემთა გადაცემას იმ სახელმწიფოებისათვის, რომლებიც კონვენციის მხარეები არ არიან.

7.1 პერსონალური მონაცემების გადაცემის სახე

ძირითადი საკითხები

- ევროკავშირისა და ევროპის საბჭოს კანონმდებლობაში მონაცემთა გადაცემა მესამე ქვეყნებისა ან საერთაშორისო ორგანიზაციებისთვის გარკვეული წესებით რეგულირდება.
- ევროკავშირის გარეთ მონაცემთა გადაცემისას მონაცემთა სუბიექტის უფლებების უზრუნველყოფა ნიშნავს, რომ ევროკავშირში წარმოქმნილ მონაცემებს თან სდევს მისი კანონმდებლობით გათვალისწინებული დაცვა.

ევროპის საბჭოს სამართალში მონაცემთა საერთაშორისო მიმოცვლა ნიშნავს პერსონალური მონაცემების გადაცემას იმ მიმღებთათვის, რომლებიც სხვა იურისდიქციას ექვემდებარებიან. [660] მონაცემთა საერთაშორისო მიმოცვლა მიმღებთან, რომელზეც ხელშემკვრელი სახელმწიფოს იურისდიქცია არ ვრცელდება, ნებადართულია მხოლოდ იმ შემთხვევაში, თუ მონაცემები დაცულია სათანადო დონეზე. [661]

659 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტები 101 და 116.

660 მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 102.

661 მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (2).

ევროკავშირის კანონმდებლობა არეგულირებს „დამუშავების პროცესში არსებული ან დამუშავებისთვის გამიზნული მონაცემების გადაცემას მესამე ქვეყნისთვის ან საერთაშორისო ორგანიზაციისთვის[...]“[662], რაც დაშვებულია მხოლოდ მაშინ, როცა დაცულია რეგულაციის მე-5 თავში წარმოდგენილი წესები.

მონაცემთა საერთაშორისო მიმოცვლა მიმღებთან, რომელიც ხელშემკვრელი სახელმწიფოს ან წევრი სახელმწიფოს იურისდიქციას ექვემდებარება, ნებადართულია, შესაბამისად, ევროპის საბჭოს ან ევროკავშირის კანონმდებლობით. ორივე სამართლებრივი სისტემა იძლევა მონაცემთა გადაცემის შესაძლებლობას ისეთი ქვეყნისთვის, რომელიც არ არის ხელშემკვრელი ან წევრი სახელმწიფო. ამ შემთხვევაში, საჭიროა გარკვეული პირობების დაცვა.

7.2 პერსონალურ მონაცემთა თავისუფალი მოძრაობა/მიმოცვლა წევრ ან ხელშემკვრელ სახელმწიფოებს შორის

ძირითადი საკითხები

- ევროკავშირში პერსონალური მონაცემების მიმოცვლა, ისევე, როგორც, გადაცემა მოდერნიზებული 108-ე კონვენციის ხელშემკვრელი სახელმწიფოებისთვის, შეზღუდვებს არ უნდა ექვემდებარებოდეს. თუმცა, მონაცემების გადაცემა წევრი სახელმწიფოდან მესამე ქვეყნისთვის ნებადართულია მხოლოდ იმ შემთხვევაში, თუ ეს უკანასკნელი აკმაყოფილებს GDPR-ით დადგენილ რეგულაციებს.

ევროპის საბჭოს კანონმდებლობით, მოდერნიზებული 108-ე კონვენციის ხელშემკვრელ მხარეებს შორის პერსონალური მონაცემები თავისუფლად უნდა იცვლებოდეს. თუმცა, ეს შეიძლება აიკრძალოს, როცა არსებობს „რეალური და სერიოზული საფრთხე, რომ მონაცემთა სხვა მხარისათვის გადაცემა გამოიწვევს კონვენციის დებულებების უგულებელყოფას“, ან გადაცემის აკრძალვა სავალდებულოა „დაცვის იმ ჰარმონიზებული წესებით, რომლებსაც იზიარებენ რეგიონული საერთაშორისო ორგანიზაციის წევრი სახელმწიფოები.“[663]

ევროკავშირის კანონმდებლობით, პერსონალური მონაცემების თავისუფალი მიმოცვლა გაერთიანების ფარგლებში არ უნდა შეიზღუდოს ან აიკრძალოს

662 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 44.

663 მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (1).

იმ მიზეზებით, რომლებიც უკავშირდება ფიზიკურ პირთა დაცვას პერსონალური მონაცემების დამუშავებისას.[664] მონაცემთა თავისუფალი მიმოცვლის სფერო გაფართოვდა შეთანხმებით ევროპული ეკონომიკური ზონის შესახებ (EEA),[665] რომლის თანახმადაც, შიდა ბაზარს ასევე განეკუთვნება ისლანდია, ლიხტენშტაინი და ნორვეგია.

მაგალითი: თუ რამდენიმე წევრ სახელმწიფოში (მათ შორის, სლოვენიასა და საფრანგეთში) შექმნილი კომპანიების საერთაშორისო ჯგუფთან აფილირებული პირი პერსონალურ მონაცემებს აგზავნის სლოვენიიდან და საფრანგეთიდან, სლოვენიის ეროვნული კანონმდებლობა არ უნდა ზღუდავდეს/კრძალავდეს მონაცემთა ასეთ მიმოცვლას პერსონალურ მონაცემთა დაცვის მიზეზებით.

თუ აღნიშნულ პირს სურს იმავე პერსონალური მონაცემების გადაგზავნა მალაიზიაში მდებარე „მშობელ კომპანიასთან“, მონაცემთა სლოვენიელმა ექსპორტიორმა უნდა გაითვალისწინოს რეგულაციის მე-5 თავში წარმოდგენილი წესები. აღნიშნული დებულებების მიზანია იმ მონაცემთა სუბიექტების პერსონალური მონაცემების დაცვა, რომლებიც ევროკავშირის იურისდიქციაში ექცევიან.

ევროკავშირის კანონმდებლობით, EEA-ს წევრ სახელმწიფოებთან პერსონალური მონაცემების მიმოცვლა ისეთი მიზნებით, როგორიცაა სისხლის სამართლის დანაშაულების პრევენცია, გამოძიება, გახსნა, დამნაშავეთა დასჯა ან სისხლისსამართლებრივი სასჯელის აღსრულება, 2016/680 დირექტივას ექვემდებარება.[666] ეს უზრუნველყოფს, რომ პერსონალური მონაცემების გაცვლა უფლებამოსილი ორგანოების მიერ ევროკავშირის ფარგლებში არ აიკრძალოს/შეიზღუდოს მონაცემთა დაცვასთან დაკავშირებული მიზეზებით. ევროპის საბჭოს კანონმდებლობით, პერსონალურ მონაცემთა დამუშავება (მათ შორის, საერთაშორისო მიმოცვლა 108-ე კონვენციის სხვა მხარეებთან),

664 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 1 (3).

665 საბჭოსა და კომისიის 1993 წლის 13 დეკემბრის გადაწყვეტილება ევროპული ეკონომიკური ზონის შესახებ შეთანხმების გაფორმებაზე, რომლის მხარეებიც არიან ევროპის თანამეგობრობა და მათი წევრი სახელმწიფოები, ასევე, ავსტრიის, ფინეთისა და ისლანდიის რესპუბლიკები, ლიხტენშტაინისა და შვედეთის სამეფოები, ნორვეგიის გაერთიანებული სამეფო, და შვეიცარიის კონფედერაცია, OJ 1994 L 1.

666 ევროპული პარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680 უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, რომელიც აუქმებს საბჭოს ჩარჩო გადაწყვეტილებას 2008/977/JHA (მონაცემთა დაცვა სამართალდამცველი და სასამართლო ორგანოებისათვის), OJ 2016 L 119.

მიზნებისა თუ მოქმედების სფეროს საფუძველზე დადგენილი გამონაკლისების გარეშე, 108-ე კონვენციის გამოყენების სფეროში ხვდება. თუმცა, ხელშემკვრელ სახელმწიფოებს უფლება აქვთ, დაადგინონ გარკვეული საგამონაკლისო შემთხვევები. EEA-ს წევრი ქვეყნები ასევე 108-ე კონვენციის მხარეები არიან.

7.3 პერსონალური მონაცემების გადაცემა მესამე ქვეყნებისა და საერთაშორისო ორგანიზაციებისთვის

ძირითადი საკითხები

- როგორც ევროპის საბჭო, ისე ევროკავშირი იძლევა პერსონალურ მონაცემთა გადაცემის შესაძლებლობას მესამე ქვეყნებისა ან საერთაშორისო ორგანიზაციებისთვის, თუკი დაკმაყოფილებულია მათი დაცვის გარკვეული პირობები:
  - ევროპის საბჭოს კანონმდებლობის თანახმად, დაცვის სათანადო დონე მიიღწევა სახელმწიფოს ან საერთაშორისო ორგანიზაციის კანონმდებლობით, ანდა სათანადო სტანდარტების არსებობით.
  - ევროკავშირის კანონმდებლობის თანახმად, მონაცემთა გადაცემა ნებადართულია, თუ მესამე ქვეყანაში ისინი სათანადოდ არის დაცული, ან მონაცემთა დამმუშავებელი თუ უფლებამოსილი პირი უზრუნველყოფს დაცვის სათანადო გარანტიებს, მათ შორის, მონაცემთა სუბიექტის აღსრულებად უფლებებსა და სამართლებრივი დაცვის საშუალებებს, მონაცემთა დაცვის სტანდარტული დებულებების ან შესასრულებლად სავალდებულო კორპორაციული წესების საფუძველზე.
- როგორც ევროკავშირის, ისე ევროპის საბჭოს სამართალში გათვალისწინებულია გამონაკლისი შემთხვევები, რომლებიც იძლევა მონაცემთა გადაცემის უფლებას გარკვეულ ვითარებაში, თუნდაც არ იყოს უზრუნველყოფილი სათანადო დაცვა ან უსაფრთხოების ზომები.

როგორც ევროპის საბჭოს, ისე ევროკავშირის კანონმდებლობა ითვალისწინებს მონაცემთა მიმოცვლას მესამე ქვეყნებსა ან საერთაშორისო ორგანიზაციებთან, თუმცა, განსხვავებული პირობების საფუძველზე. ეს პირობები ასახავს ორგანიზაციის სხვადასხვა სტრუქტურასა და მიზანს.

ევროკავშირის სამართალში პერსონალური მონაცემების გადაცემა მესამე ქვეყნებისა თუ საერთაშორისო ორგანიზაციებისთვის ნებადართულია ორი

გზით: (1) ევროკომისიის შესაბამისობის გადაწყვეტილების საფუძველზე,[667] ან (2) თუ დამმუშავებელი ან უფლებამოსილი პირი მონაცემთა სუბიექტისათვის უზრუნველყოფს უსაფრთხოების სათანადო ზომებს, მათ შორის, აღსრულებად უფლებებსა და სამართლებრივი დაცვის საშუალებებს.[668] ამ გადაწყვეტილებისა და უსაფრთხოების ზომების არარსებობის შემთხვევაში, დაშვებულია მხოლოდ რამდენიმე გამონაკლისი.

ევროპის საბჭოს სამართალში მონაცემების გადაცემა მესამე მხარისათვის ნებადართულია მხოლოდ მაშინ, როცა:

- შესაბამისი სახელმწიფოს ან საერთაშორისო ორგანიზაციის კანონმდებლობით, მათ შორის, საერთაშორისო ხელშეკრულებებით ან შეთანხმებებით, გარანტირებულია უსაფრთხოების სათანადო ზომები;

- მოქმედებს სპეციალურად ამ მიზნისთვის შექმნილი (ad hoc) ან დამტკიცებული სტანდარტული უსაფრთხოების ზომები, რომლებიც გათვალისწინებულია სავალდებულო იურიდიული ძალის მქონე და აღსრულებადი ინსტრუმენტებით, ეს ინსტრუმენტები კი დამტკიცებული და დანერგილია მონაცემთა გადაცემასა და შემდგომ დამუშავებაში მონაწილე პირების მიერ.[669]

  ევროკავშირის კანონმდებლობის მსგავსად, ამ შემთხვევაშიც დაშვებულია გარკვეული გამონაკლისები, თუკი მონაცემები სათანადო დონეზე არ არის დაცული.

7.3.1 მონაცემთა გადაცემა შესაბამისობის გადაწყვეტილების საფუძველზე

ევროკავშირის კანონმდებლობით, პერსონალური მონაცემების თავისუფალ მიმოცვლას მესამე ქვეყნებთან, სადაც მონაცემები დაცულია სათანადო დონეზე, ითვალისწინებს GDPR-ის 45-ე მუხლი. CJEU-ს განმარტებით, ტერმინი „დაცვის სათანადო დონე“ მოითხოვს, რომ მესამე ქვეყანაში ფუნდამენტური უფლებები და თავისუფლებები დაცული იყოს ისეთი დონეზე, რომელიც „არსებითად შეესაბამება[670] ევროკავშირის კანონმდებლობით გათვალისწინებულ გარანტიებს. ამავდროულად, საშუალებები, რომლებსაც მესამე ქვეყნები

667 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 45.

668 *იქვე*, მუხლი 46.

669 მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (3)(ა)(ბ).

670 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი, პუნქტი 96.

უნდა იყენებდნენ დაცვის ამ დონის უზრუნველსაყოფად, შესაძლოა განსხვავდებოდეს ევროკავშირში მოქმედი საშუალებებისგან. შესაბამისობის სტანდარტი არ მოითხოვს ევროკავშირის წესების ზედმიწევნით გამეორებას.[671]

სხვადასხვა ქვეყანაში მონაცემთა დაცვის დონე დგინდება შიდასახელმწიფოებრივი კანონმდებლობისა და შესაბამისი საერთაშორისო ვალდებულებების შეფასებით. კომისია ითვალისწინებს ქვეყნის მონაწილეობას პერსონალურ მონაცეთა დაცვის მრავალმხრივ ან რეგიონულ სისტემებში. თუ ევროკომისია დაადგენს, რომ მესამე ქვეყანა ან საერთაშორისო ორგანიზაცია უზრუნველყოფს დაცვის სათანადო დონეს, მას შეუძლია მიიღოს გადაწყვეტილება შესაბამისობაზე, რომელსაც სავალდებულო ძალა აქვს.[672] ამავდროულად, CJEU-ს განმარტებით, ეროვნული საზედამხედველო ორგანოები ინარჩუნებენ უფლებამოსილებას, რომ განიხილონ პირის საჩივარი მესამე ქვეყნისთვის გადაცემული პერსონალური მონაცემების დაცვაზე, სადაც, კომისიის გადაწყვეტილების თანახმად, დაცვის სათანადო დონე მოქმედებს. საჩივარში პირს უფლება აქვს, მიუთითოს, რომ შესაბამის ქვეყანაში არსებული კანონმდებლობა და პრაქტიკა არ უზრუნველყოფს დაცვის ასეთ დონეს.[673]

ევროკომისიას შეუძლია, შესაბამისობა შეაფასოს მესამე ქვეყნის რომელიმე ტერიტორიაზე ან კონკრეტულ სექტორში, როგორც, მაგალითად, კანადის კერძო სავაჭრო კანონმდებლობის შემთხვევაში.[674] არსებობს დასკვნებიც შესაბამისობაზე, რომლებიც შეეხება მონაცემთა გადაცემას ევროკავშირსა და მესამე ქვეყნებს შორის მოქმედი შეთანხმების საფუძველზე. ეს გადაწყვეტილებები მოიცავს მონაცემთა გადაცემის მხოლოდ და მხოლოდ ერთ რომელიმე სახეს (მაგ.: ავიაკომპანიის მიერ მგზავრთა პირადი მონაცემების (PNR) გადაცემა საზღვრის დაცვის ორგანოებისთვის, როდესაც ევროკავშირიდან ხორციელდება საერთაშორისო ფრენა გარკვეულ ქვეყნებში (იხ. ნაწილი 7.3.4).

შესაბამისობის გადაწყვეტილება ექვემდებარება მუდმივ მონიტორინგს. ევროკომისია რეგულარულად გადახედავს ასეთ გადაწყვეტილებებს და

671 *იქვე,* პუნქტი 74. ასევე, იხ: ევროპული კომისია (2017), კომისიის მიმართვა ევროპულ პარლამენტსა და საბჭოს „გლობალიზებულ სამყაროში პერსონალურ მონაცემთა გაცვლისა და დაცვის შესახებ", COM(2017)7 2017 წლის 10 იანვარი, გვ. 6.

672 განახლებული ჩამონათვალი ქვეყნებისა, რომლებთან მიმართებითაც ევროპულმა კომისიამ შესაბამისობის გადაწყვეტილება მიიღო, ხელმისაწვდომია ევროკომისიის მართლმსაჯულების გენერალური დირექტორატის ვებგვერდზე.

673 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი, პუნქტები 63 და 65– 66.

674 ევროკომისია (2002), 2001 წლის 20 დეკემბრის გადაწყვეტილება 2002/2/EC, რომელიც მიღებულია ევროპარლამენტისა და საბჭოს დირექტივის 95/46/EC შესაბამისად, კანადის პერსონალური ინფორმაციის დაცვისა და ელექტრონული დოკუმენტების შესახებ აქტით უზრუნველყოფილი პერსონალურ მონაცემთა სათანადო დაცვის შესახებ, OJ 2002 L 2.

აკვირდება მოვლენებს, რომლებაც შეიძლება გავლენა იქონიოს გადაწყვეტილების სტატუსზე. ამრიგად, თუ კომისია დაადგენს, რომ მესამე ქვეყანა ან საერთაშორისო ორგანიზაცია ვეღარ აკმაყოფილებს პირობებს, რომელთა საფუძველზეც მიღებულია შესაბამისობის გადაწყვეტილება, უფლება აქვს, შეასწოროს, შეაჩეროს, ან გააუქმოს ეს გადაწყვეტილება; ასევე, მოლაპარაკებები აწარმოოს მესამე ქვეყანასა ან საერთაშორისო ორგანიზაციასთან პრობლემური საკითხის მოსაგვარებლად.

შესაბამისობის გადაწყვეტილება, რომელსაც ევროპული კომისია იღებს 95/46/EC დირექტივის საფუძველზე, ძალაშია მანამ, სანამ არ შესწორდება, ჩანაცვლდება ან გაუქმება მის მიერ GDPR-ის 45-ე მუხლით დადგენილი წესების საფუძველზე მიღებული გადაწყვეტილებით.

დღესდღეობით, ევროკომისიის გადაწყვეტილებით, პერსონალური მონაცემების სათანადო დაცვა მოქმედებს შემდეგ ქვეყნებში: ანდორა, არგენტინა, კანადა (კომერციული ორგანიზაციები, რომლებზეც ვრცელდება აქტი პერსონალური ინფორმაციისა და ელექტრონული დოკუმენტების შესახებ - PIPEDA), ფარერის კუნძულები, გერნსი, მენის კუნძული, ისრაელი, ჯერსი, ახალი ზელანდია, შვეიცარია და ურუგვაი. რაც შეეხება მონაცემთა გადაცემას აშშ-სთვის, ევროპულმა კომისიამ 2000 წელს მიიღო შესაბამისობის გადაწყვეტილება, რომლითაც ნებადართული იყო ევროკავშირიდან პერსონალური მონაცემების გადაცემა იმ კომპანიებისათვის, რომლებიც ადასტურებდნენ, რომ იცავდნენ ასეთ მონაცემებს და მოქმედებდნენ დაცვის საშუალებათა პრინციპების (Safe Harbous principles) შესაბამისად.[675] CJEU-მ ეს გადაწყვეტილება ძალადაკარგულად გამოაცხადა 2015 წელს, 2016 წლის ივლისში კი მიიღო შესაბამისობის ახალი გადაწყვეტილება, რომელზე მიერთებაც კომპანიებს შეუძლიათ 2016 წლის 1 აგვისტოდან.

მაგალითი: *Schrems-ის საქმეში*[676] განმცხადებელი გახლდათ მაქსიმილიან შრემსი, ავსტრიის მოქალაქე, Facebook-ის დიდი ხნის მომხმარებელი. ბ-ნი შრემსის მიერ მიწოდებული მონაცემების ნაწილი Facebook-ის შვილობილმა კომპანიამ ირლანდიაში გადასცა აშშ-ში მდებარე სერვერებს, სადაც ისინი დამუშავდა. ბატონმა შრემსმა ირლანდიის მონაცემთა დაცვის ორგანოში შეიტანა საჩივარი, რომელშიც აცხადებდა, რომ ედვარდ სნოუდენის სკანდალის შედეგად აშშ-ს სადაზვერვო სამსახურებზე

675 კომისიის 2000 წლის 26 ივლისის გადაწყვეტილება 2000/520/EC ევროპარლამენტისა და საბჭოს 95/46/EC დირექტივის თანახმად, Safe Harbour-ის პრინციპებით გათვალისწინებული დაცვის ადეკვატურობისა და მასთან დაკავშირებული ხშირად დასმული კითხვების შესახებ, რომელიც მოამზადა აშშ-ს სავაჭრო დეპარტამენტმა, OJ L 215. გადაწყვეტილება CJEU-მ ძალადაკარგულად გამოაცხადა საქმეში C-632/14, *Maximilian Schrems v. Data Protection Commissioner* [GC].

676 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი.

გამოაშკარავებული ინფორმაციის გათვალისწინებით, აშშ-ს კანონმდებლობა და პრაქტიკა არ ითვალისწინებდა მისთვის გადაცემული პერსონალური მონაცემების საკმარის დაცვას. ირლანდიის საზედამხედველო ორგანომ უარი თქვა საჩივრის დაკმაყოფილებაზე, იმ მოტივით, რომ 2000 წლის 29 ივლისს კომისიის მიერ მიღებული გადაწყვეტილების თანახმად, დაცვის საშუალებათა სქემის (Safe Harbour scheme) საფუძველზე, აშშ სათანადოდ იცავს გადაცემულ პერსონალურ მონაცემებს. მოსარჩელემ გადაწყვეტილება გაასაჩივრა ირლანდიის უზენაეს სასამართლოში, ამ უკანასკნელმა კი, წინასწარი განჩინების გამოტანის თხოვნით, CJEU-ს მიმართა.

CJEU-მ დაადგინა, რომ კომისიის გადაწყვეტილება დაცვის საშუალებათა (Safe Harbour) სქემის შესახებ ძალადაკარგული იყო. პირველ რიგში, CJEU-მ აღნიშნა, რომ გადაწყვტილება იძლეოდა დაცვის საშუალებათა (Safe Harbour) პრინციპების გამოყენებაზე შეზღუდვის დაწესების საშუალებას, ეროვნული უსაფრთხოების, საჯარო ინტერესისა თუ სამართლის დაცვის მოთხოვნათა მოტივით, ან აშშ-ს შიდასახელმწიფოებრივი კანონმდებლობის საფუძველზე. ამრიგად, გადაწყვეტილება იძლეოდა იმ პირების ფუნდამენტურ უფლებებში ჩარევის საშუალებას, ვისი პერსონალური მონაცემებიც გადაეცა ან გადაცემოდა აშშ-ს.[677] სასამართლომ ასევე განმარტა, რომ გადაწყვეტილება არ შეიცავდა რაიმე დასკვნას აშშ-ში ასეთი ჩარევის შემზღუდველი წესების ან შესაბამისი სამართლებრივი დაცვის ეფექტიანი საშუალებების არსებობაზე.[678] CJEU-მ ხაზგასმით აღნიშნა, რომ იმ ფუნდამენტური უფლებებისა და თავისუფლებების დაცვის დონე, რომლებიც გარანტირებულია ევროკავშირის მასშტაბით, მოითხოვდა რომ: კანონმდებლობა, რომელიც ითვალისწინებს მე-7 და მე-8 მუხლებით დაცულ სფეროებში ჩარევას, უნდა ადგენდეს მკაფიო და ზუსტ წესებს ღონისძიების მოქმედების სფეროსა და გამოყენებაზე და აწესებდეს დაცვის მინიმალურ გარანტიებს, გამონაკლის შემთხვევებსა და შეზღუდვებს პერსონალური მონაცემების დაცვის კუთხით.[679] ვინაიდან კომისიის გადაწყვეტილებაში არ იყო მითითებული, რომ აშშ რეალურად უზრუნველყოფს დაცვის ასეთ დონეს შიდასახელმწიფოებრივი კანონმდებლობით ან საერთაშორისო ვალდებულებებით, CJEU-მ დაასკვნა, რომ იგი ვერ აკმაყოფილებდა მონაცემთა დაცვის დირექტივის მოთხოვნებს პერსონალური ინფორმაციის გადაცემასთან დაკავშირებით და ამის გამო გადაწყვეტილება ძალადაკარგული იყო.[680]

677 *იქვე,* პუნქტი 84.

678 *იქვე,* პუნქტები 88–89.

679 *იქვე,* პუნქტები 91–92.

680 *იქვე,* პუნქტები 96–97.

ამრიგად, აშშ-ში არსებული დაცვის დონე არ იყო ისეთი, როგორიცა „არსებითად შეესაბამებოდა“ ევროკავშირში გარანტირებულ ფუნდამენტურ უფლებებსა და თავისუფლებებს.[681] CJEU-მ დაადგინა ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის სხვადასხვა მუხლის დარღვევა. პირველ რიგში, ზიანი ადგებოდა მე-7 მუხლის არსს, რადგან აშშ-ს კანონმდებლობა „საჯარო ხელისუფლების წარმომადგენლებს ნებას რთავდა, ჰქონოდათ წვდომა ელექტრონული კომუნიკაციების შინაარსზე, ზოგადი საფუძვლით;“ მეორე: ზიანდებოდა 47-ე მუხლის არსიც, რადგან კანონმდებლობა მონაცემთა სუბიექტებისათვის არ ითვალისწინებდა სამართლებრივი დაცვის საშუალებებს პერსონალური მონაცემების წვდომასთან, გასწორებასა ან წაშლასთან დაკავშირებით. და ბოლოს, დაცვის საშუალებათა სისტემის (Safe Harbour arrangement) მიერ ზემოაღნიშნული მუხლების დარღვევა გამორიცხავდა პერსონალურ მონაცემთა კანონიერ დამუშავებას, რამაც გამოიწვია მე-8 მუხლის დარღვევა.

მას შემდეგ, რაც CJEU-მ დაცვის საშუალებათა სისტემა ბათილად გამოაცხადა (Safe Harbour arrangement), ევროკომისია და აშშ შეთანხმდნენ პირადი ცხოვრების ხელშეუხებლობის დაცვის ახალ სისტემაზე - EU-US Privacy Shield. 2016 წლის 12 ივლისს მიღებულ გადაწყვეტილებაში ევროკომისიამ განაცხადა, რომ პირადი ცხოვრების დამცავი ამ სისტემის საფუძველზე (Privacy Shield),[682] აშშ სათანადო დონეზე იცავს ევროკავშირიდან აშშ-ში გადაცემულ პერსონალურ მონაცემებს.

მსგავსად დაცვის საშუალებათა (Safe Harbour) სისტემისა, ევროკავშირსა და აშშ-ს შორის მოქმედი პირადი ცხოვრების დამცავი სისტემა (Privacy Shield) მიზნად ისახავს იმ პერსონალური მონაცემების დაცვას, რომლებიც აშშ-ს ევროკავშირიდან გადაეცემა კომერციული მიზნებით.[683] ამერიკულ კომპანიებს შეუძლიათ თვითსერტიფიცირება და პირადი ცხოვრების დამცავი სისტემის

681 *იქვე,* პუნქტები 73–74 და 96.

682 კომისიის 2016 წლის 12 ივლისის *გადაწყვეტილება (EU) 2016/1250,* რომელიც შეეხება ევროპარლამენტისა და საბჭოს 95/46/EC დირექტივის შესაბამისად, ევროკავშირი-აშშ-ს პირადი ცხოვრების დამცავი სისტემით (EU-U.S. Privacy Shield) უზრუნველყოფილი დაცვის ადეკვატურობას, OJ L 207. 29-ე მუხლის სამუშაო ჯგუფი მიესალმა Privacy Shield-ის გაუმჯობესებულ მექანიზმებს (Safe Harbour-ის გადაწყვეტილებასთან შედარებით) და კომისია და აშშ-ს ხელისუფლება შეაქო იმის გამო, რომ Privacy Shield-ის საბოლოო დოკუმენტებში გაითვალისწინეს სამუშაო ჯგუფის WP238 მოსაზრებაში გამოთქმული შენიშვნები შესაბამისობის გადაწყვეტილებაზე. ამავდროულად, საბჭომ რამდენიმე პრობლემას გაუსვა ხაზი. დამატებითი ინფორმაციისათვის, იხ. 29-ე მუხლის სამუშაო ჯგუფის მოსაზრება Privacy Shiled-ის შესაბამისობის გადაწყვეტილების პროექტზე (მიღებულია 2016 წლის 13 აპრილს, 16/EN WP 238).

683 დამატებითი ინფორმაციისათვის, იხ: EU-U.S. Privacy Shield-ის შესახებ ფაქტობრივი ინფორმაცია.

(Privacy Shield) მოთხოვნათა ნებაყოფლობით შესრულება. აშშ-ს უფლებამოსილი ორგანოები მონიტორინგს გაუწევენ ამ სტანდარტების დაკმაყოფილებას სერტიფიცირებული კომპანიების მიერ.

უფრო კონკრეტულად, პირადი ცხოვრების დამცავი სისტემა (Privacy Shield) ითვალისწინებს შემდეგ საკითხებს:

- მონაცემთა დაცვის ვალდებულებები იმ კომპანიებისთვის, რომლებიც ევროკავშირიდან იღებენ მონაცემებს;
- დაცვა და ზარალის ანაზღაურება ფიზიკური პირებისთვის. კერძოდ, აშშ-ს სადაზვერვო სამსახურებისგან დამოუკიდებელი ომბუდსმენის მექანიზმის შექმნა. აღნიშნული მექანიზმი განიხილავს იმ პირთა საჩივრებს, რომლებიც მიიჩნევენ, რომ მათი პერსონალური მონაცემები უკანონოდ გამოიყენეს აშშ-ს ეროვნული უსაფრთხოების უწყებებმა;
- ყოველწლიური ერთობლივი შეფასება პირადი ცხოვრების დამცავი სისტემის დანერგვაზე მონიტორინგისათვის; [684] პირველი შეფასება 2017 წლის სექტემბერში განხორციელდა. [685]

აშშ-ს მთავრობამ წერილობითი სახით შეიმუშავა გარკვეული ვალდებულებები და გარანტიები, რომლებიც პირადი ცხოვრების დამცავ სისტემას (Privacy Shield) ახლავს. ეს ითვალისწინებს შეზღუდვებსა და უსაფრთხოების ზომებს აშშ-ს მთავრობის მხრიდან პერსონალური მონაცემების წვდომაზე სამართალდამცველი და ეროვნული უსაფრთხოების მიზნებით.

7.3.2 პერსონალურ მონაცემთა გადაცემა უსაფრთხოების სათანადო ზომების საფუძველზე

მონაცემთა საჭირო დონეზე დასაცავად, როგორც ევროკავშირის, ისე ევროპის საბჭოს კანონმდებლობა ითვალისწინებს უსაფრთხოების სათანადო ზომებს დამმუშავებელსა და მონაცემთა მიმღებს შორის (მესამე ქვეყანა ან საერთაშორისო ორგანიზაცია).

ევროკავშირის კანონმდებლობით, პერსონალური მონაცემების გადაცემა მე-

684 დამატებითი ინფორმაციისათვის, იხ: ევროკომისიის ვებგვერდი EU-U.S. Privacy Shield-ის შესახებ.

685 ევროკომისიის ანგარიში ევროპარლამენტისა და საბჭოსთვის, ევროკავშირი-აშშ-ს პირადი ცხოვრების დამცავი სისტემის (Privacy Shield) ფუნქციონირების პირველ ყოველწლიურ შეფასებაზე, COM(2017) 611 2017 წლის 18 ოქტომბერი.

სამე ქვეყნის ან საერთაშორისო ორგანიზაციისთვის დასაშვებია, თუ დამმუშავებელი ან უფლებამოსილი პირი მიიღებენ უსაფრთხოების სათანადო ზომებს, ასევე, მონაცემთა სუბიექტებისთვის უზრუნველყოფენ გამოყენებად უფლებებსა და სამართლებრივი დაცვის ეფექტიან საშუალებებს.[686] უსაფრთხოების სათანადო ზომები წარმოდგენილია ევროკავშირის მონაცემთა დაცვის კანონმდებლობაში და მათი გატარება შესაძლებელია შემდეგი საშუალებებით:

- იურიდიულად სავალდებულო ძალის მქონე და აღსრულებადი ინსტრუმენტები სახელმწიფო უწყებებსა თუ ორგანოებს შორის;
- სავალდებულო ძალის მქონე კორპორაციული წესები;
- მონაცემთა დაცვის სტანდარტული დებულებები, დამტკიცებული ევროკომისიის ან საზედამხედველო ორგანოს მიერ;
- ქცევის კოდექსი;
- სერტიფიცირების მექანიზმები.[687]

უსაფრთხოების სათანადო ზომების უზრუნველყოფა ასევე შესაძლებელია ინდივიდუალური სახელშეკრულებო პირობებით, რომლებიც მოქმედებს, ერთი მხრივ, ევროკავშირში არსებულ მონაცემთა დამმუშავებელსა თუ უფლებამოსილ პირს და, მეორე მხრივ, მესამე ქვეყანის მონაცემთა მიმღებს შორის. ამავდროულად, ამ პირობების გამოყენებამდე, პერსონალური მონაცემების გადაცემა ნებადართული უნდა იყოს კომპეტენტური საზედამხედველო ორგანოს მიერ. მსგავსად, ადმინისტრაციულ შეთანხმებებში არსებული მონაცემთა დაცვის დებულებების გამოყენება შეუძლიათ სახელმწიფო ორგანოებსაც, საზედამხედველო ორგანოს მხრიდან ავტორიზების შემდეგ.[688]

ევროპის საბჭოს კანონმდებლობის თანახმად, მონაცემთა მიმოცვლა ისეთ სახელმწიფოსა ან საერთაშორისო ორგანიზაციასთან, რომელიც მოდერნიზებული 108-ე კონვენციის მხარე არ არის, ნებადართულია, როცა დაცვა უზრუნველყოფილია სათანადო დონეზე. ამის მიღწევა შესაძლებელია:

- სახელმწიფოს ან საერთაშორისო ორგანიზაციის კანონმდებლობით;
- სპეციალურად ამ მიზნით შექმნილი (ad hoc) ან სტანდარტიზებული უსაფრთხოების სათანადო ზომებით, რომლებიც წარმოდგენილია იურიდიუ-

686 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 46.

687 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები: 46 (1)(გ)(დ), (2)(ა)(ბ)(ე)(ვ) და 47.

688 *იქვე*, მუხლი 46 (3).

ლად სავალდებულო ძალის მქონე დოკუმენტში.[689]

მონაცემთა გადაცემა სახელშეკრულებო პირობების საფუძველზე

როგორც ევროპის საბჭოს, ისე ევროკავშირის კანონმდებლობაში სახელშეკრულებო პირობები მონაცემთა დამმუშავებელსა და მესამე ქვეყანაში არსებულ მონაცემთა მიმღებს შორის აღიარებულია, როგორც მონაცემთა სათანადო დონეზე დაცვის საშუალება.[690]

ევროპულმა კომისიამ, 29-ე მუხლის სამუშაო ჯგუფის დახმარებით, ევროკავშირის დონეზე შექმნა მონაცემთა დაცვის სტანდარტული პირობები, რომლებიც, კომისიის გადაწყვეტილებით, ოფიციალურად დამოწმდა, როგორც მონაცემთა სათანადო დაცვის მტკიცებულება.[691] რადგან კომისიის გადაწყვეტილებები წევრი სახელმწიფოებისათვის სავალდებულოდ შესასრულებელია, სახელმწიფო უწყებები, რომლებიც მონაცემთა გადაცემას ზედამხედველობენ, ვალდებულნი არიან, თავიანთ პროცედურებში გაითვალისწინონ სტანდარტული სახელშეკრულებო პირობები.[692] ამრიგად, თუ მონაცემთა დამმუშავებელი (რომელიც ახორციელებს მონაცემთა ექსპორტს) და მესამე ქვეყანა თანხმდებიან და ხელს აწერენ აღნიშნულ პირობებს, საზედამხედველო ორგანოს ექნება მონაცემთა უსაფრთხოების სათანადო ზომების არსებობის საკმარისი მტკიცებულება. ამავდროულად, *Shrems*-ის საქმეში CJEU-მ დაადგინა, რომ ევროპული კომისია არ არის უფლებამოსილი, შეზღუდოს ეროვნულ საზედამხედველო ორგანოთა უფლებამოსილება პერსონალური მონაცემების მესამე ქვეყნისთვის გადაცემის გასაკონტროლებლად, რომლის შესახებაც კომისიას მიღებული აქვს შესაბამისობის გადაწყვეტილება.[693] ამრიგად, ეროვნულ საზედამხედველო ორგანოებს კვლავ შეეძლებათ პერსონალური მონაცემების გადაცემის შეჩერება ან აკრძალვა, თუკი ის ხორციელდება ევროკავშირის ან მონაცემთა დაცვის ეროვნული კანონმდებლობის დარღვევით (მაგ.:მონაცემების მიმღები პატივს არ სცემს სტანდარტულ სახელშეკრულებო პირობებს).[694]

---

689 მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (3) (ბ).

690 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 46 (3); მოდერნიზებული 108-ე კონვენცია, მუხლი 14(3)(b).

691 *იქვე,* მუხლები 46 (2) (ბ) და 46 (5).

692 *იქვე,* მუხლი 46 (2)(გ).

693 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი, პუნქტები 96–98 და 102–105.

694 Shrems-ის საქმეში CJEU-ს პოზიციის გასათვალისწინებლად, კომისიამ შეასწორა გადაწყვეტილება სტანდარტული სახელშეკრულებო პირობების შესახებ. კომისიის 2016 წლის 16 დეკემბრის იმპლემენტაციის გადაწყვეტილება (EU) 2016/2297, რომლითაც შესწორდა გადაწყვეტილებები 2001/497/EC და 2010/87/EU სტანდარტული სახელშეკრულებო პირობების შესახებ, რომლებიც მიემართება მესამე ქვეყნებისა და ასეთ ქვეყნებში შექმნილი უფლებამოსილი პირებისათვის პერსონალური მონაცემების გადაცემას, ევროპარლამენტისა და საბჭოს დირექტივის 95/46/EC, OJ 2016 L344 საფუძველზე.

ევროკავშირის სამართლებრივ ჩარჩოში მონაცემთა დაცვის სტანდარტული პირობების არსებობა დამმუშავებელს არ უშლის ხელს სხვა სპეციალური (ad hoc), ინდივიდუალური სახელშეკრულებო პირობების ფორმულირებაში, რომლებიც უნდა მიიღოს საზედამხედველო ორგანომ.[695] თუმცა, ეს პირობები უნდა უზრუნველყოფდეს მონაცემთა დაცვის იმავე დონეს, რომელიც განსაზღვრულია სტანდარტულად. სპეციალური (ad hoc) პირობების მიღებისას, საზედამხედველო ორგანოები ვალდებულნი არიან, გამოიყენონ თანმიმდევრულობის მექანიზმი, რომელიც უზრუნველყოფს ერთიანი მარეგულირებელი მიდგომის არსებობას ევროკავშირის მასშტაბით.[696] ეს ნიშნავს, რომ კომპეტენტურმა საზედამხედველო ორგანომ საკუთარი გადაწყვეტილების პროექტი სახელშეკრულებო პირობებთან დაკავშირებით EDPB-ის უნდა წარუდგინოს. EDPB, თავის მხრივ, მოამზადებს შესაბამის მოსაზრებას, რომელიც საზედამხედველო ორგანომ მაქსიმალურად უნდა გაითვალისწინოს გადაწყვეტილების მიღებისას. წინააღმდეგ შემთხვევაში, ამოქმედდება EDPB-ის დავების გადაწყვეტის მექანიზმი და საბჭო მიიღებს სავალდებულო ძალის მქონე გადაწყვეტილებას.[697]

სტანდარტული სახელშეკრულებო პირობის მნიშვნელოვანი ასპექტებია:

- პირობა მიმღები მესამე პირის შესახებ, რომელიც მონაცემთა სუბიექტს საშუალებას აძლევს, ისარგებლოს სახელშეკრულებო უფლებებით, მიუხედავად იმისა, რომ არ არის ხელშეკრულების მხარე;

- მონაცემთა მიმღები (იმპორტიორი) თანახმაა, დაექვემდებაროს მონაცემთა დამმუშავებლის (ექსპორტიორის) ეროვნულ საზედამხედველო ორგანოს და/ან სასამართლოს, დავის წარმოშობის შემთხვევაში.

ერთი დამმუშავებლიდან მეორესთვის მონაცემთა გადაცემაზე ვრცელდება ორი სხვადასხვა კატეგორიის სტანდარტული პირობები, საიდანაც მონაცემთა გადამცემი მხარე ირჩევს ერთ-ერთს.[698] როდესაც დამმუშავებელი მონაცემებს გადასცემს უფლებამოსილ პირს, მხოლოდ ერთი კატეგორიის სტანდარტული

695 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 46 (3) (ა).

696 *იქვე,* მუხლი 63 და მუხლი 64 (1) (ე).

697 *იქვე,* მუხლი 64 და მუხლი 65.

698 პირველი ვარიანტი მოცემულია ევროპული კომისიის 2001 წლის 15 ივნისის გადაწყვეტილების 2001/497/EC დანართით მესამე ქვეყნებისთვის პერსონალურ მონაცემთა გადაცემის სტანდარტული სახელშეკრულებო პირობების შესახებ, 95/46/EC დირექტივის საფუძველზე, OJ 2001 L 181; მეორე ვარიანტი მოცემულია ევროპული კომისიის 2004 წლის 27 დეკემბრის 2004/915/EC გადაწყვეტილების დანართით, რომელიც ცვლის 2001/497/EC გადაწყვეტილებას და ეხება ალტერნატიული სახელშეკრულებო პირობების სტანდარტს პერსონალურ მონაცემთა გადაცემისთვის მესამე ქვეყნებში, OJ 2004 L 385.

პირობები ვრცელდება.[699] თუმცა, ამ სტანდარტულ სახელშეკრულებო პირობებთან დაკავშირებით ამჟამად სამართლებრივი პროცესი მიმდინარეობს.

მაგალითი: მას შემდეგ, რაც CJEU-მ გადაწყვეტილება დაცვის საშუალებების შესახებ (Safe Harbour Decision) ძალადაკარგულად გამოაცხადა,[700] აშშ-სთვის პერსონალური მონაცემების გადაცემა შესაბამისობის გადაწყვეტილებას ვეღარ დაეფუძნებოდა. აშშ-ს ხელისუფლებასთან მიმდინარე მოლაპარაკებებისა და შესაბამისობის ახალ გადაწყვეტილებაზე მუშაობის დროს (საბოლოო გადაწყვეტილება მიღებულია 2016 წლის 12 ივლისს),[701] მონაცემთა გადაცემა შესაძლებელი იყო სხვა სამართლებრივ საფუძველზე დაყრდნობით, როგორიცაა სტანდარტული სახელშეკრულებო პირობები ან სავალდებულო ძალის მქონე კორპორაციული წესები. რამდენიმე კომპანიამ, მათ შორის, Facebook-ის ოფისმა ირლანდიაში (რომლის წინააღმდეგაც შეტანილია საჩივარი დაცვის საშუალებათა შესახებ გადაწყვეტილების გაუქმების მოთხოვნით), მონაცემთა გადაცემა განაგრძო სტანდარტული სახელშეკრულებო პირობების საფუძველზე.

ბ-ნმა შრემსმა ირლანდიის საზედამხედველო ორგანოს მიმართა საჩივრით და მოითხოვა, შეეწყვიტათ აშშ-სთვის მონაცემთა გადაცემა სტანდარტული სახელშეკრულებო პირობების საფუძველზე. მისი თქმით, ირლანდიაში მდებარე Facebook-ის შვილობილი კომპანიიდან მისი პერსონალური მონაცემების Facebook Inc.-ისა და აშშ-ში მდებარე სერვერებისათვის გადაცემის შემთხვევაში, არ არსებობდა გარანტია, რომ ეს მონაცემები იქნებოდა დაცული. Facebook Inc.-ზე ვრცელდება აშშ-ს კანონმდებლობა, რომლის საფუძველზეც შესაძლოა აღნიშნულ კომპანიას დაეკისროს პერსონალური მონაცემების გამჟღავნების ვალდებულება (აშშ-ს სამართალდამცველი ორგანოებისათვის), ხოლო ამ პრაქტიკის გასაჩივრებისთვის, სამართლებრივი დაცვის საშუალებაზე ევროპის მოქა-

699 ევროპული კომისია (2010), 2010 წლის 5 თებერვლის გადაწყვეტილება 2010/87 პერსონალურ მონაცემთა გადაცემისთვის დადგენილი სტანდარტული სახელშეკრულებო პირობების შესახებ, მესამე ქვეყნებში დაფუძნებული უფლებამოსილი პირებისთვის ევროპული პარლამენტისა და საბჭოს 95/46/EC დირექტივის მიხედვით, OJ 2010 L 39. წინამდებარე სახელმძღვანელოს შედგენის დროს, სტანდარტული სახელშეკრულებო დებულებების გამოყენება აშშ-სთვის პერსონალური მონაცემების გადასაცემად განიხილებოდა ირლანდიაში მიმდინარე სამართალწარმოების ფარგლებში. High Court.

700 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი.

701 2016 წლის 12 ივლისის იმპლემენტაციის გადაწყვეტილება (EU) 2016/1250, რომელიც შეეხება ევროპარლამენტისა და საბჭოს 95/46/EC დირექტივის შესაბამისად, ევროკავშირი-აშშ-ს პირადი ცხოვრების დამცავი სისტემით (EU-U.S. Privacy Shield) უზრუნველყოფილ დაცვის ადეკვატურობას, OJ L 207.

ლაქეებს ხელი არ მიუწვდებათ.[702] აღნიშნული მიზნების გამო, CJEU-მ გადაწყვეტილება დაცვის საშუალებების შესახებ (Safe Harbour Decision) ძალადაკარგულად გამოაცხადა. მიუხედავად იმისა, რომ სასამართლოს ეს გადაწყვეტილება შეეხებოდა მხოლოდ დაცვის საშუალებებს, განმცხადებელმა განაცხადა, რომ CJEU-ს მიერ წამოჭრილი საკითხები ასევე მოიცავდა მონაცემთა გადაცემას სახელშეკრულებო პირობების საფუძველზე. წინამდებარე სახელმძღვანელოს მომზადებისას, საქმეს ირლანდიის უზენაესი სასამართლო განიხილავდა. განმცხადებელი აპირებს, რომ მიმართოს ევროპის მართლმსაჯულების სასამართლოს და მოითხოვოს ევროპული კომისიის იმ გადაწყვეტილების გაუქმება, რომელიც სტანდარტულ სახელშეკრულებო პირობებს ეხება. როგორც აღინიშნა მე-5 თავში, მხოლოდ CJEU-ს აქვს ევროკავშირის ინსტრუმენტის ძალადაკარგულად გამოცხადების უფლებამოსილება.

მონაცემთა გადაცემა სავალდებულო ძალის მქონე კორპორაციული წესების საფუძველზე

ევროკავშირის კანონმდებლობაში მონაცემთა საერთაშორისო გადაცემა დაშვებულია სავალდებულო ძალის მქონე კორპორაციული წესების საფუძველზე, თუკი გადაცემა ხდება იმ დაწესებულებათა ერთი ჯგუფის ფარგლებში, რომლებიც საერთო ეკონომიკურ საქმიანობას ახორციელებენ.[703] სავალდებულო ძალის მქონე კორპორაციული წესების, როგორც პერსონალურ მონაცემთა გადაცემის ინსტრუმენტის, ამოქმედებისთვის, აუცილებელია, ისინი დაამტკიცოს კომპეტენტურმა საზედამხედველო ორგანომ, თანმიმდევრულობის მექანიზმის გამოყენებით.

სავალდებულო ძალის მქონე კორპორაციული წესები მტკიცდება მაშინ, თუ მოიცავს მონაცემთა დაცვის ყველა ძირითად პრინციპს და მათ იყენებს და აღასრულებს ჯგუფის ყველა წევრი. ეს წესები მკაფიოდ უნდა ითვალისწინებდეს მონაცემთა სუბიექტების მიერ გამოსაყენებელ უფლებებს, მათ შორის, მონაცემთა დაცვის ყველა ძირითად პრინციპს, და აკმაყოფილებდეს გარკვეულ ფორმალურ მოთხოვნებს, კერძოდ: განსაზღვრავდეს დაწესებულების სტრუქტურას, აღწერდეს მონაცემთა გადაცემასა და დაცვის პრინციპების გამოყენების გზებს. აღნიშნული ინფორმაცია უნდა მიაწოდონ მონაცემთა სუბიექტებსაც. სავალდებულო ძალის მქონე კორპორაციული წესები, ამ საკითხებთან ერთად, უნდა აკონკრეტებდეს მონაცემთა სუბიექტების უფლებებსა და პასუხისმგებლობას წესების დარღვევის ნებისმიერ შემთხვევასთან მიმართე-

702 დამატებითი ინფორმაციისათვის, იხ. დაზუსტებული საჩივარი Facebook Ireland Ltd-ის წინააღმდეგ, რომელიც ირლანდიის მონაცემთა დაცვის კომისარს წარუდგინა მაქსიმილან შრემმა, 2015 წლის 1 დეკემბერი.

703 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 47.

ბით.[704] სავალდებულო ძალის მქონე კორპორაციული წესების დამტკიცებისას ამოქმედდება თანმიმდევრულობის მექანიზმი (იხ. მე-5 თავი), რაც ხელს უწყობს საზედამხედველო ორგანოებს შორის თანამშრომლობას.

თანმიმდევრულობის მექანიზმის ფარგლებში, წამყვანი საზედამხედველო ორგანო განიხილავს წარმოდგენილ კორპორაციულ წესებს, ამტკიცებს გადაწყვეტილების პროექტს და მას EDPB-ის წარუდგენს. საბჭო ამ საკითხზე ამზადებს საკუთარ მოსაზრებას, ხოლო საზედამხედველო ორგანო სავალდებულო ძალის მქონე კორპორაციულ წესებს ამტკიცებს საბჭოს მოსაზრების „მაქსიმალურად გათვალისწინებით“. მოსაზრებას არ აქვს სავალდებულო იურიდიული ძალა, მაგრამ თუ საზედამხდველო ორგანო აპირებს მის უგულებელყოფას, აქტიურდება დავების გადაწყვეტის მექანიზმი, რის შედეგადაც საბჭო ამტკიცებს სავალდებულო ძალის მქონე გადაწყვეტილებას, სრული შემადგენლობის 2/3-ით. [705]

ევროპის საბჭოს კანონმდებლობაში სპეციალური (ad hoc) და სტანდარტიზებული უსაფრთხოების ზომები, რომლებსაც ითვალისწინებს სავალდებულო იურიდიული ძალის მქონე დოკუმენტი,[706] მოიცავს სავალდებულო კორპორაციულ წესებსაც.

7.3.3 გამონაკლისები კონკრეტული გარემოებების შემთხვევაში

ევროკავშირის კანონმდებლობით, მესამე ქვეყნისთვის პერსონალური მონაცემების გადაცემა დაშვებულია შესაბამისობის გადაწყვეტილების ან უსაფრთხოების ზომების (სტანდარტული სახელშეკრულებო პირობები ან სავალდებულო ძალის მქონე კორპორაციული წესები) არარსებობის შემთხვევაშიც, ერთ-ერთი ამ პირობის საფუძველზე:

- თუ მონაცემთა სუბიექტი მკაფიოდ დაეთანხმება მონაცემთა გადაცემას;
- მონაცემთა სუბიექტი აფორმებს ან გასაფორმებლად ამზადებს ხელშეკრულებას, რისთვისაც საზღვარგარეთ მონაცემთა გადაცემა აუცილებელია;
- მონაცემთა დამმუშავებელსა და მესამე პირს შორის ფორმდება ხელშეკრულება, რაც მონაცემთა სუბიექტის ინტერესებში შედის;

704 დამატებითი ინფორმაციისთვის იხ. მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 47.

705 *იქვე,* მუხლები: 57 (1) (ტ), 58 (1) (კ), 64 (1) (ვ), 65 (1) და (2).

706 მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (3) (ბ).

- მონაცემთა გადაცემა საჭიროა საჯარო ინტერესის სფეროში შემავალი მნიშვნელოვანი მიზნებიდან გამომდინარე;

- სამართლებრივი მოთხოვნის დადგენა, განხორციელება ან დაცვა;

- მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დაცვა;

- მონაცემები გადაეცემა რეესტრიდან (ეს არის შემთხვევა, როდესაც ფართო საზოგადოებას აქვს საჯარო რეესტრში დაცულ ინფორმაციაზე წვდომის აღმატებული ინტერესი).[707]

თუ ჩამოთვლილი პირობებიდან არცერთი არ არის სახეზე და მონაცემთა გადაცემა არ ეფუძნება შესაბამისობის გადაწყვეტილებას ან დაცვის სათანადო გარანტიებს, გადაცემა შეიძლება განხორციელდეს მხოლოდ იმ შემთხვევაში, როცა ის არ არის განმეორებითი, ეხება მონაცემთა სუბიექტების მხოლოდ განსაზღვრულ რაოდენობას და აუცილებელია მონაცემთა დამმუშავებლის კანონიერი ინტერესების დასაცავად (თუ მონაცემთა სუბიექტის უფლებები არ აღემატება მის ინტერესებს).[708] ასეთ შემთხვევაში, დამმუშავებელმა უნდა შეაფასოს გადაცემასთან დაკავშირებული ყველა გარემოება და უზრუნველყოს დაცვის შესაბამისი გარანტიები; ასევე, აცნობოს საზედამხედველო ორგანოსა და მონაცემთა შესაბამის სუბიექტს როგორც გადაცემა, ისე გადაცემის კანონიერი ინტერესები.

ის ფაქტი, რომ გამონაკლისები მონაცემთა კანონიერი გადაცემის მხოლოდ უკანასკნელი საშუალებაა[709] (ნებადართულია მხოლოდ იმ შემთხვევაში, თუ არ არსებობს შესაბამისობის გადაწყვეტილება ან რაიმე სხვა დაცვის გარანტიები), ხაზს უსვამს მათ განსაკუთრებულობას, რაც ხაზგასმულია GDPR-ის პრეამბულაში.[710] საგამონაკლისო შემთხვევები გულისხმობს მონაცემთა გადაცემას კონკრეტული გარემოებების გათვალისწინებით, თანხმობის საფუძველზე, ასევე, როდესაც „გადაცემა არ არის რეგულარული და აუცილებელია“[711] ხელშეკრულების ან სამართლებრივი მოთხოვნით.

ამასთან, 29-ე მუხლის სამუშაო ჯგუფის სახელმძღვანელო პრინციპების თანახმად, კონკრეტულ სიტუაციებში გამონაკლისი დაშვებულია საკანონმდებ-

---

707 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 49.

708 *იქვე.*

709 *იქვე,* მუხლი 49 (1).

710 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი, 49(1)(ა),(ბ) და (ე) და პრეამბულა, პუნქტი 113.

711 *იქვე,* მუხლი 49(1).

ლო მოთხოვნებიდან იშვიათი გადახვევის სახით და საქმის ინდივიდუალური გარემოებების გათვალისწინებით. იგი არ გამოიყენება მონაცემთა ფართომასშტაბიანი ან განმეორებითი გადაცემისთვის.[712] ევროკავშირის მონაცემთა დაცვის ზედამხედველმა ხაზგასმით აღნიშნა, რომ 45/2001 რეგულაციის თანახმად, გამონაკლისები დაიშვება და გამოიყენება მხოლოდ „შეზღუდულ შემთხვევებში“ და „[მონაცემთა] არარეგულარული გადაცემისთვის.“[713]

მაგალითი: კომპანია Global Distribution System (GDS), რომელსაც სათავო ოფისი აქვს აშშ-ში, მსოფლიო მასშტაბით სხვადასხვა ავიაკომპანიისთვის უზრუნველყოფს ონლაინ ჯავშნების სისტემას სასტუმროებისა და კრუიზებისთვის და ამუშავებს ევროკავშირში მცხოვრები ათობით მილიონი ადამიანის პერსონალურ მონაცემებს. აშშ-ში განთავსებულ სერვერებს კომპანია მონაცემებს გადასცემს გამონაკლისის საფუძველზე, იმ მოტივით, რომ მონაცემთა გადაცემა აუცილებელია ხელშეკრულების დასადებად. ეს არ ითვალისწინებს რაიმე სხვა გარანტიებს პერსონალურ მონაცემთა დასაცავად, რომლებიც წარმოიშობა ევროპაში, გადაეცემა აშშ-ს და მიეწოდება სხვადასხვა სასტუმროს მსოფლიო მასშტაბით (დაცვის გარანტიები მონაცემთა შემდგომი გადაცემისთვისაც არ არის გათვალისწინებული). ამრიგად, კომპანია GDS არ აკმაყოფილებს GDPR-ის მოთხოვნებს მონაცემთა საერთაშორისო გადაცემასთან დაკავშირებით, რადგან იგი მასობრივი გადაცემის სამართლებრივ საფუძვლად იყენებს კანონიდან გადახვევას.

გარდა იმ შემთხვევისა, როდესაც არსებობს შესაბამისობის გადაწყვეტილება, ევროკავშირს ან წევრ სახელმწიფოს უფლება აქვს, მნიშვნელოვანი საჯარო ინტერესის საფუძველზე, მესამე ქვეყნისთვის პერსონალურ მონაცემთა გარკვეული კატეგორიების გადაცემაზე შეზღუდვები დააწესოს მაშინაც, როცა სრულდება გადაცემის სხვა პირობები. ეს შეზღუდვები გამონაკლისად უნდა ჩაითვალოს, ხოლო წევრი სახელმწიფოებს მოეთხოვებათ შესაბამისი დებულებების წარდგენა კომისიისათვის.[714]

როცა მონაცემები სათანადოდ არ არის დაცული, ევროპის საბჭოს კანონმდებლობა მონაცემთა მიმოცვლას მესამე პირთან ითვალისწინებს შემდეგი ერთ-ერთი პირობის საფუძველზე:

712 29-ე მუხლის სამუშაო ჯგუფი (2005), სამუშაო დოკუმენტი 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივის 26-ე მუხლის პირველი პუნქტის განმარტების შესახებ, WP 114, ბრიუსელი, 2005 წლის 25 ნოემბერი.

713 ევროკავშირის მონაცემთა დაცვის ზედამხედველო, პერსონალური მონაცემების გადაცემა მესამე ქვეყნებისა და საერთაშორისო ორგანიზაციებისათვის, ევროკავშირის ინსტიტუტებისა და ორგანოების მიერ, პოზიციის განაცხადი, ბრიუსელი, 2014 წლის 14 ივლისი, გვ. 15.

714 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 49(5).

- თუ არსებობს მონაცემთა სუბიექტის თანხმობა;
- ამას მოითხოვს მონაცემთა სუბიექტის ინტერესები;
- არსებობს აღმატებული კანონიერი ინტერესები - განსაკუთრებით, საჯარო - რომლებიც გათვალისწინებულია კანონით;
- ეს აუცილებელი და პროპორციული ღონისძიებაა დემოკრატიულ საზოგადოებაში .[715]

7.3.4 მონაცემთა გადაცემა საერთაშორისო შეთანხმებების საფუძველზე

ევროკავშირს შეუძლია, მესამე ქვეყნებთან დადოს საერთაშორისო შეთანხმებები, რომლებიც დაარეგულირებს პერსონალური მონაცემების გადაცემას კონკრეტული მიზნებით. ეს შეთანხმებები უნდა მოიცავდეს უსაფრთხოების შესაბამის ზომებს. GDPR არ გამორიცხავს ასეთი საერთაშორისო ხელშეკრულებების პირობების მოქმედებას.[716]

მსგავსად, წევრ სახელმწიფოებს შეუძლიათ საერთაშორისო შეთანხმებების დადება მესამე ქვეყნებსა ან საერთაშორისო ორგანიზაციებთან ფიზიკურ პირთა ფუნდამენტური უფლებებისა და თავისუფლებების სათანადო დონეზე დასაცავად, თუკი ეს შეთანხმება გავლენას არ ახდენს GDPR-ის გამოყენებაზე.

იმავე წესს ადგენს მოდერნიზებული 108-ე კონვენციის მე-12 მუხლის 3 (ა) პუნქტი.

შეთანხმებები მგზავრის პირადი მონაცემების (PNR) შესახებ, რომელიც პერსონალური მონაცემების გადაცემას ითვალისწინებს, ასეთი საერთაშორისო შეთანხმების მაგალითია.

მგზავრის პირადი მონაცემები

მგზავრთა პირად მონაცემებს (PNR) ავიაკომპანიები აგროვებენ დაჯავშნის პროცესში და ეს მოიცავს პირის სახელს, გვარს, მისამართს, საკრედიტო ბარათებისა და მგზავრის ადგილის ნომრებს. ევროკავშირს დადებული აქვს შეთანხმებები მესამე ქვეყნებთან, როგორიცაა ავსტრალია, კანადა და აშშ, PNR მონაცემების გადაცემაზე ტერორისტული ან მძიმე ტრანსნაციონალური

715 მოდერნიზებული 108-ე კონვენცია, მუხლი 14 (4).

716 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 102.

დანაშაულების პრევენციის, გამოვლენის, გამოძიებისა და დამნაშავეთა დასჯის მიზნით. ამასთან, 2016 წელს ევროკავშირმა მიიღო 2016/681 დირექტივა (ევროკავშირის PNR დირექტივა),[717] რომელიც ადგენს სამართლებრივ ჩარჩოს ევროკავშირის წევრი სახელმწიფოების მიერ მესამე ქვეყნის უფლებამოსილი უწყებებისათვის PNR მონაცემების გადასაცემად - ტერორისტული და მძიმე დანაშაულების პრევენციის, გამოვლენის, გამოძიებისა და დამნაშავეთა დასჯის მიზნით. მესამე ქვეყნის სახელმწიფო ორგანოებს PNR მონაცემები გადაეცემა ცალკეულ შემთხვევაში და ექვემდებარება ინდივიდუალურ შეფასებას, რამდენად აუცილებელი იყო ეს დირექტივაში მითითებული მიზნებისთვის და განხორციელდა თუ არა ფუნდამენტური უფლებების დაცვით. ევროკავშირსა და მესამე ქვეყნებს შორის არსებულ PNR შეთანხმებებთან დაკავშირებით, დავის საგანია მათი შესაბამისობა პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის ფუნდამენტურ უფლებებთან, რომლებიც გათვალისწინებულია ქარტიით (Charter). კანადასთან მოლაპარაკებების შემდგომ, 2014 წელს ევროკავშირმა ხელი მოაწერა შეთანხმებას PNR მონაცემების გადაცემისა და დამუშავების შესახებ. ევროპულმა პარლამენტმა გადაწყვიტა, ამ საკითხზე მიემართა CJEU-სათვის, რათა ამ უკანასკნელს დაედგინა შეთანხმების შესაბამისობა ევროკავშირის კანონმდებლობასთან, კერძოდ, ქარტიის მე-7 და მე-8 მუხლებთან.

მაგალითი: ევროკავშირი-კანადას PNR შეთანხმების კანონიერებასთან[718] მიმართებით, CJEU-მ დაადგინა, რომ შეთანხმების პროექტი არ შეესაბამებოდა ქარტიით აღიარებულ ფუნდამენტურ უფლებებს. ამრიგად, მისი გაფორმება დაუშვებელი იყო. ვინაიდან შეთანხმება პერსონალური მონაცემების დამუშავებას ითვალისწინებდა, ეს გახლდათ ჩარევა ქარტიის მე-8 მუხლით გარანტირებულ პერსონალურ მონაცემთა დაცვის უფლებაში. ამავდროულად, შეთანხმება აწესებდა შეზღუდვას მე-7 მუხლით დაცულ პირადი ცხოვრების პატივისცემის უფლებაზე, რადგან შესაძლებელია PNR მონაცემების ერთად თავმოყრა და ისე გაანალიზება, რომ დადგინდეს ფიზიკურ პირთა სამოგზაურო ჩვევები, სხვადასხვა პირს შორის ურთიერთობა, ინფორმაცია ფინანსური მდგომარეობის შესახებ, კვებასთან დაკავშირებული ჩვევები და ჯანმრთელობის მდგომარეობა, ეს კი მათ პირად ცხოვრებაში ჩარევაა.

შეთანხმებით გათვალისწინებული ჩარევა ფუნდამენტურ უფლებებში ემსახურებოდა საჯარო ინტერესს, კერძოდ, საზოგადოებრივ უსაფრთხოება-

717 ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/681 ტერორისტული და მძიმე დანაშაულების პრევენციის, გამოვლენის, გამოძიებისა და დამნაშვეთა დასჯის მიზნით მგზავრთა პირადი მონაცემების (PNR) გამოყენების შესახებ, OJ 2016 L 119.

718 CJEU, სასამართლოს (დიდი პალატა) მოსაზრება 1/15, 2017 წლის 26 ივლისი.

სა და ტერორიზმსა და მძიმე ტრანსნაციონალურ დანაშაულთან ბრძოლას. თუმცა, CJEU-ს განმარტებით, ჩარევა გამართლებულია მხოლოდ იმ მასშტაბით, რომელიც მკაცრად აუცილებელია დასახული მიზნის მისაღწევად. ანალიზის საფუძველზე, CJEU-მ დაასკვნა, რომ შეთანხმება ვერ აკმაყოფილებდა „მკაცრი აუცილებლობის“ კრიტერიუმს. გადაწყვეტილების მიღებისას CJEU-მ გაითვალისწინა შემდეგი ფაქტორები:

- ფაქტი, რომ შეთანხმება მოიცავდა განსაკუთრებული კატეგორიის მონაცემთა გადაცემას. კერძოდ, PNR-ის შეგროვებისას შეიძლება თავმოყრილიყო ისეთი განსაკუთრებული კატეგორიის მონაცემები, როგორიცაა ინფორმაცია მგზავრის რასობრივი და ეთნიკური წარმომავლობის, რელიგიური მრწამსისა თუ ჯანმრთელობის შესახებ. განსაკუთრებული კატეგორიის მონაცემების გადაცემასა და კანადის სახელმწიფო უწყებების მიერ დამუშავებას შეიძლება საფრთხე შეექმნა დისკრიმინაციის აკრძალვის პრინციპისათვის. ამრიგად, საჭირო იყო ზუსტი და მყარი საფუძველი (გარდა საზოგადოებრივი უსაფრთხოებისა და მძიმე დანაშაულთან ბრძოლისა), რომელსაც შეთანხმება არ ითვალისწინებდა. [719]

- PNR მონაცემების შენახვა ხანგრძლივად, 5 წლის ვადით, როდესაც მგზავრი აღარ იმყოფებოდა კანადის ტერიტორიაზე, სცილდებოდა მკაცრი საჭიროების ზღვარს. CJEU-მ მიიჩნია, რომ კანადის შესაბამის სახელმწიფო ორგანოებს შეეძლოთ კონკრეტულ მგზავრთა მონაცემების შენახვა (მაშინაც კი, როდესაც პირი კანადის ტერიტორიაზე აღარ იმყოფებოდა), თუ დადასტურდებოდა, რომ ისინი რისკს უქმნიდნენ საზოგადოებრივ უსაფრთხოებას; მეორე მხრივ, გაუმართლებელი იყო ყველა მგზავრის პერსონალური მონაცემების შენახვა, თუკი ირიბი მტკიცებულებაც არ არსებობდა, რომ ისინი ქმნიდნენ ასეთ საფრთხეს. [720]

108-ე კონვენციის საკონსულტაციო კომიტეტმა შეიმუშავა მოსაზრება, რომელიც შეეხება PNR შეთანხმებების გავლენას მონაცემთა დაცვაზე.[721]

მონაცემები გზავნილების შესახებ

„მსოფლიო ბანკთაშორისი საფინანსო კომუნიკაციისა და არხების საზოგადოება“ (SWIFT) დაფუძნებულია ბელგიაში და ამუშავებს ევროპული ბანკებიდან განხორციელებული გლობალური ფულადი გზავნილების დიდ ნაწილს. ვინა-

719 *იქვე,* პუნქტი 165.

720 *იქვე,* პუნქტები 204–207.

721 ევროპის საბჭოს მოსაზრება, მგზავრთა პირადი მონაცემების დამუშავების გავლენა მონაცემთა დაცვაზე, T-PD(2016)18rev, 2016 წლის 19 აგვისტო.

იდან ორგანიზაცია მონაცემებს ამუშავებდა აშშ-ში მდებარე ცენტრში, აშშ-ს სახაზინო დეპარტამენტმა მისგან გარკვეული მონაცემების გამჟღავნება მოითხოვა, კერძოდ, „ტერორიზმის დაფინანსების მონიტორინგის პროგრამის“ ფარგლებში ტერორიზმზე მიმდინარე გამოძიებისთვის.[722]

ევროკავშირის პოზიციით, ამ მონაცემების (რომლებიც ძირითადად ევროკავშირის მოქალაქეებს შეეხებოდა) გასამჟღავნებლად, არ არსებობდა საკმარისი სამართლებრივი საფუძველი. კერძოდ, დაუშვებელი იყო მონაცემების აშშ-სთვის გადაცემა მხოლოდ იმის გამო, რომ SWIFT-ის მონაცემთა დამუშავების ცენტრები აშშ-ში მდებარეობდა.

სპეციალური შეთანხმება აშშ-სა და ევროკავშირს შორის (SWIFT შეთანხმება) დაიდო 2010 წელს და მოიცავს საჭირო სამართლებრივ საფუძველს და მონაცემთა დაცვის ადეკვატურ სტანდარტებს. [723]

შეთანხმების საფუძველზე, SWIFT აშშ-ს სახაზინო დეპარტამენტს გადასცემს მონაცემებს ტერორიზმის ან მისი დაფინანსების პრევენციის, გამოძიების, გამოვლენისა და დამნაშავეთა დასჯის მიზნით. აშშ-ს სახაზინო დეპარტამენტს უფლება აქვს, SWIFT-ისგან მოითხოვოს ფინანსური ინფორმაცია, თუკი მოთხოვნა:

- მკაფიოდ ავლენს საჭირო ფინანსურ მონაცემებს;
- მკაფიოდ ასაბუთებს მათ აუცილებლობას;
- მაქსიმალურად ვიწროა და მინიმუმამდე ამცირებს მოთხოვნილი მონაცემების მოცულობას;
- არ ითხოვს ერთიან ევროპულ საგადასახადო სისტემასთან (SEPA) დაკავშირებულ მონაცემებს. [724]

722 ამ მხრივ, იხ: 29-ე მუხლის სამუშაო ჯგუფი (2011), მოსაზრება 14/2011 ფულის გათეთრებასა და ტერორიზმის ფინანსირებასთან დაკავშირებულ პერსონალურ მონაცემთა საკითხებზე, WP 186, ბრიუსელი, 13 ივნისი 2011 წელი; 29-ე მუხლის სამუშაო ჯგუფი (2006); მოსაზრება 10/2006 SWIFT-ის მიერ პერსონალურ მონაცემთა დამუშავების შესახებ, WP 128, ბრიუსელი, 22 ნოემბერი, 2006 წელი; პირადი ცხოვრების დაცვის ბელგიის კომისია *(Commission de la protection de la vie privée)* (2008), გადაწყვეტილება, 9 დეკემბერი, 2008 წელი, SWIFT scrl-სთან დაკავშირებით ინიცირებული კონტროლისა და რეკომენდაციის პროცედურა, 2008 წლის 9 დეკემბერი.

723 საბჭოს 2010 წლის 13 ივლისის გადაწყვეტილება 2010/412/EU ევროკავშირი-აშშ-ს შეთანხმებაზე, რომელიც შეეხება ფინანსურ გზავნილებს, მონაცემთა ევროკავშირიდან აშშ-სთვის გადაცემა-დამუშავებას ტერორიზმის დაფინანსების მონიტორინგის პროგრამის ფარგლებში, OJ 2010 L 195, გვ. 3 და 4. შეთანხმების ტექსტი მიმაგრებულია გადაწყვეტილებაზე, OJ 2010 L 195, გვ. 5-14.

724 *იქვე,* მუხლი 4 (2).

აშშ-ს სახაზინო დეპარტამენტის მიერ SWIFT-ისათვის გაგზავნილი თითოეული მოთხოვნის ასლი უნდა წარედგინოს ევროპის პოლიციის სამსახურს (ევროპოლს), რომელიც განსაზღვრავს, რამდენად დაცულია SWIFT-ის შეთანხმების პრინციპები.[725] თუ მათი დაცვა დადასტურდება, SWIFT ვალდებულია, მოთხოვნილი ფინანსური მონაცემები მიაწოდოს პირდაპირ აშშ-ს სახაზინო დეპარტამენტს. დეპარტამენტი, თავის მხრივ, ვალდებულია, ფინანსური მონაცემები უსაფრთხო ფიზიკურ გარემოში შეინახოს, სადაც წვდომა ექნებათ მხოლოდ ანალიტიკოსებს, რომლებიც ტერორიზმის ან ტერორიზმის დაფინანსების შემთხვევებს იძიებენ. აკრძალულია ამ ფინანსური მონაცემების ინტეგრირება სხვა მონაცემთა ბაზასთან. ზოგადად, SWIFT-ისგან გადაცემული მონაცემები უნდა წაიშალოს მიღებიდან არაუგვიანეს 5 წლის ვადაში. ფინანსური მონაცემები, რომლებიც რელევანტურია კონკრეტული გამოძიებისა ან დევნისათვის, უნდა შეინახონ მხოლოდ ამ გამოძიებისა თუ დევნის განსახორციელებლად აუცილებელი ვადით.

აშშ-ს სახაზინო დეპარტამენტს შეუძლია SWIFT-ისგან მიღებული მონაცემები გადასცეს სამართალდამცველ ორგანოებს, ასევე, საზოგადოებრივი უსაფრთხოების ან ტერორიზმის წინააღმდეგ ბრძოლის უწყებებს აშშ-ში ან მის ფარგლებს გარეთ, ოღონდ მხოლოდ ისეთი მიზნებით, როგორიცაა ტერორიზმის ან მისი დაფინანსების შემთხვევათა გამოვლენა, პრევენცია და დამნაშავეთა დასჯა. თუ ფინანსური მონაცემების გადაცემა უკავშირდება ევროკავშირის წევრი ქვეყნის მოქალაქეს ან მცხოვრებს, მესამე ქვეყნისთვის მონაცემთა გაზიარების აუცილებელი პირობაა ამ ქვეყნის უფლებამოსილი სახელმწიფო ორგანოების წინასწარი თანხმობა. გამონაკლისი დაიშვება მაშინ, თუ მონაცემთა გადაცემა აუცილებელია საზოგადოებრივი უსაფრთხოების მყისიერი და სერიოზული საფრთხეების თავიდან ასაცილებლად.

დამოუკიდებელი ზედამხედველები, მათ შორის, ევროკომისიის მიერ დანიშნული პირი, მონიტორინგს უწევენ SWIFT-ის შეთანხმების პრინციპების შესრულებას. მათ აქვთ შესაძლებლობა, რეალურ დროში და რეტროაქტიულად შეისწავლონ მოთხოვნილი მონაცემების საფუძველზე განხორციელებული ძიება, მოითხოვონ დამატებითი ინფორმაცია ამ ძიების ტერორიზმთან კავშირის გასამყარებლად და დაბლოკონ ნებისმიერი კვლევა, რომელიც, ერთი შეხედვით, არღვევს შეთანხმებით გათვალისწინებულ დაცვის გარანტიებს.

მონაცემთა სუბიექტებს უფლება აქვთ, ევროკავშირის კომპეტენტური საზედამხედველო ორგანოსგან მოითხოვონ ინფორმაცია, თუ რამდენად გარანტირებულია მათი პერსონალურ მონაცემთა დაცვის უფლება; ასევე, მოითხოვონ იმ მონაცემების გასწორება, წაშლა ან დაბლოკვა, რომლებიც SWIFT-ის შეთანხმების საფუძველზე შეაგროვა აშშ-ს სახაზინო დეპარტამენტმა. ამავდ-

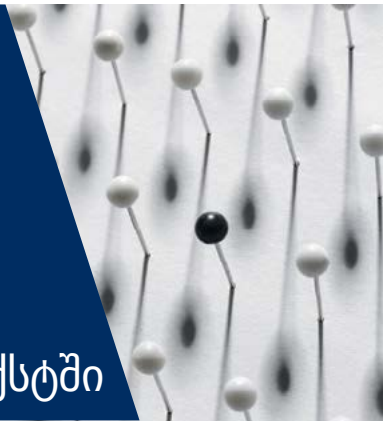
725 ევროპოლის საერთო საერთო საზედამხედველო ორგანომ ამ სფეროში განახორციელა ევროპოლის აქტივობების აუდიტი.

როულად, მონაცემთა სუბიექტების ხელმისაწვდომობის უფლებაზე შეიძლება დაწესდეს გარკვეული შეზღუდვები. წვდომაზე უარის შემთხვევაში, მონაცემთა სუბიექტს უარი წერილობით უნდა აცნობონ. წერილობითვე უნდა განემარტოს აშშ-ში ადმინისტრაციული და სამართლებრივი დაცვის საშუალებათა გამოყენების უფლება.

SWIFT-ის შეთანხმება ძალაში იყო 5-წლით. ეს ვადა გავიდა 2015 წელს და ავტომატურად გრძელდება თითო წლით, თუ ერთ-ერთი მხარე მეორეს, სულ მცირე, 6 თვით ადრე არ შეატყობინებს, რომ აღარ სურს შეთანხმების გაგრძელება. 2015, 2016 და 2017 წლებში SWIFT შეთანხმების ავტომატური გაგრძელების შედეგად, იგი მოქმედი იყო 2018 წლის აგვისტომდე.[726]

726 *იქვე,* მუხლი 23 (2).

8 მონაცემთა დაცვა პოლიციისა და სისხლის სამართლის მართლმსაჯულების კონტექსტში



ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის	**ზოგადად**	მოდერნიზებული 108-ე კონვენცია
	პოლიცია	პოლიციის რეკომენდაცია; პრაქტიკული სახელმძღვანელო პოლიციის სექტორში პერსონალური მონაცემების გამოყენების თაობაზე.
	თვალთვალი	ECtHR, *B.B. v. France,* No. 5335/06, 2009; ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 2008; ECtHR, *Allan v. the United Kingdom*, No. 48539/99, 2002; ECtHR, *Malone v. the United Kingdom,* No. 8691/79, 1984; ECtHR, *Klass and Others v. Germany,* No. 5029/71, 1978; ECtHR, *Szabó and Vissy v. Hungary,* No. 37138/14, 2016; ECtHR, *Vetter v. France,* No. 59842/00, 2005.
	კიბერდანაშაული	კიბერდანაშაულის კონვენცია

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
სხვა კონკრეტული სამართლებრივი ინსტრუმენტები		
პრუმის (Prüm) გადაწყვეტილება	**სპეციალური მონაცემებისთვის: თითის ანაბეჭდები, დნმ, ხულიგნობა, ავიამგზავრთა ინფორმაცია, სატელეკომუნიკაციო მონაცემები და ა.შ.**	მოდერნიზებული 108-ე კონვენცია, მუხლი 6; პოლიციის რეკომენდაცია, პრაქტიკული სახელმძღვანელო პოლიციის სექტორში პერსონალური მონაცემების გამოყენების თაობაზე.
შვედეთის ინიციატივა (საბჭოს ჩარჩო გადაწყვეტილება 2006/960/JHA)	**ამარტივებს ინფორმაციისა და დაზვერვის შედეგად მოპოვებული მონაცემების გაცვლას სამართალდამცველ ორგანოებს შორის**	ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 2008
დირექტივა (EU) 2016/681 ტერორისტული და მძიმე დანაშაულების პრევენციის, გამოვლენის, გამოძიებისა და დამნაშავეთა დასჯის მიზნით მგზავრთა პირადი მონაცემების (PNR) გამოყენების შესახებ; CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland and Kärntner Landesregierung and Others* [GC], 2014; CJEU, გაერთიანებული საქმეები C-203/15 და C-698/15, *Tele2 Sverige* and *Home Department v. Tom Watson and Others* [GC], 2016.	**პერსონალური მონაცემების შენახვა**	ECtHR, *B.B. v. France*, No. 5335/06, 2009

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
ევროპოლის რეგულაცია; ევროჯასტის გადაწყვეტილება.	**სპეციალური სააგენტოების მიერ**	რეკომენდაცია პოლიციის შესახებ
შენგენის II გადაწყვეტილება; VIS რეგულაცია; ევროდაკის რეგულაცია; CIS გადაწყვეტილება.	**სპეციალური ერთობლივი საინფორმაციო სისტემების მიერ**	რეკომენდაცია პოლიციის შესახებ; ECtHR, *Dalea v. France*, No. 964/07, 2010.

ბალანსის მისაღწევად, რომლის ერთ მხარესაც არის ფიზიკური პირის ინტერესი მონაცემთა დაცვის მიმართ, ხოლო მეორე მხარეს - საზოგადოების ინტერესი მონაცემთა შეგროვებისადმი დანაშაულთან ბრძოლისა და ეროვნული თუ საზოგადოებრივი უსაფრთხოების მიზნებით, ევროპის საბჭომ და ევროკავშირმა კონკრეტული სამართლებრივი ინსტრუმენტები შექმნეს. წინამდებარე ნაწილში მიმოხილულია ევროპის საბჭოს (ნაწილი 8.1) და ევროკავშირის (ნაწილი 8.2) კანონმდებლობები პოლიციისა და სისხლის სამართლის მართლმსაჯულების სფეროში მონაცემთა დაცვასთან დაკავშირებით.

8.1 ევროპის საბჭოს კანონმდებლობა მონაცემთა დაცვისა და ეროვნული უსაფრთხოების, პოლიციისა და სისხლის სამართლის მართლმსაჯულების საკითხებზე

ძირითადი საკითხები

- მოდერნიზებული 108-ე კონვენცია და ევროპის საბჭოს რეკომენდაცია პოლიციის შესახებ ვრცელდება მონაცემთა დაცვაზე საპოლიციო საქმიანობის ყველა სფეროში.

- კონვენცია კიბერდანაშაულის შესახებ (ბუდაპეშტის კონვენცია) სავალდებულო ძალის მქონე საერთაშორისო სამართლებრივი ინსტრუმენტია, რომელიც შეეხება დანაშაულებს, ჩადენილს ელექტრონული ქსელების მეშვეობით, ან მათ წინააღმდეგ. იგი რელევანტურია ისეთი დანაშაულების გამოსაძიებლადაც, რომლებიც არ მიიჩნევა კიბერდანაშაულად, თუმცა მტკიცებულება წარმოდგენილია ელექტრონული ფორმით.

ევროკავშირის სამართლისგან განსხვავებით, ევროპის საბჭოს კანონმდებლობა ვრცელდება ეროვნული უსაფრთხოების სფეროზე. ეს გულისხმობს, რომ ხელშემკვრელმა სახელმწიფოებმა ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის მოქმედების ფარგლები არ უნდა დაარღვიონ მაშინაც კი, როდესაც მათი საქმიანობა ეროვნულ უსაფრთხოებას უკავშირდება. ადამიანის უფლებათა ევროპული სასამართლოს არაერთი გადაწყვეტილება ეხება სახელმწიფოს საქმიანობას ეროვნული უსაფრთხოების კანონმდებლობისა და პრაქტიკის სენსიტიურ სფეროში. [727]

საპოლიციო და სისხლის სამართლის მართლმსაჯულების კონტექსტში, ევროპულ დონეზე, მოდერნიზებული 108-ე კონვენცია მოიცავს პერსონალურ მონაცემთა დამუშავების ყველა სფეროს და მისი დებულებები მიმართულია ზოგადად პერსონალურ მონაცემთა დამუშავების რეგულირებაზე. შესაბამისად, კონვენცია ვრცელდება მონაცემთა დაცვაზე პოლიციის და სისხლის სამართლის მართლმსაჯულების სფეროში. გენეტიკური და დანაშაულთან დაკავშირებული პერსონალური მონაცემების, სისხლის სამართლის საქმისწარმოებაზე, ნასამართლობასა და უსაფრთხოების ნებისმიერ ზომებზე ინფორმაციის, პირის მაიდენტიფიცირებელი ბიომეტრიული მონაცემებისა და განსაკუთრებული კატეგორიის პერსონალური ინფორმაციის დამუშავება დაშვებულია მხოლოდ უსაფრთხოების სათანადო ზომების არსებობისას, რათა რისკები არ შეექმნას მონაცემთა სუბიექტების ინტერესებს, უფლებებსა და ფუნდამენტურ თავისუფლებებს, განსაკუთრებით, დისკრიმინაციის მხრივ.[728]

პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოთა ამოცანები ხშირად მოითხოვს პერსონალური მონაცემების დამუშავებას, რამაც შეიძლება მძიმე შედეგები მოუტანოს შესაბამის პირებს. პოლიციის რეკომენდაცია, რომელიც ევროპის საბჭომ 1987 წელს მიიღო, წევრ სახელმწიფოებს აწვდის ინსტრუქციებს 108-ე კონვენციის პრინციპების ამოქმედებაზე, სამართალდამცველი ორგანოების მიერ პერსონალურ მონაცემთა დამუშავების კონტექსტში.[729] რეკომენდაციას ახლავს პრაქტიკული სახელმძღვანელო პოლიციის სექტორში პერსონალურ მონაცემთა გამოყენების შესახებ, რომელიც მიიღო 108-ე კონვენციის საკონსულტაციო კომიტეტმა.[730]

---

727 იხ. მაგალითად, ECtHR, *Klass and Others v. Germany, No. 5029/71, 1978* წლის 6 სექტემბერი; *ECtHR*, *Rotaru v. Romania* [GC], No. 28341/95, 2000 წლის 4 მაისი და ECtHR, *Szabó and Vissy v. Hungary,* No. 37138/14, 2016 წლის 12 იანვარი.

728 მოდერნიზებული 108-ე კონვენცია, მუხლი 6.

729 ევროპის საბჭოს მინისტრთა კომიტეტი (1987), რეკომენდაცია წევრი სახელმწიფოებისთვის Rec(87)15 პოლიციის სექტორში პერსონალურ მონაცემთა გამოყენების რეგულირების შესახებ, 1987 წლის 17 სექტემბერი, T-PD(2018)1.

730 ევროპის საბჭო, 2018; 108-ე კონვენციის საკონსულტაციო კომიტეტი, პრაქტიკული სახელმძღვანელო პოლიციის სექტორში პერსონალურ მონაცემთა გამოყენების შესახებ, T-PD (2018) 1.

მაგალითები: საქმეში *D.L. v. Bulgaria*[731] სოციალური უსაფრთხოების სამსახურმა, სასამართლო გადაწყვეტილების საფუძველზე, განმცხადებელი დაცულ საგანმანათლებლო დაწესებულებაში მოათავსა. დაწესებულება განმცხადებლის წერილობით კორესპონდენციასა და სატელეფონო საუბრებზე ახორციელებდა ბლანკეტურ და განურჩეველ თვალთვალს. ECtHR-მა დაადგინა კონვენციის მე-8 მუხლის დარღვევა, რადგან გამოყენებული ზომები არ იყო აუცილებელი დემოკრატიულ საზოგადოებაში. სასამართლოს განმარტებით, ყველაფერი უნდა გაკეთდეს, რომ დაწესებულებაში მოთავსებულ არასრულწლოვნებს გარე სამყაროსთან საკმარისი კონტაქტი ჰქონდეთ, რადგან ეს ღირსეული მოპყრობის უფლების განუყოფელი ნაწილია და აუცილებელია მათ მოსამზადებლად საზოგადოებაში რეინტეგრაციისათვის. აღნიშნული თანაბრად ეხება როგორც ვიზიტებს, ისე წერილობით კორესპონდენციასა და სატელეფონო საუბრებს. ამასთან, თვალთვალის დროს არ განარჩევდნენ კომუნიკაციას ოჯახის წევრებთან, ასევე, იმ არასამთავრობო ორგანიზაციებსა ან ადვოკატებთან, რომლებიც ბავშვთა ინტერესებს იცავენ. არც კომუნიკაციაზე მონიტორინგის გადაწყვეტილება ეფუძნებოდა კონკრეტულ საქმეში არსებული რისკების შეფასებას.

საქმეში *Dragojević v. Croatia*[732] განმცხადებელს ბრალად ედებოდა ნარკოტრეფიკინგში მონაწილეობა. იგი სასამართლომ დამნაშავედ ცნო მას შემდეგ, რაც გამომძიებელმა მოსამართლემ განმცხადებლის სატელეფონო ზარებზე ფარული მიყურადების ნებართვა გასცა. ECtHR-მა დაადგინა, რომ ღონისძიება, რომელსაც ასაჩივრებდა განმცხადებელი, იყო ჩარევა პირადი ცხოვრების პატივისცემისა და კორესპონდენციის უფლებაში. გამომძიებელი მოსამართლის მიერ გაცემული ნებართვის ერთადერთი საფუძველი გახლდათ პროკურატურის განცხადება, რომ „გამოძიების ჩატარება შეუძლებელია სხვა საშუალებებით.“ ECtHR-მა ასევე აღნიშნა, რომ სისხლის სამართლის სასამართლოებმა შეზღუდულად შეაფასეს თვალთვალის ღონისძიებათა გამოყენება, ხოლო მთავრობამ არ უზრუნველყო დაცვის საშუალებები. შესაბამისად, საქმეში დაირღვა კონვენციის მე-8 მუხლი.

8.1.1 რეკომენდაცია პოლიციის შესახებ

ECtHR-მა არაერთხელ აღნიშნა, რომ საპოლიციო ან ეროვნული უსაფრთხოების ორგანოების მიერ პერსონალური მონაცემების ჩაწერა და შენახვა ჩარევაა კონვენციის მე-8 მუხლის პირველი პუნქტით გათვალისწინებულ უფლე-

731 ECtHR, *D.L. v. Bulgaria,* No. 7472/14, 19 May 2016.

732 ECtHR, *Dragojević v. Croatia,* No. 68955/11, 2015 წლის 15 იანვარი.

ბაში. ევროპული სასამართლოს არაერთი გადაწყვეტილება ეხება ამგვარი ჩარევის კანონიერების საკითხს. [733]

მაგალითები: საქმეში *B.B. v. France*[734] განმცხადებელს მიესაჯა 15 წელი არასრულწლოვნების მიმართ ჩადენილი სქესობრივი დანაშაულისათვის, რომელიც 2000 წელს მოიხადა. ერთი წლის შემდგომ მან ნასამართლობის მოხსნა ითხოვა, მაგრამ უარი ეთქვა. 2004 წელს, საფრანგეთმა, შესაბამისი კანონმდებლობის საფუძველზე, შექმნა სქესობრივ დანაშაულში მხილებულების მონაცემთა ბაზა, განმცხადებელს კი შეატყობინეს მისი ვინაობის შეტანა ამ ბაზაში. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ სქესობრივი დანაშაულისათვის მსჯავრდებული პირის მონაცემების შენახვა კონვენციის მე-8 მუხლის მოქმედების ფარგლებში ექცეოდა. ამავდროულად, დაცვის საკმარისი მექანიზმების გამოყენებით (როგორიცაა მონაცემთა სუბიექტის უფლება, მოითხოვოს მონაცემთა წაშლა, მათი შენახვის ვადისა და მათზე წვდომის შეზღუდვა), საჯარო და კერძო ინტერესებს შორის მიღწეულია სამართლიანი ბალანსი. შესაბამისად, სასამართლომ დაადგინა, რომ საქმეში კონვენციის მე-8 მუხლი არ დარღვეულა.

საქმეში *S. and Marper v. the United Kingdom*[735] განმცხადებლებს ბრალად ედებოდათ სისხლის სამართლის დანაშაული, თუმცა სასამართლომ ორივე მათგანი უდანაშაულოდ ცნო. მიუხედავად ამისა, მათი თითის ანაბეჭდები, უჯრედული ნიმუშები და დნმ-ის პროფილები პოლიციამ მაინც შეინახა. ბიომეტრიული მონაცემების განსაზღვრული ვადით შენახვა კანონით ნებადართული იყო იმ შემთხვევაშიც, თუ პირს ბრალად ედებოდა სისხლის სამართლის დანაშაული, მაგრამ მოგვიანებით გამართლდა ან მოეხსნა ბრალდება. ECtHR-მა დაადგინა, რომ პერსონალური მონაცემების ბლანკეტური და განურჩეველი შენახვა განუსაზღვრელი ვადით, მაშინ, როდესაც სასამართლოს მიერ უდანაშაულოდ ცნობილ პირებს შეზღუდული ჰქონდათ ამ მონაცემების წაშლის მოთხოვნა, იყო არაპროპორციული ჩარევა განმცხადებლის პირადი ცხოვრების უფლებაში. სასამართლომ საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

ელექტრონული კომუნიკაციების კონტექსტში მნიშვნელოვანი საკითხია სახელმწიფო ორგანოების ჩარევა პირადი ცხოვრებისა და პერსონალური მონაცემე-

733 იხ. მაგალითად, ECtHR, *Leander v. Sweden,* No. 9248/81, 1987 წლის 26 მარტი; ECtHR, *M.M. v. the United Kingdom,* No. 24029/07, 2012 წლის 13 ნოემბერი; ECtHR, *M.K. v. France,* No. 19522/09, 2013 წლის 18 აპრილი, ან ECtHR, *Aycaguer v. France,* No. 8806/12, 2017 წლის 22 ივნისი.

734 ECtHR, *B.B. v. France,* No. 5335/06, 2009 წლის 17 დეკემბერი.

735 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 2008 წლის 4 დეკემბერი, პუნქტები 119 და 125.

ბის დაცვის უფლებაში. თვალთვალის ან კომუნიკაციაზე მონიტორინგის საშუალებები, როგორიცაა მოსასმენი აპარატები, დაშვებულია მხოლოდ კანონით გათვალისწინებულ შემთხვევებში და როცა აუცილებელია დემოკრატიულ საზოგადოებაში შემდეგი ინტერესების დასაცავად:

- სახელმწიფო უსაფრთხოების დაცვა;
- საზოგადოებრივი უსაფრთხოება;
- სახელმწიფოს მონეტარული ინტერესები;
- სისხლისსამართლებრივი დანაშაულების აღკვეთა;
- მონაცემთა სუბიექტის ან სხვათა უფლებებისა და თავისუფლებების დაცვა.

ECtHR-ს არაერთი გადაწყვეტილება აქვს მიღებული პირადი ცხოვრების ხელშეუხებლობის უფლებაში თვალთვალის გზით ჩარევის კანონიერებაზე.

მაგალითები: საქმეში *Allan v. the United Kingdom*[736] ერთ-ერთმა სახელმწიფო ორგანომ საიდუმლოდ ჩაწერა პატიმრის პირადი საუბრები მეგობართან, შეხვედრებისთვის გამოყოფილ ტერიტორიაზე, და თანაბრალდებულთან - საკანში. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ განმცხადებლის საკანში და შეხვედრებისათვის გამოყოფილ ტერიტორიაზე აუდიო და ვიდეო მოწყობილობების გამოყენება იყო ჩარევა მოსარჩელის პირადი ცხოვრების ხელშეუხებლობის უფლებაში. ვინაიდან იმ დროისათვის არ არსებობდა სამართლებრივი სისტემა, რომელიც დაარეგულირებდა ფარული ჩამწერი მოწყობილობების გამოყენებას პოლიციის მიერ, ასეთი ჩარევა მართლზომიერი არ იყო. ამრიგად, სასამართლომ საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

საქმეში *Roman Zakharov v. Russia*[737] განმცხადებელმა საჩივარი შეიტანა მობილური ქსელის 3 ოპერატორის წინააღმდეგ და მიუთითებდა პირადი ცხოვრების უფლების დარღვევაზე. კერძოდ, აცხადებდა, რომ ოპერატორებმა დაამონტაჟეს გარკვეული მოწყობილობა, რომელიც ფედერალური უსაფრთხოების სამსახურს საშუალებას აძლევდა, მონიტორინგი გაეწია მის სატელეფონო კომუნიკაციებზე, სასამართლოს ნებართვის გარეშე. ECtHR-მა დაადგინა, რომ შიდასახელმწიფოებრივი დებულებები, რომლებიც არეგულირებს კომუნიკაციებზე მონიტორინგს, არ უზრუნველყოფდა სათანადო და ეფექტიან მექანიზმებს თვითნებობისა

736 ECtHR, *Allan v. the United Kingdom,* No. 48539/99, 2002 წლის 5 ნოემბერი.

737 ECtHR, *Roman Zakharov v. Russia,* No. 47143/06, 2015 წლის 4 დეკემბერი.

და ძალაუფლების ბოროტად გამოყენებისგან დასაცავად. კერძოდ, არ ადგენდა შენახული მონაცემების წაშლის მოთხოვნას დასახული მიზნის მიღწევის შემდგომ. ამასთან, მიუხედავად იმისა, რომ აუცილებელი იყო სასამართლოს ნებართვა, მას მხოლოდ შეზღუდული შესაძლებლობა ჰქონდა კონტროლისათვის.

საქმეში *Szabó and Vissy v. Hungary*[738] განმცხადებლები აცხადებდნენ, რომ უნგრეთის კანონმდებლობა ეწინააღმდეგებოდა ევროპული კონვენციის მე-8 მუხლს, ვინაიდან არ იყო საკმარისად დეტალური და ზუსტი; ასევე, არ უზრუნველყოფდა სათანადო გარანტიებს თვითნებობისა და ძალაუფლების ბოროტად გამოყენებისგან დასაცავად. ECtHR-მა დაადგინა, რომ უნგრეთის კანონმდებლობა თვალთვალისთვის ითხოვდა არა სასამართლოს, არამედ იუსტიციის მინისტრის ნებართვას, თუმცა, სამინისტროს ზედამხედველობა აშკარად პოლიტიკური იყო და არ ეყრდნობოდა მკაცრი აუცილებლობის სავალდებულო შეფასებას. ამასთან, ეროვნული კანონმდებლობა არ ითვალისწინებდა სასამართლო გადასინჯვას, რადგან მონაცემთა სუბიექტებს შეტყობინება არ ეგზავნებოდათ. შესაბამისად, სასამართლომ საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

რადგან პოლიციის მიერ მონაცემთა დამუშავებას შეიძლება მნიშვნელოვანი გავლენა ჰქონდეს შესაბამის პირებზე, ამ სფეროში განსაკუთრებულად აუცილებელია მონაცემთა დამუშავების დეტალური წესების არსებობა. ევროპის საბჭოს რეკომენდაცია პოლიციის შესახებ ამ საკითხის მოწესრიგებას ისახავს მიზნად და გასცემს მითითებებს, თუ როგორ უნდა დაიცვან მონაცემთა ფაილები; ვის შეიძლება ჰქონდეს ამ ფაილებზე წვდომა, მათ შორის, რა პირობებს უნდა აკმაყოფილებდეს პერსონალური მონაცემების გადაცემა უცხო ქვეყნის სამართალდამცველი ორგანოებისათვის; როგორ უნდა შეძლონ მონაცემთა სუბიექტებმა თავიანთი უფლებებით სარგებლობა და რა გზით განახორციელონ კონტროლი დამოუკიდებელმა ორგანოებმა. რეკომენდაცია ითვალისწინებს მონაცემთა სათანადო უსაფრთხოების ვალდებულებასაც.

იგი არ ადგენს პერსონალურ მონაცემთა განუსაზღვრელ და განურჩეველ შეგროვებას პოლიციის მიერ და ზღუდავს დამუშავების ფარგლებს იმ დოზით, რომელიც აუცილებელია რეალური საფრთხის ან კონკრეტული სისხლისსამართლებრივი დანაშაულის პრევენციისთვის. მონაცემთა ნებისმიერი დამატებითი დამუშავება უნდა დაეფუძნოს კონკრეტულ ეროვნულ კანონმდებლობას. განსაკუთრებული კატეგორიის მონაცემების დამუშავება საჭიროა მხოლოდ იმ მოცულობით, რომელიც აბსოლუტურად აუცილებელია კონკრეტული გამოძიების პროცესში.

738 ECtHR, *Szabó and Vissy v. Hungary,* No. 37138/14, 2016 წლის 12 იანვარი.

თუ პერსონალური მონაცემები გროვდება მონაცემთა სუბიექტის ინფორმირების გარეშე, მას ამის შესახებ უნდა ეცნობოს, როგორც კი ინფორმაციის გამჟღავნება გამოძიებას ზიანს აღარ მოუტანს. მონაცემთა შეგროვებას ტექნიკური ან სხვა ავტომატიზებული საშუალებებით კონკრეტული სამართლებრივი საფუძველი უნდა ჰქონდეს.

მაგალითი: საქმეში *Versini-Campinchi and Crasnianski v. France*[739] განმცხადებელი იყო ადვოკატი, რომელსაც ერთ-ერთ კლიენტთან ჰქონდა სატელეფონო საუბარი და აღმოჩნდა, რომ კლიენტის სატელეფონო ხაზი, გამომძიებელი მოსამართლის ნებართვის საფუძველზე, ისმინებოდა. სატელეფონო საუბრის ჩანაწერზე დაყრდნობით, დადგინდა, რომ ადვოკატმა გაამჟღავნა კონფიდენციალური ინფორმაცია. პროკურორმა ამის შესახებ შეატყობინა ადვოკატთა საბჭოს, რომელმაც განმცხადებელს დააკისრა სანქცია. ECtHR-მა დაადგინა ჩარევა პირადი ცხოვრებისა და კორესპონდენციის პატივისცემის უფლებაში, არა მხოლოდ იმ პირის წინააღმდეგ, რომლის ტელეფონიც ისმინებოდა, არამედ განმცხადებლის მიმართაც, ვისი კომუნიკაციაც მიყურადების შემდგომ გაშიფრეს. ჩარევა იყო კანონის შესაბამისი და ემსახურებოდა არეულობის პრევენციის ლეგიტიმურ მიზანს. განმცხადებელმა მოითხოვა, შეეფასებინათ, თუ რამდენად კანონიერი იყო მის წინააღმდეგ დაწესებული დისციპლინური წარმოების კონტექსტში სატელეფონო საუბრის ჩანაწერის გადაცემა ადვოკატთა საბჭოსთვის. მიუხედავად იმისა, რომ მან ვერ შეძლო, მოეთხოვა ამ ჩანაწერის ანულირება, ევროპულმა სასამართლომ დაადგინა ეფექტიანი კონტროლის არსებობა, რის საფუძველზეც შესაძლებელი იყო ჩარევის შეზღუდვა დემოკრატიულ საზოგადოებაში აუცილებლობის სტანდარტით. ECtHR-ის განმარტებით, ის არგუმენტი, რომ სატელეფონო საუბრის ჩანაწერის საფუძველზე ადვოკატის წინააღმდეგ სისხლისსამართლებრივი წარმოების აღძვრას ექნებოდა „გამყინავი შედეგი“ ადვოკატსა და კლიენტს შორის კომუნიკაციის თავისუფლებაზე და, ამრიგად, კლიენტის დაცვის უფლებაზეც, საფუძველს იყო მოკლებული, ვინაიდან განმცხადებლის მიერ კონფიდენციალური ინფორმაციის გამჟღავნება სავარაუდო კანონდარღვევაზე მიუთითებდა. შესაბამისად, სასამართლომ დაადგინა, რომ საქმეში კონვენციის მე-8 მუხლი არ დარღვეულა.

ევროპის საბჭოს რეკომენდაცია პოლიციის შესახებ ადგენს, რომ პერსონალური მონაცემების შენახვისას შესაბამისმა უწყებებმა ერთმანეთისგან მკაფიოდ უნდა განარჩიონ ადმინისტრაციული მონაცემები და პოლიციის მონაცემები; მონაცემთა სუბიექტების კატეგორიები (მაგ.: ეჭვმიტანილები, პატიმრები, დაზარალებულები და მოწმეები); ასევე, უტყუარ ფაქტად მიჩნეული და ვარაუდებსა თუ მოსაზრებებზე დაფუძნებული მონაცემები.

739 ECtHR, *Versini-Campinchi and Crasnianski v. France,* No. 49176/11, 2016 წლის 16 ივნისი.

მკაცრად უნდა შეიზღუდოს საპოლიციო მონაცემების გამოყენება. ეს წესი გავლენას ახდენს საპოლიციო მონაცემების მესამე პირებისთვის გადაცემაზე. კერძოდ, მონაცემთა გადაცემა ან გამჟღავნება უნდა დარეგულირდეს იმის მიხედვით, თუ რამდენად არსებობს კანონიერი ინტერესი ინფორმაციის გაზიარებისას. ამგვარი მონაცემების გადაცემა საპოლიციო სექტორს გარეთ ნებადართული უნდა იყოს მხოლოდ კანონით გათვალისწინებული მკაფიო ვალდებულებებიდან გამომდინარე, ან შესაბამისი ნებართვის საფუძველზე.

მაგალითი: საქმეში *Karabeyoğlu v. Turkey*[740] განმცხადებლის სატელეფონო ხაზებზე მონიტორინგი ხორციელდებოდა არალეგალურ ორგანიზაციასთან დაკავშირებული სისხლისსამართლებრივი გამოძიების კონტექსტში. განმცხადებელი ეჭვმიტანილი იყო ამ ორგანიზაციის წევრობასა და დახმარება-მხარდაჭერაში. გამოტანილი გადაწყვეტილების საფუძველზე, დევნა არ დაიწყო, რის შემდეგაც პროკურორმა, რომელიც გამოძიებას ხელმძღვანელობდა, მოპოვებული ჩანაწერები წაშალა. თუმცა, მათი ასლი კვლავ რჩებოდა სასამართლო გამომძიებლებთან, რომლებმაც მასალა შემდგომ განმცხადებლის წინააღმდეგ აღძრული დისციპლინური გამოძიების კონტექსტში გამოიყენეს. ECtHR-მა დაადგინა შესაბამისი კანონმდებლობის დარღვევა, რადგან ინფორმაცია გამოყენებული იყო თავდაპირველი მიზნისგან განსხვავებული ამოცანებით და არ განადგურდა კანონით გათვალისწინებულ ვადაში. დისციპლინურ წარმოებასთან დაკავშირებით კი სასამართლომ დაადგინა, რომ განმცხადებლის პირადი ცხოვრების პატივისცემის უფლებაში ჩარევა არ შეესაბამებოდა კანონს.

მონაცემთა საერთაშორისო გადაცემა ან გამჟღავნება სხვა ქვეყნის სამართალდამცველი ორგანოებისათვის უნდა შეიზღუდოს. მასზე უნდა გავრცელდეს სპეციალური სამართლებრივი რეჟიმი, სავარაუდოდ, საერთაშორისო შეთანხმებები, გარდა იმ შემთხვევისა, როცა გამჟღავნება აუცილებელია სერიოზული და გარდაუვალი საფრთხის პრევენციისათვის.

პოლიციის მიერ მონაცემთა დამუშავებაზე უნდა დაწესდეს დამოუკიდებელი ზედამხედველობა, რათა ის შეესაბამებოდეს მონაცემთა დაცვის ეროვნულ კანონმდებლობას. მონაცემთა სუბიექტებს უნდა მიუწვდებოდეთ ხელი ყველა იმ უფლებაზე, რომლებსაც ითვალისწინებს მოდერნიზებული 108-ე კონვენცია. თუ უფლებებზე წვდომა შეზღუდულია კონვენციის მე-9 მუხლის შესაბამისად (ეფექტიანი გამოძიებისა და სასჯელის აღსრულებისათვის), მონაცემთა სუბიექტს ეროვნული კანონმდებლობით უნდა ჰქონდეს უფლება, ეს გაასაჩივროს მონაცემთა დაცვის საზედამხედველო ან სხვა რომელიმე დამოუკიდებელ ორგანოში, შიდასახელმწიფოებრივ დონეზე.

740 ECtHR, *Karabeyoğlu v. Turkey,* No. 30083/10, 2016 წლის 7 ივნისი.

8.1.2 ბუდაპეშტის კონვენცია კიბერდანაშაულის შესახებ

იმის გათვალისწინებით, რომ დანაშაულებრივი ქმედებებისას სულ უფრო ხშირად გამოიყენება მონაცემთა დამუშავების ელექტრონული სისტემები, ამ გამოწვევის დაძლევა საჭიროებს ახალ სისხლისსამართლებრივ ნორმებს. შესაბამისად, ევროპის საბჭომ მიიღო საერთაშორისო სამართლებრივი ინსტრუმენტი - კონვენცია კიბერდანაშაულის შესახებ, რომელიც ცნობილია ბუდაპეშტის კონვენციის სახელით. მისი მიზანია რეაგირება დანაშაულებზე, რომლებიც ჩადენილია ელექტრონული საშუალებების წინააღმდეგ, ან მათი გამოყენებით.[741] კონვენციაზე მიერთება შეუძლიათ ევროპის საბჭოს არაწევრ ქვეყნებსაც. 2018 წლის დასაწყისში 14 ასეთი ქვეყანა შეუერთდა კონვენციას,[742] ხოლო 7-მა არაწევრმა სახელმწიფომ მიერთების შეთავაზება მიიღო.

კონვენცია კიბერდანაშაულის შესახებ რჩება ყველაზე გავლენიან საერთაშორისო ხელშეკრულებად ინტერნეტსა და სხვა საინფორმაციო ქსელებში ჩადენილ კანონდარღვევებზე. იგი მხარეებს ავალდებულებს სისხლისსამართლებრივი ნორმების განახლებასა და ჰარმონიზებას ჰაკერული თავდასხმებისა და უსაფრთხოების სხვა დარღვევების წინააღმდეგ, როგორიცაა საავტორო უფლებების დაუცველობა, კომპიუტერის გამოყენებით ჩადენილი თაღლითობა, ბავშვთა პორნოგრაფია და სხვა უკანონო კიბერქმედებები. კონვენცია უზრუნველყოფს საერთაშორისო თანამშრომლობის ეფექტიან შესაძლებლობებსაც, მისი დამატებითი ოქმი კი შეეხება რასისტული და ქსენოფობიური პროპაგანდის კრიმინალიზაციას კომპიუტერულ ქსელებში.

მიუხედავად იმისა, რომ კონვენცია არ ისახავს მიზნად მონაცემთა დაცვის ხელშეწყობას, იგი მოიცავს იმ ქმედებათა კრიმინალიზაციას, რომლებიც შეიძლება არღვევდეს მონაცემთა სუბიექტის უფლებას მისი მონაცემების დაცვასთან დაკავშირებით; ასევე, ხელშემკვრელ მხარეებს ავალდებულებს საკანონმდებლო ღონისძიებების მიღებას, რაც სახელმწიფო ორგანოებს მისცემს ინტერნეტტრეფიკისა და შინაარსის მონიტორინგის შესაძლებლობას.[743] კონვენცია ხელშემკვრელ სახელმწიფოებს ავალდებულებს, მისი განხორციელების პროცესში სათანადოდ გაითვალისწინონ ადამიანის უფლებები

741 ევროპის საბჭოს მინისტრთა კომიტეტი (2001), კონვენცია კიბერდანაშაულის შესახებ, CETS No. 185, ბუდაპეშტი, 2001 წლის 23 ნოემბერი, ძალაშია 2004 წლის 1 ივლისიდან.

742 ავსტრალია, კანადა, ჩილე, დომინიკის რესპუბლიკა, ისრაელი, იაპონია, მავრიტისი, პანამა, სენეგალი, შრი ლანკა, ტონგა და აშშ; იხ: 185-ე ხელშეკრულების ხელმოწერებისა და რატიფიკაციების ცხრილი, 2017 წლის ივლისის მონაცემებით.

743 ევროპის საბჭოს მინისტრთა კომიტეტი (2001), კონვენცია კიბერდანაშაულის შესახებ, CETS No. 185, ბუდაპეშტი, 2001 წლის 23 ნოემბერი, მუხლი 20 და 21.

და თავისუფლებები, მათ შორის, გარანტირებული ECHR-ით (მაგ.: მონაცემთა დაცვა).[744] კიბერდანაშაულის კონვენციასთან მიერთება არ საჭიროებს 108-ე კონვენციაზე მიერთებას.

8.2 ევროკავშირის მონაცემთა დაცვის კანონმდებლობა პოლიციისა და სისხლის სამართლის მართლმსაჯულების კონტექსტში

ძირითადი საკითხები

- ვროკავშირის დონეზე, მონაცემთა დაცვას პოლიციისა და სისხლის სამართლის მართლმსაჯულების სექტორში არეგულირებენ წევრი სახელმწიფოებისა და ევროკავშირის პოლიცია და სისხლის სამართლის მართლმსაჯულების ორგანოები, როგორც ეროვნული, ისე საზღვართშორისი დამუშავების კონტექსტში.

- წევრი სახელმწიფოების დონეზე სავალდებულო მოთხოვნაა, პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის განკუთვნილი მონაცემთა დაცვის დირექტივა აისახოს ეროვნულ კანონმდებლობაშიც.

- სამართალდამცველ სფეროში სახელმწიფოთაშორისი თანამშრომლობა, განსაკუთრებით, ტერორიზმსა და საერთაშორისო დანაშაულთან ბრძოლის კუთხით, რეგულირდება სპეციალური სამართლებრივი ინსტრუმენტებით.

- მონაცემთა დაცვის სპეციალური წესები მოქმედებს ევროპის პოლიციის სამსახურისთვის (ევროპოლი), ევროკავშირის იუსტიციის სფეროში თანამშრომლობის უწყებისა (ევროჯასტი) და ევროპის ახლადშექმნილი პროკურატურისთვის. ეს ორგანოები არიან ევროკავშირის უწყებები, რომლებიც ხელს უწყობენ თანამშრომლობას საზღვართშორის სამართალდამცველ სფეროში.

- მონაცემთა დაცვის სპეციალური წესები დადგენილია იმ საერთო საინფორმაციო სისტემებისთვისაც, რომლებიც შექმნილია ევროკავშირის დონეზე ინფორმაციის სახელმწიფოთაშორისი გაცვლის მიზნით პოლიციასა და მართლმსაჯულების ორგანოებს შორის. ამის მნიშვნელოვანი მაგალითებია შენგენის საინფორმაციო სისტემა II (SIS II), სავიზო საინ-

744 *იქვე,* მუხლი 15 (1).

ფორმაციო სისტემა (VIS) და ევროდაკი (Eurodac) - ცენტრალიზებული სისტემა, რომელიც შეიცავს მესამე ქვეყნების იმ მოქალაქეებისა და მოქალაქეობის არმქონე პირების თითის ანაბეჭდებს, რომლებმაც თავშესაფრის თხოვნით მიმართეს ევროკავშირის წევრ სახელმწიფოს.

- ევროკავშირი ამჟამად აახლებს ზემოაღნიშნულ დებულებებს, რათა ისინი შესაბამებოდეს მონაცემთა დაცვის დირექტივას პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის.

8.2.1 მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის

დირექტივა 2016/680/EU უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის, ან სისხლისსამართლებრივი დევნისა და სასჯელის აღსრულების მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკური პირების დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ (მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის) [745] იცავს იმ პერსონალურ მონაცემებს, რომლებიც შეგროვდა და დამუშავდა შემდეგი მიზნებით:

- სისხლის სამართლის დანაშაულების პრევენცია, გამოძიება, გამოვლენა, სისხლისსამართლებრივი დევნა და სასჯელის აღსრულება, მათ შორის, საზოგადოებრივი უსაფრთხოების დაცვა და ასეთი საფრთხის პრევენცია;

- სისხლისსამართლებრივი სასჯელის აღსრულება; და

- პოლიციისა ან სხვა სამართალდამცველი ორგანოების მოქმედება კანონის, საზოგადოების უსაფრთხებისა და ფუნდამენტური უფლებების დასაცავად ისეთი რისკებისგან, რომლებიც შეიძლება გაუტოლდეს სისხლისსამართლებრივ დანაშაულს.

ეს დირექტივა იცავს იმ სხვადასხვა კატეგორიის პირთა პერსონალურ მონაცემებსაც, რომლებიც ჩართულნი არიან სისხლის სამართლის პროცესში (მაგ.: მოწმეები, ინფორმატორები, დაზარალებულები, ეჭვმიტანილები და თანამ-

745 ევროპის პარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680 უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნისა და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ L 119, გვ. 89 (მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის).

ზრახველები). სამართალდამცველ ორგანოებს დირექტივის დებულებების შესრულება ევალებათ მონაცემთა სამართალდამცველი მიზნებით დამუშავებისას, როგორც პერსონალურ, ისე მატერიალურ ნაწილში.[746]

ამავდროულად, გარკვეულ შემთხვევებში ამ მონაცემების გამოყენება ნებადართულია სხვადასხვა მიზნით. მონაცემების დამუშავება იმ მიზნით, რომლის გამოც არ შეგროვებულა, დაშვებულია მხოლოდ მაშინ, როცა დამუშავება კანონიერი, აუცილებელი და პროპორციულია, შიდასახელმწიფოებრივი ან ევროკავშირის კანონმდებლობის შესაბამისად.[747] სხვა მიზნებზე ვრცელდება მონაცემთა დაცვის ზოგადი რეგულაციის წესები. მონაცემთა გაზიარების აღრიცხვა და დოკუმენტირება ერთ-ერთი უფლებამოსილი ორგანოს სპეციალური ფუნქციაა და ხელს უწყობს საჩივრების საფუძველზე წარმოშობილი ვალდებულებების განმარტებას.

პოლიციისა და სისხლის სამართლის მართლმსაჯულების სფეროში უფლებამოსლ ორგანოებად მიიჩნევიან საჯარო ხელისუფლების უწყებები, ან ის ორგანოები, რომელთაც ეროვნული კანონმდებლობით მიენიჭათ საჯარო ხელისუფლების ფუნქციები[748] (მაგ.: სასჯელაღსრულების დაწესებულებები, რომლებსაც კერძო კომპანია მართავს).[749] დირექტივა ვრცელდება მონაცემთა დამუშავებაზე როგორც შიდასახელმწიფოებრივ, ისე სახელმწიფოთაშორის დონეზე, ასევე, სამართალდამცველი ორგანოებისა და ხელისუფლების უფლებამოსილი წარმომადგენლების მიერ მონაცემთა საერთაშორისო გადაცემაზე მესამე ქვეყნისა თუ საერთაშორისო ორგანიზაციებისათვის.[750] იგი არ ვრცელდება ეროვნული უსაფრთხოების სფეროზე, ასევე, პერსონალური მონაცემების დამუშავებაზე ევროკავშირის ინსტიტუტების, უწყებების, ორგანოებისა და სააგენტოების მიერ.[751]

---

746 მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის, მუხლი 2 (1).

747 *იქვე,* მუხლი 4 (2).

748 *იქვე,* მუხლი 3 (7).

749 ევროკომისია (2016), კომისიის მიმართვა ევროპარლამენტისადმი, ევროკავშირის ფუნქციონირების შესახებ ხელშეკრულების 194-ე მუხლის მე-6 პუნქტის შესაბამისად. კომუნიკაცია შეეხება: საბჭოს პოზიციას პერსონალური მონაცემების დამუშვებაზე ისეთი მიზნებით, როგორიცაა უფლებამოსილი ორგანოების მიერ სისხლის სამართლის დანაშაულების პრევენცია, გამოძიება, გამოვლენა, დევნა და სასჯელის აღსრულება; ასევე, ევროპარლამენტისა და საბჭოს დირექტივის მიღებას ამ მონაცემების თავისუფალი მიმოცვლის შესახებ. აღნიშნული დირექტივა აუქმებს საბჭოს ჩარჩო გადაწყვეტილებას 2008/977/JHA, COM(2016) 213, საბოლოო, ბრიუსელი, 2016 წლის 11 აპრილი.

750 მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის, თავი V.

751 *იქვე,* მუხლი 2 (3).

დირექტივა ძირითადად ეყრდნობა იმ პრინციპებსა და განმარტებებს, რომლებსაც შეიცავს მონაცემთა დაცვის ზოგადი რეგულაცია; ამავდროულად, ის ითვალისწინებს სამართალდამცველი სფეროს თავისებურებებს. დირექტივის ფარგლებში, ზედამხედველობას ახორციელებენ წევრი სახელმწიფოების ის ორგანოები, რომლებიც განსაზღვრულია მონაცემთა დაცვის ზოგადი რეგულაციით. დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის ახალი ვალდებულების სახით მოიცავს მონაცემთა დაცვის ოფიცრების დანიშვნასა და მონაცემთა დაცვის რისკების შეფასებას.[752] მიუხედავად იმისა, რომ ამ კონცეფციების შთაგონების წყარო გახლავთ მონაცემთა დაცვის ზოგადი რეგულაცია, დირექტივა ითვალისწინებს პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოთა სპეციფიკურობას. მონაცემების კომერციული მიზნით დამუშავებისგან განსხვავებით, რაც GDPR-ით რეგულირდება, უსაფრთხოებასთან დაკავშირებული დამუშავება, შესაძლოა, გარკვეულ მოქნილობას საჭიროებდეს. მაგალითად, მონაცემთა სუბიექტების იმავე დონით დაცვა, როგორიც გათვალისწინებულია მონაცემთა დაცვის ზოგადი რეგულაციით (ინფორმირების უფლება, პერსონალური მონაცემებზე წვდომისა თუ წაშლის უფლება), ნიშნავს, რომ სამართალდამცველი ორგანოების მხრიდან თვალთვალის ნებისმიერი ქმედება შესაძლოა არაეფექტიანი გახდეს. ამრიგად, დირექტივა არ ითვალისწინებს გამჭვირვალობის პრინციპს. მსგავსად, უსაფრთხოებასთან დაკავშირებული დამუშავების მიმართ მოქნილად უნდა გამოიყენონ მონაცემთა მინიმიზაციისა და მიზნის შეზღუდვის პრინციპები. ეს პრინციპები მოითხოვს პერსონალურ მონაცემთა დამუშავებას კონკრეტული და მკაფიოდ განსაზღვრული მიზნებით და მხოლოდ იმ მოცულობით, რომელიც საჭიროა ამ მიზნების მისაღწევად. უფლებამოსილი ორგანოების მიერ კონკრეტულ შემთხვევაში შეგროვებული და შენახული ინფორმაცია შესაძლოა უაღრესად მნიშვნელოვანი აღმოჩნდეს მომავალში სხვა საქმეების გახსნისათვის.

დამუშავების პრინციპები

მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის ითვალისწინებს უსაფრთხოების რამდენიმე მნიშვნელოვან ზომას პერსონალურ მონაცემთა გამოყენებასთან დაკავშირებით. იგი მკაფიოდ განსაზღვრავს მონაცემთა დამუშავების სახელმძღვანელო პრინციპებს. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ:

- მონაცემთა დამუშავების კანონიერება და სამართლიანობა;
- მონაცემთა შეგროვება კონკრეტული, მკაფიოდ განსაზღვრული და კანონიერი მიზნებით; ასევე, დამუშავების შესაბამისობა ამ მიზნებთან;

752 *იქვე*, შესაბამისად, მუხლები 32 და 27.

- მონაცემთა ადეკვატურობა, რელევანტურობა და პროპორციულობა - იმ მიზნებთან მიმართებით, რისთვისაც მუშავდება;

- მონაცემების სიზუსტე და, საჭიროების შემთხვევაში, განახლება; მონაცემთა დამუშავების მიზნების გათვალისწინებით, ყველა გონივრული ნაბიჯის გადადგმა არაზუსტი მონაცემების წაშლის ან გასწორებისათვის;

- მონაცემების შენახვა იმ ფორმით, რომელიც მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობას იძლევა არაუმეტეს დამუშავების მიზნებისთვის საჭირო დროით;

- მონაცემების დამუშავება ისეთი ტექნიკური თუ ორგანიზაციული ზომების გამოყენებით, რომ სათანადოდ იყოს დაცული, მათ შორის, არასანქცირებული ან უკანონო დამუშავებისგან და შემთხვევითი დაკარგვის, განადგურების ან დაზიანებისგან.[753]

დირექტივის თანახმად, დამუშავება კანონიერია, თუ ხორციელდება იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ფუნქციის შესასრულებლად. ამასთან, მონაცემები უნდა დაამუშაოს უფლებამოსილმა ორგანომ, დირექტივაში მითითებული მიზნების მისაღწევად, და ეფუძნებოდეს ევროკავშირისა და შიდასახელმწიფოებრივ კანონმდებლობას.[754] მონაცემები უნდა შეინახონ მხოლოდ საჭირო დროით, შემდეგ კი წაიშალოს ან, გარკვეული პერიოდულობით, გადაიხედოს. მონაცემები უნდა გამოიყენოს მხოლოდ უფლებამოსილმა ორგანომ, იმ მიზნებით, რომლებისთვისაც შეგროვდა, გადაეცა და გახდა ხელმისაწვდომი.

მონაცემთა სუბიექტის უფლებები

დირექტივით მონაცემთა სუბიექტისთვის გათვალისწინებულია:

- ინფორმაციის მიღების უფლება. წევრმა სახელმწიფომ დამმუშავებელს უნდა დაუწესოს ვალდებულება, რომ მონაცემთა სუბიექტს აცნობოს: ა) დამმუშავებლის ვინაობა და საკონტაქტო ინფორმაცია; 2) მონაცემთა დაცვის ოფიცრის საკონტაქტო ინფორმაცია; 3) დაგეგმილი დამუშავების მიზნები; 4) საზედამხედველო ორგანოში საჩივრის შეტანის უფლება და მისი საკონტაქტო ინფორმაცია; 5) პერსონალურ მონაცემებზე წვდომის, წაშლის, გასწორებისა და დამუშავების შეზღუდვის უფლება.[755] ამასთან,

753 *იქვე,* მუხლი 4 (1).

754 *იქვე,* მუხლი 8.

755 *იქვე,* მუხლი 13 (1).

ზოგად საინფორმაციო მოთხოვნებთან ერთად, დირექტივა ასევე ადგენს, რომ გარკვეულ შემთხვევებში, მონაცემთა სუბიექტის მიერ საკუთარი უფლებებით სარგებლობისათვის, დამმუშავებელი ვალდებულია, მიაწოდოს ინფორმაცია დამუშავების სამართლებრივი საფუძვლის შესახებ, ასევე, თუ როგორ ინახება მონაცემები. როცა პერსონალური მონაცემები გადაეცემა სხვა მიმღებს, მათ შორის, მესამე ქვეყნებსა ან საერთაშორისო ორგანიზაციებს, დამმუშავებელი ვალდებულია, სუბიექტებს მიაწოდოს ინფორმაცია მიმღებთა კატეგორიებზე. და ბოლოს, დამმუშავებელს ევალება დამატებითი ინფორმაციის მიწოდება, მონაცემთა დამუშავების კონკრეტული გარემოებების გათვალისწინებით (მაგ.: როდესაც მონაცემები გროვდება ფარული თვალთვალის შედეგად, ანუ მონაცემთა სუბიექტის ინფორმირების გარეშე). ეს უზრუნველყოფს სამართლიან დამუშავებას მონაცემთა სუბიექტის სასარგებლოდ.[756]

- პერსონალურ მონაცემებზე წვდომის უფლება. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა სუბიექტს შეეძლოს სარგებლობა პერსონალური მონაცემების დამუშავებაზე ინფორმირების უფლებით. დამუშავების შემთხვევაში, მონაცემთა სუბიექტს უნდა ჰქონდეს წვდომა გარკვეულ ინფორმაციაზე (მაგ.: დამუშავებული მონაცემების კატეგორიებზე).[757] ამ უფლების შეზღუდვა შესაძლებელია, თუ ფერხდება გამოძიება ან სისხლისსამართლებრივი დევნა, ანდა ეს საჭიროა საზოგადოებრივი უსაფრთხოების, ასევე, სხვათა უფლებებისა და თავისუფლებების დასაცავად.[758]

- პერსონალური მონაცემების გასწორების უფლება. წევრ სახელმწიფოებს ევალებათ, რომ მონაცემთა სუბიექტებს ყოველგვარი ზედმეტი დაყოვნების გარეშე შეეძლოთ, მოითხოვონ პერსონალურ მონაცემთა გასწორება. ამასთან, მონაცემთა სუბიექტს უნდა შეეძლოს არასრული პერსონალური მონაცემების შევსებაც.[759]

- პერსონალური მონაცემების წაშლისა და დამუშავების შეზღუდვის უფლება. გარკვეულ შემთხვევებში, მონაცემთა დამმუშავებელს მოეთხოვება პერსონალური მონაცემების წაშლა. ამასთან, მონაცემთა სუბიექტს მონაცემების წაშლის მოთხოვნა შეუძლია მხოლოდ მათი უკანონო დამუშავების შემთხვევაში.[760] პერსონალური მონაცემების დამუშავება შეიძლება

756 *იქვე,* მუხლი 13 (2).

757 *იქვე,* მუხლი 14.

758 *იქვე,* მუხლი 15.

759 *იქვე,* მუხლი 16 (1).

760 *იქვე,* მუხლი 16 (2).

> შეიზღუდოს, ნაცვლად წაშლისა, თუ: (1) მონაცემების სიზუსტე გასაჩივრებულია, მაგრამ შეუძლებელია პასუხის დადგენა; (2) პერსონალური მონაცემები საჭიროა მტკიცებულების სახით.[761]

როცა დამმუშავებელი უარს აცხადებს პერსონალური მონაცემების გასწორებაზე, წაშლასა ან დამუშავების შეზღუდვაზე, მონაცემთა სუბიექტს ეს წერილობით უნდა ეცნობოს. წევრ სახელმწიფოებს შეუძლიათ, შეზღუდონ ინფორმაციის მიღების უფლება, იმავე მიზეზებით, რომლებისთვისაც იზღუდება წვდომა (მათ შორის, საზოგადოებრივი უსაფრთხოების, ასევე, სხვათა უფლებებისა და თავისუფლებების დასაცავად).[762]

როგორც წესი, მონაცემთა სუბიექტს უფლება აქვს, მიიღოს ინფორმაცია მისი პერსონალური მონაცემების დამუშავებაზე; ასევე, მოითხოვოს მათი წვდომა, გასწორება, წაშლა ან დამუშავების შეზღუდვა, რაზეც შეუძლია უშუალოდ მონაცემთა დამმუშავებელს მიმართოს. ამავდროულად, დირექტივით ნებადართულია მონაცემთა სუბიექტების უფლებათა ირიბი განხორციელება, საზედამხედველო ორგანოს საშუალებით. ეს შესაძლებლობა აქტიურდება, როდესაც მონაცემთა დამმუშავებელი ზღუდავს მონაცემთა სუბიექტის უფლებას.[763] დირექტივის მე-17 მუხლი წევრ სახელმწიფოებს ავალდებულებს იმ ღონისძიებათა გატარებას, რომლებიც უზრუნველყოფს მონაცემთა სუბიექტების უფლებათა განხორციელებას საზედამხედველო ორგანოების საშუალებით. სწორედ ამიტომ, დამმუშავებელი ვალდებულია, მონაცემთა სუბიექტს შეატყობინოს ირიბი წვდომის შესაძლებლობა.

მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის მოვალეობები

პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოების მიერ მონაცემთა დაცვის დირექტივის კონტექსტში, დამმუშავებელი არის საჯარო უწყება ან სხვა ტიპის ორგანო, რომელსაც აქვს შესაბამისი უფლებამოსილება და განსაზღვრავს პერსონალურ მონაცემთა დამუშავების მიზნებსა და საშუალებებს. დირექტივა მონაცემთა დამმუშავებლისთვის ადგენს რამდენიმე ვალდებულებას სამართალდამცველი მიზნებით დამუშავებული პ ერსონალური მონაცემების მაღალ დონეზე დაცვის შესახებ.

შესაბამისი ორგანოები ვალდებულნი არიან, აღრიცხონ დამუშავების ის ოპერაციები, რომლებსაც ახორციელებენ ავტომატიზებული სისტემების ფარგლებში, ასევე, პერსონალური მონაცემების შეგროვება, გასწორება, გაცნობა

761 *იქვე,* მუხლი 16 (3).

762 *იქვე,* მუხლი 16 (4).

763 *იქვე,* მუხლი 17.

და გამჟღავნება, გადაცემის, კომბინირებისა და წაშლის ჩათვლით.[764] დირექტივის თანახმად, მიმართვისა და გამჟღავნების ჩანაწერებში უნდა მიეთითოს ოპერაციის განხორციელების დრო/თარიღი და საფუძველი. ჩანაწერები უნდა იძლეოდეს პერსონალურ მონაცემთა მიმღებისა და იმ პირის იდენტიფიცირების შესაძლებლობას, რომელიც გაეცნო მონაცემებს ან გაამჟღავნა ისინი. ჩანაწერების გამოყენება ნებადართულია მხოლოდ დამუშავების კანონიერების შესაფასებლად, თვითმონიტორინგის, პერსონალური მონაცემების მთლიანობის, უსაფრთხოებისა და სისხლისსამართლებრივი წარმოებისთვის.[765] საზედამხედველო ორგანოს მოთხოვნის საფუძველზე, მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს ევალებათ ჩანაწერების წარმოდგენა.

მონაცემთა დამმუშავებელს ეკისრება სათანადო ტექნიკური ან ორგანიზაციული ღონისძიებების გატარების ზოგადი ვალდებულება, რათა დამუშავება შეესაბამებოდეს დირექტივას და მან შეძლოს პროცესის კანონიერების დადასტურება.[766] ასეთი ღონისძიებების შექმნისას, დამმუშავებელი ვალდებულია, გაითვალისწინოს პროცესის ბუნება, მასშტაბი, კონტექსტი და, რაც მთავარია, ნებისმიერი საფრთხე, რომელიც შეიძლება დაემუქროს ფიზიკური პირის უფლებებსა და თავისუფლებებს. დამმუშავებელმა უნდა მიიღოს ისეთი შიდა პოლიტიკა და ზომები, რომლებიც ხელს უწყობს მონაცემთა დაცვის პრინციპებთან შესაბამისობას (მაგ.: მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (by design) და მონაცემთა დაცვა პირველად პარამეტრად (by default)).[767] თუ სავარაუდოა, რომ დამუშავება დიდ რისკს შეუქმნის ფიზიკურ პირთა უფლებებს (მაგ.: ახალი ტექნოლოგიების გამოყენების გამო), დამმუშავებელი ვალდებულია, პროცესის დაწყებამდე შეაფასოს მონაცემთა დაცვის რისკები.[768] დირექტივაში წარმოდგენილია იმ ღონისძიებათა ჩამონათვალიც, რომლებიც დამმუშავებელმა უნდა განახორციელოს პროცესის უსაფრთხოებისათვის. ეს მოიცავს პერსონალურ მონაცემებზე არაავტორიზებული წვდომის პრევენციას, ასევე, დამუშავების სისტემის სათანადო ფუნქციონირებას, რათა მონაცემებზე წვდომა ჰქონდეთ მხოლოდ ავტორიზებულ პირებს და გამოირიცხოს შენახული პერსონალური მონაცემების დაზიანება სისტემის მოშლის შემთხვევაში.[769] დამმუშავებელი ვალდებულია, პერსონალური მონაცემების უსაფრთხოების დარღვევა სამი დღის ვადაში აცნობოს საზედამხედველო ორგანოს. შეტყობინება უნდა აღწერდეს დარღვევის სახეს, შესაძლო შედეგებს, პერსონალური

764 *იქვე,* მუხლი 25 (1).

765 *იქვე,* მუხლი 25 (2).

766 *იქვე,* მუხლი 19

767 *იქვე,* მუხლი 20.

768 *იქვე,* მუხლი 27.

769 *იქვე,* მუხლი 29.

მონაცემების კატეგორიას, რომელთა უსაფრთხოებაც დაირღვა, და იმ სუბიექტების მიახლოებით რაოდენობას, რომლებზეც დარღვევამ გავლენა იქონია. მონაცემთა სუბიექტს დარღვევაზე შეტყობინება უნდა გაეგზავნოს „ზედმეტი დაყოვნების“ გარეშე, თუკი სავარაუდოა, რომ ეს დიდ საფრთხეს შეუქმნის მის უფლებებსა და თავისუფლებებს.[770]

დირექტივა შეიცავს ანგარიშვალდებულების პრინციპებს და მონაცემთა დამმუშავებელი ვალდებულია, მიიღოს ზომები ამ პრინციპებთან შესაბამისობისათვის. დამმუშავებელმა უნდა აღრიცხოს პროცესთან დაკავშირებულ აქტივობათა ყველა კატეგორია. ამ ჩანაწერებზე დეტალური ინფორმაცია წარმოდგენილია დირექტივის 24-ე მუხლში. ჩანაწერები საზედამხედველო ორგანოს მოთხოვნისთანავე უნდა წარედგინოს, რათა მან შეძლოს მონიტორინგი მონაცემთა დამმუშავებლის საქმიანობაზე. კიდევ ერთი მნიშვნელოვანი საშუალება ანგარიშვალდებულების გასაუმჯობესებლად გახლავთ მონაცემთა დაცვის ოფიცერი. დამმუშავებელი ვალდებულია, დანიშნოს ის, თუმცა, დირექტივა წევრ სახელმწიფოებს საშუალებას აძლევს, ასეთი ვალდებულება არ გაავრცელოს სასამართლოებსა და მართლმსაჯულების სხვა დამოუკიდებელ ორგანოებზე. მონაცემთა დაცვის ოფიცრის მოვალეობები ზოგადი რეგულაციით გათვალისწინებული ვალდებულებების იდენტურია.[771] ოფიცერი მონიტორინგს უწევს დირექტივასთან შესაბამისობას, უზრუნველყოფს ინფორმაციის მიწოდებას და კონსულტაციას უწევს იმ თანამშრომლებს, რომლებიც ამუშავებენ მონაცემებს მონაცემთა დაცვის კანონმდებლობის საფუძველზე. მონაცემთა დაცვის ოფიცერი გასცემს რჩევას რისკების შეფასებაზეც და საზედამხედველო ორგანოს საკონტაქტო პირია.

მონაცემთა გადაცემა მესამე ქვეყნისა თუ საერთაშორისო ორგანიზაციისთვის

მონაცემთა დაცვის ზოგადი რეგულაციის მსგავსად, დირექტივა ადგენს გარკვეულ პირობებს მონაცემთა მესამე ქვეყნისა თუ საერთაშორისო ორგანიზაციისათვის გადასაცემად. ევროკავშირის იურისდიქციის გარეთ მონაცემთა თავისუფალი, შეუზღუდავი გადაცემით შეიძლება საფრთხე დაემუქროს გაერთიანების კანონმდებლობით გათვალისწინებულ დაცვის მექანიზმებს. ამავდროულად, მონაცემთა მესამე ქვეყნისა თუ საერთაშორისო ორგანიზაციისთვის გადაცემა განსხვავდება ზოგადი რეგულაციით დადგენილი პირობებისგან. კერძოდ, ეს ნებადართულია, როცა:[772]

770 *იქვე,* მუხლი 30 და 31.

771 *იქვე,* მუხლი 32.

772 *იქვე,* მუხლი 35.

- აუცილებელია დირექტივის ამოცანებისთვის;

- პერსონალური მონაცემები გადაეცემა უფლებამოსილ ორგანოს, დირექტივის მნიშვნელობის ფარგლებში, ასევე, მესამე ქვეყანას ან საერთაშორისო ორგანიზაციას (თუმცა, გარკვეულ შემთხვევებში, დაშვებულია გამონაკლისები);[773]

- საზღვართშორისი თანამშრომლობის ფარგლებში მიღებული პერსონალური მონაცემების გადაცემა მესამე ქვეყნის ან საერთაშორისო ორგანიზაციისთვის საჭიროებს იმ წევრი სახელმწიფოს ავტორიზაციას, სადაც ეს მონაცემები წარმოიშვა (თუმცა, გადაუდებელი აუცილებლობის შემთხვევაში, დაშვებულია გამონაკლისები).

- ევროპის კომისიას მიღებული აქვს შესაბამისობის გადაწყვეტილება, შექმნილია დაცვის სათანადო საშუალებები, ან სახეზეა საგამონაკლისო შემთხვევა;

- პერსონალური მონაცემების შემდგომი (მეორადი) გადაცემა მესამე ქვეყნის ან საერთაშორისო ორგანიზაციისათვის საჭიროებს წინასწარ ავტორიზაციას უფლებამოსილი ორგანოს მხრიდან. ავტორიზაცია გაიცემა დანაშაულის სიმძიმისა და მიმღებ ქვეყანაში მონაცემთა დაცვის მდგომარეობის გათვალისწინებით.[774]

დირექტივის თანახმად, პერსონალური მონაცემების გადაცემა შესაძლებელია, თუ სახეზეა სამიდან ერთ-ერთი პირობა. პირველი პირობაა, რომ ევროპულ კომისიას დირექტივის თანახმად მიღებული აქვს შესაბამისობის გადაწყვეტილება. გადაწყვეტილება, შესაძლოა, ვრცელდებოდეს მესამე ქვეყნის მთლიან ტერიტორიაზე, ან ქვეყნისა თუ საერთაშორისო ორგანიზაციის კონკრეტულ სექტორზე. გასათვალისწინებელია, რომ კომისია შესაბამისობის გადაწყვეტილებას იღებს მაშინ, როცა უზრუნველყოფილია დაცვის სათანადო დონე და პირობები, დირექტივის შესაბამისად.[775] ასეთ დროს, პერსონალური მონაცემების გადაცემისთვის წევრი სახელმწიფოების ავტორიზაცია საჭირო არ არის.[776] ევროპული კომისია აკვირდება მოვლენებს, რომლებმაც შეიძლება გავლენა იქონიოს შესაბამისობის გადაწყვეტილების აღსრულებაზე. ამასთან, გადაწყვეტილება უნდა მოიცავდეს პერიოდული გადახედვის მექანიზმს. კომისიას უფლება აქვს, გააუქმოს შეასწოროს ან დროებით შეაჩეროს

773 *იქვე,* მუხლი 39.

774 *იქვე,* მუხლი 35 (1).

775 *იქვე,* მუხლი 36.

776 *იქვე,* მუხლი 36 (1).

გადაწყვეტილება, თუ არსებულ ინფორმაციაზე დაყრდნობით, მესამე ქვეყანაში ან საერთაშორისო ორგანიზაციაში მონაცემები სათანადო დონეზე არ არის დაცული. ასეთ დროს კომისია კონსულტაციებს იწყებს მათთან, არსებული მდგომარეობის გამოსასწორებლად.

შესაბამისობის გადაწყვეტილების არარსებობისას, გადაცემა შეიძლება დაეფუძნოს დაცვის სათანადო გარანტიებს. მათ ადგენს იურიდიულად სავალდებულო ძალის მქონე ინსტრუმენტი, ან მონაცემთა დამმუშავებელი, რომელიც აფასებს პერსონალურ მონაცემთა გადაცემასთან დაკავშირებულ გარემოებებს. შეფასება უნდა ითვალისწინებდეს მესამე ქვეყანასა და ევროპოლს ან ევროჯასტს შორის გაფორმებულ შეთანხმებებს, კონფიდენციალობის ვალდებულებებსა და მიზნის შეზღუდვის პრინციპებს, ასევე, გარანტიებს, რომ მონაცემებს არ გამოიყენებენ რაიმე სახის სასტიკი ან არაჰუმანური მოპყრობის მიზნით, მათ შორის, სიკვდილით დასჯისთვის.[777] შესაბამისობის გადაწყვეტილების არარსებობისას მონაცემთა გადაცემის შემთხვევაში, დამმუშავებელი ვალდებულია, საზედამხედველო ორგანოს გაუგზავნოს შეტყობინება გადასაცემი მონაცემების კატეგორიებზე.[778]

როცა არ არსებობს შესაბამისობის გადაწყვეტილება და დაცვის სათანადო გარანტიები, მონაცემთა გადაცემა დაშვებულია მხოლოდ დირექტივით გათვალისწინებულ კონკრეტულ შემთხვევებში, როგორიცაა: მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დაცვა; წევრ სახელმწიფოსა ან მესამე ქვეყანაში საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვა და მათი პრევენცია.[779]

ინდივიდუალურ და კონკრეტულ საქმეებში, უფლებამოსილი ორგანოს მიერ მონაცემთა გადაცემა მესამე ქვეყანაში არსებული მიმღებისთვის, რომელიც არ არის უფლებამოსილი ორგანო, ნებადართულია, თუ ზემოთ ჩამოთვლილ პირობებთან ერთად, დაცულია დირექტივის 39-ე მუხლით გათვალისწინებული პირობებიც. კერძოდ, გადაცემა მკაცრად აუცილებელი უნდა იყოს გადამცემი უფლებამოსილი ორგანოს ფუნქციათა შესასრულებლად. ამასთან, ეს ორგანო უნდა დარწმუნდეს, რომ ფიზიკურ პირთა უფლებები და თავისუფლებები არ გადაწონის საზოგადო ინტერესს, რომელიც მონაცემთა გადაცემის საფუძველია. ასეთ შემთხვევებში, აუცილებელია მონაცემთა გადაცემის დოკუმენტირება, ხოლო გადამცემმა უფლებამოსილმა ორგანომ შესაბამისი შეტყობინება უნდა გაუგზავნოს კომპეტენტურ საზედამხედველო ორგანოს.[780]

777 *იქვე,* პრეამბულა, პუნქტი 71.

778 *იქვე,* მუხლი 37 (1).

779 *იქვე,* მუხლი 38 (1).

780 *იქვე,* მუხლი 37 (3).

და ბოლოს, მესამე ქვეყნებსა და საერთაშორისო ორგანიზაციებთან დაკავშირებით, დირექტივა ადგენს მოთხოვნას საერთაშორისო თანამშრომლობის მექანიზმთა შემუშავებაზე, რომელიც ხელს უწყობს კანონმდებლობის ეფექტიან აღსრულებას და, შესაბამისად, მონაცემთა დაცვის საზედამხედველო ორგანოების თანამშრომლობას უცხოელ კოლეგებთან.[781]

დამოუკიდებელი ზედამხედველობა და მონაცემთა სუბიექტის დაცვის საშუალებები

თითოეული წევრი სახელმწიფო ვალდებულია, დირექტივის შესაბამისად მიღებული დებულებების გამოყენებაზე კონსულტაციისა და მონიტორინგის პასუხისმგებლობა დააკისროს ერთ ან რამდენიმე დამოუკიდებელ საზედამხედველო ორგანოს.[782] დირექტივის მიზნებით შექმნილი საზედამხედველო ორგანო შესაძლოა იყოს ის ორგანო, რომელიც ჩამოყალიბდა მონაცემთა დაცვის ზოგადი რეგულაციის ამოცანებისთვის. თუმცა, წევრ სახელმწიფოს უფლება აქვს, ამისთვის ცალკე ორგანო გამოყოს, თუკი ის დამოუკიდებლობის კრიტერიუმებს დააკმაყოფილებს. საზედამხედველო ორგანომ უნდა განიხილოს ნებისმიერი პირის საჩივარი, რომელიც ეხება მისი უფლებებისა და თავისუფლებების დაცვას შესაბამისი ორგანოების მიერ პერსონალური მონაცემების დამუშავებისას.

თუ მონაცემთა სუბიექტის უფლებები შეიზღუდება დამაჯერებელი საფუძვლით, მას უნდა მიენიჭოს კომპეტენტურ საზედამხედველო ორგანოში და/ან სასამართლოში გასაჩივრების უფლება, ეროვნულ დონეზე. როცა პირს ზიანი მიადგება დირექტივის განმახორციელებელი ეროვნული კანონმდებლობის დარღვევით, მას უფლება აქვს, მიიღოს კომპენსაცია მონაცემთა დამმუშავებლისა ან წევრი სახელმწიფოს კანონმდებლობით განსაზღვრული ნებისმიერი სხვა კომპეტენტური ორგანოსგან.[783] ზოგადად, მონაცემთა სუბიექტს ხელი უნდა მიუწვდებოდეს სამართლებრივი დაცვის საშუალებაზე იმ უფლებების ნებისმიერ დარღვევასთან დაკავშირებით, რომლებიც გარანტირებულია დრიექტივის დამნერგავი ეროვნული კანონმდებლობით.[784]

781 *იქვე,* მუხლი 40.

782 *იქვე,* მუხლი 41.

783 *იქვე,* მუხლი 56.

784 *იქვე,* მუხლი 54.

8.3 სამართალდამცველ სფეროში მონაცემთა დაცვის სხვა სპეციფიკური სამართლებრივი ინსტრუმენტები

გარდა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისთვის შექმნილი მონაცემთა დაცვის დირექტივისა, წევრი სახელმწიფოების მიერ კონკრეტულ სფეროებში დაცული ინფორმაციის გაცვლას არეგულირებს არაერთი სამართლებრივი ინსტრუმენტი, მათ შორის: საბჭოს ჩარჩო გადაწყვეტილება 2009/315/JHA წევრ სახელმწიფოებს შორის დანაშაულებზე ჩანაწერების გაცვლისას ამოღებული ინფორმაციის ორგანიზებასა და შინაარსზე; საბჭოს გადაწყვეტილება 2000/642/JHA წევრი სახელმწიფოების ფინანსური სადაზვერვო განყოფილებების თანამშრომლობაზე ინფორმაციის გაცვლის მხრივ; და 2006 წლის 18 დეკემბრის საბჭოს ჩარჩო გადაწყვეტილება 2006/960/JHA, რომელიც შეეხება ევროკავშირის წევრი სახელმწიფოების სამართალდამცველ ორგანოებს შორის ინფორმაციისა და დაზვერვის მონაცემების გაცვლის გამარტივებას.[785]

აღსანიშნავია, რომ უფლებამოსილ ორგანოებს შორის საერთაშორისო თანამშრომლობა[786] სულ უფრო მეტად ითვალისწინებს საიმიგრაციო მონაცემების გაცვლას. ეს სფერო არ მიეკუთვნება პოლიციისა და სისხლის სამართლის მართლმსაჯულებას, თუმცა, მოიცავს ბევრ ისეთ საკითხს, რომლებიც რელევანტურია პოლიციისა და სამართალდამცველი ორგანოების საქმიანობისთვის. იგივე ითქმის ევროკავშირში იმპორტირებული ან ევროკავშირიდან ექსპორტირებული საქონლის მონაცემებზეც. ევროკავშირში შიდა სასაზღვრო კონტროლის გაუქმებამ გაზარდა თაღლითობის რისკი, რის გამოც აუცილებელი გახდა წევრი ქვეყნების მიერ თანამშრომლობის გაძლიერება, ძირითადად, ინფორმაციის საერთაშორისო გაცვლის განმტკიცებით, რათა ეფექტიანად გამოვლინდეს ეროვნული და ევროკავშირის დონეზე მოქმედი საბაჟო კანონმდებლობის დარღვევები და დაიწყოს დევნა. ამასთან, მძიმე და ორგანიზებული დანაშაულებისა და ტერორიზმის მაჩვენებელი ბოლო წლებში მსოფლიო მასშტაბით გაიზარდა, რაც შესაძლოა უკავშირდებოდეს საერთაშორისო მოგ-

785 ევროკავშირის საბჭოს 2009 წლის 26 თებერვლის ჩარჩო გადაწყვეტილება 2009/315/JHA წევრ სახელმწიფოებს შორის სისხლისსამართლებრივი ჩანაწერების გაცვლისას ამოღებული ინფორმაციის ორგანიზებასა და შინაარსზე, OJ 2009 L 93; საბჭოს 2000 წლის 17 ოქტომბრის გადაწყვეტილება 2000/642/JHA წევრი ქვეყნების ფინანსური სადაზვერვო განყოფილებების თანამშრომლობაზე ინფორმაციის გაცვლის მხრივ, OJ 2000 L 271; საბჭოს 2006 წლის 18 დეკემბრის ჩარჩო გადაწყვეტილება 2006/960/JHA ევროკავშირის წევრი სახელმწიფოების სამართალდამცველ ორგანოებს შორის ინფორმაციისა და დაზვერვის მონაცემების გაცვლის გამარტივებაზე, OJ L 386.

786 ევროპული კომისიის მიმართვა ევროპულ პარლამენტსა და საბჭოს – სამართალდამცავი თანამშრომლობის გაძლიერება ევროპულ კავშირში: საინფორმაციო გაცვლის ევროპული მოდელი (EIXM), COM(2012) 735, საბოლოო, ბრიუსელი, 7 დეკემბერი 2012 წელი.

ზაურობას. ამის საფუძველზე ნათელი გახდა, რომ არაერთი საქმე მოითხოვს საზღვართშორის თანამშრომლობას პოლიციასა და სამართალდამცველ ორგანოებს შორის.[787]

პრუმის გადაწყვეტილება

ეროვნულ დონეზე არსებული მონაცემების გაზიარებით ინსტიტუციონალიზებული საერთაშორისო თანამშრომლობის მნიშვნელოვანი მაგალითია საბჭოს გადაწყვეტილება 2008/615/JHA და მისი დამნერგავი დებულებები. იგი შეეხება საერთაშორისო თანამშრომლობის გაძლიერებას, ძირითადად, ტერორიზმსა და საერთაშორისო დანაშაულთან ბრძოლის კუთხით (პრუმის გადაწყვეტილება). გადაწყვეტილების საფუძველზე პრუმის შეთანხმება 2008 წელს ჩაერთო ევროკავშირის კანონმდებლობაში.[788] პოლიციის ასეთ საერთაშორისო თანამშრომლობაზე შეთანხმებას 2005 წელს ხელი მოაწერეს შემდეგმა ქვეყნებმა: ავსტრია, ბელგია, საფრანგეთი, გერმანია, ლუქსემბურგი, ნიდერლანდები და ესპანეთი.[789]

გადაწყვეტილების მიზანია, ევროკავშირის წევრ ქვეყნებს დაეხმაროს ინფორმაციის გაზიარებაში დანაშაულის პრევენციისა და ბრძოლის მიზნებით, კერძოდ, შემდეგ სამ სფეროში: ტერორიზმი, საერთაშორისო დანაშაული და არალეგალური მიგრაცია. ამისათვის გადაწყვეტილება ადგენს დებულებებს, რომლებიც ეხება შემდეგ საკითხებს:

- ავტომატიზებული წვდომა დნმ-ის, თითის ანაბეჭდებისა და სატრანსპორტო საშუალებების სარეგისტრაციო შიდასახელმწიფოებრივ მონაცემებზე;

- მონაცემთა მიწოდება იმ ძირითად მოვლენებზე, რომლებსაც აქვს საერთაშორისო მასშტაბი;

787 ევროპული კომისია (2011), წინადადება ევროპარლამენტისა და საბჭოს დირექტივის შესახებ, რომელიც შეეხება PNR მონაცემების გამოყენებას ტერორისტული და მძიმე დანაშაულების პრევენციის, გამოვლენის, გამოძიებისა და დამნაშავეთა დასჯის მიზნით, COM(2011) 32, საბოლოო, ბრიუსელი, 2011 წლის 2 თებერვალი, გვ. 1.

788 ევროკავშირის საბჭო (2008), საბჭოს 2008 წლის 23 ივნისის გადაწყვეტილება 2008/615/JHA, რომელიც შეეხება საერთაშორისო თანამშრომლობის გააქტიურებას, განსაკუთრებით, ტერორიზმსა და სახელმწიფოთაშორის დანაშაულთან ბრძოლის მიზნით, OJ 2008 L 210.

789 კონვენცია ბელგიის სამეფოს, გერმანიის ფედერაციულ რესპუბლიკას, ესპანეთის სამეფოს, საფრანგეთის რესპუბლიკას, ლუქსემბურგის დიდ საჰერცოგოს, ნიდერლანდების სამეფოსა და ავსტრიის რესპუბლიკას შორის სახელმწიფოთაშორისი თანამშრომლობის გაძლიერებაზე, ტერორიზმთან, საერთაშორისო დანაშაულსა და არალეგალურ მიგრაციასთან ბრძოლის მხრივ.

- ინფორმაციის მიწოდება ტერორისტული აქტების პრევენციისთვის;
- სხვა ზომები, რომლებიც აძლიერებს პოლიციის თანამშრომლობას საერთაშორისო კონტექსტში.

პრუმის გადაწყვეტილების ფარგლებში ხელმისაწვდომი მონაცემთა ბაზები რეგულირდება მთლიანად შიდასახელმწიფოებრივი კანონმდებლობით, ხოლო მონაცემთა გაცვლა დამატებით წესრიგდება გადაწყვეტილებით, რომლის შესაბამისობა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისთვის შექმნილ მონაცემთა დაცვის დირექტივასთან, უნდა შეფასდეს. მონაცემთა დაცვის ეროვნული საზედამხედველო ორგანო არის ის კომპეტენტური ორგანო, რომელიც აღნიშნული მონაცემების მიმოცვლას უწევს ზედამხედველობას.

ჩარჩო გადაწყვეტილება 2006/960/JHA – შვედეთის ინიციატივა

სამართალდამცველი ორგანოების მიერ მონაცემთა გაცვლის კუთხით, საერთაშორისო თანამშრომლობის კიდევ ერთი მაგალითია ჩარჩო გადაწყვეტილება 2006/960/JHA (შვედეთის ინიციატივა).[790] იგი შეეხება სადაზვერვო მონაცემებისა და ინფორმაციის გაზიარებას და ადგენს მონაცემთა დაცვის კონკრეტულ წესებს (მუხლი 8).

ამ ინსტრუმენტის თანახმად, გაზიარებული ინფორმაციისა და დაზვერვის მონაცემების გამოყენება უნდა დარეგულირდეს ინფორმაციის მიმღები წევრი სახელმწიფოს მონაცემთა დაცვის დებულებებით, იმავე წესების შესაბამისად, რომლებიც ეხება აღნიშნულ სახელმწიფოში შეგროვებულ მონაცემებს. დამატებით, მე-8 მუხლი აცხადებს, რომ ინფორმაციისა და სადაზვერვო მონაცემების გადაცემისას, სამართალდამცველ უწყებას უფლება აქვს, დაადგინოს ეროვნული კანონმდებლობის შესაბამისი პირობები გადაცემული მონაცემების გამოყენებაზე მიმღები სამართალდამცველი ორგანოს მიერ.

ეს პირობები ასევე ვრცელდება სისხლისსამართლებრივი გამოძიების შედეგებსა ან იმ სადაზვერვო ოპერაციებზე, რომლებისთვისაც აუცილებელია ინფორმაციისა და მონაცემების გაცვლა. ამავდროულად, თუ შიდასახელმწიფოებრივი კანონმდებლობა ითვალისწინებს გამოყენების შეზღუდვასთან დაკავშირებულ გამონაკლისებს (მაგ.: სასამართლო ან საკანონმდებლო ორგანოებისათვის და ა.შ.), ინფორმაციისა და დაზვერვის მონაცემების გამოყენება

790 ევროკავშირის საბჭო (2006), საბჭოს 2006 წლის 18 დეკემბრის ჩარჩო გადაწყვეტილება 2006/960/JHA, რომელიც შეეხება წევრი სახელმწიფოების სამართალდამცველ ორგანოებს შორის ინფორმაციისა და დაზვერვის მონაცემების გაცვლის გამარტივებას, OJ L 386/89, 2006 წლის 29 დეკემბერი.

შესაძლებელია მხოლოდ წინასწარი კონსულტაციის - საფუძველზე იმ წევრ სახელმწიფოსთან, რომელიც გადასცემს მონაცემებს.

ინფორმაციისა და დაზვერვის მონაცემების გამოყენება ნებადართულია:

- იმ მიზნისთვის, რომლის გამოც ისინი გადაეცა; ან
- საზოგადოებრივი უსაფრთხოების მოსალოდნელი და სერიოზული საფრთხის თავიდან ასაცილებლად.

სხვა მიზნებით დამუშავება ნებადართულია წინასწარი კონსულტაციის საფუძველზე იმ წევრ სახელმწიფოსთან, რომელიც გადასცემს მონაცემებს.

შვედეთის ინიციატივა დამატებით განმარტავს, რომ აუცილებელია დამუშავებული პერსონალური მონაცემების დაცვა ისეთი ინსტრუმენტებით, როგორიცაა:

- ევროპის საბჭოს კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ; [791]
- კონვენციის 2001 წლის 8 ნოემბრის დამატებითი ოქმი, რომელიც შეეხება საზედამხედველო ორგანოებსა და მონაცემთა საერთაშორისო მიმოცვლას;[792]
- ევროპის საბჭოს რეკომენდაცია No. R(87) 15, რომელიც არეგულირებს პერსონალური მონაცემების გამოყენებას პოლიციის სექტორში.[793]

ევროკავშირის PNR დირექტივა

მგზავრთა პირადი მონაცემები (PNR) შეეხება ავიამგზავრთა მონაცემებს, რომლებიც გროვდება და ინახება ავიაკომპანიის ჯავშნებისა და გამგზავრების კონტროლის სისტემებში, კომერციული მიზნებით. ეს მონაცემები შეიცავს რამდენიმე ტიპის ინფორმაციას (მაგ.: მოგზაურობის თარიღები, მარშრუტი,

791 ევროპის საბჭო (1981), კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, ETS n. 108.

792 ევროპის საბჭო (2001), კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, დამატებითი პროტოკოლი, რომელიც შეეხება საზედამხედველო ორგანოებსა და მონაცემთა საზღვართშორის მიმოცვლას, ETS n. 108.

793 ევროპის საბჭო (1987), მინისტრთა კომიტეტის რეკომენდაცია წევრი სახელმწიფოებისთვის No. R (87) 15, პოლიციის სექტორში პერსონალური მონაცემების გამოყენების რეგულირებასთან დაკავშირებით (მიღებულია მინისტრთა კომიტეტის მიერ, 1987 წლის 17 სექტემბერს, მინისტრის მოადგილეების დონეზე გამართულ 410-ე შეხვედრაზე).

ბილეთის შესახებ ინფორმაცია, საკონტაქტო დეტალები, ტურისტული სააგენტო, რომელმაც დაჯავშნა ფრენა, გამოყენებული გადახდის საშუალებები, ადგილის ნომერი და ბარგზე ინფორმაცია).[794] PNR-ის დამუშავება შეიძლება დაეხმაროს სამართალდამცველ ორგანოებს მათთვის ცნობილი ან პოტენციური ეჭვმიტანილების იდენტიფიცირებაში, ასევე, შეფასებების განხორციელებაში იმ სამგზავრო ტენდენციებისა და სხვა ინდიკატორების საფუძველზე, რომლებიც, როგორც წესი, ასოცირებულია დანაშაულებრივ საქმიანობასთან. PNR მონაცემების ანალიზი იძლევა იმ პირთა სამგზავრო მარშრუტებისა და საკონტაქტო ინფორმაციის რეტროაქტიული მონიტორინგის საშუალებასაც, რომლებიც ეჭვმიტანილნი არიან დანაშაულებრივ საქმიანობაში.[795] შედეგად, სამართალდამცველი ორგანოები ახერხებენ დანაშაულებრივი ქსელების გამოვლენას. ევროკავშირს მესამე ქვეყნებთან გაფორმებული აქვს შეთანხმებები PNR მონაცემების გაცვლის მიზნით, როგორც განმარტებულია მე-7 ნაწილში. ამასთან, ევროკავშირის მასშტაბით მოქმედების PNR მონაცემების დამუშავების სისტემა, რომელიც დაინერგა 2016/681/EU დირექტივით (ევროკავშირის PNR დირექტივა).[796] ეს დირექტივა ავიაკომპანიებს უდგენს PNR მონაცემების კომპეტენტური ორგანოებისთვის გადაცემის ვალდებულებას და აწესებს მონაცემთა დაცვის მკაცრ გარანტიებს ამგვარი მონაცემების დამუშავებისა და შეგროვების კუთხით. PNR დირექტივა ვრცელდება ფრენებზე, რომლებიც ხორციელდება ევროკავშირიდან და ევროკავშირისკენ, ასევე, ევროკავშირის შიგნით, თუ წევრი სახელმწიფო ასე გადაწყვეტს.[797]

შეგროვებული PNR მონაცემები უნდა შეიცავდეს მხოლოდ ამ დირექტივით ნებადართულ ინფორმაციას. ისინი უნდა შეინახონ ერთ საინფორმაციო განყოფილებაში, უსაფრთხო ადგილას. ავიაკომპანიის მიერ მონაცემთა გადაცემიდან 6 თვის შემდეგ, საჭიროა PNR მონაცემების დეპერსონალიზაცია, ხოლო მათი შენახვა შესაძლებელია არაუმეტეს 5 წლის ვადით.[798] PNR მონაცემები იცვლება წევრ სახელმწიფოებს შორის, წევრ სახელმწიფოებსა და ევროპოლს შორის, და მესამე ქვეყნებთან, თუმცა, მხოლოდ გარკვეულ შემთხვევებში.

794 ევროპული კომისია (2011), წინადადება ევროპარლამენტისა და საბჭოს დირექტივის შესახებ, რომელიც შეეხება PNR მონაცემების გამოყენებას ტერორისტული და მძიმე დანაშაულების პრევენციის, გამოვლენის, გამოძიებისა და დამნაშავეთა დასჯის მიზნით, COM(2011) 32, საბოლოო, ბრიუსელი, 2011 წლის 2 თებერვალი, გვ. 1.

795 ევროპული კომისია (2015), ფაქტობრივი ინფორმაცია ევროკავშირის დონეზე ტერორიზმთან ბრძოლის შესახებ, კომისიის საქმიანობის, ღონისძიებებისა და ინიციატივების მიმოხილვა, 2015 წლის 11 იანვარი.

796 ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/681 ტერორისტული და მძიმე დანაშაულების პრევენციის, გამოვლენის, გამოძიებისა და დამნაშავეთა დასჯის მიზნით მგზავრთა პირადი მონაცემების (PNR) გამოყენების შესახებ, OJ 2016 L 119, გვ. 132.

797 PNR დირექტივა, L 119, გვ. 132, მუხლები 1 (1) და 2 (1).

798 *იქვე,* მუხლი 12 (1)(2).

PNR მონაცემების გადაცემა-დამუშავება და მონაცემთა სუბიექტების უფლებები უნდა შეესაბამებოდეს დირექტივას პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის და უზრუნველყოფდეს პირადი ცხოვრებისა და პერსონალური მონაცემების დაცვის მაღალ დონეს, ქარტიის, მოდერნიზებული 108-ე კონვენციისა და ადამიანის უფლებათა ევროპული კონვენციის მოთხოვნათა შესაბამისად.

ეროვნულ დონეზე არსებული დამოუკიდებელი საზედამხედველო ორგანოები, რომლებიც, PNR დირექტივის თანახმად, კომპეტენტურ ორგანოებს წარმოადგენენ, ვალდებულნი არიან, წევრ სახელმწიფოებს კონსულტაცია გაუწიონ ევროკავშირის PNR დირექტივის შესაბამისად მიღებულ დებულებებთან დაკავშირებით და მონიტორინგი განახორციელონ მათ გამოყენებაზე.

სატელეკომუნიკაციო მონაცემების შენახვა

მონაცემთა შენახვის დირექტივა,[799] რომელიც ძალადაკარგულად გამოცხადდა 2014 წლის 8 აპრილს, *Digital Rights Ireland-ის* საქმეში, სატელეკომუნიკაციო მომსახურების პროვაიდერებს ავალდებულებდა, შეენახათ მეტამონაცემები მძიმე დანაშაულებთან ბრძოლის კონკრეტული მიზნებით, მინიმუმ, 6 და, მაქსიმუმ, 24 თვის ვადით, მიუხედავად იმისა, სჭირდებოდა თუ არა პროვაიდერს ეს მონაცემები ანგარიშის გამოსაწერად ან ტექნიკური მომსახურების უზრუნველსაყოფად.

აშკარაა, რომ სატელეკომუნიკაციო მონაცემების შენახვა ჩარევაა მონაცემთა დაცვის უფლებაში.[800] თუ რამდენად გამართლებულია ეს ჩარევა, ევროკავშირის რამდენიმე სახელმწიფოში სასამართლო დავის საგანი იყო.[801]

> მაგალითი: საქმე *Digital Rights Ireland* and *Kärntner Landesregierung and Others*[802] *შეეხებოდა* Digital Rights ჯგუფის სარჩელს ირლანდიის უზენაეს სასამართლოში და ბატონი სეტლინჯერის სარჩელს ავსტრიის

799 ევროპული პარლამენტისა და საბჭოს 2006 წლის 15 მარტის დირექტივა 2006/24/EC საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების მომსახურებისას ან საჯარო კომუნიკაციების ქსელებში წარმოშობილი თუ დამუშავებული მონაცემების შენახვის შესახებ, რომელიც ცვლის დირექტივას 2002/58/EC, OJ 2006 L 105.

800 EDPS (2011), 2011 წლის 31 მაისის მოსაზრება ევროპული კომისიის მიერ საბჭოსა და პარლამენტისთვის განხორციელებული მონაცემთა შენახვის დირექტივის შეფასებითი ანგარიშის შესახებ (დირექტივა 2006/24/EC), 31 მაისი 2011 წელი.

801 გერმანია, ფედერალური საკონსტიტუციო სასამართლო *(Bundesverfassungsgericht)*, 1 BvR 256/08, 2 მარტი 2010 წელი; რუმინეთი, ფედერალური საკონსტიტუციო სასამართლო *(Curtea Constituțională a României)*, No. 1258, 8 ოქტომბერი 2009 წელი; ჩეხეთის რესპუბლიკა, საკონსტიტუციო სასამართლო *(Ústavní soud České republiky)*, 94/2011 Coll., 22 მარტი 2011 წელი.

802 CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი, პუნქტი 65.

უზენაეს სასამართლოში, იმ ეროვნული ღონისძიებების მართლზომიერებაზე, რომლებიც ითვალისწინებდა ელექტრონული სატელეკომუნიკაციო მონაცემების შენახვას. Digital Rights ჯგუფი ირლანდიის სასამართლოსგან ითხოვდა 2006/24 დირექტივისა და იმ ეროვნული კანონმდებლობის ძალადაკარგულად ცნობას, რომელიც ტერორისტულ დანაშაულებს შეეხებოდა. მსგავსად, ბატონი სეტლინჯერი და 11,000-ზე მეტი განმცხადებელი ითხოვდა, ძალადაკარგულად ეცნოთ ავსტრიის კანონი ტელეკომუნიკაციების შესახებ, რომელსაც 2006/24 დირექტივა ეროვნულ კანონმდებლობაში გადაჰქონდა.

CJEU-მ განიხილა აღნიშნული მოთხოვნები წინასწარი განჩინების გამოსატანად და დაადგინა, რომ მონაცემები, რომელთა შენახვასაც ითვალისწინებდა დირექტივა, ერთად აღებული, შეიცავდა ზუსტ ინფორმაციას შესაბამისი პირების შესახებ. ამასთან, CJEU-მ განიხილა პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის ფუნდამენტურ უფლებებში ჩარევის სიმძიმე და დაადგინა, რომ შენახვა აკმაყოფილებდა საჯარო ინტერესის სტანდარტს. კერძოდ, იგი მძიმე დანაშაულთან ბრძოლის მიზანს და, შესაბამისად, საჯარო ინტერესს ემსახურებოდა. ამის მიუხედავად, CJEU-მ დაასკვნა, რომ ევროკავშირის კანონმდებელმა დაარღვია პროპორციულობის პრინციპი ამ დირექტივის მიღებით. დირექტივა დასახული მიზნის მისაღწევად სათანადო საშუალებაა, თუმცა მისი „ფართომასშტაბიანი და განსაკუთრებით მძიმე ჩარევა პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის ფუნდამენტურ უფლებებში არ არის ისე შეზღუდული, რომ ჩარევა განხორციელდეს მხოლოდ მკაცრად აუცილებელი მოცულობით.“

2002/58/EC დირექტივა (პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ) გამონაკლისის სახით ითვალისწინებს მონაცემთა შენახვას შესაბამისი კანონმდებლობის არარსებობის პირობებშიც,[803] თუმცა, მხოლოდ მძიმე დანაშაულთან ბრძოლის მიზნით. ასეთი დროს მონაცემები უნდა შეინახონ იმ მოცულობით, რომელიც მკაცრად აუცილებელია შენახული მონაცემების კატეგორიების, კომუნიკაციის შესაბამისი საშუალებების, დაინტერესებული პირებისა და შენახვის შერჩეული ვადის გათვალისწინებით. სახელმწიფო ორგანოების წვდომა შენახულ მონაცემებზე მკაცრ პირობებს ექვემდებარება, მათ შორის, დამოუკიდებელი ორგანოს მიერ წინასწარ განხილვას. მონაცემები უნდა შეინახონ ევროკავშირის ფარგლებში.

803 ევროპული პარლამენტისა და საბჭოს 2002 წლის 12 ივლისის დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ (დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ), OJ 2002 L 201.

მაგალითი: საქმეზე *Digital Rights Ireland and Kärntner Landesregierung and Others*[804] მიღებული გადაწყვეტილების შემდეგ, CJEU-ში კიდევ ორი საქმე შევიდა იმ ზოგად ვალდებულებებზე, რომლებიც შვედეთსა და გაერთიანებულ სამეფოში ეკისრებათ ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს/პროვაიდერებს სატელეკომუნიკაციო მონაცემების შენახვასთან დაკავშირებით, 2006/24 დირექტივის მოთხოვნათა შესაბამისად. საქმეში *Tele2 Sverige* and *Home Department v. Tom Watson and Others*[805] CJEU-მ დაადგინა, რომ ეროვნული კანონმდებლობა, რომელიც ითვალისწინებს მონაცემთა ზოგად და განურჩეველ შენახვას, შესანახ მონაცემებსა და საზოგადოებრივი უსაფრთხოების რისკებს შორის კავშირის შესწავლისა და ყოველგვარი პირობების დაკონკრეტების გარეშე (მაგ.: შენახვის ვადა; გეოგრაფიული არეალი; იმ პირთა წრე, რომლებიც, სავარაუდოდ, მძიმე დანაშაულის მონაწილეები არიან), ვერ აკმაყოფილებს მკაცრი აუცილებლობის ტესტს. შედეგად, იგი არ შეიძლება გამართლებულად ჩაითვალოს დემოკრატიულ საზოგადოებაში, როგორც ამას ითვალისწინებს 2002/58/EC დირექტივა, წაკითხული ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის ჭრილში.

სამომავლო პერსპექტივები

2017 წლის იანვარში ევროკომისიამ გამოაქვეყნა ელექტრონულ კომუნიკაციებში პირადი ცხოვრების პატივისცემისა და პერსონალური მონაცემების დაცვის რეგულაციის პროექტი, რომლის მიზანია 2002/58/EC დირექტივის გაუქმება და ჩანაცვლება.[806] პროექტი არ შეიცავს რაიმე კონკრეტულ დებულებებს მონაცემთა დაცვასთან დაკავშირებით, თუმცა, წევრ სახელმწიფოებს ანიჭებს უფლებამოსილებას გარკვეული ვალდებულებებისა და უფლებების შესაზღუდად კანონის საფუძველზე, თუკი ეს აუცილებელი და პროპორციული ზომაა კონკრეტული საჯარო ინტერესების დასაცავად (მაგ.: ეროვნული უსაფრთხოება; თავდაცვა და საზოგადოებრივი უსაფრთხოება; ასევე, სისხლის-სამართლებრივი დანაშაულების პრევენცია, გამოძიება, გამოვლენა, დევნა და სასჯელის აღსრულება). [807] ამრიგად, წევრ სახელმწიფოებს უფლება აქვთ,

804 CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2-14 წლის 8 აპრილი

805 CJEU, გაერთიანებული საქმეები C-203/15 და C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* [GC], 2016 წლის 21 დეკემბერი.

806 ევროპული კომისია (2017), წინადადება ევროპარლამენტისა და საბჭოს რეგულაციასთან დაკავშირებით, რომელიც შეეხება პირადი ცხოვრების დაცვას და პერსონალური მონაცემების დამუშავებას ელექტრონულ კომუნიკაციების სექტორში და აუქმებს 2002/58/EC დირექტივას (პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ), COM(2017) 10, საბოლოო, ბრიუსელი, 2017 წლის 10 იანვარი.

807 *იქვე*, პრეამბულა, პუნქტი 26.

შეინარჩუნონ ან შექმნან მონაცემთა შენახვის ეროვნული ჩარჩო, რომელიც მოიცავს მიზნობრივ ღონისძიებებს, თუკი ეს ჩარჩო აკმაყოფილებს ევროკავშირის კანონმდებლობას და ითვალისწინებს CJEU-ს პრეცედენტულ სამართალს ელექტრონულ სივრცეში პირადი ცხოვრების დაცვის დირექტივისა და ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის განმარტებასთან დაკავშირებით.[808] წინამდებარე სახელმძღვანელოს მომზადებისას, მიმდინარეობდა დისკუსიები რეგულაციის მიღებაზე.

ევროკავშირი-აშშ-ს ქოლგა შეთანხმება სამართალდამცველი მიზნებით გაცვლილი პერსონალური მონაცემების დაცვაზე

2017 წლის 1 თებერვალს ძალაში შევიდა ევროკავშირი-აშშ-ს ქოლგა შეთანხმება სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენისა და დამნაშავეთა დასჯის მიზნით პერსონალური მონაცემების დამუშავების შესახებ.[809] ეს შეთანხმება მიზნად ისახავს ევროკავშირის მოქალაქეთა მონაცემების მაღალ დონეზე დაცვას და, ამავდროულად, ევროკავშირისა და აშშ-ს სამართალდამცველ ორგანოებს შორის თანამშრომლობის გაუმჯობესებას. იგი ავსებს, ერთი მხრივ, ევროკავშირსა და აშშ-ს, ხოლო მეორე მხრივ, წევრ სახელმწიფოებსა და აშშ-ს შორის შეთანხმებებს სამართალდამცველი ორგანოების თანამშრომლობაზე და ხელს უწყობს მონაცემთა დაცვის მკაფიო და ჰარმონიზებული წესების შექმნას ამავე სფეროში სამომავლო შეთანხმებებისთვის. ამ მხრივ, შეთანხმების მიზანია ხანგრძლივი სამართლებრივი ჩარჩოს შექმნა ინფორმაციის გაცვლის ხელშესაწყობად.

აღნიშნული შეთანხმება არ ითვალისწინებს სამართლებრივ საფუძველს პერსონალური მონაცემების გასაზიარებლად, ის შესაბამის პირებს სთავაზობს მონაცემთა დაცვის უსაფრთხოების ზომებს. შეთანხმება შეეხება პერსონალური მონაცემების ნებისმიერ დამუშავებას, რომელიც აუცილებელია სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენისა და დევნისათვის.[810]

808 იხ: პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ რეგულაციაზე წინადადების განმარტებითი მემორანდუმი, COM(2017) 10, საბოლოო, პ. 1.3.

809 იხ: ევროკავშირის საბჭო (2016), „სამართალდაცვითი თანამშრომლობის სფეროში ევროკავშირის მოქალაქეთა გაუმჯობესებული მონაცემთა დაცვის უფლებები: ევროკავშირი და აშშ ხელს აწერენ ქოლგა შეთანხმებას“, პრესრელიზი 305/16, 2016 წლის 2 ივნისი.

810 აშშ-სა და ევროკავშირს შორის შეთანხმება პერსონალური ინფორმაციის დაცვის შესახებ, სისხლისსამართლებრივი დანაშაულების პრევენციასთან, გამოძიებასთან, გამოვლენასა და დევნასთან დაკავშირებით, 2016 წლის 18 მაისი, (OR.en) 8557/16, მუხლი 3(1). ასევე, იხ: კომისიის შეტყობინება ევროკავშირი-აშშ-ს მონაცემთა დაცვის შეთანხმების მოლაპარაკებებზე, 2019 წლის 26 მაისი, MEMO/10/216 და ევროკავშირის კომისიის პრესრელიზი (2010), რომელიც შეეხება ევროკავშირი-აშშ-ს მონაცემთა დაცვის შეთანხმებით გათვალისწინებული პირადი ცხოვრების დაცვის მაღალ სტანდარტებს, 2010 წლის 26 მაისი, IP/10/609.

დოკუმენტი ასევე ადგენს უსაფრთხოების არაერთ ზომას, რათა პერსონალური მონაცემები გამოიყენონ მხოლოდ შეთანხმებაში მითითებული მიზნებით. კერძოდ, ევროკავშირის მოქალაქეებისათვის შეთანხმება ითვალისწინებს შემდეგი სახის დაცვას:

- მონაცემთა გამოყენების შეზღუდვა: პერსონალური მონაცემების გამოყენება ნებადართულია მხოლოდ სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენის ან დევნის მიზნით;

- დაცვა თვითნებური და გაუმართლებელი დისკრიმინაციისგან;

- მონაცემთა შემდგომი (მეორადი) გადაცემის პირობები: მონაცემთა შემდგომი გადაცემა ქვეყნისთვის, რომელიც ევროკავშირის წევრი არ არის (აშშ-ს გარდა), საჭიროებს იმ სახელმწიფოს უფლებამოსილი ორგანოს წინასწარ თანხმობას, რომელმაც თავდაპირველად გადასცა მონაცემები;

- მონაცემთა ხარისხი: პერსონალური მონაცემები უნდა იყოს ზუსტი, რელევანტური, განახლებული და სრული;

- დამუშავების უსაფრთხოება, პერსონალურ მონაცემთა უსაფრთხოების დარღვევაზე შეტყობინების ჩათვლით;

- განსაკუთრებული კატეგორიის მონაცემების დამუშავება დაშვებულია კანონით გათვალისწინებული უსაფრთხოების ზომების არსებობისას;

- შენახვის ვადა: პერსონალური მონაცემები უნდა შეინახონ მხოლოდ აუცილებელი ვადით;

- წვდომისა და გასწორების უფლება: გარკვეული პირობებით, ნებისმიერ პირს უფლება აქვს, ჰქონდეს წვდომა თავის პერსონალურ მონაცემებზე; ასევე, მოითხოვოს მის შესახებ არსებული არაზუსტი პერსონალური მონაცემების გასწორება;

- ავტომატიზებული გადაწყვეტილება მოითხოვს უსაფრთხოების სათანადო ზომებს, მათ შორის, ადამიანური რესურსების ჩართვის შესაძლებლობას;

- ეფექტიანი ზედამხედველობა, მათ შორის, ევროკავშირისა და აშშ-ს საზედამხედველო ორგანოების თანამშრომლობა;

- დარღვეული უფლების აღდგენა/დაცვა და სასამართლო გადაწყვეტილებების აღსრულებადობა: ევროკავშირის მოქალაქეებს[811] უფლება აქვთ,

811 აშშ-ს სამართლებრივი დაცვის აქტს ხელი მოაწერა პრეზიდენტმა ობამამ, 2016 წლის 24 თებერვალს.

შელახული უფლების აღდგენა მოითხოვონ აშშ-ს სასამართლოში, თუ აშშ-ს სახელმწიფო უწყება არ დააკმაყოფილებს მათ მოთხოვნას წვდომაზე, ან უკანონოდ გაამჟღავნებს მათ პერსონალურ მონაცემებს.

- ქოლგა შეთანხმების თანახმად, აუცილებელია, არსებობდეს სისტემა, რომლის მიხედვითაც, მონაცემთა უსაფრთხოების დარღვევის შემთხვევაში, შეტყობინება შეიძლება გაეგზავნოს იმ წევრი სახელმწიფოს კომპეტენტურ საზედამხედველო ორგანოს, სადაც ცხოვრობს პირი, ვისი მონაცემთა უსაფრთხოებაც დაირღვა. შეთანხმებით გათვალისწინებული დაცვის მექანიზმები უზრუნველყოფს ევროკავშირის მოქალაქეთა თანასწორ მოპყრობას აშშ-ში პირადი ცხოვრების უფლების დარღვევისას.[812]

8.3.1 მონაცემთა დაცვა ევროკავშირის სასამართლო და სამართალდამცველ უწყებებში

ევროპოლი

ევროკავშირის სამართალდამცველი უწყების „ევროპოლის“ სათავო ოფისი მდებარეობს ჰააგაში. მას ასევე აქვს შიდასახელმწიფოებრივი ერთეულები (ENU) ევროკავშირის თითოეულ წევრ სახელმწიფოში. ევროპოლი 1998 წელს შეიქმნა. მისი, როგორც ევროკავშირის ინსტიტუტის დღევანდელი სამართლებრივი სტატუსი ეფუძნება რეგულაციას ევროკავშირის სამართალდაცვითი თანამშრომლობის სააგენტოს შესახებ (ევროპოლის რეგულაცია).[813] ევროპოლის მიზანია, ხელი შეუწყოს ორგანიზებული დანაშაულის, ტერორიზმისა და სხვა მძიმე დანაშაულების პრევენციასა და გამოძიებას (ევროპოლის რეგულაციის დანართი 1) სახელმწიფოთაშორის დონეზე. ამ მიზნით, ევროპოლი უზრუნველყოფს ინფორმაციის გაცვლას, სადაზვერვო მონაცემების ანალიზსა და საფრთხეების შეფასებას და ასრულებს ევროკავშირის საინფორმაციო ცენტრის ფუნქციას.

812 ევროკავშირის მონაცემთა დაცვის ზედამხედველმა გამოსცა მოსაზრება ევროკავშირი-აშშ-ს შეთანხმებაზე, რომელშიც მან წარმოადგინა შემდეგი რეკომენდაციები: ა) მუხლს, რომელიც არეგულირებს მონაცემთა შენახვას არაუმეტეს საჭირო და სათანადო ვადით, უნდა დაემატოს ფრაზა: „იმ კონკრეტული მიზნებით, რისთვისაც ისინი გადაეცა“; 2) სენსიტიური მონაცემების დიდი ოდენობით გადაცემის გამორიცხვა, რაც, შეთანხმების თანახმად, შესაძლებელია. იხ: ევროკავშირის მონაცემთა დაცვის ზედამხედველი, მოსაზრება 1/2016, წინასწარი მოსაზრება აშშ-სა და ევროკავშირს შორის სისხლისსამართლებრივი დანაშაულების პრევენციასთან, გამოძიებასთან, გამოვლენასა და დევნასთან დაკავშირებული პერსონალური მონაცემების დაცვის შესახებ, პუნქტი 35.

813 ევროპარლამენტისა და საბჭოს 2016 წლის 11 მაისის რეგულაცია (EU) 2016/794, რომელიც შეეხება ევროკავშირის სამართალდაცვით სფეროში თანამშრომლობის სააგენტოს (ევროპოლი) და აუქმებს და ანაცვლებს საბჭოს შემდეგ გადაწყვეტილებებს: 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA და 2009/968/JHA, OJ 2016 L 135, გვ. 53.

საკუთარი მიზნების მისაღწევად, ევროპოლმა დააფუძნა საინფორმაციო სისტემა, რომელიც უზრუნველყოფს მონაცემთა ბაზას ევროკავშირის წევრი ქვეყნებისთვის. იგი საჭიროა სისხლის სამართლის საქმეებზე დაზვერვის ჩასატარებლად და შესაბამისი ინფორმაციის გასაცვლელად ევროპოლის შიდასახელმწიფოებრივი ერთეულების საშუალებით. სისტემა გამოიყენება იმ ინფორმაციაზე წვდომისათვის, რომელიც შეეხება ევროპოლის კომპეტენციაში შემავალ დანაშაულებში ეჭვმიტანილ ან მსჯავრდებულ პირებს, ან ვის მიმართაც არსებობს ფაქტობრივი გარემოებები ასეთი დანაშაულის ჩადენის შესახებ. ევროპოლსა და მის შიდასახელმწიფოებრივ ერთეულებს შეუძლიათ, ინფორმაცია პირდაპირ შეიტანონ ამ სისტემაში ან, პირიქით, ამოიღონ სისტემიდან. მონაცემების შეცვლა, გასწორება ან წაშლა შეუძლია მხოლოდ იმ პირს, რომელმაც ეს მონაცემები შეიყვანა. ინფორმაციის მიწოდება ევროპოლისთვის შეუძლიათ ევროკავშირის ორგანოებს, მესამე ქვეყნებსა და საერთაშორისო ორგანიზაციებს.

ევროპოლს ინფორმაციის, მათ შორის, პერსონალური მონაცემების მიღება შეუძლია საჯაროდ ხელმისაწვდომი წყაროებიდანაც (მაგ.: ინტერნეტიდან). პერსონალური მონაცემების გადაცემა ევროკავშირის ორგანოებისთვის დაშვებულია მხოლოდ მაშინ, როცა ეს აუცილებელია ევროპოლის ან ევროკავშირის შესაბამისი ორგანოს ფუნქციების შესასრულებლად. მონაცემთა გადაცემა მესამე ქვეყნისა ან საერთაშორისო ორგანიზაციებისთვის კი ნებადართულია მხოლოდ იმ შემთხვევაში, თუ ევროპული კომისია გადაწყვეტს, რომ ისინი სათანადო დონეზე იცავენ მონაცემებს (შესაბამისობის გადაწყვეტილება), ანდა არსებობს საერთაშორისო ხელშეკრულება ან თანამშრომლობის შეთანხმება. ევროპოლს კერძო პირებისა და მხარეებისგან პერსონალური მონაცემების მიღება შეუძლია მხოლოდ მკაცრად განსაზღვრულ შემთხვევებში. კერძოდ, მონაცემები უნდა გადასცეს: ევროპოლის შიდასახელმწიფოებრივმა ერთეულმა, ეროვნული კანონმდებლობის შესაბამისად; იმ მესამე ქვეყნის ან საერთაშორისო ორგანიზაციის საკონტაქტო პირმა, რომელთანაც ევროპოლს თანამშრომლობის პრაქტიკა აქვს, თანამშრომლობის შეთანხმების შესაბამისად; იმ მესამე ქვეყნის ან საერთაშორისო ორგანიზაციის წარმომადგენელმა, რომლის მიმართაც ევროკომისიამ მიიღო შესაბამისობის გადაწყვეტილება, ან ევროკავშირს გაფორმებული აქვს საერთაშორისო შეთანხმება. მონაცემები იცვლება „ინფორმაციის უსაფრთხო გაცვლის საერთაშორისო ქსელის“ (SIENA) საშუალებით.

ახალ მოვლენებთან დაკავშირებით, ევროპოლში ჩამოყალიბდა სპეციალიზებული ცენტრები. 2013 წელს შეიქმნა კიბერდანაშაულის ევროპული ცენტრი,[814] რომელიც ასრულებს ევროკავშირის კიბერდანაშაულის საინფორმაციო

814 იხ: EDPS (2012), მონაცემთა დაცვის ზედამხედველის მოსაზრება, რომელიც შეეხება ევროპული კომისიის მიმართვას კიბერდანაშაულის ცენტრის შექმნაზე, ბრიუსელი 2012 წლის 29 ივნისი.

ცენტრის ფუნქციას და ხელს უწყობს სწრაფ რეაგირებას ონლაინ დანაშაულებზე. ცენტრი ავითარებს და ნერგავს ციფრული ექსპერტიზის საშუალებებს, უზრუნველყოფს საუკეთესო პრაქტიკას გამოძიებასთან დაკავშირებით და ფოკუსირებულია ისეთ კიბერდანაშაულებზე, რომლებიც:

- ჩადენილია ორგანიზებული ჯგუფების მიერ, დიდი ოდენობის უკანონო შემოსავლის მისაღებად, მაგალითად ონლაინ თაღლითობა;
- მნიშვნელოვან ზიანს აყენებს დაზარალებულს (მაგ.: ბავშვთა სექსუალური ექსპლუატაცია ინტერნეტით);
- გავლენას ახდენს ევროკავშირის კრიტიკულ ინფრასტრუქტურასა და საინფორმაციო სისტემებზე.

2016 წლის იანვარში შექმნილი ევროპული კონტრტერორისტული ცენტრი (ECTC) ოპერაციულ მხარდაჭერას უზრუნველყოფს იმ წევრი სახელმწიფოებისთვის, რომლებიც ტერორისტულ დანაშაულებს იძიებენ. ცენტრი ცოცხალ რეჟიმში მიღებულ ოპერაციულ მონაცემებს ადარებს ევროპოლის ხელთ არსებულ ინფორმაციას, სწრაფად ააშკარავებს შესაბამის ფინანსურ მინიშნებებს და აანალიზებს ხელმისაწვდომ საგამოძიებო ინფორმაციას ტერორისტულ ქსელზე სრული სურათის შესაქმნელად. [815]

ევროპოლის მიგრანტთა კონტრაბანდის ცენტრი (EMSC) 2016 წლის თებერვალში შეიქმნა, 2015 წლის ნოემბერში გამართული საბჭოს შეხვედრის შემდგომ. მისი ამოცანაა წევრი სახელმწიფოების მხარდაჭერა მიგრანტთა კონტრაბანდაში მონაწილე დანაშაულებრივი ქსელების მიზანში ამოღებასა და დაშლაში. EMSC ასრულებს საინფორმაციო ცენტრის ფუნქციას, რომელიც მხარდაჭერას უწევს კატანიასა (იტალია) და პირეოსში (საბერძნეთი) მდებარე რეგიონული სამუშაო ჯგუფის ოფისებს. ეს უკანასკნელი შიდასახელმწიფოებრივ ორგანოებს სხვადასხვა სფეროში უწევს დახმარებას, მათ შორის, დაზვერვის მონაცემების გაზიარებაში, სისხლის სამართლის საქმეების გამოძიებასა და მიგრანტთა კონტრაბანდის დანაშაულებრივი ქსელების სამართლებრივ დევნაში.[816]

მონაცემთა დაცვის რეჟიმი, რომელიც ევროპოლის საქმიანობას არეგულირებს, გაძლიერებულია და ეფუძნება ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაციის პრინციპებს.[817] იგი ასევე შეესაბამება მონაცემთა დაცვის

815 იხ: ევროპოლის ვებგვერდი.

816 იხ. ევროპოლის ვებგვერდი.

817 ევროპული პარლამენტისა და საბჭოს 2000 წლის 18 დეკემბრის რეგულაცია (EC) No. 45/2001 ვროკავშირის ინსტიტუტებისა და ორგანოების მიერ პერსონალური მონაცემების დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ 2001 L 8, 41–48 მუხლები.

დირექტივას პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისთვის, მოდერნიზებულ 108-ე კონვენციას და რეკომენდაციას პოლიციის შესახებ.

პერსონალური მონაცემების დამუშავება ისეთ პირებთან მიმართებით, როგორებიც არიან სისხლის სამართლის საქმეებში დაზარალებულები, მოწმეები, ასეთ დანაშულზე ინფორმაციის მიმწოდებლები, ან 18 წლამდე პირები, დაიშვება მხოლოდ იმ შემთხვევაში, თუ ეს პროპორციული და მკაცრად აუცილებელია ევროპოლის კომპეტენციაში შემავალ დანაშულებთან ბრძოლისა და პრევენციისათვის.[818] განსაკუთრებული კატეგორიის მონაცემების დამუშავება ნებადართულია ასეთივე გარემოებებისას, ამასთანავე, როცა ეს ინფორმაცია ავსებს ევროპოლის მიერ დამუშავებულ სხვა პერსონალურ მონაცემებს.[819] ორივე შემთხვევაში მხოლოდ ევროპოლს აქვს შესაბამის მონაცემებზე წვდომა.[820]

მონაცემთა შენახვა შეიძლება მხოლოდ აუცილებელი და პროპორციული ვადით, რომელიც უნდა გადაიხედოს 3 წელიწადში ერთხელ. წინააღმდეგ შემთხვევაში, ისინი წაიშლება ავტომატურად.[821]

ევროპოლს გარკვეულ შემთხვევებში უფლება აქვს, პერსონალური მონაცემები გადასცეს ევროკავშირის ორგანოს ან პირდაპირ მესამე ქვეყნისა თუ საერთაშორისო ორგანიზაციის შესაბამის უწყებას/განყოფილებას.[822]თუ სავარაუდოა, რომ უსაფრთხოების დარღვევა მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებზე მწვავე და უარყოფით გავლენას იქონიებს, ევროპოლი ვალდებულია, ეს დაუყოვნებლივ შეატყობინოს მონაცემთა სუბიექტს.[823] ევროპოლის მიერ პერსონალური მონაცემების დამუშავების მონიტორინგს წევრი სახელმწიფოს დონეზე ახორციელებს ეროვნული საზედამხედველო ორგანო.[824]

EDPS-ს პასუხისმგებელია ფიზიკურ პირთა უფლებებისა და თავისუფლებების დაცვასა და მონიტორინგზე ევროპოლის მიერ პერსონალური მონაცემების დამუშავებისას, ასევე, ორივე მხარისთვის კონსულტაციის გაწევაზე პერსონალურ მონაცემთა დამუშავების შესახებ. ამ მიზნით, EDPS ასრულებს საგამოძიე-

818 ევროპოლის რეგულაცია, მუხლი 30 (1).

819 *იქვე,* მუხლი 30 (2).

820 *იქვე,* მუხლი 30 (3).

821 *იქვე,* მუხლი 31.

822 *იქვე,* შესაბამისად, მუხლები 24 და 25.

823 *იქვე,* მუხლი 35.

824 ევროპოლის რეგულაცია, მუხლი 42.

ბო და საჩივრების განმხილველი ორგანოს როლს და ეროვნულ საზედამხედველო ორგანოებთან მჭიდროდ თანამშრომლობს.[825] EDPS და ეროვნული საზედამხედველო ორგანოები ერთმანეთს, სულ მცირე, წელიწადში ორჯერ ხვდებიან, თანამშრომლობის საბჭოს ფორმატით, რომელსაც საკონსულტაციო ფუნქციები აქვს.[826] წევრი სახელმწიფო ვალდებულია, საკანონმდებლო დონეზე შექმნას საზედამხედველო ორგანო, რომელსაც ექნება უფლებამოსილება, მონიტორინგი გაუწიოს ევროპოლისთვის პერსონალურ მონაცემთა გადაცემის დასაშვებობას, ევროპოლიდან მონაცემების მიღებას ან ნებისმიერ კომუნიკაციას მათ შორის.[827] წევრ სახელმწიფოებს ასევე მოეთხოვებათ, რომ ეროვნული საზედამხედველო ორგანო სრულიად დამოუკიდებლად ასრულებდეს ევროპოლის რეგულაციით გათვალისწინებულ ფუნქციებსა და მოვალეობებს.[828] დამუშავების კანონიერების შესაფასებლად, საქმიანობაზე თვითმონიტორინგის, ასევე, მონაცემთა მთლიანობისა და უსაფრთხოების დაცვის მიზნით, ევროპოლი აწარმოებს ჩანაწერებსა და დოკუმენტაციას შესაბამისი აქტივობების აღსარიცხად. ეს ჩანაწერები შეიცავს ინფორმაციას მონაცემთა ავტომატური დამუშავების შესახებ, კერძოდ, ისეთ საკითხებზე, როგორიცაა შეგროვება, გასწორება, კონსულტაცია, გამჟღავნება, კომბინირება და წაშლა.[829]

EDPS-ის გადაწყვეტილების გასაჩივრება შესაძლებელია მართლმსაჯულების ევროპულ სასამართლოში.[830] ნებისმიერ პირს, რომელსაც მონაცემთა უკანონო დამუშავების შედეგად ზიანი მიადგა, უფლება აქვს, მიიღოს კომპენსაცია ევროპოლისა (CJEU-ში სარჩელის შეტანის გზით) ან პასუხისმგებელი წევრი სახელმწიფოსგან (ეროვნულ სასამართლოში სარჩელის შეტანის გზით).[831] ამასთან, ევროპოლის საქმიანობაზე ზედამხედველობა შეუძლია წევრი სახელმწიფოების საკანონმდებლო ორგანოებისა და ევროპული პარლამენტის ერთობლივი საპარლამენტო მონიტორინგის ჯგუფს (JPSG).[832] თითოეულ პირს აქვს უფლება, ჰქონდეს წვდომა მის შესახებ ევროპოლის სისტემაში დაცულ ნებისმიერ პერსონალურ ინფორმაციაზე და, საჭიროების შემთხვევაში, მოითხოვოს მათი შემოწმება, გასწორება ან წაშლა. ამ უფლებებთან დაკავშირებით დაშვებულია გარკვეული გამონაკლისი შემთხვევები და შეზღუდვები.

825 *იქვე,* მუხლები 43 და 44.

826 *იქვე,* მუხლი 45.

827 *იქვე,* მუხლი 42 (1).

828 *იქვე,* მუხლი 42 (1).

829 *იქვე,* მუხლი 40.

830 *იქვე,* მუხლი 48.

831 *იქვე,* მუხლი 50.

832 *იქვე,* მუხლი 51.

ევროჯასტი

ევროკავშირის ერთ-ერთი ორგანო ევროჯასტი (Eurojust) შეიქმნა 2002 წელს. მისი სათავო ოფისი ჰააგაში მდებარეობს. ევროჯასტი ხელს უწყობს სახელმწიფოთაშორის სამართლებრივ თანამშრომლობას მძიმე დანაშაულების გამოძიებისა და დევნის პროცესში.[833] მის კომპეტენციებში შედის:

- სხვადასხვა წევრი სახელმწიფოს უფლებამოსილი ორგანოების მიერ ერთობლივი გამოძიებების სტიმულირება და კოორდინაციის გაუმჯობესება;

- სასამართლო სფეროში თანამშრომლობის მოთხოვნათა და გადაწყვეტილებათა აღსრულების ხელშეწყობა.

ევროჯასტის ფუნქციებს ასრულებენ წევრი სახელმწიფოების მიერ დანიშნული წარმომადგენლები. კერძოდ, თითოეული ქვეყანა ევროჯასტში ნიშნავს ერთ მოსამართლეს ან პროკურორს, რომლის სტატუსიც რეგულირდება ეროვნული კანონმდებლობით. მათ აქვთ სასამართლო სფეროში თანამშრომლობის წახალისებისა და გაუმჯობესების უფლებამოსილება. ამასთან, ევროჯასტის წევრები მოქმედებენ ერთობლივად, კოლეგიის ფორმატში სპეციალური ფუნქციების შესასრულებლად.

ევროჯასტს აქვს პერსონალური მონაცემების დამუშავების უფლება, თუ ეს აუცილებელია მისი მიზნების მისაღწევად. ამავდროულად, აღნიშნული მონაცემები უნდა შეიცავდეს კონკრეტულ ინფორმაციას პირებზე, რომლებიც ეჭვმიტანილნი ან მსჯავრდებულნი არიან ევროჯასტის კომპეტენციით გათვალისწინებული სისხლისსამართლებრივი დანაშაულების ჩადენასა თუ მათში მონაწილეობაში, ანდა იყვნენ ასეთი დანაშაულების მსხვერპლნი ან მოწმეები.[834] გამონაკლის შემთხვევებში, ევროჯასტს უფლება აქვს, შეზღუდული ვადით დაამუშაოს ვრცელი მონაცემები, რომლებიც შეეხება სამართალდარღვევის გარემოებებს, თუ ეს გადაუდებელი აუცილებლობაა მიმდინარე გამოძიებისათვის. საკუთარი უფლებამოსილების ფარგლებში, ევროჯასტი თანამ-

833 ევროკავშირის საბჭოს 2002 წლის 28 თებერვლის გადაწყვეტილება 2002/187/JHA მძიმე დანაშაულის წინააღმდეგ ბრძოლის გაძლიერებისთვის ევროჯასტის შექმნის შესახებ OJ 2002 L 63; ევროკავშირის საბჭოს 2003 წლის 18 ივნისის გადაწყვეტილება 2003/659/JHA ცვლილებებზე საბჭოს გადაწყვეტილებაში 2002/187/JHA მძიმე დანაშაულის წინააღმდეგ ბრძოლის გაძლიერებისთვის ევროჯასტის შექმნის შესახებ, OJ 2003 L 44; ევროკავშირის საბჭოს 2009 წლის 16 დეკემბრის გადაწყვეტილება 2009/426/JHA ევროჯასტის გაძლიერებასა და ცვლილებებზე გადაწყვეტილებაში 2002/187/JHA მძიმე დანაშაულის წინააღმდეგ ბრძოლის გაძლიერებისთვის ევროჯასტის შექმნის შესახებ OJ 2009 L 138 (გადაწყვეტილებები ევროჯასტის შესახებ).

834 საბჭოს გადაწყვეტილების 2002/187/JHA კონსოლიდირებული ვერსია, 2003/659/JHA და 2009/426/JHA გადაწყვეტილებების გათვალისწინებით, მუხლი 15, პუნქტი 2.

შრომლობს ევროკავშირის ინსტიტუტებთან, ორგანოებსა და სააგენტოებთან და ცვლის პერსონალურ მონაცემებს. თანამშრომლობა და ინფორმაციის გაზიარება ევროჯასტს შეუძლია მესამე ქვეყნებსა და ორგანიზაციებთანაც.

ამ ორგანომ უნდა უზრუნველყოს მონაცემთა დაცვის ის დონე, რომელიც გათვალისწინებულია, სულ მცირე, მოდერნიზებული 108-ე კონვენციითა და მისი შემდგომი შესწორებებით. მონაცემთა გაცვლის შემთხვევებში, აუცილებელია კონკრეტული წესებისა და შეზღუდვების დაცვა, რომლებსაც ადგენს თანამშრომლობის შეთანხმება ან სამუშაო ხელშეკრულება, დადებული ევროჯასტის საბჭოს გადაწყვეტილებებისა და მონაცემთა დაცვის წესების შესაბამისად.[835]

ევროჯასტში შექმნილი დამოუკიდებელი საერთო საზედამხედველო ორგანოს (JSB) მოვალეობაში შედის მონიტორინგი ევროჯასტის მიერ პერსონალური მონაცემების დამუშავებაზე. ფიზიკურ პირებს უფლება აქვთ, საზედამხედველო ორგანოს მიმართონ საჩივრით, თუ ევროჯასტი არ დააკმაყოფილებს მათ მოთხოვნას პერსონალურ მონაცემებზე წვდომის, გასწორების, დაბლოკვის ან წაშლის შესახებ. მონაცემების უკანონოდ დამუშავების შემთხვევაში, ევროჯასტს პირისთვის მიყენებულ ნებისმიერ ზიანზე პასუხისმგებლობა დაეკისრება იმ წევრი სახელმწიფოს ეროვნული კანონმდებლობით, სადაც მდებარეობს მისი სათავო ოფისი (ნიდერლანდები).

სამომავლო პერსპექტივები

ევროპულმა კომისიამ 2013 წლის ივლისში წარმოადგინა რეგულაციის პროექტი ევროჯასტის რეფორმირებაზე. პროექტს ერთვოდა წინადადება ევროპის პროკურატურის შექმნის შესახებ (იხ: ქვემოთ). რეგულაციის მიზანია ევროჯასტის ფუნქციებისა და სტრუქტურის სრულყოფა, ლისაბონის ხელშეკრულების შესაბამისად; ასევე, მისი ოპერაციული (რომლებსაც კოლეგია ასრულებს) და ადმინისტრაციული ფუნქციების გამიჯვნა. ეს წევრ სახელმწიფოებს ოპერაციულ ფუნქციებზე ფოკუსირების შესაძლებლობას მისცემს და შეიქმნება ახალი აღმასრულებელი საბჭო, რომელიც კოლეგიას ადმინისტრაციული ფუნქციების შესრულებაში დაეხმარება.[836]

ევროკავშირის პროკურატურა

წევრ სახელმწიფოებს აქვთ ექსკლუზიური უფლებამოსილება, სამართლებრივი დევნა განახორციელონ თაღლითობისა და ევროკავშირის ბიუჯეტის არამიზნობრივი გამოყენების მიმართ, თუ ამ დანაშაულს, სავარაუდოდ, გა-

835 პროცედურული წესები ევროჯასტში პერსონალურ მონაცემთა დამუშავებისა და დაცვის შესახებ, OJ 2005 C 68/01, 19 მარტი 2005 წელი, გვ. 1.

836 იხ. ევროკომისიის ვებგვერდი ევროჯასტის შესახებ.

ვლენა ექნება სხვა წევრ სახელმწიფო(ებ)ზეც. ასეთი დანაშაულების გამოძიების, დევნის და დამნაშავეთა დასჯის მნიშვნელობა გაიზარდა, განსაკუთრებით, არსებული ეკონომიკური კრიზისის ფონზე.[837] ევროპულმა კომისიამ წარმოადგინა რეგულაცია ევროკავშირის დამოუკიდებელი პროკურატურის შექმნასთან (EPPO) დაკავშირებით. [838] მისი მიზანია იმ სისხლისსამართლებრივ დანაშაულებთან ბრძოლა, რომლებიც გავლენას ახდენს ევროკავშირის ფინანსურ ინტერესებზე. EPPO შეიქმნება გაუმჯობესებული თანამშრომლობის პროცედურის ფარგლებში, რაც, სულ მცირე, 9 წევრ სახელმწიფოს საშუალებას მისცემს, ევროკავშირის სტრუქტურებით გათვალისწინებულ რომელიმე სფეროში ჰქონდეთ გაძლიერებული თანამშრომლობა, გაერთიანების სხვა ქვეყნების მონაწილეობის გარეშე. [839] გაუმჯობესებული თანამშრომლობა მოიცავს ისეთ სახელმწიფოებს, როგორიცაა: ბელგია, ბულგარეთი, ხორვატია, კვიპროსი, ჩეხეთის რესპუბლიკა, ესტონეთი, ფინეთი, საფრანგეთი, გერმანია, საბერძნეთი, ლატვია, ლიეტუვა, ლუქსემბურგი, პორტუგალია, რუმინეთი, სლოვენია, სლოვაკეთი და ესპანეთი. ამ ფორმატში გაწევრიანების სურვილი გამოთქვეს ავსტრიამ და იტალიამაც.[840]

ევროკავშირის პროკურატურას ექნება თაღლითობისა და იმ სხვა დანაშაულების გამოძიებისა თუ დევნის უფლებამოსილება, რომლებიც გავლენას ახდენს ევროკავშირის ფინანსურ ინტერესებზე. ამის მიზანია, ეფექტიანი კოორდინაცია გაუწიოს გამოძიებასა და სამართლებრივ დევნას სხვადასხვა წევრი სახელმწიფოს სამართლებრივი სისტემების პირობებში, ასევე, გააუმჯობესოს რესურსების გამოყენება და ინფორმაციის გაცვლა ევროკავშირის დონეზე.[841]

EPPO-ს უხელმძღვანელებს ევროკავშირის პროკურორი, რომელსაც თითოეულ წევრ სახელმწიფოში ეყოლება, სულ მცირე, 1 წარმომადგენელი (ადგილობრივი პროკურორი), პასუხისმგებელი ამ სახელმწიფოში ჩატარებულ გამოძიებებსა და სამართლებრივ დევნაზე.

წინადადება დამოუკიდებელი პროკურატურის შექმნის შესახებ მოიცავს მყარ გარანტიებს იმ პირთა დასაცავად, რომლებიც EPPO-ს მიერ წარმოებულ გა-

837 ევროკომისია (2013), წინადადება საბჭოს რეგულაციაზე, რომელიც შეეხება ვროკავშირის პროკურატურის შექმნას, COM(2013) 534, საბოლოო, ბრიუსელი, 2013 წლის 17 ივლისი, გვ. 1 და კომისიის ვებგვერდი EPPO-ს შესახებ.

838 ევროკომისია (2013), წინადადება საბჭოს რეგულაციაზე, რომელიც შეეხება ვროკავშირის პროკურატურის შექმნას, COM(2013) 534, საბოლოო, ბრიუსელი, 2013 წლის 17 ივლისი.

839 ხელშეკრულება ევროკავშირის ფუნქციონირების შესახებ, მუხლები 86 (1) და 329 (1).

840 იხ. ევროკავშირის საბჭო (2017), პრესრელიზი, „20 წევრი სახელმწიფო ევროკავშირის პროკურატურის შექმნის დეტალებზე თანხმდება“, 2017 წლის 8 ივნისი

841 ევროკომისია (2013), წინადადება საბჭოს რეგულაციის შესახებ, რომელიც შეეხება ევროკავშირის პროკურატურის შექმნას, COM(2013) 534, საბოლოო, ბრიუსელი, 2013 წლის 17 ივლისი, გვ. 1 და კომისიის ვებგვერდი EPPO-ს შესახებ.

მოძიებებში მონაწილეობენ (როგორც გათვალისწინებულია ეროვნულ და ევროკავშირის კანონმდებლობებში, ასევე, ფუნდამენტურ უფლებათა ქარტიაში). საგამოძიებო ღონისძიებები, რომლებსაც მნიშვნელოვანი შეხება აქვთ ფუნდამენტურ უფლებებთან, საჭიროებს წინასწარი ნებართვის გაცემას ეროვნული სასამართლოების მიერ.[842] EPPO-ს გამოძიებები ექვემდებარება ეროვნული სასამართლოების მხრიდან განხილვას. [843]

EPPO-ს ადმინისტრაციული მიზნებით პერსონალური მონაცემების დამუშავებაზე ვრცელდება ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაცია, [844] ოპერაციული მიზნებით დამუშავება კი ექვემდებარება მონაცემთა დაცვის ცალკე რეჟიმს, რომელიც ევროპოლისა და ევროჯასტის საქმიანობის მარეგულირებელი წესების მსგავსია, ვინაიდან EPPO-ს ფუნქციები მოიცავს პერსონალური მონაცემების დამუშავებას შიდასახელმწიფოებრივ დონეზე არსებულ სამართალდამცველ ორგანოებსა და პროკურატურასთან ერთად. ამრიგად, მონაცემთა დაცვის წესები, რომლებიც EPPO-ს საქმიანობაზე ვრცელდება, პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოების მონაცემთა დაცვის დირექტივით გათვალისწინებული წესების მსგავსია. EPPO-ს შექმნის ინიციატივის თანახმად, პერსონალური მონაცემების დამუშავება უნდა აკმაყოფილებდეს კანონიერებისა და სამართლიანობის, მიზნის შეზღუდვის, მონაცემთა მინიმაზიციის, სიზუსტის, მთლიანობისა და კონფიდენციალობის პრინციპებს. EPPO-მ მაქსიმალურად მკაფიოდ უნდა განარჩიოს მონაცემთა სუბიექტების კატეგორიები (მაგ.: სისხლის სამართლის დანაშაულში ბრალდებული პირები, ეჭვმიტანილი პირები, დაზარალებულები და მოწმეები). იგი უნდა ამოწმებდეს დამუშავებული პერსონალური მონაცემების ხარისხს და ფაქტებზე დაფუძნებულ მონაცემებს მაქსიმალურად განარჩევდეს პირად შეფასებებზე დაფუძნებული მონაცემებისგან.

ინიციატივა ითვალისწინებს დებულებებს მონაცემთა სუბიექტების შესახებ. მათ შორის აღსანიშნავია ინფორმაციის მიღების, პერსონალურ მონაცემებზე წვდომის, გასწორების, წაშლისა და დამუშავების შეზღუდვის უფლება. ინიციატივის თანახმად, ამ უფლებებით სარგებლობა შესაძლებელია ირიბად, EDPS-ის საშუალებით. ინიციატივა ითვალისწინებს დამუშავების უსაფრთხოებისა და ანგარიშვალდებულების პრინციპებსაც და EPPO-ს ავალდებულებს შესაბამისი ტექნიკური და ორგანიზაციული ზომების მიღებას, რათა მონაცემები სათანადო დონეზე იყოს დაცული, აღირიცხოს დამუშავებასთან დაკავშირებუ-

842 ევროკომისია (2013), წინადადება საბჭოს რეგულაციის შესახებ, რომელიც შეეხება ვროკავშირის პროკურატურის შექმნას, COM(2013) 534, საბოლოო, ბრიუსელი, 2013 წლის 17 ივლისი, მუხლი 26 (4).

843 *იქვე,* მუხლი 36.

844 ევროპული პარლამენტისა და საბჭოს 2000 წლის 18 დეკემბრის რეგულაცია (EC) No. 45/2001 ვროკავშირის ინსტიტუტებისა და ორგანოების მიერ პერსონალური მონაცემების დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ 2001 L 8.

ლი ნებისმიერი საქმიანობა და დამუშავების დაწყებამდე შეფასდეს რისკები, თუკი მისი ტიპიდან გამომდინარე (მაგ.: დამუშავება ახალი ტექნოლოგიების გამოყენებით), სავარაუდოა, რომ დიდი საფრთხე შეექმნება ფიზიკურ პირთა უფლებებს. და ბოლოს, ინიციატივა ითვალისწინებს კოლეგიის მიერ მონაცემთა დაცვის ოფიცრის დანიშვნას, რომელიც სათანადოდ უნდა ჩაერთოს პერსონალური მონაცემების დაცვასთან დაკავშირებულ ყველა საკითხში. მან, ასევე უნდა უზრუნველყოს EPPO-ს შესაბამისობა მონაცემთა დაცვის არსებულ კანონმდებლობასთან.

8.3.2 მონაცემთა დაცვა ევროკავშირის საერთო საინფორმაციო სისტემებში

წევრ სახელმწიფოებს შორის მონაცემთა გაცვლასა და ევროკავშირის დონეზე საერთაშორისო დანაშაულთან ბრძოლის სპეციალიზებული ორგანოების შექმნასთან ერთად (მაგ.: ევროპოლი, ევროჯასტი და EPPO), შემუშავდა რამდენიმე სახის საერთო საინფორმაციო სისტემაც. ეს სისტემები ხელს უწყობს თანამშრომლობასა და მონაცემთა გაცვლას ეროვნულ და ევროკავშირის უფლებამოსილ ორგანოებს შორის, კერძოდ, ისეთ სფეროებში, როგორიცაა: საზღვრის დაცვა, იმიგრაცია, თავშესაფრის მოთხოვნა და საბაჟო საკითხები. ევროკავშირის კანონმდებლობისგან დამოუკიდებელი საერთაშორისო შეთანხმების საფუძველზე შენგენის ზონის შექმნასთან ერთად, მრავალმხრივი შეთანხმებებით ჩამოყალიბდა ამ გაერთიანების საინფორმაციო სისტემა (SIS), რომელიც შემდგომ ევროკავშირის კანონმდებლობაში გაერთიანდა. სავიზო საინფორმაციო სისტემა (VIS), ევროდაკი, ევროსური და საბაჟო საინფორმაცი სისტემა (CIS) შემუშავდა იმ ინსტრუმენტების სახით, რომლებსაც ევროკავშირის კანონმდებლობა არეგულირებს.

ამ სისტემებზე კონტროლს ახორციელებენ ეროვნული საზედამხედველო ორგანოები და EDPS. მაღალი დონის დაცვისათვის, აღნიშნული ორგანოები თანამშრომლობენ ზედამხედველობის საკოორდინაციო ჯგუფების (SCG) ფორმატში, რაც აერთიანებს ისეთ ფართომასშტაბიან საინფორმაციო-ტექნოლოგიურ სისტემებს, როგორიცაა: 1) ევროდაკი; 2) სავიზო საინფორმაციო სისტემა; 3) შენგენის საინფორმაციო სისტემა; 4) საბაჟო საინფორმაციო სისტემა და 5) შიდა ბაზრის საინფორმაციო სისტემა.[845] ზედამხედველობის საკოორდინაციო ჯგუფები, როგორც წესი, არჩეული თავმჯდომარის ხელმძღვანელობით ხვდებიან წელიწადში ორჯერ. ისინი ამტკიცებენ სახელმძღვანელო პრინციპებს, განიხილავენ სახელმწიფოთაშორის შემთხვევებს ან ადგენენ ინსპექტირების საერთო ჩარჩოს.

845 იხ. ევროკავშირის მონაცემთა დაცვის ზედამხედველის ვებგვერდი ზედამხედველობის კოორდინაციაზე.

ფართომასშტაბიანი საინფორმაციო ტექნოლოგიური სისტემების ევროპული სააგენტო (eu-LISA) [846] შეიქმნა 2012 წელს. მის ფუნქციებში შედის შენგენის საინფორმაციო სისტემის მეორე თაობის (SIS II), სავიზო საინფორმაციო სისტემისა (VIS) და ევროდაკის ოპერაციული მართვა. eu-LISA-ს მთავარი მიზანია საინფორმაციო ტექნოლოგიური სისტემების ეფექტიანობა, უსაფრთხოება და მდგრადი მუშაობა. სააგენტო პასუხისმგებელია ისეთი ზომების მიღებაზეც, რომლებიც უზრუნველყოფს სისტემებისა და მონაცემების დაცულობას.

შენგენის საინფორმაციო სისტემა

1985 წელს, ყოფილი ევროპული თანამეგობრობის რამდენიმე წევრმა ქვეყანამ ბენილუქსის ეკონომიკური გაერთიანების წევრ სახელმწიფოებთან - გერმანიასა და საფრანგეთთან - დადო შეთანხმება საერთო საზღვრების ეტაპობრივ გაუქმებაზე (შენგენის შეთანხმება). ეს მიზნად ისახავდა პირთა თავისუფალი გადაადგილების ზონის შექმნას შენგენის ტერიტორიაზე, სასაზღვრო კონტროლის გარეშე.[847] ღია საზღვრების პირობებში საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, შენგენის ზონის გარე საზღვრებზე შეიქმნა გაძლიერებული სასაზღვრო კონტროლი და დამყარდა მჭიდრო თანამშრომლობა შიდასახელმწიფოებრივ პოლიციასა და სამართალდამცველ ორგანოებს შორის.

შენგენის შეთანხმებაში სხვა სახელმწიფოების გაერთიანების შედეგად, სისტემა საბოლოოდ ინტეგრირდა ევროკავშირის სამართლებრივ სისტემაში, ამსტერდამის ხელშეკრულების საფუძველზე.[848] გადაწყვეტილება დაინერგა 1999 წელს. შენგენის საინფორმაციო სისტემის უახლესი ვერსია, ე.წ. SIS III, ამოქმედდა 2013 წლის 9 აპრილს. ამჟამად იგი ემსახურება ევროკავშირის წევრი ქვეყნების უმრავლესობას,[849] ასევე, ისლანდიას, ლიხტენშტაინს, ნორ-

846 ევროპული პარლამენტისა და საბჭოს 2011 წლის 25 ოქტომბრის რეგულაცია (EU) No. 1077/2011 თავისუფლების, უსაფრთხოებისა და მართლმსაჯულების სფეროში ფართომასშტაბიანი ინფორმაციული ტექნოლოგიების სისტემათა ევროპული სააგენტოს დაფუძნების შესახებ, OJ 2011 L 286.

847 შეთანხმება ბენილუქსის ეკონომიკური კავშირის ქვეყნების მთავრობას, გერმანიის ფედერაციულ რესპუბლიკასა და საფრანგეთის რესპუბლიკას შორის საერთო საზღვრებზე შემოწმების ეტაპობრივი გაუქმების შესახებ, OJ 2000 L 239.

848 ევროპული გაერთიანება (1997), ამსტერდამის ხელშეკრულება, რომელსაც ცვლილება შეაქვს ევროპული კავშირის ხელშეკრულებაში, ევროპული გაერთიანების შექმნისა და დაკავშირებულ აქტებში, OJ 1997 C 340.

849 ხორვატია, კვიპროსი და ირლანდია ახორციელებენ მოსამზადებელ სამუშაოებს SIS II-ში ინტეგრაციის მიზნით, თუმცა, ისინი ჯერ არ არიან სისტემის წევრები. შენგენის საინფორმაციო სისტემაზე ინფორმაცია ხელმისაწვდომია ევროკომისიის მიგრაციისა და შინაგან საკითხთა გენერალური დირექტორატის ვებგვერდზე.

ვეგიასა და შვეიცარიას.[850] SIS II-ზე წვდომა აქვთ ევროპოლსა და ევროჯასტ-საც.

SIS II-ში ერთიანდება: ცენტრალური სისტემა (C-SIS), შიდასახელმწიფოებრივი სისტემა (N-SIS) ევროკავშირის თითოეულ წევრ ქვეყანაში, და ცენტრალურ და შიდასახელმწიფოებრივ სისტემებს შორის საკომუნიკაციო ინფრასტრუქტურა. C-SIS მოიცავს ევროკავშირის წევრი სახელმწიფოების მიერ შეყვანილ კონკრეტულ მონაცემებს პირებისა და ობიექტების შესახებ. C-SIS-ს იყენებენ შიდასახელმწიფოებრივი სასაზღვრო კონტროლის, პოლიციის, საბაჟო, სავიზო და სამართალდამცველი ორგანოები, შენგენის ზონის მასშტაბით. ევროკავშირის თითოეულ წევრ სახელმწიფოში ფუნქციონირებს შენგენის შიდასახელმწიფოებრივი საინფორმაციო სისტემა (N-SIS), C-SIS-ის დუბლიკატი, რომელიც მუდმივად განახლებადია, C-SIS-თან ერთად. SIS-ის სისტემაში არსებობს განგაშის რამდენიმე ტიპი:

- პირს არ აქვს უფლება, შევიდეს ან დარჩეს შენგენის ტერიტორიაზე;
- პირი ან ობიექტი იძებნება სასამართლო ან სამართალდამცველი ორგანოების მიერ (მაგ.: ევროკავშირის დაკავების ორდერი, ფრთხილი შემოწმების მოთხოვნა);
- პირი გამოცხადებულია დაკარგულად;
- საქონელი, როგორიცაა ბანკნოტები, ავტომანქანები, სატვირთო ფურგონები, იარაღი ან საიდენტიფიკაციო დოკუმენტები, აღიარებულია მოპარულად ან დაკარგულ საკუთრებად.

განგაშის შემთხვევაში რეაგირების მიზნით ხდება შესაბამისი აქტივობების ინიცირება SIRENE-ის ბიუროს საშუალებით. SIS II-ს აქვს ახალი ფუნქციები. კერძოდ, სისტემაში ამჟამად შესაძლებელია შემდეგი ინფორმაციის შეყვანა: ბიომეტრიული მონაცემები (თითის ანაბეჭდები და ფოტოები); ახალი კატეგორიები (მოპარული გემები, საჰაერო ხომალდები, კონტეინერები ან გადახდის საშუალებები); გაძლიერებული განგაში პირებსა და ობიექტებზე; ევროკავშირის დაკავების ორდერის (EAW) ასლები ძებნილი პირების დაკავების, ჩაბარებისა და ექსტრადირებისთვის.

SIS II ეფუძნება ორ ურთიერთშემავსებელ აქტს - SIS II-ის გადაწყვეტილება-

850 ევროპული პარლამენტისა და საბჭოს 2006 წლის 20 დეკემბრის რეგულაცია (EC) No. 1987/2006 შენგენის საინფორმაციო სისტემის მეორე თაობის შექმნის, ოპერირებისა და გამოყენების შესახებ, OJ 2006 L 381 (SIS II) და ევროკავშირის საბჭოს 2007 წლის 12 ივნისის გადაწყვეტილება 2007/533/JHA შენგენის საინფორმაციო სისტემის მეორე თაობის შექმნის, ოპერირებისა და გამოყენების შესახებ, (SIS II), OJ 2007 L 205.

სა[851] და რეგულაციას.[852] ევროკავშირის კანონმდებლებმა განსხვავებული სამართლებრივი საფუძვლები გამოიყენეს გადაწყვეტილებისა და რეგულაციის მისაღებად. გადაწყვეტილება არეგულირებს SIS II-ის გამოყენებას, სისხლის სამართლის საკითხებზე პოლიციასა და სასამართლო ორგანოებს შორის თანამშრომლობით გათვალისწინებული მიზნებით (ევროკავშირის ყოფილი მესამე ბურჯი). რეგულაცია ვრცელდება განგაშის პროცედურებზე, რომლებიც შეეხება ვიზებს, თავშესაფარს, იმიგრაციასა და ფიზიკურ პირთა თავისუფალ გადაადგილებასთან დაკავშირებულ სხვა საკითხებს (ყოფილი პირველი ბურჯი). თითოეული სვეტისათვის გათვალისწინებული განგაშის პროცედურები სხვადასხვა აქტით დარეგულირდა, რადგან ეს ორი აქტი (გადაწყვეტილება და რეგულაცია) მიღებულია ლისაბონის ხელშეკრულებამდე და ბურჯების სტრუქტურის გაუქმებამდე.

ორივე სამართლებრივი აქტი შეიცავს წესებს მონაცემთა დაცვის შესახებ. SIS II-ის გადაწყვეტილება კრძალავს განსაკუთრებული კატეგორიის მონაცემთა დამუშავებას[853] და ადგენს, რომ პერსონალური მონაცემების დამუშავება რეგულირდება მოდერნიზებული 108-ე კონვენციით.[854] ამასთან, ფიზიკურ პირებს ენიჭებათ უფლება, ჰქონდეთ წვდომა მათ შესახებ SIS II-ში შეტანილ პერსონალურ მონაცემებზე.[855]

SIS II-ის რეგულაცია არეგულირებს პირობებსა და პროცედურებს იმ მონაცემების შესაყვანად, რომლებიც უკავშირდება მესამე ქვეყნის მოქალაქეებისთვის უარის თქმას ევროკავშირის ტერიტორიაზე შესვლასა ან დარჩენაზე; ასევე, ადგენს დამატებითი ინფორმაციის გაცვლის წესებს წევრ სახელმწიფოში შესვლის ან დარჩენისათვის.[856] რეგულაცია შეიცავს მონაცემთა დაცვის წესებსაც. დაუშვებელია განსაკუთრებული კატეგორიის მონაცემების დამუშავება, როგორც ეს განმარტებულია მონაცემთა დაცვის ზოგადი რეგულაციის მე-9 მუხლის პირველ პუნქტში.[857] SIS II-ის რეგულაცია გარკვეულ უფლებებსაც ანიჭებს მონაცემთა სუბიექტებს, კერძოდ:

---

851 ევროკავშირის საბჭო (2007), საბჭოს 2007 წლის 12 ივნისის გადაწყვეტილება 2007/533/JHA შენგენის საინფორმაციო სისტემის მეორე თაობის შექმნის, ოპერირებისა და გამოყენების შესახებ, OJ L 205, 2007 წლის 7 აგვისტო.

852 ევროპული პარლამენტისა და საბჭოს 2006 წლის 20 დეკემბრის რეგულაცია (EC) No. 1987/2006 შენგენის საინფორმაციო სისტემის მეორე თაობის შექმნის, ოპერირებისა და გამოყენების შესახებ, OJ 2006 L 381, 2006 წლის 28 დეკემბერი.

853 SIS II გადაწყვეტილება, მუხლი 56; SIS II რეგულაცია, მუხლი 40.

854 SIS II გადაწყვეტილება, მუხლი 57.

855 SIS II გადაწყვეტილება, მუხლი 58; SIS II რეგულაცია, მუხლი 41.

856 SIS II რეგულაცია, მუხლი 2.

857 *იქვე,* მუხლი 40.

- მონაცემთა სუბიექტის შესახებ არსებულ პერსონალურ მონაცემებზე წვდომა;[858]

- ფაქტობრივად უზუსტო მონაცემების გასწორება;[859]

- უკანონოდ შენახული მონაცემების წაშლა; [860] და

- შეტყობინების მიღება, თუ მონაცემთა სუბიექტზე სისტემაში გამოცხადებულია განგაში. ინფორმაცია მონაცემთა სუბიექტს წერილობითი სახით უნდა მიეწოდოს, იმ ადგილობრივი გადაწყვეტილების ასლთან ერთად (ან მასზე მითითებით), რომლის საფუძველზეც სისტემაში გამოცხადდა განგაში.[861]

ინფორმაციის მიღების უფლება არ მოქმედებს, თუ: 1) პერსონალური მონაცემები არ მოუპოვებიათ მონაცემთა სუბიექტისგან და ინფორმირება შეუძლებელია ან არაპროპორციულ ძალისხმევას მოითხოვს; 2) მონაცემთა სუბიექტი უკვე ფლობს შესაბამის ინფორმაციას; 3) ეროვნული კანონმდებლობა იძლევა ამ უფლების შეზღუდვის საშუალებას, მათ შორის, ეროვნული უსაფრთხოების ან სისხლის სამართლებრივი დანაშაულების პრევენციის მიზნით. [862]

როგორც SIS II გადაწყვეტილების, ისე SIS II რეგულაციის თანახმად, SIS II-ზე წვდომის უფლებით სარგებლობა შესაძლებელია ნებისმიერ წევრ სახელმწიფოში, ასეთ მოთხოვნაზე რეაგირება კი უნდა განხორციელდეს წევრ სახელმწიფოში მოქმედი კანონმდებლობის შესაბამისად.[863]

> მაგალითი: საქმეში *Dalea v. France*[864] განმცხადებელს უარი ეთქვა საფრანგეთის ვიზაზე, რადგან საფრანგეთის შესაბამისი ორგანოების მიერ შენგენის საინფორმაციო სისტემაში შეტანილი ინფორმაციის თანახმად, ამ პირს ქვეყანაში შესვლა ეკრძალებოდა. განმცხადებელმა საფრანგეთის მონაცემთა დაცვის კომისიას და შემდგომ სახელმწიფო საბჭოს მოსთხოვა მონაცემებზე წვდომა, მათი გასწორება ან წაშლა, მაგრამ უშედეგოდ. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ განმცხადებლის შესახებ შენგენის საინფორმაციო სისტემაში არსებული

858 *იქვე,* მუხლი 41 (1).

859 *იქვე,* მუხლი 41 (5).

860 *იქვე,* მუხლი 41 (5).

861 *იქვე,* მუხლი 42 (1).

862 *იქვე,* მუხლი 42 (2).

863 SIS II რეგულაცია, მუხლი 41 (1) და SIS II გადაწყვეტილება, მუხლი 58.

864 ECtHR, *Dalea v. France,* No. 964/07, 2010 წლის 2 თებერვალი.

ჩანაწერი კანონმდებლობას შეესაბამებოდა და ეროვნული უსაფრთხოების დაცვის კანონიერ მიზანს ემსახურებოდა. ვინაიდან განმცხადებელმა ვერ დაასაბუთა შენგენის ზონაში შესვლაზე უარის თქმით მიყენებული ზიანი და არსებობდა საკმარისი ზომები განმცხადებლის დაუსაბუთებელი გადწყვეტილებებისგან დასაცავად, მისი პირადი ცხოვრების პატივისცემის უფლებაში ჩარევა იყო პროპორციული. შესაბამისად, კონვენციის მე-8 მუხლის საფუძველზე განმცხადებლის მიერ შეტანილი განაცხადი სასამართლომ დასაშვებად არ ცნო.

ადგილობრივ საინფორმაციო სისტემას (N-SIS) მართავს ევროკავშირის თითოეულ წევრ სახელმწიფოში არსებული კომპეტენტური საზედამხედველო ორგანო, რომელიც N-SIS-ში ატარებს მონაცემთა დამუშავების ოპერაციების აუდიტს, სულ მცირე, 4 წელიწადში ერთხელ.[865] ეროვნული საზედამხედველო ორგანოები და EDPS, ერთმანეთთან თანამშრომლობით, უზრუნველყოფენ N-SIS-ის კოორდინირებულ ზედამხედველობას. ამავდროულად, EDPS-ის პასუხისმგებლობაში შედის C-SIS-ის კონტროლიც. გამჭვირვალობის მიზნით, საქმიანობის ერთობლივი ანგარიში ეგზავნება ევროპარლამენტს, საბჭოსა და eu-LISA-ს, ყოველ ორ წელიწადში ერთხელ. SIS II-ის ზედამხედველობის საკოორდინაციო ჯგუფი (SCG) შექმნილია SIS-ის კონტროლის კოორდინირებისთვის. ჯგუფი წელიწადში ორჯერ იკრიბება და მის შემადგენლობაში არიან: EDPS-ის წევრები; იმ სახელმწიფოებში არსებული საზედამხედველო ორგანოების წარმომადგენლები, რომლებმაც SIS II დანერგეს; ისლანდიის, ლიხტენშტაინის, ნორვეგიისა და შვეიცარიის საზედამხედველო ორგანოების წარმომადგენლები (სისტემა მათზეც ვრცელდება, რაკი შენგენის ზონის წევრები არიან).[866] SIS II ჯერჯერობით არ მოიცავს კვირპოსს, ხორვატიასა და ირლანდიას. შესაბამისად, ისინი SCG-ში დამკვირვებლების სტატუსით მონაწილეობენ. SCG-ის კონტექსტში, EDPS და ეროვნული საზედამხედველო ორგანოები აქტიურად თანამშრომლობენ, ცვლიან ინფორმაციას, ეხმარებიან ერთმანეთს აუდიტსა და ინსპექტირებაში, ქმნიან ჰარმონიზებულ წინადადებებს პოტენციური პრობლემების გადაჭრის საერთო გზების გამოსავლენად და ხელს უწყობენ ცნობიერების ამაღლებას მონაცემთა დაცვის უფლებებზე.[867] საკოორდინაციო ჯგუფი სახელმძღვანელო პრინციპებსაც ამტკიცებს მონაცემთა სუბიექტების დასახმარებლად (მაგ.: წვდომის უფლებით სარგებლობის შესახებ).[868]

865 SIS II რეგულაცია, მუხლი 60 (2).

866 იხ: ევროკავშირის მონაცემთა დაცვის ზედამხედველის ვებგვერდი შენგენის საინფორმაციო სისტემის შესახებ.

867 SIS II რეგულაცია, მუხლი 46 და SIS II გადაწყვეტილება, მუხლი 62.

868 იხ. SIS II SCG, შენგენის საინფორმაციო სისტემა. წვდომის უფლებით სარგებლობის სახელმძღვანელო, ხელმისაწვდომია EDPS-ის ვებგვერდზე.

სამომავლო პერსპექტივები

2016 წელს ევროკომისიის მიერ SIS-ის შეფასების შედეგებმა აჩვენა,[869] რომ შიდასახელმწიფოებრივ დონეზე შექმნილი მექანიზმები მონაცემთა სუბიექტებს საშუალებას აძლევს, მოითხოვონ SIS II-ში არსებულ პერსონალურ მონაცემებზე წვდომა, მათი გასწორება და წაშლა, ანდა მიიღონ კომპენსაცია არაზუსტი მონაცემების გამო. SIS II-ის ეფექტიანობის გასაუმჯობესებლად, ევროკომისიამ წარმოადგინა 3 ახალი რეგულაციის შექმნის წინადადება:

- რეგულაცია სასაზღვრო შემოწმებათა სფეროში SIS-ის შექმნის, ოპერირებისა და გამოყენების შესახებ, რითაც გაუქმდება SIS II-ის რეგულაცია;

- რეგულაცია პოლიციისა და სისხლის სამართლის მართლმსაჯულების საკითხებზე თანამშრომლობის სფეროებში SIS-ის შექმნის, ოპერირებისა და გამოყენების შესახებ, რითაც უქმდება SIS II-ის გდაწყვეტილება;

- რეგულაცია SIS-ის გამოყენებაზე მესამე ქვეყნის მოქალაქეთა დასაბრუნებლად, რომლებიც ევროკავშირის ტერიტორიაზე არალეგალურად იმყოფებიან.

აღსანიშნავია, რომ წარმოდგენილი ინიციატივები SIS II-ის რეჟიმში შემავალ თითის ანაბეჭდებსა და ფოტოებთან ერთად, სხვა კატეგორიის ბიომეტრიული მონაცემების დამუშავების საშუალებასაც იძლევა. SIS ბაზაში შესაძლებელი იქნება სახისა თუ ხელისგულის ანაბეჭდებისა და დნმ-ის პროფილების შენახვაც. მაშინ, როდესაც SIS II-ის რეგულაცია და გადაწყვეტილება იძლევა პირის თითის ანაბეჭდებით იდენტიფიცირების შესაძლებლობას, წარმოდგენილი ინიციატივებით ასეთი ძიება სავალდებულო ხდება, თუ ვინაობის დადგენა სხვა გზით შეუძლებელია. სისტემაში ძიება და ადამიანების იდენტიფიცირება მოხდება სახის გამოსახულებების, ფოტოებისა და ხელისგულის ანაბეჭდების გამოყენებით, როგორც კი ეს ტექნიკურად იქნება შესაძლებელი. ახალი წესები ბიომეტრიული მახასიათებლების შესახებ განსაკუთრებულ საფრთხეებს უქმნის ფიზიკურ პირთა უფლებებს. კომისიის ინიციატივებზე წარმოდგენილ მოსაზრებაში[870] EDPS-მა აღნიშნა, რომ ბიომეტრიული მონაცემები უაღრესად სენსიტიურია და მათი გაერთიანება ასეთ ფართო მასშტაბის მონაცემთა ბაზაში უნდა დაეფუძნოს SIS-ში შეტანის აუცილებლობის მტკიცებულებას. სხვა

869 ევროპული კომისია (2016), კომისიის ანგარიში ევროპარლამენტსა და საბჭოს, შენგენის საინფორმაციო სისტემის მეორე თაობის (SIS II) შეფასების შესახებ, (EC) No. 1987/2006 რეგულაციის 24 (5), 43 (3) და 50 (5) და 2007/533/JHA გადაწყვეტილების 59 (3) და 66 (5) მუხლების შესაბამისად, COM(2016) 880, საბოლოო, ბრიუსელი, 2016 წლის 21 დეკემბერი.

870 EDPS (2017), EDPS-ის მოსაზრება შენგენის საინფორმაციო სისტემის ახალი სამართლებრივი საფუძვლის შესახებ, მოსაზრება 7/2017, 2017 წლის 2 მაისი.

სიტყვებით რომ ვთქვათ, EDPS-მა მიიჩნია, რომ აუცილებელია, დამატებით განიმარტოს, რა ტიპის ინფორმაციის შეტანა შეიძლება დნმ-ის პროფილში. ვინაიდან დნმ-ის პროფილი მოიცავს სენსიტიურ ინფორმაციას (მაგ.: ჯანმრთელობის პრობლემებთან დაკავშირებით), SIS-ში შენახული დნმ-ის პროფილი უნდა შეიცავდეს: „მხოლოდ მინიმალურ ინფორმაციას, რომელიც მკაცრად აუცილებელია დაკარგული პირების იდენტიფიცირებისათვის და გამორიცხავს ინფორმაციას, რომელიც ცალსახად შეეხება ჯანმრთელობის მდგომარეობას, რასობრივ წარმომავლობასა და ნებისმიერ სხვა სენსიტიურ ინფორმაციას.“ [871]ამავდროულად, წარმოდგენილი ინიციატივები აწესებს უსაფრთხოების დამატებით ზომებს, რათა მონაცემები შეგროვდეს და დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც მკაცრად აუცილებელია ოპერაციულ დონეზე, ხოლო მათზე წვდომა ჰქონდეთ მხოლოდ იმ პირებს, რომელთაც აქვთ პერსონალური მონაცემების დამუშავების ოპერაციული საჭიროება.[872] წარმოდგენილი ინიციატივების საშუალებით, eu-LISA შეძლებს, წევრ სახელმწიფოებს რეგულარულად წარუდგინოს ანგარიშები მონაცემთა ხარისხის შესახებ, რათა პერიოდულად გადაიხედოს საინფორმაციო სისტემებში შეტანილი ინფორმაცია მონაცემთა ხარისხის უზრუნველსაყოფად.[873]

სავიზო-საინფორმაციო სისტემა

სავიზო-საინფორმაციო სისტემა (VIS), რომელსაც ასევე eu-LISA მართავს, შექმნილია ევროკავშირის საერთო სავიზო პოლიტიკის დანერგვის ხელშესაწყობად.[874] VIS შენგენის სახელმწიფოებს საშუალებას აძლევს, სავიზო მონაცემები გაცვალონ ცენტრალიზებული სისტემის მეშვეობით, რომელიც მესამე ქვეყნებში მდებარე შენგენის სახელმწიფოთა საკონსულოებს აკავშირებს გაერთიანების ყველა გარე სასაზღვრო-გამშვებ პუნქტთან. VIS ამუშავებს მო-

871 *იქვე,* პუნქტი 22.

872 ევროპული კომისია (2016), წინადადება ევროპარლამენტის და საბჭოს რეგულაციაზე, რომელიც შეეხება შენგენის საინფორმაციო სისტემის (SIS) შექმნას, ოპერირებასა და მართვას პოლიციისა და სისხლის სამართლის მართლმსაჯულების საკითხებზე თანამშრომლობის სფეროებში, რომელსაც შესწორება შეაქვს (EU) No. 515/2014 რეგულაციაში და აუქმებს (EC) No. 1986/2006 რეგულაციას, საბჭოს გადაწყვეტილებას 2007/533/JHA და კომისიის გადაწყვეტილებას 2010/261/EU, COM(2016) 883, საბოლოო, ბრიუსელი, 2016 წლის 21 დეკემბერი.

873 *იქვე,* გვ. 15.

874 ევროკავშირის საბჭოს 2004 წლის 8 ივნისის გადაწყვეტილება 2004/512/EC სავიზო საინფორმაციო სისტემის (VIS) შექმნის შესახებ, OJ 2004 L 213; ევროპარლამენტისა და საბჭოს 2008 წლის 9 ივლისის რეგულაცია (EC) No. 767/2008, რომელიც შეეხება სავიზო საინფორმაციო სისტემას (VIS) და წევრ სახელმწიფოებს შორის მონაცემების გაცვლას მოკლევადიან ვიზებთან დაკავშირებით, OJ 2008 L 218 (VIS რეგულაცია); ევროკავშირის საბჭოს 2008 წლის 23 ივნისის გადაწყვეტილება 2008/633/JHA, რომელიც შეეხება VIS-ზე წვდომას წევრი სახელმწიფოების შესაბამისი ორგანოებისა და ევროპოლის მიერ ტერორისტული და მძიმე დანაშაულების პრევენციის, გამოვლენისა და გამოძიების მიზნით, OJ 2008 L 218.

ნაცემებს მოკლევადიან სავიზო განაცხადებზე, შენგენის ზონაში ვიზიტის ან ტრანზიტის მიზნით. ეს სისტემა სასაზღვრო ორგანოებს საშუალებას აძლევს, ბიომეტრიული მონაცემების მეშვეობით (განსაკუთრებით, თითის ანაბეჭდებით) განსაზღვრონ, არის თუ არა ვიზის წარმდგენი პირი მისი მართლზომიერი მფლობელი და მოახდინონ მისი იდენტიფიცირება დოკუმენტების არქონის ან გაყალბების შემთხვევაში.

ევროპარლამენტისა და საბჭოს რეგულაცია (EC) No. 767/2008, რომელიც შეეხება სავიზო საინფორმაციო სისტემას და ევროკავშირის წევრ ქვეყნებს შორის მონაცემთა გაცვლას მოკლევადიან ვიზებთან დაკავშირებით (VIS რეგულაცია), არეგულირებს ამ მიზნებით პერსონალური მონაცემების გადაცემის წესებსა და პირობებს; ასევე, ზედამხედველობას უწევს სავიზო განაცხადებზე მიღებულ გადაწყვეტილებებს, მათ შორის, ანულირების, გაუქმების ან გახანგრძლივების შესახებ.[875] VIS რეგულაცია ძირითადად შეეხება განმცხადებლის მონაცემებს, ვიზებს, ფოტოებს, თითის ანაბეჭდებს, წინა და თანმხლებ პირთა განაცხადებს, ასევე, მომწვევი პირების მონაცემებს.[876] VIS-ზე წვდომა მონაცემების შეყვანის, გასწორების ან წაშლის მიზნით მკაცრად არის შეზღუდული და ამ შესაძლებლობით სარგებლობა მხოლოდ სავიზო ორგანოების წარმომადგენლებს შეუძლიათ. ამავდროულად, საკონსულტაციო მონაცემებზე წვდომით სარგებლობენ სავიზო ორგანოებისა და კომპეტენტური ორგანოების წარმომადგენლები, გარე სასაზღვრო კვეთის წერტილებში შემოწმების, საიმიგრაციო შემოწმებისა და თავშესაფრის კონტროლისთვის.

გარკვეული პირობებისას, ევროკავშირის წევრი სახელმწიფოს პოლიციის ორგანოებსა და ევროპოლს შეუძლიათ, მოითხოვონ წვდომა VIS-ში შეყვანილ მონაცემებზე, ტერორისტული და დანაშაულებრივი ქმედებების პრევენციის, გამოვლენისა და გამოძიების მიზნებით.[877] როგორც აღინიშნა, მიზნის შეზღუდვის პრინციპი (იხ. თავი 3.2) საჭიროებს, რომ პერსონალური მონაცემები დამუშავდეს მხოლოდ კონკრეტული, ცალსახა და ლეგიტიმური მიზნებით, დამუშავება იყოს ადეკვატური, რელევანტური და არ აჭარბებდეს იმ ამოცანას, რისთვისაც ისინი დამუშავდა. ვინაიდან VIS შექმნილია, როგორც საერთო სავიზო პოლიტიკის იმპლემენტაციის მხარდასაჭერი ინსტრუმენტი,

875 VIS რეგულაცია, მუხლი 1.

876 ევროპული პარლამენტისა და საბჭოს 2008 წლის 9 ივლისის (EC) No. 767/2008 რეგულაციის მე-5 მუხლი, რომელიც შეეხება სავიზო საინფორმაციო სისტემას (VIS) და წევრ სახელმწიფოებს შორის მონაცემების გაცვლას მოკლევადიან ვიზებთან დაკავშირებით (VIS რეგულაცია), OJ 2008 L 218.

877 ევროკავშირის საბჭო (2008), საბჭოს 2008 წლის 23 ივნისის გადაწყვეტილება 2008/633/JHA, რომელიც შეეხება წევრი ქვეყნებისა და ევროპოლის მიერ განსაზღვრული უფლებამოსილი ორგანოების მიერ VIS-ზე წვდომას, ტერორისტული ქმედებებისა და სხვა მძიმე დანაშაულების პრევენციის, გამოვლენისა და გამოძიების მიზნებით, OJ 2008 L 218.

მიზნის შეზღუდვის პრინციპი დარღვეულად ჩაითვლება, თუ VIS გადაიქცევა სამართალდამცველ ინსტრუმენტად. ამ მიზეზით, ეროვნულ სამართალდამცველ ორგანოებსა და ევროპოლს არ აქვთ VIS-ის მონაცემთა ბაზაზე რუტინული წვდომის უფლება. წვდომა დაშვებულია მხოლოდ ცალკეულ შემთხვევებში და უსაფრთხოების მკაცრი ზომების არსებობისას. ამ ორგანოების მიერ VIS-ზე წვდომასა და მასში დაცული მონაცემების გამოყენებას არეგულირებს საბჭოს გადაწყვეტილება 2008/633/JHA.[878]

ამასთან, VIS-ის რეგულაცია ითვალისწინებს მონაცემთა სუბიექტების უფლებებს, მათ შორის, როგორიცაა:

- შესაბამისი წევრი სახელმწიფოსგან ინფორმაციის მიღება იმ პირის ვინაობისა და საკონტაქტო მონაცემების შესახებ, რომელიც პასუხისმგებელია დამუშავებაზე ამ სახელმწიფოში და რომლის მიზნებისთვისაც ხორციელდება ეს პროცესი VIS-ის ფარგლებში; იმ პირთა კატეგორიები, რომლებსაც შეიძლება გადაეცეს მონაცემები (მიმღებთა კატეგორიები) და მონაცემთა შენახვის ვადა. სავალდებულოა ვიზის განმცხადებელთა ინფორმირება, რომ მათი პერსონალური მონაცემების შეგროვება VIS-ის ფარგლებში სავალდებულოა ამ პირთა სავიზო განაცხადის განსახილველად. ამასთან, წევრმა სახელმწიფოებმა ვიზის განმცხადებლებს უნდა განუმარტონ მათი უფლებები მონაცემებზე წვდომის, გასწორების ან წაშლის მხრივ, ასევე, პროცედურები, რომლებიც მათ აძლევს ამ უფლებებით სარგებლობის საშუალებას. [879]

- მათ შესახებ VIS-ში შეტანილ პერსონალურ მონაცემებზე წვდომა.[880]

- მცდარი/არასწორი ინფორმაციის გასწორება.[881]

- უკანონოდ შენახული მონაცემების წაშლა.[882]

VIS-ზე ზედამხედველობის მიზნით შეიქმნა სპეციალური საკოორდინაციო ჯგუფი (SCG). ჯგუფში ერთიანდებიან: EDPS-ისა და ეროვნული საზედამხედველო ორგანოების წარმომადგენლები, რომლებიც წელიწადში ორჯერ იკრიბებიან; ევროკავშირის 28 წევრი სახელმწიფოს, ასევე, ისლანდიის, ლიხტენშტაინის, ნორვეგიისა და შვეიცარიის წარმომადგენლები.

878 *იქვე.*

879 VIS რეგულაცია, მუხლი 37.

880 *იქვე,* მუხლი 38 (1).

881 *იქვე,* მუხლი 38 (2).

882 *იქვე,* მუხლი 38 (2).

ევროდაკი

Eurodac ნიშნავს/განიმარტება, როგორც ევროპული დაქტილოსკოპია (European Dactyloscopy).[883] ამ ცენტრალიზებულ სისტემაში ერთიანდება იმ მესამე ქვეყნის მოქალაქეებისა და მოქალაქეობის არმქონე პირების თითის ანაბეჭდები, რომლებმაც თავშესაფრის მოთხოვნით მიმართეს ევროკავშირის წევრ ქვეყანას.[884] სისტემა ფუნქციონირებს 2003 წლის იანვრიდან, საბჭოს 2725/2000 რეგულაციის მიღების შემდგომ. რეგულაციის შესწორებული ვარიანტი ძალაში შევიდა 2015 წელს. იგი ადგენს კრიტერიუმებსა და მექანიზმებს, რომელთა მეშვეობითაც განისაზღვრება თავშესაფრის მაძიებლის განაცხადის განხილვაზე პასუხისმგებელი სახელმწიფო, როდესაც განაცხადი ევროკავშირის ტერიტორიაზე შეაქვს მესამე ქვეყნის მოქალაქეს ან მოქალაქეობის არმქონე პირს (დუბლინის III რეგულაცია, 343/2003).[885] ევროდაკში დაცული პერსონალური მონაცემების გამოყენება შესაძლებელია მხოლოდ ამ რეგულაციის ხელშესაწყობად.[886]

ეროვნულ სამართალდამცველ ორგანოებსა და ევროპოლს აქვთ უფლება, სისხლის სამართლის გამოძიებასთან დაკავშირებული თითის ანაბეჭდები შეადარონ ევროდაკში დაცულ მონაცემებს, თუმცა, მხოლოდ და მხოლოდ ტერორისტული და სხვა მძიმე დანაშაულების პრევენციის, გამოვლენისა და გამოძიების მიზნით. ვინაიდან ევროდაკი ევროკავშირის თავშესაფრის პოლიტიკის დანერგვის ინსტრუმენტია და არა სამართალდამცველი მექანიზმი, სამართალდამცველ ორგანოებს მონაცემთა ბაზაზე ხელი მიუწვდებათ მხოლოდ კონკრეტულ შემთხვევებსა და გარემოებებში, მკაცრად განსაზღვრული პირობებით.[887] მონაცემების შემდგომ გამოყენებას სამართალდამცველი მიზ-

883 იხ. ევროკავშირის მონაცემთა დაცვის ზედამხედველის ვებგვერდი ევროდაკზე.

884 საბჭოს 2000 წლის 11 დეკემბრის (EC) No. 2725/2000 რეგულაცია, რომელიც შეეხება ევროდაკის შექმნას თითის ანაბეჭდების შესადარებლად, დუბლინის კონვენციის ეფექტიანი გამოყენებისათვის, OJ 2000 L 316; საბჭოს 2002 წლის 28 თებერვლის რეგულაცია (EC) No. 407/2002, რომელიც განსაზღვრავს (EC) No. 2725/2000 რეგულაციის განხორციელების კონკრეტულ წესებს, OJ 2002 L 62 (ევროდაკის რეგულაციები); ევროპარლამენტისა და საბჭოს 2013 წლის 26 ივნისის რეგულაცია (EU) No. 603/2013, რომელიც შეეხება ევროდაკის შექმნას თითის ანაბეჭდების შესადარებლად, (EU) No. 604/2013 რეგულაციის ეფექტიანი გამოყენებისათვის, რითაც შესწორდა EU) No. 1077/2011 რეგულაცია. OJ 2013 L 180, გვ. 1, ევროდაკის შესწორებული რეგულაცია.

885 ევროპარლამენტისა და საბჭოს 2013 წლის 26 ივნისის რეგულაცია (EU) No. 604/2013, რომელიც ადგენს კრიტერიუმებსა და მექანიზმებს თავშესაფრის მაძიებლის განაცხადის განხილვაზე პასუხისმგებელი წევრი სახელმწიფოს განსაზღვრისთვის, როდესაც განაცხადი ევროკავშირის წევრ ქვეყანაში შეაქვს მესამე ქვეყნის მოქალაქეს ან მოქალაქეობის არმქონე პირს, OJ 2013 L 180 (დუბლინის III რეგულაცია).

886 ევროდაკის შესწორებული რეგულაცია, OJ 2013 L 180, გვ. 1, მუხლი 1 (1).

887 *იქვე*, მუხლი 1 (2).

ნებით არეგულირებს მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის, დუბლინის III რეგულაციის ხელშეწყობისთვის გამოყენება კი წესრიგდება მონაცემთა დაცვის ზოგადი რეგულაციით. აკრძალულია წევრი სახელმწიფოს ან ევროპოლის მიერ ევროდაკის შესწორებული რეგულაციის საფუძველზე მოპოვებული პერსონალური მონაცემების შემდგომი გადაცემა მესამე ქვეყნისთვის, საერთაშორისო ორგანიზაციისა ან კერძო დაწესებულებისთვის, რომელიც შექმნილია ევროკავშირის გარეთ.[888]

ევროდაკის ცენტრალურ განყოფილებას მართავს eu-LISA, თითის ანაბეჭდების შენახვისა და შედარების მიზნით; იგი ასევე აერთიანებს ევროკავშირის წევრ სახელმწიფოებს შორის ელექტრონული მონაცემების გადაცემის სისტემას და მონაცემთა ცენტრალურ ბაზას. წევრი სახელმწიფოები იღებენ და გადასცემენ მესამე ქვეყნის მოქალაქეებისა და მოქალაქეობის არმქონე პირთა ანაბეჭდებს, რომელთა ასაკი, სულ მცირე, 14 წელია და რომლებიც წევრი სახელმწიფოს ტერიტორიაზე ითხოვენ თავშესაფარს, ან დაკავებულნი არიან შიდა საზღვრის უკანონო გადაკვეთის გამო. წევრ სახელმწიფოებს უფლება აქვთ, მიიღონ და გადასცენ ტრეიტორიაზე უნებართვოდ მყოფ მესამე ქვეყნის მოქალაქეთა და მოქალაქეობის არმქონე პირთა ანაბეჭდებიც.

ნებისმიერ წევრ სახელმწიფოს შეუძლია ევროდაკის გამოყენება და თითის ანაბეჭდების შედარების მოთხოვნა, თუმცა მათი გასწორების, შევსების ან წაშლის უფლება მხოლოდ იმ წევრ სახელმწიფოს აქვს, რომელმაც შეაგროვა და გადასცა მონაცემები.[889] eu-LISA დამუშავებას აღრიცხავს მონაცემთა დაცვაზე მონიტორინგისა და მათი უსაფრთხოების მიზნით.[890] შიდასახელმწიფოებრივი სახედამხედველო ორგანოები მონაცემთა სუბიექტებს დახმარებას და კონსულტაციას უწევენ თავიანთი უფლებების განხორციელების შესახებ.[891] თითის ანაბეჭდების შეგროვება და გადაცემა კონტროლდება ეროვნული სასამართლოების მხრიდან.[892] ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაცია[893] და EDPS-ის ზედამხედველობა ვრცელდება ცენტრალური სისტემის დამუშავებაზე, რომელსაც მართავს eu-LISA.[894] თუ პირს ზიანი მია-

888 *იქვე,* მუხლი 35.

889 *იქვე,* მუხლი 27.

890 *იქვე,* მუხლი 28.

891 *იქვე,* მუხლი 29.

892 *იქვე,* მუხლი 29.

893 ევროპული პარლამენტისა და საბჭოს 2000 წლის 18 დეკემბრის რეგულაცია (EC) No. 45/2001 ევროკავშირის ინსტიტუტებისა და ორგანოების მიერ პერსონალური მონაცემების დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ 2001 L 8.

894 ევროდაკის შესწორებული რეგულაცია, OJ 2013 L 180, გვ. 1, მუხლი 31.

დგება უკანონო დამუშავების ან იმ ქმედების შედეგად, რომელიც არ შეესაბამება ევროდაკის რეგულაციას, უფლება აქვს, მიიღოს კომპენსაცია ზიანზე პასუხისმგებელი წევრი სახელმწიფოსგან.[895] უნდა აღინიშნოს, რომ თავშესაფრის მაძიებლები ადამიანთა განსაკუთრებით მოწყვლადი ჯგუფები არიან, რომელთაც ხშირად დიდი და რისკიანი გზა აქვთ გავლილი. ამის გამო, ხშირად თავშესაფრის მინიჭებაზე განაცხადის განხილვისას, პრაქტიკაში მათი უფლებების განხორციელება და კომპენსაციის მიღება შესაძლოა რთული აღმოჩნდეს.

სამართალდამცველი მიზნებით ევროდაკის გამოსაყენებლად, წევრი სახელმწიფოები ვალდებულნი არიან, გამოყონ სპეციალური უწყებები, რომელთაც ექნებათ წვდომის მოთხოვნის უფლება; ასევე, ორგანოები, რომლებიც შეაფასებენ შედარებაზე მოთხოვნის კანონიერებას.[896] ევროდაკში დაცულ მონაცემებზე სახელმწიფო ორგანოებისა და ევროპოლის წვდომის მხრივ მკაცრი პირობებია დაწესებული. ორგანოს მონაცემებზე წვდომის დასაბუთებული ელექტრონული მოთხოვნის წარდგენა შეუძლია მხოლოდ მას შემდეგ, რაც მონაცემებს შეადარებს სხვა ხელმისაწვდომ საინფორმაციო სისტემებში დაცულ ინფორმაციას (მაგ.: შიდასახელმწიფოებრივ დონეზე არსებული თითის ანაბეჭდების ბაზები და VIS). უნდა არსებობდეს საზოგადოებრივი უსაფრთხოების დაცვის აღმატებული ინტერესი, რომლის საფუძველზეც მონაცემთა შედარება მიზნის პროპორციული იქნება. ის ასევე უნდა იყოს აუცილებელი, კონკრეტული ვითარების შესაბამისი და ეყრდნობოდეს გონივრულ საფუძველს, რომ შედარება მნიშვნელოვნად შეუწყობს ხელს სისხლისსამართლებრივი დანაშაულის პრევენციას, გამოვლენას ან გამოძიებას. შედარება განსაკუთრებით მნიშვნელოვანია, როცა ეჭვმიტანილი, ტერორისტული დანაშაულის ან სხვა მძიმე დანაშაულის ჩამდენი პირი ან დაზარალებული, სავარაუდოდ, ხვდება იმ კატეგორიაში, რომლებზეც ვრცელდება თითის ანაბეჭდების შეგროვება ევროდაკის სისტემის ფარგლებში. დასაშვებია მხოლოდ თითის ანაბეჭდების შედარება, რისთვისაც ევროპოლმა ნებართვა უნდა მოიპოვოს იმ წევრი სახელმწიფოებისგან, რომლებმაც ასეთი მონაცემები შეაგროვეს.

ევროდაკში შენახული პერსონალური მონაცემები, რომლებიც უკავშირდება თავშესაფრის მაძიებელთა განაცხადებს, ინახება თითის ანაბეჭდების აღების დღიდან 10 წლის ვადით, თუ მონაცემთა სუბიექტი წევრი სახელმწიფოს მოქალაქეობას არ მიიღებს. ამ შემთხვევაში, მონაცემები დაუყოვნებლივ უნდა წაიშალოს. ინფორმაცია უცხო ქვეყნის მოქალაქეებზე, რომლებიც გარე საზღვრის უნებართვოდ გადაკვეთისთვის არიან დაკავებულნი, 18 თვე ინახება და უნდა წაიშალოს, როგორც კი მონაცემთა სუბიექტი მიიღებს ბინადრობის

895 *იქვე,* მუხლი 37.

896 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*, No. 2, გვ. 108–129.

ნებართვას ან წევრი სახელმწიფოს მოქალაქეობას, ანდა დატოვებს ევროკავშირის ტერიტორიას. იმ პირთა მონაცემები, რომლებსაც მიენიჭათ თავშესაფარი, მომდევნო 3 წლის განმავლობაში ხელმისაწვდომი უნდა დარჩეს ტერორისტული და სხვა სახის სისხლისსამართლებრივი დანაშაულების პრევენციის, გამოვლენისა და გამოძიებისათვის.

ევროკავშირის წევრი სახელმწიფოების გარდა, ევროდაკი ვრცელდება ისლანდიაზე, ნორვეგიაზე, ლიხტენშტაინსა და შვეიცარიაზეც, საერთაშორისო შეთანხმებების თანახმად.

ევროდაკის ზედამხედველობის საკოორდინაციო ჯგუფი (SCG) შედგება EDPS-ის წარმომადგენლებისა და ეროვნული საზდამხედველო ორგანოებისაგან, და წელიწადში ორჯერ იკრიბება. ჯგუფის წევრები არიან ევროკავშირის 28 წევრი სახელმწიფოს, ასევე, ისლანდიის, ლიხტენშტაინის, ნორვეგიისა და შვეიცარიის წარმომადგენლები.[897]

სამომავლო პერსპექტივები

2016 წლის მაისში ევროკომისიამ გამოაქვეყნა წინადადება ევროდაკის რეგულაციის ახალი შესწორების შესახებ, კერძოდ, იმ რეფორმის ფარგლებში, რომლის მიზანიც იყო საერთო ევროპული თავშესაფრის სისტემის (CEAS) ფუნქციონირების გაუმჯობესება.[898] წარმოდგენილი შესწორება მნიშვნელოვანია, რადგან არსებითად განავრცობს ევროდაკის თავდაპირველი მონაცემთა ბაზის ფარგლებს. იგი შეიქმნა CEAS-ის განხორციელების მხარდასაჭერად. კერძოდ, ევროდაკში დაცული თითის ანაბეჭდები საშუალებას იძლევა, განისაზღვროს წევრი სახელმწიფო, რომელიც პასუხისმგებელია ევროკავშირში შეტანილი თავშესაფრის მოთხოვნის განხილვაზე. წარმოდგენილი ინიციატივა ითვალისწინებს მონაცემთა ბაზის მოქმედების ფარგლების განვრცობას, რითაც ხელს შეუწყობს არარეგულარულ მიგრანტთა დაბრუნებას.[899] შიდასახელმწიფოებრივი ორგანოები მონაცემთა ბაზას გამოიყენებენ მესამე ქვეყნის იმ მოქალაქეთა საიდენტიფიკაციოდ, რომლებიც არარეგულარულად შევიდნენ ან რჩებიან ევროკავშირის ტერიტორიაზე. ამ გზით ისინი მოიპოვებენ მტკიცებულებას, რომლითაც წევრ სახელმწიფოებს დაეხმარებიან ასეთი პირების დაბრუნებაში. ამასთან, რაკი არსებული სამართლებრივი რეჟიმი აწესებს მხოლოდ თითის ანაბეჭდების შეგროვება-შენახვის მოთხოვნას, წარმო-

897 იხ. ევროკავშირის მონაცემთა დაცვის ზედამხედველის ვებგვერდი ევროდაკზე.

898 ევროპული კომისია, წინადადება ევროპარლამენტისა და საბჭოს რეგულაციაზე ევროდაკის შექმნის შესახებ, თითის ანაბეჭდების შესადარებლად, რომლის მიზანია (EU) No. 604/2013 რეგულაციის ეფექტიანი გამოყენება. რეგულაცია ადგენს კრიტერიუმებსა და მექანიზმებს თავშესაფრის მაძიებლის განაცხადის განხილვაზე პასუხისმგებელი წევრი სახელმწიფოს განსაზღვრისთვის, როდესაც ევროკავშირის წევრ ქვეყანაში განაცხადი შეაქვს მესამე ქვეყნის მოქალაქეს ან მოქალაქეობის არმქონე პირს, COM(2016) 272, საბოლოო, 2016 წლის 4 მაისი.

899 იხ. წინადადების განმარტებითი ბარათი, გვ.3.

დგენილი წინადადება ითვალისწინებს ფიზიკურ პირთა სახის გამოსახულების შეგროვებასაც,[900] რაც ბიომეტრიული მონაცემების სხვა ტიპს განეკუთვნება. 2013 წლის რეგულაციის თანახმად, ბიომეტრიული მონაცემების აღება შეიძლება იმ მოზარდებისგან, რომელთა მინიმალური ასაკი 14 წელია. წარმოდგენილი წინადადებით კი ეს ასაკი 6 წლამდე შემცირდება.[901] რეგულაციის მოქმედების სფეროს გაფართოება ნიშნავს ჩარევას უფრო მეტი ადამიანის პირადი ცხოვრებისა და მონაცემთა დაცვის უფლებებში. ამის დასაბალანსებლად, აღნიშნული შეთავაზება და ევროპარლამენტის LIBE კომიტეტის მიერ წარმოდგენილი შესწორებები[902] ითვალისწინებს მონაცემთა დაცვის მოთხოვნათა განმტკიცებას. სახელმძღვანელოს შემუშავებისას, ევროპარლამენტი და საბჭო წარმოდგენილ წინადადებას განიხილავდა.

ევროსური

ევროკავშირის სასაზღვრო მეთვალყურეობის სისტემა (ევროსური)[903] შექმნილია შენგენის გარე საზღვრებზე კონტროლის გასაუმჯობესებლად. მისი მიზანია არარეგულარული იმიგრაციისა და საზღვართშორისი დანაშაულების გამოვლენა, პრევენცია და აღკვეთა, ასევე, ინფორმაციის გაცვლა და ოპერატიული თანამშრომლობის გაუმჯობესება ეროვნულ საკოორდინაციო ცენტრებსა და ფრონტექსს (Frontex) შორის. ფრონტექსი გახლავთ ევროკავშირის სააგენტო, რომლის ფუნქციაა ინტეგრირებული სასაზღვრო მართვის ახალი კონცეფციის შემუშავება და გამოყენება.[904] მისი ზოგადი ამოცანებია:

900 ევროკომისია, წინადადება ევროპარლამენტისა და საბჭოს რეგულაციაზე ევროდაკის შექმნის შესახებ, თითის ანაბეჭდების შესადარებლად, რომლის მიზანია (EU) No. 604/2013 რეგულაციის ეფექტიანი გამოყენება. რეგულაცია ადგენს კრიტერიუმებსა და მექანიზმებს თავშესაფრის მაძიებლის განაცხადის განხილვაზე პასუხისმგებელი წევრი სახელმწიფოს განსაზღვრისთვის, როდესაც განაცხადი ევროკავშირის წევრ ქვეყანაში შეაქვს მესამე ქვეყნის მოქლაქეს ან მოქალაქეობის არმქონე პირს, COM(2016) 272 საბოლოო, 2016 წლის 4 მაისი, მუხლი 2 (1).

901 *იქვე*, მუხლი 2 (2).

902 ევროპარლამენტი, ანგარიში, წინადადება ევროპარლამენტისა და საბჭოს რეგულაციაზე ევროდაკის შექმნის შესახებ, თითის ანაბეჭდების შესადარებლად, რომლის მიზანია (EU) No. 604/2013 რეგულაციის ეფექტიანი გამოყენება. რეგულაცია ადგენს კრიტერიუმებსა და მექანიზმებს თავშესაფრის მაძიებლის განაცხადის განხილვაზე პასუხისმგებელი წევრი სახელმწიფოს განსაზღვრისთვის, როდესაც ევროკავშირის წევრ ქვეყანაში განაცხადი შეაქვს მესამე ქვეყნის მოქალაქეს ან მოქალაქეობის არმქონე პირს, PE 597.620v03-00, 2017 წლის 7 ივნისი.

903 ევროპარლამენტისა და საბჭოს 2013 წლის 22 ოქტომბრის რეგულაცია (EU) No. 1052/2013 ევროპული სასაზღვრო მეთვალყურეობის სისტემის შექმნაზე (ევროსური), OJ 2013 L 295.

904 ევროპარლამენტისა და საბჭოს 2016 წლის 14 სექტემბრის რეგულაცია (EU) No. 2916/1624 ევროპული სასაზღვრო და სანაპირო დაცვის შესახებ, რომლითაც ცვლილებები შედის ევროპარლამენტისა და საბჭოს რეგულაციაში (EU) 2016/399 და უქმდება: ევროპარლამენტისა და საბჭოს რეგულაცია (EC) No. 863.2007, საბჭოს რეგულაცია (EC) No. 2007/2004 და გადაწყვეტილება 2005/267/EC, OJ L 251.

- იმ არარეგულარულ მიგრანტთა შემცირება, რომლებიც ევროკავშირში შედიან შეუმჩნევლად;

- არარეგულარულ მიგრანტთა გარდაცვალების შემთხვევების შემცირება, ზღვაში მათი სიცოცხლის გადარჩენით;

- ევროკავშირის შიდა უსაფრთხოების განმტკიცება, საზღვართშორისი დანაშაულის პრევენციისათვის.[905]

გარე საზღვრების მქონე ყველა სახელმწიფოში ევროსური 2013 წლის 2 დეკემბერს ამუშავდა, ხოლო დანარჩენ ქვეყნებში - 2014 წლის 1 დეკემბერს. რეგულაცია ვრცელდება წევრ სახელმწიფოთა გარე სახმელეთო, საზღვაო და საჰაერო საზღვრების მეთვალყურეობაზე. ევროსური პერსონალურ მონაცემებს შეზღუდული მასშტაბით ცვლის და ამუშავებს, რადგან წევრ სახელმწიფოებსა და ფრონტექსს მხოლოდ საიდენტიფიკაციო ნომრების გაცვლის უფლება აქვთ. ევროსური აწვდის ისეთ ოპერატიულ ინფორმაციას, როგორიცაა, საპატრულო პოლიციისა და მომხდარი შემთხვევების ადგილმდებარეობა. ამასთან, როგორც წესი, გაცვლილი ინფორმაცია არ უნდა შეიცავდეს პერსონალურ მონაცემებს.[906] გამონაკლის შემთხვევებში, ევროსურის ფარგლებში პერსონალურ მონაცემთა გაცვლისას, რეგულაცია ადგენს მოთხოვნას ევროკავშირის მონაცემთა დაცვის ზოგადი საკანონმდებლო ჩარჩოს სრულად გავრცელებაზე.[907]

ამრიგად, ევროსური უზრუნველყოფს მონაცემთა დაცვის უფლებას. კერძოდ, ევროსურის თანახმად, მონაცემთა გაცვლა უნდა აკმაყოფილებდეს იმ კრიტერიუმებსა და დაცვის გარანტიებს, რომლებიც გათვალისწინებულია მონაცემთა დაცვის დირექტივით პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისთვის და ზოგადი რეგულაციით.[908]

905 იხ. ასევე, ევროპული კომისია (2008), კომისიის მიმართვა ევროპული პარლამენტის საბჭოს, ევროპულ ეკონომიკურ და სოციალურ კომიტეტსა და რეგიონულ კომიტეტს: ევროპული სასაზღვრო მეთვალყურეობის სისტემის (ევროსური) შექმნის განხილვა, COM(2008) 68, საბოლოო, ბრიუსელი, 13 თებერვალი 2008 წელი; ევროპული კომისია (2011), ევროპული პარლამენტისა და საბჭოს ევროპული სასაზღვრო მეთვალყურეობის სისტემის (ევროსური) შექმნაზე რეგულაციის პროექტის გავლენის შეფასება, შიდა სამუშაო დოკუმენტი, SEC(2011) 1536, საბოლოო, ბრიუსელი, 12 დეკემბერი 2011 წელი, გვ. 18.

906 ევროპული კომისია, ევროსური: შენგენის გარე საზღვრების დაცვა - მიგრანტთა სიცოცხლის დაცვა, მოკლედ ევროსურის შესახებ, 2013 წლის 29 ნოემბერი.

907 რეგულაცია 1052/2013, პრეამბულა, პუნქტი 13 და მუხლი 13.

908 *იქვე*, პრეამბულა, პუნქტი 13 და მუხლი 13.

საბაჟო საინფორმაციო სისტემა

ევროკავშირის დონეზე შექმნილია კიდევ ერთი მნიშვნელოვანი ინსტრუმენტი - საბაჟო საინფორმაციო სისტემა (CIS).[909] შიდა ბაზრის ჩამოყალიბების პროცესში, გაუქმდა ევროკავშირის ტერიტორიაზე საქონლის მოძრაობასთან დაკავშირებული ყველა სახის შემოწმება და ფორმალობა, რამაც თაღლითობის მომეტებული რისკი შექმნა. ამ რისკის დასაბალანსებლად, გააქტიურდა თანამშრომლობა წევრი სახელმწიფოების საბაჟო ადმინისტრაციებს შორის. CIS-ის მიზანია, წევრი სახელმწიფოების დახმარება ეროვნული და ევროკავშირის საბაჟო და სასოფლო-სამეურნეო კანონმდებლობათა სერიოზული დარღვევების პრევენციის, გამოძიებისა და სამართლებრივი დევნის პროცესში. CIS შეიქმნა ორი სამართლებრივი აქტის საფუძველზე: საბჭოს რეგულაცია (EC) No. 515/97 ეროვნულ დონეზე არსებული სხვადასხვა ადმინისტრაციული ორგანოს თანამშრომლობის შესახებ, რომლის მიზანია თაღლითობის აღკვეთა საბაჟო კავშირისა და საერთო სასოფლო-სამეურნეო პოლიტიკის კონტექსტში; და საბჭოს დირექტივა 2009/917/JHA, რომლის მიზანია დახმარება საბაჟო კანონმდებლობის მძიმე დარღვევათა პრევენციის, გამოძიებისა და სამართლებრივი დევნისას. ეს ნიშნავს, რომ CIS მოიცავს არა მხოლოდ სამართალდამცველ სფეროს.

CIS-ში დაცულია პერსონალური მონაცემები ფართო მოხმარების საგნებზე, სატრანსპორტო საშუალებებზე, ბიზნესზე, პირებზე, საქონელსა და ნაღდ ფულზე, რომლებსაც შეეხო დაკავება, ჩამორთმევა ან კონფისკაცია. მონაცემთა კატეგორიები, რომელთა დამუშავებაც შეიძლება, მკაფიოდ არის განსაზღვრული. ესენია: შესაბამისი პირის სახელი, ეროვნება, სქესი, დაბადების ადგილი და თარიღი, სისტემაში მონაცემების შეტანის მიზეზი და სატრანსპორტო საშუალების სარეგისტრაციო ნომერი.[910] ამ ინფორმაციის გამოყენება შესაძლებელია მხოლოდ დათვალიერების, ანგარიშგების ან კონკრეტული ინსპექტირებისათვის, ასევე, სტრატეგიული თუ ოპერაციული ანალიზის ჩასატარებლად იმ პირებზე, რომლებიც საბაჟო დებულებების დარღვევაში არიან ეჭვმიტანილნი.

CIS-ზე წვდომა აქვთ ეროვნულ საბაჟო, საგადასახადო, სასოფლო-სამეურნეო, საზოგადოებრივი ჯანდაცვისა და სამართალდამცველ ორგანოებს, ასევე, ევროპოლსა და ევროჯასტს.

---

909 ევროკავშირის საბჭოს 1995 წლის 26 ივლისის აქტი, რომელიც შეეხება ინფორმაციული ტექნოლოგიების შესახებ კონვენციის შექმნას საბაჟო მიზნებისთვის, OJ 1995 C 316, შესწორებულია ევროკავშირის საბჭოს მიერ (2009); 1997 წლის 13 მარტის რეგულაცია No. 515/97 წევრი ქვეყნების ადმინისტრაციული ორგანოების ურთიერთდახმარებასა და წევრ ქვეყნებსა და კომისიას შორის თანამშრომლობაზე, რომლის მიზანია კანონმდებლობის სწორი მოქმედება საბაჟო და აგრარულ სფეროში; საბჭოს 2009 წლის 30 ნოემბრის გადაწყვეტილება 2009/917/JHA საბაჟო მიზნებისთვის ინფორმაციული სისტემების გამოყენებაზე, OJ 2009 L 323 (CIS გადაწყვეტილება).

910 იხ. CIS გადაწყვეტილება, მუხლები 24, 25 და 28.

პერსონალური მონაცემების დამუშავება უნდა აკმაყოფილებდეს კონკრეტულ წესებს, რომლებიც დადგენილია შემდეგი სამართლებრივი აქტებით: No. 515/97 რეგულაცია და საბჭოს 2009/917/JHA გადაწყვეტილება, მონაცემთა დაცვის ზოგადი რეგულაცია, ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაცია, მოდერნიზებული 108-ე კონვენცია და საპოლიციო რეკომენდაცია. EDPS ზედამხედველობას უწევს CIS-ის შესაბამისობას (EC) No. 45/2001 რეგულაციასთან, ასევე, მართავს წელიწადში, სულ მცირე, 1 შეხვედრას მონაცემთა დაცვის ეროვნული ორგანოების წარმომადგენლებთან, რომელთა უფლებამოსილებაშიც შედის CIS-ის ზედამხედველობა.

ევროკავშირის საინფორმაციო სისტემების ფუნქციური თავსებადობა

მიგრაციის მართვა, ევროკავშირის გარე საზღვრების ინტეგრირებული მართვა და ტერორიზმისა თუ საზღვართშორისი დანაშაულის წინააღმდეგ ბრძოლა მნიშვნელოვან გამოწვევებს ქმნის და გლობალიზებულ სამყაროში სულ უფრო კომპლექსური ხდება. ბოლო რამდენიმე წელია, ევროკავშირი მუშაობს ახალ სრულფასოვან მიდგომაზე უსაფრთხოების დაცვასა და შენარჩუნებასთან დაკავშირებით, ევროკავშირის ფასეულობებისა და ფუნდამენტური თავისუფლებების რისკქვეშ დაყენების გარეშე. ამ ძალისხმევის ფარგლებში, ინფორმაციის ეფექტიანი გაცვლა, ერთი მხრივ, ეროვნულ სამართალდამცველ ორგანოებსა და, მეორე მხრივ, წევრ სახელმწიფოებსა და ევროკავშირის შესაბამის სააგენტოებს შორის, უაღრესად მნიშვნელოვანია.[911] ევროკავშირის საზღვრის მართვისა და შიდა უსაფრთხოების საინფორმაციო სისტემებს განსაზღვრული აქვთ შესაბამისი ამოცანები, ინსტიტუციური მოწყობა, მონაცემთა სუბიექტები და მომხმარებლები. ევროკავშირი მუშაობს იმ ხარვეზების დაძლევაზე, რომლებიც ახასიათებს (მაგ.: SIS II, VIS და ევროდაკი) ევროკავშირის მონაცემთა ფრაგმენტირებულ მართვას სხვადასხვა საინფორმაციო სისტემას შორის, და იკვლევს ფუნქციური თავსებადობის შესაძლებლო-

911 ევროკომისიის მიმართვა ევროპარლამენტსა და საბჭოს: უფრო მყარი და ჭკვიანი საინფორმაციო სისტემები სასაზღვრო უსაფრთხოებისათვის, COM(2016) 205, საბოლოო, ბრიუსელი, 2016 წლის 6 აპრილი; ევროკომისიის მიმართვა ევროპარლამენტს, ევროპულ საბჭოსა და საბჭოს: მობილურობის სამყაროში უსაფრთხოების გაუმჯობესება: ინფორმაციის გაუმჯობესებული გაზიარება ტერორიზმის წინააღმდეგ ბრძოლაში და მყარი გარე საზღვრები, COM(2016) 602, საბოლოო, ბრიუსელი, 2016 წლის 14 სექტემბერი; ევროკომისიის წინადადება ევროპარლამენტისა და საბჭოს რეგულაციაზე, რომელიც შეეხება შენგენის საინფორმაციო სისტემის გამოყენებას არარეგალურად მცხოვრები მესამე ქვეყნის მოქალაქეების დაბრუნებისათვის; ასევე, იხ. კომისიის მიმართვა ევროპარლამენტს, ევროპულ საბჭოსა და საბჭოს: ეფექტიანი და ჭეშმარიტი უსაფრთხოების კავშირის შესაქმნელად შესრულებული სამუშაოების მე-7 ანგარიში, COM(2017) 261, საბოლოო, ბრიუსელი, 2017 წლის 16 მაისი.

ბებს.[912] მისი მთავარი მიზანია, უფლებამოსილ სამართალდამცველ, საბაჟო და სასამართლო ორგანოებს სისტემატურად ჰქონდეთ მათი მოვალეობების შესასრულებლად საჭირო ინფორმაცია; ამავდროულად, შენარჩუნდეს ბალანსი პირადი ცხოვრების პატივისცემას, მონაცემთა დაცვასა და სხვა ფუნდამენტურ უფლებებთან.

ფუნქციური თავსებადობა გულისხმობს „საინფორმაციო სისტემების შესაძლებლობას, გაცვალოს და გააზიაროს მონაცემები.“[913] მონაცემთა გაცვლა არ უნდა არღვევდეს წვდომისა და გამოყენების მკაცრ პირობებს, რომლებსაც ადგენს მონაცემთა დაცვის ზოგადი რეგულაცია, მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის, ევროკავშირის ფუნდამენტურ უფლებათა ქარტია და სხვა შესაბამისი წესები. მონაცემთა მართვის ინტეგრირებული გადაწყვეტა არ უნდა ახდენდეს გავლენას ისეთ პრინციპებზე, როგორიცაა მიზნის შეზღუდვა, ასევე, მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (by design) და მონაცემთა დაცვა პირველად პარამეტრად (by default).[914]

ამ სამი საინფორმაციო სისტემისა (SIS II, VIS და ევროდაკი) და ფუნქციური გაუმჯობესების გარდა, კომისიამ წარმოადგინა წინადადება საზღვრის მართვის მეოთხე ცენტრალიზებული სისტემის შექმნაზე, რომელიც მესამე ქვეყნის მოქალაქეებთან დაკავშირებულ საკითხებზე იმუშავებს. ეს „შესვლისა და გასვლის სისტემა“ (Entry-Exit System), იგივე EES,[915] როგორც მოსალოდ-

912 ევროკავშირის საბჭო (2005), ჰააგის პროგრამა: ევროკავშირში თავისუფლების, უსაფრთხოებისა და მართლმსაჯულების განმტკიცება, OJ 2005 C 53, ევროკომისია (2010), კომისიის მიმართვა ევროპარლამენტსა და საბჭოს: თავისუფლების, უსაფრთხოებისა და მართლმსაჯულების სფეროში ინფორმაციის მართვის მიმოხილვა, COM(2010) 385, საბოლოო; ევროკომისია (2016), კომისიის მიმართვა ვროპულ პარლამენტსა და საბჭოს: უფრო მყარი და ჭკვიანი საინფორმაციო სისტემები სასაზღვრო უსაფრთხოებისათვის, COM(2016) 205, საბოლოო, ბრიუსელი, 2016 წლის 6 აპრილი; ევროკომისია (2016), კომისიის 2016 წლის 17 ივნისის გადაწყვეტილება, რომელიც შეეხება საინფორმაციო სისტემებისა და ფუნქციური თავსებადობის შესახებ ექსპერტთა მაღალი დონის ჯგუფის შექმნას, OJ 2016 C 257.

913 ევროკომისია (2016), კომისიის მიმართვა ვროპულ პარლამენტსა და საბჭოს: უფრო მყარი და ჭკვიანი საინფორმაციო სისტემები სასაზღვრო უსაფრთხოებისათვის, COM(2016) 205, საბოლოო, ბრიუსელი, 2016 წლის 6 აპრილი, გვ.14.

914 *იქვე,* გვ. 4–5.

915 ევროკომისია (2016), ევროპული პარლამენტისა და საბჭოს რეგულაცია შესვლა/გასვლის სისტემის (EES) შექმნის შესახებ, მესამე ქვეყნის იმ მოქალაქეთა შესვლის/გასვლის მონაცემებისა და შესვლაზე უარის დასარეგისტრირებლად, რომლებიც ევროკავშირის წევრი სახელმწიფოს გარე საზღვრებს კვეთენ; რეგულაცია EES-ზე წვდომის პირობების განსაზღვრის შესახებ, სამართალდამცველი მიზნებისთვის, რითაც შესწორდა რეგულაციები (EC) No. 767/2008 და (EU) No. 1077/2011, COM(2016) 194, საბოლოო, ბრიუსელი, 2016 წლის 6 აპრილი.

ნელია, 2020 წლისთვის განხორციელდება.[916] კომისიამ გამოაქვეყნა ევროპული სამგზავრო ინფორმაციისა და ავტორიზაციის სისტემის (ETIAS) შექმნის წინადადებაც.[917] ETIAS შეაგროვებს ინფორმაციას პირებზე, რომლებიც ვიზის გარეშე მოგზაურობენ ევროკავშირში, რითაც გააუმჯობესებს არარეგულარული მიგრაციისა და უსაფრთხოების შემოწმების შესაძლებლობას.

916 ევროპული კომისია (2016), კომისიის მიმართვა ევროპულ პარლამენტსა და საბჭოს: უფრო მყარი და ჭკვიანი საინფორმაციო სისტემები სასაზღვრო უსაფრთხოებისათვის, COM(2016) 205, საბოლოო, ბრიუსელი, 2016 წლის 6 აპრილი, გვ. 5.

917 ევროპული კომისია (2016), წინადადება ევროპული პარლამენტისა და საბჭოს რეგულაციის შესახებ, რომელიც შეეხება ევროპული სამოგზაურო ინფორმაციისა და ავტორიზაციის სისტემის (ETIAS) შექმნას და რომლითაც შესწორდა რეგულაციები: (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/794 და (EU) 2016/1624, COM(2016) 731, საბოლოო, 2016 წლის 16 ნოემბერი.

9 მონაცემთა სხვადასხვა კატეგორია და მათი დაცვის წესები

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის ზოგადი რეგულაცია; დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ.	**ელექტრონული კომუნიკაციები**	მოდერნიზებული 108-ე კონვენცია; რეკომენდაცია სატელეკომუნიკაციო სერვისების შესახებ.
მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 89	**შრომითი ურთიერთობები**	მოდერნიზებული 108-ე კონვენცია; რეკომენდაცია დასაქმების შესახებ; ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 2007.
მონაცემთა დაცვის ზოგადი დირექტივა, მუხლი 9 (2)(თ)(ი)	**სამედიცინო მონაცემები**	მოდერნიზებული 108-ე კონვენცია; რეკომენდაცია სამედიცინო მონაცემების შესახებ; ECtHR, *Z v. Finland*, No. 22009/93, 1997.
კლინიკური ცდების რეგულაცია	**კლინიკური ცდები**	
მონაცემთა დაცვის ზოგადი რეგულაცია მუხლი 6 (4), მუხლი 89		მოდერნიზებული 108-ე კონვენცია; რეკომენდაცია სტატისტიკური მონაცემების შესახებ.

ევროკავშირი	განხილული საკითხები	ევროპის საბჭო
რეგულაცია (EC) No. 223/2009 ევროპული სტატისტიკის შესახებ; CJEU, C-524/06, *Huber v. Bundesrepublik Deutschland* [GC], 2008.	**ოფიციალური სტატისტიკა**	მოდერნიზებული 108-ე კონვენცია; რეკომენდაცია სტატისტიკური მონაცემების შესახებ.
დირექტივა 2014/65/EU ფინანსურ ინსტრუმენტებში არსებული ბაზრების შესახებ; რეგულაცია (EU) No. 648/2012 OTC დერივატივების, ცენტრალური მხარეებისა და სავაჭრო საცავების შესახებ; რეგულაცია (EC) No. 1060/2009 საკრედიტო სარეიტინგო სააგენტოების შესახებ; დირექტივა 2007/64/EC შიდა ბაზარზე არსებული გადახდის სერვისების შესახებ.	**ფინანსური მონაცემები**	მოდერნიზებული 108-ე კონვენცია; რეკომენდაცია 90 (19) გადახდებისა და სხვა დაკავშირებული ოპერაციების შესახებ; ECtHR, *Michaud v. France*, No. 12323/11, 2012.

ზოგ სფეროში, ევროპის მასშტაბით შემუშავდა სპეციალური სამართლებრივი ინსტრუმენტები, რომლებიც დეტალურად განავრცობს მოდერნიზებულ 108-ე კონვენციასა და მონაცემთა დაცვის ზოგადი რეგულაციის წესებს კონკრეტულ შემთხვევებთან დაკავშირებით.

9.1 ელექტრონული კომუნიკაციები

ძირითადი საკითხები

- სატელეკომუნიკაციო სექტორში მონაცემთა დაცვის სპეციალური ინსტრუმენტები, ძირითადად, სატელეფონო მომსახურებასთან დაკავშირებით, წარმოდგენილია ევროპის საბჭოს 1995 წლის რეკომენდაციაში.
- პერსონალური მონაცემების დამუშავება, რომლებიც ეხება ევროკავშირის დონეზე საკომუნიკაციო მომსახურების მიწოდებას, რეგულირდება დირექტივით პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ (e-Privacy დირექტივა).
- ელექტრონული კომუნიკაციების კონფიდენციალობა ვრცელდება კომუნიკაციის არა მხოლოდ შინაარსზე, არამედ სხვა მეტამონაცემებზეც (ვის შორის ხდება კომუნიკაცია, როდის და რა ხანგრძლივობით; ადგილი, საიდანაც გადაიცემა მონაცემები).

საკომუნიკაციო ქსელებს აქვს მოსმენებისა და კომუნიკაციის შემოწმების/დაკვირვების დამატებითი შესაძლებლობები, რითაც იზრდება მომხმარებელთა პირად სივრცეში უკანონო ჩარევის რისკი. შესაბამისად, აუცილებელი გახდა მონაცემთა დაცვის სპეციალური რეგულაციების მიღება იმ კონკრეტული საფრთხეების დასაძლევად, რომლებიც საკომუნიკაციო ქსელების მომხმარებლებს ემუქრება.

1995 წელს ევროპის საბჭომ გამოაქვეყნა რეკომენდაცია სატელეკომუნიკაციო სფეროში მონაცემთა დაცვაზე, რომელიც, ძირითადად, სატელეფონო მომსახურებებს ეხებოდა.[918] რეკომენდაციის თანახმად, სატელეკომუნიკაციო სფეროში პერსონალურ მონაცემთა შეგროვებისა და დამუშავების მიზნები უნდა მოიცავდეს შემდეგ საკითხებს: მომხმარებლის დაკავშირება კონკრეტულ ქსელთან, კონკრეტული სატელეკომუნიკაციო მომსახურების მიწოდება, ანგარიშგება, შემოწმება (verify), ოპტიმალური ტექნიკური ოპერაციების ჩატარება, ქსელისა და მომსახურების განვითარება.

განსაკუთრებული ყურადღება დაეთმო საკომუნიკაციო ქსელების გამოყენებით პირდაპირი მარკეტინგის შეტყობინებათა გაგზავნას. ზოგადად, ისინი არ უნდა გაეგზავნოს მომხმარებელს, რომელმაც ცალსახად თქვა უარი სარეკლამო შეტყობინების მიღებაზე. ავტომატიზებული ზარის მოწყობილობები, რომლებიც გზავნის წინასწარ ჩაწერილ სარეკლამო ინფორმაციას, უნდა გამოიყენონ მხოლოდ მომხმარებლის მკაფიო თანხმობის შემთხვევაში, შიდასახელმწიფოებრივი კანონმდებლობით კი დეტალური წესები განისაზღვროს ამ სფეროში.

ევროკავშირის სამართლებრივ ჩარჩოში 1997 წელს განხორციელებული პირველი მცდელობის შემდეგ, 2002 წელს მიიღეს დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ (e-Privacy დირექტივა), რომელიც შესწორდა 2009 წელს. მიზანი გახლდათ მონაცემთა დაცვის მანამდე არსებული დირექტივის დებულებათა შევსება და სატელეკომუნიკაციო სექტორზე მორგება.[919]

---

918 ევროპის საბჭო, მინისტრთა კომიტეტი (1995), რეკომენდაცია REC (95)4 წევრი ქვეყნებისთვის სატელეკომუნიკაციო, კერძოდ, სატელეფონო მომსახურების სფეროში პერსონალურ მონაცემთა დაცვის შესახებ, 7 თებერვალი 1995 წელი.

919 ევროპული პარლამენტისა და საბჭოს 2002 წლის 12 ივლისის დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ, OJ 2002 L 201 (დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ), რომელიც შეიცვალა ევროპული პარლამენტისა და საბჭოს 2009 წლის 25 ნოემბრის დირექტივით 2009/136/EC. ეს უკანასკნელი ცვლის: დირექტივას 2002/22/EC, რომელიც ეხება უნივერსალური მომსახურებისა და ელექტრონული საკომუნიკაციო ქსელებისა თუ მომსახურების მომხმარებელთა უფლებებს; და რეგულაციას (EC) NO. 2006/2004 მომხმარებელთა დაცვის კანონმდებლობის მოქმედებაზე პასუხისმგებელი შიდასახელმწიფოებრივი ორგანოების თანამშრომლობის შესახებ, OJ 2009 L 337.

პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების დირექტივის მოქმედების სფერო შეზღუდულია და მოიცავს მხოლოდ საჯარო ქსელებით განხორციელებულ საკომუნიკაციო მომსახურებას.

ეს დირექტივა განასხვავებს 3 კატეგორიის მონაცემებს:

- მონაცემები კომუნიკაციისას გაგზავნილ შეტყობინებათა შინაარსზე (ეს მონაცემები მკაცრად კონფიდენციალურია);
- მონაცემები, რომლებიც აუცილებელია კომუნიკაციის დამყარებისა და წარმართვისათვის (ე.წ. მეტამონაცემები დირექტივაში მოხსენიებულია „ტრეფიკის მონაცემებად“ და მოიცავს ინფორმაციას მხარეებს შორის კომუნიკაციაზე, მის დროსა და ხანგრძლივობაზე);
- მეტამონაცემებს შორის ზოგიერთი უშუალოდ საკომუნიკაციო მოწყობილობის ადგილმდებარეობას ეხება (ე.წ. ადგილმდებარეობის განმსაზღვრელი მონაცემები). ამავდროულად, ეს არის ინფორმაცია საკომუნიკაციო მოწყობილობების მომხმარებელთა ადგილსამყოფელზეც, განსაკუთრებით, როცა საქმე ეხება მობილური კავშირგაბმულობის მოწყობილობის მომხმარებლებს.

ტრეფიკის მონაცემების გამოყენება სერვისის მიმწოდებელს შეუძლია მხოლოდ ანგარიშსწორებისა და მომსახურების მიზნებით. მონაცემთა სუბიექტის თანხმობით, ნებადართულია ამ მონაცემების გადაცემა სხვა დამმუშავებლისთვის, რომელიც დამატებით მომსახურებას სთავაზობს მომხმარებლებს (მაგ.: ინფორმაციის მიწოდება მომხმარებლის სიახლოვეს მდებარე მეტროსადგურის ან აფთიაქის შესახებ; ამინდის პროგნოზი მომხმარებლის ადგილსამყოფელის მიხედვით).

პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების დირექტივის მე-15 მუხლის თანახმად, ელექტრონულ ქსელებში დაცულ მონაცემებზე სხვა სახის წვდომა უნდა აკმაყოფილებდეს მონაცემთა დაცვის უფლებაში კანონიერი ჩარევის მოთხოვნებს, როგორც გათვალისწინებულია ECHR-ის მე-8 მუხლის მე-2 პუნქტით და დადასტურებულია ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 და 52-ე მუხლებით. ეს შეიძლება მოიცავდეს წვდომას დანაშაულებათა გამოძიების მიზნით.

პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების დირექტივაში 2009 წელს განხორციელებული ცვლილებების თანახმად:[920]

920 ევროპული პარლამენტისა და საბჭოს 2009 წლის 25 ნოემბრის დირექტივა 2009/136/EC. იგი ცვლის: დირექტივას 2002/22/EC, რომელიც შეეხება უნივერსალური მომსახურების, ასევე, ელექტრონული საკომუნიკაციო ქსელებისა თუ მომსახურების მომხმარებელთა უფლებებს; დირექტივას 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ; და რეგულაციას (EC) No. 2006/2004 მომხმარებელთა დაცვის კანონმდებლობის მოქმედებაზე პასუხისმგებელი შიდასახელმწიფოებრივი ორგანოების თანამშრომლობის შესახებ, OJ 2009 L 337.

- შეზღუდვები, რომლებიც დაწესებულია ელფოსტის გაგზავნაზე პირდაპირი მარკეტინგის მიზნებით, ასევე გავრცელდა მოკლე ტექსტურ შეტყობინებებზე, მულტიმედიურ შეტყობინებებსა და სხვა მსგავს სერვისებზე; მარკეტინგული ელფოსტის გაგზავნა ნებადართულია მხოლოდ არსებულ მომხმარებლებთან, თუ მათ ხელმისაწვდომი გახადეს თავიანთი ელფოსტის მისამართი და ასეთ მომსახურებას არ ეწინააღმდეგებიან.

- წევრ სახელმწიფოებს დაეკისრათ ვალდებულება, არასასურველი (unsolicited) კომუნიკაციის აკრძალვის დარღვევებთან დაკავშირებით უზრუნველყონ სამართლებრივი დაცვის საშუალება.[921]

- ე.წ. „Cookie ფაილების“ დანერგვა (კომპიუტერული პროგრამა, რომელიც მონიტორინგს უწევს და აფიქსირებს კომპიუტერის მომხმარებლის აქტივობას) აღარ არის ნებადართული მომხმარებლის თანხმობის გარეშე. შიდასახელმწიფოებრივი კანონმდებლობა დეტალურად უნდა არეგულირებდეს თანხმობის გამოხატვასა და მოპოვებას, რათა მონაცემთა სუბიექტი საკმარისად იყოს დაცული.[922]

როცა უსაფრთხოება ირღვევა არაავტორიზებული წვდომის, მონაცემთა დაკარგვის ან განადგურების შედეგად, აუცილებელია კომპეტენტური საზედამხედველო ორგანოს დაუყოვნებელი ინფორმირება. აბონენტებს ინფორმაცია უნდა მიეწოდოთ იმ შემთხვევაში, თუ შესაძლებელია, რომ ზიანი მიადგეთ ასეთი დარღვევის შედეგად.[923]

მონაცემთა შენახვის დირექტივის[924] თანახმად, საკომუნიკაციო მომსახურების მიმწოდებლები ვალდებულნი იყვნენ, შეენახათ მონაცემები. თუმცა, დირექტივა CJEU-მ ძალადაკარგულად გამოაცხადა (დეტალური ინფორმაციისათვის იხ. ნაწილი 8.3).

სამომავლო პერსპექტივები

2017 წლის იანვარში ევროკომისიამ დაამტკიცა e-Privacy რეგულაციის ახალი პროექტი, რომელიც ძველ დირექტივას ჩაანაცვლებს. მისი მიზანი იგი-

921 იხ. შესწორებული დირექტივა, მუხლი 13.

922 იხ. იქვე, მე-5 მუხლი; იხ. ასევე, 29-ე მუხლის სამუშაო ჯგუფი (2012), მოსაზრება 04/2012 „Cookie ფაილების“ თაობაზე თანხმობის გამონაკლისის შესახებ, CP 194, ბრიუსელი, 7 ივნისი 2012 წელი.

923 იხ. ასევე, 29-ე მუხლის სამუშაო ჯგუფი (2011), სამუშაო დოკუმენტი 01/2011 ევროკავშირის პერსონალურ მონაცემთა დამუშავების წესების დარღვევის მოწესრიგებასა და სამომავლო პოლიტიკის განვითარების რეკომენდაციებზე, WP 184, ბრიუსელი, 5 აპრილი 2011 წელი.

924 ევროპული პარლამენტისა და საბჭოს 2006 წლის 15 მარტის დირექტივა 2006/24/EC საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების მომსახურებისას ან საჯარო კომუნიკაციების ქსელებში წარმოშობილი თუ დამუშავებული მონაცემების შენახვის შესახებ, რომელიც ცვლის დირექტივას 2002/58/EC, OJ 2006 L 105.

ვე რჩება: „ფიზიკური და იურიდიული პირების ფუნდამენტური უფლებებისა და თავისუფლებების დაცვა ელექტრონული კომუნიკაციების მომსახურებათა მიწოდებისა და გამოყენებისას (კერძოდ, როგორიცაა პირადი ცხოვრების ხელშეუხებლობისა და კომუნიკაციის პატივისცემა) და ფიზიკურ პირთა დაცვა პერსონალური მონაცემების დამუშავებისას.“ ამავდროულად, დოკუმენტის ახალი პროექტი უზრუნველყოფს ელექტრონული კომუნიკაციების მონაცემებისა და სერვისების თავისუფალ მიმოცვლას ევროკავშირის ფარგლებში. [925] მონაცემთა დაცვის ზოგადი რეგულაცია ძირითადად შეეხება ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლით დაცულ უფლებებს, ხოლო წარმოდგენილი რეგულაციის მიზანია ქარტიის მე-8 მუხლის ჩართვა ევროკავშირის მეორად კანონმდებლობაში.

რეგულაციის საშუალებით, მანამდე არსებული დირექტივის დებულებები მოერგება ახალ ტექნოლოგიებსა და ბაზრის რეალობას და მონაცემთა დაცვის ზოგად რეგულაციასთან ერთად შექმნის კომპლექსურ და თანმიმდევრულ საკანონმდებლო ჩარჩოს. შესაბამისად, e-Privacy დირექტივა იქნება მონაცემთა დაცვის ზოგადი რეგულაციის *lex specialis* და მას მოარგებს ელექტრონული კომუნიკაციის იმ მონაცემებზე, რომლებიც „პერსონალურად“ მიიჩნევა. ახალი რეგულაცია მოიცავს „ელექტრონული კომუნიკაციების მონაცემთა“ დამუშავებას, მათი შინაარსისა და მეტამონაცემების ჩათვლით, რომლებიც შეიძლება არ განეკუთვნებოდეს პერსონალურ მონაცემებს. რეგულაცია მხოლოდ ევროკავშირის მასშტაბით ვრცელდება, მათ შორის, ე.წ. over-the-top (OTP) მომსახურების მიმწოდებლებზე, ასევე, იმ შემთხვევებზეც, როდესაც ევროკავშირში მოპოვებული მონაცემები გაერთიანების გარეთ მუშავდება. OTP მომსახურების მიმწოდებლები მომხმარებლებს ინტერნეტის საშუალებით აწვდიან შინაარსს, მომსახურებას ან აპლიკაციებს, ქსელის ოპერატორის ან ინტერნეტმომსახურების მიმწოდებლის (ISP) პირდაპირი მონაწილეობის გარეშე. ასეთი მაგალითებია: Skype (ხმოვანი და ვიდეოზარები), WhatsApp (მოკლე ტექსტური შეტყობინებები), Google (ძიება), Spotify (მუსიკა) ან Netflix (ვიდეოკონტენტი). მონაცემთა დაცვის ზოგადი რეგულაციის აღსრულების მექანიზმები გავრცელდება ახალ რეგულაციაზე.

e-Privacy რეგულაციის მიღება დაგეგმილი იყო 2018 წლის 25 მაისამდე. ამ დროისათვის, მონაცემთა დაცვის ზოგადი რეგულაცია ევროკავშირის ყველა წევრ სახელმწიფოზე გავრცელდა. თუმცა, ეს დამოკიდებულია შეთანხმების მიღწევაზე ევროპარლამენტსა და საბჭოს შორის. [926]

925 წინადადება ევროპული პარლამენტისა და საბჭოს რეგულაციაზე, რომელიც შეეხება პერსონალური მონაცემების დამუშავებას და პირადი ცხოვრების ხელშეუხებლობის დაცვას ელექტრონული კომუნიკაციების სექტორში და რომლითაც უქმდება დირექტივა 2002/58/EC, COM(2017) 10, საბოლოო, მუხლი 1.

926 დამატებითი ინფორმაციისათვის, იხ. ევროპული კომისია (2017), კომისიამ მაღალი დონის წესები წარმოადგინა პირადი ცხოვრების დასაცავად ელექტრონული კომუნიკაციების სფეროში და ევროკავშირის ინსტიტუტებისათვის მონაცემთა დაცვის წესების გასაახლებლად, პრესრელიზი, 2017 წლის 10 იანვარი.

9.2 მონაცემები დასაქმების შესახებ

ძირითადი საკითხები

- შრომითი ურთიერთობების მხრივ მონაცემთა დაცვის სპეციალური წესები წარმოდგენილია ევროპის საბჭოს რეკომენდაციაში დასაქმების მონაცემთა შესახებ.
- მონაცემთა დაცვის ზოგად რეგულაცია შრომით ურთიერთობებს მოიხსენიებს მხოლოდ განსაკუთრებული კატეგორიის მონაცემთა დამუშავების კონტექსტში.
- ნებაყოფლობითი თანხმობის ვალიდურობა, როგორც დასაქმებულის მონაცემთა დამუშავების სამართლებრივი საფუძველი, შესაძლოა საეჭვო/პრობლემატური იყოს იმ ეკონომიკური დისბალანსის გათვალისწინებით, რომელიც არსებობს დასაქმებულსა და დამსაქმებელს შორის. თანხმობის გარემოებები ყურადღებით უნდა შეფასდეს.

მონაცემთა დამუშავება შრომით ურთიერთობებში რეგულირდება ევროკავშირის ზოგადი კანონმდებლობით პერსონალური მონაცემების დაცვის შესახებ. ამავდროულად, არსებობს რეგულაცია[927], რომელიც აწესრიგებს ევროპული ინსტიტუტების მიერ პერსონალური მონაცემების დამუშავებას კონკრეტულად დასაქმების კონტექსტში. მონაცემთა დაცვის ზოგად რეგულაციაში შრომითი ურთიერთობები მოხსენიებულია მე-9 მუხლის მე-2 პუნქტში, რომლის თანახმადაც, პერსონალური მონაცემების დამუშავება ნებადართულია მონაცემთა დამმუშავებლის ან მონაცემთა სუბიექტის მოვალეობათა შესრულებისას ან კონკრეტული უფლებებით სარგებლობისას დასაქმების სფეროში.

მონაცემთა დაცვის ზოგადი რეგულაციით, დასაქმებულს უნდა მიეცეს შესაძლებლობა, მკაფიოდ განასხვაოს მონაცემები, რომელთა დამუშავებაზეც/შენახვაზეც ნებაყოფლობით თანხმობას აცხადებს, და შენახვის მიზნები. თანხმობის გაცემამდე დასაქმებულებს უნდა განემარტოთ თავიანთი უფლებები და მონაცემთა შენახვის ვადაც. თუ პერსონალურ მონაცემთა უსაფრთხოების დარღვევა მომეტებულ რისკს შეუქმნის ფიზიკური პირის უფლებებსა და თავისუფლებებს, დამსაქმებელი ვალდებულია, ეს აცნობოს დასაქმებულებს. რეგულაციის 88-ე მუხლის თანახმად, წევრ სახელმწიფოებს უფლება აქვთ, დაადგინონ კონკრეტული წესები, რათა პერსონალურ მონაცემებთან მიმართებით დაცული იყოს პირის უფლებები და თავისუფლებები დასაქმების კონტექსტში.

927 ევროპული პარლამენტისა და საბჭოს 2000 წლის 18 დეკემბრის რეგულაცია (EC) No. 45/2001 ვროკავშირის ინსტიტუტებისა და ორგანოების მიერ პერსონალური მონაცემების დამუშავებისას ფიზიკურ პირთა დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, OJ 2001 L 8.

მაგალითი: *Worten-ის*[928] საქმე შეეხებოდა ყოველდღიურად ნამუშევარი დროისა და შესვენების პერიოდების აღრიცხვას, რაც პერსონალურ მონაცემებს განეკუთვნება. ეროვნული კანონმდებლობა დამსაქმებელს ავალდებულებდა, აღნიშნული ინფორმაცია ხელმისაწვდომი ყოფილიყო იმ სახელმწიფო ორგანოებისთვის, რომლებიც სამუშაო პირობების მონიტორინგზე არიან პასუხისმგებელნი. შედეგად, ამ უწყებებს ექნებოდათ პირდაპირი წვდომა შესაბამის პერსონალურ მონაცემებზე. თუმცა, მეორე მხრივ, მონაცემებზე წვდომა აუცილებელი იყო სახელმწიფოს მხრიდანაც, რათა მას მონიტორინგი განეხორციელებინა სამუშაო პირობების კანონიერებაზე.[929]

ევროპის საბჭომ 1989 წელს გამოაქვეყნა რეკომენდაცია დასაქმების მონაცემების შესახებ, რომელიც 2015 წელს შესწორდა.[930] რეკომენდაცია შეეხება პერსონალური მონაცემების დამუშავებას დასაქმების მიზნებისთვის, როგორც კერძო, ისე საჯარო სექტორში. დამუშავება უნდა აკმაყოფილებდეს გარკვეულ პრინციპებსა და შეზღუდვებს, როგორიცაა, მაგალითად, გამჭვირვალობა და კონსულტაციის გავლა დასაქმებულის წარმომადგენელთან მანამ, სანამ სამუშაო ადგილას მონიტორინგის სისტემები განთავსდება. რეკომენდაციის თანახმად, დასაქმებულის მიერ ინტერნეტის მოხმარებაზე მონიტორინგის ნაცვლად, დამსაქმებლებმა უნდა მიიღონ პრევენციული ღონისძიებები (მაგ.: გამოიყენონ ფილტრები).

კვლევა დასაქმების კონტექსტში მონაცემთა დაცვის ყველაზე გავრცელებული პრობლემების შესახებ ხელმისაწვდომია 29-ე მუხლის სამუშაო ჯგუფის სამუშაო დოკუმენტში.[931] ჯგუფმა გააანალიზა თანხმობის, როგორც დასაქმებულზე მონაცემების დამუშავების სამართლებრივი საფუძვლის მნიშვნელობა[932] და დაადგინა, რომ დასაქმებულსა და დამსაქმებელს შორის არსებული ეკონომიკური დისბალანსი ხშირად ეჭვს წარმოშობს დასაქმებულის მიერ გამოხატული თანხმობის ნებაყოფლობითობაზე. შესაბამისად, დასაქმების კონტექსტში თანხმობის ვალიდურობის შეფასებისას, გულდასმით უნდა განიხილონ გარემოებები, რომლებსაც ის ეფუძნება.

928 CJEU, *C-342/12*, *Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)*, 30 May 2013, პუნქტი 19.

929 *იქვე*, პუნქტი 43.

930 ევროპის საბჭო, მინისტრთა კომიტეტის (2015) რეკომენდაცია Rec(2015)5 წევრი სახელმწიფოებისთვის, დასაქმების კონტექსტში პერსონალური მონაცემების დამუშავების შესახებ, 2015 წლის აპრილი.

931 29-ე მუხლის სამუშაო ჯგუფი (2017), მოსაზრება 2/2017 სამსახურში მონაცემთა დამუშავების შესახებ, WP 249, ბრიუსელი, 2017 წლის 8 ივნისი.

932 29-ე მუხლის სამუშაო ჯგუფი (2005), სამუშაო დოკუმენტი 95/46/EC დირექტივის 26-ე მუხლის პირველი პუნქტის საერთო განმარტებასთან დაკავშირებით, WP 114, ბრიუსელი, 2005 წლის 25 ნოემბერი.

დღევანდელ ტიპურ სამუშაო გარემოში მონაცემთა დაცვის ფართოდ გავრცელებული პრობლემაა დასაქმებულთა ელექტრონული კომუნიკაციების კანონიერი მონიტორინგის ფარგლები. პრობლემის გადაჭრის შედარებით მარტივ გზად მიიჩნევა სამუშაო ადგილზე საკომუნიკაციო მოწყობილობათა პირადი მიზნებით გამოყენების აკრძალვა. ამავდროულად, ასეთი ზოგადი აკრძალვა შესაძლოა არაპროპორციული და არარეალისტური იყოს. ამ კონტექსტში, განსაკუთრებით საინტერესოა ECtHR-ის გადაწყვეტილებები საქმეებზე: *Copland v. the United Kingdom* და *Bărbulescu v. Romania*.

მაგალითები: საქმე *Copland v. the United Kingdom*[933] შეეხებოდა კოლეჯის თანამშრომლის მიერ ელფოსტისა და ინტერნეტის მოხმარების ფარულ მონიტორინგს. დამსაქმებელს სურდა, დაედგინა, გადაჭარბებულად ხომ არ იყენებდა დასაქმებული კოლეჯის კუთვნილ მოწყობილობებს პირადი მიზნებისთვის. ECtHR-მა დაადგინა, რომ საწარმოს ტერიტორიიდან განხორციელებულ სატელეფონო ზარებზე ვრცელდება პირადი ცხოვრებისა და კორესპონდენციის პატივისცემა. შესაბამისად, ევროპული კონვენციის მე-8 მუხლი იცავს სამსახურიდან განხორციელებულ ზარებს და ელფოსტით გაგზავნილ წერილებს, ასევე, ინტერნეტის მოხმარებაზე მონიტორინგით მოპოვებულ ინფორმაციას. განმცხადებლის შემთხვევაში, არ არსებობდა დებულებები, რომლებიც დაარეგულირებდა, რა პირობებში შეუძლია დამსაქმებელს, მონიტორინგი გაუწიოს დასაქმებულის მიერ ტელეფონის, ელფოსტისა და ინტერნეტის გამოყენებას. შესაბამისად, ჩარევა არ იყო კანონიერი. სასამართლომ საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

საქმეში *Bărbulescu v. Romania*[934] განმცხადებელი სამსახურიდან დაითხოვეს სამუშაო ადგილას და სამუშაო საათებში ინტერნეტის მოხმარების გამო, რაც არღვევდა შიდა რეგულაციებს. დამსაქმებელი მონიტორინგს უწევდა მის კომუნიკაციებს. ჩანაწერები, რომლებიც მხოლოდ პირად გზავნილებს შეიცავდა, დასაქმებულმა ეროვნულ დონეზე გამართულ სასამართლო პროცესზე წარმოადგინა. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ ეს შემთხვევა ექცეოდა კონვენციის მე-8 მუხლის ფარგლებში, თუმცა ღიად დატოვა საკითხი, თუ რამდენად შეიძლებოდა, განმცხადებელს ჰქონოდა პირადი ცხოვრების ხელშეუხებლობის გონივრული მოლოდინი დამსაქმებლის შემზღუდავი რეგულაციების გათვალისწინებით. ამავდროულად, სასამართლომ დაადგინა, რომ დამსაქმებლის ინსტრუქციები სამუშაო ადგილას პირად სოციალურ ცხოვრებას მთლიანად ვერ აღკვეთდა.

933 ECtHR, *Copland v. the United Kingdom,* No. 62617/00, 2007 წლის 3 აპრილი.

934 ECtHR, *Bărbulescu v. Romania* [GC], No. 61496/08, 2017 წლის 5 სექტემბერი, პუნქტი 121.

რაც შეეხება საჩივრის არსებით მხარეს, სასამართლომ დაადგინა: ხელშემკვრელმა სახელმწიფოებმა თავისუფალი შეფასების ფარგლებში უნდა განსაზღვრონ, რამდენად საჭიროა სამართლებრივი ჩარჩოს შექმნა იმ პირობების დარეგულირებისათვის, რომლებშიც დამსაქმებელი გააკონტროლებს დასაქმებულთა არაპროფესიულ ელექტრონულ და სხვა სახის კომუნიკაციებს სამუშაო ადგილას. ამავდროულად, შიდასახელმწიფოებრივმა ორგანოებმა უნდა უზრუნველყონ, რომ ღონისძიებებს, რომლებსაც დამსაქმებელი გაატარებს კორესპონდენციასა და სხვა ტიპის კომუნიკაციაზე მონიტორინგის მიზნით, მათი მასშტაბისა და ხანგრძლივობის მიუხედავად, თან ახლდეს სათანადო და საკმარისი უსაფრთხოების ზომები ძალაუფლების ბოროტად გამოყენებისგან დასაცავად. პროპორციულობა და პროცედურული გარანტიების არსებობა თვითნებობის წინააღმდეგ აუცილებელია. ევროპულმა სასამართლომ კონკრეტულ ვითარებაში გამოავლინა რამდენიმე რელევანტური ფაქტორი, მათ შორის: დამსაქმებლის მხრიდან მონიტორინგის მასშტაბი და დასაქმებულის პირად ცხოვრებაში ჩარევის ხარისხი; რა შედეგები მოაქვს ამას დასაქმებულისთვის; და უზრუნველყოფილია თუ არა უსაფრთხოების სათანადო ზომები. ამასთან, სახელმწიფოს ძალისხმევით, კომუნიკაციაზე მონიტორინგის შემთხვევაში, დასაქმებულს უნდა ჰქონდეს წვდომა დაცვის საშუალებებზე შესაბამისი იურისდიქციის სასამართლო ორგანოს წინაშე წარსადგენად, რათა დადგინდეს, სულ მცირე, სადავო ღონისძიების კანონიერება და რამდენად დაცული იყო შესაბამისი კრიტერიუმები.

ამ შემთხვევაში, ECHR-მა დაადგინა მე-8 მუხლის დარღვევა, რადგან სახელმწიფო ორგანოებმა სათანადოდ ვერ დაიცვეს განმცხადებლის პირადი ცხოვრებისა და კორესპონდენციის პატივისცემის უფლება; შესაბამისად, ვერ მიაღწიეს სათანადო ბალანსს სასწორზე დადებულ ინტერესებს შორის.

დასაქმების შესახებ რეკომენდაციის თანახმად, პერსონალური მონაცემები დასაქმების მიზნებით უნდა შეგროვდეს პირდაპირ დასაქმებულისგან.

შერჩევის პროცესში შეგროვებული პერსონალური მონაცემები უნდა შემოიფარგლებოდეს მხოლოდ იმ ინფორმაციით, რომელიც აუცილებელია კანდიდატისა და მისი პოტენციალის შესაბამისობის შესაფასებლად.

რეკომენდაცია ცალკე ეხება კონკრეტული დასაქმებულის მიერ შესრულებული სამუშაოს ან პოტენციალის განსაზღვრისთვის საჭირო მონაცემებს, რომლებიც უნდა ეფუძნებოდეს სამართლიან და ღირსეულ შეფასებას და არ იყოს შეურაცხმყოფელი. ამ მოთხოვნას ადგენს მონაცემთა სამართლიანი დამუშავებისა და სიზუსტის პრინციპები.

მონაცემთა დაცვის სამართალში დამსაქმებელსა და დასაქმებულს შორის ურთიერთობის სპეციფიკური ასპექტია დასაქმებულთა წარმომადგენლების

ფუნქცია. ისინი შეიძლება იღებდნენ პერსონალურ მონაცემებს, თუ ეს აუცილებელია დასაქმებულთა ინტერესების დასაცავად, ან კოლექტიური შეთანხმებებით გათვალისწინებულ მოვალეობათა შესრულებისა და მონიტორინგისათვის.

დასაქმების მიზნებით შეგროვებული განსაკუთრებული კატეგორიის პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ კონკრეტულ შემთხვევებში და შიდასახელმწიფოებრივი კანონმდებლობით დადგენილი უსაფრთხოების ზომების შესაბამისად. დამსაქმებელს უფლება აქვს, დასაქმებულს ან განმცხადებელს დაუსვას კითხვები მისი ჯანმრთელობის მდგომარეობაზე, მოითხოვოს სამედიცინო წესით შემოწმება, თუ ეს აუცილებელია შემდეგი მიზნებით: სამუშაოსთან შესაბამისობის დადგენა; პრევენციული მედიცინით გათვალისწინებულ მოთხოვნათა შესრულება; სოციალური შეღავათების გამოყოფა; ან სასამართლო მოთხოვნებზე რეაგირება. ჯანმრთელობის მდგომარეობის მონაცემები უნდა შეგროვდეს უშუალოდ დასაქმებულისგან. დაუშვებელია ასეთი მონაცემების სხვა წყაროსგან შეგროვება, გარდა იმ შემთხვევისა, როდესაც არსებობს დასაქმებულის მკაფიო და ინფორმირებული თანხმობა, ან ამას ითვალისწინებს შიდასახელმწიფოებრივი კანონმდებლობა.

რეკომენდაციის თანახმად, დასაქმებულებს უნდა ეცნობოთ: მათი პერსონალური მონაცემების დამუშავების მიზნები; შენახული პერსონალური მონაცემების კატეგორიები; ინფორმაცია პირებზე, რომლებსაც ეს მონაცემები რეგულარულად გადაეცემათ; ასევე, გადაცემის მიზანი და სამართლებრივი საფუძველი. ელექტრონულ მონაცემებზე წვდომა სამუშაო ადგილას ნებადართულია მხოლოდ უსაფრთხოების ან სხვა კანონიერი მიზნების საფუძველზე და მას შემდეგ, რაც დასაქმებულები მიიღებენ ინფორმაციას ამის შესახებ.

დასაქმებულებს უნდა ჰქონდეთ უფლება, მოითხოვონ თავიანთ მონაცემებზე წვდომა, მათი გასწორება ან წაშლა. თუ მუშავდება შეფასებითი მონაცემები, დასაქმებულს უნდა ჰქონდეს გასაჩივრების უფლებაც. ამავდროულად, ასეთ უფლებებზე შეიძლება დაწესდეს დროებითი შეზღუდვა შიდა გამოძიების მიზნებით. თუ დასაქმებულს უარი ეთქვა დასაქმების პერსონალური მონაცემების წვდომაზე, გასწორებასა ან წაშლაზე, შიდასახელმწიფოებრივი კანონმდებლობა უნდა ადგენდეს შესაბამის პროცედურებს გასაჩივრებისათვის.

9.3 სამედიცინო მონაცემები

ძირითადი საკითხები

- სამედიცინო მონაცემები განსაკუთრებული კატეგორიის მონაცემებია, რომლებიც განსაკუთრებული დაცვით სარგებლობს.

პერსონალური მონაცემები სუბიექტის ჯანმრთელობის მდგომარეობაზე განსაკუთრებულ კატეგორიას მიეკუთვნება, მონაცემთა დაცვის ზოგადი დირექტივის მე-9 მუხლის პირველი პუნქტისა და მოდერნიზებული 108-ე კონვენციის მე-6 მუხლის შესაბამისად. ამრიგად, სამედიცინო მონაცემებზე, არაგანსაკუთრებული კატეგორიის მონაცემებისაგან განსხვავებით, დამუშავების გამკაცრებული რეჟიმი ვრცელდება. მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, აკრძალულია ჯანმრთელობის შესახებ პერსონალური მონაცემების („მონაცემთა სუბიექტის ჯანმრთელობის მდგომარეობის ამსახველი ყველა მონაცემი, რომლებიც შეიცავს ინფორმაციას მისი ფიზიკური ან სულიერი ჯანმრთელობის წარსული, ამჟამინდელი და მომავალი მდგომარეობის შესახებ“) დამუშავება.[935] რეგულაცია კრძალავს გენეტიკური და ბიომეტრიული მონაცემების დამუშავებასაც, გარდა მე-9 მუხლის მე-2 პუნქტით გათვალისწინებული შემთხვევებისა. ორივე ტიპის მონაცემები შეტანილია „მონაცემთა განსაკუთრებული კატეგორიების“ ჩამონათვალში.[936]

მაგალითი: საქმეში *Z v. Finland*[937] განმცხადებლის ყოფილმა მეუღლემ, რომელიც აივ ვირუსით იყო ინფიცირებული, სქესობრივი დანაშაულები ჩაიდინა. საბოლოოდ, სასამართლომ იგი დამნაშავედ ცნო მკვლელობის მცდელობისთვის, რადგან დაზარალებულები გაცნობიერებულად დააყენა აივ ინფიცირების რისკქვეშ. ეროვნულმა სასამართლომ მთლიანი გადაწყვეტილება და საქმის მასალები 10 წლის ვადით კონფიდენციალურად ცნო, მიუხედავად იმისა, რომ განმცხადებელი ამას 10 წელზე მეტი ხნით ითხოვდა. კონფიდენციალობის მოთხოვნა სააპელაციო სასამართლომ არ დააკმაყოფილა და თავის გადაწყვეტილებაში განმცხადებლისა და მისი ყოფილი მეუღლის სახელები სრულად მიუთითა. ECtHR-მა დაადგინა, რომ ასეთი ჩარევა არ იყო აუცილებელი დემოკრატიულ საზოგადოებაში, რადგან სამედიცინო მონაცემების დაცვას ფუნდამენტური მნიშვნელობა აქვს პირადი და ოჯახური ცხოვრების პატივისცემის უფლებისთვის, განსაკუთრებით, როდესაც საქმე ეხება აივ ინფექციებზე ინფორმაციას (იმ სტიგმის გათვალისწინებით, რომელიც აღნიშნულ დაავადებას ახლავს ზოგიერთ საზოგადოებაში). ამრიგად, სასამართლომ დაადგინა, რომ მიღებიდან 10 წლის შემდეგ წვდომის დაშვება სააპელაციო სასამართლოს გადაწყვეტილებაზე, რომელიც შეიცავდა ინფორმაციას განმცხადებლის ვინაობისა და ჯანმრთელობის მდგომარეობის შესახებ, დაარღვევდა კონვენციის მე-8 მუხლს.

935 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 35.

936 *იქვე,* მუხლი 2.

937 ECtHR, *Z v. Finland,* No. 22009/93, 1997 წლის 25 თებერვალი, პუნქტები 94 და 112; ECtHR, *M.S. v. Sweden,* No. 20837/92, 1997 წლის 27 აგვისტო; ECtHR, *L.L. v. France,* No. 7508/02, 2006 წლის 10 ოქტომბერი; ECtHR, *I v. Finland,* No. 20511/03, 2008 წლის 17 ივლისი; ECtHR, *K.H. and Others v. Slovakia,* No. 32881/04, 2009 წლის 28 აპრილი; ECtHR, *Szuluk v. the United Kingdom,* No. 36936/05, 2009 წლის 2 ივნისი.

ევროკავშირის კანონმდებლობაში, მონაცემთა დაცვის ზოგადი რეგულაციის მე-9 მუხლის 2 (თ) პუნქტი სამედიცინო მონაცემების დამუშავების ნებართვას იძლევა ისეთი მიზნებით, როგორიცაა: პრევენციული მედიცინა, სამედიცინო დიაგნოზის დასმა, მკურნალობის კურსის ან ჯანდაცვის მომსახურების მართვა. დამუშავება დასაშვებია მხოლოდ სამედიცინო პერსონალისთვის, რომელსაც ეკისრება პროფესიული საიდუმლოს დაცვის ვალდებულება, ასევე, მსგავსი ვალდებულების მქონე სხვა პირებისთვის.[938]

ევროპის საბჭოს 1997 წლის რეკომენდაცია სამედიცინო მონაცემების შესახებ უფრო დეტალურად განავრცობს 108-ე კონვენციის პრინციპებს სამედიცინო სფეროში მონაცემთა დამუშავებაზე. [939] რეკომენდაციაში წარმოდგენილი წესები შეესაბამება მონაცემთა დაცვის ზოგადი რეგულაციის დებულებებს შემდეგ საკითხებთან დაკავშირებით: სამედიცინო მონაცემების დამუშავების კანონიერი მიზნები; პროფესიული საიდუმლოების ვალდებულების დაცვა იმ პირთა მიერ, რომლებიც ჯანმრთელობის მონაცემებს იყენებენ; და მონაცემთა სუბიექტების უფლებები მონაცემთა გამჭვირვალობის, წვდომის, გასწორებისა და წაშლის მოთხოვნის კუთხით. ამასთან, კანონიერად დამუშავებული სამედიცინო მონაცემები პერსონალმა არ უნდა გადასცეს სამართალდამცველ ორგანოებს, თუ „გარანტირებული არ იქნება უსაფრთხოების სათანადო ზომები იმგვარი გამჟღავნების პრევენციისთვის, რომელიც არ შეესაბამება კონვენციის მე-8 მუხლით გარანტირებულ პირადი ცხოვრების პატივისცემის უფლებას.“[940] შიდასახელმწიფოებრივი კანონმდებლობა „ფორმულირებული უნდა იყოს საკმარისი სიზუსტით და უზრუნველყოფდეს ადეკვატურ სამართლებრივ დაცვას თვითნებობის წინააღმდეგ.“ [941]

ამასთან, რეკომენდაცია სამედიცინო მონაცემების შესახებ შეიცავს სპეციალურ დებულებებს ჯერ კიდევ არშობილი ბავშვებისა და ქმედუუნარო პირების სამედიცინო და გენეტიკური მონაცემების დამუშავებაზე. სამეცნიერო კვლევა ცალსახად აღიარებულია, როგორც მონაცემთა საჭირო ვადაზე მეტხანს შენახვის საფუძველი, თუმცა, ეს შემთხვევა, როგორც წესი, მოითხოვს მონაცემთა ანონიმიზაციას. რეკომენდაცია სამედიცინო მონაცემების შესახებ, კერძოდ, მისი მე-12 მუხლი, დეტალურად არეგულირებს შემთხვევებს, სადაც მკვლევარებს სჭირდებათ პერსონალური მონაცემები და ანონიმიზებული ინფორმაცია არ კმარა.

სამეცნიერო საჭიროებათა დაკმაყოფილებისა და, ამავდროულად, პაციენტთა ინტერესების დაცვის კიდევ ერთი საშუალებაა ფსევდონიმიზაცია. ფსე-

938 See also ECtHR, *Biriuk v. Lithuania,* No. 23373/03, 25 November 2008.

939 ევროპის საბჭო, მინისტრთა კომიტეტი (1997), რეკომენდაცია REC(97)5 წევრი ქვეყნებისთვის სამედიცინო მონაცემების დაცვის შესახებ, 13 თებერვალი, 1997 წელი. ამჟამად რეკომენდაცია გადახედვის პროცესშია.

940 ECtHR, *Avilkina and Others v. Russia,* No. 1585/09, 2013 წლის 6 ივნისი, პუნქტი. 53.

941 *ECtHR, L.H. v. Latvia,* No. 52019/07, 29 April 2014, პუნქტი 59.

ვდონიმიზაციის კონცეფციას მონაცემთა დაცვის კონტექსტში უფრო დეტალურად განიხილავს 2.1.1 ნაწილი.

ევროკავშირის 2016 წლის რეკომენდაცია გენეტიკური ტესტირების შედეგად მიღებულ მონაცემებზე ასევე შეეხება მონაცემთა დამუშავებას სამედიცინო სფეროში.[942] რეკომენდაცია უაღრესად მნიშვნელოვანია eHealth-ისათვის, რომელიც ხელს უწყობს სამედიცინო მზრუნველობას საინფორმაციო/საკომუნიკაციო ტექნოლოგიების გამოყენებით. აღნიშნულის მაგალითია პაციენტის ორსულობის ტესტის შედეგების გაგზავნა ჯანდაცვის ერთი პროვაიდერიდან მეორესათვის. აღნიშნული რეკომენდაცია მიზნად ისახავს იმ პირთა უფლებების დაცვას, ვისი პერსონალური მონაცემებიც მუშავდება დაზღვევის მიზნებით, რათა თავიდან აიცილონ პირის ჯანმრთელობის, ფიზიკური უვნებლობის, ასაკისა და გარდაცვალების რისკები. ჯანმრთელობის მონაცემთა დამუშავებისათვის სადაზღვევო კომპანიას შესაბამისი საფუძველი უნდა ჰქონდეს, რომელიც იქნება რისკის ბუნებისა და მნიშვნელობის პროპორციული. ასეთი მონაცემების დამუშავება დამოკიდებულია სუბიექტის თანხმობაზე. დამზღვევს ასევე მოეთხოვება დაცვის გარანტიების დანერგვა ჯანმრთელობის მონაცემების შენახვის კუთხით.

კლინიკური ცდები, რაც გულისხმობს პაციენტებზე ახალი მედიკამენტების გამოცდას კვლევით გარემოში და შედეგების დოკუმენტირებას, მნიშვნელოვან გავლენას ახდენს მონაცემთა დაცვაზე. ამ საკითხს არეგულირებს ევროპარლამენტისა და საბჭოს 2014 წლის 16 აპრილის რეგულაცია (EU) No. 536/2014 ადამიანებისათვის განკუთვნილი სამედიცინო პროდუქტების კლინიკური ცდების შესახებ, რითაც გაუქმდა დირექტივა 2001/20/EC (კლინიკური ცდების რეგულაცია).[943] კლინიკური ცდების რეგულაციის ძირითადი ელემენტებია:

- განცხადების შეტანის გამარტივებული პროცედურა ევროკავშირის პორტალის საშუალებით; [944]
- კლინიკური ცდებზე განცხადების შეფასების ვადები; [945]

942 ევროპის საბჭო, მინისტრთა კომიტეტი (2016), რეკომენდაცია Rec(2016)8 წევრი სახელმწიფოებისთვის, ჯანმრთელობის მონაცემთა დამუშავებაზე სადაზღვევო მიზნებით, გენეტიკური ანალიზის შედეგების ჩათვლით, 2016 წლის 26 ოქტომბერი.

943 ევროპული პარლამენტისა და საბჭოს 2014 წლის 16 აპრილის რეგულაცია (EU) No. 536/2014 ადამიანებისათვის განკუთვნილი სამედიცინო პროდუქტების კლინიკური ცდების შესახებ, რომლითაც უქმდება დირექტივა 2001/20/EC (კლინიკური ცდების რეგულაცია), OJ 2014 L 158.

944 რეგულაცია კლინიკური ცდების შესახებ, მუხლი 5 (1).

945 *იქვე,* მუხლი 5 (2)–(5).

- შეფასებაში ეთიკის კომიტეტის მონაწილეობა, წევრი სახელმწიფოს და ევროპული კანონმდებლობის შესაბამისად;[946]

- კლინიკური ცდებისა და შედეგების გამჭვირვალობის გაუმჯობესება.[947]

მონაცემთა დაცვის ზოგადი რეგულაცია ადგენს, რომ სამედიცინო კვლევაში მონაწილეობაზე თანხმობა ექვემდებარება (EU) No. 536/2014 რეგულაციას.[948]

ამჟამად ევროკავშირის დონეზე მზადდება არაერთი საკანონმდებლო და სხვა ინიციატივა პერსონალური მონაცემების შესახებ ჯანდაცვის სექტორში.[949]

ელექტრონული ჩანაწერები ჯანმრთელობის შესახებ

ეს არის „კომპლექსური სამედიცინო ჩანაწერები ან მსგავსი დოკუმენტები, რომლებიც შეიცავს ინფორმაციას პირის ფიზიკური ან სულიერი ჯანმრთელობის წარსული, ამჟამინდელი და მომავალი მდგომარეობის შესახებ, ელექტრონული ფორმით, და ხელმისაწვდომია სამედიცინო მკურნალობის და მასთან მჭიდროდ დაკავშირებული მიზნებით.“[950] ელექტრონული ჩანაწერები ჯანმრთელობის შესახებ პაციენტის სამედიცინო ისტორიის ელექტრონული ვერსიაა და შეიძლება შეიცავდეს კლინიკურ მონაცემებს ამ პირის შესახებ (მაგ.: სამედიცინო ისტორია, ჯანმრთელობის პრობლემები და მდგომარეობა, მედიკამენტები და მკურნალობა, სამედიცინო შემოწმებისა თუ ლაბორატორიული ანალიზების შედეგები და დასკვნები). აღნიშნული ელექტრონული ფაილები, რომლებიც შეიძლება შეიცავდეს მთლიან სამედიცინო ჩანაწერებს ან უბრალოდ ამონაწერს/რეზიუმეს, ხელმისაწვდომია საერთო პრაქტიკოსის, ფარმაცევტისა და ჯანდაცვის სფეროს სხვა მუშაკისათვის. ამ ჩანაწერებს ეხება eHealth-ის კონცეფციაც.

მაგალითი: ბ-ნი „A“ დაეზღვია კომპანიაში „B“ (მზღვეველი), რომელმაც „A“-სგან შეაგროვა ინფორმაცია ჯანმრთელობის არსებულ პრობლემებსა და დაავადებებზე. მზღვეველი ვალდებულია, ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემები, მათ შორის, „A“-სიც, შეინახოს სხვა მონაცემებისგან განცალკევებულად; ეს ნიშნავს, რომ „A“-ს ჯანმრ-

946 *იქვე,* მუხლი 2, პუნქტი 2 (11).

947 *იქვე,* მუხლი 9 (1) და პრეამბულა, პუნქტი 67.

948 მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 156 და 161.

949 EDPS (2013), მონაცემთა დაცვის ევროპული ზედამხედველის მოსაზრება კომისიის მიმართვაზე, „eHealth-ის სამოქმედო გეგმა 2012-2020 – ინოვაციური ჯანდაცვა 21-ე საუკუნეში“, ბრიუსელი, 27 მარტი 2013 წელი.

950 კომისიის 2008 წლის 2 ივლისის რეკომენდაცია ჯანმრთელობის მონაცემების აღრიცხვის სისტემათა საერთაშორისო ფუნქციურ თავსებადობაზე, მუხლი 3 (გ).

> თელობის მონაცემებზე წვდომა ექნება სადაზღვევო კომპანიის მხოლოდ იმ თანამშრომელს, რომელიც „A“-ს საქმეზე მუშაობს.

ამავდროულად, ჯანმრთელობაზე ინფორმაციის შემცველ ელექტრონულ ფაილებთან მიმართებით, წამოიჭრება მონაცემთა დაცვის გარკვეული პრობლემები, როგორიცაა მათი ხელმისაწვდომობა, სათანადოდ შენახვა და წვდომა მონაცემთა სუბიექტის მიერ.

2014 წლის 10 აპრილს ევროკომისიამ გამოაქვეყნა ე.წ. „მწვანე დოკუმენტი“ (Green Paper) მობილური ჯანდაცვის შესახებ (mHealth), იმის გათვალისწინებით, რომ mHealth სწრაფად მზარდი სფეროა, რომელსაც აქვს ჯანდაცვის სფეროს საფუძვლიანად შეცვლის, ასევე, მისი ეფექტიანობისა და ხარისხის გაუმჯობესების პოტენციალი. ამ ტერმინში იგულისხმება სამედიცინო და საზოგადოებრივი ჯანდაცვის პრაქტიკის მხარდაჭერა მობილური მოწყობილობების (მაგ.: მობილური ტელეფონები, პაციენტის მონიტორინგის მოწყობილობა, პერსონალური ციფრული ასისტენტები და სხვა უკაბელო ტექნიკა) და აპლიკაციებით (მაგ.: კეთილდღეობის აპლიკაცია), რომელთა დაკავშირებაც შესაძლებელია სამედიცინო მოწყობილობებსა ან სენსორებთან.[951] დოკუმენტი მიმოიხილავს პერსონალურ მონაცემთა დაცვის უფლებასთან დაკავშირებულ რისკებს, რაც შესაძლოა წარმოიშვას mHealth-ის განვითარების შედეგად. დოკუმენტის თანახმად, ჯანმრთელობასთან დაკავშირებული მონაცემების სენსიტიურობის გათვალისწინებით, mHealth უნდა განვითარდეს იმგვარად, რომ მოიცვას პაციენტთა მონაცემების უსაფრთხოების დაცვის კონკრეტული და შესაფერისი მექანიზმები (მაგ.: დაშიფვრა) და ვინაობის დადგენის სათანადო საშუალებები, უსაფრთხოების რისკების შესამცირებლად. mHealth-ის მიმართ ნდობისათვის, სასიცოცხლოდ მნიშვნელოვანია შესაბამისობა პერსონალური მონაცემების დაცვის წესებთან, მათ შორის, მონაცემთა სუბიექტისთვის შეტყობინების ვალდებულების შესრულება, ასევე, მონაცემთა უსაფრთხოებისა და კანონიერი დამუშავების პრინციპების დაცვა.[952] ამ მიზნით, სხვადასხვა დაინტერესებული მხარეების, მათ შორის, ჯანდაცვისა და საინფორმაციო/საკომუნიკაციო ტექნოლოგიების ექსპერტთა მონაწილეობით, შეიქმნა ქცევის კოდექსი.[953] წინამდებარე სახელმძღვანელოზე მუშაობის დროს, ქცევის კოდექსს განიხილავდა 29-ე მუხლის სამუშაო ჯგუფი, რომელმაც ფორმალურად უნდა დაამტკიცოს კოდექსი.

951 ევროპული კომისია (20140), „მწვანე დოკუმენტი მობილური ჯანდაცვის შესახებ (mHealth)“, COM(2014) 219, საბოლოო, ბრიუსელი, 2014 წლის 10 აპრილი.

952 *იქვე,* გვ. 8.

953 პირადი ცხოვრების საკითხებზე ქცევის კოდექსის პროექტი მობილური ჯანდაცვის აპლიკაციებისათვის, 2016 წლის 7 ივნისი.

9.4 მონაცემთა დამუშავება კვლევისა და სტატისტიკური მიზნებისთვის

ძირითადი საკითხები

- სტატისტიკური მიზნებით შეგროვებული მონაცემები არ უნდა გამოიყენონ ნებისმიერი სხვა ამოცანისთვის.
- დასაშვებია ნებისმიერი მიზნით კანონიერად შეგროვებული მონაცემების გამოყენება სტატისტიკური, სამეცნიერო ან ისტორიული კვლევისთვის, თუკი არსებობს უსაფრთხოების სათანადო ზომები. ამ მიზნით მესამე მხარისთვის მონაცემთა გადაცემამდე, შესაძლებელია მონაცემთა ანონიმიზაცია ან ფსევდონიმიზაცია.
- ევროკავშირის კანონმდებლობით, მონაცემთა დამუშავება სტატისტიკური და სამეცნიერო/ისტორიული კვლევის მიზნებისთვის დასაშვებია, თუ არსებობს უსაფრთხოების სათანადო ზომები მონაცემთა სუბიექტების უფლებებისა და თავისუფლებებს დასაცავად, რაც, შესაძლოა მოიცავდეს ფსევდონიმიზაციას.[954] ევროკავშირის კანონმდებლობა და შიდასახელმწიფოებრივი კანონმდებლობა შესაძლებელია ითვალისწინებდეს გარკვეულ გამონაკლისებს, თუ აღნიშნული უფლებები შეუძლებელს გახდის ან მნიშვნელოვნად შეაფერხებს კვლევის კანონიერი მიზნების მიღწევას.[955] გამონაკლისის სახით, შეიძლება შეიზღუდოს მონაცემთა სუბიექტის უფლებები მონაცემებზე წვდომის, მათი გასწორების, დამუშავების შეზღუდვისა და შეწყვეტის მოთხოვნის კუთხით.

დამმუშავებელს უფლება აქვს, სტატისტიკური ან სამეცნიერო/ისტორიული კვლევისთვის გამოიყენოს ნებისმიერი მიზნით კანონიერად შეგროვებული მონაცემები, თუმცა, ასეთი მესამე მხარისთვის გადაცემამდე, საჭიროა მონაცემების ანონიმიზაცია ან ფსევდონიმიზაცია, კონტექსტის გათვალისწინებით, გარდა იმ შემთხვევისა, როცა არსებობს მონაცემთა სუბიექტის თანხმობა, ან ამ უფლებას კონკრეტულად ადგენს ეროვნული კანონმდებლობა. ფსევდონიმიზებულ მონაცემებზე, ანონიმიზებულისგან განსხვავებით, ვრცელდება მონაცემთა დაცვის ზოგადი რეგულაცია. [956]

ამრიგად, რეგულაციის თანახმად, კვლევის მიზნებით მონაცემთა გამოყენება ექვემდებარება მონაცემთა დაცვის ზოგადი წესებისგან განსხვავებულ მოპ-

954 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 89 (1).

955 *იქვე*, მუხლი 89 (2).

956 *იქვე*, პრეამბულა 26.

ყრობას. ამის მიზანია კვლევის შეფერხების თავიდან აცილება და ევროპული კვლევითი სივრცის შექმნა, TFEU-ს მე-19 მუხლის შესაბამისად. ეს საშუალებას იძლევა, ფართოდ განიმარტოს პერსონალური მონაცემების დამუშავება ისეთი მიზნებით, როგორიცაა სამეცნიერო (მათ შორის, ტექნოლოგიური განვითარების) კვლევა და დემონსტრირება, ასევე, საბაზისო, გამოყენებითი და კერძო პირის მიერ დაფინანსებული კვლევები. რეგულაცია აღიარებს სხვადასხვა რეესტრში მონაცემთა შეგროვებისა და დამუშავების მნიშვნელობას კვლევითი მიზნებით, ასევე, სირთულეებს, რომლებიც უკავშირდება პერსონალურ მონაცემთა დამუშავების შემდგომი მიზნების სრულად იდენტიფიცირებას ამ მონაცემების შეგროვებისას.[957] აღნიშნული მიზეზის გამო, რეგულაციის მიხედვით, მონაცემთა დამუშავება კვლევითი მიზნებით, მონაცემთა სუბიექტის თანხმობის გარეშე, ნებადართულია მხოლოდ უსაფრთხოების შესაბამისი ზომების არსებობისას.

მონაცემთა სტატისტიკური მიზნებით გამოყენების ერთ-ერთი მნიშვნელოვანი მაგალითია ოფიციალური სტატისტიკა, რომელსაც აწარმოებენ ეროვნულ და ევროკავშირის დონეზე არსებული სტატისტიკის სამსახურები, შესაბამისი კანონმდებლობების საფუძველზე. ამ კანონმდებლობათა თანახმად, მოქალაქეები და ორგანიზაციები, როგორც წესი, ვალდებულნი არიან, გაუმჟღავნონ მონაცემები სტატისტიკურ სამსახურებს. სტატისტიკის სამსახურის თანამშრომლებს აქვთ პროფესიული საიდუმლოების შენახვის სპეციალური ვალდებულებები, რომლებიც სათანადოდ უნდა შესრულდეს. ეს ვალდებულებები მნიშვნელოვანია იმისათვის, რომ მოქალაქეებს ჰქონდეთ მაღალი ნდობა, რაც გავლენას ახდენს მონაცემთა ხელმისაწვდომობაზე სტატისტიკის ორგანოებისათვის.[958]

ევროპული რეგულაცია სტატისტიკის შესახებ (EC) No. 223/2009 (ევროპული სტატისტიკის რეგულაცია) მნიშვნელოვან წესებს შეიცავს მონაცემთა დაცვაზე ოფიციალური სტატისტიკის კონტექსტში. ამგვარად, შეიძლება ითქვას, ეს რეგულაცია მისაღებია ეროვნულ დონეზე არსებული შესაბამისი სამართლებრივი დებულებებისათვის.[959] რეგულაცია შეიცავს პრინციპს, რომლის თანახ-

957 *იქვე,* პრეამბულა, პუნქტები 33, 157 და 159.

958 *იქვე,* მუხლი 90.

959 ევროპული პარლამენტისა და საბჭოს 2009 წლის 11 მარტის რეგულაცია (EC) No. 223/2009 ევროპული სტატისტიკის შესახებ, რომლითაც უქმდება პარლამენტისა და საბჭოს რეგულაცია (EC, Euratom) No. 1101/2008 ევროპული გაერთიანების სტატისტიკური სამსახურისთვის იმ მონაცემთა გადაცემაზე, რომლებზეც ვრცელდება სტატისტიკური კონფიდენციალობა; საბჭოს რეგულაცია (EC) No. 322/97 გაერთიანების სტატისტიკის შესახებ; და საბჭოს გადაწყვეტილება 89/382/EEC ევროპული გაერთიანების სტატისტიკური პროგრამების Euratom-ის კომიტეტის შექმნაზე, OJ 2009 L 87, როგორც შესწორებულია ევროპული პარლამენტისა და საბჭოს 2015 წლის 29 აპრილის რეგულაციით EU) 2015/759, რომელსაც შესწორებები შეაქვს რეგულაციაში (EC) No. 223/2009 ევროპული სტატისტიკის შესახებ, OJ 2015 L 123.

მადაც ოფიციალურ სტატისტიკასთან დაკავშირებული საქმიანობა საჭიროებს მკაფიო სამართლებრივ საფუძველს.[960]

მაგალითი: საქმეში *Huber v. Bundesrepublik Deutschland*[961] ავსტრიელი ბიზნესმენი, რომელიც გერმანიაში გადავიდა საცხოვრებლად, აცხადებდა, რომ გერმანიის სახელმწიფო ორგანოების მიერ უცხო ქვეყნის მოქალაქეთა პერსონალური მონაცემების შეგროვება და ცენტრალურ რეესტრში შენახვა სტატისტიკური მიზნებით არღვევდა მის უფლებებს, დადგენილს მონაცემთა დაცვის დირექტივით. ვინაიდან 95/46 დირექტივის მიზანია მონაცემთა თანაბარ დონეზე დაცვა ყველა წევრ სახელმწიფოში, CJEU-მ დაადგინა, რომ ევროკავშირში დაცვის მაღალი დონის უზრუნველსაყოფად, 7(ე) მუხლში წარმოდგენილ აუცილებლობის კონცეფციას სხვადასხვა წევრ სახელმწიფოში განსხვავებული მნიშვნელობა ვერ ექნება. ამრიგად, კონცეფცია, რომელსაც ევროკავშირის კანონმდებლობაში დამოუკიდებელი მნიშვნელობა აქვს, უნდა განიმარტოს იმგვარად, რომ ბოლომდე აისახოს 95/46 დირექტივის მიზანი. CJEU-მ აღნიშნა, რომ სტატისტიკური მიზნებისთვის უნდა მოითხოვებოდეს მხოლოდ ანონიმური ინფორმაცია, და დაადგინა, რომ გერმანიის რეესტრი არ შეესაბამება აუცილებლობის მოთხოვნას, გათვალისწინებულს 7 (ე) მუხლით.

ევროპის საბჭოს კანონმდებლობის კონტექსტში, მონაცემთა შემდგომი დამუშავება სამეცნიერო/ისტორიული ან სტატისტიკური მიზნებით შესაძლებელია საჯარო ინტერესის გამო, თუმცა უნდა არსებობდეს დაცვის სათანადო გარანტიები.[962] მონაცემთა სუბიექტის უფლებების შეზღუდვა სტატისტიკური მიზნებით დამუშავებისას ნებადართულია, თუ მათ უფლებებსა და თავისუფლებებს რეალური საფრთხე არ ემუქრება.[963]

რეკომენდაცია სტატისტიკური მონაცემების შესახებ, რომელიც გამოიცა 1997 წელს, შეეხება სტატისტიკურ საქმიანობას საჯარო და კერძო სექტორებში.[964]

960 ეს პრინციპი დეტალურად გავრცობილია Eurostat-ის პრაქტიკის კოდექსში, რომელიც, ევროპული სტატისტიკის რეგულაციის მე-11 მუხლის თანახმად, ადგენს ეთიკის სახელმძღვანელო დებულებებს ოფიციალური სტატისტიკის წარმოებაზე, მათ შორის, პერსონალურ მონაცემთა სწორად გამოყენებაზე;

961 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 16 December 2008; იხ. პუნქტი 68.

962 მოდერნიზებული 108-ე კონვენცია, მუხლი 5 (4) (ბ).

963 *იქვე*, მუხლი 11 (2).

964 ევროპის საბჭო, მინისტრთა კომიტეტი (1997), რეკომენდაცია REC (97)18 წევრი ქვეყნებისთვის სტატისტიკური მიზნებით შეგროვებული და დამუშავებული პერსონალური მონაცემების შესახებ, 30 სექტემბერი 1997 წელი.

დაუშვებელია მონაცემთა დამმუშავებლის მიერ სტატისტიკური მიზნებით შეგროვებული მონაცემების გამოყენება სხვა ამოცანებისთვის. ამასთანავე, რეკომენდაცია სტატისტიკური მონაცემების შესახებ დასაშვებად მიიჩნევს მონაცემთა გადაცემას მესამე პირებისთვის, თუ მიზანი მხოლოდ სტატისტიკის წარმოებაა. ასეთ შემთხვევაში, მხარეები უნდა შეთანხმდნენ და წერილობით განსაზღვრონ სტატისტიკის შემდგომი კანონიერი გამოყენების ფარგლები. ვინაიდან ეს ვერ ჩაანაცვლებს მონაცემთა სუბიექტის თანხმობას, საჭიროების შემთხვევაში, ეროვნული კანონმდებლობა უნდა ითვალისწინებდეს დაცვის სათანადო გარანტიებს (მაგ.: გამჟღავნებამდე მონაცემთა ანონიმიზაცია ან ფსევდონიმიზაცია), რათა შემცირდეს პერსონალური მონაცემების ბოროტად გამოყენების რისკები.

სტატისტიკური კვლევის სფეროში მომუშავე პროფესიონალებს შიდასახელმწიფოებრივი კანონმდებლობით უნდა დაეკისროთ საიდუმლოების დაცვის პროფესიული ვალდებულება, როგორც ოფიციალური სტატისტიკის შემთხვევაში. ეს უნდა გავრცელდეს ინტერვიუერებსა და პერსონალურ მონაცემთა სხვა შემგროვებლებზეც, თუ ისინი მუშაობენ მონაცემთა სუბიექტებისა და სხვა პირებისგან მონაცემების შეგროვების სფეროში.

როცა კანონი არ ითვალისწინებს პერსონალური მონაცემების გამოყენებას სტატისტიკური გამოკითხვისთვის, საჭიროა მონაცემთა სუბიექტის თანხმობა, რათა გამოყენება იყოს კანონიერი, ან პირს ჰქონდეს, სულ მცირე, გასაჩივრების შესაძლებლობა. თუ პერსონალურ მონაცემებს სტატისტიკური მიზნებით აგროვებენ ინტერვიუერები, მათ მკაფიოდ უნდა განემარტოთ, არის თუ არა მონაცემთა მიწოდება სავალდებულო ეროვნული კანონმდებლობის თანახმად.

როდესაც სტატისტიკური კვლევის ჩატარება შეუძლებელია ანონიმიზებული მონაცემების გამოყენებით და საჭიროებს პერსონალურ მონაცემებს, ამ მიზნით შეგროვებული მონაცემების ანონიმიზაციას შესაძლებლობისთანავე უნდა მიმართონ. სტატისტიკური კვლევის შედეგები არ უნდა იძლეოდეს, სულ მცირე, რომელიმე მონაცემთა სუბიექტის იდენტიფიცირების საშუალებას, გარდა იმ შემთხვევისა, როცა ეს არ ქმნის რაიმე აშკარა რისკს.

სტატისტიკური ანალიზის შემდეგ, საჭიროა გამოყენებული პერსონალური მონაცემების წაშლა ან ანონიმიზაცია. ასეთ შემთხვევებში, რეკომენდაცია სტატისტიკური მონაცემების შესახებ ითვალისწინებს მაიდენტიფიცირებელი მონაცემების განცალკევებულად შენახვას. ეს ნიშნავს, რომ შიფრის კოდი ან ჩამონათვალი, რომელიც შეიცავს მაიდენტიფიცირებელ სიმბოლოებს, სხვა მონაცემებისგან გამიჯნულად უნდა შეინახონ.

9.5 ფინანსური მონაცემები

ძირითადი საკითხები

- მიუხედავად იმისა, რომ მოდერნიზებული 108-ე კონვენციის ან მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, ფინანსური მონაცემები განსაკუთრებულ კატეგორიას არ მიეკუთვნება, მათი დამუშავება უსაფრთხოების გარკვეულ ზომებს მოითხოვს, რათა მონაცემები იყოს სწორი, მათი უსაფრთხოება კი - დაცული.

- ელექტრონული ანგარიშსწორების სისტემები მოითხოვს მონაცემთა დაცვის სტანდარტების გათვალისწინებას ახალი პროდუქტის ან მომსახურების შექმნისას (by Design) და მონაცემთა დაცვას პირველად პარამეტრად (by Default).

- ნამდვილობის შესაბამისი მექანიზმების საჭიროებიდან გამომდინარე, ამ სფეროში შეიძლება წარმოიშვას მონაცემთა დაცვის კონკრეტული პრობლემები.

მაგალითები: საქმეში *Michaud v. France*[965] განმცხადებელმა, ფრანგმა იურისტმა, გაასაჩივრა ვალდებულება, რომელიც მას ფრანგული კანონმდებლობით ეკისრებოდა და ითვალისწინებდა ადმინისტრაციული ორგანოების ინფორმირებას კლიენტის მიერ ფულის სავარაუდო გათეთრების შესახებ. ევროპულმა სასამართლომ დაადგინა, რომ იურისტებზე დაწესებული ვალდებულება, ადმინისტრაციული ორგანოებისთვის ეცნობებინათ ისეთი ინფორმაცია, რომელიც ხელთ ჩაუვარდათ ინფორმაციის პროფესიული მიზნით გაცვლისას, იყო ჩარევა კონვენციის მე-8 მუხლით დაცულ კორესპონდენციისა და პირადი ცხოვრების პატივისცემის უფლებაში, ვინაიდან ეს კონცეფცია მოიცავს პროფესიულ ან საქმიან ქმედებებს. თუმცა, ჩარევა შეესაბამებოდა კანონს და ემსახურებოდა კანონიერ მიზანს - კერძოდ, საზოგადოებრივი წესრიგის დარღვევისა და დანაშაულის პრევენციას. იურისტები ვალდებულნი არიან, გარკვეული გარემოებებისას შესაბამის უწყებებს შეატყობინონ საეჭვო საქმიანობის შესახებ. ამგვარად, ECtHR-მა დაადგინა, რომ ეს ვალდებულება იყო პროპორციული. სასამართლოს დასკვნით, საქმეში კონვენციის მე-8 მუხლი არ დარღვეულა.

965 ECtHR, *Michaud v. France,* No. 12323/11, 2012 წლის 6 დეკემბერი; ასევე, იხ. ECtHR, *Niemietz v. Germany,* No. 13710/88, 1992 წლის 16 დეკემბერი, პუნქტი 29, და ECtHR, *Halford v. the United Kingdom,* No. 20605/92, 1997 წლის 25 ივნისი, პუნქტი 42.

საქმეში *M.N. and Others v. San Marino*[966] განმცხადებელმა (იტალიის მოქალაქე) ფიდუციური შეთანხმება გააფორმა კომპანიასთან, რომლის საქმიანობაზეც დაწყებული იყო გამოძიება. შესაბამისად, კომპანიაში მიმდინარეობდა (ელექტრონული) დოკუმენტაციის ჩხრეკისა და ამოღების საგამოძიებო ღონისძიება. განმცხადებელმა საჩივარი შეიტანა სან მარინოს სასამართლოში, სადაც აცხადებდა, რომ სავარაუდო დანაშაულებთან კავშირი არ ჰქონდა. სასამართლომ მისი საჩივარი დაუშვებლად ცნო - იმ მოტივით, რომ იგი „დაინტერესებული მხარე“ არ გახლდათ. ECtHR-მა დაადგინა, რომ განმცხადებელს, „დაინტერესებული მხარისგან“ განსხვავებით, სასამართლო დაცვაზე ხელი არ მიუწვდებოდა, თუმცა კი მასზე არსებული მონაცემები ექვემდებარებოდა ჩხრეკასა და ამოღებას. ამრიგად, სასამართლომ საქმეზე დაადგინა მე-8 მუხლის დარღვევა.

საქმეში *G.S.B. v. Switzerlan*[967] განმცხადებლის საბანკო ანგარიშებზე ინფორმაცია გაეგზავნა აშშ-ს საგადასახადო ორგანოებს, შვეიცარიასა და აშშ-ს შორის ადმინისტრაციული თანამშრომლობის შეთანხმების საფუძველზე. ECtHR-მა დაადგინა, რომ გადაცემა არ არღვევდა კონვენციის მე-8 მუხლს, რადგან განმცხადებლის პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევა გათვალისწინებული იყო კანონით, ემსახურებოდა კანონიერ მიზანს და იყო შესაბამისი საჯარო ინტერესის პროპორციული.

მონაცემთა დაცვის ზოგადი სამართლებრივი ჩარჩოს (როგორც გათვალისწინებულია 108-ე კონვენციით) გავრცელებას ფინანსურ ანგარიშსწორებაზე ითვალისწინებს ევროპის საბჭოს 1990 წლის რეკომენდაცია Rec(90)19 of 1990.[968] იგი განმარტავს ანგარიშსწორების კონტექსტში მონაცემთა კანონიერი შეგროვებისა და გამოყენების ფარგლებს, განსაკუთრებით, საკრედიტო ბარათებით გადახდისას; ასევე, შიდასახელმწიფოებრივი კანონმდებლებისთვის ადგენს დეტალურ რეკომენდაციებს შემდეგ საკითხებზე: მესამე მხარისათვის ანგარიშსწორების მონაცემთა გადაცემის წესები, შენახვის მაქსიმალური ვადები, გამჭვირვალობა, უსაფრთხოება, საზღვართშორისი გადაცემის ზედამხედველობა და სამართლებრივი დაცვის საშუალებები. ევროპის საბჭომ შეიმუშავა მოსაზრება საგადასახადო მონაცემების გადაცემაზეც,[969] რომელშიც წარმოდგენილია შესაბამისი რეკომენდაციები და გასათვალისწინებელი საკითხები.

966 ECtHR, *M.N. and Others v. San Marino,* No. 28005/12, 2015 წლის 7 ივლისი.

967 ECtHR, *G.S.B. v. Switzerland,* No. 28601/11 2015 წლის 22 დეკემბერი.

968 ევროპის საბჭო, მინისტრთა კომიტეტი (1990), რეკომენდაცია No. R(90)19 გადახდებისა და სხვა დაკავშირებული ოპერაციებისთვის გამოყენებულ პერსონალურ მონაცემთა დაცვის შესახებ, 13 სექტემბერი 1990 წელი.

969 ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი (2014), მოსაზრება, თუ რა გავლენა აქვს მონაცემთა დაცვის მექანიზმებს სახელმწიფოთა შორის მონაცემების ავტომატურ გაცვლაზე, ადმინისტრაციული და საგადასახადო მიზნებით, 2014 წლის 4 ივნისი.

ევროპული სასამართლოს თანახმად, კონვენციის მე-8 მუხლით დაშვებულია ფინანსური მონაცემების, კერძოდ, პირის საბანკო რეკვიზიტების გადაცემა, თუ ეს განსაზღვრულია კანონით, ემსახურება კანონიერ მიზანს და შესაბამისი საჯარო ინტერესის პროპორციულია.[970]

ევროკავშირის სამართალში, ელექტრონული ანგარიშსწორების სისტემები, რომლებიც პერსონალური მონაცემების დამუშავებას ითვალისწინებს, უნდა აკმაყოფილებდეს მონაცემთა დაცვის ზოგადი რეგულაციის მოთხოვნებს და, შესაბამისად, ისეთ პრინციპებსაც, როგორიცაა მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (by Design) და მონაცემთა დაცვა პირველად პარამეტრად (by Default). პირველი მონაცემთა დამმუშავებელს ავალდებულებს სათანადო ტექნიკური და ორგანიზაციული ღონისძიებების გატარებას მონაცემთა დაცვის პრინციპების დასანერგად, ხოლო მეორე გულისხმობს მონაცემთა დამმუშავებლის მიერ მხოლოდ იმ პერსონალური მონაცემების დამუშავებას, რომლებიც აუცილებელია კონკრეტული მიზნისთვის (იხ. ნაწილი 4.4). რაც შეეხება ფინანსურ მონაცემებს, CJEU-ს თანახმად, გადაცემული საგადასახადო მონაცემები შეიძლება განეკუთვნებოდეს პერსონალურ მონაცემებს.[971] 29-ე მუხლის სამუშაო ჯგუფმა წევრი სახელმწიფოებისთვის შეიმუშავა სახელმძღვანელო პრინციპები, მათ შორის, მონაცემთა დაცვის წესებთან შესაბამისობის კრიტერიუმები, როდესაც პერსონალური მონაცემები საგადასახადო მიზნებით იცვლება ავტომატური საშუალებების გამოყენებით.[972] ამასთან, შექმნილია არაერთი სამართლებრივი ინსტრუმენტი ფინანსური ბაზრის, საკრედიტო დაწესებულებებისა და საინვესტიციო ფირმების საქმიანობის დასარეგულირებლად.[973] სხვა სამართლებრივი მექანიზმები ხელს უწყობს ბრძოლას ინსაიდერული გარიგებებისა და ბაზრით მანიპულაციის წინააღმდეგ.[974] ქვემოთ წარმოდგე-

970 ECtHR, *G.S.B. v. Switzerland,* No. 28601/11, 2015 წლის 22 დეკემბერი.

971 CJEU, C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others,* 2015 წლის 1 ოქტომბერი, პუნქტი 29.

972 29-ე მუხლის მონაცემთა დაცვის სამუშაო ჯგუფი (2015), WP29-ის განცხადება სახელმწიფოთა შორის მონაცემთა ავტომატურ გაცვლაზე ადმინისტრაციული და საგადასახადო მიზნებით, 14/EN WP 230.

973 ევროპული პარლამენტისა და საბჭოს 2014 წლის 15 მაისის დირექტივა 2014/65/EU საფინანსო ინსტრუმენტების ბაზრების შესახებ, რომლითაც შესწორებები შევიდა 2002/92/EC და 2011/61/EU დირექტივებში, OJ 2014 L 173; ევროპული პარლამენტისა და საბჭოს 2015 წლის 15 მაისის რეგულაცია (EU) No. 600/2014 საფინანსო ინსტრუმენტების ბაზრების შესახებ, რომლითაც შესწორებები შევიდა რეგულაციაში (EU) No. 648/2012, OJ 2014 L 173; ევროპული პარლამენტისა და საბჭოს 2013 წლის 26 ივნისის დირექტივა 2013/36/EU, რომელიც შეეხება ხელმისაწვდომობას საკრედიტო დაწესებულებათა საქმიანობაზე და გონივრულ ზედამხედველობას ამ დაწესებულებებსა და საინვესტიციო ფირმებზე. დოკუმენტით შესწორდა დირექტივა 2002/87/EC და გაუქმდა დირექტივები: 2006/48/EC და 2006/49/EC, OJ 2013 L 176.

974 ევროპული პარლამენტისა და საბჭოს 2014 წლის 16 აპრილის რეგულაცია (EU) No. 596/2014 ბაზრის ბოროტად გამოყენების შესახებ (ბაზრის ბოროტად გამოყენების რეგულაცია), რომლითაც გაუქმდა ევროპული პარლამენტისა და საბჭოს რეგულაცია 2003/6/EC და კომისიის დირექტივები: 2003/124/EC, 2003/125/EC და 2004/72/EC, OJ 2014 L 173.

ნილია ძირითადი მიმართულებები, რომლებიც გავლენას ახდენს მონაცემთა დაცვაზე:

- მონაცემთა შენახვა ფინანსური ტრანზაქციების შესახებ;
- პერსონალური მონაცემების გადაცემა მესამე ქვეყნებისთვის;
- სატელეფონო საუბრების ან ელექტრონული კომუნიკაციების ჩაწერა, მათ შორის, კომპეტენტური ორგანოების უფლებამოსილება, მოითხოვონ ჩაწერილი სატელეფონო და ტრეფიკის მონაცემები;
- პერსონალურ მონაცემთა გამჟღავნება, მათ შორის, სანქციების გამოქვეყნება;
- კომპეტენტური ორგანოების საზედამხედველო და საგამოძიებო უფლებამოსილებები, მათ შორის, ადგილზე შემოწმება და კერძო ტერიტორიაზე შესვლა დოკუმენტების ამოღების მიზნით;
- დარღვევებზე ანგარიშგების მექანიზმები, ე.ი. მხილების (whisle-blowing) სქემები;
- თანამშრომლობა წევრი ქვეყნების კომპეტენტურ ორგანოებსა და ევროპული ფასიანი ქაღალდებისა და ბაზრის ოფიციალურ ორგანოს (ESMA) შორის.

ამ სფეროში არსებობს სხვა საკითხებიც, რომლებიც ცალკე რეგულირდება, მაგალითად, მონაცემთა შეგროვება მონაცემთა სუბიექტების ფინანსურ მდგომარეობაზე[975] ან საერთაშორისო ანგარიშსწორება საბანკო გადარიცხვების საშუალებით, რომელსაც გარდაუვლად მოსდევს პერსონალური მონაცემების გადაცემა.[976]

975 ევროპული პარლამენტისა და საბჭოს 2009 წლის 16 სექტემბრის რეგულაცია (EC) No. 1060/2009 საკრედიტო სარეიტინგო სააგენტოების შესახებ, OJ 2009 L 302 და ცოტა ხნის წინათ შესწორებული ევროპული პარლამენტისა და საბჭოს 2014 წლის 16 აპრილის დირექტივა, რომლითაც შესწორდა დირექტივები: 2003/71/EC და 2009/138/EC და რეგულაციები: (EC) No. 1060/2009, (EU) No. 1094/2010 და (EU) No. 1095/2010 ევროპული საზედამხედველო ორგანოების (ევროპული სადაზღვევო და შრომითი პენსიების სააგენტო და ევროპული ფასიანი ქაღალდებისა და ბაზრების სააგენტო) უფლებამოსილებათა კუთხით, OJ 2014 L 153; ევროპული პარლამენტისა და საბჭოს 2013 წლის 21 მაისის რეგულაცია, რომლითაც შესწორდა რეგულაცია (EC) No. 1060/2009 საკრედიტო სარეიტინგო სააგენტოების შესახებ, OJ 2013 L 146.

976 ევროპული პარლამენტისა და საბჭოს 2007 წლის 13 ნოემბრის დირექტივა 2007/64/EC შიდა ბაზარზე ანგარიშსწორების მომსახურების შესახებ, რომლითაც შესწორდა დირექტივები: 97/7/EC, 2002/65/EC, 2005/60/EC და 2006/48/EC და გაუქმდა დირექტივა 97/5/EC, OJ 2007 L 319, შესწორებული ევროპული პარლამენტისა და საბჭოს დირექტივით 2009/111/EC, რომლითაც შესწორდა დირექტივები 2006/48/EC, 2006/49/EC და 2007/64/EC, OJ 2009 L 302.

10

პერსონალურ მონაცემთა დაცვის თანამედროვე გამოწვევები

ციფრული ანუ საინფორმაციო ტექნოლოგიების ეპოქა ხასიათდება კომპიუტერების, ინტერნეტისა და ციფრული ტექნოლოგიების ფართო მოხმარებით. იგი მოიცავს დიდი მოცულობით მონაცემების, მათ შორის, პერსონალური მონაცემების შეგროვებასა და დამუშავებას. გლობალიზებულ ეკონომიკაში ეს ნიშნავს, რომ იზრდება მონაცემთა საერთაშორისო გადაცემის შემთხვევები. ასეთ დამუშავებას ყოველდღიურ ცხოვრებაში მნიშვნელოვანი და ხილული სარგებელი მოაქვს. კერძოდ, საძიებო სისტემები ხელს უწყობს წვდომას დიდი მოცულობის ინფორმაციასა და ცოდნაზე; სოციალური ქსელები ადამიანებს საშუალებას აძლევს, მსოფლიო მასშტაბით დაამყარონ კომუნიკაცია, გამოხატონ მოსაზრებები და მხარი დაუჭირონ სოციალურ, გარემოსდაცვით თუ პოლიტიკურ საკითხებს; კომპანიებისა და მომხმარებლებისთვის სარგებელი მოაქვს ეფექტიანი მარკეტინგის ტექნოლოგიებს, რაც, საბოლოოდ, დადებითად აისახება ეკონომიკის ზრდაზე. ტექნოლოგია და პერსონალური მონაცემების დამუშავება შეუცვლელი ინსტრუმენტებია სახელმწიფო ორგანოებისთვისაც, კერძოდ, დანაშაულსა და ტერორიზმთან ბრძოლაში. მსგავსად, ე.წ. „დიდი მონაცემები“ (Big Data) – დიდი ოდენობით ინფორმაციის შეგროვება, შენახვა და გაანალიზება ტენდენციების გამოვლენისა და ქცევის წინასწარ განსაზღვრის მიზნით, საზოგადოებისათვის საკმაოდ ღირებულია, აუმჯობესებს პროდუქტიულობას, საჯარო სექტორის მუშაობასა და სოციალურ ჩართულობას.[977]

მიუხედავად არაერთი სარგებლისა, ციფრული ეპოქა გარკვეულ გამოწვევებს ქმნის პირადი ცხოვრებისა და მონაცემების დაცვის კუთხითაც, რადგან გრო-

977 ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი, სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, T-PD(2017)01, სტრასბურგი, 2017 წლის 23 იანვარი.

ვდება დიდი მოცულობის პერსონალური ინფორმაცია, რომელიც სულ უფრო კომპლექსური და გაუმჭვირვალე გზებით მუშავდება. ტექნოლოგიურმა პროგრესმა შექმნა მასობრივი მონაცემები. მათი ჯვარედინი შემოწმება და შემდგომი ანალიზი ტენდენციების გამოსავლენად ან ალგორითმებზე დაფუძნებულ გადაწყვეტილებათა მისაღებად, რომლებიც ადამიანის ქცევასა და პირად ცხოვრებას უპრეცედენტო დონეზე სწავლობს, სულ უფრო მარტივდება.[978]

ახალი ტექნოლოგიები საკმაოდ ძლიერია, საშიშიც კი, თუ არასათანადო ხელში აღმოჩნდება. მათი გამოყენებით სახელმწიფო ორგანოები ახორციელებენ მასობრივ თვალთვალს, რაც ერთ-ერთი მაგალითია, თუ რა მნიშვნელოვანი გავლენა შეიძლება ჰქონდეს ტექნოლოგიას ადამიანის უფლებებზე. 2013 წელს ედვარდ სნოუდენმა გაამჟღავნა ინფორმაცია ინტერნეტისა და სატელეფონო კომუნიკაციების ფართომასშტაბიან თვალთვალზე სადაზვერვო უწყებათა მხრიდან. ამან საზოგადოება დააფიქრა საფრთხეებზე, რომლებსაც თვალთვალი უქმნის პირად ცხოვრებას, დემოკრატიულ მმართველობასა და გამოხატვის თავისუფლებას. მასობრივი თვალთვალი და ტექნოლოგიები, რომლებიც პერსონალური მონაცემების გლობალიზებული შეგროვების, დამუშავებისა და ფართომასშტაბიანი წვდომის შესაძლებლობას იძლევა, საფრთხეს უქმნის პირადი ცხოვრების უფლებას;[979] მან შესაძლოა უარყოფითი გავლენა იქონიოს პოლიტიკურ კულტურაზეც და ჰქონდეს გამყინავი ეფექტი დემოკრატიაზე, კრეატიულობასა და ინოვაციაზე.[980] იმ შიშის გამო, რომ სახელმწიფო შეიძლება მუდმივად მონიტორინგს უწევდეს და აანალიზებდეს მოქალაქეთა ქცევასა და მოქმედებებს, ადამიანებმა შეიძლება შეწყვიტონ საკუთარი მოსაზრებების გამოხატვა გარკვეულ საკითხებზე და სიფრთხილე გამოიჩინონ.[981] ამის გათვალისწინებით, გარკვეულმა საჯარო დაწესებულებებმა, კვლევითმა ცენტრებმა და სამოქალაქო ორგანიზაციებმა გადაწყვიტეს, გაეანალიზებინათ ახალი ტექნოლოგიების პოტენციური გავლენა საზოგადოებაზე. 2015 წელს ევროკავშირის მონაცემთა დაცვის ზედამხედველმა წამოიწყო რამდენიმე ინიციატივა, რომელთა მიზანია, შეაფასოს „დიდი მონაცე-

978 ევროპული პარლამენტი (2017), რეზოლუცია „დიდი მონაცემების“ ფუნდამენტურ უფლებებზე გავლენის შესახებ: პირადი ცხოვრება, მონაცემთა დაცვა, დისკრიმინაციის აღკვეთა, უსაფრთხოება და სამართლის დაცვა. (P8_TA-PROV(2017)0076, სტრასბურგი, 2017 წლის 14 მარტი.

979 იხ. გაერო, გენერალური ასამბლეა, სპეციალური მომხსენებლის ანგარიში ტერორიზმთან ბრძოლისას ადამიანის უფლებებისა და ფუნდამენტური თავისუფლებების ხელშეწყობისა და დაცვის შესახებ, ბენ ემერსონი, A/69/397, 2014 წლის 23 სექტემბერი, პუნქტი 59. ასევე, იხ. ECtHR, ფაქტობრივი მონაცემები მასობრივი თვალთვალის შესახებ, 2017 წლის ივლისი.

980 EDPS (2015), დიდი მონაცემების გამოწვევების დაძლევა, მოსაზრება 7/2015, ბრიუსელი, 2015 წლის 19 ნოემბერი.

981 იხ. CJEU, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი, პუნქტი 37.

მებისა“ და „ნივთების ინტერნეტის“ (Internet of Things) გავლენა ეთიკაზე. აღსანიშნავია, რომ ევროკავშირის მონაცემთა დაცვის ხელმძღვანელმა შექმნა ეთიკის საკონსულტაციო ჯგუფი. მისი ამოცანაა „ღია და ინფორმირებული დისკუსიის წახალისება ციფრულ ეთიკაზე, რაც ევროკავშირს დაეხმარება იმ სარგებლის გაცნობიერებაში, რომელიც ტექნოლოგიას მოაქვს საზოგადოებისა თუ ეკონომიკისთვის და, ამავდროულად, განამტკიცებს ადამიანის უფლებებსა და თავისუფლებებს, განსაკუთრებით, პირადი ცხოვრებისა და მონაცემთა დაცვის კუთხით.“ [982]

პერსონალური მონაცემების დამუშავება ძლიერი ინსტრუმენტია კორპორაციების ხელში. იგი იძლევა ინფორმაციის მიღების შესაძლებლობას პირის ჯანმრთელობასა ან ფინანსურ მდგომარეობაზე, რასაც შემდგომ კორპორაციები იყენებენ ადამიანების შესახებ მნიშვნელოვანი გადაწყვეტილებების მისაღებად, როგორიცაა სადაზღვევო პრემიის ოდენობა თუ გადახდისუნარიანობის განსაზღვრა. მონაცემთა დამუშავების ტექნიკამ შესაძლოა გავლენა იქონიოს დემოკრატიულ პროცესებზეც, როდესაც მათ პოლიტიკოსები ან კორპორაციები იყენებენ ამომრჩევლებზე გავლენის მოსახდენად (მაგ.: ამომრჩეველთა კომუნიკაციების მიზანში ამოღებით). სხვა სიტყვებით რომ ვთქვათ, თავდაპირველად მიიჩნეოდა, რომ პირადი ცხოვრების ხელშეუხებლობის უფლება გულისხმობდა ადამიანების დაცვას სახელმწიფო ორგანოთა უსაფუძვლო ჩარევისგან, ხოლო თანამედროვე ეპოქაში ამ უფლებას შესაძლოა საფრთხე დაემუქროს კერძო აქტორების მხრიდანაც. ეს წარმოშობს გარკვეულ კითხვებს ტექნოლოგიისა და პროგნოზული ანალიზის გამოყენებასთან დაკავშირებით, ისეთი გადაწყვეტილებების მისაღებად, რომლებიც გავლენას ახდენს ადამიანთა ყოველდღიურ ცხოვრებაზე და განამტკიცებს ფუნდამენტური უფლებების დაცვის მნიშვნელობას პერსონალური მონაცემების დამუშავებისას.

მონაცემთა დაცვა მჭიდროდ უკავშირდება ტექნოლოგიურ, სოციალურ და პოლიტიკურ ცვლილებებს. შესაბამისად, შეუძლებელია სამომავლო გამოწვევების სრული ჩამონათვალის განსაზღვრა. წინამდებარე თავი განიხილავს გარკვეულ საკითხებს ისეთ თემებთან დაკავშირებით, როგორიცაა „დიდი მონაცემები“, ინტერნეტში არსებული სოციალური ქსელები და ევროკავშირის ერთიანი ციფრული ბაზარი. ეს ანალიზი არ არის ამომწურავი მონაცემთა დაცვის კონტექსტში, თუმცა მიმოხილულია შესაძლო ინტერაქციების ფართო სპექტრი ადამიანების ახალ ანუ მოდერნიზებულ აქტივობებსა და მონაცემთა დაცვას შორის.

982 EDPS, 2015 წლის 3 დეკემბრის გადაწყვეტილება, რომელიც შეეხება გარე საკონსულტაციო ჯგუფის შექმნას მონაცემთა დაცვის ეთიკური განზომილებების შესახებ (ეთიკის საკონსულტაციო ჯგუფი), 2015 წლის 3 დეკემბერი, პრეამბულა, პუნქტი 5.

10.1 „დიდი მონაცემები“, ალგორითმები და ხელოვნური ინტელექტი

ძირითადი საკითხები

- ინოვაციები საინფორმაციო/საკომუნიკაციო ტექნოლოგიების სფეროში ცხოვრების ახალ სტილს ქმნის, სადაც სოციალური ურთიერთობები, მეწარმეობა, კერძო და საჯარო სერვისები ციფრულად ერთმანეთთან არის დაკავშირებული და სულ უფრო მეტი მონაცემების გენერირებას ახდენს. მათი დიდი ნაწილი პერსონალური მონაცემია.
- მთავრობებს, საწარმოებსა და მოქალაქეებს სულ უფრო ხშირად უწევთ მონაცემებით მართულ ეკონომიკაში მუშაობა, სადაც თვითონ მონაცემები იქცა ფასიან აქტივებად.
- „დიდი მონაცემების“ კონცეფცია გულისხმობს როგორც მონაცემებს, ისე მათ ანალიზს.
- პერსონალური მონაცემები, რომლებიც მუშავდება „დიდი მონაცემების“ ანალიზის ფარგლებში, რეგულირდება ევროკავშირისა და ევროპის საბჭოს კანონმდებლობით.
- მონაცემთა დაცვის წესებსა ან უფლებებთან დაკავშირებული გამონაკლისები მხოლოდ გარკვეულ სიტუაციებს ეხება, როდესაც უფლებით სარგებლობა შეუძლებელია, ან საჭიროებს მონაცემთა დამმუშავებლის არაპროპორციულ ძალისხმევას.
- გადაწყვეტილებების მხოლოდ ავტომატური საშუალებებით მიღება ზოგადად აკრძალულია, გარდა გარკვეული გამონაკლისი შემთხვევებისა.
- უფლებათა რეალიზების კუთხით, დიდი მნიშვნელობა ენიჭება მონაცემთა სუბიექტების ცნობიერების ამაღლებას და მათი მხრიდან კონტროლის შესაძლებლობას.

დღევანდელ სამყაროში, რომელიც სულ უფრო დამოკიდებული ხდება ციფრულ ტექნოლოგიებზე, ნებისმიერი აქტივობა ტოვებს ციფრულ კვალს, რომლის შეგროვება, დამუშავება, შეფასება თუ ანალიზი შესაძლებელია. ახალი საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარებასთან ერთად, კიდევ უფრო მეტი მონაცემი გროვდება და აღირიცხება.[983] ტექნო-

983 ევროკომისიის მიმართვა ევროპულ პარლამენტს, საბჭოს, ეკონომიკურ და სოციალურ კომიტეტს და რეგიონების კომიტეტს, მონაცემთა სწრაფად განვითარებადი ეკონომიკის შესახებ, COM(2014) 442, საბოლოო, ბრიუსელი, 2014 წლის 2 ივლისი.

ლოგია, რომელიც იძლევა მასობრივი მონაცემების ანალიზის, შეფასებისა და სასარგებლო დასკვნების გაკეთების შესაძლებლობას, მხოლოდ ცოტა ხნის წინათ გაჩნდა. მანამდე მონაცემების შეფასება ტენდენციებისა და ჩვევების გამოსავლენად შეუძლებელი იყო მათი დიდი მოცულობის, კომპლექსურობის, არაეფექტური სტრუქტურისა და სწრაფი მიმოცვლის გამო.

10.1.1 „დიდი მონაცემების“, ალგორითმებისა და ხელოვნური ინტელექტის განმარტება

დიდი მონაცემები

ტერმინი „დიდი მონაცემები“ საკმაოდ პოპულარულია და, კონტექსტის მიხედვით, შესაძლოა რამდენიმე მნიშვნელობა ჰქონდეს. როგორც წესი, იგი გულისხმობს „მზარდ ტექნოლოგიურ შესაძლებლობას, რომელიც უკავშირდება ახალი და პროგნოზული ცოდნის შეგროვებას, დამუშავებას და ამოღებას დიდი ოდენობისა თუ მოცულობის და ფართო სპექტრის მონაცემებიდან.“[984] ამგვარად, „დიდი მონაცემების“ კონცეფცია გულისხმობს როგორც თავად მონაცემებს, ისე მათ დამუშავებას.

მონაცემთა წყაროები სხვადასხვაგვარია და მოიცავს ადამიანებს, მათ პერსონალურ მონაცემებს, დანადგარებსა თუ სენსორებს, კლიმატის შესახებ ინფორმაციას, სატელიტურ გამოსახულებებს, ციფრულ სურათებსა და ვიდეოებს, ან GPS სიგნალებს. თუმცა, ამ ინფორმაციის დიდი ნაწილი პერსონალურ მონაცემებს განეკუთვნება (სახელი, ფოტო, ელფოსტის მისამართი, საბანკო რეკვიზიტები, GPS-ის საშუალებით მიღებული მონაცემები, სოციალურ ქსელებში გამოქვეყნებული პოსტები, სამედიცინო ინფორმაცია ან კომპიუტერის IP მისამართი).[985]

დიდი მონაცემები გულისხმობს მასობრივი მონაცემებისა და ხელმისაწვდომი ინფორმაციის ანალიზსა და შეფასებას - სასარგებლო ინფორმაციის მოპო-

984 სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, T-PD(2017)01, სტრასბურგი, 2017 წლის 23 იანვარი, გვ. 2; ევროპული კომისიის მიმართვა ევროპულ პარლამენტს, საბჭოს, ეკონომიკურ და სოციალურ კომიტეტს და რეგიონების კომიტეტს, მონაცემთა სწრაფად განვითარებადი ეკონომიკის შესახებ, COM(2014) 442, საბოლოო, ბრიუსელი, 2014 წლის 2 ივლისი, გვ. 4; საერთაშორისო სატელეკომუნიკაციო კავშირი (2015), რეკომენდაცია Y.3600 „დიდი მონაცემების“ შესახებ.

985 ევროკომისია, ფაქტობრივი მონაცემები ევროკავშირის მონაცემთა დაცვის რეფორმისა და „დიდი მონაცემების“ შესახებ; ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტის სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, T-PD(2017)01, სტრასბურგი, 2017 წლის 23 იანვარი, გვ.2.

ვებას დიდი მონაცემების გასაანალიზებლად. ეს ნიშნავს, რომ შეგროვებული მონაცემებისა და ინფორმაციის გამოყენება შესაძლებელია თავდაპირველი მიზნისგან განსხვავებული ამოცანებით (მაგ.: სტატისტიკური ტენდენციები, ან სამიზნე აუდიტორიაზე მორგებული სერვისები, როგორიცაა რეკლამა). მეტიც, „დიდი მონაცემების“ შეგროვების, დამუშავებისა და შეფასებისთვის საჭირო ტექნოლოგიების პირობებში, შესაძლებელია ნებისმიერი ინფორმაციის კომბინირება/გაერთიანება და ხელახლა შეფასება: ფინანსური ტრანზაქციები, გადახდისუნარიანობა, სამედიცინო მკურნალობა, პირადი მოხმარება, პროფესიული საქმიანობა, ადგილმდებარეობა და მარშრუტები, ინტერნეტის გამოყენება, ელექტრონული ბარათები და სმარტფონები, ვიდეოთვალთვალი ან კომუნიკაციაზე მონიტორინგი. „დიდი მონაცემების“ ანალიზი მათ ახალ რაოდენობრივ განზომილებას სძენს, რომლის შეფასება და რეალურ დროში გამოყენებაც შესაძლებელია (მაგ.: მომხმარებელზე მორგებული სერვისების მისაწოდებლად).

ალგორითმები და ხელოვნური ინტელექტი

ხელოვნური ინტელექტი (AI) გულისხმობს კომპიუტერული მანქანების ინტელექტს, რომლებიც „ჭკვიანი აგენტებივით“ იქცევიან. ნებისმიერ კომპიუტერულ მანქანას, რომელსაც შესაბამისი პროგრამა აქვს, შეუძლია თავისი გარემოს აღქმა და ალგორითმების საფუძველზე მოქმედება. ტერმინი AI გამოიყენება მაშინ, როდესაც კომპიუტერული მანქანა მიმართავს „კოგნიტური“ ფუნქციების იმიტაციას (მაგ.: სწავლა და პრობლემების გადაჭრა, რაც, ძირითადად ფიზიკურ პირებს ახასიათებთ).[986] გადაწყვეტილების მიღების იმიტაციისათვის, თანამედროვე ტექნოლოგიები და კომპიუტერული პროგრამები იყენებენ ალგორითმებს, რომელთა საფუძველზეც კომპიუტერული მანქანები „ავტომატურ გადაწყვეტილებებს“ იღებენ. ალგორითმი არის გამოთვლის, მონაცემთა დამუშავების, შეფასების, ავტომატური მსჯელობისა და გადაწყვეტილების მიღების ეტაპობრივი პროცედურა.

მსგავსად „დიდი მონაცემების“ ანალიზისას, ხელოვნური ინტელექტი და მის საფუძველზე შექმნილი ავტომატური გადაწყვეტილებები საჭიროებს დიდი ოდენობით მონაცემების შეგროვებასა და დამუშავებას. მონაცემების წყარო შეიძლება იყოს თავად მოწყობილობა (მუხრუჭების გადახურება, საწვავის დონე და ა.შ.) ან გარემო (მაგ.: პროფილირება ეყრდნობა ავტომატური გადაწყვეტილების მიღებას, წინასწარ განსაზღვრული ტენდენციებისა და ფაქტორების შესაბამისად).

986 Stuart Russel and Peter Norvig, Artificial Intelligence: A Modern Approach (2nd ed.), 2003, Upper Saddle River, New Jersey: Prentice Hall, pp. 27, 32–58, 968–972; Stuart Russel and Peter Norvig, Artificial Intelligence: A Modern Approach (3rd ed.), 2009, Upper Saddle River, New Jersey: Prentice Hall, p. 2.

მაგალითი: პროფილირება და მიზანმიმართული რეკლამა

პროფილირება ეფუძნება „დიდ მონაცემებს“ და გულისხმობს იმ ტენდენციების გამოვლენას, რომლებიც „პიროვნულ ნიშან-თვისებებს“ ასახავს (მაგ.: ინტერნეტით ყიდვისას კომპანიები, ვირტუალურ კალათაში განთავსებული პროდუქციის მიხედვით, ხშირად, მომხმარებლებს სთავაზობენ პროდუქციას, რომელიც მათ „ასევე დააინტერესებთ“). რაც მეტია მონაცემები, მით უფრო ნათელია სურათი მომხმარებლის შესახებ. მაგალითისათვის, სმარტფონები მომხმარებელზე ინფორმაციის მიღების მნიშვნელოვანი წყაროა.

თანამედროვე ფსიქოგრაფია (მეცნიერება, რომელიც ადამიანის პიროვნულ მახასიათებლებს შეისწავლის) იყენებს OCEAN-ის მეთოდს, რომლის საფუძველზეც განისაზღვრება ადამიანების სხვადასხვა ტიპი. ამ მეთოდის მიხედვით, პიროვნულ მახასიათებელთა 5 ძირითად განზომილებაში („დიდი ხუთეული“) ერთიანდება: ღიაობა (რამდენად ღიაა ადამიანი სიახლის მიმართ), პატიოსნება, ექსტრავერტულობა (რამდენად კომუნიკაბელურია პირი), თანხმობისთვის მზაობა და ნეიროტიზმი (რამდენად მოწყვლადია ის). ამ ინფორმაციის საფუძველზე ხდება პიროვნების პროფილირება; განისაზღვრება, რა სჭირდება და რისი ეშინია მას; როგორ მოიქცევა იგი კონკრეტულ სიტუაციაში და ა.შ. ეს მონაცემები ივსება დამატებითი ინფორმაციით პიროვნების შესახებ, რომელიც სხვა წყაროებიდან მოიპოვება, როგორიცაა: მონაცემთა ბროკერები, სოციალური ქსელები (მათ შორის, მოწონებული პოსტები და გამოქვეყნებული ფოტოები), ინტერნეტში მოსმენილი მუსიკა, GPS და მონაცემებზე მონიტორინგი.

შემდგომ, იმ პროფილების შედარების საფუძველზე, რომლებიც შექმნილია „დიდი მონაცემების“ანალიზის ტექნიკით, ვლინდება ერთნაირი ტენდენციები და დგება პიროვნულ მახასიათებელთა „კლასტერები“ (კატეგორიები). მიღებული კლასტერული მონაცემების „შებრუნებით“ და ქცევასა თუ დამოკიდებულებებზე მონაცემების გამოყენებით, განისაზღვრება კონკრეტული პირის პიროვნული მახასიათებლები. შეგროვებული მონაცემების საფუძველზე, რომლებიც მოიცავს ინფორმაციას სოციალურ ქსელში მოწონებული პოსტების, მოსმენილი მუსიკისა თუ ნანახი ფილმების შესახებ, იქმნება მკაფიო სურათი კონკრეტული პირის პიროვნულ მახასიათებლებზე. ეს ბიზნესებს საშუალებას აძლევს, თავიანთი რეკლამა და/ან ინფორმაცია მოარგონ ადამიანთა კონკრეტულ კატეგორიებს. და რაც ყველაზე მნიშვნელოვანია, ამ მონაცემების დამუშავება შესაძლებელია რეალურ დროში.[987]

987 დამუშავების ტექნოლოგიები და ახალი კომპიუტერული პროგრამები რეალურ დროში აანალიზებს ინფორმაციას, თუ რა მოსწონს პიროვნებას, რას ყიდულობს ან ამატებს საყიდლების ვირტუალურ კალათაში, და სთავაზობს „პროდუქტებს“, რომლებიც, შეგროვებულ ინფორმაციაზე დაყრდნობით, დააინტერესებს პირს.

10.1.2 „დიდი მონაცემების“ სარგებლისა და რისკების დაბალანსება

დამუშავების თანამედროვე ტექნოლოგიების მეშვეობით, შესაძლებელია: დიდი მოცულობის მონაცემების გამოყენება; ახალი მონაცემების სწრფი იმპორტი და რეალურ დროში დამუშავება მყისიერი რეაგირებისათვის (კომპლექსური მოთხოვნების დროსაც); რამდენიმე და ერთდროული მოთხოვნის დაკმაყოფილება და სხვადასხვა ტიპის მონაცემების ანალიზი (ფოტოები, შეტყობინებები და ციფრები). ამ ტექნოლოგიური ინოვაციების წყალობით შესაძლებელია მასობრივი მონაცემებისა და ინფორმაციის სტრუქტურირება, დამუშავება და შეფასება რეალურ დროში. [988] დიდი მოცულობის მონაცემთა ანალიზი უზრუნველყოფს შედეგებს, რომელთა მიღებაც მცირე ინფორმაციის გაანალიზებით შეუძლებელია. „დიდი მონაცემების“ გამოყენებამ შექმნა ახალი ბიზნესმიმართულებები და მომსახურებები, როგორც მომხმარებლებისთვის, ისე ბიზნესისთვის. 2020 წლამდე, სავარაუდოდ, ევროკავშირის მოქალაქეთა პერსონალური მონაცემების ღირებულება 1 ტრილიონ ევრომდე გაიზრდება.[989] „დიდი მონაცემები“ იძლევა ახალ შესაძლებლობებს, რომლებიც ეფუძნება მასობრივი მონაცემების შეფასებას ახალი სოციალური, ეკონომიკური და სამეცნიერო ინფორმაციის მოსაპოვებლად, რაც სარგებელს მოუტანს როგორც კერძო, ისე საჯარო სექტორს.[990]

„დიდი მონაცემების“ ანალიზის საფუძველზე შესაძლებელია სასარგებლო ინფორმაციის მოპოვება სამეცნიერო და სამედიცინო სფეროებში (მაგ.: ჯანდაცვის, საკვების უვნებლობის, „ჭკვიანი“ სატრანსპორტო სისტემების, ენე-

988 „დიდი მონაცემების“ დასამუშავებლად კომპიუტერული პროგრამის შემუშავება ჯერ კიდევ ადრეულ ფაზაშია. თუმცა, ცოტა ხნის წინათ შეიქმნა პროგრამები მასობრივი მონაცემებისა და ინფორმაციის რეალურ დროში ანალიზისათვის. „დიდი მონაცემების“ სტრუქტურული დამუშავებისა და ანალიზის შესაძლებლობა ქმნის პროფილირებისა და მიზანმიმართული რეკლამის ახალ საშუალებებს. ევროპული კომისიის მიმართვა ევროპულ პარლამენტს, საბჭოს, ევროპულ ეკონომიკურ და სოციალურ კომიტეტს და რეგიონების კომიტეტს, მონაცემთა სწრაფად განვითარებადი ეკონომიკის შესახებ, COM(2014) 442, საბოლოო, ბრიუსელი, 2014 წლის 2 ივლისი; ევროკომისია, ფაქტობრივი მონაცემები ევროკავშირის მონაცემთა დაცვის რეფორმისა და „დიდი მონაცემების“ შესახებ; ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტის სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, 2017 წლის 23 იანვარი, გვ. 2.

989 ევროკომისიის ფაქტობრივი მონაცემები ევროკავშირის მონაცემთა დაცვის რეფორმისა და „დიდი მონაცემების“ შესახებ.

990 მონაცემთა დაცვისა და პირადი ცხოვრების კომისრების საერთაშორისო კონფერენცია (2014); ევროპული კომისიის მიმართვა ევროპულ პარლამენტს, საბჭოს, ეკონომიკურ და სოციალურ კომიტეტს და რეგიონების კომიტეტს, მონაცემთა სწრაფად განვითარებადი ეკონომიკის შესახებ, COM(2014) 442, საბოლოო, ბრიუსელი, 2014 წლის 2 ივლისი, გვ. 2; ევროკავშირის კომისია, ფაქტობრივი მონაცემები ევროკავშირის მონაცემთა დაცვის რეფორმისა და „დიდი მონაცემების“ შესახებ; ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტის სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, 2017 წლის 23 იანვარი, გვ.1.

რგოეფექტურობის ან ურბანული დაგეგმარების სფეროებში). ინფორმაციის რეალურ დროში ანალიზი გამოიყენება დანერგილი სისტემების გასაუმჯობესებლად. კვლევის დროს ახალი ინფორმაციის მოპოვება შესაძლებელია დიდი ოდენობის მონაცემისა და სტატისტიკური შეფასებების შეჯერებით, განსაკუთრებით, ისეთ სფეროებში, სადაც მონაცემებს მხოლოდ არაავტომატური საშუალებებით აფასებდნენ. მასობრივი ინფორმაციის ანალიზზე დაყრდნობით, შესაძლებელია მკურნალობის ახალი გზების შემუშავება, რომლებიც მოერგება კონკრეტული პაციენტების საჭიროებებს. კომპანიები იმედოვნებენ, რომ „დიდი მონაცემების“ ანალიზი საშუალებას მისცემთ, მოიპოვონ კონკურენტული უპირატესობა, დაზოგონ თანხები და შექმნან ახალი ბიზნესსფეროები, პირდაპირი და ინდივიდუალური მომსახურების შეთავაზებით; სახელმწიფო უწყებები კი ფიქრობენ, რომ „დიდი მონაცემების“ ანალიზით შეძლებენ სისხლის სამართლის მართლმსაჯულებაში არსებული სიტუაციის გაუმჯობესებას. ევროპის ერთიანი ციფრული ბაზრის სტრატეგია მონაცემებით მართულ ტექნოლოგიებსა თუ სერვისებს და „დიდ მონაცემებს“ მიიჩნევს ევროკავშირში ეკონომიკური ზრდის, ინოვაციისა და ციფრულ ტექნოლოგიებზე გადასვლის კატალიზატორად.[991]

ამავდროულად, „დიდი მონაცემები“ შეიცავს რისკებსაც, რომლებიც უკავშირდება მის 3 ძირითად მახასიათებელს (three Vs): მოცულობა, სიჩქარე და მრავალფეროვნება. მოცულობა გულისხმობს დასამუშავებელი მონაცემების რაოდენობას, მრავალფეროვნება მიუთითებს განსხვავებული ტიპის მონაცემთა არსებობაზე, ხოლო სიჩქარე აღნიშნავს მონაცემთა დამუშავების სისწრაფეს. მონაცემთა დაცვასთან დაკავშირებული საკითხები წარმოიშობა ისეთ შემთხვევებში, როდესაც „დიდი მონაცემები“ გამოიყენება ადამიანებსა და/ან მათ ჯგუფებზე გადაწყვეტილებების მისაღებად.[992] „დიდი მონაცემების“ ჭრილში არსებულ რისკებს, რომლებიც პირადი მონაცემებისა და ცხოვრების დაცვას უკავშირდება, მიმოიხილავს EDPS-ისა და 29-ე სამუშაო ჯგუფის მოსაზრებები, ევროპული პარლამენტის რეზოლუციები და ევროპის საბჭოს პოლიტიკის დოკუმენტები.[993]

---

991 ევროპული პარლამენტის 2017 წლის 14 მარტის რეზოლუცია „დიდი მონაცემების“ ფუნდამენტურ უფლებებზე გავლენის შესახებ: პირადი ცხოვრება, მონაცემთა დაცვა, დისკრიმინაციის აღკვეთა, უსაფრთხოება და სამართლის დაცვა (2016/2225 (INI)).

992 ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი, სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკურიპირებისდაცვისშესახებ,T-PD(2017)01,სტრასბურგი,2017წლის23იანვარი,გვ.2.

993 იხ: EDPS (2015), დიდი მონაცემების გამოწვევების დაძლევა, მოსაზრება 7/2015, 2015 წლის 19 ნოემბერი; EDPS (2016), „დიდი მონაცემების ეპოქაში ფუნდამენტური უფლებების თანმიმდევრული აღსრულება“, 8/2016, 2016 წლის 23 სექტემბერი; ევროპული პარლამენტი (2016), ევროპული პარლამენტის 2017 წლის 14 მარტის რეზოლუცია „დიდი მონაცემების“ ფუნდამენტურ უფლებებზე გავლენის შესახებ: პირადი ცხოვრება, მონაცემთა დაცვა, დისკრიმინაციის აღკვეთა, უსაფრთხოება და სამართლის დაცვა, P8_TA(2017)0076, სტრასბურგი, 2017 წლის 14 მარტი; ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი, სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, T-PD(2017)01, სტრასბურგი, 2017 წლის 23 იანვარი.

აღნიშნული რისკები მოიცავს „დიდი მონაცემების“ ბოროტად გამოყენებას მათ მიერ, ვისაც მასობრივ ინფორმაციაზე მიუწვდება ხელი, მანიპულაციის, დისკრიმინაციის, ან კონკრეტული ადამიანებისა თუ მათი ჯგუფების შევიწროებით.[994] პიროვნებაზე პერსონალური მონაცემების ან ინფორმაციის შეგროვების, დამუშავებისა და შეფასების დროს, ამ მონაცემების/ინფორმაციის გამოყენებამ შეიძლება დაარღვიოს ფუნდამენტური უფლებები და თავისუფლებები, რაც პირადი ცხოვრების ხელშეუხებლობის უფლების მასშტაბებს სცდება. იმის „გაზომვა“, თუ რა გავლენა ექნება „დიდი მონაცემების“ გამოყენებას პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვის უფლებებზე, შეუძლებელია. ევროპული პარლამენტის თანახმად, არ არსებობს მეთოდოლოგია, რომელიც მტკიცებულებაზე დაყრდნობით შეაფასებს „დიდი მონაცემების“ ზემოქმედებას მთლიანობაში, თუმცა, მოპოვებულ მტკიცებულებებზე დაყრდნობით, „დიდი მონაცემების“ ანალიზს მნიშვნელოვანი ჰორიზონტალური გავლენა აქვს როგორც კერძო, ისე საჯარო სექტორზე.[995]

მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად, ფიზიკურ პირებს უფლება აქვთ, მათზე გადაწყვეტილებები არ მიიღონ ავტომატური საშუალებებით, მათ შორის, პროფილირებით.[996] პირადი ცხოვრების ხელშეუხებლობის დაცვის საკითხი წარმოიშობა მაშინ, როცა მონაცემების დამუშავების შეწყვეტის მოთხოვნა საჭიროებს ადამიანური რესურსის ჩარევას, მონაცემთა სუბიექტისთვის მოსაზრების გამოხატვისა და გადაწყვეტილების გასაჩივრების შესაძლებლობის მიცემას.[997] ეს საფრთხეს უქმნის პერსონალური მონაცემების სათანადო დაცვას, როცა, მაგალითად, ადამიანური რესურსის ჩარევა შეუძლებელია, ანდა გამოყენებულ ალგორითმებს კომპლექსური სახე აქვს, მონაცემების მოცულობა კი იმდენად დიდია, რომ ვერ ხერხდება კონკრეტული გადაწყვეტილების დასაბუთება და/ან მონაცემთა სუბიექტის წინასწარ ინფორმირება თანხმობის მისაღებად. ხელოვნური ინტელექტისა და ავტომატური გადაწყვეტილების მაგალითია იპოთეკურ სესხებზე განაცხადების განხილვა. განაცხადები უარყოფილია, თუ განმცხადებელი ვერ აკმაყოფილებს წინასწარ განსაზღვრულ პარამეტრებსა და ფაქტორებს.

994 მონაცემთა დაცვისა და პირადი ცხოვრების კომისრების საერთაშორისო კონფერენცია (2014), რეზოლუცია დიდი მონაცემების შესახებ.

995 ევროპული პარლამენტი (2016), 2017 წლის 14 მარტის რეზოლუცია „დიდი მონაცემების“ ფუნდამენტურ უფლებებზე გავლენის შესახებ: პირადი ცხოვრება, მონაცემთა დაცვა, დისკრიმინაციის აღკვეთა, უსაფრთხოება და სამართლის დაცვა, სტრასბურგი, 2017 წლის 14 მარტი (2016/2225(INI)).

996 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 22.

997 *იქვე,* მუხლი 22 (3).

10.1.3 მონაცემთა დაცვის ძირითადი პრობლემები

მონაცემთა დაცვის ძირითადი პრობლემები უკავშირდება, ერთი მხრივ, დამუშავებული პერსონალური მონაცემების მოცულობასა და ფართო სპექტრს, ხოლო მეორე მხრივ, დამუშავებასა და მის შედეგებს. კომპლექსური ალგორითმებისა და კომპიუტერული პროგრამების დანერგვა, რათა მასობრივი მონაცემები გარდაიქმნას გადაწყვეტილების მიღების რესურსად, გავლენას ახდენს ადამიანებსა და მათ ჯგუფებზე, განსაკუთრებით, პროფილირებისა და იარლიყების „მიკერებისას“ და, საბოლოო ჯამში, წარმოქმნის მონაცემთა დაცვის პრობლემებს.[998]

მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის პასუხისმგებლობის განსაზღვრა

„დიდი მონაცემები“ და ხელოვნური ინტელექტი გარკვეულ კითხვებს წარმოშობს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის პასუხისმგებლობის კუთხით: ვისი საკუთრებაა დიდი ოდენობით შეგროვებული და დამუშავებული მონაცემები? ვინ ამუშავებს „ჭკვიანი“ კომპიუტერული აპარატურისა და პროგრამების გამოყენებით მოპოვებულ მონაცემებს? რა პასუხისმგებლობა ეკისრება დამუშავების პროცესის თითოეულ მონაწილეს? რა მიზნებით შეიძლება „დიდი მონაცემების“ გამოყენება?

პასუხისმგებლობის საკითხი ხელოვნური ინტელექტის კონტექსტში განსაკუთრებული გამოწვევაა, რადგან ხელოვნური ინტელექტი იღებს გადაწყვეტილებებს, რომლებიც ეფუძნება მის მიერვე დამუშავებულ მონაცემებს. მონაცემთა დაცვის ზოგადი რეგულაცია ადგენს საკანონმდებლო ჩარჩოს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის პასუხისმგებლობასთან დაკავშირებით. პერსონალური მონაცემების უკანონო დამუშავება პასუხისმგებლობას აკისრებს მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს.[999] ხელოვნური ინტელექტი და გადაწყვეტილების ავტომატური საშუალებებით მიღება წარმოშობს კითხვას, თუ ვინ არის პასუხისმგებელი დარღვევებზე, რომლებიც გავლენას ახდენს მონაცემთა სუბიექტების პირადი ცხოვრების უფლებაზე; ხელოვნური ინტელექტისა და ალგორითმის პროდუქტებად მიჩნევა კი აჩენს კითხვებს პერსონალურ და პროდუქტის პასუხისმგებლობებთან დაკავშირებით (პირველი რეგულირდება მონაცემთა დაცვის ზოგადი რეგულაციით, მეორე კი ამ დოკუმენტის ფარგლებში არ ექცევა).[1000] საჭიროა ისეთი წესები, რომლე-

998 ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი, სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, გვ. 2.

999 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 77–79 და 82.

1000 ევროპული პარლამენტი, ევროპული სამოქალაქო კანონის წესები რობოტულ ტექნოლოგიაში, შიდა პოლიტიკის გენერალური დირექტორატი, 2016 წლის ოქტომბერი, გვ.14.

ბიც შეავსებს სიცარიელეს პერსონალურ და პროდუქტის პასუხისმგებლობებს შორის, რობოტიკისა და ხელოვნური ინტელექტის გამოყენების შემთხვევებში, მათ შორის, გადაწყვეტილებათა ავტომატური საშუალებებით მიღებისას.[1001]

გავლენა მონაცემთა დაცვის პრინციპებზე

„დიდი მონაცემების“ ბუნება, ანალიზი და გამოყენება, რომელიც განხილულია ზემოთ, კითხვის ნიშნის ქვეშ აყენებს მონაცემთა დაცვის ევროპული კანონმდებლობის ზოგიერთი ტრადიციული, ფუნდამენტური პრინციპის გამოყენებას.[1002] ეს, ძირითადად, უკავშირდება კანონიერების, მონაცემთა მინიმიზაციის, მიზნის შეზღუდვისა და გამჭვირვალობის პრინციპებს.

მონაცემთა მინიმიზაციის პრინციპის თანახმად, პერსონალური მონაცემები უნდა იყოს შესაბამისი, რელევანტური და მხოლოდ იმ მოცულობის, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნებისთვის. თუმცა, შეიძლება ითქვას, რომ „დიდი მონაცემების“ ბიზნესმოდელი მონაცემთა მინიმიზაციის ანტითეზაა, რადგან მაქსიმალურად დიდი ოდენობით მონაცემს მოითხოვს, ხშირად, დაუზუსტებელი მიზნებით.

იგივე ეხება მიზნის შეზღუდვის პრინციპს, რომლის თანახმადაც მონაცემები უნდა დამუშავდეს კონკრეტული მიზნებისთვის. ამასთან, დაუშვებელია მონაცემთა გამოყენება შეგროვების თავდაპირველ მიზანთან შეუთავსებელი ამოცანებით, გარდა იმ შემთხვევისა, როცა არსებობს შესაბამისი სამართლებრივი საფუძველი (მაგ.: მონაცემთა სუბიექტის თანხმობა) (იხ. ნაწილი 4.1.1).

და ბოლოს, „დიდი მონაცემები“ ეწინააღმდეგება მონაცემთა სიზუსტის პრინციპს, რადგან გულისხმობს მონაცემთა შეგროვებას სხვადასხვა წყაროდან, მათი შემოწმების და/ან დაზუსტების გარეშე.[1003]

კონკრეტული წესები და უფლებები

ზოგადად, პერსონალურ მონაცემებზე, რომლებიც მუშავდება „დიდი მონაცემების“ ანალიზის ფარგლებში, ვრცელდება მონაცემთა დაცვის კანონმდებლო-

1001 რობერტო ვიოლას სიტყვა ევროპულ პარლამენტში გამართულ მედიასემინარზე რობოტიკის ევროპული კანონმდებლობის შესახებ (SPEECH 16/02/2017); ევროპული პარლამენტის განცხადება რობოტიკისა და ხელოვნური ინტელექტის სამოქალაქო პასუხისმგებლობის წესებზე, კომისიის თხოვნის პასუხად.

1002 ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი, სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, T-PD(2017)01, სტრასბურგი, 2017 წლის 23 იანვარი.

1003 „დიდი მონაცემების ეპოქაში ფუნდამენტური უფლებების თანმიმდევრული აღსრულება“, მოსაზრება 8/2016, 2016 წლის 23 სექტემბერ, გვ. 8.

ბა. ამავდროულად, ევროკავშირისა და ევროპის საბჭოს კანონმდებლობები ადგენს კონკრეტული წესებსა და გამონაკლის შემთხვევებს, რომლებიც შეეხება კომპლექსური მონაცემების დამუშავებას ალგორითმების გამოყენებით.

ევროპის საბჭოს კანონმდებლობაში, მოდერნიზებული 108-ე კონვენცია მონაცემთა სუბიექტებს ანიჭებს ახალ უფლებებს, რათა უფრო ეფექტიანად აკონტროლონ თავიანთი პერსონალური ინფორმაცია „დიდი მონაცემების“ ეპოქაში. მაგალითად, მოდერნიზებული კონვენციის მე-9 მუხლის 1 (ა)(გ)(დ) პუნქტის თანახმად, მონაცემთა სუბიექტებს უფლება აქვთ: არ დაექვემდებარონ გადაწყვეტილებას, რომელიც მნიშვნელოვან გავლენას ახდენს მათზე და ეფუძნება მხოლოდ და მხოლოდ ავტომატურ დამუშავებას, მათი მოსაზრებების გაუთვალისწინებლად; მოთხოვნისთანავე მიიღონ ინფორმაცია დამუშავების მიზეზების შესახებ, თუ შედეგები მათზე გავლენას ახდენს; და ისარგებლონ მონაცემთა დამუშავების შეწყვეტის უფლებით. მოდერნიზებული 108-ე კონვენციის სხვა დებულებები, განსაკუთრებით, გამჭვირვალობისა და დამატებითი ვალდებულებების შესახებ, ავსებს კონვენციის მიერ შექმნილ დამ-ცავ მექანიზმებს, რომელთა მიზანია ციფრულ გამოწვევებთან გამკლავება.

ევროკავშირის სამართალში, გარდა GDPR-ის 23-ე მუხლში წარმოდგენილი შემთხვევებისა, გამჭვირვალობის პრინციპი დაცული უნდა იყოს პერსონალური მონაცემების ნებისმიერი დამუშავებისას. ეს პრინციპი განსაკუთრებით მნიშვნელოვანია ინტერნეტმომსახურებისა და მონაცემთა სხვა კომპლექსური ავტომატური დამუშავების კუთხით, როგორიცაა ალგორითმების გამოყენება გადაწყვეტილების მიღებისას. მონაცემთა დამუშავების სისტემის მახასიათებლები მონაცემთა სუბიექტს საშუალებას უნდა აძლევდეს, რეალურად გაიაზროს, რა ემართება მის მონაცემებს. გამჭვირვალე და სამართლიანი დამუშავებისათვის, მონაცემთა დაცვის ზოგადი რეგულაცია დამმუშავებელს ავალდებულებს, რომ მონაცემთა სუბიექტს მიაწოდოს ეფექტიანი ინფორმაცია ავტომატური გადაწყვეტილების მიღებისას გამოყენებულ ლოგიკაზე/კრიტერიუმებზე, პროფილირების ჩათვლით.[1004] ევროპის საბჭოს მინისტრთა კომიტეტი თავის რეკომენდაციაში, რომელიც შეეხება გამოხატვის თავისუფლებისა და პირადი ცხოვრების ხელშეუხებლობის უფლებას, ქსელის ნეიტრალობასთან დაკავშირებით აღნიშნავს, რომ ინტერნეტპროვაიდერებმა „მომხმარებლებს უნდა მიაწოდონ მკაფიო, სრული და საჯაროდ ხელმისაწვდომი ინფორმაცია ტრეფიკის მართვის პრაქტიკაზე, რამაც შესაძლოა გავლენა მოახდინოს კონტენტის, აპლიკაციისა თუ მომსახურების ხელმისაწვდომობასა და გავრცელებაზე მომხმარებელთა მიერ.“[1005] ანგარიშები ინტერნეტ ტრეფიკის მართვის

1004 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 13 (2) (ვ).

1005 ევროპის საბჭო, მინისტრთა კომიტეტი (2016), რეკომენდაცია CM/Rec(2016)1 წევრი სახელმწიფოებისთვის გამოხატვის თავისუფლებისა და პირადი ცხოვრების უფლების დაცვის შესახებ, ქსელის ნეიტრალურობასთან დაკავშირებით, 2016 წლის 13 იანვარი, პუნქტი 5.1.

შესახებ, რომელსაც ყველა წევრ სახელმწიფოში კომპეტენტური ორგანოები ამზადებენ, ღიად და გამჭვირვალედ უნდა მომზადდეს და საჯაროდ და უსასყიდლოდ იყოს ხელმისაწვდომი.[1006]

მაშინაც, როცა მონაცემები პირდაპირ მონაცემთა სუბიექტებისგან არ გროვდება, დამმუშავებელი ვალდებულია, მათ მიაწოდოს ინფორმაცია არა მხოლოდ კონკრეტული მონაცემების შეგროვებასა და დაგეგმილ დამუშავებაზე (იხ. ნაწილი 6.1.1), არამედ, თუ საჭიროა, ავტომატური გადაწყვეტილების პროცესების არსებობაზეც, ასევე, „გამოყენებული ლოგიკის/კრიტერიუმების, საჭიროებასა და იმ შედეგებზე, რომლებიც შეიძლება ჰქონდეს მონაცემთა სუბიექტისთვის.“[1007] როცა პერსონალური მონაცემები არ გროვდება პირდაპირ მონაცემთა სუბიექტისგან, მონაცემთა დაცვის ზოგადი რეგულაცია განმარტავს, რომ დამმუშავებელი არ არის ვალდებული, მონაცემთა სუბიექტს მიაწოდოს ასეთი ინფორმაცია, თუკი ეს „შეუძლებელია ან მოითხოვს არაპროპორციულად დიდ/გაუმართლებელ ძალისხმევას“.[1008] ამავდროულად, 29-ე მუხლის სამუშაო ჯგუფმა სახელმძღვანელო პრინციპებში, რომლებიც შეეხება ავტომატური საშუალებებით ინდივიდუალური გადაწყვეტილებების მიღებასა და პროფილირებას 2016/679 რეგულაციის მიზნებისთვის, აღნიშნა, რომ დამუშავების კომპლექსურობა არ უნდა გამორიცხავდეს დამმუშავებლის მიერ მონაცემთა სუბიექტის მკაფიოდ ინფორმირებას დამუშავების მიზნებსა და გამოყენებულ ანალიზზე.[1009]

საკუთარი მონაცემების წვდომის, შესწორებისა და წაშლის უფლებასა და დამუშავების შეზღუდვის მოთხოვნაზე იგივე გამონაკლისი არ ვრცელდება. თუმცა, დამმუშავებლის მოვალეობა, მონაცემთა სუბიექტს შეატყობინოს მისი პერსონალური მონაცემების შესწორების ან წაშლის შესახებ (იხ. ნაწილი 6.1.4), შესაძლოა გაუქმდეს, თუ „ეს შეუძლებელია, ან მოითხოვს არაპროპორციულად დიდ ძალისხმევას“.[1010]

GDPR-ის 21-ე მუხლის თანახმად, მონაცემთა სუბიექტებს ასევე აქვთ უფლება, მოითხოვონ დამუშავების შეწყვეტა (იხ. ნაწილი 6.1.6), მათ შორის, „დიდი მონაცემების“ ანალიზის შემთხვევაში. დამმუშავებელი ამ ვალდებულებისგან თავისუფლდება, თუ დაამტკიცებს უფრო მნიშვნელოვანი კანონიერი ინტერესების არსებობას. ამავდროულად, პირდაპირ მარკეტინგის მიზნით დამუშავებაზე მსგავსი გამონაკლისი არ ვრცელდება.

1006 *იქვე,* პუნქტი 5.2.

1007 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 13 (2)(ვ) და 14 (2)(ზ).

1008 *იქვე,* მუხლი 14 (5) ბ.

1009 29-ე მუხლის სამუშაო ჯგუფი, სახელმძღვანელო პრინციპები რეგულაციის მიზნებისთვის ინდივიდუალური გადაწყვეტილების ავტომატური მიღებისა და პროფილირების შესახებ, wp251, 2017 წლის 3 ოქტომბერი, გვ.14

1010 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 19.

ამ უფლებებიდან გადახვევა შეიძლება მოითხოვოს დამმუშავებელმა, თუ პერსონალური მონაცემების დამუშავება ემსახურება საჯარო ინტერესს, სამეცნიერო/ისტორიული კვლევის ან სტატისტიკურ მიზნებს. [1011]

რაც შეეხება პროფილირებას და გადაწყვეტილების მიღებას ავტომატური საშუალებებით, GDPR ადგენს კონკრეტულ წესს. კერძოდ, 22-ე მუხლის პირველი პუნქტის თანახმად, „მონაცემთა სუბიექტებს უფლება აქვთ, მათზე არ მიიღონ მხოლოდ ავტომატიზებული გადაწყვეტილებები - მათ შორის, პროფილირების მეშვეობით - რომლებსაც სამართლებრივი ან სხვა სახის მნიშვნელოვანი შედეგები ექნება ამ პირებისთვის.“ 29-ე მუხლის სამუშაო ჯგუფის სახელმძღვანელო პრინციპებში ხაზგასმით აღნიშნულია, რომ ეს მუხლი ადგენს ზოგად აკრძალვას გადაწყვეტილების მხოლოდ ავტომატური საშუალებებით მიღებაზე.[1012] ეს აკრძალვა შეიძლება არ გავრცელდეს მონაცემთა დამმუშავებელზე, თუ გადაწყვეტილება: 1) აუცილებელია მონაცემთა სუბიექტსა და დამმუშავებელს შორის დადებული ხელშეკრულების შესასრულებლად; 2) ნებადართულია ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით; 3) ეფუძნება მკაფიოდ გამოხატულ თანხმობას.[1013]

ინდივიდუალური კონტროლი

„დიდი მონაცემების“ ანალიზის კომპლექსურობის, ასევე მის გარშემო გამჭვირვალობის ნაკლებობის გამო, შეიძლება გადასახედი გახდეს ინდივიდუალური კონტროლის იდეა. ეს უნდა მოერგოს არსებულ სოციალურ და ტექნოლოგიურ კონტექსტს, ფიზიკურ პირთა ცოდნის მიხედვით. ამრიგად, „დიდი მონაცემების“ კონტექსტში მონაცემთა დაცვა უნდა ითვალისწინებდეს უფრო ფართო კონტროლს მათ გამოყენებაზე. ეს იდეა ინდივიდუალურ კონტროლს გარდაქმნის უფრო კომპლექსურ პროცესად, რომელიც მოიცავს მონაცემთა გამოყენების რისკების მრავლობითი გავლენის შეფასებას.[1014]

„დიდი მონაცემების“ გამოყენების ეფექტიანობა დამოკიდებულია იმაზე, თუ რამდენად კარგად განსაზღვრავს იგი სამიზნე პირთა (მომხმარებელთა) სურვილებსა და ქცევას. სულ უფრო მეტად იხვეწება პროგნოზირების არსებული მოდელები, რომლებიც „დიდი მონაცემების“ გამოყენებას ეფუძნება. ბოლო

1011 *იქვე,* მუხლი 89 (2) (3).

1012 29-ე მუხლის სამუშაო ჯგუფი, სახელმძღვანელო პრინციპები რეგულაციის მიზნებისათვის ინდივიდუალური გადაწყვეტილების ავტომატურად მიღებისა და პროფილირების შესახებ, wp251, 2017 წლის 3 ოქტომბერი, გვ. 9.

1013 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 22 (2).

1014 ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი, სახელმძღვანელო პრინციპები „დიდი მონაცემების“ სამყაროში პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვის შესახებ, T-PD(2017)01, სტრასბურგი, 2017 წლის 23 იანვარი.

პერიოდში, მონაცემების გამოყენების მიზანი იყო არა მხოლოდ პიროვნულ მახასიათებელთა კატეგორიების შექმნა (ე.წ. ქცევები და დამოკიდებულებები), არამედ, პირის ქცევის გაანალიზება მისი ხმის, მოკლე ტექსტური შეტყობინების აკრეფის სიხშირის, ან სხეულის ტემპერატურის საფუძველზე. ამ ინფორმაციის გამოყენება შესაძლებელია რეალურ დროში, „დიდი მონაცემების“ შეფასების შედეგად მიღებული ცოდნის გამოყენებით (მაგ.: პიროვნების გადახდისუნარიანობის შეფასება ბანკის წარმომადგენელთან გამართული შეხვედრისას). შეფასება ეფუძნება არა პირის ღირსებებს, რომელმაც ბანკს სესხზე განაცხადით მიმართა, არამედ, ქცევით მახასიათებლებს, მიღებულს „დიდი მონაცემების“ ანალიზისა და შეფასების შედეგად (მაგ.: როგორია განმცხადებლის ხმის ტემბრი თუ სხეულის ტემპერატურა, ან როგორ იყენებს ჟესტების ენას).

პროფილირება და მიზანმიმართული რეკლამა პრობლემას არ ქმნის, თუ სამიზნე აუდიტორიისათვის ცნობილია, რომ რეკლამა მორგებულია მათ საჭიროებებზე. პროფილირება პრობლემად იქცევა მაშინ, როდესაც გამოიყენება ადამიანთა მანიპულირებისთვის, ანუ გარკვეული კატეგორიის ადამიანთა მოსაძებნად პოლიტიკური კამპანიისთვის. მაგალითად, პოლიტიკურმა პარტიამ ამომრჩეველთა ჯგუფთან, რომელსაც გადაწყვეტილება ჯერ არ მიუღია, შეიძლება გამოიყენოს მათ „პიროვნულ თვისებებსა“ და დამოკიდებულებებზე მორგებული პოლიტიკური გზავნილები. კიდევ ერთი პრობლემაა პროფილირების გამოყენება გარკვეული პირებისთვის საქონელსა და სერვისებზე წვდომის შესაზღუდად. „დიდი მონაცემებისა“ და პერსონალური ინფორმაციის ბოროტად გამოყენების თავიდან აცილება შესაძლებელია ფსევდონიმიზაციის გზით (იხ. ნაწილი 2.1.1).[1015] შემთხვევები, სადაც პერსონალური მონაცემები რეალურად ანონიმიზებულია - ანუ არ არსებობს ინფორმაცია, რომელიც ტოვებს მონაცემთა სუბიექტთან დაკავშირებულ კვალს - მონაცემთა დაცვის ზოგადი რეგულაციის ფარგლებს გარეთ ხვდება. „დიდი მონაცემების“ დამუშავებაში მონაცემთა სუბიექტისა და ფიზიკური პირის თანხმობა გამოწვევაა მონაცემთა დაცვის კანონმდებლობისთვის. ეს მოიცავს პირის თანხმობას მის საჭიროებებს მორგებულ რეკლამასა და პროფილირებაზე (რაც ხორციელდება „მომხმარებელთან კომუნიკაციის“ მიზნით), ასევე, მასობრივი პერსონალური მონაცემების გამოყენებაზე, ინფორმაციას დაფუძნებული ანალიტიკური ინსტრუმენტების სრულყოფისა და შემუშავებისთვის. „დიდი მონაცემების“ დამუშავების შესახებ ინფორმირებულობა ან მისი ნაკლებობა წარმოშობს კითხვებს მონაცემთა სუბიექტების მიერ უფლებებით სარგებლობაზე, იმის გათვალისწინებით, რომ „დიდი მონაცემების“ დამუშავება ეყრდნობა მხოლოდ ალგორითმებს დაქვემდებარებულ ფსევდონიმიზებულ და ანონიმიზებულ ინფორმაციას. ფსევდონიმიზებული მონაცემები მონაცემთა დაცვის ზოგადი რეგულაციის მოქმედების სფეროში ხვდება, ანონიმიზებული მონაცემები კი მის ფარგლებში არ ექცევა. „დიდი მონაცემების“ ანალიზში განსაკუთრებული

1015 *იქვე,* გვ. 2.

მნიშვნელობა ენიჭება ინდივიდუალურ კონტროლსა და ინფორმირებულობას პერსონალური მონაცემების დამუშავებაზე. წინააღმდეგ შემთხვევაში, მონაცემთა სუბიექტებს არ ეცოდინებათ, ვინ არის დამმუშავებელი ან უფლებამოსილი პირი, რაც მათ ართმევს თავიანთი უფლებებით ეფექტიანად სარგებლობის შესაძლებლობას.

10.2 web 2.0 და 3.0: სოციალური ქსელები და ნივთების ინტერნეტი

ძირითადი საკითხები

- სოციალური ქსელები ონლაინ კომუნიკაციის პლატფორმებია, სადაც ადამიანები რეგისტრირდებიან ან ქმნიან თანამოაზრეთა ქსელებს.
- „ნივთების ინტერნეტი“ გულისხმობს ნივთების კავშირს ინტერნეტსა და ერთმანეთთან.
- სოციალურ ქსელებში პერსონალურ მონაცემთა დამუშავების ყველაზე გავრცელებული სამართლებრივი საფუძველია მონაცემთა სუბიექტის თანხმობა.
- სოციალური ქსელების მომხმარებლებზე, ზოგადად, ვრცელდება „გამონაკლისი, რომელიც უკავშირდება პერსონალური მონაცემების დამუშავებას ოჯახური საქმიანობის ფარგლებში;“ ამავდროულად, ასეთი გამონაკლისები კონკრეტულ კონტექსტში არ დაიშვება.
- სოციალური ქსელების პროვაიდერებზე არ ვრცელდება „ოჯახური საქმიანობის ფარგლებში დამუშავებასთან დაკავშირებული გამონაკლისი“.
- ამ სფეროში მონაცემთა უსაფრთხოების დასაცავად, დიდი მნიშვნელობა ენიჭება მონაცემთა დაცვის სტანდარტების გათვალისწინებას ახალი პროდუქტის ან მომსახურების შექმნისას (by Design) და მონაცემთა დაცვას პირველად პარამეტრად (by Default).

10.2.1 Web 2.0 და 3.0-ის განმარტება

სოციალური ქსელები

თავდაპირველად, ინტერნეტი შეიქმნა კომპიუტერების ერთმანეთთან დასაკავშირებლად და მონაცემთა გაცვლის მიზნით მოკლე ტექსტური შეტყობინებების გასაგზავნად. ვებგვერდები მომხმარებლებს მხოლოდ კონტენტის პასიუ-

რად ნახვის შესაძლებლობას აძლევდნენ.[1016] web 2.0-ის ეპოქაში, ინტერნეტი გარდაიქმნა ფორუმად, სადაც მომხმარებლებს შეეძლოთ ერთმანეთთან ინტერაქცია, თანამშრომლობა და შინაარსის/ინფორმაციის შექმნა, ასევე, კოლაბორაცია. ეს ეპოქა ხასიათდებოდა მნიშვნელოვანი წარმატებითა და სოციალური ქსელების ფართო გამოყენებით, რაც ახლა მილიონობით ადამიანის ყოველდღიური ცხოვრების ნაწილია.

სოციალური ქსელები ანუ „სოციალური მედია“ შეიძლება ფართოდ განისაზღვროს, როგორც „ონლაინ კომუნიკაციის პლატფორმები, სადაც ადამიანები რეგისტრირდებიან ან ქმნიან თანამოაზრეთა ქსელებს“.[1017] ქსელში გასაწევრიანებლად ან მის შესაქმნელად, ადამიანებმა უნდა წარმოადგინონ პერსონალური მონაცემები და შექმნან საკუთარი პროფილი. სოციალური ქსელები მომხმარებლებს აძლევს ციფრული „კონტენტის“ გენერირების საშუალებას, რაც შეიძლება მოიცავდეს ფოტოებსა და ვიდეოებს, საგაზეთო ბმულებსა და პერსონალურ პოსტებს საკუთარი მოსაზრებების გამოსახატავად. ონლაინ კომუნიკაციის პლატფორმების საშუალებით, მომხმარებლებს შეუძლიათ ერთმანეთთან ინტერაქცია და კომუნიკაცია. აღსანიშნავია, რომ პოპულარული სოციალური ქსელების უმრავლესობაზე რეგისტრაცია უფასოა. მომხმარებლებს საფასურის გადახდა არ მოეთხოვებათ, სამაგიეროდ, სოციალური ქსელები შემოსავალს იღებენ მიზანმიმართული რეკლამებიდან. რეკლამის განმთავსებლები დიდ სარგებელს ხედავენ სოციალურ ქსელებში ყოველდღიურად გამჟღავნებული პერსონალური მონაცემებისგან. ინფორმაცია მომხმარებელთა ასაკის, სქესის, ადგილმდებარეობისა და ინტერესების შესახებ მათ საშუალებას აძლევს, თავიანთი რეკლამებით „შესაფერის“ ადამიანებს მიწვდნენ.

ევროპის საბჭოს მინისტრთა კომიტეტმა მიიღო რეკომენდაცია, სოციალურ ქსელებთან დაკავშირებით ადამიანის უფლებათა დაცვის შესახებ,[1018] რომელიც, სხვა საკითხებთან ერთად, შეეხება მონაცემთა დაცვას. 2018 წელს მინისტრთა კომიტეტმა მიიღო ამ ტიპის კიდევ ერთი რეკომენდაცია ინტერნეტ შუამავლების როლებსა და პასუხისმგებლობებზე.[1019]

1016 ევროპული კომისია (2016), ევროპაში ნივთების ინტერნეტის განვითარება, SWD(2016) 110, საბოლოო.

1017 29-ე მუხლის სამუშაო ჯგუფი (2009), მოსაზრება 5/2009 ინტერნეტში სოციალური ქსელების გამოყენების შესახებ, WP 163, 2009 წლის 12 ივნისი, გვ. 4.

1018 ევროპის საბჭო, მინისტრთა კომიტეტი, რეკომენდაცია CM/Rec(2012)4 წევრი სახელმწიფოებისთვის სოციალურ ქსელებთან დაკავშირებით ადამიანის უფლებათა დაცვის შესახებ, 2012 წლის 4 აპრილი.

1019 ევროპის საბჭო, მინისტრთა კომიტეტი, რეკომენდაცია CM/Rec(2018)2 წევრი სახელმწიფოებისთვის ინტერნეტშუამავლების უფლება-მოვალეობათა შესახებ, 2018 წლის 7 მარტი.

მაგალითი: ნორა ძალიან ბედნიერია, რადგან პარტნიორმა ხელი სთხოვა. მას სურს, ახალი ამბავი მეგობრებსა და ოჯახის წევრებს გაუზიაროს. შესაბამისად, გადაწყვეტს, სოციალურ ქსელში დაწეროს ემოციური პოსტი თავისი სიხარულის გამოსახატავად, ხოლო ურთიერთობის სტატუსში მიუთითოს „დანიშნული.“ ამის შემდეგ, ნორა თავის პროფილზე ხედავს რეკლამებს საქორწინო კაბებსა და ყვავილების მაღაზიებზე. რატომ ხდება ასე?

Facebook-ზე რეკლამის შექმნისას, საქორწინო კაბებისა და ყვავილების მაღაზიები კონკრეტულ პარამეტრებს ნიშნავენ, რათა შეძლონ ისეთ ადამიანებთან წვდომა, როგორიცაა ნორა. პროფილის თანახმად, ნორა ის ქალია, რომელიც ცოტა ხნის წინათ დაინიშნა და პარიზში ცხოვრობს იმ ადგილთან ახლოს, სადაც რეკლამის განმათავსებელი მაღაზიები მდებარეობს. შესაბამისად, იგი პროფილზე შესვლისთანავე ხედავს რეკლამას.

ნივთების ინტერნეტი

ინტერნეტის განვითარების პროცესში მომდევნო ნაბიჯია „ნივთების ინტერნეტი“ (IoT): web 3.0-ის ეპოქა. IoT-ს საშუალებით, შესაძლებელია ტექნიკის ერთმანეთთან დაკავშირება. IoT ნივთებსა და ადამიანებს ურთიერთკავშირის შესაძლებლობას აძლევს, რათა მათ სხვებს გაუზიარონ ინფორმაცია თავიანთი ან/და მათ გარშემო არსებული მდგომარეობის შესახებ.[1020] IoT და ერთმანეთთან დაკავშირებული მოწყობილობები უკვე რეალობაა. მომდევნო წლებში მოსალოდნელია IoT-ის მასშტაბების მნიშვნელოვნად გაზრდა. შეიქმნება და კიდევ უფრო განვითარდება „ჭკვიანი“ მოწყობილობები, რასაც მოჰყვება „ჭკვიანი“ ქალაქების, სახლებისა და ბიზნესების შექმნა.

მაგალითი: IoT-ს განსაკუთრებული სარგებელი მოაქვს ჯანდაცვის სფეროში. კომპანიებმა უკვე შექმნეს მოწყობილობები, სენსორები და აპლიკაციები, რომლებიც იძლევა პაციენტის ჯანმრთელობაზე მონიტორინგის საშუალებას. სპეციალური უკაბელო მოწყობილობებით უკვე შესაძლებელია მარტოხელა ხანდაზმული ადამიანების ყოველდღიურ რუტინაზე მონიტორინგი. მოწყობილობა საგანგაშო სიგნალს იძლევა, თუ გამოვლინდება რაიმე სერიოზული ცვლილება: მაგალითად, ხანდაზმული ადამიანები ხშირად იყენებენ სენსორს, რომელიც წაქცევის შესახებ სიგნალს გადასცემს. ამ სენსორებს წაქცევის ზუსტი იდენტიფიცირება შეუძლია, რაზეც შეტყობინება ეგზავნება ექიმს ან ოჯახის წევრს.

მაგალითი: ბარსელონა ცნობილი „ჭკვიანი“ ქალაქია. 2012 წლიდან ქალაქში ინოვაციური ტექნოლოგიები დაინერგა, რომელთა მიზანია საზოგადოებრივი ტრანზიტის, ნარჩენების მართვის, პარკინგისა და გარე გა-

1020 ევროპული კომისია (2016), ევროპაში ნივთების ინტერნეტის განვითარება, SWD(2016) 110 final.

ნათების „ჭკვიანი“ სისტემების შექმნა. მაგალითად, ნარჩენების მართვის გასაუმჯობესებლად, ქალაქი „ჭკვიან ურნებს“ იყენებს. ეს იძლევა ნარჩენების ოდენობაზე მონიტორინგის საშუალებას, რაც შეგროვების პროცესის ოპტიმიზაციას განაპირობებს. სავსე ურნები მობილური კომუნიკაციის ქსელით სიგნალებს გადასცემენ ნარჩენების მართვის კომპანიას. კომპანია გეგმავს საუკეთესო მარშრუტს ნარჩენების შესაგროვებლად და სავსე ურნების დასაცლელად.

10.2.2 სარგებლისა და რისკების დაბალანსება

სოციალური ქსელების გაფართოება და წარმატება გასულ ათწლეულში მიუთითებს მათ მნიშვნელოვან სარგებელზე. მაგალითად, მიზანმიმართული რეკლამა (როგორც წარმოდგენილ მაგალითშია განხილული) კომპანიებს აძლევს სასურველ აუდიტორიაზე წვდომისა და სპეციფიკური ბაზრის შეთავაზების საშუალებას. მომხმარებლის ინტერესებზე მორგებული რეკლამები, შეიძლება ითქვას, მომხმარებლის ინტერესებშიც შედის. ამასთან, სოციალური ქსელები და მედია დადებით გავლენას ახდენს საზოგადოებასა და ცვლილებებზე. ისინი მომხმარებლებს სთავაზობენ საინტერესო საკითხებზე კომუნიკაციის, ინტერაქციის, ასევე, ჯგუფებისა და ღონისძიებების შექმნის შესაძლებლობას.

მოსალოდნელია, რომ IoT მნიშვნელოვან სარგებელს მოუტანს ეკონომიკას. იგი ევროკავშირის იმ სტრატეგიის ნაწილია, რომელიც ერთიანი ციფრული ბაზრის შექმნას ისახავს მიზნად. 2020 წლამდე ევროკავშირში სოციალური ქსელების მომხმარებელთა რაოდენობის 6 მილიარდამდე გაზრდას ელიან, რაც მნიშვნელოვან ეკონომიკურ სარგებელს მოიტანს ისეთი გზებით, როგორიცაა ინოვაციური სერვისები და აპლიკაციები, უკეთესი ჯანდაცვა, მომხმარებელთა საჭიროებების უკეთ გააზრება და გაუმჯობესებული ეფექტიანობა.

ამავდროულად, სოციალური მედიის მომხმარებლებზე დიდი ოდენობით პერსონალურ ინფორმაციას აგროვებენ და ამუშავებენ სერვისის ოპერატორები. შესაბამისად, სოციალური ქსელების გაფართოებას გარკვეული პრობლემებიც ახლავს პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვის კუთხით. მათ შეიძლება საფრთხეები შეუქმნან პირად ცხოვრებასა და გამოხატვის თავისუფლებას ისეთი ინსტრუმენტების ნაკლებობით, როგორიცაა: „სამართლებრივი და პროცედურული დაცვის გარანტიები (რამაც შესაძლოა მომხმარებელთა გამორიცხვა გამოიწვიოს); მოზარდებისა და ახალგაზრდების სათანადო დაცვა საზიანო კონტენტისა და ქცევისგან; სხვათა უფლებების პატივისცემა; პირადი ცხოვრების დაცვის ხელშემწყობი სტანდარტული პარამეტრები; პერსონალური მონაცემების შეგროვებისა და დამუშავების მიზნებთან დაკავშირებული გამჭვირვალობა.“ [1021] ევროპის მონაცემთა დაცვის კანონმდებლობამ სცადა რეაგირება პირადი ცხოვრების ხელშეუხებ-

1021 ევროპის საბჭო, რეკომენდაცია Rec(2012)4 წევრი სახელმწიფოებისთვის სოციალურ ქსელებთან დაკავშირებით ადამიანის უფლებათა დაცვის შესახებ, 2012 წლის 4 აპრილი.

ლობის/მონაცემთა დაცვის გამოწვევებზე, რომლებსაც სოციალური მედია ქმნის. სოციალური მედიისა და ქსელური სერვისების კონტექსტში განსაკუთრებული მნიშვნელობა ენიჭება ისეთ პრინციპებს, როგორიცაა თანხმობა, პირადი ცხოვრების ხელშეუხებლობის/მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (by Design) და მონაცემთა დაცვა პირველად პარამეტრად (by Default), ასევე, ფიზიკური პირების უფლებები.

IoT-ის კონტექსტში, დიდი ოდენობით პერსონალური მონაცემები გენერირდება სხვადასხვა ურთიერთდაკავშირებული მოწყობილობიდან, რაც, ასევე, შეიცავს პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის რისკებს. გამჭვირვალობა ევროპის მონაცემთა დაცვის კანონმდებლობის მნიშვნელოვანი ნაწილია, თუმცა, ურთიერთდაკავშირებულ მოწყობილობათა სიმრავლის გამო, ყოველთვის ნათელი არ არის, ვის შეუძლია მონაცემების შეგროვება, წვდომა და გამოყენება IoT-ის მეშვეობით. [1022] ევროკავშირისა და ევროპის საბჭოს კანონმდებლობით, გამჭვირვალობის პრინციპი ადგენს მონაცემთა დამმუშავებლის ვალდებულებას, მკაფიო და მარტივი ენით შეატყობინოს მონაცემთა სუბიექტებს, თუ როგორ გამოიყენება მათი მონაცემები. შესაბამის პირებს მკაფიოდ უნდა განემარტოთ რისკები, წესები, უსაფრთხოების ზომები და უფლებები მათი პერსონალური მონაცემების დამუშავებასთან მიმართებით. IoT-სთან დაკავშირებული მოწყობილობები, ასევე, დამუშავების ოპერაციებისა და მონაცემების სიმრავლე კიდევ ერთი გამოწვევაა მონაცემთა დამუშავებაზე მკაფიო და ინფორმირებული თანხმობის გაცემის კუთხით (თუ ასეთი პროცესი თანხმობას ეფუძნება). ხშირად, ადამიანები ვერ იგებენ ამგვარი დამუშავების ტექნიკურ ასპექტებს, შესაბამისად, გაცემული თანხმობის შედეგებსაც.

პრობლემურია უსაფრთხოების დაცვაც, რადგან ერთმანეთთან დაკავშირებული მოწყობილობები უსაფრთხოების განსაკუთრებულად მაღალი რისკის ქვეშ დგანან. ასეთ მოწყობილობებს უსაფრთხოების სხვადასხვა დონე აქვთ. ისინი ოპერირებენ IT ინფრასტრუქტურის სტანდარტებს მიღმა და შეიძლება არ ჰქონდეთ სათანდო სიმძლავრე და ტევადობა უსაფრთხოების კომპიუტერული პროგრამის განსათავსებლად, ან ისეთი ტექნიკის გამოსაყენებლად, როგორიცაა დაშიფვრა, ფსევდონიმიზაცია ან ანონიმიზაცია მომხმარებელთა პერსონალური ინფორმაციის დაცვის მიზნით.

მაგალითი: გერმანიაში მარეგულირებლებმა გადაწყვიტეს, აეკრძალათ სათამაშოების ინტერნეტთან დაკავშირება, შესაძლო გავლენების გამო ბავშვთა პირადი ცხოვრების ხელშეუხებლობის უფლებაზე. მარეგულირებლებმა მიიჩნიეს, რომ თოჯინა სახელად „კაილა“, რომელიც ინტერნეტთან იყო დაკავშირებული, ფარული თვალთვალის მოწყობილობა გახლდათ. კერძოდ: თოჯინა აუდიო კითხვებს უსვამდა ბავშვებს, რომლებიც

1022 ევროკავშირის მონაცემთა დაცვის ზედამხედველი (2017), ნივთების ინტერნეტის გააზრება.

მისი საშუალებით ერთობოდნენ; უგზავნიდა ციფრულ მოწყობილობაში არსებულ აპლიკაციას, რომელსაც აუდიო ინფორმაცია ტექსტურ ფორმატში გადაჰყავდა და პასუხებს ინტერნეტში ეძებდა; შემდეგ აპლიკაცია პასუხებს უგზავნიდა თოჯინას, რომელიც მათ ახმოვანებდა. თოჯინის საშუალებით, შესაძლებელი იყო ბავშვისა და მის სიახლოვეს მყოფი ზრდასრული ადამიანების კომუნიკაციების ჩაწერა და აპლიკაციისთვის გადაგზავნა. თოჯინის მწარმოებლებს უსაფრთხოების სათანადო ზომები რომ არ მიეღოთ, მისი გამოყენება შესაძლებელი იქნებოდა საუბრებზე მოსმენის მიზნით.

10.2.3 მონაცემთა დაცვის პრობლემები

თანხმობა

ევროპაში პერსონალური მონაცემების დამუშავება კანონიერია მხოლოდ იმ შემთხვევაში, თუ ითვალისწინებს მონაცემთა დაცვის ევროპული კანონმდებლობა. სოციალური ქსელების პროვაიდერებისთვის, ზოგადად, დამუშავების საფუძველი გახლავთ მონაცემთა სუბიექტების თანხმობა, რომელიც უნდა იყოს ნებაყოფლობითი, კონკრეტული, ინფორმირებული და მკაფიო (იხ. ნაწილი 4.1.1). [1023] ნებაყოფლობითი თანხმობა ნიშნავს, რომ მონაცემთა სუბიექტს უნდა შეეძლოს რეალური არჩევანის გაკეთება. თანხმობა კონკრეტული და ინფორმირებულია, როცა გასაგებად, მკაფიოდ და ზუსტად მიუთითებს მონაცემთა დამუშავების მასშტაბზე, მიზნებსა და შედეგებზე. სოციალური მედიის კონტექსტში, არსებობს ეჭვები, თუ რამდენად ნებაყოფლობითი, კონკრეტული და ინფორმირებულია თანხმობა ყველა იმ დამუშავებისთვის, რომლებსაც სოციალური ქსელების ოპერატორები და მესამე პირები ახორციელებენ.

მაგალითი: სოციალურ ქსელში დარეგისტრირების მსურველი, ხშირად, პერსონალური მონაცემების სხვადასხვა სახის დამუშავებას უნდა დათანხმდეს საჭირო განმარტებებისა და ალტერნატიული შესაძლებლობების გარეშე. ქსელში დარეგისტრირებისას მომხმარებელი თანხმობას აცხადებს ქცევითი რეკლამის მიღებაზე. 29-ე მუხლის სამუშაო ჯგუფმა თავის მოსაზრებაში თანხმობის განმარტების შესახებ აღნიშნა: „ზოგიერთი სოციალური ქსელის მნიშვნელობის გათვალისწინებით, მომხმარებელთა გარკვეული კატეგორიები (მაგ.: თინეიჯერები) მზად არიან, დათანხმდნენ ქცევითი რეკლამის მიღებას, რათა თავიდან აიცილონ სოციალური ინტერაქციებიდან ნაწილობრივ გამორიცხვის რისკი. მომხმარებელს უნდა შეეძლოს, ნებაყოფლობითი და კონკრეტული თანხმობის გამოხატვა ქცე-

1023 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლები 4 და 7; მოდერნიზებული 108-ე კონვენცია, მუხლი 5.

ვითი რეკლამის მიღებაზე და ეს არ უნდა განსაზღვრავდეს ამ მომხმარებლის წვდომას სოციალურ ქსელზე.“ [1024]

მონაცემთა დაცვის ზოგადი რეგულაციით, დაუშვებელია 16 წლამდე ასაკის მოზარდების პერსონალური მონაცემების დამუშავება მათი თანხმობის საფუძველზე.[1025] ასეთ შემთხვევაში, თანხმობა უნდა გამოხატოს მშობელმა ან მეურვემ. არასრულწლოვნებს განსაკუთრებული დაცვა სჭირდებათ, რადგან ნაკლები ინფორმაცია აქვთ მონაცემთა დამუშავების რისკებსა და შედეგებზე. ეს უაღრესად მნიშვნელოვანია სოციალური მედიის კონტექსტში, სადაც ბავშვები უფრო მოწყვლადები არიან სოციალური მედიის გამოყენების უარყოფითი შედეგების მიმართ, როგორიცაა კიბერბულინგი, ონლაინადევნება და პერსონალური მონაცემების მითვისება (identity theft).

უსაფრთხოება და პირადი ცხოვრების ხელშეუხებლობის/ მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას *(by Design)* და მონაცემთა დაცვა პირველად პარამეტრად *(by Default)*

პერსონალური მონაცემების დამუშავება შეიცავს უსაფრთხოების რისკებს, ვინაიდან დარღვეულმა უსაფრთხოებამ შეიძლება გამოიწვიოს დამუშავებული მონაცემების შემთხვევითი ან უკანონო განადგურება, დაკარგვა, შეცვლა, არაავტორიზებული წვდომა ან გამჟღავნება. ევროპის მონაცემთა დაცვის კანონმდებლობის თანახმად, დამმუშავებელსა და უფლებამოსილ პირებს მოეთხოვებათ სათანადო ტექნიკური და ორგანიზაციული ღონისძიებების გატარება მონაცემთა დამუშავების ოპერაციებში არაავტორიზებული ჩარევის ასარიდებლად. ეს ვალდებულება ეხებათ სოციალური ქსელების პროვაიდერებსაც, რომლებზეც ვრცელდება მონაცემთა დაცვის ევროპული წესები.

პირადი ცხოვრების ხელშეუხებლობის/მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (by Design) და მონაცემთა დაცვა პირველად პარამეტრად (by Default) მონაცემთა დამმუშავებლებს ავალდებულებს, რომ დაიცვან მათ მიერ შემუშავებული პროდუქტების უსაფრთხოება და ავტომატურად გამოიყენონ პირადი ცხოვრებისა და მონაცემების დაცვის შესაბამისი პარამეტრები. კერძოდ, პირის სოციალურ ქსელში დარეგისტრირებისას, დაუშვებელია, სერვისის მიმწოდებელმა ახალი მომხმარებლის ყველა ინფორმაციაზე წვდომა უზრუნველყოს დანარჩენი მომხმარებლებისთვისაც. ასეთ დროს უნდა არსებობდეს პირადი ცხოვრების

1024 29-ე მუხლის სამუშაო ჯგუფი (2011), მოსაზრება 15/2011 თანხმობის განმარტების შესახებ, WP 187, 2011 წლის 13 ივლისი, გვ. 18.

1025 იხ: მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 8. ევროკავშირის წევრ სახელმწიფოებს უფლება აქვთ, კანონით დაადგინონ უფრო დაბალი ასაკი, რომელიც არ უნდა იყოს 13 წელზე ნაკლები.

ხელშეუხებლობისა და მონაცემთა დაცვის ავტომატური პარამეტრები, რათა მომხმარებელზე ინფორმაცია ხელმისაწვდომი იყოს მხოლოდ მის მიერ არჩეული პირებისთვის. ამ წრის გაფართოება შესაძლებელია მხოლოდ მას შემდეგ, რაც მომხმარებელი თვითონ შეიტანს ცვლილებებს ავტომატურ პარამეტრებში. ზოგჯერ, შესაბამისი ღონისძიებების მიუხედავად, მაინც ირღვევა პერსონალურ მონაცემთა უსაფრთხოება. სერვისის მიმწოდებელი ვალდებულია, მომხმარებლებს გაუგზავნოს შეტყობინება, თუ მომხდარი მათ უფლებებსა და თავისუფლებებს მაღალ რისკს უქმნის.[1026]

პირადი ცხოვრების ხელშეუხებლობის/მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას (by Design) და მონაცემთა დაცვა პირველად პარამეტრად (by Default) განსაკუთრებით მნიშვნელოვანია სოციალური ქსელების კონტექსტში, რადგან არაავტორიზებული წვდომის გარდა, პერსონალური ინფორმაციის სოციალური მედიით გაზიარება დამატებით რისკებსაც ქმნის. ხშირად, ეს ხდება იმის გამო, რომ ადამიანს კარგად არ ესმის, ვის შეიძლება ჰქონდეს წვდომა მის მონაცემებზე და როგორ გამოიყენება ეს ინფორმაცია. სოციალური მედიის აქტიურ მოხმარებასთან ერთად, სულ უფრო იზრდება პერსონალურ მონაცემთა მითვისების (identity theft) შემთხვევები და დაზარალებულთა რაოდენობა.

მაგალითი: პერსონალური მონაცემების მითვისება (identity theft), ვინაობის მოპარვის ფენომენი, გულისხმობს ერთი პირის მიერ მეორის (დაზარალებულის) ინფორმაციის, მონაცემების ან დოკუმენტების მოპოვებას და თავის საკუთრებად გასაღებას, ამ პირის სახელით საქონლისა და სერვისების მისაღებად. მაგალითად, პოლი, რომელსაც სოციალურ ქსელში შექმნილი აქვს პროფილი, მასწავლებელად მუშაობს და თავისი საზოგადოების აქტიური წევრია. იგი საკმაოდ კომუნიკაბელურია და სოციალური ქსელის ანგარიშს, პირადი ცხოვრების ხელშეუხებლობასა და მონაცემთა დაცვის პარამეტრებს დიდ ყურადღებას არ აქცევს. პოლს სოციალურ ქსელში ბევრი მეგობარი ჰყავს, მათ შორის ადამიანები, რომელთაც პირადად არ იცნობს. იგი დიდ სკოლაში მუშაობს და სკოლის ფეხბურთის გუნდს წვრთნის. პოლს ჰგონია, რომ ეს უცნობი ადამიანები მშობლები ან სკოლის მეგობრები არიან. მას პროფილზე განთავსებული აქვს თავისი ელფოსტის მისამართი და დაბადების თარიღი. ამასთან, პოლი რეგულარულად აქვეყნებს თავისი ძაღლის, ტობის სურათებს, რომლებსაც ახლავს წარწერები (მაგ.: „მე და ტობი დილაობით დავრბივართ“ და ასე შემდეგ). პოლი ვერ ხვდება, რომ ერთ-ერთი ყველაზე პოპულარული კითხვა ელფოსტაში შესაღწევად შეეხება შინაური ცხოველის სახელს. პოლის პროფილზე ხელმისაწვდომი ინფორმაციის გამოყენებით, ნიკი ადვილად ახერხებს პოლის ანგარიშების გატეხას.

1026 *იქვე*, მუხლი 34.

ფიზიკურ პირთა უფლებები

სოციალური ქსელის პროვაიდერები ვალდებულნი არიან, პატივი სცენ ფიზიკურ პირთა უფლებებს (იხ. ნაწილი 6.1), მათ შორის, ინფორმირებას დამუშავების მიზანსა და მონაცემთა პირდაპირი მარკეტინგისთვის გამოყენებაზე. ფიზიკურ პირს აქვს უფლება, მოითხოვოს სოციალური ქსელის პლატფორმაზე გენერირებული პერსონალური მონაცემების წვდომა ან წაშლა. მაშინაც კი, როდესაც პირი თანხმობას განაცხადებს პერსონალური მონაცემების დამუშავებაზე და ინფორმაციას ატვირთავს ონლაინ რეჟიმში, უნდა შეეძლოს „დავიწყების“ მოთხოვნა, თუკი სოციალური ქსელის მომსახურება აღარ მოესურვება. მონაცემთა პორტირების უფლება მომხმარებლებს აძლევს საშუალებას, მიიღონ სოციალური ქსელისთვის მიწოდებული პერსონალური მონაცემების ასლი, სტრუქტურირებულ, ჩვეულებრივად გამოყენებულ, ელექტრონულ და პორტირებად ფორმატში, და გადაუგზავნონ სოციალური ქსელის სხვა პროვაიდერს.[1027]

მონაცემთა დამმუშავებელი

სოციალური მედიის კონტექსტში ერთ-ერთი რთული და გავრცელებული საკითხია მონაცემთა დამმუშავებლის განსაზღვრა. კერძოდ, ვინ არის პირი, რომელსაც ეკისრება ვალდებულება და პასუხისმგებლობა მონაცემთა დაცვის წესებთან შესაბამისობაზე. მონაცემთა დაცვის ევროპული კანონმდებლობით, სოციალური ქსელების პროვაიდერები მონაცემთა დამმუშავებლად მიიჩნევიან. ეს აშკარად ჩანს „მონაცემთა დამმუშავებლის“ ცნების ფართო განმარტებით, ასევე, იმ ფაქტიდან გამომდინარე, რომ სწორედ პროვაიდერები განსაზღვრავენ პერსონალური მონაცემების დამუშავების მიზანსა და საშუალებებს. ევროკავშირის კანონმდებლობით, დამმუშავებელი, რომელიც მონაცემთა სუბიექტს მომსახურებას აწვდის ევროკავშირში, ვალდებულია, დაემორჩილოს მონაცემთა დაცვის ზოგადი რეგულაციის დებულებებს, მაშინაც კი, თუ პროვაიდერი შექმნილია ევროკავშირის გარეთ.

შესაძლებელია, სოციალური ქსელების მომხმარებლები მონაცემთა დამმუშავებლად ჩაითვალონ? თუ პირი პერსონალურ მონაცემებს ამუშავებს „ცალსახად პირადი ან ოჯახური საქმიანობის ფარგლებში“, მასზე მონაცემთა დაცვის წესები არ ვრცელდება. ეს მონაცემთა დაცვის ევროპულ კანონმდებლობაში ცნობილია „ოჯახური საქმიანობის ფარგლებში დაშვებულ გამონაკლისად“. თუმცა, ზოგ შემთხვევაში, სოციალური ქსელის მომხმარებელი გამონაკლისის ფარგლებში არ ექცევა.

მომხმარებლები ინტერნეტში ნებაყოფლობით აზიარებენ საკუთარ მონაცემებს, რომლებიც შეიძლება სხვა პირთა პერსონალურ ინფორმაციასაც შეიცავდეს.

1027 მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 21.

მაგალითი: პოლს ერთ-ერთ ძალიან პოპულარულ სოციალურ ქსელში შექმნილი აქვს პროფილი. მას მსახიობობა სურს და ხშირად თავის პროფილზე აქვეყნებს ფოტოებს, ვიდეოებსა და პოსტებს, რომლებშიც ხელოვნების სიყვარულზე საუბრობს. მისი მომავლისთვის პოპულარობა ძალიან მნიშვნელოვანია. შესაბამისად, პოლმა გადაწყვიტა საკუთარი პროფილის გასაჯაროება და მასზე წვდომის დაშვება როგორც ქსელის მომხმარებლების, ისე გარეშე პირებისთვის. შეუძლია პოლს მის მეგობარ სარასთან ერთად გადაღებული ფოტოები და ვიდეოები გამოაქვეყნოს სარას თანხმობის გარეშე? სარა სკოლის მასწავლებელია და ცდილობს, პირადი და სამსახურებრივი ცხოვრება მაქსიმალურად გამიჯნოს ერთმანეთისგან. იგი არ არის სოციალური ქსელების მომხმარებელი, თუმცა, ერთ დღეს აღმოაჩენს, რომ პოლმა სოციალურ ქსელში განათავსა მისი ფოტო, გადაღებული წვეულებაზე. ასეთ შემთხვევაში, პოლის მიერ მონაცემთა დამუშავება არ ექვემდებარება ევროკავშირის კანონმდებლობას, რადგან „ოჯახური საქმიანობის ფარგლებში დაშვებული გამონაკლისია“.

ამავდროულად, მომხმარებლებმა უნდა გაიაზრონ, რომ სხვა პირებზე ინფორმაციის ატვირთვამ, თანხმობის გარეშე, შესაძლოა დაარღვიოს მათი პირადი ცხოვრების ხელშეუხებლობა და მონაცემთა დაცვის უფლება. „ოჯახური საქმიანობის ფარგლებში დაშვებული გამონაკლისის“ შემთხვევაშიც კი (მაგ.: როდესაც მომხმარებლის პროფილი ხელმისაწვდომია მხოლოდ განსაზღვრული პირებისთვის), სხვების პერსონალური ინფორმაციის გამოქვეყნებამ შესაძლოა პასუხისმგებლობა დააკისროს პირს. მიუხედავად იმისა, რომ მონაცემთა დაცვის წესები არ ვრცელდება ოჯახური საქმიანობის ფარგლებში დაშვებულ გამონაკლისზე, პასუხისმგებლობა შეიძლება მომდინარეობდეს სხვა, მაგალითად, ცილისწამებისა და ღირსების შელახვის მარეგულირებელი ნორმებიდან. და ბოლოს, ასეთი გამონაკლისი იცავს მხოლოდ სოციალური ქსელების მომხმარებლებს. დამმუშავებელსა და უფლებამოსილ პირზე, რომლებიც უზრუნველყოფენ საშუალებებს მონაცემთა ოჯახური საქმიანობის ფარგლებში დასამუშავებლად, ვრცელდება ევროკავშირის მონაცემთა დაცვის კანონმდებლობა. [1028]

პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების დირექტივის რეფორმით, მონაცემთა დაცვის, პირადი ცხოვრების ხელშეუხებლობისა და უსაფრთხოების წესები, რომლებიც ამჟამად ვრცელდება სატელეკომუნიკაციო მომსახურების პროვაიდერებზე, შეეხება კომპიუტერულ ტექნიკებს შორის კომუნიკაციასა (machine-to-machine communication) და ელექტრონული კომუნიკაციების მომსახურებებსაც, მათ შორის, მაგალითად, over the topმომსახურებას.

1028 იქვე, პრეამბულა 18.

დამატებითი საკითხავი

თავი 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. 'Four fundamental rights: finding the balance', *International Data Privacy Law*, Vol. 6, No. 3, pp. 195–209.

González Fuster, G. and Gellert, G. (2012), 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), pp. 73–82.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. and Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), *EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation*.

Kranenborg, H. (2015), 'Google and the Right to be Forgotten', *European Data Protection Law Review*, Vol. 1, No. 1, pp. 70–79.

Lynskey, O. (2014), 'Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order', *International and Comparative Law Quarterly*, Vol. 63, No. 3, pp. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Kokott, J. and Sobotta, C. (2013), 'The distinction between privacy and data protection in the case law of the CJEU and the ECtHR', *International Data Privacy Law*, Vol. 3, No. 4, pp. 222–228.

EDRi, *An introduction to data protection*, Brussels.

Frowein, J. and Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. and Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munich, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. and Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brussels, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, No. 5, pp. 281–288.

Warren, S. and Brandeis, L. (1890), *The right to privacy*, *Harvard Law Review,* Vol. 4, No. 5, pp. 193–220.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

თავი 2

Acquisty, A., and Gross R. (2009), *Predicting Social Security numbers from public data, Proceedings of the National Academy of Science*, 7 July 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., and Blondel V. D. (2013), 'Unique in the Crowd: the Privacy Bounds of Human Mobility', *Nature Scientific Reports*, Vol. 3, 2013.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. and Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review*, Vol. 57, No. 6, pp. 1701–1777.

Samarati, P. and Sweeney, L. (1998), *Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression*, Technical Report SRI-CSL-98-04.

Sweeney, L. (2002), 'K-Anonymity: A Model for Protecting Privacy' *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, Vol. 10, No. 5, pp. 557–570.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice.*

თავები 3-6

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' in: Grabitz, E., Hilf, M. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Curren, L. and Kaye, J. (2010), 'Revoking consent: a 'blind spot' in data protection law?', *Computer Law & Security Review*, Vol. 26, No. 3 pp. 273–283.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. and Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, Vol. 22, No. 6, pp. 1–5.

De Hert, P. and Papakonstantinou, V. (2012), 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer Law & Security Review*, Vol. 28, No. 2, pp. 130–142.

Feretti, Federico (2012), '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, No. 2, pp. 473–506.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Publications Office of the European Union (Publications Office).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Vienna, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Publications Office.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. and Saxby, S. (2011), '30 years on – The review of the Council of Europe Data Protection Convention 108', *Computer Law & Security Review*, Vol. 27, No. 3, pp. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment.*

თავი 7

European Data Protection Supervisor (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Article 29 Working Party (2005), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.*

თავი 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, London, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlin, Springer.

Europol (2012), *Data Protection at Europol*, Luxembourg, Publications Office.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, The Hague, Eurojust.

De Hert, P. and Papakonstantinou, V. (2012), *The Police and Criminal Justice Data Protection Directive: Comment and Analysis, Computers & Law Magazine of SCL*, Vol. 22, No. 6, pp. 1–5.

Drewer, D. and Ellermann, J. (2012), 'Europol's data protection framework as an asset in the fight against cybercrime'*, ERA Forum*, Vol. 13, No. 3, pp. 381–395.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem', *European Law Review*, Vol. 36, No. 5, pp. 722–776.

Santos Vara, J. (2013), *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.

თავი 9

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem', *European Law Review*, Vol. 36, No. 5, pp. 722–776.

Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

თავი 10

El Emam, K. and Álvarez, C. (2015), 'A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques', *International Data Privacy Law*, Vol. 5, No. 1, pp. 73–87.

Mayer-Schönberger, V. and Cate, F. (2013), 'Notice and consent in a world of Big Data', *International Data Privacy Law*, Vol. 3, No. 2, pp. 67–73.

Rubistein, I. (2013), 'Big Data: The End of Privacy or a New Beginning?', *International Data Privacy Law*, Vol. 3, No. 2, pp. 74–87.

პრეცედენტული სამართალი

ადამიანის უფლებათა ევროპული სასამართლოს პრეცედენტული სამართალი

პერსონალურ მონაცემებზე ხელმისაწვდომობა:

Gaskin v. the United Kingdom, No. 10454/83, 1989 წლის 7 ივლისი;
Godelli v. Italy, No. 33783/09, 2012 წლის 25 სექტემბერი;
K.H. and Others v. Slovakia, No. 32881/04, 2009 წლის 28 აპრილი;
Leander v. Sweden, No. 9248/81, 1987 წლის 26 მარტი;
M.K. v. France, No. 19522/09, 2013 წლის 18 აპრილი;
Odièvre v. France [GC], No. 42326/98, 2003 წლის 13 თებერვალი.

მონაცემთა დაცვის დაბალანსება გამოხატვის თავისუფლებასა და ინფორმაციის მიღების უფლებასთან

Axel Springer AG v. Germany [GC], No. 39954/08, 2012 წლის 7 თებერვალი;
Bohlen v. Germany, No. 53495/09, 2015 წლის 19 თებერვალი;
Coudec and Hachette Filipacchi Associés v. France [GC], No. 40454/07, 2015 წლის; 10 ნოემბერი;
Magyar Helsinki Bizottság v. Hungary [GC], No. 18030/11, 2016 წლის 8 ნოემბერი;
Müller and Others v. Switzerland, No. 10737/84, 1988 წლის 24 მაისი;
Vereinigung bildender Künstler v. Austria, No. 68354/01, 2007 წლის 25 იანვარი;
Von Hannover v. Germany (No. 2) [GC], Nos. 40660/08 and 60641/08, 2012 წლის 7 თებერვალი;
Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No. 931/13, 2017 წლის 27 ივნისი.

მონაცემთა დაცვის დაბალანსება რელიგიის თავისუფლებასთან

Sinan Işık v. Turkey, No. 21924/05, 2010 წლის 2 თებერვალი.

გამოწვევები ინტერნეტში მონაცემთა დაცვის კუთხით

K.U. v. Finland, No. 2872/02, 2008 წლის 2 დეკემბერი.

მონაცემთა სუბიექტის თანხმობა

Elberte v. Latvia, No. 61243/08, 2015 წლის 13 იანვარი;
Sinan Işık v. Turkey, No. 21924/05, 2010 წლის 2 თებერვალი;
Y v. Turkey, No. 648/10, 2015 წლის 17 თებერვალი.

კორესპონდენცია

Amann v. Switzerland [GC], No. 27798/95, 2000 წლის 16 თებერვალი;
Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, No. 62540/00, 2007 წლის 28 ივნისი;
Bernh Larsen Holding AS and Others v. Norway, No. 24117/08, 2013 წლის 14 მარტი;
Cemalettin Canli v. Turkey, No. 22427/04, 2008 წლის 18 ნოემბერი;
D.L. v. Bulgaria, No. 7472/14, 2016 წლის 19 მაისი;
Dalea v. France, No. 964/07, 2010 წლის 2 თებერვალი;
Gaskin v. the United Kingdom, No. 10454/83, 1989 წლის 7 ივლისი;
Haralambie v. Romania, No. 21737/03, 2009 წლის 27 ოქტომბერი;
Khelili v. Switzerland, No. 16188/07, 2011 წლის 18 ოქტომბერი;
Leander v. Sweden, No. 9248/81, 1987 წლის 26 მარტი;
Malone v. the United Kingdom, No. 8691/79, 1984 წლის 2 აგვისტო;
Rotaru v. Romania [GC], No. 28341/95, 2000 წლის 4 მაისი;
S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 2008 წლის 4 დეკემბერი;
Shimovolos v. Russia, No. 30194/09, 2011 წლის 21 ივნისი;
Silver and Others v. the United Kingdom, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 1983 წლის 25 მარტი;
The Sunday Times v. the United Kingdom, No. 6538/74, 1979 წლის 26 აპრილი.

ნასამართლობის მონაცემთა ბაზა

Aycaguer v. France, No. 8806/12, 2017 წლის 22 ივნისი;
B.B. v. France, No. 5335/06, 2009 წლის 17 დეკემბერი;
Brunet v. France, No. 21010/10, 2014 წლის 18 სექტემბერი;
M.K. v. France, No. 19522/09, 2013 წლის 18 აპრილი;
M.M. v. the United Kingdom, No. 24029/07, 2012 წლის 13 ნოემბერი.

მონაცემთა უსაფრთხოება

Haralambie v. Romania, No. 21737/03, 2009 წლის 27 ოქტომბერი;
K.H. and Others v. Slovakia, No. 32881/04, 2009 წლის 28 აპრილი.

დნმ-ის მონაცემთა ბაზები

S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 2008 წლის 4 დეკემბერი.

GPS მონაცემები

Uzun v. Germany, No. 35623/05, 2010 წლის 2 სექტემბერი.

ჯანმრთელობასთან დაკავშირებული მონაცემები

Avilkina and Others v. Russia, No. 1585/09, 2013 წლის 6 ივნისი;
Biriuk v. Lithuania, No. 23373/03, 2008 წლის 25 ნოემბერი;
I v. Finland, No. 20511/03, 2008 წლის 17 ივლისი;
L.H. v. Latvia, No. 52019/07, 2014 წლის 29 აპრილი;
L.L. v. France, No. 7508/02, 2006 წლის 10 ოქტომბერი;
M.S. v. Sweden, No. 20837/92, 1997 წლის 27 აგვისტო;
Szuluk v. the United Kingdom, No. 36936/05, 2009 წლის 2 ივნისი;
Y v. Turkey, No. 648/10, 2015 წლის 17 თებერვალი;
Z v. Finland, No. 22009/93, 1997 წლის 25 თებერვალი.

ვინაობა

Ciubotaru v. Moldova, No. 27138/04, 2010 წლის 27 აპრილი;
Godelli v. Italy, No. 33783/09, 2012 წლის 25 სექტემბერი;
Odièvre v. France [GC], No. 42326/98, 2003 წლის 13 თებერვალი.

ინფორმაცია პროფესიული საქმიანობის შესახებ

G.S.B. v. Switzerland, No. 28601/11, 2015 წლის 22 დეკემბერი;
M.N. and Others v. San Marino, No. 28005/12, 2015 წლის 7 ივლისი;
Michaud v. France, No. 12323/11, 2012 წლის 6 დეკემბერი;
Niemietz v. Germany, No. 13710/88, 1992 წლის 16 დეკემბერი.

კომუნიკაციაზე მონიტორინგი

Amann v. Switzerland [GC], No. 27798/95, 2000 წლის 16 თებერვალი;
Brito Ferrinho Bexiga Villa-Nova v. Portugal, No. 69436/10, 2015 წლის 1 დეკემბერი;
Copland v. the United Kingdom, No. 62617/00, 2007 წლის 3 აპრილი;
Halford v. the United Kingdom, No. 20605/92, 1997 წლის 25 ივნისი;

Iordachi and Others v. Moldova, No. 25198/02, 2009 წლის 10 თებერვალი;
Kopp v. Switzerland, No. 23224/94, 1998 წლის 25 მარტი;
Liberty and Others v. the United Kingdom, No. 58243/00, 2008 წლის 1 ივლისი;
Malone v. the United Kingdom, No. 8691/79, 1984 წლის 2 აგვისტო;
Mustafa Sezgin Tanrıkulu v. Turkey, No. 27473/06, 2017 წლის 18 ივლისი;
Pruteanu v. Romania, No. 30181/05, 2015 წლის 3 თებერვალი;
Szuluk v. the United Kingdom, No. 36936/05, 2009 წლის 2 ივნისი.

პასუხისმგებელ პირთა ვალდებულებები

B.B. v. France, No. 5335/06, 2009 წლის 17 დეკემბერი;
I v. Finland, No. 20511/03, 2008 წლის 17 ივლისი;
Mosley v. the United Kingdom, No. 48009/08, 2011 წლის 10 მაისი.

პერსონალური მონაცემები

Amann v. Switzerland [GC], No. 27798/95, 2000 წლის 16 თებერვალი;
Uzun v. Germany, No. 35623/05, 2010 წ;
Bernh Larsen Holding AS and Others v. Norway, No. 24117/08, 2013 წლის 14 მარტი.

ფოტოები

Sciacca v. Italy, No. 50774/99, 2005 წლის 11 იანვარი;
Von Hannover v. Germany, No. 59320/00, 2004 წლის 24 ივნისი.

დავიწყების უფლება

Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 2006 წლის 6 ივნისი;
Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No. 931/13, 2017 წლის 27 ივნისი.

მონაცემთა დამუშავების შეწყვეტის უფლება

Leander v. Sweden, No. 9248/81, 1987 წლის 26 მარტი;
M.S. v. Sweden, No. 20837/92, 1997 წლის 27 აგვისტო;
Mosley v. the United Kingdom, No. 48009/08, 2011 წლის 10 მაისი;
Rotaru v. Romania [GC], No. 28341/95, 2000 წლის 4 მაისი;
Sinan Işık v. Turkey, No. 21924/05, 2010 წლის 2 თებერვალი.

განსაკუთრებული კატეგორიის მონაცემები

Brunet v. France, No. 21010/10, 2014 წლის 18 სექტემბერი;
I v. Finland, No. 20511/03, 2008 წლის 17 ივლისი;
Michaud v. France, No. 12323/11, 2012 წლის 6 დეკემბერი;
S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 2008 წლის 4 დეკემბერი.

ზედამხედველობა და აღსრულება (სხვადასხვა აქტორის, მათ შორის, საზედამხედველო ორგანოების მოვალეობები)

I v. Finland, No. 20511/03, 2008 წლის 17 ივლისი;
K.U. v. Finland, No. 2872/02, 2008 წლის 2 დეკემბერი;
Von Hannover v. Germany, No. 59320/00, 2004 წლის 24 ივნისი;
Von Hannover v. Germany (No. 2) [GC], Nos. 40660/08 და 60641/08, 2012 წლის 7 თებერვალი.

თვალთვალის მეთოდები

Allan v. the United Kingdom, No. 48539/99, 2002 წლის 5 ნოემბერი;
Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, No. 62540/00, 2007 წლის 28 ივნისი;
Bărbulescu v. Romania [GC], No. 61496/08, 2017 წლის 5 სექტემბერი;
D.L. v. Bulgaria, No. 7472/14, 2016 წლის 19 მაისი;
Dragojević v. Croatia, No. 68955/11, 2015 წლის 15 იანვარი;
Karabeyoğlu v. Turkey, No. 30083/10, 2016 წლის 7 ივნისი;
Klass and Others v. Germany, No. 5029/71, 1978 წლის 6 სექტემბერი;
Rotaru v. Romania [GC], No. 28341/95, 2000 წლის 4 მაისი;
Szabó and Vissy v. Hungary, No. 37138/14, 2016 წლის 12 იანვარი;
Taylor-Sabori v. the United Kingdom, No. 47114/99, 2002 წლის 22 ოქტომბერი;
Uzun v. Germany, No. 35623/05, 2010 წლის 2 სექტემბერი;
Versini-Campinchi and Crasnianski v. France, No. 49176/11, 2016 წლის 16 ივნისი;
Vetter v. France, No. 59842/00, 2005 წლის 31 მაისი;
Vukota-Bojić v. Switzerland, No. 61838/10, 2016 წლის 18 ოქტომბერი;
Roman Zakharov v. Russia [GC], No. 47143/06, 2015 წლის 4 დეკემბერი.

ვიდეოთვალთვალი

Köpke v. Germany, No. 420/07, 2010 წლის 5 დეკემბერი;
Peck v. the United Kingdom, No. 44647/98, 2003 წლის 28 იანვარი.

ხმის ნიმუშები

Wisse v. France, No. 71611/01, 2005 წლის 20 დეკემბერი;
P.G. and J.H. v. the United Kingdom, No. 44787/98, 2001 წლის 25 სექტემბერი.

ევროკავშირის მართლმსაჯულების სასამართლოს პრეცედენტული სამართალი

მონაცემთა დაცვის დირექტივასთან დაკავშირებული პრეცედენტული სამართალი

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme,* 2017 წლის 4 მაისი;

[კანონიერი დამუშავების პრინციპები: მესამე მხარის კანონიერი ინტერესი]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni,* 2017 წლის 9 მარტი;

[პერსონალური მონაცემების წაშლის უფლება; მონაცემთა დამუშავების შეწყვეტის მოთხოვნის უფლება]

გაერთიანებული საქმეები C-203/15 და C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* [GC], 2016 წლის 21 დეკემბერი;

[ელექტრონული კომუნიკაციების კონფიდენციალობა; ელექტრონული კომუნიკაციების პროვაიდერები; გადაადგილებისა და ადგილმდებარეობის განმსაზღვრელი მონაცემების ზოგადი და განურჩეველი შენახვა; სასამართლო და დამოუკიდებელი ადმინისტრაციული ორგანოს კონტროლის არარსებობა; ევროკავშირის ადამიანის ფუნდამენტურ უფლებათა ქარტია; შესაბამისობა ევროკავშირის კანონმდებლობასთან]

C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland,* 2016 წლის 19 ოქტომბერი;

[„პერსონალური მონაცემების" განმარტება; ინტერნეტ პროტოკოლის მისამართები; მონაცემთა შენახვა ონლაინ მედიაპროვაიდერის მიერ; ეროვნული კანონმდებლობა, რომლის თანახმადაც მონაცემთა დამმუშავებლის კანონიერი ინტერესები მხედველობაში არ მიიღება]

C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 2015 წლის 6 ოქტომბერი;

[კანონიერი დამუშავების პრინციპი; ფუნდამენტური უფლებები; ე.წ. დაცვის საშუალებათა (Safe Harbour) გადაწყვეტილების კანონიერება; დამოუკიდებელი საზედამხედველო ორგანოს უფლებამოსილება]

C-230/14, *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság,* 2015 წლის 1 ოქტომბერი;

[ეროვნული საზედამხედველო ორგანოს უფლებამოსილება]

C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others,* 2015 წლის 1 ოქტომბერი;

[პერსონალური მონაცემების დამუშავებაზე ინფორმირების უფლება]

C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů,* 2014 წლის 11 დეკემბერი;

[„მონაცემთა დამუშავებისა“ და „მონაცემთა დამმუშავებლის“ კონცეფცია]

C-473/12, *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and Others,* 2013 წლის 7 ნოემბერი;

[პერსონალური მონაცემების დამუშავებაზე ინფორმირების უფლება]

T-462/12 R, *Pilkington Group Ltd v. European Commission,* Order of the President of the General Court, 2013 წლის 11 მარტი;

C-342/12, *Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT),* 2013 წლის 30 მაისი;

[„პერსონალური მონაცემების“ კონცეფცია; ნამუშევარი დროს აღრიცხვა; მონაცემთა ხარისხისა და კრიტერიუმების პრინციპები მათი კანონიერი დამუშავებისათვის; იმ ეროვნული უწყებების წვდომა პერსონალურ მონაცემებზე, რომლებიც მონიტორინგს უწევენ სამუშაო პირობებს; დამსაქმებლის მოვალეობა, უზრუნველყოს აღრიცხულ ნამუშევარ დროზე წვდომა და მისი დაუყოვნებლივ გამოყენება]

გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 2014 წლის 8 აპრილი;

[ევროკავშირის მონაცემთა შენახვის დირექტივის დარღვევა; კანონიერი დამუშავება; მიზნისა და შენახვის ვადის შეზღუდვა]

C-288/12, *European Commission v. Hungary* [GC], 2014 წლის 8 აპრილი;

[მონაცემთა დაცვის ზედამხედველის გათავისუფლების კანონიერება]

გაერთიანებული საქმეები C-141/12 და C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S,* 2014 წლის 17 ივლისი;

[მონაცემთა სუბიექტის წვდომის ფარგლები; ფიზიკური პირების დაცვა პერსონალური მონაცემების დამუშავებისას; „პერსონალური მონაცემების“ კონცეფცია; მონაცემები, რომლებიც უკავშირდება ბინადრობის ნებართვის მოთხოვნას; სამართლებრივი ანალიზი, რომელიც წარმოდგენილია გადაწყვეტილების მიღებამდე მომზადებულ ადმინისტრაციულ დოკუმენტში; ევროკავშირის ფუნდამენტურ უფლებათა ქარტია]

C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 წლის 13 მაისი;

[საძიებო სისტემის პროვაიდერის ვალდებულება, მონაცემთა სუბიექტის თხოვნის საფუძველზე, თავი შეიკავოს პერსონალური მონაცემების შეტანისგან ძიების შედეგებში; მონაცემთა დაცვის დირექტივის გამოყენება; „მონაცემთა დამუშავების“ კონცეფცია; „მონაცემთა დამმუშავებლის“ მნიშვნელობა, მონაცემთა დაცვის დაბალანსება გამოხატვის თავისუფლებასთან; „დავიწყების“ უფლება]

C-614/10, *European Commission v. Republic of Austria* [GC], 2012 წლის 16 ოქტომბერი;

[ეროვნული საზედამხედველო ორგანოს დამოუკიდებლობა]

გაერთიანებული საქმეები C-468/10 და C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado,* 2011 წლის 24 ნოემბერი;

[მონაცემთა დაცვის ზოგადი დირექტივის 7 (ვ) მუხლის - „სხვათა კანონიერი ინტერესები“ - სწორად დანერგვა ეროვნულ კანონმდებლობაში]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV,* 2012 წლის 16 თებერვალი;

[სოციალური ქსელის პროვაიდერთა მოვალეობა - ქსელის მომხმარებელთა მიერ მუსიკალური და აუდიო-ვიზუალური ნაშრომების უკანონო გამოყენების პრევენცია]

C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* 2011 წლის 24 ნოემბერი;

[საინფორმაციო საზოგადოება, საავტორო უფლებები, ინტერნეტი, ე.წ. „peer-to-peer„ კომპიუტერული პროგრამები; ინტერნეტმომსახურების მიმწოდებლები; ელექტრონული კომუნიკაციის გამფილტრავი სისტემის დანერგვა ფაილების გაზიარებით საავტორო უფლებების დარღვევის წინააღმდეგ; გადაცემული ინფორმაციის მონიტორინგის ზოგადი ვალდებულების არარსებობა]

C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland,* 2011 წლის 5 მაისი;

[განახლებული თანხმობის აუცილებლობა]

გაერთიანებული საქმეები C-92/09 და C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 2010 წლის 9 ნოემბერი;

[„პერსონალური მონაცემების“ კონცეფცია; ევროკავშირის სასოფლო-სამეურნეო ფონდების ბენეფიციართა პერსონალური მონაცემების გამოქვეყნების სამართლებრივი ვალდებულების პროპორციულობა]

C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer,* 2009 წლის 9 მაისი;
[მონაცემთა სუბიექტის წვდომის უფლება]

C-518/07, *European Commission v. Federal Republic of Germany* [GC], 2010 წლის 9 მარტი;
[ეროვნული საზედამხედველო ორგანოს დამოუკიდებლობა]

C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [GC], 2008 წლის 16 დეკემბერი;
[„ჟურნალისტური საქმიანობის“ კონცეფცია მონაცემთა დაცვის დირექტივის მე-9 მუხლის ფარგლებში]

C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 2008 წლის 16 დეკემბერი;
[სტატისტიკურ რეესტრში უცხო ქვეყნის მოქალაქეებზე მონაცემთა შენახვის კანონიერება]

C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 2008 წლის 29 იანვარი;
[„პერსონალური მონაცემების“ კონცეფცია; ინტერნეტმომსახურების მიმწოდებელთა მოვალეობა, ინტელექტუალური საკუთრების დაცვის ასოციაციებს გაუმჟღავნონ იმ პირთა ვინაობა, რომლებიც მოიხმარენ KaZaA-ს ფაილების გაცვლის პროგრამებს]

C-101/01, *Criminal proceedings against Bodil Lindqvist,* 2003 წლის 6 ნოემბერი;
[პერსონალურ მონაცემთა სპეციალური კატეგორიები]

გაერთიანებული საქმეები C-465/00, C-138/01 და C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Jospeh Lauermann v. Österreichischer Rundfunk,* 2003 წლის 20 მაისი;
[გარკვეული საჯარო დაწესებულებების მიერ დასაქმებულთა ხელფასებზე მონაცემების გამოქვეყნების სამართლებრივი ვალდებულების პროპორციულობა]

C434/16, *Peter Nowak v. Data Protection Commissioner, Opinion of the Advocate General Kokott,* 2017 წლის 20 ივლისი;
[„პერსონალური მონაცემების“ კონცეფცია; საგამოცდო ნამუშევარზე წვდომის უფლება; გამომცდელის შესწორებები]

C-291/12, *Michael Schwarz v. Stadt Bochum,* 2013 წლის 17 ოქტომბერი
[წინასწარ გადაწყვეტილებაზე მითითება; თავისუფლების, უსაფრთხოებისა და მართლმსაჯულების სფერო; ბიომეტრიული პასპორტი; თითის ანაბეჭდები; სამართლებრივი საფუძველი; პროპორციულობა]

2016/681 დირექტივასთან დაკავშირებული პრეცედენტული სამართალი

სასამართლოს (დიდი პალატა) მოსაზრება 1/15 , 2017 წლის 26 ივლისი;
[სამართლებრივი საფუძველი; კანადასა და ევროკავშირს შორის მგზავრთა პირადი მონაცემების გადაცემასა და დამუშავებაზე შეთანხმების პროექტი; პროექტის შესაბამისობა TFEU-ს მე-16 მუხლთან, ასევე, Charter-ის მუხლებთან: 7 , 8 , 51 (1)]

ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაციასთან დაკავშირებული პრეცედენტული სამართალი

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission,* 2015 წლის 16 ივლისი;
[დოკუმენტებზე წვდომა]

C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.* [GC], 2010 წლის 29 ივნისი;
[დოკუმენტებზე წვდომა]

2002/58/EC დირექტივასთან დაკავშირებული პრეცედენტული სამართალი

C-536/15, *Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC),* 2017 წლის 15 მარტი;
[არადისკრიმინაციული პრინციპი; მომხმარებელთა მონაცემებზე წვდომა საჯარო ცნობარში შეტანის გზით; მომხმარებელთა თანხმობა; განსხვავება წევრი სახელმწიფოს მიხედვით, სადაც ხელმისაწვდომია საჯარო ცნობარი და საცნობარო სამსახური]

გაერთიანებული საქმეები C-203/15 და C-698/15, *Tele2 Sverige AB v. Post- och telestryrelsen and Secretary of State for the Home Department v. Tom Watson and Others* [GC], 2016 წლის 21 დეკემბერი;
[ელექტრონული კომუნიკაციების კონფიდენციალობა; ელექტრონული კომუნიკაციის პროვაიდერები; ტრეფიკისა და ადგილმდებარეობის განმსაზღვრელი მონაცემების ზოგადი და განურჩეველი შენახვა; სასამართლო და დამოუკიდებელი ადმინისტრაციული ორგანოს კონტროლის არარსებობა; ევროკავშირის ადამიანის ფუნდამენტურ უფლებათა ქარტია; ევროკავშირის კანონმდებლობასთან შესაბამისობა]

C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* 2011 წლის 24 ნოემბერი;

[საინფორმაციო საზოგადოება, საავტორო უფლებები, ინტერნეტი, ე.წ. „peer-to-peer“ კომპიუტერული პროგრამები; ინტერნეტმომსახურების მიმწოდებლები; ელექტრონული კომუნიკაციის გამფილტრავი სისტემის დანერგვა ფაილების გაზიარებით საავტორო უფლებების დარღვევის წინააღმდეგ; გადაცემულ ინფორმაციაზე მონიტორინგის ზოგადი ვალდებულების არარსებობა]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB,* 2012 წლის 19 აპრილი.

[საავტორო და მომიჯნავე უფლებები; მონაცემების ინტერნეტით დამუშავება; ექსკლუზიური უფლების დარღვევა; აუდიოწიგნები, რომლებიც ხელმისაწვდომია FTP სერვერის საშუალებით, ინტერნეტში, ინტერნეტპროვაიდერის მიერ უზრუნველყოფილი IP მისამართის საშუალებით; ინტერნეტმომსახურების მიმწოდებელის ვალდებულება, წარმოადგინოს IP-ის მომხმარებლის სახელი და მისამართი, სასამართლოს მოთხოვნის შესაბამისად]

ინდექსი

ევროკავშირის მართლმსაჯულების სასამართლოს პრეცედენტული სამართალი

ადამიანის უფლებათა ევროპული სასამართლოს პრეცედენტული სამართალი

ეროვნული სასამართლოების პრეცედენტული სამართალი

ინფორმაცია ევროკავშირის ფუნდამენტურ უფლებათა სააგენტოს შესახებ ხელმისაწვდომია ინტერნეტით, კერძოდ, FRA-ს ვებგვერდზე: fra.europa.eu.

დამატებითი ინფორმაცია ადამიანის უფლებათა ევროპული სასამართლოს პრეცედენტული სამართლის შესახებ ხელმისაწვდომია სასამართლოს ვებგვერდზე: echr.coe.int. HUDOC-ის საძიებო პორტალზე წარმოდგენილია სასამართლოს გადაწყვეტილებები და განჩინებები ინგლისურ და/ან ფრანგულ ენებზე, ასევე, თარგმანები, რეზიუმეები, პრესრელიზები და სხვა ინფორმაცია სასამართლოს მუშაობის შესახებ.

როგორ მივიღოთ ევროკავშირის პუბლიკაციები

ევროპის საბჭოს გამომცემლობა ნაშრომებს გამოსცემს ორგანიზაციის საქმიანობის ყველა სფეროში, როგორიცაა: ადამიანის უფლებები, სამართლებრივი მეცნიერებები, ჯანდაცვა, ეთიკა, სოციალური ურთიერთობები, გარემო, განათლება, კულტურა, სპორტი, ახალგაზრდების საკითხები და ძეგლთა დაცვა. ვრცელ კატალოგში არსებული წიგნებისა და ელექტრონული გამოცემების შეკვეთა შესაძლებელია ინტერნეტით (http://book.coe.int/).

ვირტუალური საკითხავი „ოთახი“ მომხმარებლებს საშუალებას აძლევს, უფასოდ გაეცნონ გამოქვეყნებული ნაშრომების ამონარიდებს ან კონკრეტული ოფიციალური დოკუმენტების მთლიან ტექსტებს.

ინფორმაცია ევროპის საბჭოს კონვენციებზე, სრული ტექსტის ჩათვლით, ხელმისაწვდომია ევროპის საბჭოს საერთაშორისო ხელშეკრულებების სამდივნოს ვებგვერდზე: http://conventions.coe.int/.

საინფორმაციო ტექნოლოგიების სწრაფი განვითარების გამო, აუცილებელია პერსონალურ მონაცემთა დაცვა. ეს არის უფლება, რომელიც დაცულია ევროკავშირისა და ევროპის საბჭოს ინსტრუმენტებით და უკავშირდება ახალ და მნიშვნელოვან გამოწვევებს, როგორიცაა თვალთვალი, კომუნიკაციაზე კონტროლი და მონაცემთა შენახვა. წინამდებარე სახელმძღვანელო შექმნილია სამართალმცოდნეებისათვის, რომელთა სპეციალიზაციაც არ არის მონაცემთა დაცვა. ნაშრომი აღწერს ევროკავშირისა და ევროპის საბჭოს შესაბამის სამართლებრივ ჩარჩოს, განმარტავს საკვანძო სამართლებრივ პრეცედენტებს და მოკლედ მიმოიხილავს ევროკავშირის მართლმსაჯულების სასამართლოსა და ადამიანის უფლებათა ევროპული სასამართლოს ძირითად გადაწყვეტილებებს. სახელმძღვანელოში წარმოდგენილია ჰიპოთეტური სცენარებიც, მონაცემთა დაცვის ცვალებად სფეროში ურთიერთდაკავშირებული საკითხების პრაქტიკული ილუსტრაციისათვის.

ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო

Schwarzenbergplatz 11 - 1040 Vienna - Austria
ტელ. +43 (1) 580 30-0 - ფაქსი +43 (1) 580 30-699
fra.europa.eu - info@fra.europa.eu - @EURightsAgency

ევროპის საბჭო
ადამიანის უფლებათა ევროპული სასამართლო

67075 Strasbourg Cedex - France
ტელ. +33 (0) 3 88 41 20 18 - ფაქსი +33 (0) 3 88 41 27 30
echr.coe.int - publishing@echr.coe.int - @ECHR_ECHR

ევროკავშირის მონაცემთა დაცვის ზედამხედველი

Rue Wiertz 60 – 1047 Brussels – Belgium
Tel. +32 2 283 19 00
www.edps.europa.eu - edps@edps.europa.eu - @EU_EDPS

ISBN 978-9941-9658-9-0