

მონაცემთა დაცვის ეპროპული სამართალი

სახელმძღვანელო



„იურისტების სამყარო“

© ძირითადი უფლებების ევროპული კავშირის სააგენტო, 2014
ევროპის საბჭო, 2014

სამომავლო განახლება ხელმისაწვდომი იქნება ძირითადი უფლებების ევროპული კავშირის სააგენტოს ვებ-გვერდზე fra.europa.eu, ევროპის საბჭოს ვებ-გვერდზე coe.int/dataprotection, და ადამიანის უფლებათა ევროპული სასამართლოს ვებ-გვერდზე echr.coe.int სასამართლო გადაწყვეტილებათა განყოფილებაში

მომსახურება Europe Direct დაგეხმარებათ მიიღოთ პასუხები ევროპული კავშირის შესახებ შეკითხვებზე

ტელეფონის ნომერი(*):
00 800 6 7 8 9 10 11

(*) ინფორმაცია, ისევე როგორც ზარების უმეტესობა, არის უფასო (თუმცა ზოგიერთმა ოპერატორმა, სატელეფონო ჯიხურმა ან სასტუმრომ შესაძლებელია დაადგინოს საფასური)

ევროპული კავშირის შესახებ დამატებითი ინფორმაცია ხელმისაწვდომია ინტერნეტში (<http://europa.eu>).

ISBN (ქართულენოვანი) 978-9941-9406-3-7

ეს სახელმძღვანელო შედგენილ იქნა ინგლისურ ენაზე და დასრულდა 2014 წლის აპრილში. ძირითადი უფლებების ევროპული კავშირის სააგენტო (FRA), ევროპის საბჭო (CoE) და ადამიანის უფლებათა ევროპული სასამართლო (ECTHR) არ არის პასუხისმგებელი სხვა ენებზე თარგმნის ხარისხზე. ამ სახელმძღვანელოში გამოხატული შეხედულებები არ ავალდებულებს ევროპის საბჭოსა და ადამიანის უფლებათა ევროპულ სასამართლოს. სახელმძღვანელოში შერჩეულია კომენტარები და ინსტრუქციები. ევროპის საბჭო და ადამიანის უფლებათა ევროპული სასამართლო არ არიან პასუხისმგებლები მის შინაარსზე, ასევე, არც მათი აღნიშვნა მოცემულ ჩამონათვალში გულისხმობს რაიმე ფორმით ამ პუბლიკაციების მხარდაჭერას. სხვა პუბლიკაციები არის მოცემული ადამიანის უფლებათა ევროპული სასამართლოს ბიბლიოთეკის ვებ-გვერდზე: echr.coe.int.

თბილისი, 2015
გამომცემლობა „იურისტების საფარო“



მონაცემთა დაცვის ევროპული სამართალი

- სახელმძღვანელო -
(თარგმანი)

თარგმანის ავტორი: კახაბერ გოშაძე

რედაქტორი: მალხაზ ბეგიაშვილი

წინასიტყვაობა

მონაცემთა დაცვის ევროპული სამართლის აღნიშნული სახელმძღვანელო ერთობლივად იქნა შემუშავებული ძირითადი უფლებების ევროპული კავშირის სააგენტოსა (FRA) და ევროპის საბჭოს მიერ, ადამიანის უფლებათა ევროპული სასამართლოს სამდივნოსთან ერთად. ეს არის რიგით მესამე იურიდიული სახელმძღვანელო, რომელიც ერთობლივად შემუშავდა ძირითადი უფლებების ევროპული კავშირის სააგენტოსა და ევროპის საბჭოს მიერ. 2011 წლის მარტში, გამოიცა პირველი სახელმძღვანელო ევროპული ანტიდისკრიმინაციული სამართლის შესახებ, 2013 წლის ივნისში – მეორე სახელმძღვანელო თავშესაფართან, საზღვრებთან და იმიგრაციასთან დაკავშირებული ევროპული სამართლის შესახებ.

ჩვენ გადაწყვეტიტ გაავაგრძელოთ ჩვენი თანამშრომლობა მეტად აქტუალურ საკითხზე, კერძოდ, პერსონალურ მონაცემთა დაცვაზე, რომელიც დღეს თითოეულ ჩვენთაგანს ეხება. ამ სფეროში ევროპა სარგებლობს ერთ-ერთი ყველაზე მეტად დამცავი სისტემით, რომელიც დაფუძნებულია ევროპის საბჭოს 108-ე კონვენციაზე, ევროპული კავშირის (EU) ინსტრუმენტებზე, ასევე, ადამიანის უფლებათა ევროპული სასამართლოსა (ECTHR) და მართლმსაჯულების ევროპული კავშირის სასამართლოს (CJEU) გადაწყვეტილებებზე.

აღნიშნული სახელმძღვანელოს მიზანია აამაღლოს ცნობიერება და ცოდნა მონაცემთა დაცვის წესების შესახებ ევროპული კავშირისა და ევროპის საბჭოს წევრ ქვეყნებში, მკითხველებისთვის მიმართვის მთავარ საგნად არსებობის გზით. იგი შექმნილია სპეციალიზაციის არმქონე სამართალმცოდნეებისთვის, მოსამართლეებისთვის, მონაცემთა დაცვის ეროვნული ორგანოებისთვის და სხვა პირებისთვის, რომლებიც მუშაობენ მონაცემთა დაცვის სფეროში.

2009 წლის დეკემბერში, ლისაბონის ხელშეკრულების ძალაში შესვლით, ევროპული კავშირის ძირითად უფლებათა ქარტიამ იურიდიულად სავალდებულო ძალა შეიძინა და პერსონალურ მონაცემთა დაცვის უფლებამ განცალკევებული ძირითადი უფლების სტატუსი მოიპოვა. ევროპის საბჭოს 108-ე კონვენციი-

სა და ევროპული კავშირის ინსტრუმენტების – რომლებმაც გაკვალეს გზა მონაცემთა დაცვისათვის ევროპაში, ასევე, მართლმსაჯულების ევროპული კავშირის სასამართლოსა და ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებების უკეთესი გააზრება მნიშვნელოვანია მოცემული ძირითადი უფლების დაცვისათვის.

ჩვენ გვსურს მადლობა გადავუხადოთ ადამიანის უფლებების ლუდვიგ ბოლცმანის ინსტიტუტს მის მიერ შეტანილი წვლილისთვის ამ სახელმძღვანელოს შექმნისას. ჩვენ, ასევე, გვსურს გამოვხატოთ ჩვენი მადლიერება მონაცემთა დაცვის ევროპული ზედამხედველის სამსახურის მიმართ შექმნის პროცესში არსებული უკუკავშირისთვის. აღნიშნული სახელმძღვანელოს მომზადებისას ჩვენ, ასევე, მადლობას ვუხდით ევროპული კომისიის მონაცემთა დაცვის განყოფილებას.

ფილიპ ბუალა

ევროპის საბჭო, ადამიანის
უფლებები და კანონის
უზენაესობა,
გენერალური დირექტორი

მორტენ კიერუმი

ძირითადი უფლებების
ევროპული კავშირის
სააგენტოს დირექტორი

მთარგმნელისგან

პერსონალური მონაცემების დაცვა ადამიანის ერთ-ერთი უმნიშვნელოვანესი უფლებაა. მისი აქტუალურობა საზოგადოებრივი ურთიერთობებისა და ტექნოლოგიური საშუალებების განვითარებასთან ერთად უფრო და უფრო მატულობს. უნდა აღინიშნოს, რომ ევროპული ქვეყნებისგან განსხვავებით, მონაცემთა დაცვის სამართლებრივი რეგულირების პროცესი საქართველოში არც თუ ისე დიდი ხნის წინ დაიწყო. საქართველოს პარლამენტმა 2005 წლის 28 ოქტომბერს მოახდინა ევროპის საბჭოს 108-ე კონვენციის რატიფიცირება, ასევე, მნიშვნელოვან მოვლენას ჰქონდა ადგილი 2011 წლის 28 დეკემბერს, როდესაც მიღებულ იქნა კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, ხოლო 2013 წლის 27 ივლისს პარლამენტმა განახორციელა 108-ე კონვენციის დამატებითი ოქმის რატიფიცირება. აქედან გამომდინარე, ნათელია, რომ მონაცემთა დაცვის სფეროში აღებული გეზი ევროპული სტანდარტის დამკვიდრებისა და მისი უზრუნველყოფისკენ არის მიმართული, რაც მოცემული სფეროს სამომავლო დახვეწისა და განმტკიცების შესაძლებლობას ქმნის.

მონაცემთა დაცვას დიდი ყურადღება ექცევა ევროპის მასშტაბით. ამის დადასტურებაა ევროპული კავშირისა და ევროპის საბჭოს ფარგლებში მიღებული არაერთი სავალდებულო სამართლებრივი თუ სარეკომენდაციო სახის დოკუმენტი. ამასთან, მოცემული სფეროს განვითარებაში უდიდესი წვლილი შეაქვს ადამიანის უფლებათა ევროპული სასამართლოსა და მართლმსაჯულების ევროპული კავშირის სასამართლოს მიერ გამოტანილ გადაწყვეტილებებს, რომელიც ეხება პირადი ცხოვრების, მათ შორის, პერსონალური მონაცემების დაცვას.

მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო განიხილავს ევროპის მასშტაბით მოქმედ იმ სამართლებრივ თუ სარეკომენდაციო სახის დოკუმენტებს, რომელიც ეხება პერსონალური მონაცემების დაცვას. აქედან გამომდინარე, სახელმძღვანელოს ქართულ ენაზე თარგმნის გადაწყვეტილება ორი მიზეზის გამო იქნა მიღებული: პირველი, მონაცემთა დაცვის ქართული სამართლებრივი ნორმები ახდენს ევროპული სტან-

დარტის დამკვიდრებას და მეორე, მოცემული სახელმძღვანელო ამომწურავად განიხილავს ევროპაში არსებულ პერსონალურ მონაცემებთან დაკავშირებულ ძირითად წესებს. ვიმედოვნებ, რომ არსებული თარგმანი ხელს შეუწყობს მონაცემთა დაცვის სფეროს განვითარებასა და განმტკიცებას საქართველოში.

ამასთან, განეული შრომისა და მხარდაჭერისთვის, მსურს მადლობა გადავუხადო სახელმძღვანელოს ქართულენოვანი თარგმანის რედაქტორს - საქართველოს უნივერსიტეტის სამართლის სკოლის პროფესორს, ბატონ მალხაზ ბეგიაშვილს და გამომცემლობა „იურისტების სამყარო“-ს სამუშაო ჯგუფს.

**კახაბერ გოშაძე,
იურისტი , საქართველოს უნივერსიტეტის
სამართლის სკოლის დოქტორანტი.**

12 იანვარი, 2015 წელი.

სარჩევი

წინასიტყვაობა	3
მთარგმნელისგან	5
აბრევიატურები	11
როგორ გამოვიყენოთ სახელმძღვანელო	14
1. მონაცემთა დაცვის ევროპული სამართლის კონტექსტი და საფუძვლები	17
1.1. უფლება მონაცემთა დაცვაზე	18
1.1.1. ადამიანის უფლებათა ევროპული კონვენცია.....	18
1.1.2. ევროპის საბჭოს 108-ე კონვენცია	20
1.1.3. მონაცემთა დაცვის ევროპული კავშირის სამართალი.....	23
1.2. მანონასწორებელი უფლებები	29
1.2.1. გამოხატვის თავისუფლება	31
1.2.2. დოკუმენტებთან წვდომა	35
1.2.3. ხელოვნებისა და მეცნიერების თავისუფლება.....	41
1.2.4. საკუთრების დაცვა.....	43
2. მონაცემთა დაცვის ტერმინოლოგია	45
2.1. პერსონალური მონაცემი	47
2.1.1. ცნება „პერსონალური მონაცემი“-ს მთავარი ასპექტები	47
2.1.2. პერსონალური მონაცემების განსაკუთრებული კატეგორიები.....	57
2.1.3. ანონიმიზებული და ფსევდონიმიზებული მონაცემები....	58
2.2. მონაცემთა დამუშავება	61
2.3. პერსონალურ მონაცემთა მომხმარებლები.....	64
2.3.1. დამმუშავებლები და უფლებამოსილი პირები	64
2.3.2. მიმღებები და მესამე პირები.....	72
2.4. თანხმობა	74
2.4.1. კანონიერი ძალის მქონე თანხმობის ელემენტები.....	75

2.4.2. გაცემული თანხმობის ნებისმიერ დროს უკან გამოთხოვის უფლება	81
3. მონაცემთა დაცვის ევროპული სამართლის საკვანძო პრინციპები	82
3.1. კანონიერი დამუშავების პრინციპი	84
3.1.1. მართლზომიერი ჩარევის საფუძვლები ადამიანის უფლებათა ევროპული კონვენციის მიხედვით.....	84
3.1.2. კანონიერი შეზღუდვის პირობები ევროპული კავშირის ქარტიის მიხედვით.....	88
3.2. მიზნის კონკრეტულობისა და ლიმიტირების პრინციპი.....	91
3.3. მონაცემთა ხარისხის პრინციპები.....	94
3.3.1. მონაცემთა შესაბამისობის პრინციპი	94
3.3.2. მონაცემთა სისწორის პრინციპი.....	95
3.3.3. მონაცემთა ლიმიტირებული შენახვის პრინციპი	97
3.4. მონაცემთა სამართლიანი დამუშავების პრინციპი	98
3.4.1. გამჭვირვალობა	99
3.4.2. ნდობის დამყარება	99
3.5. ანგარიშვალდებულების პრინციპი	101
4. მონაცემთა დაცვის ევროპული სამართლის წესები	104
4.1. კანონიერი დამუშავების წესები.....	106
4.1.1. არასენსიტიური კატეგორიის მონაცემთა კანონიერი დამუშავება.....	107
4.1.2. განსაკუთრებული კატეგორიის მონაცემთა კანონიერი დამუშავება.....	114
4.2. დამუშავების უსაფრთხოების წესები.....	119
4.2.1. მონაცემთა უსაფრთხოების ელემენტები.....	120
4.2.2. კონფიდენციალურობა	123
4.3. დამუშავების გამჭვირვალობის წესები	125
4.3.1. ინფორმირება	127

4.3.2. შეტყობინება	130
4.4. წესები შესაბამისობის მხარდაჭერის შესახებ	131
4.4.1. წინასწარი შემოწმება	132
4.4.2. პერსონალურ მონაცემთა დაცვის პასუხისმგებელი პირები.....	133
4.4.3. ქცევის კოდექსები	134
 5. მონაცემთა სუბიექტის უფლებები და მათი რეალიზაცია	136
5.1. მონაცემთა სუბიექტის უფლებები.....	139
5.1.1. წვდომის უფლება.....	140
5.1.2. გასაჩივრების უფლება	149
5.2. დამოუკიდებელი ზედამხედველობა	152
5.3. სამართლებრივი დაცვა და სანქციები	158
5.3.1. დამმუშავებლის წინაშე დაყენებული მოთხოვნები	159
5.3.2. საზედამხედველო ორგანოში შეტანილი მოთხოვნები.....	161
5.3.3. სასამართლოში შეტანილი სარჩელი	162
5.3.4. სანქციები	169
 6. მონაცემთა საერთაშორისო გადაცემა.....	171
6.1. მონაცემთა საერთაშორისო გადაცემის არსი.....	172
6.2. მონაცემთა თავისუფალი გადაადგილება ევროპული კავშირის წევრ ქვეყნებს ან 108-ე კონვენციის ხელმომწერ მხარეებს შორის	174
6.3. მონაცემთა თავისუფალი გადაადგილება მესამე ქვეყნებში	175
6.3.1. მონაცემთა თავისუფალი გადაადგილება ადეკვატური დაცვის არსებობის საფუძველზე.....	176
6.3.2. მონაცემთა თავისუფალი გადაადგილება კონკრეტულ შემთხვევებში.....	178

6.4. მონაცემთა გაცემის შეზღუდვა მესამე ქვეყნებში	180
6.4.1. სახელშეკრულებო პირობები.....	181
6.4.2. სავალდებულო საკორპორაციო წესები (BCRs)	183
6.4.3. სპეციალური საერთაშორისო შეთანხმებები	184
7. მონაცემთა დაცვა პოლიციის სექტორსა და სისხლისსამართლებრივი მართლმსაჯულების სფეროში.....	190
7.1. ევროპის საბჭოს კანონმდებლობა მონაცემთა დაცვის შესახებ პოლიციის სექტორსა და სისხლისსამართლებრივი მართლმსაჯულების კონტექსტში	191
7.1.1. რეკომენდაცია პოლიციის შესახებ	192
7.1.2. ბუდაპეშტის კონვენცია კიბერდანაშაულის შესახებ.....	196
7.2. მონაცემთა დაცვის ევროპული კავშირის კანონმდებლობა პოლიციის და სისხლისსამართლებრივ საკითხებში	198
7.2.1. მონაცემთა დაცვის ჩარჩო გადანყვეტილება.....	198
7.2.2. მონაცემთა დაცვის მეტად სპეციფიკური სამართლებრივი ინსტრუმენტები პოლიციისა და კანონის აღმასრულებელი ორგანოების საერთაშორისო კოოპერაციისას.....	201
7.2.3. მონაცემთა დაცვა Europol-სა და Eurojust-ში	203
7.2.4. მონაცემთა დაცვა ევროპული კავშირის საერთო საინფორმაციო სისტემებში	208
8. მონაცემთა დაცვის სხვა სპეციალური ევროპული კანონები.....	218
8.1. ელექტრონული კომუნიკაციები	219
8.2. დასაქმების შესახებ მონაცემები	225
8.3. სამედიცინო მონაცემები	229
8.4. მონაცემთა დამუშავება სტატისტიკური მიზნებისთვის ..	232
8.5. ფინანსური მონაცემები.....	237
დამატებითი ლიტერატურა	240
სასამართლო გადაწყვეტილებები	244

აბრევიატურები

BCR (Binding Corporate Rule) – სავალდებულო საკორპორაციო წესი

CCTV (Closed Circuit Television) – ვიდეოთვალთვალის სისტემა

CETS (Council of Europe Treaty Series) – ევროპის საბჭოს შეთანხმებათა სერიები

Charter (Charter of Fundamental Rights of the European Union) – ძირითად უფლებათა ევროპული კავშირის ქარტია

CIS (Customs Information System) – საბაჟო საინფორმაციო სისტემა

CJEU – (Court of Justice of the European Union (Prior to December 2009, it was called the European Court of Justice, ECJ)) – მართლმსაჯულების ევროპული კავშირის სასამართლო (2009 წლის დეკემბრამდე იგი იწოდებოდა, როგორც მართლმსაჯულების ევროპული სასამართლო))

CoE (Council of Europe) – ევროპის საბჭო

Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe)) – 108-ე კონვენცია (პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ კონვენცია (ევროპის საბჭო))

CRM (Customer Relations Management) – მომხმარებელთან ურთიერთობის მენეჯმენტი

C-SIS (Central Schengen Information System) – შენგენის ცენტრალური საინფორმაციო სისტემა

EAW (European Arrest Warrant) – დაკავების ევროპული ბრძანება

EC (European Community) – ევროპული გაერთიანება

ECHR (European Convention on Human Rights) – ადამიანის უფლებათა ევროპული კონვენცია

ECtHR (European Court of Human Rights) – ადამიანის უფლებათა ევროპული სასამართლო

EDPS (European Data Protection Supervisor) – მონაცემთა დაცვის ევროპული ზედამხედველი

EEA (European Economic Area) – ევროპული ეკონომიკური ზონა

EFTA (European Free Trade Association) – თავისუფალი ვაჭრობის ევროპული ასოციაცია

ENISA (European Network and Information Security Agency) – ქსელისა და ინფორმაციის უსაფრთხოების ევროპული სააგენტო

ENU (Europol National Unit) – ევროპოლის შიდასახელმწიფოებრივი ერთეული

ESMA (European Securities and Markets Authority) – ფასიანი ქაღალდებისა და ბაზრის ევროპული ორგანო

eTEN (Trans-European Telecommunication Networks) – ტრანს-ევროპული სატელეკომუნიკაციო ქსელები

EU (European Union) – ევროპული კავშირი

EuroPriSe (European Privacy Seal) – პირადი ცხოვრების ევროპული ხარისხის ბეჭედი

eu-LISA (EU Agency for Large-scale IT Systems) – ფართომასშტაბიანი ინფორმაციული სისტემების ევროპული კავშირის სააგენტო

FRA (European Union Agency for Fundamental Rights) – ძირითადი უფლებების ევროპული კავშირის სააგენტო

GPS (Global Positioning System) – გლობალური პოზიციური სისტემა

JSB (Joint Supervisory Body) – საერთო საზედამხედველო ორგანო

NGO (Non-Governmental Organisation) – არასამთავრობო ორგანიზაცია

N-SIS (National Schengen Information System) – შენგენის შიდასახელმწიფოებრივი საინფორმაციო სისტემა

OECD (Organisation for Economic Co-operation and Development) – ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია

PIN (Personal Identification Number) – პერსონალური საიდენტიფიკაციო ნომერი

PNR (Passenger Name Record) – მგზავრის სახელის ჩანაწერი

SEPA (Single Euro Payments Area) – ევროთი ანგარიშსწორების საერთო სივრცე

SIS (Schengen Information System) შენგენის საინფორმაციო სისტემა

SWIFT (Society for Worldwide Interbank Financial Telecommunication) – მსოფლიო ბანკთაშორისი ფინანსური ტელეკომუნიკაციის საზოგადოება

TEU (Treaty on European Union) – ხელშეკრულება ევროპული კავშირის შესახებ

TFEU (Treaty on the Functioning of the European Union) – ხელშეკრულება ევროპული კავშირის ფუნქციონირების შესახებ

UDHR (Universal Declaration of Human Rights) – ადამიანის უფლებათა საყოველთაო დეკლარაცია

UN (United Nations) – გაერთიანებული ერები

VIS (Visa Information System) – სავიზო საინფორმაციო სისტემა

როგორ გამოვიყენოთ სახელმძღვანელო

მოცემული სახელმძღვანელო წარმოადგენს მონაცემთა დაცვის სფეროში ევროპულ კავშირსა და ევროპის საბჭოში მოქმედი კანონმდებლობის მიმოხილვას.

სახელმძღვანელო შექმნილია იმ მოქმედი სამართალმცოდნეების დასახმარებლად, რომლებიც არ არიან კომპეტენტურნი მონაცემთა დაცვის სფეროში; იგი განკუთვნილია იურისტებისთვის, მოსამართლეებისთვის ან სხვა პრაქტიკოსებისთვის, ასევე, სხვადასხვა სახის დაწესებულებებში მომუშავე პირებისთვის, მათ შორის, არასამთავრობო ორგანიზაციებისთვის (NGOs), რომელთა წინაშეც შესაძლებელია დაისვას მონაცემთა დაცვასთან დაკავშირებული სამართლებრივი საკითხები.

სახელმძღვანელო წარმოადგენს საორიენტაციო დოკუმენტს მონაცემთა დაცვის შესახებ როგორც ევროპული კავშირის კანონმდებლობის, ისე ადამიანის უფლებათა ევროპული კონვენციის მიხედვით და განმარტავს, თუ როგორ არის ეს სფერო რეგულირებული ევროპული კავშირის სამართლისა და ადამიანის უფლებათა ევროპული კონვენციის, ასევე, ევროპის საბჭოს კონვენციის – პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ (108-ე კონვენცია) და ევროპის საბჭოს სხვა ინსტრუმენტების მიხედვით. თითოეული თავი, პირველ რიგში, ადგენს მოქმედი სამართლებრივი დებულებების ცხრილს, სადაც მოცემულია ორი დამოუკიდებელი ევროპული სამართლებრივი სისტემიდან შერჩეული მნიშვნელოვანი პრეცედენტები. შემდგომ, წარმოდგენილია ორი დამოუკიდებელი ევროპული სამართლებრივი სისტემის შესაბამისი სამართლებრივი აქტები ერთმანეთის მიმდევრობით, რამდენადაც ისინი შესაძლებელია ეხებოდეს თითოეულ საკითხს. აღნიშნული მკითხველს აძლევს საშუალებას იხილოს, თუ როდის ხდება სამართლებრივი სისტემების თანხვედრა და გამიჯვნა.

ცხრილები, თითოეული თავის დასაწყისში, გამოყოფს საკითხებს, რომლებიც განხილულია მოცემულ თავში, ასახელებს რა, მოქმედ სამართლებრივ დებულებებს და სხვა შესაბამის მასალას, როგორიცაა სასამართლო პრაქტიკა. საკითხების რიგითობა შესაძლებელია მცირედ განსხვავდებოდეს მოცემულ

თავში არსებული ტექსტის სტრუქტურასთან შედარებით, თუ ეს სასურველია მასალის მოკლედ წარმოჩენისთვის. ცხრილი მოიცავს როგორც ევროპის საბჭოს, ისე ევროპული კავშირის კანონმდებლობას. აღნიშნული დაეხმარება მომხმარებლებს მოიძიონ მათთვის სასურველ საკითხთან დაკავშირებული საკვანძო ინფორმაცია, განსაკუთრებით მაშინ, თუ მათზე ვრცელდება მხოლოდ ევროპის საბჭოს კანონმდებლობა.

პირებმა ევროპული კავშირის არანევრი, თუმცა ევროპის საბჭოს ნევრი ქვეყნებიდან, ასევე, ადამიანის უფლებათა ევროპული კონვენციისა და 108-ე კონვენციის ხელმომწერი ქვეყნებიდან, ევროპის საბჭოს განყოფილებაზე პირდაპირი გადასვლით შეუძლიათ იხილონ მათთვის რელევანტური ინფორმაცია თავიანთი სახელმწიფოს მიხედვით. პირებმა ევროპული კავშირის ქვეყნებიდან უნდა გამოიყენონ ორივე განყოფილება, რამდენადაც მოცემულ ქვეყნებზე ვრცელდება ორივე სამართლებრივი სისტემა. მათ, ვისაც სჭირდებათ კონკრეტულ საკითხზე მეტი ინფორმაცია, დამატებითი სია, მეტად სპეციფიკურ თემებზე, მოცემულია ამ სახელმძღვანელოს დამატებითი ლიტერატურის განყოფილებაში.

ევროპის საბჭოს კანონმდებლობა წარმოდგენილია ადამიანის უფლებათა ევროპული სასამართლოს (ECtHR) გადაწყვეტილებების მოკლე ციტირებით. ისინი შერჩეულ იქნა სასამართლოს იმ მრავალ გადაწყვეტილებათაგან, რომლებიც შეეხება მონაცემთა დაცვის საკითხებს.

ევროპული კავშირის კანონმდებლობა მოცემულია იმ ნორმებით, რომელიც მიღებულ იქნა ხელშეკრულებებისა და ევროპული კავშირის ძირითად უფლებათა ქარტიის დებულებების თანახმად და განხილულია მართლმსაჯულების ევროპული კავშირის სასამართლოს პრეცედენტული სამართლის მიხედვით (2009 წლამდე მართლმსაჯულების ევროპული კავშირის სასამართლო (CJEU) ინოდებოდა, როგორც მართლმსაჯულების ევროპული სასამართლო (ECJ)).

სახელმძღვანელოში განმარტებული ან მითითებული პრეცედენტები წარმოადგენს ადამიანის უფლებათა ევროპული სასამართლოსა და მართლმსაჯულების ევროპული კავშირის სასამართლოს პრეცედენტების მნიშვნელოვან მაგალითებს. სახელ-

მძღვანელოს ბოლოს მოცემული საორიენტაციო დებულებები განკუთვნილია მკითხველის დასახმარებლად, სასამართლო გადაწყვეტილების ინტერნეტის მეშვეობით მოძიებისთვის.

დამატებით, სავარაუდო შინაარსის მქონე პრაქტიკული მაგალითები მოცემულია გრაფებში ნაცრისფერ ფონზე, რათა თვალსაჩინო გახდეს მონაცემთა დაცვის ევროპული წესების პრაქტიკაში გამოყენების საკითხი, კერძოდ, იმ შემთხვევაში, როდესაც არ არსებობს ადამიანის უფლებათა ევროპული სასამართლოსა და მართლმსაჯულების ევროპული კავშირის სასამართლოს შესაბამისი გადაწყვეტილებები მოცემულ საკითხზე. გრაფები, რომლებიც მოცემულია, ასევე, შეიცავს სასამართლო გადაწყვეტილებებისგან განსხვავებულ, სხვა წყაროებიდან აღებული მაგალითებს, როგორიცაა კანონმდებლობა.

სახელმძღვანელო იწყება იმ ორი სამართლებრივი სისტემის მნიშვნელობის მოკლე აღწერით, რომელიც დადგენილია ადამიანის უფლებათა ევროპული კონვენციითა და ევროპული კავშირის კანონმდებლობით (პირველი თავი). მე-2-მე-8 თავები მოიცავს შემდეგ საკითხებს:

- მონაცემთა დაცვის ტერმინოლოგია;
- მონაცემთა დაცვის ევროპული სამართლის საკვანძო პრინციპები;
- მონაცემთა დაცვის ევროპული სამართლის წესები;
- მონაცემთა სუბიექტის უფლებები და მათი რეალიზაცია;
- მონაცემთა საერთაშორისო გადაცემა;
- მონაცემთა დაცვა პოლიციის სექტორსა და სისხლისსამართლებრივი მართლმსაჯულების სფეროში;
- მონაცემთა დაცვის სხვა სპეციალური ევროპული კანონები.

1. მონაცემთა დაცვის ევროპული სამართლის კონტექსტი და საფუძვლები

ევროპული კავშირი	განხილული საკითხები	ევროპის საბჭო
უფლება მონაცემთა დაცვაზე		
დირექტივა 95/46/EC პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ (მონაცემთა დაცვის დირექტივა). OJ 1995 L 281		ადამიანის უფლებათა ევროპული კონვენცია (ECHR), მე-8 მუხლი (პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და მიმოწერის დაცვის უფლება). პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ კონვენცია (108-ე კონვენცია).
მანონასწორებელი უფლებები		
მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები C-92/09 და C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 2010 წელი	ზოგადად	
მართლმსაჯულების ევროპული კავშირის სასამართლო, C-73/07, Tietosuoja ja valtuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, 2008 წელი	გამოხატვის თავისუფლება	ადამიანის უფლებათა ევროპული სასამართლო, Axel Springer AG v. Germany, 2012 ადამიანის უფლებათა ევროპული სასამართლო, Mosley v. the United Kingdom, 2011 წელი
	ხელოვნებისა და მეცნიერების თავისუფლება	ადამიანის უფლებათა ევროპული სასამართლო, Vereinigung bildender Künstler v. Austria, 2007 წელი
მართლმსაჯულების ევროპული კავშირის სასამართლო, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 წელი	საკუთრების დაცვა	
მართლმსაჯულების ევროპული კავშირის სასამართლო, C-28/08 P, European Commission v. The Bavarian Lager Co. Ltd, 2010 წელი	დოკუმენტებთან წვდომა	ადამიანის უფლებათა ევროპული სასამართლო, Társaság a Szabadságjogokért v. Hungary, 2009 წელი

1.1. უფლება მონაცემთა დაცვაზე

საკვანძო დებულებები

- ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის თანახმად, პერსონალურ მონაცემთა შეგროვებისა და გამოყენებისგან დაცვის უფლება წარმოადგენს პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და მიმონერის დაცვის უფლების ნაწილს.
- ევროპის საბჭოს 108-ე კონვენცია არის პირველი საერთაშორისო სამართლებრივი ინსტრუმენტი, რომელიც ეხება უშუალოდ მონაცემთა დაცვას.
- ევროპული კავშირის კანონმდებლობის მიხედვით, მონაცემთა დაცვა პირველად მოწესრიგდა მონაცემთა დაცვის დირექტივით.
- ევროპული კავშირის კანონმდებლობის მიხედვით, მონაცემთა დაცვა აღიარებულ იქნა, როგორც ძირითადი უფლება.

ფიზიკური პირის პირად სფეროში სხვების, განსაკუთრებით კი, სახელმწიფოს ჩარევისგან დაცვის უფლება საერთაშორისო სამართლებრივ დოკუმენტში პირველად განვიხილეთ იქნა გაერთიანებული ერების (UN) 1948 წლის ადამიანის უფლებათა საყოველთაო დეკლარაციის (UDHR) მე-12 მუხლში, პირადი და ოჯახური ცხოვრების დაცვის სახით.¹ ევროპაში ადამიანის უფლებათა საყოველთაო დეკლარაციამ გავლენა იქონია ადამიანის უფლებათა დაცვის სხვა ინსტრუმენტების წარმოქმნაზე.

1.1.1. ადამიანის უფლებათა ევროპული კონვენცია

ევროპის საბჭო ფორმირებულ იქნა მეორე მსოფლიო ომის შემდგომ, რათა მოეხდინა ევროპის სახელმწიფოების გაერთიანება კანონის უზენაესობის, დემოკრატიის, ადამიანის უფლებათა და სოციალური განვითარების განმტკიცებისთვის. ამ მიზ-

¹ გაერთიანებული ერები, ადამიანის უფლებათა საყოველთაო დეკლარაცია, 1948 წლის 10 დეკემბერი.

ნით, ევროპის საბჭომ 1950 წელს მიიღო ადამიანის უფლებათა ევროპული კონვენცია, რომელიც ძალაში 1953 წელს შევიდა.

სახელმწიფოებს გააჩნიათ საერთაშორისო ვალდებულება კონვენციასთან შესაბამისობის მხრივ. ამჟამად ევროპის საბჭოს ყველა წევრ ქვეყანას ინტეგრირებული ან ადაპტირებული აქვს კონვენციის დებულებები შიდასახელმწიფოებრივ კანონმდებლობაში, რომელიც ავალდებულებს მათ იმოქმედონ კონვენციით მოცემული დებულებების შესაბამისად.

ხელმოწერი მხარეების მიერ, კონვენციით ნაკისრი ვალდებულებების უზრუნველსაყოფად, 1959 წელს საფრანგეთში, კერძოდ, სტრასბურგში შეიქმნა ადამიანის უფლებათა ევროპული სასამართლო. სასამართლო უზრუნველყოფს სახელმწიფოების მიერ კონვენციით ნაკისრი თავიანთი ვალდებულებების შესრულებას ინდივიდების, ინდივიდთა ჯგუფების, არასამთავრობო ორგანიზაციების ან იურიდიული პირების მიერ კონვენციის შესაძლო დარღვევებთან დაკავშირებით შეტანილი საჩივრების განხილვის მეშვეობით. 2013 წელს ევროპის საბჭოში გაერთიანებული იყო 47 წევრი ქვეყანა, მათგან 28 ქვეყანა არის ამავდროულად ევროპული კავშირის წევრი. აუცილებელი არ არის, რომ განმცხადებელი სასამართლოში იყოს რომელიმე წევრი ქვეყნის ეროვნების მქონე. სასამართლო, ასევე, იხილავს დავებს სახელმწიფოებს შორის, რომელიც შეტანილია ევროპის საბჭოს რომელიმე წევრი ქვეყნის მიერ სხვა წევრი ქვეყნის წინააღმდეგ.

პერსონალური მონაცემების დაცვის უფლება წარმოადგენს იმ უფლებათა ნაწილს, რომელიც დაცულია ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლით, რის მიხედვითაც უზრუნველყოფილია პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და მიმოწერის დაცვის უფლება და განსაზღვრულია პირობები, როდესაც დასაშვებია ამ უფლების შეზღუდვა.²

სასამართლო პრაქტიკის ფარგლებში, ადამიანის უფლებათა ევროპულმა სასამართლომ განიხილა მრავალი საქმე, სადაც ნამოიჭრა მონაცემთა დაცვის საკითხი, მათ შორის, არა მხოლოდ

2 ევროპის საბჭო, ადამიანის უფლებათა ევროპული კონვენცია, CETS No. 005, 1950 წელი.

ისეთი შემთხვევები, როგორცაა პირად კომუნიკაციაში ჩარევა,³ თვალთვალის სხვადასხვა ფორმა⁴ და სახელმწიფო ორგანოების მხრიდან პერსონალური მონაცემების შენახვისგან დაცვა.⁵ სასამართლომ განმარტა, რომ კონვენციის მე-8 მუხლი სახელმწიფოებს ავალდებულებს არა მარტო თავი შეიკავონ ნებისმიერი მოქმედებისგან, რამაც შესაძლოა დაარღვიოს კონვენციით აღიარებული ეს უფლება, არამედ მათ, გარკვეული პირობების არსებობისას, გააჩნიათ პოზიტიური ვალდებულება აქტიურად დაიცვან პირადი და ოჯახური ცხოვრების უფლება.⁶ აღნიშნულ საქმეთა უმეტესობა დეტალურად იქნება განხილული შესაბამის თავებში.

1.1.2. ევროპის საბჭოს 108-ე კონვენცია

1960-იან წლებში ინფორმაციული ტექნოლოგიების წარმოშობასთან ერთად, გაჩნდა იმ დეტალური წესების მზარდი მოთხოვნილება, რომელიც დაიცავდა ფიზიკური პირების პერსონალურ მონაცემებს. 1970-იანი წლების შუა პერიოდისთვის, ევროპის საბჭოს მინისტრთა კომიტეტმა მიიღო მრავალი რეზოლუცია პერსონალურ მონაცემთა დაცვის შესახებ, ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლთან მიმართებით.⁷ 1981 წელს, პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ კონვენცია (108-ე

3 მაგ. იხ. ადამიანის უფლებათა ევროპული სასამართლო, *Malone v. United Kingdom*, No. 8691/79, 2 აგვისტო 1984 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *Copland v. United Kingdom*, No. 62617/00, 3 აპრილი 2007 წელი.

4 მაგ. იხ. ადამიანის უფლებათა ევროპული სასამართლო, *Klass and Others v. Germany*, No. 5029/71, 6 სექტემბერი 1978 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *Uzun v. Germany*, No. 35623/05, 2 სექტემბერი 2010 წელი.

5 მაგ. იხ. ადამიანის უფლებათა ევროპული სასამართლო, *Leander v. Sweden*, No. 9248/81, 26 მარტი 1987 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *S. and Marper v. the United Kingdom*, No. 30562/04, 4 დეკემბერი 2008 წელი.

6 მაგ. იხ. ადამიანის უფლებათა ევროპული სასამართლო, *I. v. Finland*, No. 20511/03, 17 ივლისი 2008 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *K.U. v. Finland*, No. 2872/02, 2 დეკემბერი 2008 წელი.

7 ევროპის საბჭო, მინისტრთა კომიტეტი (1973), რეზოლუცია (73) 22 კერძო სექტორში მონაცემთა ელექტრონულ საცავებთან დაკავშირებით ფიზიკური პირების პირადი ცხოვრების დაცვის შესახებ, 26 სექტემბერი 1973 წელი; ევროპის საბჭო, მინისტრთა კომიტეტი (1974), რეზოლუცია (74) 29 საჯარო სექტორში ელექტრონულ მონაცემთა საცავებთან დაკავშირებით ფიზიკური პირების პირადი ცხოვრების დაცვის შესახებ, 20 სექტემბერი 1974 წელი.

კონვენცია)⁸ მზად იყო ხელმოწერისთვის. 108-ე კონვენცია იყო და კვლავ რჩება ერთადერთ საერთაშორისო სამართლებრივ ინსტრუმენტად მონაცემთა დაცვის სფეროში.

108-ე კონვენცია ვრცელდება ყველა სახის მონაცემთა დამუშავებაზე, განხორციელებული როგორც კერძო, ისე საჯარო სექტორის მიერ, როგორცაა მონაცემთა დამუშავება სამართალდამცავი და კანონის აღმასრულებელი ორგანოების მიერ. იგი იცავს ფიზიკურ პირებს უფლების დარღვევისგან, რომელიც შესაძლებელია თან სდევდეს პერსონალური მონაცემების შეგროვებასა და დამუშავებას და, ამავდროულად, მიმართულია პერსონალურ მონაცემთა საერთაშორისო გადაცემის მოწესრიგებისკენ. პერსონალურ მონაცემთა შეგროვებისა და დამუშავების მხრივ, ის პრინციპები, რომლებიც მოცემულია კონვენციაში, ეხება მონაცემთა სამართლიან და კანონიერ შეგროვებასა და ავტომატურ დამუშავებას, შენახვას კონკრეტული ლეგიტიმური მიზნებისთვის და მოცემულ მიზანთან შეუთავსებელი მიზნით გამოყენების დაუშვებლობას, ასევე, მხოლოდ იმ ვადით შენახვას რაც წარმოადგენს აუცილებლობას. პრინციპები, ასევე, ეხება მონაცემთა ხარისხს, კერძოდ კი იმას, რომ მონაცემები უნდა იყოს ადეკვატური, შესაბამისი, ზუსტი და არ უნდა იყოს ჭარბი (პროპორციულობა).

პერსონალურ მონაცემთა შეგროვებისა და დამუშავებისთვის დამატებითი გარანტიების უზრუნველსაყოფად, შესაბამისი დამცავი სამართლებრივი მექანიზმის არსებობის გარეშე, კონვენცია დაუშვებლად მიიჩნევს განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავებას, როგორცაა პიროვნების რასობრივი კუთვნილება, პოლიტიკური შეხედულებები, ჯანმრთელობის მდგომარეობის შესახებ მონაცემები, რელიგიური შეხედულებები, სქესობრივი ცხოვრება და სისხლის-სამართლებრივ საქმესთან დაკავშირებული ჩანაწერები.

კონვენცია, ასევე, აღიარებს ფიზიკური პირის უფლებას იცოდეს თუ რა ინფორმაცია არის მის შესახებ შენახული და, საჭიროების შემთხვევაში, მოითხოვოს მათი შესწორება. კონვენციით დადგენილი უფლებების შეზღუდვა დასაშვებია მხოლოდ

8 ევროპის საბჭო, პერსონალური მონაცემების ავტომატური დამუშავებისა და ფიზიკურ პირთა დაცვის შესახებ კონვენცია, CETS No. 108, 1981 წელი.

აღმატებული ინტერესის არსებობისას, როგორცაა სახელმწიფო უსაფრთხოება ან თავდაცვა.

მიუხედავად იმისა, რომ კონვენცია ადგენს პერსონალურ მონაცემთა თავისუფალი გადაადგილების შესაძლებლობას მის ხელმომწერ სახელმწიფოთა შორის, იგი განსაზღვრავს გარკვეულ შეზღუდვებსაც მონაცემთა იმ სახელმწიფოებში გადაცემასთან დაკავშირებით, სადაც სამართლებრივი მონესრიგება არ განსაზღვრავს ადეკატურ დაცვას.

108-ე კონვენციით მოცემული ძირითადი პრინციპებისა და ნესების შემდგომი დახვეწისთვის, არასავალდებულო ხასიათის რამოდენიმე რეკომენდაცია იქნა მიღებული ევროპის საბჭოს მინისტრთა კომიტეტის მიერ (იხ. მე-6-მე-8 თავები).

ევროპული კავშირის ყველა წევრ ქვეყანას რატიფიცირებული აქვს 108-ე კონვენცია. 1999 წელს, 108-ე კონვენციაში შეტანილ იქნა ცვლილებები ევროპული კავშირის ხელმომწერ მხარედ განსაზღვრისთვის.⁹ 2001 წელს მიღებული იქნა 108-ე კონვენციის დამატებითი ოქმი, რომელიც განსაზღვრავს დებულებებს მონაცემთა საერთაშორისო გადაცემის თაობაზე იმ სახელმწიფოებში, რომლებიც არ არიან კონვენციის ხელმომწერი მხარეები, ე.წ. მესამე ქვეყნები, და, ასევე, შეიცავს დებულებებს მონაცემთა დაცვის შიდასახელმწიფოებრივი საზედამხედველო ორგანოების სავალდებულო შექმნის შესახებ.¹⁰

შემდგომი პერსპექტივები

108-ე კონვენციის მოდერნიზების შესახებ გადწყვეტილების თანახმად, 2011 წელს განხორციელებულმა საჯარო კონსულტაციებმა შესაძლებელი გახადა დადგენილი ყოფილიყო ამ სამუშაოს ორი ძირითადი მიზანი: პირადი ცხოვრების დაცვის გაძლიერება ციფრულ სივრცეში და კონვენციის მაკონტროლე-

⁹ ევროპის საბჭო, პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ კონვენციის (ETS No. 108) ცვლილებები, რომელიც უფლებას აძლევს ევროპულ გაერთიანებას შეერთების თაობაზე, მიღებული მინისტრთა კომიტეტის მიერ სტრასბურგში, 1999 წლის 15 ივნისს; 108-ე კონვენციის შეცვლილი ვერსიის 23-ე მუხლის მე-2 პუნქტი.

¹⁰ ევროპის საბჭო, პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ კონვენციის დამატებითი ოქმი ზედამხედველი ორგანოებისა და მონაცემთა საერთაშორისო გადაცემის შესახებ, CETS No. 181, 2001 წელი.

ბელი მექანიზმის გაძლიერება.

108-ე კონვენცია ღიაა ხელმოწერისთვის ევროპის საბჭოს არაწევრი ქვეყნებისთვისაც, მათ შორის, არაევროპული ქვეყნებისთვის. კონვენციის, როგორც უნივერსალური სტანდარტის პოტენციალი და მისი ღია ხასიათი შესაძლოა გახდეს მონაცემთა დაცვის გლობალურ დონეზე განვითარების საფუძველი.

ამჟამად, 108-ე კონვენციის ხელმომწერი 46 სახელმწიფოდან 45 ევროპის საბჭოს წევრია. ურუგვაი, პირველი არაევროპული სახელმწიფო, 2013 წლის აგვისტოში გახდა კონვენციის ხელმომწერი მხარე, ხოლო მაროკო, რომელიც მოწვეულ იქნა მინისტრთა კომიტეტის მიერ 108-ე კონვენციის ხელმოწერის მიზნით, არის ამ პროცესის ფორმალიზების ეტაპზე.

1.1.3. მონაცემთა დაცვის ევროპული კავშირის სამართალი

ევროპული კავშირის კანონმდებლობა შედგება ხელშეკრულებებისა და ევროპული კავშირის „მეორადი“ კანონმდებლობისგან. ხელშეკრულებები, კერძოდ, ხელშეკრულება ევროპული კავშირის (TEU) შესახებ და ხელშეკრულება ევროპული კავშირის ფუნქციონირების (TFEU) შესახებ, დამტკიცებულ იქნა ევროპული კავშირის ყველა წევრი ქვეყნის მიერ და იწოდება, როგორც ევროპული კავშირის „პირველადი“ კანონმდებლობა. ევროპული კავშირის რეგულაციები, დირექტივები და გადაწყვეტილებები მიიღება ევროპული კავშირის იმ ინსტიტუტების მიერ, რომლებსაც ხელშეკრულების საფუძველზე მინიჭებული აქვთ საამისო უფლებამოსილება; ისინი, ძირითადად, მოიხსენიება, როგორც ევროპული კავშირის „მეორადი“ კანონმდებლობა.

მონაცემთა დაცვის შესახებ ევროპული კავშირის მთავარი სამართლებრივი ინსტრუმენტი არის ევროპული პარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ (მონაცემთა დაცვის დირექტივა).¹¹ იგი მიღებულ იქნა 1995 წელს, იმ დროს, როდესაც ევროპული კავშირის რამოდენიმე წევრ ქვე-

¹¹ მონაცემთა დაცვის დირექტივა, OJ 1995 L 281, გვ. 31.

ყანას უკვე მიღებული ჰქონდა მონაცემთა დაცვის შესახებ კანონები. შიდა ბაზრის ფარგლებში საქონლის, კაპიტალის, მომსახურებისა და ადამიანების თავისუფალი გადაადგილება მოითხოვდა მონაცემთა თავისუფალ გადაადგილებასაც, რაც ვერ განხორციელდებოდა იქამდე, სანამ ევროპული კავშირის წევრი ქვეყნები არ დაანესებდნენ მონაცემთა დაცვის უნიფიცირებულ მაღალ სტანდარტს.

რამდენადაც მონაცემთა დაცვის დირექტივის მიღების მიზანი იყო შიდასახელმწიფოებრივ დონეზე მონაცემთა დაცვის კანონთა ჰარმონიზება,¹² დირექტივა, გარკვეულწილად, ითვალისწინებს მისი მიღების დროს არსებული მონაცემთა დაცვის შიდასახელმწიფოებრივი კანონების სპეციფიკას. მართლმსაჯულების ევროპული კავშირის სასამართლოს აზრით, „დირექტივა 95/46 განკუთვნილია იმისთვის, რათა ევროპული კავშირის ყველა წევრ ქვეყანაში უზრუნველყოს ფიზიკური პირების უფლებებისა და თავისუფლებების დაცვის დონის თანაბრობა პერსონალურ მონაცემთა დამუშავებასთან მიმართებით. ამ სფეროში მოქმედი შიდასახელმწიფოებრივი კანონმდებლობის ჰარმონიზებამ არ უნდა გამოიწვიოს დადგენილი დაცვის დონის შემცირება, არამედ, უნდა უზრუნველყოს დაცვის მაღალი დონის დამკვიდრება ევროპულ კავშირში. შესაბამისად, აღნიშნული შიდასახელმწიფოებრივი კანონების ჰარმონიზება არ არის დაყვანილი მხოლოდ მინიმალურ ჰარმონიზაციამდე, არამედ იგი მიზნად ისახავს მის სრულ ჰარმონიზებას.“¹³ შესაბამისად, დირექტივის იმპლემენტაციისას, ევროპული კავშირის წევრ ქვეყნებს გააჩნიათ მოქმედების შეზღუდული არეალი.

მონაცემთა დაცვის დირექტივა შექმნილია პირადი ცხოვრების უფლების იმ პრინციპების გამყარებისა და განვრცობისთვის, რომლებიც უკვე მოცემულია 108-ე კონვენციით. ის ფაქტი, რომ 1995 წელს ევროპული კავშირის თხუთმეტივე წევრი იყო იმავედროულად 108-ე კონვენციის ხელმომწერი მხარე, გამოორიცხავს ურთიერთსაწინააღმდეგო წესების არსებობას აღნიშნულ ორ სამართლებრივ ინსტრუმენტში. თუმცა, მონაცემთა

12 მაგ. იხ. მონაცემთა დაცვის დირექტივა, პრეამბულის პირველი, მე-4, მე-7 და მე-8 პუნქტები.

13 მართლმსაჯულების ევროპული კავშირის სასამართლო, 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 (FECEDM) v. Administración del Estado, 24 ნოემბერი 2011 წელი, პარაგ. 28-29.

დაცვის დირექტივა, მსგავსად 108-ე კონვენციის მე-11 მუხლისა, საშუალებას იძლევა მიღებულ იქნეს დაცვის დამატებითი ინსტრუმენტები, კერძოდ, დამოუკიდებელი საზედამხედველო ორგანოს წარდგენამ, როგორც მექანიზმის, რომელიც უზრუნველყოფს მონაცემთა დაცვის წესების შესრულების გაუმჯობესებას, დაამტკიცა, რომ შეაქვს მნიშვნელოვანი წვლილი მონაცემთა დაცვის ევროპული კანონმდებლობის ეფექტურ მოქმედებაში. (შედეგად, ეს დებულება გადმოტანილ იქნა ევროპის საბჭოს სამართლებრივ სისტემაში 2001 წელს, 108-ე კონვენციის დამატებითი ოქმის მიღების სახით.)

მონაცემთა დაცვის დირექტივის ტერიტორიული მოქმედება სცდება ევროპული კავშირის 28 სახელმწიფოს, მოიცავს რა, მის არანევრ ქვეყნებსაც, რომლებიც არიან ევროპის ეკონომიკური ზონის (EEA)¹⁴ წევრები, კერძოდ, ისლანდია, ლიხტენშტაინი და ნორვეგია.

ლუქსემბურგის მართლმსაჯულების ევროპული კავშირის სასამართლოს, განსჯადობის მიხედვით, შეუძლია დაადგინოს შეასრულა თუ არა წევრმა ქვეყანამ მონაცემთა დაცვის დირექტივით გათვალისწინებული ვალდებულებები და გამოიტანოს წინასწარი გადაწყვეტილებები (დასკვნები) დირექტივის მოქმედებისა და ინტერპრეტაციის თაობაზე წევრ ქვეყნებში მისი ეფექტური და უნიფიცირებული მოქმედების უზრუნველსაყოფად. მონაცემთა დაცვის დირექტივის გავრცელების მხრივ, მნიშვნელოვან გამოწვევის წარმოადგენს ე.წ. პირადი მიზნები, კერძოდ პერსონალურ მონაცემთა დამუშავება მხოლოდ პირადი მიზნებისთვის.¹⁵ ამგვარი დამუშავება ძირითადად მიიჩნევა ინდივიდის პირადი თავისუფლების შემადგენელ ნაწილად.

მონაცემთა დაცვის დირექტივის მიღების პერიოდისთვის ევროპული კავშირის ძალაში შესული „პირველადი“ კანონმდებლობის შესაბამისად, დირექტივის მატერიალური ფარგლები შეზღუდულია შიდა ბაზრის საკითხებამდე. მისი გავრცელების ფარგლებს გარეთ დარჩენილი ყველაზე მნიშვნელოვანი საკითხებია პოლიციის საქმიანობა და სისხლისსამართლებრივ სფეროში თანამშრომლობა. ამ კუთხით მონაცემთა დაცვა მოწესრიგებულია სხვადასხვა სამართლებრივი ინსტრუმენტებით,

¹⁴ შეთანხმება ევროპული ეკონომიკური ზონის შესახებ, OJ 1994 L 1, რომელიც ძალაში შევიდა 1994 წლის 1 იანვარს.

¹⁵ მონაცემთა დაცვის დირექტივა, მე-3 მუხლის მე-2 პუნქტის მე-2 აბზაცი.

რომლებიც დეტალურად არის აღწერილი მე-7 თავში.

რამდენადაც მონაცემთა დაცვის დირექტივა ვრცელდება მხოლოდ ევროპული კავშირის წევრ ქვეყნებში, საჭირო გახდა დამატებითი სამართლებრივი ინსტრუმენტი, რათა მონაცემთა დაცვა გარანტირებული ყოფილიყო ევროპული კავშირის ინსტიტუტებისა და ორგანოების მიერ. ამ მიზანს ემსახურება რეგულაცია (EC) No. 45/2001 გაერთიანების დაწესებულებებისა და ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ (ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის რეგულაცია).¹⁶

ამასთან, იმ სფეროებშიც კი, რომლებზეც ვრცელდება მონაცემთა დაცვის დირექტივა, სხვა უფლებებთან განონასწორების დროს, სასურველი სიზუსტისთვის, ხშირად საჭიროა მონაცემთა დაცვის მეტად დეტალური დებულებები. არსებობს შესაბამისი ორი მაგალითი, დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პირადი ცხოვრების დაცვისა და პერსონალურ მონაცემთა დამუშავების შესახებ (პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების დირექტივა)¹⁷ და დირექტივა 2006/24/EC საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების მომსახურებისას ან საჯარო კომუნიკაციების ქსელებში წარმოშობილი ან დამუშავებული მონაცემების შენახვის შესახებ (მონაცემთა შენახვის დირექტივა), რომელსაც შეაქვს ცვლილებები 2002/58/EC დირექტივაში.¹⁸ სხვა მაგალითები განხილული იქნება მე-8 თავში. მათი დებულებები შესაბამისობაში უნდა იყოს მონაცემთა დაცვის დირექტივასთან.

16 ევროპული პარლამენტისა და საბჭოს 2000 წლის 18 დეკემბრის რეგულაცია (EC) No. 45/2001 გაერთიანების დაწესებულებებისა და ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ, OJ 2001 L 8.

17 ევროპული პარლამენტისა და საბჭოს 2002 წლის 12 ივლისის დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პირადი ცხოვრების დაცვისა და პერსონალურ მონაცემთა დამუშავების შესახებ (პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების დირექტივა), OJ 2002 L 201.

18 ევროპული პარლამენტისა და საბჭოს 2006 წლის 15 მარტის დირექტივა 2006/24/EC საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების მომსახურებისას ან საჯარო კომუნიკაციების ქსელებში წარმოშობილი ან დამუშავებული მონაცემების შენახვის შესახებ (მონაცემთა შენახვის დირექტივა), რომელსაც ცვლილებები შეაქვს 2002/58/EC დირექტივაში, OJ 2006 L105, გამოცხადდა ძალადაკარგულად 2014 წლის 8 აპრილს.

ძირითად უფლებათა ევროპული კავშირის ქარტია (Charter)

ევროპული გაერთიანების სადამფუძნებლო ხელშეკრულებები არ შეიცავს რაიმე მითითებას ადამიანის უფლებების ან მათი დაცვის შესახებ. მას შემდეგ, რაც მართლმსაჯულების ევროპულ სასამართლოში განსახილველად წარდგენილ იქნა საქმეები ევროპული კავშირის კანონმდებლობის მოქმედების ფარგლებში ადამიანის უფლებათა შესაძლო დარღვევის შესახებ, თავის მხრივ, აღნიშნულმა განავითარა ახალი მიდგომები. ფიზიკური პირებისთვის დაცვის მინიჭების მიზნით, მან მოახდინა ძირითადი უფლებების ე.წ. ევროპული სამართლის ზოგად პრინციპებში ჩართვა. მართლმსაჯულების ევროპული კავშირის სასამართლოს თანახმად, მოცემული ზოგადი პრინციპები თანხვედრაშია შიდასახელმწიფოებრივი კონსტიტუციებითა და ადამიანის უფლებათა შეთანხმებებით მოცემულ ადამიანის უფლებათა დაცვის დებულებებთან, კერძოდ, ადამიანის უფლებათა ევროპულ კონვენციაში მოცემულ დებულებებთან. მართლმსაჯულების ევროპული კავშირის სასამართლომ განაცხადა, რომ იგი უზრუნველყოფს ევროპული კავშირის კანონმდებლობის შესაბამისობას ამ პრინციპებთან.

იმის აღიარებით, რომ ევროპული კავშირის პოლიტიკას შესაძლოა გავლენა ჰქონოდა ადამიანის უფლებებზე, ხოლო მოქალაქეებს მეტად დაახლოვებულად ეგრძნოთ თავი ევროპულ კავშირთან, 2000 წელს ევროპულმა კავშირმა წარადგინა ძირითად უფლებათა ევროპული კავშირის ქარტია. აღნიშნული ქარტია ახდენს ევროპელი მოქალაქეების მთელი რიგი სამოქალაქო, პოლიტიკური, ეკონომიკური და სოციალური უფლებების ინკორპორაციას, ევროპული კავშირის წევრი ქვეყნებისთვის საერთო კონსტიტუციური ტრადიციებისა და წევრი ქვეყნების საერთაშორისო ვალდებულებების სინთეზის მეშვეობით. ქარტიაში მოცემული უფლებები არის დაყოფილი ექვს ნაწილად: ღირსება, თავისუფლებები, თანასწორობა, სოლიდარობა, მოქალაქეთა უფლებები და მართლმსაჯულება.

თავდაპირველად, როგორც მხოლოდ პოლიტიკური დოკუმენტი, ქარტიამ, როგორც ევროპული კავშირის „პირველადი“

კანონმდებლობის ნაწილმა სამართლებრივად სავალდებულო ძალა შეიძინა¹⁹ 2009 წლის 1 დეკემბერს ლისაბონის ხელშეკრულების ძალაში შესვლით.²⁰

ევროპული კავშირის „პირველადი“ კანონმდებლობა, ასევე, მოიცავს ევროპული კავშირის ძირითად უფლებამოსილებას – გამოსცეს ნორმატიული აქტები მონაცემთა დაცვის საკითხებზე (ევროპული კავშირის ფუნქციონირების შესახებ შეთანხმების მე-16 მუხლი).

ქარტია არა მარტო უზრუნველყოფს პირადი და ოჯახური ცხოვრების პატივისცემას (მე-7 მუხლი), არამედ ადგენს უფლებას მონაცემთა დაცვაზეც (მე-8 მუხლი), განსაკუთრებით ამაღლებს მისი დაცვის დონეს და განსაზღვრავს ძირითად უფლებად ევროპული კავშირის სამართალში. ევროპული კავშირის ინსტიტუტები, ისევე როგორც მისი წევრი ქვეყნები, ვალდებული არიან დაიცვან და უზრუნველყონ ამ უფლების პატივისცემა, რომელიც ვრცელდება ევროპული კავშირის წევრ ქვეყნებზე გაერთიანების კანონმდებლობის იმპლემენტირებისას (ქარტიის 51-ე მუხლი). მონაცემთა დაცვის დირექტივის მიღებიდან რამოდენიმე წლის შემდეგ ფორმულირებული ქარტიის მე-8 მუხლი გაგებულ უნდა იქნეს, როგორც მის მიღებამდე არსებული მონაცემთა დაცვის ევროპული კავშირის კანონმდებლობის განმტკიცებად. ამავდროულად, ქარტია, მე-8 მუხლის პირველი პუნქტით, არა მარტო მკაფიოდ ადგენს უფლებას მონაცემთა დაცვაზე, არამედ, ამავე მუხლის მეორე პუნქტით განსაზღვრავს მონაცემთა დაცვის საკვანძო პრინციპებს. დასასრულს, ქარტიის მე-8 მუხლის მესამე პუნქტი ადგენს, რომ აღნიშნული პრინციპების იმპლემენტირება უნდა უზრუნველყოს დამოუკიდებელმა საზედამხედველო ორგანომ.

19 ევროპული კავშირი (2012), ძირითად უფლებათა ევროპული კავშირის ქარტია, OJ 2012 C 326.

20 იხ. კონსოლიდირებული ვერსიები ევროპული გაერთიანების თაობაზე (2012), ევროპული კავშირის შესახებ OJ 2012 C 326 და ევროპული გაერთიანების (2012) შესახებ ხელშეკრულებები, ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულება, OJ 2012 C 326.

შემდგომი პერსპექტივები

2012 წლის იანვარში, ევროპულმა კომისიამ წარადგინა მონაცემთა დაცვის რეფორმის პაკეტი, განაცხადა რა, რომ სწრაფი ტექნოლოგიური პროგრესისა და გლობალიზაციის გათვალისწინებით მონაცემთა დაცვის არსებული წესები საჭიროებდა მოდერნიზებას. რეფორმის პაკეტი შედგება მონაცემთა დაცვის ძირითადი რეგულაციის პროექტისგან,²¹ რომელიც განკუთვნილია როგორც მონაცემთა დაცვის დირექტივის, ასევე მონაცემთა დაცვის ახალი ძირითადი დირექტივის²² ჩასანაცვლებლად, რომელიც უზრუნველყოფს მონაცემთა დაცვას სისხლისმამართლებრივ საქმეებზე პოლიციისა და სამართლებრივი თანამშრომლობის სფეროებში. აღნიშნული სახელმძღვანელოს გამოცემისას მიმდინარეობდა რეფორმის პაკეტზე მუშაობა.

1.2. მანონასწორებელი უფლებები

საკვანძო დებულება

- უფლება მონაცემთა დაცვაზე არ არის აბსოლუტური უფლება; იგი უნდა იქნეს დაბალანსებული სხვა უფლებებთან მიმართებაში.

ქარტიის მე-8 მუხლის მიხედვით პერსონალურ მონაცემთა დაცვის ძირითადი უფლება „არ არის აბსოლუტური უფლება, იგი უნდა იქნეს განხილული საზოგადოებაში მისი დანიშნულების მიხედვით.“²³ შესაბამისად, ქარტიის 52-ე მუხლის პირველი პუნქ-

21 ევროპული კომისია (2012), ევროპული პარლამენტისა და საბჭოს რეგულაციის პროექტი პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ (მონაცემთა დაცვის ძირითადი რეგულაცია), COM (2012) 11 final, ბრიუსელი, 2012 წლის 25 იანვარი.

22 ევროპული კომისია (2012), ევროპული პარლამენტისა და საბჭოს დირექტივის პროექტი კომპუტენტური ორგანოების მიერ დანაშაულის აღკვეთის, გამოძიების, გახსნის, დევნის ან სასჯელთა აღსრულებისას პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ (მონაცემთა დაცვის ძირითადი დირექტივა), COM (2012) 10 final, ბრიუსელი, 2012 წლის 25 იანვარი.

23 მაგ. იხ. მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები C-92/09 და C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 2010, 9 ნოემბერი, 2010 წელი, პარაგ. 48.

ტი ადგენს, რომ შესაძლებელია ქარტიის მე-7 და მე-8 მუხლებით დადგენილი უფლებების რეალიზაციაზე გავრცელდეს შეზღუდვები, თუ ეს შეზღუდვები ეფუძნება კანონს, იცავს აღნიშნული უფლებებისა და თავისუფლებების არსს და მიღებულია პროპორციულობის პრინციპის საფუძველზე, ასევე, მიზნად ისახავს ევროპული კავშირის მიერ აღიარებული საზოგადოებრივი ინტერესის დაკმაყოფილებას და აუცილებელია საამისოდ ან სხვა-თა უფლებებისა და თავისუფლებების დასაცავად.²⁴

ადამიანის უფლებათა ევროპული კონვენციით, მონაცემთა დაცვა დადგენილია მე-8 მუხლით (პირადი და ოჯახური ცხოვრების დაცვა) და, ქარტიის მსგავსად, აღნიშნული უფლება რეალიზებულ უნდა იქნეს სხვა უფლებებთან განონასწორების მეშვეობით. კონვენციის მე-8 მუხლის მე-2 პუნქტის თანახმად „სახელმწიფო ხელისუფლების ორგანოები არ უნდა ჩაერიონ აღნიშნული უფლების განხორციელებაში, გარდა იმ შემთხვევისა თუ ეს არის კანონით გათვალისწინებული და აუცილებელი დემოკრატიულ საზოგადოებაში სხვათა უფლებებისა და თავისუფლებების დასაცავად.“

შედეგად, როგორც ადამიანის უფლებათა ევროპულმა სასამართლომ, ისე მართლმსაჯულების ევროპული კავშირის სასამართლომ არერთხელ აღნიშნა, აუცილებელია სხვა უფლებებთან განონასწორება, როდესაც ხდება კონვენციის მე-8 მუხლისა და ქარტიის მე-8 მუხლის რეალიზაცია ან განმარტება.²⁵ რამოდენიმე მნიშვნელოვანი მაგალითი ასახავს თუ როგორ არის ეს ნონასწორობა დაცული

24 იქვე, პარაგ. 50.

25 ადამიანის უფლებათა ევროპული სასამართლო, Von Hannover v. Germany (No. 2) [GC], Nos. 40660/08 and 60641/08, 7 თებერვალი 2012 წელი; მართლმსაჯულების ევროპული კავშირის სასამართლო, 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, 24 ნოემბერი 2011 წელი, პარაგ. 48; მართლმსაჯულების ევროპული კავშირის სასამართლო, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 იანვარი 2008 წელი, პარაგ. 68. იხ. ასევე, ევროპის საბჭო (2013), ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებები, რომელიც ეხება პერსონალურ მონაცემთა დაცვას, DP (2013) Case law, ხელმისაწვდომია: www.coe.int/t/dghl/standardsetting/data-protection/Judgments/DP2013CaseLaw_Eng_FINAL.pdf.

1.2.1. გამოხატვის თავისუფლება

ერთ-ერთი უფლება, რომელიც შესაძლებელია დაუპირისპირდეს მონაცემთა დაცვის უფლებას არის გამოხატვის თავისუფლება.

გამოხატვის თავისუფლება დაცულია ქარტიის მე-11 მუხლით (გამოხატვისა და ინფორმაციის თავისუფლება). ეს უფლება მოიცავს „აზრების ქონის თავისუფლებას და ინფორმაციისა და იდეების მიღებისა და გაცემის თავისუფლებას სახელმწიფო ჩარევისა და საზღვრების გარეშე.“ მე-11 მუხლი შეესაბამება ადამიანის უფლებათა ევროპული კონვენციის მე-10 მუხლს. ქარტიის 52-ე მუხლის მე-3 პუნქტის მიხედვით, რამდენადაც ქარტია შეიცავს უფლებებს, რომლებიც შეესაბამება ადამიანის უფლებათა ევროპული კონვენციით აღიარებულ უფლებებს „ამ უფლებების მნიშვნელობა და ფარგლები უნდა იყოს კონვენციით მოცემული ანალოგიის მსგავსი.“ შეზღუდვები, რომლებიც შეიძლება კანონის შესაბამისად დაწესდეს ქარტიის მე-11 მუხლით აღიარებულ უფლებაზე, არ უნდა გასცდეს შეზღუდვის იმ ფარგლებს, რაც დაწესებულია კონვენციის მე-10 მუხლის მე-2 პუნქტით, სხვა სიტყვებით, იგი უნდა იყოს დადგენილი კანონით და იყოს აუცილებელი დემოკრატიულ საზოგადოებაში „სხვათა უფლებებისა და რეპუტაციის დასაცავად.“ აღნიშნული კონცეფცია, ასევე, ეხება უფლებას მონაცემთა დაცვაზე.

პერსონალურ მონაცემთა დაცვისა და გამოხატვის თავისუფლებას შორის ურთიერთობა მოწესრიგებულია მონაცემთა დაცვის დირექტივის მე-9 მუხლით, დასათაურებული როგორც „პერსონალურ მონაცემთა დამუშავება და გამოხატვის თავისუფლება.“²⁶ ამ მუხლის თანახმად, წევრი ქვეყნები ვალდებული არიან დაადგინონ რიგი გამონაკლისები და შეზღუდვები მონაცემთა დაცვაზე, დირექტივის II, IV და VI თავებით დადგენილ პირადი ცხოვრების უფლებასთან მიმართებით. მსგავსი გამონაკლისები შესაძლებელია დადგინდეს მხოლოდ ჟურნალისტიკური, სახელოვნებო ან ლიტერატურული მიზნებისთვის, რომელიც ექცევა გამოხატვის თავისუფლების ძირითადი უფლების ფარგლებში იმდენად, რამდენადაც ეს აუცილებელია პირადი

26 მონაცემთა დაცვის დირექტივა, მე-9 მუხლი.

ცხოვრების შეთავსებისთვის იმ წესებთან, რომელიც არეგულირებს გამოხატვის თავისუფლებას.

მაგალითი: საქმეზე *Tietosuoja- ja valtuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*,²⁷ მართლმსაჯულების ევროპული კავშირის სასამართლოს სთხოვეს განემარტა მონაცემთა დაცვის დირექტივის მე-9 მუხლი და განესაზღვრა ურთიერთობა მონაცემთა დაცვასა და პრესის თავისუფლებას შორის. სასამართლოს უნდა განეხილა *Markkinapörssi*-ს და *Satamedia*-ს მიერ 1.2 მილიონი ფიზიკური პირის შესახებ საგადასახადო მონაცემების გავრცელების საკითხი, რომელიც კანონიერად იქნა მოპოვებული ფინეთის საგადასახადო ორგანოდან. კერძოდ, სასამართლოს უნდა განესაზღვრა თუ რამდენად იყო მიჩნეული მხოლოდ ჟურნალისტური მიზნებისთვის განხორციელებულ ქმედებად, იმ პერსონალური მონაცემების დამუშავება, რომელიც საგადასახადო ორგანოებმა გახადეს ხელმისაწვდომი, რათა მობილური ტელეფონის მომხმარებლებს მიეღოთ სხვა პირთა საგადასახადო მონაცემები. იმის დადგენის შემდეგ, რომ მონაცემთა დაცვის დირექტივის მე-3 მუხლის პირველი პუნქტის თანახმად *Satakunnan*-ის ქმედება მიიჩნეოდა პერსონალური მონაცემების დამუშავებად, სასამართლო შეუდგა დირექტივის მე-9 მუხლის განმარტებას. პირველ ეტაპზე, სასამართლომ ხაზი გაუსვა გამოხატვის თავისუფლების, როგორც უფლების აუცილებლობას ნებისმიერ დემოკრატიულ საზოგადოებაში და აღნიშნა, რომ ცნებები დაკავშირებული თავისუფლებასთან, როგორიცაა ჟურნალისტიკა, უნდა იქნეს ფართოდ განმარტებული. შემდეგ, სასამართლომ დაადგინა – იმისათვის, რათა მიღწეულ იქნეს ბალანსი ორ ძირითად უფლებას შორის, გამონაკლისები და შეზღუდვები უნდა დაწესდეს მონაცემთა დაცვაზე იმდენად, რამდენადაც ეს აუცილებელია. ამ პირობების გათვალისწინებით, სასამართლომ მიიჩნია, რომ ქმედებები, განხორციელებული *Markkinapörssi*-სა და *Satamedia*-ს მიერ, რომელიც ეხებოდა მონაცემთა გამოყენებას იმ დოკუმენტებიდან, რომელიც ადგილობრივი კანონმდებლობის მიხედვით საჯარო რეესტრში იყო განთავსებული, შესაძლებელია იქნეს კლასიფიცირებული ჟურნალისტური მიზნებისთვის განკუთვნილი ქმედებად, თუ მიზანი იყო საზოგადოებისთვის ინფორმაციის, მოსაზრებებისა და იდეების მიწოდება, მიუხედავად იმ საშუალებისა რაც გამოყენებული იყო მათი გადაცემისთვის. სასამართლომ, ასევე, დაადგინა, რომ აღნიშნული ქმედებები არ არის დაყვანილი მხოლოდ მედიაზე და შესაძლებელია განხორციელდეს არაკომერციული საქმიანობის მიზნებიდან გამომდინარე. თუმცა, მართლმსაჯულების ევროპული კავშირის

27 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-73/07, *Tietosuoja- ja valtuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16 დეკემბერი 2008 წელი, პარაგ. 56, 61 და 62.

სასამართლომ ეროვნულ სასამართლოებს განსასაზღვრად დაუტოვა საკითხი, თუ რამდენად ჰქონდა ადგილი აღნიშნულს მოცემულ შემთხვევაში.

მონაცემთა დაცვის უფლებისა და გამოხატვის თავისუფლების ურთიერთქმედებასთან დაკავშირებით ადამიანის უფლებათა ევროპულმა სასამართლომ გამოსცა რამოდენიმე მნიშვნელოვანი გადაწყვეტილება

მაგალითი: საქმეზე *Axel Springer AG v. Germany*,²⁸ ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ შიდასახელმწიფოებრივი სასამართლოს მიერ დადგენილი აკრძალვა გაზეთის მფლობელზე, რომელსაც სურდა გამოექვეყნებინა ცნობილი მსახიობის დაკავებისა და დაპატიმრების შესახებ სტატია, არღვევდა კონვენციის მე-10 მუხლს. სასამართლომ არაერთხელ აღნიშნა თავისი პრეცედენტებით დადგენილი კრიტერიუმი, რომელიც ეხება გამოხატვის თავისუფლების განონასწორებას პირადი ცხოვრების დაცვის უფლებასთან მიმართებით:

- პირველი – იყო თუ არა სტატია საზოგადოებრივი ინტერესის შემცველი: პიროვნების დაკავება და მსჯავრდება იყო საჯარო სამართლებრივი ფაქტი და შესაბამისად საჯარო ინტერესის შემცველი;
- მეორე – იყო თუ არა მოცემული პიროვნება საჯარო ფიგურა: პიროვნება იყო მსახიობი და საკმარისად ცნობილი, რათა მიჩნეული ყოფილიყო საჯარო ფიგურად; და
- მესამე – როგორ იქნა ინფორმაცია მოპოვებული და იყო თუ არა იგი სანდო: ინფორმაცია მონოდებული იყო სახელმწიფო ბრალმდებლის სამსახურის მიერ და გამოქვეყნებული ინფორმაციის სისწორე არ იყო სადავო მხარეთა შორის.

ამასთან, ადამიანის უფლებათა ევროპულმა სასამართლომ განაცხადა, რომ კომპანიის მიმართ დანესებული შეზღუდვები პუბლიკაციის თაობაზე არ იყო სათანადოდ პროპორციული განმცხადებლის პირადი ცხოვრების დაცვის უზრუნველსაყოფად. სასამართლომ დაადგინა კონვენციის მე-10 მუხლის დარღვევა.

28 ადამიანის უფლებათა ევროპული სასამართლო, *Axel Springer AG v. Germany* [GC], No. 39954/08, 7 თებერვალი 2012 წელი, პარაგ. 90 და 91.

მაგალითი: საქმეზე *Von Hannover v. Germany* (No. 2),²⁹ სასამართლომ ვერ დაადგინა პირადი ცხოვრების დაცვის უფლების დარღვევა კონვენციის მე-8 მუხლის საფუძველზე, როდესაც მონაკოს პრინცესა კაროლინას უარი ეთქვა სასამართლოს ამკრძალავი ბრძანების გამოცემაზე, რაც მოთხოვნილი იყო არდადეგების დროს მისი და მისი მეუღლის თხილამურებზე სრიალისას გადაღებული ფოტოს გამოქვეყნების აკრძალვის თაობაზე. ფოტოსურათს თან ახლდა სტატია, რომელიც, გარდა სხვა საკითხებისა, იუწყებოდა პრინცი რაინიერის სუსტ ჯანმრთელობაზე. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ შიდასახელმწიფოებრივმა სასამართლოებმა სიფრთხილით მოახდინეს გამომცემელი კომპანიების გამოსაბრუნებელი თანხების დაგდება და განმცხადებლების პირადი ცხოვრების დაცვის უფლების ბალანსი. ადგილობრივი სასამართლოების მიერ პრინცი რაინიერის ავადმყოფობის შესახებ ინფორმაციის კლასიფიკაცია, როგორც თანამედროვე საზოგადოებაში არსებული მოვლენა, არ იყო უსაფუძვლო და სასამართლო დაეთანხმა იმას, რომ ფოტოსურათი, სტატიის კონტენტისგან გამომდინარე, გარკვეულ დონეზე მაინც ემსახურებოდა საზოგადოებრივი ინტერესის საკითხს. სასამართლომ დაადგინა, რომ კონვენციის მე-8 მუხლის დარღვევას არ ჰქონდა ადგილი.

ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებებში, ამ უფლებათა ბალანსის დროს ერთ-ერთი მნიშვნელოვანი კრიტერიუმი არის ის, თუ რამდენად ემსახურება ან არა გამოხატვა ზოგად საჯარო ინტერესს.

მაგალითი: *Mosley v. the United Kingdom*,³⁰ ეროვნულმა ყოველკვირეულმა გაზეთმა გამოაქვეყნა განმცხადებლის ინტიმური ფოტოსურათები. შემდგომ მან სასამართლოში განაცხადა კონვენციის მე-8 მუხლის დარღვევის შესახებ, რამდენადაც მას არ ჰქონდა საშუალება მოეთხოვა ფოტოსურათების გამოქვეყნების აკრძალვა იმის გამო, რომ გაზეთისთვის არ იყო დადგენილი წინასწარი შეტყობინების ვალდებულება იმ პირის მიმართ, ვისი პირადი ცხოვრებაც ირღვეოდა მოცემული მასალის გამოქვეყნების შედეგად. გამომდინ-

29 ადამიანის უფლებათა ევროპული სასამართლო, *Von Hannover v. Germany* (No. 2) [GC], Nos. 40660/08 and 60641/08, 7 თებერვალი 2012 წელი, პარაგ. 118 და 124.

30 ადამიანის უფლებათა ევროპული სასამართლო, *Mosley v. the United Kingdom*, No. 48009/08, 10 მაისი 2011 წელი, პარაგ. 129 და 130.

არე იქიდან, რომ ამგვარი მასალის გავრცელებას, ძირითადად, ჰქონდა გასართობი დატივრთვა და არა საგანმანათლებლო, იგი უდავოდ სარგებლობდა ადამიანის უფლებათა ევროპული კონვენციის მე-10 მუხლით დადგენილი დაცვით, უპირატესი იყო რა, კონვენციის მე-8 მუხლის მოთხოვნებთან მიმართებით, რომლის თანახმად, ინფორმაცია იყო პირადი, ინტიმური ბუნების და შესაბამისად არ არსებობდა საჯარო ინტერესი მისი გავრცელებისთვის. თუმცა, გარკვეული სიფრთხილე უნდა ყოფილიყო მიღებული იმ წინაპირობების განხილვისას, რომელიც შესაძლოა მოქმედებდეს, როგორც ცენზურა პუბლიკაციისთვის. იმის გათვალისწინებით თუ რა შედეგი ექნებოდა წინასწარი შეტყობინების მოთხენას, მისი მართებულობისა და ეფექტურობის გათვალისწინებით და, ასევე, არსებული დისკრეციის ფარგლებში, სასამართლომ დაადგინა, რომ წინასწარი შეტყობინების სამართლებრივად სავალდებულო მოთხოვნა არ იყო გათვალისწინებული მე-8 მუხლით. შესაბამისად, სასამართლომ მიიჩნია, რომ მე-8 მუხლის დარღვევას არ ჰქონდა ადგილი.

მაგალითი: *Biriuk v. Lithuania*,³¹ აპლიკანტი ითხოვდა ზიანის ანაზღაურებას ყოველდღიური გაზეთისგან, რამდენადაც გამოქვეყნდა სტატია აპლიკანტის აივ-ით (შიდსი) ინფიცირების შესახებ. საქმის თანახმად, აღნიშნული ინფორმაცია დამონმებულ იქნა სამედიცინო პერსონალის მიერ ადგილობრივ ჰოსპიტალში. სასამართლომ არ მიიჩნია, რომ სტატია ემსახურებოდა საჯარო ინტერესთან დაკავშირებულ მიზანს და არაერთხელ აღნიშნა, რომ არა მხოლოდ ჯანმრთელობის შესახებ მონაცემების, არამედ, ზოგადად, პერსონალური მონაცემების დაცვა, პიროვნებისთვის იყო ფუნდამენტური მნიშვნელობის მქონე მისი პირადი და ოჯახური ცხოვრების დაცვის უფლების რეალიზებისთვის, რაც უზრუნველყოფილია კონვენციის მე-8 მუხლით. სასამართლომ ყურადღება გაამახვილა იმ ფაქტზე, რომ გაზეთში არსებული ინფორმაციის თანახმად, ჰოსპიტალის სამედიცინო პერსონალმა პაციენტის აივ-ით ინფიცირების შესახებ ინფორმაცია გასცა სამედიცინო საიდუმლოების დაცვის ვალდებულების აშკარა დარღვევით. შესაბამისად, სახელმწიფომ ვერ უზრუნველყო განმცხადებლის პირადი და ოჯახური ცხოვრების უფლების დაცვა. სასამართლომ დაადგინა მე-8 მუხლის დარღვევა.

1.2.2. დოკუმენტებთან წვდომა

ქარტიის მე-11 მუხლსა და კონვენციის მე-10 მუხლზე დაყრდნობით, ინფორმაციის თავისუფლება იცავს არა მხოლოდ ინფორმაციის გავრცელების, არამედ მისი მიღების უფლებასაც. არსებობს უფლების რეალიზაციის მზარდი მოთხოვნა სახელ-

31 ადამიანის უფლებათა ევროპული სასამართლო, *Biriuk v. Lithuania*, No. 23373/03, 25 ნოემბერი 2008 წელი.

მნიშვნელოვან მიმართ გამოქვირვალობის თაობაზე, დემოკრატიული საზოგადოების ფუნქციონირებისთვის. უკანასკნელი ორი ათწლეულის განმავლობაში, სახელმწიფო ორგანოების ხელთ არსებულ დოკუმენტებთან წვდომის უფლება აღიარებულ იქნა მნიშვნელოვან უფლებად ევროპული კავშირის თითოეული მოქალაქისთვის, ასევე, ყველა ფიზიკური თუ იურიდიული პირათვის, რომელიც ცხოვრობს ან რეგისტრირებულია წევრ სახელმწიფოებში.

ევროპის საბჭოს კანონმდებლობის მიხედვით, აღსანიშნავია ოფიციალურ დოკუმენტებთან წვდომის შესახებ რეკომენდაციით მოცემული პრინციპები, რომელმაც განაპირობა ოფიციალურ დოკუმენტებთან წვდომის შესახებ კონვენციის შემუშავება (2005-ე კონვენცია).³² ევროპული კავშირის კანონმდებლობის მიხედვით, დოკუმენტებთან წვდომის უფლება დადგენილია ევროპული პარლამენტის, საბჭოსა და კომისიის დოკუმენტებთან წვდომის შესახებ 1049/2001 რეგულაციით (დოკუმენტებთან წვდომის რეგულაცია).³³ ქარტიის 42-ე მუხლი და ევროპული კავშირის ფუნქციონირების შესახებ შეთანხმების მე-15 მუხლის მე-3 პუნქტი განაცხადობს ამ უფლების ფარგლებს „კავშირის დანესებულებების, ორგანოების, სამსახურებისა და სააგენტოების დოკუმენტებზეც, მათი შენახვის ფორმის მიუხედავად.“ ქარტიის 52-ე მუხლის მე-2 პუნქტის შესაბამისად, დოკუმენტებთან წვდომის უფლება, ასევე, შესაძლებელია რეალიზებულ იქნეს იმ პირობებითა და ფარგლებით, რაც დადგენილია ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულების მე-15 მუხლის მე-3 პუნქტით. აღნიშნული უფლება შესაძლოა დაუპირისპირდეს მონაცემთა დაცვის უფლებას თუ დოკუმენტებთან წვდომის შედეგად მუქავდება სხვათა პერსონალური მონაცემები. სახელმწიფო ორგანოების ხელთ არსებულ ინფორმაციასთან წვდომის მოთხოვნა შესაძლოა საჭიროებდეს ბალანსს იმ პირების მონაცემთა დაცვის უფლებასთან, რომელთა მონაცემებიც მოცემულია მოთხოვნილ დოკუმენტებში.

32 ევროპის საბჭო, მინისტრთა კომიტეტი (2002), რეკომენდაცია Rec(2002)2 წევრი ქვეყნებისთვის ოფიციალურ დოკუმენტებთან წვდომის შესახებ, 21 თებერვალი 2002 წელი; ევროპის საბჭო, კონვენცია ოფიციალურ დოკუმენტებთან წვდომის შესახებ, CETS No. 205, 18 ივნისი 2009 წელი. კონვენცია ჯერ კიდევ არ არის ძალაში შესული.

33 ევროპული პარლამენტისა და საბჭოს 2001 წლის 30 მაისის რეგულაცია (EC) No. 1049/2001 ევროპული პარლამენტის, საბჭოსა და კომისიის დოკუმენტებთან საჯარო წვდომის შესახებ, OJ 2001 L 145.

მაგალითი: საქმეზე *European Commission v. Bavarian Lager*,³⁴ მართლმსაჯულების ევროპული კავშირის სასამართლომ განსაზღვრა მონაცემთა დაცვის უფლების ფარგლები ევროპული კავშირის დანესებულებათა ხელთ არსებულ დოკუმენტებთან წვდომის კონტექსტში და, ასევე, 1049/2001 (დოკუმენტებთან წვდომის რეგულაცია) და 45/2001 (მონაცემთა დაცვის რეგულაცია) რეგულაციებს შორის ურთიერთობა. 1992 წელს დაარსებული *Bavarian Lager* ახორციელებს ჩამოსხმული გერმანული ლუდის იმპორტირებას გაერთიანებულ სამეფოში, ძირითადად, ტავერნებისა და ბარებისთვის. კომპანიას შეექმნა სირთულეები, რამდენადაც ბრიტანული კანონმდებლობა, ფაქტობრივად, უპირატეს მგომარეობაში აყენებდა ადგილობრივ მწარმოებლებს. *Bavarian Lager*-ის საჩივარზე საპასუხოდ, ევროპულმა კომისიამ გადაწყვიტა წამოეწყო დავა გაერთიანებული სამეფოს წინააღმდეგ მისი ვალდებულებების შეუსრულებლობის გამო, რის შედეგადაც მას უნდა შეეცავალა სადავო დებულებები და მოეყვანა იგი ევროპული კავშირის კანონმდებლობასთან შესაბამისობაში. შემდეგ, *Bavarian Lager*-მა სთხოვა კომისიას, სხვა დოკუმენტებთან ერთად, წარმოედგინა იმ შეხვედრის ჩანაწერების ასლი, რომელსაც ესწრებოდნენ კომისიის წარმომადგენლები, ბრიტანული მხარე და *Confédération des Brasseurs du Marché Commun (CBMC)*. კომისია დათანხმდა გამოექვეყნებინა შეხვედრის გარკვეული დოკუმენტები, თუმცა ამოიღო ჩანაწერებში არსებული ხუთი პიროვნების სახელი, რამდენადაც ორმა განაცხადა მკაფიო უარი მათი ვინაობის გამხელაზე, ხოლო დანარჩენთან ვერ მოხერხდა დაკავშირება. 2004 წლის 18 მარტის გადაწყვეტილებით კომისიამ უარი განუცხადა *Bavarian Lager*-ს ახალი საჩივრის საფუძველზე ჩანაწერების სრული ვერსიის წარდგენის თაობაზე, უთითებდა რა, აღნიშნული პიროვნებების პირადი ცხოვრების დაცვაზე, რაც გარანტირებული იყო მონაცემთა დაცვის დირექტივით. რამდენადაც კომპანიის მოთხოვნა არ დაკმაყოფილდა, *Bavarian Lager*-მა მიმართა მართლმსაჯულების ევროპული კავშირის პირველი ინსტანციის სასამართლოს, რომელმაც გააუქმა კომისიის გადაწყვეტილება 2007 წლის 8 ნოემბრის გადაწყვეტილებით (საქმე T-194/04, *Bavarian Lager v. Commission*) დაადგინა რა, რომ იმ პირების მხოლოდ სახელების გამჟღავნება, რომლებიც ესწრებოდნენ შეხვედრას თავიანთი ორგანიზაციების წარმომადგენლების რანგში, არ წარმოადგენდა პირადი ცხოვრების შეზღუდვას და არ აყენებდა მათ პირად ცხოვრებას საფრთხის ქვეშ.

კომისიის მიერ გადაწყვეტილების გასაჩივრებისას, მართლმსაჯულების ევროპული კავშირის სასამართლომ გააუქმა პირველი ინსტანციის სასამართლოს გადაწყვეტილება. მართლმსაჯულების ევროპული კავშირის სასამართლომ აღნიშნა, რომ დოკუმენტებთან

34 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.*, 29 ივნისი 2010 წელი, პარაგ. 60, 63, 76, 78 და 79.

წვდომის რეგულაცია ამკვიდრებს „მკაფიო და გაძლიერებული დაცვის სისტემას იმ პირთა პერსონალური მონაცემების მიმართ, რომელიც კონკრეტულ შემთხვევებში შესაძლოა მიწოდებულ იქნეს საზოგადოებისთვის.“ მართლმსაჯულების ევროპული კავშირის სასამართლოს თანახმად, როდესაც პერსონალური მონაცემების შემცველ დოკუმენტებთან წვდომის მოთხოვნა დაფუძნებულია დოკუმენტებთან წვდომის რეგულაციაზე, სრულად ხდება მონაცემთა დაცვის რეგულაციის დებულებების ამოქმედება. შემდგომში, სასამართლომ დაასკვნა, რომ კომისიამ სწორი გადაწყვეტილება მიიღო, როდესაც არ დააკმაყოფილა წვდომის მოთხოვნა 1996 წლის ოქტომბრის მთლიან ჩანაწერებზე. შეხვედრის ხუთი მონაწილის თანხმობის არ არსებობისას, კომისიამ საკმარისად დააკმაყოფილა ხელმისაწვდომობის ვალდებულება დოკუმენტის იმ ვერსიის გაცემით, სადაც სახელები იყო ამოღებული.

ამასთან, სასამართლოს თანახმად, „რამდენადაც Bavarian Lager-მა დამატებით არ წარმოადგინა სათანადო და ლეგიტიმური საფუძველი ან საკმარისი არგუმენტი პერსონალურ მონაცემთა გადაცემის მართლზომიერების დასასაბუთებლად, კომისიამ ვერ შეძლო მხარეთა საპირისპირო ინტერესების ერთმანეთთან შედარება. ასევე, მან ვერ შეძლო დაედგინა არსებობდა თუ არა რაიმე მიზეზი მონაცემთა სუბიექტების ლეგიტიმური ინტერესების დარღვევისთვის,“ რაც მოითხოვებოდა მონაცემთა დაცვის რეგულაციით.

ამ გადაწყვეტილებაზე დაყრდნობით, მონაცემთა დაცვის უფლებაში ჩარევა დოკუმენტებთან წვდომის გზით საჭიროებს კონკრეტულ და მართლზომიერ საფუძველს. დოკუმენტებთან წვდომის უფლება ავტომატურად ვერ გადანონის პერსონალურ მონაცემთა დაცვის უფლებას.³⁵

წვდომის მოთხოვნის კონკრეტული საკითხი, ასევე, განხილულ იქნა ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებაშიც.

35 იხ. მონაცემთა დაცვის ევროპული ზედამხედველის (EDPS) დეტალური განხილვა (2011), პერსონალური მონაცემების შემცველი დოკუმენტების საჯარო წვდომა Bavarian Lager-ის გადაწყვეტილების შემდგომ, ბრიუსელი, 24 მარტი 2011 წელი, ხელმისაწვდომია:

www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

მაგალითი: საქმეზე *Társaság a Szabadságjogokért v. Hungary*,³⁶ განმცხადებელმა – ადამიანის უფლებების დამცველმა არასამართლებრივ ორგანიზაციამ, საკონსტიტუციო სასამართლოსგან მოითხოვა მიმდინარე საქმის შესახებ ინფორმაციაზე წვდომა. პარლამენტის იმ ნევრთან კონსულტაციის გარეშე, რომელმაც საქმე წარადგინა სასამართლოში განსახილველად, საკონსტიტუციო სასამართლომ უარი განაცხადა წვდომის მინიჭებაზე, იმ მიზეზით, რომ „გარეშე“ პირებისთვის საქმის თაობაზე მიმართვა შესაძლებელი იყო მხოლოდ მოსარჩელის ნებართვის საფუძველზე. ადგილობრივმა სასამართლოებმა გაიზიარეს ეს მიდგომა, იმ მიზეზით, რომ მოცემული პერსონალური მონაცემების დაცვა ვერ იქნებოდა გადანონილი სხვა კანონიერი ინტერესებით, მათ შორის, საჯარო ინფორმაციასთან წვდომის ინტერესით. განმცხადებელი მოქმედებდა, როგორც „საზოგადოებრივი დარაჯი“, რომელთა ქმედებებიც სარგებლობდა დაცვის იგივე ხარისხით, რაც მინიჭებული აქვს პრესას. პრესის თავისუფლებასთან მიმართებით, ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ საზოგადოებას ჰქონდა უფლება მიეღო საჯარო ინტერესის მქონე ინფორმაცია. განმცხადებლის მიერ მოთხოვნილი ინფორმაცია იყო „მზა და ხელმისაწვდომი“ და არ ითხოვდა მონაცემთა რაიმე სახის შეგროვებას. ასეთ ვითარებაში, სახელმწიფოს გააჩნდა ვალდებულება ხელი არ შეეშალა განმცხადებლის მიერ მოთხოვნილი ინფორმაციის გაცემაზე. საბოლოოდ, სასამართლომ დაადგინა, რომ დაბრკოლებები, რომლებმაც შეაფერხა საზოგადოებრივი ინტერესის შემცველ ინფორმაციასთან წვდომა, შექმლო ყოფილიყო ხელისშემშლელი იმ პირებისთვის ვინც მუშაობდა მედიაში ან მსგავს სფეროში, მათი უმნიშვნელოვანესი ფუნქციის – „საზოგადოებრივი დარაჯის“ მოვალეობის შესრულებისას. სასამართლომ დაადგინა მე-10 მუხლის დარღვევა.

ევროპული კავშირის კანონმდებლობის თანახმად, გამჭვირვალობის აუცილებლობა მტკიცეა და დგენილი. გამჭვირვალობის პრინციპი განსაზღვრულია ევროპული კავშირის შესახებ ხელშეკრულების პირველი და მე-10 მუხლებით, ხოლო ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულების მე-15 მუხლის პირველი პუნქტით.³⁷ 1049/2001 რეგულაციის პრეამბულის მე-2 პუნქტის თანახმად, მოქალაქეებს უფლება აქვთ მეტად მჭიდრო მონაწილეობა მიიღონ გადაწყვეტილების მიღების პროცესში, რაც უზრუნველყოფს დემოკრატიულ საზოგადოებაში

36 ადამიანის უფლებათა ევროპული სასამართლო, *Társaság a Szabadságjogokért v. Hungary*, No. 37374/05, 14 აპრილი 2009 წელი; იხ. პარაგ. 27, 36–38.

37 ევროპული კავშირი (2012), ევროპული კავშირისა და ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულების კონსოლიდირებული ვერსია, OJ 2012 C 326.

სახელმწიფო ადმინისტრაციის მეტად ლეგიტიმურ ფუნქციონირებას, მეტ ეფექტურობასა და ანგარიშვალდებულებას მოქალაქის წინაშე.³⁸

საბჭოს რეგულაცია 1290/2005 საერთო აგრარული პოლიტიკის დაფინანსების შესახებ და კომისიის რეგულაცია 259/2008 განსაზღვრავს დეტალურ წესებს მისი გამოყენებისთვის, ადგენს რა, ინფორმაციის გამოქვეყნების მოთხოვნას აგრარულ სექტორში ევროპული კავშირის კონკრეტული ფონდების ბენეფიციარებისა და, ასევე, თითოეული ბენეფიციარის მიერ მიღებული ხარჯების შესახებ.³⁹ გამოქვეყნება უნდა ემსახუროდეს სახელმწიფო ადმინისტრაციის მიერ საჯარო ფინანსების სწორი გამოყენების კონტროლის მიზნებს. აღნიშნული გამოქვეყნების პროპორციულობა სადავო გახადა რამოდენიმე ბენეფიციარმა.

მაგალითი: საქმეზე Volker and Markus Schecke and Hartmut Eifert v. Land Hessen,⁴⁰ მართლმსაჯულების ევროპული კავშირის სასამართლოს უნდა განეხილა ევროპული კავშირის კანონმდებლობით მოთხოვნილი ევროპული კავშირის აგრარული სუბსიდიების ბენეფიციართა სახელებისა და მათ მიერ მიღებული თანხების გამოქვეყნების მიზანშეწონილობა.

სასამართლომ აღნიშნა, რომ მონაცემთა დაცვის უფლება არ არის აბსოლუტური და ვებ-გვერდზე ევროპული კავშირის ორი აგრარული ფონდის ბენეფიციარების სახელებისა და მათ მიერ მიღებული თანხების ზუსტი ოდენობის გამოქვეყნება, ზოგადად, წარმოადგენს, ჩარევას მათ პირად ცხოვრებაში, ხოლო კონკრეტულად – პერსონალურ მონაცემთა დაცვის სფეროში.

სასამართლომ მიიჩნია, რომ მოცემული ჩარევა ქარტიის მე-7 და მე-8 მუხლებით დადგენილ უფლებაში განხორციელებული იყო კან-

38 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-41/00 P, Interporc Im- und Export GmbH v. Commission of the European Communities, 6 მარტი 2003, პარაგ. 39; და მართლმსაჯულების ევროპული კავშირის სასამართლო, C-28/08 P, European Commission v. The Bavarian Lager Co. Ltd., 29 ივნისი 2010 წელი, პარაგ. 54.

39 საბჭოს 2005 წლის 21 ივნისის რეგულაცია საერთო აგრარული პოლიტიკის დაფინანსების შესახებ (EC) No. 1290/2005, OJ 2005 L 209; და კომისიის 2008 წლის 18 მარტის რეგულაცია (EC) No. 259/2008 საბჭოს (EC) No. 1290/2005 რეგულაციის ამოქმედების დეტალური წესების განსაზღვრის შესახებ ევროპული აგრარული საგარანტიო ფონდისა (EAGF) და სასოფლო განვითარების ევროპული აგრარული ფონდის (EAFRD) ბენეფიციარების შესახებ ინფორმაციის გამოქვეყნების თაობაზე, OJ 2008 L 76.

40 მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები C-92/09 და C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 ნოემბერი 2010 წელი, პარაგ. 47–52, 58, 66–67, 75, 86 და 92.

ონის საფუძველზე და უზრუნველყოფდა ევროპული კავშირის მიერ აღიარებული საზოგადოებრივი ინტერესის მიზნის დაკმაყოფილებას, კერძოდ, გაერთიანების ფონდების გამოყენების თაობაზე გამჭვირვალობის გაძლიერებას. თუმცა, სასამართლომ აღნიშნა, რომ ფიზიკური პირების სახელების გამოქვეყნება, რომლებიც იყვნენ ევროპული კავშირის აგრარული დახმარების ორი ფონდის ბენეფიციარები და, ასევე, მათ მიერ მიღებული თანხების ზუსტი ოდენობის მითითება არაპროპორციული იყო და არ იყო მართლზომიერი ქარტიის 52-ე მუხლის პირველი პუნქტის მიხედვით. შესაბამისად, სასამართლომ ევროპული კავშირის აგრარული ფონდების ბენეფიციარების შესახებ ევროპული კავშირის კანონმდებლობა ნაწილობრივ გააუქმა.

1.2.3. ხელოვნებისა და მეცნიერების თავისუფლება

მორიგი უფლება, რომელიც უნდა იქნეს დაბალანსებული პირადი ცხოვრების პატივისცემისა და მონაცემთა დაცვის უფლებასთან არის ხელოვნებისა და მეცნიერების თავისუფლება, დაცული ქარტიის მე-13 მუხლით. ეს უფლება მომდინარეობს, უპირველესად, აზრისა და გამოხატვის თავისუფლებისგან და რეალიზებულ უნდა იქნეს ქარტიის პირველი მუხლის (ღირსება) გათვალისწინებით. ადამიანის უფლებათა ევროპული სასამართლო აღნიშნავს, რომ ხელოვნების თავისუფლება დაცულია ადამიანის უფლებათა ევროპული კონვენციის მე-10 მუხლით.⁴¹ ქარტიის მე-13 მუხლით გარანტირებული უფლება, ასევე, შესაძლებელია დაექვემდებაროს შეზღუდვებს, მსგავსად კონვენციის მე-10 მუხლისა.⁴²

მაგალითი: საქმეზე *Vereinigung bildender Künstler v. Austria*,⁴³ ავსტრიულმა სასამართლოებმა აუკრძალეს განმცხადებელ ასოციაციას იმ ნახატის გამოფენის გაგრძელება, რომელზეც დატანილი იყო სხვადასხვა საჯარო პირების თავების გამოსახულებები (ფოტოსურათები) სექსუალურ კონტექსტში. ავსტრიელმა პარლამენტარმა, რომლის თავის გამოსახულებაც გამოყენებულ იქნა ნახატზე, მიმართა სასამართლოს განმცხადებელი ასოციაციის წინააღმდეგ, ნახატის გამოფენის აკრძალვის თაობაზე ბრძანების გამოცემის მიზნით.

41 ადამიანის უფლებათა ევროპული სასამართლო, *Müller and Others v. Switzerland*, No. 10737/84, 24 მაისი 1988 წელი.

42 ძირითად უფლებათა ქარტიასთან დაკავშირებული განმარტებები, OJ 2007 C 303.

43 ადამიანის უფლებათა ევროპული სასამართლო, *Vereinigung bildender Künstler v. Austria*, No. 68345/01, 25 იანვარი 2007 წელი; იხ. ძირითადად პარაგ. 26 და 34.

ადგილობრივმა სასამართლომ მისი მიმართვის საფუძველზე გამოცხადდა ამკრძალავი ბრძანება. ადამიანის უფლებათა ევროპულმა სასამართლომ არაერთხელ აღნიშნა, რომ კონვენციის მე-10 მუხლი ვრცელდებოდა იმ იდეების გავრცელებაზე, რომელიც იყო გამოძევები, შოკისმომგვრელი ან შემანუშებელი სახელმწიფოსთვის ან მოსახლეობის რომელიმე ნაწილისთვის. იმ პირებისთვის, რომლებმაც შექმნეს, წარადგინეს, გაავრცელეს ან გამოფინეს ხელოვნების ნიმუშები, რომელიც ემსახურებოდა იდეებისა და მოსაზრებების გაცვლას, სახელმწიფოს არ უნდა განეხორციელებინა მათი გამოხატვის თავისუფლების გადამეტებული ხელყოფა. იქიდან გამომდინარე, რომ ნახატი იყო მხოლოდ კოლაჟი და გამოყენებულ იქნა მხოლოდ პირთა თავების გამოსახულებები, ხოლო მათი სხეული იყო დახატული არარეალური და გაზვიადებული ფორმით, რის მიზანსაც რეალურად არ წარმოადგენდა სინამდვილის ასახვა ან რეალობის ჩვენება, სასამართლომ აღნიშნა, რომ „ნახატი ნაკლებად სავარაუდოა იქნეს მიჩნეული ისეთად, თითქოს გამოხატავდეს პირადი ცხოვრების დეტალებს, არამედ ის უფრო დაკავშირებული იყო გამოსახული პირების, როგორც პოლიტიკოსების სტატუსთან,“ შესაბამისად, „მოცემულობის ფარგლებში, გამოსახულ პირებს უნდა გამოეჩინათ მეტი მოთმინება კრიტიკის წინაშე.“ ორი ინტერესის შეპირისპირების საფუძველზე, სასამართლომ დაადგინა, რომ ნახატის შემდგომ გამოქვეყნებაზე განუსაზღვრელი შეზღუდვა იყო არაპროპორციული. სასამართლომ დაადგინა კონვენციის მე-10 მუხლის დარღვევა.

მეცნიერებასთან მიმართებით, მონაცემთა დაცვის ევროპული კანონმდებლობა აცნობიერებს მის განსაკუთრებულ მნიშვნელობას საზოგადოებისთვის. შესაბამისად, შემცირებულია ძირითადი შეზღუდვები პერსონალურ მონაცემთა გამოყენების მხრივ. მონაცემთა დაცვის დირექტივით და 108-ე კონვენციით ნებადართულია მონაცემთა შენახვა სამეცნიერო კვლევებისთვის იმ შემთხვევაშიც კი, თუ ისინი აღარ არის საჭირო შეგროვების თავდაპირველი მიზნისთვის. მეტიც, პერსონალურ მონაცემთა შემდგომი გამოყენება სამეცნიერო კვლევებისთვის არ იქნება მიჩნეული შეუთავსებელ მიზნად. შიდასახელმწიფოებრივ კანონებს გააჩნიათ ვალდებულება დაადგინონ დეტალური დებულებები, მათ შორის, დაცვის აუცილებელი ზომები სამეცნიერო კვლევების ინტერესის მოსაწესრიგებლად მონაცემთა დაცვის უფლებასთან მიმართებით (იხ. პარაგრაფები 3.3.3 და 8.4).

1.2.4. საკუთრების დაცვა

საკუთრების დაცვის უფლება განმტკიცებულია ადამიანის უფლებათა ევროპული კონვენციის პირველი დამატებითი ოქმის პირველი მუხლით და ქარტიის მე-17 მუხლის პირველი პუნქტით. საკუთრების უფლების ერთ-ერთი მნიშვნელოვანი ასპექტი არის ინტელექტუალური საკუთრების დაცვა, დადგენილი ქარტიის მე-17 მუხლის მე-2 პუნქტით. ევროპული კავშირის საკანონმდებლო სისტემაში შესაძლებელია მოიძებნოს რამოდენიმე დირექტივა, რომელიც მიზნად ისახავს ინტელექტუალური საკუთრების ეფექტურ დაცვას, კერძოდ, საავტორო უფლების დაცვას. ინტელექტუალური საკუთრება მოიცავს არა მხოლოდ ლიტერატურულ და სახელოვნებო საკუთრებას, არამედ, ასევე, პატენტებს, სავაჭრო ნიშნებსა და მომიჯნავე უფლებებს.

როგორც მართლმსაჯულების ევროპული კავშირის სასამართლოს გადაწყვეტილებებმა ცხადყო, საკუთრების ძირითადი უფლების დაცვა დაბალანსებული უნდა იყოს სხვა ფუნდამენტურ უფლებებთან, მათ შორის, მონაცემთა დაცვის უფლებასთან.⁴⁴ არსებობს საქმეები, სადაც საავტორო უფლებების დამცველი დანესებულებები მოითხოვდნენ ინტერნეტის მომწოდებლებისგან ინტერნეტის ბაზაზე დაფუძნებული საზიარო ფაილური პლატფორმის მომხმარებელთა ვინაობის გამხელას. მსგავსი პლატფორმები ინტერნეტის მომხმარებლებს ხშირად აძლევს მუსიკალური ფაილების უფასოდ გადმოწერის საშუალებას, მიუხედავად იმისა, რომ ეს მასალა დაცულია საავტორო უფლებით.

მაგალითი: საქმე *Promusicae v. Telefónica de España*⁴⁵ ეხებოდა ესპანური ინტერნეტ-პროვაიდერის – *Telefónica*-ს უარს გაემჟღავნებინა *Promusicae*-სთვის – მუსიკალური პროდიუსერებისა და აუდიო-ვიზუალური ჩანაწერების გამომცემელთა არაკომერციული ორგანიზაციისთვის – კონკრეტული პირების პერსონალური მონაცემები, რომლებიც სარგებლობდნენ ინტერნეტ-სერვისებთან წვდომით. *Pro-*

44 ადამიანის უფლებათა ევროპული სასამართლო, *Ashby Donald and Others v. France*, No. 36769/08, 10 იანვარი 2013 წელი.

45 მართლმსაჯულების ევროპული კავშირის სასამართლო, *C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 იანვარი 2008 წელი, პარაგ. 54 და 60.

musicae ითხოვდა ინფორმაციის გამოქვეყნებას სასამართლო დავის დაწყების მიზნით იმ პირების მიმართ, რომლებიც ფონოგრამებზე წვდომის მიზნით სარგებლობდნენ ფაილური გაცვლის სისტემით, რომელ ფონოგრამებზეც მართვის უფლება ჰქონდათ Promusicae-ს წევრებს. ესპანურმა სასამართლომ საკითხი დასვა მართლმსაჯულების ევროპული კავშირის სასამართლოს წინაშე, იმ მიზნით, რომ გაერკვია თუ რამდენად უნდა ყოფილიყო გაერთიანების კანონმდებლობის მიხედვით საავტორო უფლების ეფექტური დაცვის მისაღწევად აღნიშნული პერსონალური მონაცემები მინოდებული სასამართლო წარმოებისთვის. იგი ეხებოდა დირექტივებს 2000/31, 2001/29 და 2004/48, ასევე ქარტიის მე-17 და 47-ე მუხლებს. სასამართლო მივიდა დასკვნამდე, რომ აღნიშნული დირექტივები, ისევე როგორც პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ დირექტივა (2002/58/EC), არ უკრძალავს ევროპული კავშირის წევრ ქვეყნებს სამოქალაქო დავის პროცესში საავტორო უფლების ეფექტური დაცვის უზრუნველსაყოფად განისაზღვროს პერსონალურ მონაცემთა გამჟღავნების ვალდებულება.

სასამართლომ აღნიშნა, რომ საქმე ამავდროულად ეხებოდა ორი ძირითადი უფლების დაცვის მოთხოვნათა შეთავსების საკითხს, კერძოდ, პირადი ცხოვრების პატივისცემის უფლების - საკუთრების დაცვის უფლებასთან და, ასევე, ეფექტური სამართლებრივი დაცვის საშუალების განსაზღვრას.

სასამართლომ დაასკვნა, რომ „აღნიშნული დირექტივების იმპლემენტირებისას წევრი ქვეყნები ვალდებული არიან სიფრთხილით დაეყრდნონ ამ დირექტივების განმარტებას, რაც საშუალებას მისცემს მათ, გაერთიანების საკანონმდებლო სისტემით დაცულ სხვადასხვა ძირითად უფლებას შორის, მოძებნონ სამართლიანი ბალანსი. შემდგომში, დირექტივით დადგენილი ზომების იმპლემენტირებისას, წევრი ქვეყნების სახელმწიფო ორგანოები და სასამართლოები ვალდებული არიან არა მხოლოდ განმარტონ მათი შიდასახელმწიფოებრივი კანონმდებლობა დირექტივასთან შესაბამისად, არამედ უზრუნველყონ, რომ არ განახორციელონ მათი ისეთი განმარტება, რომელიც იქნება წინააღმდეგობაში აღნიშნულ ძირითად უფლებებთან ან გაერთიანების კანონმდებლობის სხვა ძირითად პრინციპებთან, როგორიცაა პროპორციულობის პრინციპი.“⁴⁶

46 იქვე, პარაგ. 65 და 68; იხ. ასევე, მართლმსაჯულების ევროპული კავშირის სასამართლო, C-360/10, SABAM v. Netlog N.V., 16 თებერვალი 2012 წელი.

2. მონაცემთა დაცვის ტერმინოლოგია

ევროპული კავშირი	განხილული საკითხები	ევროპის საბჭო
პერსონალური მონაცემები		
მონაცემთა დაცვის დირექტივა, მე-2 მუხლი, -ა- ქვეპუნქტი მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები C-92/09 და C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 ნოემბერი 2010 წელი მართლმსაჯულების ევროპული კავშირის სასამართლო, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 იანვარი 2008 წელი	სამართლებრივი განმარტება	108-ე კონვენცია, მე-2 მუხლი, -ა- ქვეპუნქტი ადამიანის უფლებათა ევროპული სასამართლო, Bernh Larsen Holding AS and Others v. Norway, No. 24117/08, 14 მარტი 2013 წელი
მონაცემთა დაცვის დირექტივა, მე-8 მუხლი, პირველი პუნქტი მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, Bodil Lindqvist, 6 ნოემბერი 2003 წელი	პერსონალურ მონაცემთა განსაკუთრებული კატეგორიები (სენსიტიური მონაცემები)	108-ე კონვენცია, მე-6 მუხლი
მონაცემთა დაცვის დირექტივა, მე-6 მუხლი, პირველი პუნქტი, -ე ქვეპუნქტი	ანონიმიზებული ან ფსევდონიმიზებული მონაცემები	108-ე კონვენცია, მე-5 მუხლი, -ე ქვეპუნქტი 108-ე კონვენცია, განმარტებითი ბარათი, 42-ე მუხლი
მონაცემთა დამუშავება		
მონაცემთა დაცვის დირექტივა, მე-2 მუხლი, -ბ- ქვეპუნქტი მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, Bodil Lindqvist, 6 ნოემბერი 2003 წელი	ცნებები	108-ე კონვენცია, მე-2 მუხლი, -ც- ქვეპუნქტი

მონაცემთა მომხმარებლები		
მონაცემთა დაცვის დირექტივა, მე-2 მუხლი, -d- ქვეპუნქტი	დამმუშავებელი	108-ე კონვენცია, მე-2 მუხლი, -d- ქვეპუნქტი რეკომენდაცია პროფილირების შესახებ, პირველი მუხლი, -f- ქვეპუნქტი*
მონაცემთა დაცვის დირექტივა, მე-2 მუხლი, -e- ქვეპუნქტი მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, Bodil Lindqvist, 6 ნოემბერი 2003 წელი	უფლებამოსილი პირი	რეკომენდაცია პროფილირების შესახებ, პირველი მუხლი, -h- ქვეპუნქტი
მონაცემთა დაცვის დირექტივა, მე-2 მუხლი, -g- ქვეპუნქტი	მიმღები	108-ე კონვენცია, დამატებითი ოქმი, მე-2 მუხლი, პირველი პუნქტი
მონაცემთა დაცვის დირექტივა, მე-2 მუხლი, -f- ქვეპუნქტი	მესამე მხარე	
თანხმობა		
მონაცემთა დაცვის დირექტივა, მე-2 მუხლი, -h- ქვეპუნქტი მართლმსაჯულების ევროპული კავშირის სასამართლო, C-543/09, Deutsche Telekom AG v. Bundesrepublik Deutschland, 5 მაისი 2011 მაისი	კანონიერი ძალის მქონე თანხმობის განმარტება და წინაპირობები	რეკომენდაცია სამედიცინო მონაცემების შესახებ, მე-6 მუხლი და სხვა შესაბამისი რეკომენდაციები

*შენიშვნა: ევროპის საბჭო, მინისტრთა კომიტეტი (2010), რეკომენდაცია Rec(2010)13 ნევრი ქვეყნებისთვის პროფილირების კონტექსტში პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ (რეკომენდაცია პროფილირების შესახებ), 23 ნოემბერი 2010 წელი.

2.1. პერსონალური მონაცემი

საკვანძო დებულებები

- მონაცემი არის პერსონალური თუ იგი უკავშირდება იდენტიფიცირებულ ან, სულ მცირე, იდენტიფიცირებად პიროვნებას – მონაცემთა სუბიექტს.
- პირი იდენტიფიცირებადია, როდესაც შესაძლებელია დამატებითი ინფორმაციის მოპოვება მნიშვნელოვანი ძალისხმევის გარეშე, რომელიც იძლევა მონაცემთა სუბიექტის იდენტიფიცირების საშუალებას.
- ავთენტურობის (ნამდვილობის) დამტკიცება ნიშნავს იმის დადასტურებას, რომ კონკრეტულ პირს ეკუთვნის კონკრეტული ვინაობა ან/და უფლებამოსილია განახორციელოს გარკვეული ქმედებები.
- არსებობს განსაკუთრებული კატეგორიის მონაცემები, ე.წ. სენსიტიური მონაცემები, განერილი 108-ე კონვენციით და მონაცემთა დაცვის დირექტივით, რომელიც მოითხოვს გაძლიერებულ დაცვას და, შესაბამისად, ექვემდებარება მკაცრ სამართლებრივ მონესრიგებას.
- მონაცემი არის ანონიმირებული თუ ის აღარ შეიცავს რაიმე იდენტიფიკატორს; მონაცემი არის ფსევდონიმირებული თუ იდენტიფიკატორები არის დაშიფრული.
- განსხვავებით ანონიმირებული მონაცემებისგან, ფსევდონიმირებული მონაცემები წარმოადგენს პერსონალურ მონაცემებს.

2.1.1. ცნება „პერსონალური მონაცემი“-ს მთავარი ასპექტები

როგორც ევროპული კავშირის, ისე ევროპის საბჭოს კანონმდებლობის თანახმად, „პერსონალური მონაცემი“ განმარტებულია, როგორც ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს,⁴⁷ ანუ, ინფორმაცია პირის შესახებ, რომლის ვინაობა ცნობილია ან შეიძლება

47 მონაცემთა დაცვის დირექტივა, მე-2 მულის -a-ქვეპუნქტი; 108-ე კონვენცია, მე-2 მუხლის -a-ქვეპუნქტი;

დადგინდეს დამატებითი ინფორმაციის მოძიების შედეგად.

თუ აღნიშნული პირის შესახებ მუშავდება მონაცემები, ეს პირი იწოდება როგორც „მონაცემთა სუბიექტი.“

ფიზიკური პირი

მონაცემთა დაცვის უფლება წარმოშობილია პირადი ცხოვრების დაცვის უფლებიდან. პირადი ცხოვრების კონცეფცია უკავშირდება ადამიანებს. შესაბამისად, ფიზიკური პირები არიან მონაცემთა დაცვის უპირველესი ბენეფიციარები. ამასთან, მუხლი 29 სამუშაო ჯგუფის მოსაზრების თანახმად, მონაცემთა დაცვის ევროპული სამართლით მხოლოდ ცოცხალი ინდივიდი არის დაცული.⁴⁸

როგორც ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკა ცხადყოფს, ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლთან მიმართებით, რთულია პირადი და პროფესიული ცხოვრების სრული განცალკევება.⁴⁹

მაგალითი: საქმეზე *Amann v. Switzerland*,⁵⁰ სახელმწიფო ორგანოები აწარმოებდნენ განმცხადებლის ბიზნეს-საქმიანობასთან დაკავშირებული სატელეფონო საუბრების მოსმენას. ამ სატელეფონო საუბრებზე დაყრდნობით მათ ჩაატარეს გამოძიება და ეროვნული თავდაცვის მონაცემთა რეესტრში შეავსეს გრაფა განმცხადებლის შესახებ. მიუხედავად იმისა, რომ მოსმენა ეხებოდა ბიზნეს-საქმიანობასთან დაკავშირებულ სატელეფონო ზარებს, სასამართლომ ამ ზარების შესახებ მონაცემთა შეგროვება აღიარა როგორც განმცხადებლის პირად ცხოვრებასთან დაკავშირებული საკითხი. მან აღნიშნა, რომ ცნება „პირადი ცხოვრება“ არ უნდა იქნეს განმარტებული ვიწროდ, რამდენადაც პირადი ცხოვრების პატივისცემა მოიცავს სხვა ადამიანებთან ურთიერთობების წარმოქმნას და მათ განვითარებას. ამასთან, არ არსებობდა მართლზომიერი მიზეზი, რათა „პირადი ცხოვრების“ ცნებიდან მომხდარიყო პროფესიული და საქმიანი ქმედებების გამორიცხვა. ამგვარი ფართო განმარტება თანხვედრაშია 108-ე კონვენციით დადგენილ განმარტებასთან.

48 მუხლი 29 სამუშაო ჯგუფი (2007), მოსაზრება 4/2007 პერსონალური მონაცემის კონცეფციის შესახებ, WP 136, 20 ივნისი 2007 წელი, გვ. 22.

49 მაგ. იხ. ადამიანის უფლებათა ევროპული სასამართლო, *Rotaru v. Romania* [GC], No. 28341/95, 4 მაისი 2000 წელი, პარაგ. 43; ადამიანის უფლებათა ევროპული სასამართლო, *Niemietz v. Germany*, 13710/88, 16 დეკემბერი 1992 წელი, პარაგ. 29.

50 ადამიანის უფლებათა ევროპული სასამართლო, *Amann v. Switzerland* [GC], No. 27798/95, 16 თებერვალი 2000 წელი, პარაგ. 65.

შემდგომ, სასამართლომ დაადგინა, რომ მოცემულ საქმეზე ჩარევა არ იყო კანონის შესაბამისი, რამდენადაც შიდასახელმწიფოებრივი კანონმდებლობა არ შეიცავდა სპეციალურ და დეტალურ დებულებებს ინფორმაციის მოპოვების, ჩანერისა და შენახვის შესახებ. სასამართლომ დადგინა კონვენციის მე-8 მუხლის დარღვევა.

ამასთან, თუ პროფესიული ცხოვრების საკითხები შესაძლებელია დაექვემდებაროს მონაცემთა დაცვას, საკითხავია, მხოლოდ ფიზიკური პირები უნდა სარგებლობდნენ თუ არა ამგვარი დაცვით? კონვენციით მოცემული უფლებები დადგენილია არა მხოლოდ ფიზიკური პირებისთვის, არამედ ყველასთვის.

ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკაში არსებობს გადანყვეტილებები იურიდიული პირების განცხადების საფუძველზე მონაცემთა დაცვის უფლების დარღვევის შესახებ კონვენციის მე-8 მუხლის მიხედვით. მიუხედავად ამისა, სასამართლომ განიხილა საქმე საცხოვრებლისა და მიმონერის უფლების დაცვის ქრილში, ნაცვლად პირადი ცხოვრებისა:

მაგალითი: საქმე *Bernh Larsen Holding AS and Others v. Norway*⁵¹ ეხებოდა სამი ნორვეგიული კომპანიის საჩივარს საგადასახადო ორგანოს მიერ გამოტანილ გადანყვეტილებაზე, რომლითაც მათ დაევალებათ სამივე კომპანიის საერთო კომპიუტერულ სერვერზე არსებული ყველა მონაცემის ასლის მიწოდება საგადასახადო ორგანოსთვის.

ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ განმცხადებელი კომპანიებისთვის მსგავსი ვალდებულების დადგენა ეწინააღმდეგებოდა კონვენციის მე-8 მუხლით დაცულ საცხოვრებლისა და მიმონერის დაცვის უფლებას. თუმცა, სასამართლომ დაადგინა, რომ საგადასახადო ორგანოს ჰქონდა დაცვის ეფექტური და სათანადო მექანიზმები უფლების ბოროტად გამოყენების წინააღმდეგ: განმცხადებელი კომპანიები წინასწარ იყვნენ გაფრთხილებულნი; უფლება ჰქონდათ და შეეძლოთ გაეკეთებინათ შენიშვნები ადგილზე შემოწმების დროს; ასევე, მონაცემები უნდა განადგურებულიყო საგადასახადო რევიზიის დასრულებისთანავე. ამ ვითარების გათვალისწინებით, დაცული იყო სამართლიანი ბალანსი განმცხადებელი კომპანიების უფლებას – დაცული ყოფილი-

51 ადამიანის უფლებათა ევროპული სასამართლო, *Bernh Larsen Holding AS and Others v. Norway*, No. 24117/08, 14 მარტი 2013 წელი; იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლო, *Liberty and Others v. the United Kingdom*, No. 58243/00, 1 ივლისი 2008 წელი.

ყო მათი საცხოვრებლისა და მიმოწერის პატივისცემის უფლება და, შესაბამისად, მათთან დასაქმებულ პირთა პირადი ცხოვრების დაცვის ინტერესები – საგადასახადო შეფასების განხორციელების მიზნით არსებული ეფექტური შემონმების საჯარო ინტერესთან მიმართებით. სასამართლომ დაადგინა, რომ კონვენციის მე-8 მუხლის დარღვევას არ ჰქონდა ადგილი.

108-ე კონვენციის თანახმად, მონაცემთა დაცვა, უპირველეს ყოვლისა, ეხება ფიზიკური პირების დაცვას; თუმცა ხელმომწერ მხარეებს, შიდასახელმწიფოებრივი კანონმდებლობით, შეუძლიათ გაავრცელონ მონაცემთა დაცვა იურიდიულ პირებზეც, როგორცაა კომერციული კომპანიები და ასოციაციები. მონაცემთა დაცვის ევროპული კავშირის კანონმდებლობა, ზოგადად, არ ვრცელდება იურიდიული პირების დაცვაზე, მონაცემთა დამუშავების მხრივ. შიდასახელმწიფოებრივი კანონმდებლები არ არიან შეზღუდულები ამ საკითხის რეგულირებისას.⁵²

მაგალითი: საქმეზე Volker and Markus Schecke and Hartmut Eifert v. Land Hessen.⁵³ მართლმსაჯულების ევროპული კავშირის სასამართლომ, აგრარული დახმარების ბენეფიციართა პერსონალური მონაცემების გამოქვეყნებასთან დაკავშირებით აღნიშნა, რომ „იდენტიფიცირების შემთხვევაში იურიდიულ პირებს შეუძლიათ მოითხოვონ მათი უფლებების დაცვა ქარტიის მე-7 და მე-8 მუხლებით, თუ იურიდიული პირის ოფიციალური სახელწოდება ერთი ან მეტი ფიზიკური პირის ვინაობის ადგენს. პირადი ცხოვრების პატივისცემის უფლება პერსონალურ მონაცემთა დამუშავების მხრივ, რომელიც აღიარებულია ქარტიის მე-7 და მე-8 მუხლებით, მოიცავს ნებისმიერ ინფორმაციას, რომელიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.“⁵⁴

პირის იდენტიფიცირებაუნარიანობა

როგორც ევროპული კავშირის, ისე ევროპის საბჭოს კანონმდებლობის მიხედვით, ინფორმაცია შეიცავს მონაცემებს პირის შესახებ თუ:

52 მონაცემთა დაცვის დირექტივა, პრეამბულის 24-ე პუნქტი.

53 მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები C-92/09 და C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 ნოემბერი 2010 წელი, პარაგ. 53.

54 იქვე, პარაგ. 52.

- პირი ამ ინფორმაციაში არის იდენტიფიცირებული; ან
- პირი არ არის იდენტიფიცირებული, მაგრამ აღწერილია

ამ ინფორმაციაში იმგვარად, რომ არსებობს მონაცემთა სუბიექტის ვინაობის დადგენის საშუალება, შემდგომი ძიების შედეგად.

ინფორმაციის ორივე სახეობა თანაბრად დაცულია მონაცემთა დაცვის ევროპული სამართლით. ადამიანის უფლებათა ევროპულმა სასამართლომ არაერთხელ აღნიშნა, რომ ადამიანის უფლებათა ევროპული კონვენციის მიხედვით, „პერსონალური მონაცემი“-ს ცნება მსგავსია 108-ე კონვენციით მოცემული ანალოგის, განსაკუთრებით მაშინ, როდესაც ეხება იდენტიფიცირებული ან იდენტიფიცირებადი პირების საკითხს.⁵⁵

პერსონალური მონაცემის სამართლებრივი განმარტებები აღარ აკონკრეტებს თუ როდის არის პირი იდენტიფიცირებული.⁵⁶ აშკარა იდენტიფიკაცია მოითხოვს იმ ელემენტებს, რომლითაც შესაძლებელია პიროვნების აღწერა იმგვარად, რომ იგი იყოს გამორჩევადი სხვა დანარჩენი პირებისგან და ამოცნობადი, როგორც ინდივიდი. პიროვნების სახელი არის ამგვარი აღმწერი ელემენტის უპირველესი მაგალითი. გამონაკლის შემთხვევებში, სხვა იდენტიფიკატორებს შესაძლოა ჰქონდეს სახელის მსგავსი ეფექტი. მაგალითად, საჯარო პირებიდან მიმართებით, საკმარისია მოხსენიებულ იქნეს მათი თანამდებობა, მაგალითად, ევროპული კომისიის პრეზიდენტი.

მაგალითი: საქმეზე *Promusicae*,⁵⁷ მართლმსაჯულების ევროპული კავშირის სასამართლომ აღნიშნა: „უდავოა, რომ *Promusicae*-ს მიერ გარკვეული (ფაილური საზიარო ინტერნეტ-პლატფორმის) მომხმარებლების სახელებისა და მისამართების მოთხოვნა გულისხმობს პერსონალურ მონაცემთა ხელმისაწვდომობის უზრუნველყოფას, ანუ ინფორმაციის, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად დიზიკურ პირებს, 95/46/EC დირექტივის მე-2 მუხლის -a- ქვეპუნქტის თანახმად. *Telefónica*-ს მიერ შენახული ინფორმაციის მიწოდება, როგორც აცხადებს *Promusicae* და რასაც არ

55 იხ. ადამიანის უფლებათა ევროპული სასამართლო, *Amann v. Switzerland* [GC], No. 27798/95, 16 თებერვალი 2000 წელი, პარაგ. 65 et al.

56 იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლო, *Odièvre v. France* [GC], No. 42326/98, 13 თებერვალი 2003 წელი; და ადამიანის უფლებათა ევროპული სასამართლო, *Godelli v. Italy*, No. 33783/09, 25 სექტემბერი 2012 წელი.

57 მართლმსაჯულების ევროპული კავშირის სასამართლო, *C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 იანვარი 2008, პარაგ. 45.

უარყოფს Telefónica, წარმოადგენს პერსონალურ მონაცემთა დამუშავებას 2002/58 დირექტივის მე-2 მუხლის პირველი პუნქტის თანახმად, რომელიც უნდა იქნეს განხილული 95/46 დირექტივის მე-2 მუხლის -b- ქვეპუნქტთან ერთად.“

რამდენადაც ბევრი სახელი არ არის უნიკალური, პიროვნების ვინაობის დადგენას შესაძლოა დაჭირდეს დამატებითი იდენტიფიკატორები პიროვნების სხვასთან გაიგივების თავიდან აცილების მიზნით. ხშირად გამოიყენება დაბადების თარიღი და ადგილი. დამატებით, გარკვეულ ქვეყნებში შემოღებულ იქნა პერსონიფიცირებული ნომრები პიროვნებათა უკეთ გამორჩევისთვის. ბიომეტრიული მონაცემი, როგორიცაა თითის ანაბეჭდები, ციფრული ფოტოები ან თვალის ბადურის სკანირება, პიროვნებების იდენტიფიკაციისთვის ტექნოლოგიურ ეპოქაში სულ უფრო მნიშვნელოვანი ხდება.

მონაცემთა დაცვის ევროპული კანონმდებლობის მოქმედებისთვის, აუცილებელი არ არის მონაცემთა სუბიექტის იდენტიფიცირება მაღალი სიზუსტით; საკმარისია მოცემული პიროვნება იყოს იდენტიფიცირებადი. პიროვნება ითვლება იდენტიფიცირებაუნარიანად თუ ინფორმაციის ნაწილი შეიცავს იდენტიფიკაციის ელემენტებს, რის ფარგლებშიც შესაძლებელია პირის იდენტიფიცირება, პირდაპირ ან არაპირდაპირ.⁵⁸ მონაცემთა დაცვის დირექტივის პრეამბულის 26-ე პუნქტის თანახმად, ათვლის წერტილია ის, თუ რამდენად არის შესაძლებელი იდენტიფიცირების არსებული საშუალებები იყოს ხელმისაწვდომი და მართვადი ინფორმაციის სავარაუდო სამომავლო მომხმარებლებისთვის; ეს მოიცავს იმ მესამე პირებსაც, რომლებიც არიან მიმღებები (იხ. პარაგრაფი 2.3.2).

⁵⁸ მონაცემთა დაცვის დირექტივა, მე-2 მუხლის -a- ქვეპუნქტი.

მაგალითი: ადგილობრივი ხელისუფლება გადაწყვეტს შეაგროვოს მონაცემები გადაჭარბებული სისწრაფით მოძრავი ავტომანქანების შესახებ. უღებს ფოტოსურათს ავტომანქანებს და ავტომატურად აფიქსირებს დროსა და ადგილს, რათა მიაწოდოს მონაცემები შესაბამის დაწესებულებას, ხოლო ამ უკანასკნელმა დააჯარიმოს პირები სიჩქარის შეზღუდვის დარღვევისთვის. მონაცემთა სუბიექტი ასაჩივრებს, ამბობს, რომ ადგილობრივ ხელისუფლებას მონაცემთა დაცვის კანონის საფუძველზე არ გააჩნია სამართლებრივი საფუძველი ამ მონაცემთა შესაგროვებლად. ადგილობრივი ხელისუფლება აცხადებს, რომ იგი არ აგროვებს პერსონალურ მონაცემებს. სანომრე ნიშნები, მისი განცხადებით, არის მონაცემები ანონიმიზებული პირების შესახებ. ადგილობრივ ხელისუფლებას არ გააჩნია სამართლებრივი უფლებამოსილება განახორციელოს წვდომა ავტოსატრანსპორტო საშუალების საერთო რეესტრთან, რათა გამოარკვიოს ავტომანქანის მესაკუთრის ან მძღოლის ვინაობა.

ამგვარი დასაბუთება არ არის დირექტივის პრეამბულის 26-ე პუნქტთან თანხვედრაში. იმის გათვალისწინებით, რომ მონაცემთა შეგროვების მიზანი არის დამრღვევთა მკაფიო იდენტიფიცირება და დაჯარიმება, მეტად სავარაუდოა, რომ ადგილი ექნება იდენტიფიცირების მცდელობას. მიუხედავად იმისა, რომ ადგილობრივ ხელისუფლებას არ გააჩნია იდენტიფიცირების საშუალებებზე პირდაპირი წვდომა, ისინი გადასცემენ მონაცემებს უფლებამოსილ ორგანოს, პოლიციას, რომელსაც გააჩნია ამგვარი საშუალებები. პრეამბულის 26-ე პუნქტი, ასევე, ამკარად ვრცელდება იმ ვითარებაზეც, სადაც მეტად სავარაუდოა, რომ მონაცემთა შემდგომი მიმღებები, არა მხოლოდ მისი დაუყოვნებლივი მომხმარებელი, შეეცდებიან მოახდინონ ინდივიდის იდენტიფიცირება. პრეამბულის ამავე პუნქტის ქრილში, ადგილობრივი ხელისუფლების მოქმედება უთანაბრდება იდენტიფიცირებადი პიროვნებების შესახებ მონაცემთა შეგროვებას, და, შესაბამისად, საჭიროებს სამართლებრივ საფუძველს მონაცემთა დაცვის კანონმდებლობის მიხედვით.

ევროპის საბჭოს კანონმდებლობის მიხედვით, იდენტიფიცირებაუნარიანობა მსგავსადაა გაგებული. მაგალითად, საგადახდო მონაცემთა შესახებ რეკომენდაციის,⁵⁹ პირველი მუხლის მე-2 პუნქტი, ადგენს, რომ პიროვნება არ უნდა იქნეს მიჩნეული იდენტიფიცირებაუნარიანად თუ იდენტიფიცირება მოითხოვს არაგონივრულად დიდ დროს, ხარჯებს ან ძალისხმევას.

59 ევროპის საბჭო, მინისტრთა კომიტეტი (1990), რეკომენდაცია Rec(90) 19 საგადახდო და სხვა დაკავშირებული ოპერაციების მიზნით გამოყენებულ პერსონალურ მონაცემთა დაცვის შესახებ. 13 სექტემბერი 1990 წელი.

ავთენტურობის (ნამდვილობის) დადასტურება

ეს არის პროცედურა, რომლის მიხედვით პირს შეუძლია დაადასტუროს, რომ იგი ფლობს გარკვეულ ვინაობას ან/და არის უფლებამოსილი შეასრულოს გარკვეული ქმედებები, როგორიცაა, დაცულ ტერიტორიაზე შესვლა ან თანხის გამოტანა საბანკო ანგარიშიდან. ავთენტურობა შესაძლებელია დადასტურებულ იქნეს ბიომეტრიული მონაცემების შედარების გზით, როგორიცაა ფოტოსურათის ან პასპორტში თითის ანაბეჭდის შედარება პიროვნების მიერ წარდგენილ მონაცემებთან, მაგალითად, საიმიგრაციო კონტროლის დროს; ან იმ ინფორმაციის მოთხოვნის გზით, რომელიც ეცოდინება მხოლოდ იმ პირს, რომელსაც უკავშირდება კონკრეტული ვინაობა ან ავტორიზაცია, მაგალითად პერსონალური საიდენტიფიკაციო ნომერი (PIN) ან პაროლი; ან კონკრეტული გასაღების წარდგენის მეშვეობით, რომელიც უნდა იყოს მხოლოდ კონკრეტული ვინაობისა და ავტორიზაციის მქონე პირის მფლობელობაში, როგორიცაა სპეციალური ჩიპური ბარათი ან საბანკო სეიფის გასაღები. განსხვავებით პაროლებისა და ჩიპური ბარათებისგან, ზოგჯერ, პერსონალურ საიდენტიფიკაციო ნომრებთან ერთად, როგორც ინსტრუმენტი, გამოიყენება ელექტრონული ხელმოწერები, რომელიც შესაძლებელს ხდის ელექტრონულ კომუნიკაციებში პირის ვინაობისა და ავთენტურობის დადგენას.

მონაცემთა ბუნება

ინფორმაციის ნებისმიერი სახეობა შესაძლებელია იყოს პერსონალური მონაცემი, თუ იგი უკავშირდება პიროვნებას.

მაგალითი: დასაქმებულის სამუშაოს შესრულების შეფასება ზედამხედველის მიერ, რომელიც არის შენახული დასაქმებულის პირად ფაილში, წარმოადგენს დასაქმებულის შესახებ არსებულ პერსონალურ ინფორმაციას, მიუხედავად იმისა, რომ იგი შესაძლოა ნაწილობრივ ან სრულად გამოხატავდეს ზედამხედველის პირად მოსაზრებას, როგორიცაა: „დასაქმებული არ არის გულმოდგინე საკუთარი სამუშაოს მიმართ“ და, არა დადასტურებულ ინფორმაციას, როგორიცაა: „დასაქმებული ხუთი კვირის მანძილზე გათავისუფლებული იყო სამუშაოს შესრულებისგან უკანასკნელი ექვსი თვის განმავლობაში.“

პერსონალური მონაცემი მოიცავს ინფორმაციას, რომელიც მიეკუთვნება პირის პირად ცხოვრებას და ასევე ინფორმაციას მისი პროფესიული ან საზოგადო ცხოვრების შესახებ.

Amman-ის საქმეზე,⁶⁰ ადამიანის უფლებათა ევროპულმა სასამართლომ განმარტა ცნება „პერსონალური მონაცემი,“ როგორც არა მხოლოდ პირის პირად სფეროსთან დაკავშირებული ტერმინი. (იხ. პარაგრაფი 2.1.1). პერსონალური მონაცემის ამგვარი გაგება, ასევე, რელევანტურია მონაცემთა დაცვის დირექტივასთან მიმართებით:

მაგალითი: საქმეზე Volker and Markus Schecke and Hartmut Eifert v. Land Hessen,⁶¹ მართლმსაჯულების ევროპული კავშირის სასამართლომ დაადგინა: „არ აქვს მნიშვნელობა იმას, რომ გამოქვეყნებული ინფორმაცია შეიცავდა პროფესიული ხასიათის ქმედებების შესახებ მონაცემებს. ამ საკითხთან დაკავშირებით, ადამიანის უფლებათა ევროპულმა სასამართლომ კონვენციის მე-8 მუხლის განმარტებაზე დაყრდნობით აღნიშნა, რომ ცნება „პირადი ცხოვრება“ არ უნდა იქნეს განმარტებული ვიწროდ და არ არსებობს მართლზომიერი მიზეზი იმისათვის, რათა პროფესიული საქმიანობის ფარგლებში არსებული ქმედებები განცალკევებულ იქნეს პირადი ცხოვრების ცნებიდან.“

მონაცემები უკავშირდება პირებს მაშინაც, თუ ინფორმაციის შინაარსი არაპირდაპირ ავლენს პირის შესახებ მონაცემებს. ზოგიერთ შემთხვევაში, სადაც არის ახლო კავშირი საგანთან ან მოვლენასთან – მაგალითად, ერთი მხრივ მობილური ტელეფონი, ავტომობილი, ავარიული შემთხვევა, და მეორე მხრივ – პიროვნება, მაგალითად, როგორც მფლობელი, მომხმარებელი და დაზარალებული – ინფორმაცია საგნის ან მოვლენის შესახებ, ასევე, უნდა იქნეს მიჩნეული პერსონალურ მონაცემად.

60 იხ. ადამიანის უფლებათა ევროპული სასამართლო, Amann v. Switzerland, No. 27798/95, 16 თებერვალი 2000 წელი, პარაგ. 65.

61 გაერთიანებული საქმეები C-92/09 და C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 ნოემბერი 2010 წელი, პარაგ. 59.

მაგალითი: საქმეზე *Uzun v. Germany*,⁶² დაბომბვით შეტევებთან საეჭვო კავშირის გამო, განმცხადებელსა და ერთ პირზე, ამ უკანასკნელის ავტომობილში დამონტაჟებული გლობალური პოზიციური სისტემის (GPS) მონაცემების მეშვეობით, ხორციელდებოდა თვალთვალი. ამ საქმეში, ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ განმცხადებელზე დაკვირვება GPS-ის მეშვეობით მოიცავდა ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლით დაცული პირადი ცხოვრების უფლებაში ჩარევას. თუმცა, GPS-ის მეშვეობით დაკვირვება იყო კანონთან შესაბამისი და პროპორციული რამოდენიმე მკვლელობის მცდელობების გამოძიების მიზანთან, შესაბამისად, აუცილებელი იყო დემოკრატიულ საზოგადოებაში. სასამართლომ აღნიშნა, რომ კონვენციის მე-8 მუხლის დარღვევას ადგილი არ ჰქონდა.

მონაცემის არსებობის ფორმა

ფორმა, რომლითაც პერსონალური მონაცემები შენახული ან გამოყენებულია, არ ახდენს გავლენას მონაცემთა დაცვის კანონმდებლობის მოქმედებაზე. წერიტი ან ვერბალური კომუნიკაცია შესაძლებელია შეიცავდეს პერსონალურ ინფორმაციას და გამოსახულებებსაც,⁶³ მათ შორის, ვიდეოთვალთვალის სისტემის (CCTV) ჩანაწერებს⁶⁴ ან ხმას.⁶⁵ ელექტრონულად ჩანერილი ინფორმაცია, ასევე, ინფორმაცია დატანილი ქალაქდზე, შესაძლოა იყოს პერსონალური მონაცემი; ადამიანის ქსოვილის უჯრედული სინჯებიც კი შესაძლებელია იყოს პერსონალური მონაცემი, რამდენადაც ის შეიცავს პირის დნმ-ის კოდს.

62 ადამიანის უფლებათა ევროპული სასამართლო, *Uzun v. Germany*, No. 35623/05, 2 სექტემბერი 2010 წელი.

63 ადამიანის უფლებათა ევროპული სასამართლო, *Von Hannover v. Germany*, No. 59320/00, 24 ივნისი 2004 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *Sciacca v. Italy*, No. 50774/99, 11 იანვარი 2005 წელი.

64 ადამიანის უფლებათა ევროპული სასამართლო, *Peck v. the United Kingdom*, No. 44647/98, 28 იანვარი 2003 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *Köpke v. Germany*, No. 420/07, 5 ოქტომბერი 2010 წელი.

65 მონაცემთა დაცვის დირექტივა, პრეამბულის მე-16 და მე-17 პუნქტები; ადამიანის უფლებათა ევროპული სასამართლო, *P.G. and J.H. v. the United Kingdom*, No. 44787/98, 25 სექტემბერი 2001 წელი, პარაგ. 59 და 60; ადამიანის უფლებათა ევროპული სასამართლო, *Wisse v. France*, No. 71611/01, 20 დეკემბერი 2005 წელი.

2.1.2. პერსონალური მონაცემების განსაკუთრებული კატეგორიები

როგორც ევროპული კავშირის, ისე ევროპის საბჭოს კანონმდებლობის მიხედვით, არსებობს პერსონალური მონაცემების განსაკუთრებული კატეგორიები, რომელიც, თავიანთი ბუნების თანახმად, დამუშავებისას შესაძლოა შეიცავდეს რისკებს მონაცემთა სუბიექტებისთვის და, შესაბამისად, საჭიროებს გაძლიერებულ დაცვას. სპეციალური კატეგორიის მონაცემთა (სენსიტიური მონაცემები) დამუშავება შესაძლებელია ნებადართულ იქნეს მხოლოდ დაცვის სპეციალური ზომების არსებობის გათვალისწინებით.

განსაკუთრებული კატეგორიის მონაცემთა განმარტებისას, 108-ე კონვენციის მე-6 მუხლი და მონაცემთა დაცვის დირექტივის მე-8 მუხლი ადგენს შემდეგ კატეგორიებს:

- პერსონალური მონაცემი რასისა და ეთნიკური წარმომავლობის შესახებ;
- პერსონალური მონაცემი პოლიტიკური შეხედულებების, რელიგიური ან სხვა შეხედულებების შესახებ; და
- პერსონალური მონაცემი, რომელიც უკავშირდება ჯანმრთელობის მდგომარეობას ან სქესობრივ ცხოვრებას.

მაგალითი: საქმეზე Bodil Lindqvist,⁶⁶ მართლმსაჯულების ევროპული კავშირის სასამართლომ აღნიშნა - „მითითება იმ ფაქტზე, რომ ინდივიდმა დაიზიანა საკუთარი ტერფი და იმყოფება ნახევრად-სამკურნალო მდგომარეობაში, წარმოადგენს პერსონალურ მონაცემს 95/46 დირექტივის მე-8 მუხლის პირველი პუნქტის თანახმად.“

მონაცემთა დაცვის დირექტივა, დამატებით, „სავაჭრო გაერთიანების წევრობა“-ს განსაზღვრავს, როგორც სენსიტიურ მონაცემს, რამდენადაც ეს ინფორმაცია შესაძლებელია იყოს პოლიტიკური შეხედულების ან ასოცირების მკაფიო მაჩვენებელი.

108-ე კონვენცია, პერსონალურ მონაცემს, რომელიც ეხება სასამართლობას, ასევე, განსაზღვრავს სენსიტიურ მონაცემად.

მონაცემთა დაცვის დირექტივის მე-8 მუხლის მე-7 პუნქტი ავალდებულებს წევრ ქვეყნებს განსაზღვრონ ის პირობები, თუ

66 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, Bodil Lindqvist, 6 ნოემბერი 2003 წელი, პარაგ. 51.

რა შემთხვევაში ექვემდებარება დამუშავებას ეროვნული საიდენტიფიკაციო ნომერი ან ნებისმიერი სხვა იდენტიფიკატორი.

2.1.3. ანონიმირებული და ფსევდონიმირებული მონაცემები

პერსონალურ მონაცემთა ლიმიტირებული შენახვის პრინციპის თანახმად, რომელიც მოცემულია 108-ე კონვენციით და მონაცემთა დაცვის დირექტივით (დეტალურად განხილულია მესამე თავში), მონაცემები შენახულ უნდა იქნეს „მონაცემთა სუბიექტების იდენტიფიცირებადი ფორმით იმ ვადის განმავლობაში, რაც აუცილებელია მონაცემთა შეგროვების ან მათი შემდგომი დამუშავების მიზნის მისაღწევად.“⁶⁷ შესაბამისად, მონაცემი უნდა იქნეს ანონიმირებული თუ დამუშავებელს სურს მათი შენახვა იმ ვადის გასვლის შემდეგ, რაც საჭირო იყო საწყისი მიზნის მისაღწევად.

ანონიმირებული მონაცემი

მონაცემები არის ანონიმირებული თუ პერსონალური მონაცემებიდან იდენტიფიცირების შემცველი ყველა ელემენტი არის გაუქმებული. არც ერთი ის ელემენტი არ შეიძლება დარჩეს ინფორმაციაში, რომელიც გარკვეული ძალისხმევის გამოყენების შედეგად, შესაძლებელს გახდის მოცემული პიროვნებების იდენტიფიცირებას.⁶⁸ იმ შემთხვევაში, თუ მონაცემები წარმატებით იქნა ანონიმირებული, ისინი აღარ მიიჩნევა პერსონალურ მონაცემებად.

როდესაც პერსონალური მონაცემი აღარ ემსახურება თავდაპირველ მიზანს, მაგრამ უნდა იქნეს შენახული პერსონიფიცირებული ფორმით ისტორიული, სტატისტიკური ან სამეცნიერო მიზნებისთვის, დირექტივითა და 108-ე კონვენციით ეს შესაძლებელია იმ პირობით, რომ შესაბამისი დამცავი ღონისძიებები უნდა იქნეს დადგენილი მონაცემთა უკანონო გამოყენების წინააღმდეგ.⁶⁹

67 მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -ე ქვეპუნქტი და 108-ე კონვენცია, მე-5 მუხლის -ე ქვეპუნქტი.

68 იქვე. პრეამბულის 26-ე პუნქტი.

69 იქვე, მე-6 მუხლის პირველი პუნქტის -ე ქვეპუნქტი; და 108-ე კონვენცია, მე-5 მუხლის -ე ქვეპუნქტი.

ფსევდონიმირებული მონაცემები

პერსონალური მონაცემები შეიცავს იდენტიფიკატორებს, როგორიცაა სახელი, დაბადების თარიღი, სქესი და მისამართი. როდესაც პერსონალური ინფორმაცია არის ფსევდონიმირებული, იდენტიფიკატორები ჩანაცვლებულია ფსევდონიმებით. ფსევდონიმირება მიიღწევა პერსონალურ მონაცემებში იდენტიფიკატორების დაშიფრვით.

ფსევდონიმირებული მონაცემები არ არის გამოკვეთილად მოხსენიებული 108-ე კონვენციის ან მონაცემთა დაცვის დირექტივის სამართლებრივ განმარტებებში. თუმცა, 108-ე კონვენციის განმარტებითი ბარათის 42-ე მუხლი ადგენს, რომ „მოთხოვნა, რომელიც ეხება მონაცემთა სახელების შემცველი ფორმით შენახვის ვადებს, არ ნიშნავს იმას, რომ მონაცემები გარკვეული დროის შემდეგ უნდა იყოს აუცილებლად განცალკევებული იმ პიროვნების სახელისგან, რომელსაც ეკუთვნის მონაცემები, არამედ, არ უნდა იყოს შესაძლებელი მონაცემთა დაკავშირება მათ იდენტიფიკატორებთან.“ აღნიშნული შესაძლოა მიღწეულ იქნეს მონაცემთა ფსევდონიმირებით. ყველა იმ პირისათვის, რომელიც არ ფლობს განშიფრვის გასაღებს, ფსევდონიმირებული მონაცემები შესაძლოა რთულად იდენტიფიცირებადი იყოს. ფსევდონიმისა და განშიფრვის კოდის ფლობით პიროვნების ვინაობასთან კავშირი ისევ არსებობს. მათთვის, ვინც უფლებამოსილია გამოიყენოს განშიფრვის კოდი, ხელახლა იდენტიფიცირება მარტივადაა შესაძლებელი. დაცული უნდა იყოს არაუფლებამოსილი პირების მიერ განშიფრვის კოდის გამოყენება.

რამდენადაც მონაცემთა ფსევდონიმირება არის ერთ-ერთი ყველაზე მნიშვნელოვანი საშუალება, რათა ფართო მასშტაბით იქნეს მიღწეული მონაცემთა დაცვა, იქ, სადაც მონაცემთა გამოყენებისგან სრულად თავის არიდება შეუძლებელია, საჭიროა მეტად დეტალურად იქნეს განმარტებული ამ ქმედების თანმიმდევრულობა და შედეგები.

მაგალითი: წინადადება „ჩარლზ სპენსერი, დაბადებული 1967 წლის 3 აპრილს, არის ოთხი შვილის მამა, ორი ბიჭის და ორი გოგოს“ შესაძლებელია ფსევდონიმირებულ იქნეს რამოდენიმე გზით:

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

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

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

მომხმარებლები, რომლებსაც აქვთ წვდომა ფსევდონიმირებულ მონაცემებზე, ზოგადად, ვერ შეძლებენ მოახდინონ 1967 წლის 3 აპრილს დაბადებული ჩარლზ სპენსერის იდენტიფიცირება მონაცემიდან 324 ან YESz320I. შესაბამისად, ფსევდონიმირებული მონაცემები არის უფრო მეტად დაცული არასანქცირებული გამოყენებისგან.

პირველი მაგალითი ნაკლებად უსაფრთხოა. თუ წინადადება „ჩ.ს. 1967 არის ოთხი შვილის მამა, ორი ბიჭის და ორი გოგოს“ გამოყენებული იქნება პატარა სოფლის მასშტაბით, სადაც ჩარლზ სპენსერი ცხოვრობს, იგი შესაძლოა ადვილად ამოცნობადი იყოს. ფსევდონიმირების მეთოდი გავლენას ახდენს მონაცემთა დაცვის ეფექტურობაზე.

პერსონალური მონაცემები დაშიფრული იდენტიფიკატორებით ბევრ შემთხვევაში გამოიყენება, როგორც პიროვნებების ვინაობის საიდუმლოდ შენახვის საშუალება. ეს განსაკუთრებით საჭიროა იმ შემთხვევაში, როდესაც მონაცემთა დამმუშავებლებმა უნდა უზრუნველყონ, რომ მათ საქმე აქვთ შესაბამის მონაცემთა სუბიექტებთან, თუმცა არ მოითხოვენ ან არ უნდა იცოდნენ მონაცემთა სუბიექტების ნამდვილი ვინაობა. ეს იმ შემთხვევაში თუ, მაგალითად, მკვლევარი სწავლობს პაციენტთა სამედიცინო ისტორიას, რომელთა ვინაობა არის ცნობილი მხოლოდ იმ ჰოსპიტალისთვის, სადაც ისინი მკურნალობდნენ და საიდანაც მკვლევარი მოიპოვებს ფსევდონიმირებულ სამედიცინო ისტორიას. ამავდროულად, ფსევდონიმირება არის ძლიერი საშუალება პირადი ცხოვრების გამაძლიერებელ ტექნოლოგიებს შორის. იგი შეიძლება მოგვევლინოს მნიშვნელოვან ელემენტად პირადი ცხოვრების იმპლემენტაციებისთვის დიზაინის

შესაბამისად (Privacy by Design). აღნიშნული გულისხმობს, მონაცემთა დაცვის დანერგვას მონაცემთა დამუშავების გაძლიერებული სისტემების საშუალებებით.

2.2. მონაცემთა დამუშავება

საკანძო დებულებები

- ცნება „დამუშავება“ უპირველესად გულისხმობს ავტომატურ დამუშავებას.
- ევროპული კავშირის კანონმდებლობის მიხედვით, დამუშავება, ასევე, ეხება არაავტომატურ დამუშავებას სტრუქტურულ ფაილურ სისტემებში.
- ევროპის საბჭოს კანონმდებლობის მიხედვით, „დამუშავების“ ცნება შესაძლებელია განვრცობილ იქნეს შიდასახელმწიფოებრივი კანონმდებლობებით არაავტომატურ დამუშავებაზე გავრცელების მიზნით.

მონაცემთა დამუშავება 108-ე კონვენციისა და ევროპული კავშირის დირექტივის თანახმად, უპირველესად, ფოკუსირებულია მონაცემთა ავტომატურ დამუშავებაზე.

ევროპის საბჭოს კანონმდებლობის მიხედვით, ავტომატური დამუშავება გულისხმობს, რომ ზოგიერთ ეტაპზე ავტომატური დამუშავების ოპერაციათა შორის პერსონალურ მონაცემთა არაავტომატური დამუშავება გახდეს საჭირო. მსგავსად ამისა, ევროპული კავშირის კანონმდებლობის მიხედვით, მონაცემთა ავტომატური დამუშავება განმარტებულია, როგორც „პერსონალურ მონაცემზე განხორციელებული ოპერაციები, სრულად ან ნაწილობრივ ავტომატური საშუალებებით.“⁷⁰

მაგალითი: საქმეზე Bodil Lindqvist,⁷¹ მართლმსაჯულების ევროპული კავშირის სასამართლომ დაადგინა, რომ:

„ვებ-გვერდის მეშვეობით სხვადასხვა პირებისთვის მიმართვა და მათი იდენტიფიცირება სახელით ან სხვა საშუალებით, მაგალითად, მათი ტელეფონის ნომრის ან მათი სამუშაო პირობების ან ჰობის შეს-

70 108-ე კონვენცია, მე-2 მუხლის -c- ქვეპუნქტი და მონაცემთა დაცვის დირექტივა, მე-2 მუხლის -b- ქვეპუნქტი და მე-3 მუხლის პირველი პუნქტი.

71 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, Bodil Lindqvist, 6 ნოემბერი 2003, პარაგ. 27.

ახებ ინფორმაციით, წარმოადგენს „პერსონალურ მონაცემთა დამუშავებას სრულად ან ნაწილობრივ ავტომატური საშუალებებით“ 95/46 დირექტივის მესამე მუხლის პირველი პუნქტის თანახმად.“

მონაცემთა არაავტომატური დამუშავება, ასევე, მოითხოვს მონაცემთა დაცვას.

ევროპული კავშირის კანონმდებლობის მიხედვით მონაცემთა დაცვა არავითარ შემთხვევაში არ არის შეზღუდული მხოლოდ მონაცემთა ავტომატურ დამუშავებაზე. შესაბამისად, მონაცემთა დაცვა ვრცელდება არაავტომატურ ფაილურ სისტემაში პერსონალურ მონაცემთა დამუშავებაზეც, ანუ გარკვეული ფორმით, სტრუქტურირებულ საქალაქში.⁷² მონაცემთა დაცვის ამგვარი გაფართოების მიზეზი არის შემდეგი:

- საქალაქები შესაძლებელია დალაგებულ იქნეს ისე, რომ ამარტივებდეს და შესაძლებელს ხდიდეს ინფორმაციის სწრაფ მოძიებას; და
- პერსონალურ მონაცემთა შენახვა სტრუქტურირებულ საქალაქებში შესაძლებელს ხდის იმ შეზღუდვების თავის თავის არიდებას, რაც დადგენილია კანონმდებლობით ავტომატურ მონაცემთა დამუშავებაზე.⁷³

ევროპის საბჭოს კანონმდებლობის მიხედვით, 108-ე კონვენცია უპირველესად არეგულირებს მონაცემთა დამუშავებას მონაცემთა ავტომატურ ფაილებში.⁷⁴ იგი ასევე იძლევა შესაძლებლობას, რომ, შიდასახელმწიფოებრივი კანონმდებლობით, დაცვა გავრცელდეს არაავტომატურ დამუშავებაზეც. 108-ე კონვენციის ხელმომწერმა ბევრმა სახელმწიფომ გამოიყენა ეს შესაძლებლობა და მოახდინა შესაბამისი დეკლარირება ევროპის საბჭოს გენერალურ სამდივნოში.⁷⁵ მონაცემთა დაცვის ფარგლების განვრცობა, ამგვარი დეკლარაციის შესაბამისად, უნდა შეეხოს ყველა სახის არაავტომატურ მონაცემთა დამუშავებას და არ უნდა იქნეს შეზღუდული მონაცემთა დამუშავებაზე მხო-

72 მონაცემთა დაცვის დირექტივა, მე-3 მუხლის პირველი პუნქტი.

73 იქვე, პრეამბულის, 27-ე პუნქტი.

74 108-ე კონვენცია, მე-2 მუხლის -b- ქვეპუნქტი.

75 იხ. 108-ე კონვენციის მე-3 მუხლის მე-2 პუნქტის -c- ქვეპუნქტის ფარგლებში განხორციელებული დეკლარაციები.

ლოდ ავტომატურ ფაილურ სისტემებში.⁷⁶

დამუშავების არსებული ოპერაციების ბუნების გათვალისწინებით, დამუშავების ცნება ფართოა როგორც ევროპული კავშირის, ისე ევროპის საბჭოს კანონმდებლობის მიხედვით: „პერსონალურ მონაცემთა დამუშავება ნიშნავს ნებისმიერ ოპერაციას, როგორიცაა, შეგროვება, ჩანერა, ორგანიზება, შენახვა, ადაპტირება, შეცვლა, გადმოწერა, განხილვა, გამოყენება, გამჟღავნება გადაცემით, გავრცელებით ან სხვაგვარად ხელმისაწვდომად გახდომა, დალაგება ან კომბინაცია, დაბლოკვა, წაშლა ან განადგურება“,⁷⁷ რაც განხორციელებულია პერსონალური მონაცემის მიმართ. ცნება დამუშავება, ასევე, მოიცავს ქმედებებს, როდესაც მონაცემი აღარ არის ერთი კონკრეტული დამმუშავებლის პასუხისმგებლობის ქვეშ და გადაეცემა სხვა დამმუშავებლის პასუხისმგებლობის ფარგლებს.

მაგალითი: დამსაქმებლები თავიანთი დასაქმებულების შესახებ აგროვებენ და ამუშავებენ მონაცემებს, მათ შორის, ინფორმაციას მათი ანაზღაურების შესახებ. აღნიშნული ქმედების ლეგიტიმურობის სამართლებრივი საფუძველი არის შრომითი ხელშეკრულება.

დამსაქმებლები ვალდებული არიან გადაუგზავნონ მათი თანამშრომლების ანაზღაურების შესახებ მონაცემები საგადასახადო ორგანოს. გადაგზავნა, ასევე, მიიჩნევა მონაცემთა დამუშავებად 108-ე კონვენციის და დირექტივის მოცემული ცნების განმარტებიდან გამომდინარე. თუმცა, ამგვარი გამჟღავნების სამართლებრივი საფუძველი აღარ არის შრომითი ხელშეკრულება. აუცილებელია არსებობდეს დამატებითი სამართლებრივი საფუძველი დამუშავების იმ ოპერაციებისთვის, რომელიც გულისხმობს დამსაქმებლის მიერ ანაზღაურების შესახებ მონაცემთა გადაგზავნას საგადასახადო ორგანოსთვის. აღნიშნული სამართლებრივი საფუძველი, როგორც წესი, მოცემულია შიდასახელმწიფოებრივი საგადასახადო კანონმდებლობით. ამგვარი დანაწესის გარეშე, მონაცემთა გადაცემა ჩაითვლება უკანონო დამუშავებად.

76 იხ. 108-ე კონვენციის მე-3 მუხლის მე-2 პუნქტის ფორმულირება.

77 მონაცემთა დაცვის დირექტივა, მე-2 მუხლის -ბ- ქვეპუნქტი. მსგავსად ამისა, იხ. 108-ე კონვენციის მე-2 მუხლის -ც- ქვეპუნქტი.

2.3. პერსონალურ მონაცემთა მომხმარებლები

საკვანძო დებულებები

- ნებისმიერი პირი, რომელიც გადანაცვებს სხვათა პერსონალური მონაცემების დამუშავებას არის „დამმუშავებელი“, მონაცემთა დაცვის კანონმდებლობის თანახმად; თუ რამოდენიმე პირი მიიღებს ამგვარ გადანაცვებებს, ისინი შესაძლოა იყვნენ „თანა-დამმუშავებლები.“
- „უფლებამოსილი პირი“ არის იურიდიულად დამოუკიდებელი პირი, რომელიც ამუშავებს პერსონალურ მონაცემებს მონაცემთა დამმუშავებლისთვის.
- „უფლებამოსილი პირი“ ხდება დამმუშავებელი თუ იგი გამოიყენებს მონაცემებს საკუთარი მიზნებისთვის და არ შეასრულებს დამმუშავებლის მიერ მიცემულ მითითებებს.
- ნებისმიერი პირი, რომელიც დამმუშავებლისგან მიიღებს მონაცემს არის „მონაცემთა მიმღები.“
- „მესამე პირი“ არის ფიზიკური ან იურიდიული პირი, რომელიც არ მოქმედებს დამმუშავებლის მიერ მიცემული მითითებების შესაბამისად (და არ არის მონაცემთა სუბიექტი).
- „მიმღები მესამე პირი“ არის ფიზიკური ან იურიდიული პირი, რომელიც სამართლებრივად დამოუკიდებელია დამმუშავებლისგან, მაგრამ იღებს მისგან პერსონალურ მონაცემებს.

2.3.1. დამმუშავებლები და უფლებამოსილი პირები

დამმუშავებლად ან უფლებამოსილ პირად ყოფნის ყველაზე მნიშვნელოვანი შედეგი არის სამართლებრივი პასუხისმგებლობის გავცრელება იმ ვალდებულებების შესრულებაზე, რაც დადგენილია მონაცემთა დაცვის კანონმდებლობით. მხოლოდ ისინი, რომლებიც არიან პასუხისმგებლები მოქმედი სამართლით, შესაძლებელია მოგვევლინონ მოცემულ პოზიციებზე. კერძო სექტორში, ეს, ძირითადად, არის ფიზიკური ან იურიდიული პირი; საჯარო სექტორში, ეს, ძირითადად, არის სახელმწიფო ორგანო. სხვა პირები, როგორიცაა დაწესებულებები და ორგანოები სამართლებრივი ფორმის გარეშე, შესაძლებელია იყვნენ დამმუ-

შავებლები ან უფლებამოსილი პირები, იმ შემთხვევაში, თუ აღნიშნულს ადგენს კონკრეტული სამართლებრივი დებულებები.

მაგალითი: როდესაც კომპანია „მზის ნათების“ მარკეტინგის განყოფილება გეგმავს მონაცემთა დამუშავებას მარკეტინგული კვლევებისთვის, ამ შემთხვევაში, კომპანია და არა მარკეტინგის განყოფილება იქნება დამმუშავებელი. მარკეტინგული განყოფილება ვერ იქნება დამმუშავებელი, რამდენადაც მას არ გააჩნია დამოუკიდებელი იურიდიული პირის სტატუსი.

კომპანიების ჯგუფის შემთხვევაში, სათავე კომპანია და თითოეული წევრი, რომლებიც არიან დამოუკიდებელი იურიდიული პირები, ჩაითვლებიან დამოუკიდებელ დამმუშავებლებად ან უფლებამოსილ პირებად. იურიდიულად დამოუკიდებელი პირის სტატუსიდან გამომდინარე, კომპანიის ჯგუფის წევრებს შორის მონაცემთა გადაცემას დასჭირდება სპეციალური სამართლებრივი საფუძველი. პერსონალური მონაცემის გაცვლის დროს არ არსებობს პრივილეგია იმგვარი გადაცემისთვის, რომელიც ხორციელდება ერთი ჯგუფის ქვეშ მოქმედ დამოუკიდებელ იურიდიულ პირებს შორის.

აუცილებელია ყურადღება იქნეს გამახივლებული ფიზიკური პირების მოვალეობებზეც ამ კონტექსტში. ევროპული კავშირის კანონმდებლობის მიხედვით, როდესაც ფიზიკური პირები ამუშავებენ სხვების პერსონალურ ინფორმაციას აშკარად პირადი მიზნებისთვის, მათზე არ ვრცელდება მონაცემთა დაცვის დირექტივის წესები, ისინი არ მიიჩნევიან დამმუშავებლებად.⁷⁸

თუმცა, სასამართლო პრაქტიკამ გამოავლინა, რომ მონაცემთა დაცვის კანონმდებლობა აუცილებლად მოქმედებს თუ ფიზიკური პირი, ინტერნეტის გამოყენებისას, გამოაქვეყნებს მონაცემს სხვების შესახებ.

78 მონაცემთა დაცვის დირექტივა, პრეამბულის მე-12 პუნქტი და მე-3 მუხლის მე-2 პუნქტის ბოლო აბზაცი.

მაგალითი: მართლმსაჯულების ევროპული კავშირის სასამართლომ საქმეზე Bodil Lindqvist⁷⁹ აღნიშნა, რომ:

„ვებ-გვერდის მეშვეობით სხვადასხვა პირებისთვის მიმართვა და მათი იდენტიფიცირება სახელით ან სხვა საშუალებით წარმოადგენს პერსონალურ მონაცემთა დამუშავებას სრულად ან ნაწილობრივ ავტომატური საშუალებებით 95/46 დირექტივის მესამე მუხლის პირველი ნაწილის თანახმად.“⁸⁰

პერსონალური მონაცემების ამგვარი დამუშავება არ მიიჩნევა წმინდად პირადი ან საშინაო მიზნებისთვის დამუშავებად, რაც არ ექცევა მონაცემთა დაცვის დირექტივის ფარგლებში, რამდენადაც ამგვარი გამონაკლისი „უნდა განიმარტოს, როგორც მხოლოდ იმ ქმედებების შემცველი, რომელიც განხორციელებულია ინდივიდთა პირადი ან ოჯახური ცხოვრების ფარგლებში, რაც არ არის სახეზე თუ პერსონალურ მონაცემთა დამუშავება, რომელიც მოიცავს ინეტრენტში გამოქვეყნებას, ხდება იმგვარად, რომ ეს მონაცემი ხელმისაწვდომია პირთა განუსაზღვრელი წრისთვის.“⁸¹

დამმუშავებელი

ევროპული კავშირის კანონმდებლობის მიხედვით, დამმუშავებელი განიმარტება, როგორც ნებისმიერი პირი, რომელიც „დამოუკიდებლად ან სხვებთან ერთად განსაზღვრავს პერსონალურ მონაცემთა დამუშავების მიზნებსა და საშუალებებს.“⁸² დამმუშავებლის გადანაცვლებით განისაზღვრება თუ რატომ და როგორ უნდა დამუშავდეს მონაცემები. ევროპის საბჭოს კანონმდებლობის მიხედვით, „დამმუშავებლის“ ცნება დამატებით გულისხმობს იმასაც, რომ დამმუშავებელი წვეტს თუ რა სახის პერსონალური მონაცემი იქნეს შენახული.⁸³

108-ე კონვენციაში მოცემული დამმუშავებლის განმარტება ეხება დამმუშავებლად ყოფნის შემდგომ ასპექტებსაც, რაც საჭიროებს გათვალისწინებას. ეს განმარტება მოიცავს საკითხს თუ ვის შეუძლია კანონიერად დაამუშავოს კონკრეტული მონაცემი კონკრეტული მიზნისთვის. თუმცა, სადაც შესაძლო უკა-

79 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, Bodil Lindqvist, 6 ნოემბერი 2003 წელი.

80 იქვე, პარაგ. 27.

81 იქვე, პარაგ. 47.

82 მონაცემთა დაცვის დირექტივა, მე-2 მუხლის -d- ქვეპუნქტი.

83 108-ე კონვენცია, მე-2 მუხლის -d- ქვეპუნქტი.

ნონო დამუშავებას აქვს ადგილი და უნდა დადგინდეს პასუხისმგებელი დამმუშავებელი, ეს იქნება ის ფიზიკური ან იურიდიული პირი, კომპანია ან სახელმწიფო ორგანო, რომელიც წვეტს მონაცემთა დამუშავების საკითხს, მიუხედავად იმისა, გააჩნდა თუ არა მას საამისო სამართლებრივი ვალდებულება,⁸⁴ რომელიც შემდგომში მიჩნეულ იქნება დამმუშავებლად. შესაბამისად, ნაშლის შესახებ მოთხოვნა ყოველთვის უნდა იქნეს დაყენებული „ფაქტობრივი“ დამმუშავებლის მიმართ.

თანა-დამუშავება

მონაცემთა დაცვის დირექტივით განსაზღვრული „დამმუშავებლის“ ცნება ადგენს, რომ შესაძლოა არსებობდნენ რამოდენიმე სამართლებრივად დამოუკიდებელი პირები, რომლებიც ერთობლივად ან სხვებთან ერთად მოქმედებენ, როგორც მონაცემთა დამმუშავებლები. ეს ნიშნავს, რომ ისინი ერთად წყვეტენ დაამუშავონ მონაცემი საზიარო მიზნისთვის.⁸⁵ აღნიშნული სამართლებრივად დასაშვებია, თუმცა მხოლოდ იმ შემთხვევაში თუ სპეციალური სამართლებრივი საფუძველი ადგენს მონაცემთა ერთობლივი დამუშავების შესაძლებლობას, საერთო მიზნისთვის.

მაგალითი: კლიენტების შესახებ არსებული მონაცემთა ბაზა, რომელიც ადმინისტრირებულია რამოდენიმე საკრედიტო დაწესებულების მიერ, არის თანა-დამმუშავების გავრცელებული მაგალითი. როდესაც პიროვნება საკრედიტო ხაზის შესახებ განაცხადს ავსებს ბანკში, რომელიც არის ერთ-ერთი თანა-დამმუშავებელი, ბანკი ამონმებს მონაცემთა ბაზას, რაც ეხმარება მას მიიღოს გაცნობიერებული გადაწყვეტილება განმცხადებლის გადახდისუნარიანობის შესახებ.

რეგულაციები ცხადად არ ადგენენ იმას, მოითხოვს თუ არა თანა-დამმუშავებლობა სრულად საზიარო მიზნის არსებობას, ან არის თუ არა საკმარისი ის, რომ მათი მიზნები მხოლოდ ნაწილობრივ იკვეთებოდეს. თუმცა, ევროპის ფარგლებში არ არსებ-

84 იხ. ასევე, მუხლი 29 სამუშაო ჯგუფი (2010), მოსაზრება 1/2010 „დამმუშავებლისა“ და „უფლებამოსილი პირის“ ცნებების შესახებ, WP 169, ბრიუსელი, 16 თებერვალი 2010 წელი, გვ. 15.

85 მონაცემთა დაცვის დირექტივა, მე-2 მუხლის -d- ქვეპუნქტი.

ობს რელევანტური პრაქტიკა და, ასევე, არ არსებობს სიცხადე იმ შედეგებზე, რაც უკავშირდება პასუხისმგებლობას. მუხლი 29 სამუშაო ჯგუფი ემხრობა თანა-დამმუშავებლის ცნების ფართო განმარტებას, რაც მიზნად ისახავს გარკვეულ მოქნილობას მონაცემთა დამუშავების არსებული რეალობიდან გამომწვეული გაზრდილი კომპლექსურობის სათანადო რეგულირებისთვის.⁸⁶ საქმე, რომელშიც ჩართული იყო მსოფლიო ბანკთაშორისი ფინანსური ტელეკომუნიკაციის საზოგადოება (SWIFT), ასახავს სამუშაო ჯგუფის პოზიციას.

მაგალითი: ე.წ. SWIFT-ის საქმეში, ევროპული საბანკო დანესებულებები იყენებდნენ SWIFT-ს, სანცის ეტაპზე, როგორც უფლებამოსილ პირს, საბანკო ტრანზაქციების პროცესში მონაცემთა გადაცემის უზრუნველსაყოფად. SWIFT-მა გასცა საბანკო ტრანზაქციების შესახებ მონაცემები, შენახული აშშ-ის კომპიუტერული მომსახურების სერვის ცენტრში, აშშ-ის ხაზინის დეპარტამენტისთვის, იმ ევროპული საბანკო დანესებულებების პირდაპირი მითითების გარეშე, რომლებიც იყენებდნენ მას. მუხლი 29 სამუშაო ჯგუფი, ვითარების კანონიერების შეფასების პროცესში, მივიდა დასკვნამდე, რომ ევროპული საბანკო ინსტიტუტები, რომლებიც იყენებდნენ SWIFT-ს და თავად SWIFT განხილული უნდა ყოფილიყვნენ, როგორც თანა-დამმუშავებლები, რომლებსაც გააჩნდათ პასუხისმგებლობა ევროპელი მოქალაქეების წინაშე მათი მონაცემების აშშ-ის სახელმწიფო ორგანოებისთვის გადაცემის დროს.⁸⁷ გამჟღავნების შესახებ გადანაცემების მიღებით SWIFT-მა უკანონოდ მოიპოვა დამმუშავებლის სტატუსი. საბანკო დანესებულებებმა აშკარად ვერ შეასრულეს საკუთარი ვალდებულება გაენიათ ზედამხედველობა უფლებამოსილი პირისათვის და, შესაბამისად, სრულად ვერ გათავისუფლდებოდნენ დამმუშავებლის პასუხისმგებლობიდან. აღნიშნული ვითარება გულისხმობს თანა-დამმუშავებას.

86 მუხლი 29 სამუშაო ჯგუფი (2010), მოსაზრება 1/2010 „დამმუშავებლისა“ და „უფლებამოსილი პირის“ ცნებების შესახებ, WP 169, ბრიუსელი, 16 თებერვალი 2010, გვ. 19.

87 მუხლი 29 სამუშაო ჯგუფი (2006), მოსაზრება 10/2006 მსოფლიო ბანკთაშორისი ფინანსური ტელეკომუნიკაციის საზოგადოების (SWIFT) მიერ პერსონალურ მონაცემთა დამუშავების თაობაზე, WP 128, ბრიუსელი, 22 ნოემბერი 2006 წელი.

უფლებამოსილი პირი

ევროპული კავშირის კანონმდებლობის მიხედვით, უფლებამოსილი პირი განმარტებულია, როგორც პირი, რომელიც ამუშავებს პერსონალურ მონაცემს მონაცემთა დამმუშავებლისთვის.⁸⁸ მოქმედებების შესრულება, რაც დაკისრებულია უფლებამოსილი პირისთვის, შესაძლებელია იყოს ლიმიტირებული ძალზედ კონკრეტულ დავალებამდე ან შინაარსამდე, ასევე, შესაძლებელია იყოს ზოგადი და ყოვლისმომცველი.

ევროპის საბჭოს კანონმდებლობის მიხედვით, უფლებამოსილი პირის ცნება თანხვედრაშია ევროპული კავშირის სამართლებრივი სისტემით მოცემულ ანალოგთან.

უფლებამოსილი პირები, გარდა სხვებისთვის მონაცემთა დამუშავებისა, ასევე, შესაძლოა გახდნენ მონაცემთა დამოუკიდებელი დამმუშავებლები თუ ისინი დაამუშავებენ მონაცემებს საკუთარი მიზნებისთვის, მაგ. მათი დასაქმებულების ადმინისტრირებისთვის, გაყიდვების ან ანგარიშსწორებისთვის.

მაგალითი: კომპანია „მუდმივი მზადყოფნა“ სპეციალიზებულია სხვა კომპანიების ადამიანური რესურსების განყოფილებისთვის მონაცემთა დამუშავებაზე. ამ ფუნქციის გათვალისწინებით, კომპანია არის უფლებამოსილი პირი.

თუ კომპანია დაამუშავებს მონაცემებს საკუთარი დასაქმებულების შესახებ, იგი იმოქმედებს, როგორც მონაცემთა დამმუშავებელი, მისი, როგორც დამსაქმებლის ვალდებულებების შესრულების მიზნიდან გამომდინარე.

დამმუშავებელსა და უფლებამოსილ პირს შორის არსებული ურთიერთობა

როგორც დადგინდა, დამმუშავებელი არის პირი, რომელიც განსაზღვრავს დამუშავების მიზნებსა და საშუალებებს.

⁸⁸ მონაცემთა დაცვის დირექტივა, მე-2 მუხლის -e- ქვეპუნქტი.

მაგალითი: კომპანია „მზის სხივის“ დირექტორი გადაწყვეტს, რომ კომპანია „მთვარის შუქმა“, რომელიც არის საბაზრო ანალიტიკის ექსპერტი, განახორციელოს ბაზრის ანალიზი კომპანია „მზის სხივისთვის“, ამ უკანასკნელის მომხმარებლების მონაცემების მიხედვით. მიუხედავად იმისა, რომ დამუშავების საშუალებების განსაზღვრა დელეგირებული აქვს „მთვარის შუქს“, კომპანია „მზის სხივი“ მაინც რჩება დამმუშავებლად, ხოლო „მთვარის შუქი“ მხოლოდ უფლებამოსილი პირია, რამდენადაც, მათ შორის არსებული ხელშეკრულების თანახმად, „მთვარის შუქს“ შეუძლია გამოიყენოს „მზის სხივის“ მომხმარებლების მონაცემები მხოლოდ იმ მიზნებისთვის, რაც განსაზღვრულია ამ უკანასკნელის მიერ.

თუ დამუშავების საშუალებათა განსაზღვრის უფლებამოსილება დელეგირებულია უფლებამოსილ პირზე, დამმუშავებელი აღარ უნდა ჩაერიოს უფლებამოსილი პირის მიერ გადაწყვეტილების მიღების პროცესში, რომელიც უკავშირდება დამუშავების საშუალებებს. მთლიანობაში, პასუხისმგებლობა მაინც დამმუშავებელზეა, რომელმაც უნდა უხელმძღვანელოს უფლებამოსილ პირს, მის მიერ მიღებული გადაწყვეტილებების მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის უზრუნველყოფის მიზნით. შესაბამისად, ხელშეკრულება, რომელიც უკრძალავს დამმუშავებელს ჩაერთოს უფლებამოსილი პირის მიერ მიღებულ გადაწყვეტილებებში, შესაძლოა იწვევდეს თანა-დამმუშავებას, როდესაც ორივე მხარე იზიარებს დამმუშავებელის სამართლებრივ პასუხისმგებლობას.

ამასთან, თუ უფლებამოსილი პირი არ დაიცავს დამმუშავებლის მიერ განსაზღვრულ მონაცემთა გამოყენების შეზღუდვებს, უფლებამოსილი პირი გახდება მონაცემთა დამმუშავებელი იმდენად, რამდენადაც იგი არ შეასრულებს დამმუშავებლის მიერ მითითებულ ინსტრუქციებს. მაღალი ალბათობით, აღნიშნულის შესაბამისად, უფლებამოსილი პირი გახდება უკანონო დამმუშავებელი. შედეგად, თავდაპირველი დამმუშავებელი ვალდებული იქნება განმარტოს, თუ როგორ გასცდა უფლებამოსილი პირი საკუთარი მანდატის ფარგლებს. აღსანიშნავია, რომ მუხლი 29 სამუშაო ჯგუფი, ამგვარ ვითარებაში, იხრება თანა-დამმუშავებლობის დადგენაზე, რამდენადაც ეს უზრუნველყოფს მონაცემთა სუბიექტების ინტერესთა საუკეთესო და-

ცვას.⁸⁹ თანა-დამმუშავებლობის მნიშვნელოვანი შედეგი არის საერთო და ორმხრივი პასუხისმგებლობა ზიანისთვის, რაც მონაცემთა სუბიექტებს ანიჭებს ფართო სამართლებრივი დაცვის შესაძლებლობას.

შესაძლებელია წარმოიშვას საკითხი პასუხისმგებლობის განაწილებაზეც, სადაც დამმუშავებელი არის მცირე საწარმო და უფლებამოსილი პირი – დიდი კორპორაცია, რომელსაც შეუძლია საკუთარი მომსახურების პირობების დიქტატი. ამგვარ ვითარებაში, მუხლი 29 სამუშაო ჯგუფი აღნიშნავს, რომ პასუხისმგებლობის სტანდარტი არ უნდა იქნეს დაქვეითებული ეკონომიკური დისბალანსის საფუძველზე, არამედ, შენარჩუნებულ უნდა იქნეს დამმუშავებლისა და უფლებამოსილი პირის სწორი გააზრება.⁹⁰

სიზუსტისა და გამჭვირვალობისთვის, დამმუშავებელსა და უფლებამოსილ პირს შორის არსებული ურთიერთობა უნდა იყოს განსაზღვრული წერილობითი ხელშეკრულებით.⁹¹ ამგვარი კონტრაქტის არ არსებობა წარმოადგენს დამმუშავებლის ვალდებულების დარღვევას, რომლის თანახმად, ორმხრივი პასუხისმგებლობა წერილობითი ფორმით უნდა იყოს განსაზღვრული, რისი არარსებობაც იწვევს სანქციებს.⁹²

უფლებამოსილმა პირებმა შესაძლოა განიზრახონ გარკვეული დავალებების დელეგირება ქვე-უფლებამოსილი პირებისთვის. აღნიშნული სამართლებრივად დასაშვებია და დამოკიდებულია დამმუშავებელსა და უფლებამოსილ პირს შორის არსებული სახელშეკრულებო პირობების დეტალებზე, რაც მოიცავს პირობებს დამმუშავებლის თანხმობის აუცილებლობის თაობაზე ყოველ კონკრეტულ შემთხვევაში, ან პირობებს მხოლოდ ინ-

89 მუხლი 29 სამუშაო ჯგუფი (2010), მოსაზრება 1/2010 „დამმუშავებლისა“ და „უფლებამოსილი პირის“ ცნებების შესახებ, WP 169, ბრიუსელი, 16 თებერვალი 2010 წელი, გვ. 25; და მუხლი 29 სამუშაო ჯგუფი (2006), მოსაზრება 10/2006 მსოფლიო ბანკთაშორის ფინანსური ტელეკომუნიკაციის საზოგადოების მიერ პერსონალურ მონაცემთა დამუშავების თაობაზე, WP 128, ბრიუსელი, 22 ნოემბერი 2006 წელი.

90 მუხლი 29 სამუშაო ჯგუფი, მოსაზრება 1/2010 „დამმუშავებლისა“ და „უფლებამოსილი პირის“ ცნებების შესახებ, WP 169, ბრიუსელი, 16 თებერვალი 2010 წელი, გვ. 26.

91 მონაცემთა დაცვის დირექტივა, მე-17 მუხლის მე-3 და მე-4 პუნქტები.

92 მუხლი 29 სამუშაო ჯგუფი (2010), მოსაზრება 1/2010 „დამმუშავებლისა“ და „უფლებამოსილი პირის“ ცნებების შესახებ, WP 169, ბრიუსელი, 16 თებერვალი 2010 წელი, გვ. 27.

ფორმირების საკმარისობის შესახებ.

ევროპის საბჭოს კანონმდებლობის მიხედვით, დამმუშავებლისა და უფლებამოსილი პირის ცნებათა მოცემული განმარტება სრულიად იდენტურია, რაც გამომდინარეობს 108-ე კონვენციის თანახმად მიღებული რეკომენდაციების გათვალისწინებით.⁹³

2.3.2. მიმღებები და მესამე პირები

განსხვავება ამ ორი კატეგორიის პირებს შორის, რომელთა ცნება მონაცემთა დაცვის დირექტივით იქნა წარმოდგენილი, მდგომარეობს, ძირითადად, მონაცემთა დამმუშავებელთან არსებულ დამოკიდებულებაში და, შესაბამისად, დამმუშავებლის ხელთ არსებულ პერსონალურ მონაცემებზე წვდომის უფლებიდან გამომდინარე.

„მესამე პირი“ არის ის, რომელიც სამართლებრივად გაცალკევებულია დამმუშავებლისგან. შესაბამისად, მონაცემთა გამჟღავნება მესამე პირისთვის ყოველთვის საჭიროებს სპეციალურ სამართლებრივ საფუძველს. მონაცემთა დაცვის დირექტივის მე-2 მუხლის -f- ქვეპუნქტის თანახმად, მესამე პირი არის „ნებისმიერი ფიზიკური ან იურიდიული პირი, სახელმწიფო დაწესებულება, სააგენტო ან სხვა ნებისმიერი ორგანო, რომელიც არ არის მონაცემთა სუბიექტი, დამმუშავებელი, უფლებამოსილი პირი ან დამმუშავებლის და უფლებამოსილი პირის უშუალო დაქვემდებარებაში მყოფი პირი, გააჩნიათ მონაცემთა დამმუშავების უფლებამოსილება.“ ეს ნიშნავს, რომ პირები, რომლებიც მუშაობენ ორგანიზაციისთვის, რომელიც სამართლებრივად დამოუკიდებელია დამმუშავებლისგან, იმ შემთხვევაშიც კი, თუ იგი მიეკუთვნება კომპანიების გარკვეულ ჯგუფს ან ჰოლდინგს, მიიჩნევიან „მესამე პირებად.“ მეორე მხრივ, ბანკის ფილიალები, რომლებიც ამუშავებენ მომხმარებლის ანგარიშებს, მათი ხელმძღვანელების პირდაპირი მოთხოვნით, არ მიიჩნევიან „მესამე პირებად.“⁹⁴

93 იხ. მაგალითად, რეკომენდაცია პროფილირების შესახებ, პირველი მუხლი.

94 მუხლი 29 სამუშაო ჯგუფი (2010), მოსაზრება 1/2010 „დამმუშავებლისა“ და „უფლებამოსილი პირის“ ცნებების შესახებ, WP 169, ბრიუსელი, 16 თებერვალი 2010 წელი, გვ. 31.

„მიმღები“ მეტად ფართო ცნებაა ვიდრე „მესამე პირი“. მონაცემთა დაცვის დირექტივის მე-2 მუხლის -გ- ქვეპუნქტის თანახმად, მიმღები ნიშნავს „ნებისმიერ ფიზიკურ ან იურიდიულ პირს, სახელმწიფო დაწესებულებას, სააგენტოს ან ნებისმიერ სხვა ორგანოს, ვისაც გადაეცა მონაცემები, როგორც მესამე პირს ან სხვა პირს.“ მიმღები შესაძლებელია იყოს დამმუშავებლისგან ან უფლებამოსილი პირისგან დამოუკიდებელი, რომელიც იქნება, ამ შემთხვევაში, მესამე პირი, ან რომელიმე პირი დამმუშავებლის ან უფლებამოსილი პირის შიდა სტრუქტურაში, როგორიცაა დასაქმებული ან იმავე კომპანიის ან დაწესებულების სხვა განყოფილება.

განსხვავება მიმღებებსა და მესამე პირებს შორის საყურადღებოა მხოლოდ მონაცემთა კანონიერი გადაცემის პირობებიდან გამომდინარე. დამმუშავებლის და უფლებამოსილი პირის დასაქმებულებს, დამატებითი სამართლებრივი საფუძვლის გარეშე, შეუძლიათ იყვნენ პერსონალური მონაცემების მიმღებები, თუ ისინი ჩართულნი არიან დამმუშავებლის ან უფლებამოსილი პირის მიერ წარმოებულ დამუშავების ოპერაციებში. მეორე მხრივ, მესამე პირი, რომელიც არის იურიდიულად დამოუკიდებელი დამმუშავებლისა და უფლებამოსილი პირისგან, არ არის უფლებამოსილი გამოიყენოს დამმუშავებლის მიერ დამუშავებული პერსონალური მონაცემები, გარდა იმ შემთხვევისა თუ არ იქნება დადგენილი სპეციალური სამართლებრივი საფუძვლები კონკრეტული შემთხვევისთვის. მონაცემთა „მიმღები მესამე პირები“, შესაბამისად, ყოველთვის საჭიროებენ სამართლებრივი საფუძვლის არსებობას პერსონალურ მონაცემთა კანონიერი მიღებისთვის.

მაგალითი: უფლებამოსილი პირის დასაქმებული, რომელიც იყენებს პერსონალურ მონაცემებს დამსაქმებლის მიერ მისთვის დაკისრებული დავალებების შესასრულებლად, წარმოადგენს მონაცემთა მიმღებს, მაგრამ არა მესამე პირს, რამდენადაც იგი იყენებს მონაცემებს უფლებამოსილი პირის სახელით და მის მიერ გაცემული ინსტრუქციების შესაბამისად.

თუ, იგივე დასაქმებული გადაწყვეტს, რომ გამოიყენოს მონაცემი საკუთარი მიზნებისთვის და მიჰყიდოს ის სხვა კომპანიას, მაშინ, დასაქმებული იმოქმედებს, როგორც მესამე პირი. იგი აღარ ასრულებს უფლებამოსილი პირის (დამსაქმებლის) მითითებებს. როგორც მესამე პირი, დასაქმებულს დასჭირდება სამართლებრივი საფუძველი მონაცემთა მიღებისა და გაყიდვისთვის. ამ მაგალითით, დასაქმებული აშკარად არ ფლობს ამგვარ სამართლებრივ საფუძველს, შესაბამისად, ეს ქმედებები იქნება უკანონო.

2.4. თანხმობა

საკვანძო დებულებები

- თანხმობა, როგორც პერსონალურ მონაცემთა დამუშავების სამართლებრივი საფუძველი, უნდა იყოს ნებაყოფლობითი, ინფორმირებული და კონკრეტული.
- თანხმობა გაცხადებული უნდა იყოს გასაგებად. თანხმობა შესაძლებელია გაცემული იყოს აშკარად ან იმგვარი ქმედებით, რომელიც არ ტოვებს ეჭვის საფუძველს იმის თაობაზე, რომ მონაცემთა სუბიექტი თანხმდება საკუთარი მონაცემის დამუშავებას.
- თანხმობის საფუძველზე განსაკუთრებული მონაცემების დამუშავება საჭიროებს აშკარა თანხმობას.
- თანხმობა შესაძლებელია ნებისმიერ დროს იქნეს გამოთხოვილი.

თანხმობა ნიშნავს „მონაცემთა სუბიექტის სურვილების თაობაზე განხორციელებულ ნებისმიერ ნებაყოფლობით, კონკრეტულ და ინფორმირებულ გამოხატულებას.“⁹⁵ ბევრ შემთხვევაში, იგი არის მონაცემთა კანონიერი დამუშავების სამართლებრივი საფუძველი (იხ. პარაგრაფი 4.1).

⁹⁵ მონაცემთა დაცვის დირექტივა, მე-2 მუხლის -h- ქვეპუნქტი.

2.4.1. კანონიერი ძალის მქონე თანხმობის ელემენტები

მონაცემთა სუბიექტებისგან კანონიერი თანხმობის მიღებისთვის ევროპული კავშირის კანონმდებლობა გამოყოფს კანონიერი ძალის მქონე თანხმობის სამ ელემენტს, მათ შესახებ არსებულ მონაცემთა გამოყენების მიზნით:

- თანხმობის გაცემისას მონაცემთა სუბიექტი არ უნდა იმყოფებოდეს ზეწოლის ქვეშ;
- მონაცემთა სუბიექტი ჯეროვნად უნდა იყოს ინფორმირებული თანხმობის გაცემის მიზნისა და შედეგების შესახებ; და
- თანხმობის ფარგლები რაც შეიძლება მეტად კონკრეტული უნდა იყოს.

მხოლოდ იმ შემთხვევაში, თუ ყველა ზემოაღნიშნული მოთხოვნა არის დაკმაყოფილებული, მონაცემთა დაცვის კანონმდებლობის მიხედვით თანხმობა იქნება კანონიერი ძალის მქონე.

108-ე კონვენცია არ შეიცავს თანხმობის ცნების განმარტებას; მისი განმარტების საკითხი დელეგირებულია შიდასახელმწიფოებრივი კანონმდებლობებისთვის. თუმცა, ევროპის საბჭოს კანონმდებლობის მიხედვით, კანონიერი ძალის მქონე თანხმობის ელემენტები თანხვედრაშია ზემოაღნიშნულთან, რაც განერილია 108-ე კონვენციის შესაბამისად მიღებული რეკომენდაციებით.⁹⁶ თანხმობასთან დაკავშირებული მოთხოვნები ევროპული სამოქალაქო სამართლით აღიარებული ნების კანონიერი გამოვლენისთვის დადგენილი მოთხოვნების მსგავსია.

სამოქალაქო სამართლის მიხედვით, თანხმობასთან დაკავშირებული დამატებითი მოთხოვნები, როგორიცაა სამართლებრივი მოცულობა, ჩვეულებრივ ვრცელდება მონაცემთა დაცვის სფეროზეც, რამდენადაც ეს მოთხოვნები წარმოადგენს ძირითად სამართლებრივ წინაპირობებს. იმ პირების კანონთან შეუსაბამო თანხმობა, რომელთაც არ გააჩნიათ ქმედუნარიანობა, გამოიწვევს მონაცემთა დამუშავების სამართლებრივი საფუძვლის არ არსებობას მათ შესახებ მონაცემთა დამუშავებისთვის.

96 იხ. მაგ. 108-ე კონვენცია, რეკომენდაცია სტატისტიკის მონაცემთა შესახებ, მე-6 პუნქტი.

თანხმობა შესაძლოა გაცემულ იქნეს ცხადად⁹⁷ ან შინაარსობრივად. ეს უკანასკნელი არ ტოვებს ეჭვებს მონაცემთა სუბიექტის ნების თაობაზე და შესაძლებელია განხორციელებული იყოს როგორც სიტყვიერად, ისე – წერილობით; უკანასკნელი გამომდინარეობს კონკრეტული ვითარებიდან. ნებისმიერი თანხმობა გაცემული უნდა იყოს მკაფიოდ.⁹⁸ ეს ნიშნავს, რომ არ უნდა არსებობდეს გონივრული ეჭვი იმის შესახებ, რომ მონაცემთა სუბიექტს უნდოდა განეცხადებინა თანხმობა მის შესახებ მონაცემის დამუშავებაზე. უბრალო უმოქმედობის თანხმობად მიჩნევა არ აკმაყოფილებს მკაფიო თანხმობის პირობას. თუ დასამუშავებელი მონაცემები არის სენსიტიური, აშკარა თანხმობა აუცილებელი პირობაა და გაცხადებული უნდა იყოს მკაფიოდ.

ნებაყოფლობითი თანხმობა

ნებაყოფლობით თანხმობას კანონიერი ძალა გააჩნია მხოლოდ მაშინ „თუ მონაცემთა სუბიექტს აქვს შესაძლებლობა თავად განახორციელოს არჩევანი და არ არსებობს შეცდომაში შეყვანის, დაშინების, იძულების ან აშკარა ნეგატიური შედეგის დადგომის შესაძლებლობა იმ შემთხვევაში, თუ იგი არ განაცხადებს თანხმობას.“⁹⁹

მაგალითი: ბევრ აეროპორტში, მგზავრებს უწევთ სხეულის სკანერში გავლა ჩასხდომის ზონაში მოხვედრის მიზნით.¹⁰⁰ იმის გათვალისწინებით, რომ სკანირების დროს მგზავრების მონაცემები მუშავდება, ეს უნდა განხორციელდეს მონაცემთა დაცვის დირექტივის მე-7 მუხლით დადგენილი რომელიმე სამართლებრივი საფუძვლით (იხ. პარაგრაფი 4.1). სხეულის სკანერში გავლა, ზოგ შემთხვევაში, წარმოადგენს მგზავრის არჩევანს, რაც ნიშნავს იმას, რომ მათი თანხმობა მონაცემთა დამუშავებას მართლზომიერს გახდის. თავის მხრივ, მგზავრებს შესაძლოა ჰქონდეთ განცდა, რომ სკანერში გავლაზე უარის თქმა გამოიწვევს ეჭვს ან კონტროლის დამატებითი სამუალებების ამოქმედებას, როგორიცაა გაჩხრეკა. ბევრი მგზავრი თანხმობას აცხადებს სკანირებაზე იმიტომ, რომ თავი აარიდოს დამატებით

97 მონაცემთა დაცვის დირექტივა, მე-8 მუხლის მე-2 პუნქტი.

98 იქვე, მე-7 მუხლის -ა- ქვეპუნქტი და 26-ე მუხლის პირველი პუნქტი.

99 იხ. ასევე, მუხლი 29 სამუშაო ჯგუფი (2011), მოსაზრება 15/2011 თანხმობის ცნების შესახებ, WP 187, ბრიუსელი, 13 ივლისი 2011 წელი, გვ. 12.

100 იქვე, გვ. 15.

სირთულეებს ან შეფერხებებს. ამგვარი თანხმობა შესაძლებელია არ იყოს საკმარისად ნებაყოფლობითი.

შესაბამისად, ზუსტი სამართლებრივი საფუძველი შესაძლებელია მოიძებნოს მხოლოდ კანონმდებლის სამართლებრივ აქტში, მიღებული მონაცემთა დაცვის დირექტივის მე-7 მუხლის -e- ქვეპუნქტის საფუძველზე, რაც მგზავრებისთვის იწვევს თანამშრომლობის ვალდებულებას აღმატებული საჯარო ინტერესის გამო. ამგვარი აქტი შესაძლოა კვლავ იძლეოდეს სკანიერების ან გაჩხრეკვის არჩევის შესაძლებლობას, მაგრამ მხოლოდ როგორც სასაზღვრო კონტროლის დამატებითი საშუალება, რაც აუცილებელია კონკრეტული პირობების გათვალისწინებით. აღნიშნული ევროპულმა კომისიამ ასახა თავის ორ რეგულაციაში უსაფრთხოების სკანერების შესახებ 2011 წელს.¹⁰¹

ნებაყოფლობით თანხმობას შესაძლოა, ასევე, საფრთხე შეექმნას სიტუაციებში, სადაც არსებობს სუბორდინაცია, საგრძნობი ეკონომიკური დისბალანსის არსებობისას დამმუშავებელს (რომელიც იცავს მონაცემს) და მონაცემთა სუბიექტს (რომელიც იძლევა თანხმობას) შორის.¹⁰²

101 კომისიის 2011 წლის 10 ნოემბრის რეგულაცია (EU) No. 1141/2011 სამოქალაქო ავიაციის უსაფრთხოების საერთო საბაზისო სტანდარტების დამატების შესახებ ევროპული კავშირის აეროპორტებში უსაფრთხოების სკანერების გამოყენების თაობაზე, რომელსაც ცვლილება შეაქვს No. 272/2009 რეგულაციაში (EC), OJ 2011 L 293, და კომისიის 2011 წლის 11 ნოემბრის საიმპლემენტაციო რეგულაცია (EU) No. 1147/2011, სამოქალაქო ავიაციის უსაფრთხოების საერთო საბაზისო სტანდარტის იმპლემენტაციის შესახებ ევროპული კავშირის აეროპორტებში უსაფრთხოების სკანერის გამოყენების თაობაზე, რომელსაც ცვლილება შეაქვს No. 185/2010 რეგულაციაში (EU), OJ 2011 L 294.

102 იხ. ასევე, მუხლი 29 სამუშაო ჯგუფი (2001), მოსაზრება 8/2001 პრომით კონტექსტში პერსონალური მონაცემების დამუშავების შესახებ, WP 48, ბრიუსელი, 13 სექტემბერი 2001 წელი; და მუხლი 29 სამუშაო ჯგუფი (2005), 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივის საერთო განმარტების შესახებ სამუშაო დოკუმენტი, WP 114, ბრიუსელი, 25 ნოემბერი 2005 წელი.

მაგალითი: დიდი კომპანია გეგმავს შექმნას რეესტრი, რომელიც მოიცავს ყველა დასაქმებულის სახელს, მათ ფუნქციებსა და სამუშაო მისამართებს, მხოლოდ კომპანიის შიდა კომუნიკაციების გაუმჯობესების მიზნით. ადამიანური რესურსების მართვის განყოფილების უფროსს სურს თითოეულ თანამშრომელზე რეესტრში განათავსოს ფოტოსურათი, რათა, მაგალითად, მარტივი იყოს კოლეგების შეხვედრებზე ამოცნობა. დასაქმებულების წარმომადგენლები ითხოვენ, რომ აღნიშნული უნდა განხორციელდეს მხოლოდ თითოეული დასაქმებულის თანხმობის საფუძველზე.

ამგვარ სიტუაციაში, დასაქმებულების თანხმობა უნდა იქნეს მიჩნეული სამართლებრივ საფუძვლად რეესტრში ფოტოსურათების დამუშავებისთვის, ვინაიდან აშკარაა, რომ რეესტრში ფოტოსურათის გამოქვეყნებას არ ექნება ნეგატიური შედეგი და მეტიც, ასევე ცხადია, რომ დასაქმებულისთვის არ დადგება ნეგატიური შედეგი თუ იგი არ დაეთანხმება საკუთარი ფოტოსურათის გამოქვეყნებას რეესტრში.

ეს არ ნიშნავს იმას, რომ თანხმობა ვერასოდეს იქნება კანონიერი ძალის მქონე თუ თანხმობაზე უარის გაცხადება წარმოშობს ნეგატიურ შედეგებს. თუ, მაგალითად, უარის თქმა სუბერმარკეტის ბარათის აღების შესახებ იწვევს მხოლოდ იმას, რომ კონკრეტული საქონლის ფასების შესახებ ინფორმაცია ვერ იქნება მიღებული, თანხმობა კვლავ რჩება კანონიერი ძალის მქონე სამართლებრივ საფუძვლად იმ მომხმარებელთა პერსონალური მონაცემის დამუშავებისთვის, რომლებმაც განაცხადეს თანხმობა ამგვარი ბარათის აღების შესახებ. არ არსებობს სუბორდინაციული დაქვემდებარება კომპანიასა და მომხმარებელს შორის და შედეგები, თანხმობის განუცხადებლობის შემთხვევაში, არ არის მონაცემთა სუბიექტისთვის იმდენად მნიშვნელოვანი, რომ მოახდინოს თავისუფალი არჩევანის პრევენცია.

მეორე მხრივ, თუ საკმაოდ მნიშვნელოვანი საქონელი ან მომსახურება შესაძლებელია მიღებულ იქნეს მხოლოდ იმ შემთხვევაში, თუ გარკვეული პერსონალური მონაცემი არის გადაცემული მესამე პირებისთვის, მონაცემთა სუბიექტის თანხმობა საკუთარი მონაცემის გამჟღავნების თაობაზე, ძირითადად, ვერ ჩაითვლება თავისუფალ გადაწყვეტილებად, და, შესაბამისად, არ იქნება კანონიერი ძალის მქონე მონაცემთა დაცვის სამართლის თანახმად.

მაგალითი: მგზავრებსა და ავიახაზებს შორის არსებული შეთანხმება, რომლის თანახმად ავიახაზები აწვდის ე.წ. მგზავრის სახელის ჩანაწერს (PNR), კერძოდ, მონაცემს მათი ვინაობის, კვების წესის ან ჯანმრთელობის პრობლემების შესახებ, შესაბამისი ქვეყნის საიმეგრაციო ორგანოს, ვერ იქნება მიჩნეული კანონიერი ძალის მქონე თანხმობად მონაცემთა დაცვის კანონმდებლობის მიხედვით, რამდენადაც მგზავრებს არ აქვთ არჩევანის შესაძლებლობა, როდესაც მათ სურთ კონკრეტული ქვეყნის სტუმრობა. მონაცემების ამგვარი გადაცემის კანონიერებისათვის საჭიროა სხვა სამართლებრივი საფუძველი, ძირითადად, სპეციალური კანონი.

ინფორმირებული თანხმობა

მონაცემთა სუბიექტს უნდა ჰქონდეს საკმარისი ინფორმაცია გადაწყვეტილების მიღებამდე. არის თუ არა მიწოდებული საკმარისი ინფორმაცია შესაძლებელია განისაზღვროს ყოველ კონკრეტულ შემთხვევაში. ძირითადად, ინფორმირებული თანხმობა მოიცავს საკითხის ზუსტად და ადვილად გასაგებ აღწერას, რაზეც მოითხოვება თანხმობა და, ამასთან, ნათელს ხდის თანხმობის გაცემის ან არ გაცემის შედეგებს. ინფორმირებისთვის გამოყენებული ენა უნდა იყოს ადაპტირებული ინფორმაციის შესაძლო ადრესატებისთვის.

ინფორმაცია, ასევე, უნდა იყოს ადვილად ხელმისაწვდომი მონაცემთა სუბიექტებისთვის. ინფორმაციის ხელმისაწვდომობა და გამჭვირვალობა არის მნიშვნელოვანი ელემენტი. ინტერნეტ-სივრცეში, ინფორმირების თანმიმდევრული შეტყობინებები შესაძლოა სწორი მიდგომა აღმოჩნდეს, რამდენადაც, ინფორმაციის არსებულ ვერსიასთან ერთად, მონაცემთა სუბიექტისთვის ხელმისაწვდომი იქნება მეტად განვრცობილი ვარიანტიც.

კონკრეტული თანხმობა

კანონიერი ძალის არსებობისთვის, თანხმობა, ასევე, უნდა იყოს კონკრეტული. ეს აუცილებელი პირობაა, თანხმობის საგნის შესახებ მიწოდებული ინფორმაციის ხარისხთან ერთად. ამ კონტექსტში, რიგითი მონაცემთა სუბიექტის გონივრული მოლოდინი რელევანტური იქნება. მონაცემთა სუბიექტს შესაძლოა ხელმეორედ ეთხოვოს თანხმობის გაცემა თუ დამუშავების ოპე-

რაციები უნდა იქნეს დამატებული ან შეცვლილი იმგვარად, რომ ამის განჭვრეტა, გონივრულობის ფარგლებში, შეუძლებელი იყო თავდაპირველი თანხმობის გაცემის დროს.

მაგალითი: საქმეზე Deutsche Telekom AG,¹⁰³ მართლმსაჯულების ევროპული კავშირის სასამართლოს წინაშე დადგა საკითხი, თუ რამდენად სჭირდებოდა ტელეკომ-პროვაიდერს, პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ დირექტივის¹⁰⁴ მე-12 მუხლის საფუძველზე, მისი აბონენტების პერსონალური მონაცემების გადაცემისთვის განახლებული თანხმობის მიღება მონაცემთა სუბიექტებისგან, რამდენადაც, თავდაპირველად თანხმობის გაცემისას მიმღებები არ იყვნენ დასახელებულნი.

სასამართლომ დაადგინა, რომ ამ მუხლის თანახმად, მონაცემთა გადაცემამდე განახლებული თანხმობის მიღება არ იყო აუცილებელი, ვინაიდან მონაცემთა სუბიექტებს მოცემული პირობის საფუძველზე შესაძლებლობა ჰქონდათ თანხმობა განეცხადებინათ მხოლოდ დამუშავების მიზნისთვის, რაც გულისხმობს მათი მონაცემების გამოქვეყნებას, და არ შეეძლოთ აერჩიათ ის მიმართულებები, სადაც შესაძლოა ყოფილიყო მათი მონაცემები გამოქვეყნებული.

როგორც სასამართლომ აღნიშნა „ეს გამომდინარეობს პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების დირექტივის მე-12 მუხლის კონტექსტუალური და სისტემური განმარტებიდან, სადაც მე-12 მუხლის მე-2 პუნქტის საფუძველზე არსებული თანხმობა ეხება პერსონალურ მონაცემთა საჯარო წყაროში გამოქვეყნების მიზანს და არა კონკრეტული წყაროს პროვაიდერის ვინაობას.“¹⁰⁵ გარდა ამისა, „ეს არის საჯარო წყაროში პერსონალური მონაცემების გამოქვეყნება სპეციალური მიზნისთვის, რომელიც შესაძლებელია აღმოჩნდეს ზიანის მომტანი აბონენტისთვის“¹⁰⁶ და არა მოცემული პუბლიკაციის ავტორისთვის.

103 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-543/09, Deutsche Telekom AG v. Germany, 5 მაისი 2011 წელი; იხ. ძირითადად პარაგ. 53 და 54.

104 ევროპული პარლამენტისა და საბჭოს 2002 წლის 12 ივლისის დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პირადი ცხოვრების დაცვისა და პერსონალურ მონაცემთა დამუშავების შესახებ, OJ 2002 L 201 (პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების დირექტივა).

105 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-543/09, Deutsche Telekom AG v. Germany, 5 მაისი 2011 წელი; იხ. ძირითადად, პარაგ. 61.

106 იქვე, იხ. ძირითადად, პარაგ. 62.

2.4.2. გაცემული თანხმობის ნებისმიერ დროს უკან გამოთხოვის უფლება

მონაცემთა დაცვის დირექტივა არ შეიცავს გაცემული თანხმობის ნებისმიერ დროს უკან გამოთხოვის ზოგად უფლებას. თუმცა ფართოდ აღიარებულია, რომ ამგვარი უფლება არსებობს და მონაცემთა სუბიექტებისთვის უნდა იყოს შესაძლებელი ამ უფლების რეალიზაცია საკუთარი შეხედულებისამებრ. გაცემული თანხმობის გამოთხოვის შესახებ არ უნდა მოითხოვებოდეს ახსნა-განმარტება და თანხმობის გაუქმებას არ უნდა სდევდეს ნეგატიური შედეგები ან რაიმე სარგებლის გაუქმება, რაც თავდაპირველად არსებობდა მონაცემთა გამოყენების შედეგად.

მაგალითი: მომხმარებელი თანხმდება სარეკლამო ელ-ფოსტის მიღებას მისამართზე, რომელსაც ის აწვდის მონაცემთა დამმუშავებელს. თუ მომხმარებელი გამოითხოვს თანხმობას, დამმუშავებელმა დაუყოვნებლივ უნდა შეწყვიტოს სარეკლამო ელ-ფოსტის გაგზავნა. არავითარი სანქციები, როგორიცაა პირგასამტეხლო, არ უნდა იქნეს დადგენილი.

თუ მომხმარებელი სასტუმროს ოთახის ღირებულებაზე იღებდა 5%-იან ფასდაკლებას მისი მონაცემების სარეკლამო შეტყობინებებისთვის გამოყენების გამო, თანხმობის გამოთხოვა სარეკლამო ელ-ფოსტის მიღების თაობაზე, შემდგომში, არ უნდა გახდეს აღნიშნული ფასდაკლებული პროცენტების უკან დაბრუნების მოთხოვნის საფუძველი.

3. მონაცემთა დაცვის ევროპული სამართლის საკვანძო პრინციპები

ევროპული კავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -a- და -b- ქვეპუნქტები მართლმსაჯულების ევროპული კავშირის სასამართლო, C-524/06, Huber v. Germany, 2008 წლის 16 დეკემბერი მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები C-92/09 და C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 ნოემბერი 2010 წელი	კანონიერი დამუშავების პრინციპი	108-ე კონვენცია, მე-5 მუხლის -a- და -b- ქვეპუნქტები ადამიანის უფლებათა ევროპული სასამართლო, Rotaru v. Romania [GC], No. 28341/95, 4 მაისი 2000 წელი ადამიანის უფლებათა ევროპული სასამართლო Taylor-Sabori v. the United Kingdom, No. 47114/99, 22 იანვარი 2002 წელი ადამიანის უფლებათა ევროპული სასამართლო, Peck v. the United Kingdom, No. 44647/98, 28 იანვარი 2003 წელი ადამიანის უფლებათა ევროპული სასამართლო, Khelili v. Switzerland, No. 16188/07, 18 ოქტომბერი 2011 წელი ადამიანის უფლებათა ევროპული სასამართლო, Leander v. Sweden, No. 9248/81, 26 მარტი 1987 წელი
მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -b- ქვეპუნქტი	მიზნის კონკრეტულობისა და ლიმიტირების პრინციპი	108-ე კონვენცია, მე-5 მუხლის -b- ქვეპუნქტი
მონაცემთა ხარისხის პრინციპები		
მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -c- ქვეპუნქტი	მონაცემთა შესაბამისობა	108-ე კონვენცია, მე-5 მუხლის -c- ქვეპუნქტი
მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -d- ქვეპუნქტი	მონაცემთა სიზუსტე	108-ე კონვენცია, მე-5 მუხლის -d- ქვეპუნქტი

მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -e- ქვეპუნქტი	მონაცემთა ლიმიტირებული შენახვა	108-ე კონვენცია, მე-5 მუხლის -e- ქვეპუნქტი
მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -e- ქვეპუნქტი	გამონაკლისი სამეცნიერო და სტატისტიკური კვლევებისთვის	108-ე კონვენცია, მე-9 მუხლის მე-3 ნაწილი
მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -a- ქვეპუნქტი	სამართლიანი და-მუშავეების პრინციპი	108-ე კონვენცია, მე-5 მუხლის -a- ქვეპუნქტი ადამიანის უფლებათა ევროპული სასამართლო, Haralambie v. Romania, No. 21737/03, 27 ოქტომბერი 2009 წელი ადამიანის უფლებათა ევროპული სასამართლო, K.H. and Others v. Slovakia, No. 32881/04, 28 აპრილი 2009 წელი
მონაცემთა დაცვის დირექტივა, მე-6 მუხლის მე-2 პუნქტი	ანგარიშვალ-დებულების პრინციპი	

108-ე კონვენციის მე-5 მუხლით დადგენილი პრინციპები განამტკიცებს მონაცემთა დაცვის ევროპული სამართლის არსს. ისინი გვხვდება მონაცემთა დაცვის დირექტივის მე-6 მუხლშიც, როგორც დასაბამი დირექტივის შემდგომ მუხლებში მოცემული მეტად დეტალური დებულებებისთვის. მონაცემთა დაცვის ნებისმიერი შემდგომი კანონმდებლობა, ევროპის საბჭოს ან ევროპული კავშირის დონეზე, უნდა იყოს შესაბამისი აღნიშნულ პრინციპებთან და უნდა იქნეს გათვალისწინებული შესაბამისი კანონმდებლობის ინტერპრეტირებისას. ნებისმიერი გამონაკლისი ან შეზღუდვა აღნიშნულ ძირითად პრინციპებზე შესაძლებელია დადგენილ იქნეს შიდასახელმწიფოებრივ დონეზე.¹⁰⁷ ის უნდა იყოს დადგენილი კანონით, ემსახურებოდეს ლეგიტიმურ მიზანს და უნდა იყოს აუცილებელი დემოკრატიულ საზოგადოებაში. სამივე პირობა უნდა იყოს სახეზე.

107 108-ე კონვენცია, მე-9 მუხლის მე-2 პუნქტი; მონაცემთა დაცვის დირექტივა, მე-13 მუხლის მე-2 პუნქტი.

3.1. კანონიერი დამუშავების პრინციპი

საკვანძო დებულებები

- დამუშავების კანონიერების პრინციპის გასააზრებლად, აუცილებელია შევხებით მონაცემთა დაცვის უფლების კანონიერი შეზღუდვის პირობებს ქარტიის 52-ე მუხლის პირველი პუნქტის ჩრილში და მოთხოვნებს მართლზომიერი ჩარევისთვის ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის მე-2 პუნქტის მიხედვით.
- შესაბამისად, პერსონალურ მონაცემთა დამუშავება არის კანონიერი მხოლოდ იმ შემთხვევაში თუ:
 1. არის შესაბამისობაში კანონთან; და
 2. ემსახურება ლეგიტიმურ მიზანს; და
 3. აუცილებელია დემოკრატიულ საზოგადოებაში ლეგიტიმური მიზნის მისაღწევად.

ევროპული კავშირისა და ევროპის საბჭოს მონაცემთა დაცვის კანონმდებლობის მიხედვით, კანონიერი დამუშავების პრინციპი არის პირველი დასახელებული პრინციპი; იგი განმტკიცებულია თითქმის იდენტური ფორმით 108-ე კონვენციის მე-5 მუხლსა და მონაცემთა დაცვის დირექტივის მე-6 მუხლში.

არც ერთი ზემოაღნიშნული მუხლი არ შეიცავს „კანონიერი დამუშავების“ განმარტებას. მოცემული სამართლებრივი ცნებების გასაგებად, აუცილებელია ყურადღება გავამახვილოთ ადამიანის უფლებათა ევროპული კონვენციით გათვალისწინებულ მართლზომიერ ჩარევაზე, რომელიც განმარტებულია ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკის შესაბამისად და, ასევე, კანონიერი შეზღუდვისთვის დაწესებული პირობების გათვალისწინებით, ქარტიის 52-ე მუხლის თანახმად.

3.1.1. მართლზომიერი ჩარევის საფუძვლები ადამიანის უფლებათა ევროპული კონვენციის მიხედვით

პერსონალურ მონაცემთა დამუშავება შესაძლებელია იწვევდეს მონაცემთა სუბიექტის პირადი ცხოვრების პატივისცემის უფლების დარღვევას. თუმცა, პირადი ცხოვრების პატივის-

ცემის უფლება არ არის აბსოლუტური უფლება და უნდა იქნეს განონანსორებული და შეთავსებული სხვა ლეგიტიმურ ინტერესებთან, იქნება ეს სხვა პირთა ინტერესები (კერძო ინტერესები) თუ, ზოგადად, საზოგადოებრივი (საჯარო) ინტერესები. არსებობს ბევრი შემთხვევა, სადაც პერსონალურ მონაცემთა დამუშავება და, შესაბამისად, მონაცემთა დაცვის უფლებაში ჩარევა გარდაუვალია, როდესაც არსებობს სხვათა ან საზოგადოების ლეგიტიმური ინტერესი.

პირობები, რა დროსაც სახელმწიფოს მხრიდან ჩარევა მართლზომიერია არის ქვემოთ მოყვანილი.

კანონთან შესაბამისობა

ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკის თანახმად, ჩარევა არის კანონის შესაბამისი, თუ საფუძველს წარმოადგენს შიდასახელმწიფოებრივი კანონმდებლობა, რომელსაც გააჩნია გარკვეული სტანდარტები. კანონი უნდა იყოს „ხელმისაწვდომი მოცემული პირებისთვის, ხოლო მისი შედეგები განჭვრეტადი.“¹⁰⁸ წესი განჭვრეტადია თუ „არის ფორმულირებული საკმარისი სიზუსტით, რათა ნებისმიერ ინდივიდს მიეცეს საშუალება, საჭიროების შემთხვევაში, შესაბამისი მითითების საფუძველზე განსაზღვროს მისი მოქმედება.“¹⁰⁹ „ამ შემთხვევაში, კანონით მოთხოვნილი სიზუსტის ხარისხი დამოკიდებული იქნება კონკრეტულ გარემოებებზე.“¹¹⁰

108 ადამიანის უფლებათა ევროპული სასამართლო, *Amann v. Switzerland* [GC], No. 27798/95, 16 თებერვალი 2000 წელი, პარაგ. 50; იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლო, *Kopp v. Switzerland*, No. 23224/94, 25 მარტი 1998 წელი, პარაგ. 55 და ადამიანის უფლებათა ევროპული სასამართლო, *lordachi and Others v. Moldova*, No. 25198/02, 10 თებერვალი 2009 წელი, პარაგ. 50.

109 ადამიანის უფლებათა ევროპული სასამართლო, *Amann v. Switzerland* [GC], No. 27798/95, 16 თებერვალი 2000 წელი, პარაგ. 56; იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლო, *Malone v. the United Kingdom*, No. 8691/79, 2 აგვისტო 1984 წელი, პარაგ. 66; ადამიანის უფლებათა ევროპული სასამართლო, *Silver and Others v. the United Kingdom*, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 მარტი 1983 წელი, პარაგ. 88.

110 ადამიანის უფლებათა ევროპული სასამართლო, *The Sunday Times v. the United Kingdom*, No. 6538/74, 26 აპრილი 1979 წელი, პარაგ. 49; იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლო, *Silver and Others v. the United Kingdom*, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 მარტი 1983 წელი, პარაგ. 88.

მაგალითი: საქმეზე *Rotaru v. Romania*,¹¹¹ ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა, რამდენადაც რუმინული სამართლით დასაშვები იყო საიდუმლო ფაილებში შენახვის მიზნით იმ ინფორმაციის შეგროვება, ჩანერა და დაარქივება, რაც გავლენას ახდენდა ეროვნულ უსაფრთხოებაზე, თანაც, ამ უფლებამოსილებათა შესრულებისას, შეზღუდვების დადგენის გარეშე, რაც ორგანოებს აძლევდა შეხედულებისამებრ მოქმედების საშუალებას. მაგალითად, შიდასახელმწიფოებრივი კანონმდებლობა არ განსაზღვრავდა ინფორმაციის იმ სახეს, რომელიც უნდა დამუშავებულიყო, ასევე ადამიანების კატეგორიებს ვისზეც უნდა ყოფილიყო გამოყენებული თვალთვალის ზომები, პირობები, რა დროსაც ამგვარი ზომები უნდა ყოფილიყო მიღებული ან თავად გამოყენების პროცედურა დაცული. მოცემული ნაკლოვანებების გამო, სასამართლომ აღნიშნა, რომ შიდასახელმწიფოებრივი კანონმდებლობა არ იყო შესაბამისობაში განჭვრეტადობის მოთხოვნასთან, ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის მიხედვით და, შესაბამისად, ეს მუხლი დარღვეულ იქნა.

მაგალითი: საქმეზე *Taylor-Sabori v. the United Kingdom*,¹¹² განმცხადებელი აყვანილ იქნა პოლიციის თვალთვალის ქვეშ. განმცხადებლის პეიჯერიდან სპეციალური ტექნოლოგიის გამოყენებით პოლიციამ შეძლო განმცხადებელთან გაგზავნილ შეტყობინებებზე წვდომა. შემდგომ იგი დააკავეს და ბრალად დასდეს ნარკოტიკული საშუალების საიდუმლო მომარაგება. მისი სასამართლო პროცესის ნაწილი ეხებოდა პეიჯერის მესიჯების მიმოწერას, რომელიც გაშიფრულ იქნა პოლიციის მიერ. თუმცა, განმცხადებლის სასამართლო პროცესის მიმდინარეობისას, ბრიტანულ კანონმდებლობაში არ მოიპოვებოდა დებულება, რომელიც არეგულირებდა პირადი სატელეკომუნიკაციო სისტემების მეშვეობით განხორციელებულ კომუნიკაციაზე წვდომას. შესაბამისად, მის უფლებებში ჩარევა არ იყო „კანონთან შესაბამისი.“ სასამართლომ დაადგინა, რომ ადგილი ჰქონდა კონვენციის მე-8 მუხლის დარღვევას.

111 ადამიანის უფლებათა ევროპული სასამართლო, *Rotaru v. Romania* [GC], No. 28341/95, 4 მაისი 2000 წელი, პარაგ. 57; იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლო, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, No. 62540/00, 28 ივნისი 2007 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *Shimovolos v. Russia*, No. 30194/09, 21 ივნისი 2011 წელი; და ადამიანის უფლებათა ევროპული სასამართლო, *Vetter v. France*, No. 59842/00, 31 მაისი 2005 წელი.

112 ადამიანის უფლებათა ევროპული სასამართლო, *Taylor-Sabori v. the United Kingdom*, No. 47114/99, 22 ოქტომბერი 2002 წელი.

ლეგიტიმური მიზნის დაკმაყოფილება

ლეგიტიმური მიზანი შესაძლებელია იყოს საჯარო ინტერესთა შორის ერთ-ერთი ან სხვათა უფლებებისა და თავისუფლებების დაცვა.

მაგალითი: საქმეზე *Peck v. the United Kingdom*,¹¹³ განმცხადებელმა გადაწყვიტა თავის მოკვლა ქუჩაში, მაჯის გადაჭრით, რა დროსაც, არ იცოდა, რომ ამ მცდელობისას ვიდეოთვალთვალის (CCTV) კამერა იღებდა მას. იმის შემდეგ, რაც პოლიციამ, რომელიც ახორციელებდა მონიტორინგს, გადაარჩინა იგი, ვიდეოჩანაწერი გადაეცა მედიას, რომელმაც გამოაქვეყნა იგი განმცხადებლის სახის დაფარვის გარეშე. სასამართლომ დაადგინა, რომ რელევანტური და საკმარისი მიზეზი, სახელმწიფო ორგანოს მიერ ჩანაწერის საჯაროდ პირდაპირ გადაცემის მართლზომიერებისთვის განმცხადებლის თანხმობის ან მისი ვინაობის დაფარვის გარეშე, არ არსებობდა. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

აუცილებელი დემოკრატიულ საზოგადოებაში

ადამიანის უფლებათა ევროპულმა სასამართლომ განაცხადა: „აუცილებლობის ცნება გულისხმობს, რომ ჩარევა დაკავშირებულია მომეტებულ საზოგადოებრივ საჭიროებასთან, კერძოდ, მისალწვეი ლეგიტიმური მიზნის პროცესორციულია.“¹¹⁴

მაგალითი: საქმეში *Khelili v. Switzerland*,¹¹⁵ პოლიციის მიერ შემონმებისას განმცხადებელს აღმოაჩნდა სატარებელი საკონტაქტო ბარათები, რომელზეც ეწერა: „სასიამოვნო, მოხდენილი ქალი, ორმოც წლამდე ასაკის, შეხვდება მამაკაცს სასმელის დალევისა და პერიოდულად სეირნობის მიზნით. ტელეფონის ნომერი.“ განმცხადებელი იუწყებოდა, რომ აღნიშნული აღმოჩენის შედეგად, პოლიციამ თავიანთ ბაზაში იგი „მეძვად“ მოიხსენია, რა საქმიანობასაც იგი კატეგორიულად უარყოფდა. განმცხადებელმა მოითხოვა სიტყვა „მეძავის“ ამოშლა პოლიციის კომპიუტერული ბაზიდან. სასამართლომ აღიარა, რომ, ზოგადად, ინდივიდის პერსონალური მონაცემების შენახვა იმ საფუძვლით, რომ პირმა შესაძლოა ჩაიდინოს სხვა

113 ადამიანის უფლებათა ევროპული სასამართლო, *Peck v. the United Kingdom*, No. 44647/98, 28 იანვარი 2003, ძირითადად პარაგ. 85.

114 ადამიანის უფლებათა ევროპული სასამართლო, *Leander v. Sweden*, No. 9248/81, 26 მარტი 1987 წელი, პარაგ. 58.

115 ადამიანის უფლებათა ევროპული სასამართლო, *Khelili v. Switzerland*, No. 16188/07, 18 ოქტომბერი 2011 წელი.

სამართალდარღვევა, გარკვეული შემთხვევების გათვალისწინებით, შესაძლოა იყოს თანაზომიერი. თუმცა, განმცხადებლის საქმეში, პროსტიტუციაზე მითითება იყო ძალიან ბუნდოვანი და ზოგადი, არ იყო გამყარებული კონკრეტული ფაქტებით, რამდენადაც იგი არასდროს ყოფილა გასამართლებული პროსტიტუციისთვის და, შესაბამისად, კონვენციის მე-8 მუხლის თანახმად, ვერ იქნებოდა მიჩნეული მომეტებული საზოგადოებრივი საჭიროების ხარისხის მქონედ. აღიარებული, როგორც ორგანოთა ვალდებულება, დემიტკიცებინათ განმცხადებლის შესახებ ჩანერილ მონაცემთა სისწორე და, ასევე, განმცხადებლის უფლებებში ჩარევის სერიოზულობის გათვალისწინებით, სასამართლომ დაადგინა, რომ წლების განმავლობაში პოლიციის მიერ სიტყვა „მეძავის“ შენახვა შესაბამის ჩანაწერებში არ წარმოადგენდა აუცილებლობას დემოკრატიულ საზოგადოებაში. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

მაგალითი: საქმეზე *Leander v. Sweden*,¹¹⁶ ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ იმ პიროვნებების ფარული შემოწმება, რომლებსაც სურთ დაიკავონ ეროვნული უსაფრთხოების უზრუნველსაყოფად არსებული პოზიცია, თავისი არსით, არ იყო წინააღმდეგობაში დემოკრატიულ საზოგადოებაში აუცილებლობის მოთხოვნასთან. მონაცემთა სუბიექტის ინტერესების დასაცავად უსაფრთხოების სპეციალური ზომები განსაზღვრული იყო შიდასახელმწიფოებრივი კანონით, მაგალითად, კონტროლს ახორციელებდა პარლამენტი და იუსტიციის კანცლერი, რამაც სასამართლო მიიყვანა დასკვნამდე, რომ პერსონალის კონტროლის შვედური სისტემა შეესაბამებოდა კონვენციის მე-8 მუხლის მე-2 პუნქტის მოთხოვნებს. არსებული დისკრეციიდან გამომდინარე, მოპასუხე სახელმწიფოს თანახმად, აპლიკანტის საქმეში ეროვნული უსაფრთხოების ინტერესები წინ იდგა ინდივიდუალურ ინტერესებზე. სასამართლომ დაადგინა, რომ კონვენციის მე-8 მუხლის დარღვევას ადგილი არ ჰქონდა.

3.1.2. კანონიერი შეზღუდვის პირობები ევროპული კავშირის ქარტიის მიხედვით

ქარტიის სტრუქტურა და სიტყვათაწყობა განსხვავებულია კონვენციისგან. ქარტია არ საუბრობს აღიარებულ უფლებებში ჩარევის შესახებ, თუმცა იგი შეიცავს დებულებებს განმტკიცებული უფლებების რეალიზაციის შეზღუდვების თაობაზე.

52-ე მუხლის პირველი პუნქტის თანახმად, ქარტიით აღიარ-

¹¹⁶ ადამიანის უფლებათა ევროპული სასამართლო, *Leander v. Sweden*, No. 9248/81, 26 მარტი 1987 წელი, პარაგ. 59 და 67.

რებული უფლებებისა და თავისუფლებების და, შესაბამისად, პერსონალურ მონაცემთა დაცვის უფლების რეალიზაციის შეზღუდვა პერსონალურ მონაცემთა დამუშავების სახით, ნებადართულია მხოლოდ მაშინ თუ იგი:

- დადგენილია კანონით; და
- იცავს მონაცემთა დაცვის ძირითად არსს; და
- აუცილებელია, ექვემდებარება პროპორციულობის პრინციპს; და
- ემსახურება გაერთიანების მიერ აღიარებულ საზოგადო ინტერესის მიზნებს ან საჭიროა სხვათა უფლებებისა და თავისუფლებების დასაცავად.

მაგალითი: საქმეზე Volker and Markus Schecke,¹¹⁷ მართლმსაჯულების ევროპული კავშირის სასამართლომ დაასკვნა, რომ კონკრეტული აგრარული ფონდების ბენეფიციარი ფიზიკური პირების პერსონალური მონაცემების გამოქვეყნების ვალდებულების დაკისრებით, რომელიც არ ადგენდა განსხვავებას გარკვეული კრიტერიუმების მიხედვით, კერძოდ, პირების მიერ დახმარების მიღების პერიოდების, მათი სიხშირის ან ხასიათისა და ოდენობის გათვალისწინებით, საბჭო და კომისია გასცდა პროპორციულობის პრინციპით დადგენილ შეზღუდვებს.

შესაბამისად, სასამართლომ დაადგინა, რომ აუცილებელი იყო საბჭოს რეგულაციის 1290/2005 კონკრეტული დებულებების, ხოლო 259/3008 რეგულაციის სრულიად ძალადაკარგულად გამოცხადება.¹¹⁸

მიუხედავად განსხვავებული სიტყვათაწყობისა, ქარტიის 52-ე მუხლის პირველი პუნქტით დადგენილი კანონიერი დამუშავების პირობები მსგავსია კონვენციის მე-8 მუხლის მე-2 პუნქტის. გარდა ამისა, ქარტიის 52-ე მუხლის პირველი პუნქტით

117 მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები, C-92/09 და C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 ნოემბერი 2010 წელი, პარაგ. 89 და 86.

118 საბჭოს 2005 წლის 21 ივნისის რეგულაცია საერთო აგრარული პოლიტიკის დაფინანსების შესახებ (EC) No. 1290/2005, OJ 2005 L 209; და კომისიის 2008 წლის 18 მარტის რეგულაცია (EC) No. 259/2008 საბჭოს (EC) No. 1290/2005 რეგულაციის ამოქმედების დეტალური წესების განსაზღვრის შესახებ ევროპული აგრარული საგარანტიო ფონდისა (EAGF) და სასოფლო განვითარების ევროპული აგრარული ფონდის (EAFRD) ბენეფიციარების შესახებ ინფორმაციის გამოქვეყნების თაობაზე, OJ 2008 L 76.

განსაზღვრული პირობები უნდა იქნეს განხილული, როგორც კონვენციის მე-8 მუხლის მეორე პუნქტთან თანხვედრაში მყოფი, რამდენადაც ქარტიის 52-ე მუხლის მე-3 პუნქტი, პირველი წინადადებით, ადგენს: „რამდენადაც ქარტია განსაზღვრავს უფლებებს, რომელიც თანხვედრაშია ადამიანის უფლებებისა და ძირითადი თავისუფლებების დაცვის კონვენციით გარანტირებულ უფლებებთან, მათი შინაარსი და ფარგლები არის კონვენციით მოცემული უფლებების მსგავსი.“

თუმცა, 52-ე მუხლის მესამე პუნქტის ბოლო წინადადების თანახმად, „ეს დებულება არ უკრძალავს კავშირის სამართალს დაადგინოს მეტად ფართო დაცვა.“ კონვენციის მე-8 მუხლის მეორე პუნქტისა და ქარტიის 52-ე მუხლის მესამე პუნქტის პირველი წინადადების შედარების შედეგად, ეს მხოლოდ იმას ნიშნავს, რომ კონვენციის მე-8 მუხლის მე-2 პუნქტით გათვალისწინებული მართლზომიერი ჩარევის პირობები, ქარტიის თანახმად, წარმოადგენს მინიმალურ მოთხოვნას მონაცემთა დაცვის უფლების კანონიერი შეზღუდვისთვის. შესაბამისად, ევროპული კავშირის სამართლის მიხედვით, პერსონალური მონაცემების კანონიერი დამუშავება მოითხოვს, სულ მცირე, კონვენციის მე-8 მუხლის მე-2 პუნქტით დადგენილი პირობების დაცვას. ამავდროულად, ევროპული კავშირის კანონმდებლობით, შესაძლოა განისაზღვროს დამატებითი მოთხოვნები, კონკრეტულ შემთხვევებში.

კანონიერი დამუშავების პრინციპების თანხვედრა ევროპული კავშირისა და კონვენციის დებულებებს შორის, ასევე, განმტკიცებულია ევროპული კავშირის შესახებ ხელშეკრულების მე-6 მუხლის მესამე პუნქტით, რომლის თანახმად „ძირითადი უფლებები, გარანტირებული ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციით, აყალიბებს კავშირის სამართლის ძირითად პრინციპებს.“

3.2. მიზნის კონკრეტულობისა და ლიმიტირების პრინციპი

საკვანძო დებულებები

- მონაცემთა დამუშავების მიზანი ნათლად უნდა იყოს განსაზღვრული დამუშავების დაწყებამდე.
- ევროპული კავშირის კანონმდებლობის მიხედვით, დამუშავების მიზანი უნდა იყოს მკაფიოდ დადგენილი; ევროპის საბჭოს კანონმდებლობის თანახმად, ამ საკითხის განსაზღვრის უფლება აქვთ უშუალოდ სახელმწიფოებს.
- მონაცემთა დამუშავება განუსაზღვრელი მიზნისთვის არ არის შესაბამისობაში მონაცემთა დაცვის სამართალთან.
- სხვა მიზნისთვის მონაცემთა შემდგომი გამოყენება საჭიროებს დამატებით სამართლებრივ საფუძველს თუ დამუშავების ახალი მიზანი შეუთავსებელია თავდაპირველ მიზანთან.
- მესამე მხარისთვის მონაცემთა გადაცემა არის ახალი მიზანი, რაც საჭიროებს დამატებით სამართლებრივ საფუძველს.

არსობრივად, მიზნის კონკრეტულობისა და ლიმიტირების პრინციპი ნიშნავს, რომ პერსონალურ მონაცემთა დამუშავების ლეგიტიმურობის საკითხი დამოკიდებულია დამუშავების მიზანზე.¹¹⁹ მიზანი უნდა იყოს განსაზღვრული და გაცხადებული დამუშავებლის მიერ მონაცემთა დამუშავების დაწყებამდე.¹²⁰ ევროპული კავშირის კანონმდებლობის მიხედვით, ეს უნდა განხორციელდეს დეკლარირებით, სხვა სიტყვებით, შესაბამისი საზედამხედველო ორგანოსთვის შეტყობინების გზით ან შიდა დოკუმენტით მაინც, რომელიც დამუშავებელმა ხელმისაწვდომი უნდა გახადოს შემონმგებისთვის ზედამხედველი ორგანოსთვის და, ასევე, იყოს ხელმისაწვდომი მონაცემთა სუბიექტისთვის.

პერსონალური მონაცემების დამუშავება განუსაზღვრელი ან/და შეუზღუდავი მიზნებისთვის უკანონოა.

119 108-ე კონვენცია, მე-5 მუხლის -b- ქვეპუნქტი; მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -b- ქვეპუნქტი.

120 იხ. ასევე, მუხლი 29 სამუშაო ჯგუფი (2013), მოსაზრება 03/2013 მიზნის ლიმიტირების შესახებ, WP 203, ბრიუსელი, 2 აპრილი 2013 წელი.

მონაცემთა დამუშავების ყოველ ახალ მიზანს უნდა ჰქონდეს საკუთარი კონკრეტული სამართლებრივი საფუძველი და ვერ დაეფუძნება იმ ფაქტს, რომ მონაცემები იქნა თავდაპირველად მიღებული ან დამუშავებული სხვა ლეგიტიმური მიზნისთვის. თავის მხრივ, ლეგიტიმური დამუშავება ლიმიტირებულია მხოლოდ მის საწყის მიზნამდე და დამუშავების ნებისმიერი სხვა მიზანი ითხოვს დამოუკიდებელ და ახალ სამართლებრივ საფუძველს. მონაცემთა გამჟღავნება მესამე მხარისთვის საჭიროებს ფრთხილ მიდგომას, რამდენადაც გამჟღავნება წარმოადგენს ახალ მიზანს და, შესაბამისად, მოითხოვს სამართლებრივ საფუძველს, რომელიც განსხვავებულია მონაცემთა შეგროვების მიზნისგან.

მაგალითი: ავიახაზები აგროვებს მონაცემებს საკუთარი მგზავრების შესახებ, რათა განახორციელოს დაჯავშნა ფრენების სათანადო მართვისთვის. ავიახაზებს სჭირდება შემდეგი სახის მონაცემები: მგზავრების ადგილის ნომრები; სპეციალური ფიზიკური შეზღუდვების საჭიროების შესახებ ინფორმაცია, როგორცაა ეტლი; და სპეციალური საკვების მოთხოვნილება, როგორცაა რელიგიური წესების თანახმად დაშვებული საკვები. თუ ამ მონაცემთა გადაცემას, რომელიც ჩანერილია მგზავრის სახელის ჩანაწერში (PNR), ავიახაზებისგან ჩაფრენის ადგილას მოითხოვს საიმისგრაფიო სამსახური, ეს მონაცემები იქნება გამოყენებული საიმისგრაფიო კონტროლის მიზნებისთვის, რომელიც განსხვავდება მონაცემთა შეგროვების თავდაპირველი მიზნისგან. შესაბამისად, ამ მონაცემთა გადაცემა საიმისგრაფიო სამსახურისთვის საჭიროებს ახალ და დამოუკიდებელ სამართლებრივ საფუძველს.

როდესაც განიხილება კონკრეტული მიზნის ფარგლები და მოცულობა, 108-ე კონვენცია და მონაცემთა დაცვის დირექტივა ეყრდნობა თავსებადობის კონცეფციას: მონაცემთა გამოყენება თავსებადი მიზნებისთვის დაშვებულია მხოლოდ საწყისი სამართლებრივი საფუძველით. თუმცა, რას ნიშნავს „თავსებადი“, არ არის განსაზღვრული და ექვემდებარება განმარტებას ყოველი კონკრეტული ვითარებიდან გამომდინარე.

მაგალითი: კომპანია „მზის სხივის“ მომხმარებლების მონაცემთა გაყიდვა, რომელიც მოპოვებულია მომხმარებელთან ურთიერთობების მართვის პროცესში, პირდაპირი მარკეტინგის კომპანია „მთვარის შუქისთვის“, რომელსაც სურს ამ მონაცემთა გამოყენება სხვა კომპანიების მარკეტინგული პროგრამების ხელშეწყობისთვის – ნარმოადგენს ახალ მიზანს, რომელიც შეუთავსებელია მომხმარებელთან ურთიერთობის მართვის მიზნებთან, ანუ კომპანია „მზის სხივის“ მიერ მომხმარებელთა მონაცემების შეგროვების თავდაპირველ მიზანთან. „მთვარის შუქისთვის“ მონაცემთა მიყიდვა მოითხოვს დამოუკიდებელ სამართლებრივ საფუძველს.

საპირისპიროდ, კომპანია „მზის სხივის“ მიერ მომხმარებელთან ურთიერთობის მართვის პროცესში მოპოვებული მონაცემების გამოყენება საკუთარი მარკეტინგული მიზნებისთვის, რაც გულისხმობს კომპანიის პროდუქციის შესახებ მარკეტინგული შეტყობინებების გაგზავნას მომხმარებელთათვის, მიიჩნევა თავსებად მიზნად.

მონაცემთა დაცვის დირექტივა მკაფიოდ ადგენს, რომ „მონაცემთა შემდგომი დამუშავება ისტორიული, სტატისტიკური ან სამეცნიერო მიზნებისთვის არ უნდა ჩაითვალოს შეუსაბამოდ, თუ ნევრი ქვეყნები ადგენენ დაცვის შესაბამის მექანიზმებს.“¹²¹

მაგალითი: კომპანია „მზის ნათება“ შეაგროვა და შეინახა მომხმარებელთან ურთიერთობის მართვის (CRM) მონაცემები საკუთარი მომხმარებლების შესახებ. კომპანიის მიერ ამ მონაცემთა შემდგომი გამოყენება დასაშვებია მომხმარებლების შესყიდვების თავისებურებათა სტატისტიკური ანალიზისთვის, რამდენადაც სტატისტიკა არის თავსებადი მიზანი. დამატებითი სამართლებრივი საფუძველი, როგორიცაა მონაცემთა სუბიექტების თანხმობა, არ არის საჭირო.

თუ იგივე მონაცემები უნდა გადაეცეს მესამე მხარეს, მაგალითად კომპანიას „ვარსკვლავთნათება“, მხოლოდ სტატისტიკური მიზნებისთვის, გადაცემა დასაშვებია დამატებითი სამართლებრივი საფუძვლის გარეშე, მაგრამ მხოლოდ იმ შემთხვევაში თუ მიღებულია უსაფრთხოების შესაბამისი ზომები, როგორიცაა მონაცემთა სუბიექტების ვინაობის გასაიდუმლოება, რამდენადაც ვინაობა, ძირითადად, არ არის საჭირო სტატისტიკური მიზნებისთვის.

¹²¹ ამგვარი შიდასახელმწიფოებრივი საკანონმდებლო დებულების მაგალითი მოცემულია ავსტრიის მონაცემთა დაცვის აქტით, (Datenschutzgesetz), Fed. Law Gazette I No. 165/1999, პარაგ. 46, ხელმისაწვდომია ინგლისურ ენაზე: www.dsk.gv.at/DocView.axd?CobId=41936.

3.3. მონაცემთა ხარისხის პრინციპები

საკვანძო დებულებები

- მონაცემთა ხარისხის პრინციპები უნდა იქნეს იმპლემენტირებული მონაცემთა დამმუშავებლის მიერ დამუშავების ნებისმიერ პროცესში.
- მონაცემთა ლიმიტირებული შენახვის პრინციპი აუცილებელს ხდის მონაცემის ნაშლას მაშინვე, როდესაც ის აღარ არის საჭირო იმ მიზნისთვის, რომლისთვისაც შეგროვდა.
- გამონაკლისები ლიმიტირებული შენახვის პრინციპისგან უნდა იქნეს დადგენილი კანონით და საჭიროებს უსაფრთხოების დამატებით სპეციალურ ზომებს მონაცემთა სუბიექტების დასაცავად.

3.3.1. მონაცემთა შესაბამისობის პრინციპი

მხოლოდ ისეთი მონაცემები შეიძლება დამუშავდეს, რომელიც არის „ადეკვატური, შესაბამისი და არ არის ჭარბი იმ მიზნიდან გამომდინარე, რომლისთვისაც ისინი შეგროვდა ან/და შემდგომში დამუშავდა.“¹²² დასამუშავებლად არჩეულ მონაცემთა კატეგორიები უნდა იყოს აუცილებელი დამუშავების გაცხადებული საერთო მიზნის მისაღწევად და დამმუშავებელმა მკაცრად უნდა შეზღუდოს მონაცემთა დამუშავება იმ ინფორმაციამდე, რაც არის შესაბამისი მხოლოდ დამუშავების კონკრეტული მიზნისთვის.

თანამედროვე საზოგადოებაში, შესაბამისობის პრინციპს გააჩნია დამატებითი მნიშვნელობა: პირადი ცხოვრების გამაძლიერებელი სპეციალური ტექნოლოგიების გამოყენებით, ზოგჯერ, შესაძლებელია საერთოდ თავიდან იქნეს აცილებული პერსონალურ მონაცემთა გამოყენება, ან გამოყენებულ იქნეს ფსევდონიმირებული მონაცემები, რომელიც შედეგად იძლევა პირად ცხოვრებასთან თავსებად მიდგომებს. ეს ძირითადად მიზანშეწონილია დამუშავების მასშტაბური სისტემებისთვის.

122 108-ე კონვენცია, მე-5 მუხლის -c- ქვეპუნქტი; მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -c- ქვეპუნქტი.

მაგალითი: ქალაქის საბჭო ქალაქის საზოგადოებრივი ტრანსპორტის სისტემის მუდმივ მომხმარებლებს გარკვეულ საფასურად სთავაზობს ჩიპურ ბარათებს. ბარათის ზადაპირზე დატანილია მომხმარებლის სახელი წერილობითი ფორმით და, ასევე, ელექტრონული ფორმით – ჩიპზე. მიუხედავად იმისა, ავტობუსი იქნება გამოყენებული თუ ტრამვაი, ჩიპური ბარათი უნდა იქნეს გატარებული დამონტაჟებული წასაკითხი მოწყობილობების პირისპირ. მონაცემები, რომლებიც იკითხება დამონტაჟებული მოწყობილობის მიერ ელექტრონულად მოწმდება მონაცემთა იმ ბაზაში, რომელიც შეიცავს სამგზავრო ბარათების შემსყიდველი ადამიანების სახელებს.

სისტემა არ მოქმედებს შესაბამისობის პრინციპის გათვალისწინებით მართებულად: იმის შემოწმება, თუ რამდენად არის ინდივიდი უფლებამოსილი გამოიყენოს სატრანსპორტო საშუალებები შესაძლებელია იქნეს განხორციელებული ჩიპზე დატანილი პერსონალური მონაცემების ბაზასთან შედარების გარეშეც. საკმარისი იქნებოდა, მაგალითად, ბარათის ჩიპზე სპეციალური ელექტრონული გამოსახულების არსებობა, როგორიცაა შტრიხ-კოდი, რომელიც წამკითხველი მოწყობილობის პირისპირ გატარებისას დაადასტურებდა ბარათის სისწორეს. ამგვარი სისტემა არ ჩაინერდა თუ ვის მიერ და რა დროს იქნა გამოყენებული ბარათი. პერსონალური მონაცემი არ შეგროვდებოდა, რაც წარმოადგენს ოპტიმალურ გადაწყვეტას შესაბამისობის პრინციპის მიხედვით, რამდენადაც ეს პრინციპი ადგენს მონაცემთა შეგროვების მინიმუმამდე დაყვანის ვალდებულებას.

3.3.2. მონაცემთა სისწორის პრინციპი

დამმუშავებელმა, რომელიც ფლობს პერსონალურ ინფორმაციას, არ უნდა გამოიყენოს იგი, თუ გონივრულობის ფარგლებში არ მიიღებს შესაბამის ზომებს მონაცემთა სისწორისა და განახლების უზრუნველსაყოფად.

მონაცემთა სისწორის უზრუნველყოფის ვალდებულება უნდა იქნეს განხილული მონაცემთა დამუშავების მიზნიდან გამომდინარე.

მაგალითი: ავეჯის გამყიდველმა კომპანიამ შეაგროვა მომხმარებლების ვინაობა და მისამართი ანგარიშსწორების მიზნებისთვის. ექვსი თვის შემდეგ, იმავე კომპანიას სურს მარკეტინგის კამპანიის დაწყება და უნდა, რომ დაუკავშირდეს ყოფილ მომხმარებლებს. ამ მიზნით, კომპანიას სურს განახორციელოს წვდომა რეზიდენტების ეროვნულ რეესტრზე, რომელიც, დიდი ალბათობით, შეიცავს განახლებულ მისამართებს, რამდენადაც რეზიდენტებს აქვთ რეესტრისთვის მათი მოქმედი მისამართის შეტყობინების ვალდებულება. ამ რეესტრში არსებულ მონაცემებზე წვდომა დასაშვებია მხოლოდ იმ პირებისთვის, რომლებსაც გააჩნიათ მართლზომიერი მიზეზი.

ამ შემთხვევაში, კომპანია ვერ გამოიყენებს იმ არგუმენტს, რომ მონაცემები უნდა იყოს სწორი და განახლებული, რათა რეზიდენტების რეესტრიდან შეაგროვოს ყოფილი მომხმარებლების განახლებული მისამართები. მონაცემები შეგროვებულ იქნა ანგარიშსწორების პროცესში; ამ მიზნისთვის, გაყიდვის დროს არსებული მისამართი საკმარისი იყო. არ არსებობს სამართლებრივი საფუძველი ახალი მისამართების შესაგროვებლად, რამდენადაც მარკეტინგი არ არის მონაცემთა დაცვის უფლებაზე მაღლა მდგომი ინტერესი, და, შესაბამისად, რეესტრის მონაცემებთან წვდომა არ იქნება მართლზომიერი.

შეიძლება წარმოიშვას შემთხვევები, როდესაც შენახული მონაცემების განახლება სამართლებრივად აკრძალულია, რამდენადაც მონაცემთა შენახვის მიზანს მომხდარი მოვლენები წარმოადგენს.

მაგალითი: სამედიცინო ოპერაციის ჩანაწერები არ უნდა იქნეს შეცვლილი, სხვა სიტყვებით „განახლებული,“ იმ შემთხვევაშიც კი, თუ ჩანაწერში არსებული შენიშვნები შემდგომში მცდარი აღმოჩნდება. ამ ვითარებაში, შესაძლებელია გაკეთდეს მხოლოდ დამატებები იმ შენიშვნებისადმი, რაც მოცემულია ჩანაწერებში იმდენად, რამდენადაც მითითებული იქნება, როგორც შემდგომ ეტაპზე განხორციელებული მოქმედება.

მეორე მხრივ, არსებობს შემთხვევები, სადაც მონაცემთა სისწორის რეგულარული შემოწმება, მათ შორის, განახლება არის აუცილებელი, იმ პოტენციური ზიანის გამო, რაც შეიძლება მიადგეს მონაცემთა სუბიექტს არაზუსტი მონაცემების დატოვების შემთხვევაში.

მაგალითი: თუ პირს სურს ხელშეკრულების გაფორმება საბანკო დაწესებულებასთან, ბანკი, ჩვეულებისამებრ, ამონმებს სავარაუდო მომხმარებლის გადახდისუნარიანობას. ამ მიზნისთვის, არსებობს სპეციალური მონაცემთა ბაზები, რომელიც შეიცავს ფიზიკური პირების საკრედიტო ისტორიის შესახებ მონაცემებს. თუ ამგვარი მონაცემთა ბაზა ინდივიდის შესახებ შეიცავს არასწორ ან მოძველებულ მონაცემებს, ეს პირი შესაძლოა აღმოჩნდეს რთულ სიტუაციაში. ამგვარი მონაცემთა ბაზების დამმუშავებლებმა უნდა გასწიონ შესაბამისი ძალისხმევა სისწორის პრინციპის დაცვის უზრუნველსაყოფად.

ამასთან, მონაცემები, რომელიც ეხება ვარაუდს და არა ფაქტებს, როგორცაა დანაშაულის გამოძიება, შესაძლებელია შეგორვებულ და შენახულ იქნეს თუ დამმუშავებელს გააჩნია ამგვარი ინფორმაციის შეგროვების სამართლებრივი საფუძველი და თუ იგი საკმარისად მართლზომიერია აღნიშნული ექვის ფორმირებისთვის.

3.3.3. მონაცემთა ლიმიტირებული შენახვის პრინციპი

მონაცემთა დაცვის დირექტივის მე-6 მუხლის პირველი პუნქტის -e- ქვეპუნქტი, ისევე როგორც 108-ე კონვენციის მე-5 მუხლის -e- ქვეპუნქტი, ავალდებულებს წევრ ქვეყნებს პერსონალური მონაცემების „შენახვას იმგვარი ფორმით, რომელიც იძლევა მონაცემთა სუბიექტების იდენტიფიცირების საშუალებას იმ ვადით, რაც საჭიროა მონაცემთა შეგროვების მიზნის მიღწევისთვის ან შემდგომი დამუშავების მიზნისთვის“. შესაბამისად, მონაცემები უნდა იქნეს განადგურებული ამ მიზნების მიღწევისთანავე.

საქმეზე S. and Marper, ადამიანის უფლებათა ევროპულმა სასამართლომ დაასკვნა, რომ ევროპის საბჭოს რელევანტური ინსტრუმენტების ძირითადი პრინციპები, ხელშემკვრელი მხარეების კანონმდებლობა და პრაქტიკა მოითხოვს მონაცემთა პროპორციულ შენახვას შეგროვების მიზანთან მიმართებით, შეზღუდული ვადით, განსაკუთრებით, პოლიციის სექტორში.¹²³

123 ადამიანის უფლებათა ევროპული სასამართლო, S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 დეკემბერი 2008 წელი; იხ. ასევე, მაგ. ადამიანის უფლებათა ევროპული სასამართლო M.M. v. the United Kingdom, No. 24029/07, 13 ნოემბერი 2012 წელი.

პერსონალურ მონაცემთა შენახვის ვადების შეზღუდვა ვრცელდება მხოლოდ იმ მონაცემებზე, რომლითაც შესაძლებელია მონაცემთა სუბიექტის იდენტიფიცირება. იმ მონაცემების კანონიერი შენახვა, რომელიც აღარ არის საჭირო, შესაძლოა უზრუნველყოფილ იქნეს ანონიმიზაციით ან ფსევდონიმიზაციით.

მონაცემთა შენახვა სამომავლო სამეცნიერო, ისტორიული ან სტატისტიკური გამოყენებისთვის, მონაცემთა დაცვის დირექტივის მიხედვით, არის მკაფიოდ გამოცალკევებული მონაცემთა ლიმიტირებული შენახვის პრინციპისგან.¹²⁴ პერსონალურ მონაცემთა მიმდინარე შენახვასა და გამოყენებას თან უნდა სდევდეს შიდასახელმწიფოებრივი კანონმდებლობით დადგენილი უსაფრთხოების ზომები.

3.4. მონაცემთა სამართლიანი დამუშავების პრინციპი

საკვანძო დებულებები

- სამართლიანი დამუშავება გულისხმობს მის გამჭვირვალობას, განსაკუთრებით, მონაცემთა სუბიექტების წინაშე.
- დამმუშავებლებმა მონაცემთა სუბიექტებს, მათ შესახებ მონაცემთა დამუშავებამდე, უნდა აცნობონ, სულ მცირე, დამუშავების მიზნის, დამმუშავებლის ვინაობისა და მისი მისამართის შესახებ.
- გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა, პერსონალურ მონაცემთა საიდუმლო და ფარული დამუშავება არ უნდა ხორციელდებოდეს.
- მონაცემთა სუბიექტებს უფლება აქვთ განახორციელონ წვდომა საკუთარ მონაცემებზე დამუშავების ადგილის მიუხედავად.

სამართლიანი დამუშავების პრინციპი, უპირველესად, არეგულირებს მონაცემთა დამმუშავებელსა და მონაცემთა სუბიექტს შორის ურთიერთობას.

124 მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -e ქვეპუნქტი.

3.4.1. გამჭვირვალობა

აღნიშნული პრინციპი ადგენს დამმუშავებლის ვალდებულებას მოახდინოს მონაცემთა სუბიექტების ინფორმირება მათი მონაცემების გამოყენების თაობაზე.

მაგალითი: საქმეზე *Haralambie v. Romania*,¹²⁵ განმცხადებელი ითხოვდა სიღუმლო სამსახურის მიერ მის შესახებ შენახულ ინფორმაციაზე წვდომას, თუმცა მისი მოთხოვნა დაკმაყოფილებულ იქნა მხოლოდ ხუთი წლის შემდეგ. ადამიანის უფლებათა ევროპულმა სასამართლომ არაერთხელ აღნიშნა, რომ ინდივიდებს, რომელთა შესახებ სახელმწიფო დანესებულების მიერ შენახული იყო პერსონალური ფაილები, წვდომასთან მიმართებით გააჩნდათ სასიცოცხლო ინტერესი. სახელმწიფო ორგანოს ჰქონდა ამგვარ ინფორმაციასთან წვდომის უზრუნველსაყოფად ეფექტური პროცედურის დადგენის ვალდებულება. სასამართლომ აღნიშნა, რომ არც შენახული ფაილების რიცხვი და არც არქივირებასთან დაკავშირებული პრობლემები არ ხდიდა მართლზომიერს განმცხადებლის ფაილებზე წვდომის მოთხოვნის ხუთი წლით გადავადებას. სახელმწიფო ორგანოებმა ვერ უზრუნველყვეს განმცხადებლისთვის ეფექტური და ხელმისაწვდომი პროცედურის არსებობა, რათა მას გონივრულ ვადაში ჰქონოდა საკუთარ პერსონალურ ფაილებზე წვდომის განხორციელების შესაძლებლობა. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

დამმუშავების მოქმედებები უნდა იყოს განმარტებული მონაცემთა სუბიექტებისთვის მარტივად აღქმადი ფორმით, რაც უზრუნველყოფს მათ მიერ მონაცემებზე შემდგომი პროცდურების გააზრებას. მონაცემთა სუბიექტს, თუ მისი მონაცემები მუშავდება, მოთხოვნის შემთხვევაში, ასევე, აქვს უფლება დამმუშავებლისგან მიიღოს ინფორმაცია დამმუშავების არსებობა-არარსებობის შესახებ, ხოლო დადებითი პასუხის შემთხვევაში, მიიღოს ინფორმაცია თუ რომელი მონაცემი მუშავდება.

3.4.2. ნდობის დამყარება

დამმუშავებლებმა უნდა დაუსაბუთონ მონაცემთა სუბიექტებსა და საზოგადოებას, რომ ისინი ამუშავებენ მონაცემებს

¹²⁵ ადამიანის უფლებათა ევროპული სასამართლო, *Haralambie v. Romania*, No. 21737/03, 27 ოქტომბერი 2009 წელი.

კანონიერად და გამჭვირვალედ. დამუშავების მოქმედებები არ უნდა იქნეს წარმოებული საიდუმლოდ და არ უნდა გააჩნდეს გაუთვალისწინებელი ნეგატიური ეფექტი. დამუშავებლები უნდა დარწმუნდნენ, რომ მომხმარებლები, კლიენტები ან მოქალაქეები, არიან ინფორმირებულნი მათი მონაცემების გამოყენების თაობაზე. ამასთან, შესაძლებლობის ფარგლებში, დამუშავებლებმა უნდა იმოქმედონ მონაცემთა სუბიექტების მოთხოვნების სწრაფი შესრულების გზით, განსაკუთრებით მაშინ, თუ თანხმობა წარმოადგენს მონაცემთა დამუშავების სამართლებრივ საფუძველს.

მაგალითი: საქმეზე *K.H. and Others v. Slovakia*,¹²⁶ განმცხადებელი იყო რომანული ეთნიკური წარმოშობის მქონე რვა ქალბატონი, რომლებიც ორსულობისა და მშობიარობის დროს განთავსებულნი იყვნენ აღმოსავლეთ სლოვაკეთის ორ ჰოსპიტალში, რის შემდეგაც, მცდელობების მიუხედავად, ვერც ერთი მათგანი ვერ დაფეხმძიმდა. ეროვნულმა სასამართლოებმა დაავალდებულეს ჰოსპიტალები, რომ დაეშვათ განმცხადებლები და მათი წარმომადგენლები სამედიცინო ჩანაწერებთან, წერილობითი ამონაწერების გაკეთების მიზნით, თუმცა უარი მიიღეს დოკუმენტების ფოტოასლების გაკეთების თაობაზე, მათი უკანონოდ გამოყენების თავიდან ასაცილებლად. სახელმწიფოს პოზიტიური ვალდებულება, კონვენციის მე-8 მუხლის თანახმად, აუცილებლად მოიცავს ვალდებულებას, რომ მონაცემთა სუბიექტებისთვის ხელმისაწვდომი იყოს მათ შესახებ არსებული მონაცემების ასლები. სახელმწიფოს უნდა განესაზღვრა პერსონალურ მონაცემთა ასლის გადაღების პირობები, ან, საჭიროების შემთხვევაში, დაედგინა შესაბამისი სათანადო მიზეზები მათ აღსაკვეთად. განმცხადებლების საქმეზე, შიდასახელმწიფოებრივმა სასამართლოებმა მართლზომიერად ჩათვალეს სამედიცინო ჩანაწერების ასლის გადაღების აკრძალვა, უპირველესად, შესაბამისი ინფორმაციის უკანონოდ გამოყენების თავიდან აცილების მიზნით. თუმცა, ადამიანის უფლებათა ევროპულმა სასამართლომ ვერ დაადგინა თუ რამდენად შეეძლოთ განმცხადებლებს, რომლებსაც მიეცათ წვდომის უფლება სრულ სამედიცინო ჩანაწერებზე, უკანონოდ გამოყენებისა და ინფორმაცია მათ შესახებ. ამასთან, უკანონო გამოყენების ამგვარი რისკი შესაძლოა ყოფილიყო თავიდან აცილებული სხვა საშუალებების გამოყენებით, როგორიცაა იმ პირთა შეზღუდვა, რომელთაც გააჩნიათ წვდომა ფაილებზე და არა განმცხადებლებისთვის ფაილების ასლის გადაღების აკრძალვით. სახელმწიფომ ვერ

126 ადამიანის უფლებათა ევროპული სასამართლო, *K.H. and Others v. Slovakia*, No. 32881/04, 28 აპრილი 2009 წელი.

უზრუნველყო საკმარისად არგუმენტირებული მიზეზების წარმოდგენა, რათა განმცხადებლებისთვის უარი ეთქვა მათი ჯანმრთელობის შესახებ ინფორმაციის გაცემაზე. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

ინტერნეტ-მომსახურებებთან დაკავშირებით, მონაცემთა დამუშავების სისტემათა თავისებურებები უნდა ქმნიდეს საშუალებას მონაცემთა სუბიექტებისთვის რეალურად იცოდნენ თუ რა ვითარებაა მათ მონაცემებთან დაკავშირებით.

სამართლიანი დამუშავება, ასევე, ნიშნავს, რომ დამმუშავებლები მზად არიან გასცდნენ იმ მოთხოვნების სავალდებულო სამართლებრივ მინიმუმს, რაც მონაცემთა სუბიექტების წინაშე აკისრიათ, თუ ამას მოითხოვს მონაცემთა სუბიექტის ლეგიტიმური ინტერესი.

3.5. ანგარიშვალდებულების პრინციპი

საკანძო დებულებები

- ანგარიშვალდებულება მოითხოვს დამმუშავებლების მიერ იმ ზომების აქტიურ იმპლემენტირებას, რომელიც უზრუნველყოფს მონაცემთა დაცვის განმტკიცებას დამუშავების პროცესის მიმდინარეობისას.
- დამმუშავებლები პასუხისმგებლები არიან დამუშავების ოპერაციების მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის უზრუნველყოფაზე.
- დამმუშავებლებმა ნებისმიერ დროს უნდა შეძლონ მონაცემთა სუბიექტებისთვის ასევე, საზოგადოებისთვისა და საზედამხედველო ორგანოებისთვის, მონაცემთა დაცვის დებულებებთან შესაბამისობის დასაბუთება.

ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციამ (OECD) 2013 წელს შეიმუშავა პირადი ცხოვრების სახელმძღვანელო, სადაც ხაზგასმულია დამმუშავებლების მნიშვნელოვანი როლი მონაცემთა დაცვის პრაქტიკული რეალიზაციისას. სახელმძღვანელო ავითარებს ანგარიშვალდებულების პრინციპს იმ მხრივ, რომ „მონაცემთა დამმუშავებელი

ვალდებული უნდა იყოს შეასრულოს ის მოთხოვნები, რაც დადგენილია მოცემული პრინციპებით.¹²⁷

იმ დროს, როდესაც 108-ე კონვენცია არ აკეთებს დათქმას დამმუშავებლების ანგარიშვალდებულების პრინციპზე, ტოვებს რა, ამ საკითხს ღიად შიდასახელმწიფოებრივი კანონით რეგულირებისთვის, მონაცემთა დაცვის დირექტივის მე-6 მუხლის მე-2 პუნქტი ადგენს, რომ დამმუშავებელმა უნდა უზრუნველყოს პირველი პუნქტით დადგენილი პრინციპების შესრულება.

მაგალითი: ანგარიშვალდებულების პრინციპის განმტკიცების საკანონმდებლო მაგალითი მოცემულია პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების 2002/58/EC დირექტივის 2009 წლის ცვლილებებით.¹²⁸ მე-4 მუხლის შეცვლილი ვერსიის თანახმად, დირექტივა ადგენს უსაფრთხოების პოლიტიკის იმპლემენტაციის ვალდებულებას, კერძოდ, „უსაფრთხოების პოლიტიკის იმპლემენტირებას პერსონალურ მონაცემთა დამუშავების მხრივ.“ რამდენადაც, ამ დირექტივით მოცემულია უსაფრთხოებისთვის განკუთვნილი დებულებები, კანონმდებელმა გადანყვიტა, რომ აუცილებელი იყო დადგენილი ყოფილიყო მკაფიო მოთხოვნა უსაფრთხოების პოლიტიკის არსებობისა და იმპლემენტირების მიზნით.

მუხლი 29 სამუშაო ჯგუფის მოსაზრების¹²⁹ თანახმად, ანგარიშვალდებულების არსი მდგომარეობს დამმუშავებლის ვალდებულებაში, რომ:

- დაადგინოს ზომები, რომელიც, სტანდარტული პირობების გათვალისწინებით, უზრუნველყოფს მონაცემთა დაცვის წესების განმტკიცებას დამუშავების ოპერაცია-

127 OECD (2013), სახელმძღვანელო პერსონალურ მონაცემთა საერთაშორისო გადაცემისა და პირადი ცხოვრების დაცვის რეგულირების შესახებ, მუხლი 14.

128 ევროპული პარლამენტისა და საბჭოს 2009 წლის 25 ნოემბრის დირექტივა 2009/136/EC, რომელსაც ცვლილებები შეაქვეს უნივერსალური მომსახურებისა და ელექტრონულ საკომუნიკაციო ქსელებსა და მომსახურებასთან დაკავშირებულ მომხმარებელთა უფლებების შესახებ დირექტივაში 2002/22/EC, ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ დირექტივაში 2002/58/EC და მომხმარებელთა დაცვის კანონმდებლობის აღსრულების თაობაზე პასუხისმგებელ შიდასახელმწიფოებრივ ორგანოთა შორის თანამშრომლობის შესახებ რეგულაციაში (EC) No. 2006/2004 OJ 2009 337, გვ. 11.

129 მუხლი 29 სამუშაო ჯგუფი, მოსაზრება 3/2010 ანგარიშვალდებულების პრინციპის შესახებ, WP 173, ბრიუსელი, 13 ივლისი 2010 წელი.

თა კონტექსტში; და

- მოამზადოს დოკუმენტაცია, რომელიც ასაბუთებს მონაცემთა სუბიექტებისა და საზედამხედველო ორგანოების წინაშე იმ ზომების არსებობას, რაც მიღებულია მონაცემთა დაცვის წესების უზურუნველსაყოფად.

შესაბამისად, ანგარიშვალდებულების პრინციპი დამუშავებლებისგან მოითხოვს, რომ ისინი არ დაელოდონ მონაცემთა სუბიექტების ან საზედამხედველო ორგანოების მხრიდან მითითებას ნაკლოვანებებზე და აქტიურად მოახდინონ წესებთან შესაბამისობის დემონსტრირება.

4. მონაცემთა დაცვის ევროპული სამართლის წესები

ევროპული კავშირი	განხილული საკითხები	ევროპის საბჭო
არასენსიტიურ მონაცემთა კანონიერი დამუშავების წესები		
მონაცემთა დაცვის დირექტივა, მე-7 მუხლის -a- ქვეპუნქტი	თანხმობა	რეკომენდაცია პროფილირების შესახებ, მე-3 მუხლის მე-4 პუნქტის -b- ქვეპუნქტი და მე-3 მუხლის მე-6 პუნქტი
მონაცემთა დაცვის დირექტივა, მე-7 მუხლის -b- ქვეპუნქტი	(წინა) სახელშეკრულებო ურთიერთობა	რეკომენდაცია პროფილირების შესახებ, მე-3 მუხლის მე-4 პუნქტის -b- ქვეპუნქტი
მონაცემთა დაცვის დირექტივა, მე-7 მუხლის -c- ქვეპუნქტი	დამმუშავებლის სამართლებრივი ვალდებულებები	რეკომენდაცია პროფილირების შესახებ, მე-3 მუხლის მე-4 პუნქტის -a- ქვეპუნქტი
მონაცემთა დაცვის დირექტივა, მე-7 მუხლის -d- ქვეპუნქტი	მონაცემთა სუბიექტის სასიცოცხლო ინტერესები	რეკომენდაცია პროფილირების შესახებ, მე-3 მუხლის მე-4 პუნქტის -b- ქვეპუნქტი
მონაცემთა დაცვის დირექტივა, მე-7 მუხლის -d- ქვეპუნქტი და მე-8 მუხლის მე-4 პუნქტი მართლმსაჯულების ევროპული კავშირის სასამართლო, C-524/06, Huber v. Germany, 16 დეკემბერი 2008 წელი	საჯარო ინტერესი და სახელმწიფო ორგანოს უფლებამოსილებები	რეკომენდაცია პროფილირების შესახებ, მე-3 მუხლის მე-4 პუნქტის -b- ქვეპუნქტი
მონაცემთა დაცვის დირექტივა, მე-7 მუხლის -f- ქვეპუნქტი და მე-8 მუხლის მე-2 და მე-3 პუნქტი მართლმსაჯულების ევროპული კავშირის სასამართლო, 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 (FECEDM) v. Administración del Estado, 24 ნოემბერი 2011 წელი	სხვათა ლეგიტიმური ინტერესები	რეკომენდაცია პროფილირების შესახებ, მე-3 მუხლის მე-4 პუნქტის -b- ქვეპუნქტი

სენსიტიური მონაცემების კანონიერი დამუშავების წესები		
მონაცემთა დაცვის დირექტივა, მე-8 მუხლის პირველი პუნქტი	დამუშავების ზოგადი აკრძალვა	108-ე კონვენცია, მე-6 მუხლი
მონაცემთა დაცვის დირექტივა, მე-8 მუხლის მე-2 და მე-4 პუნქტები	გამონაკლისები ზოგადი აკრძალვიდან	108-ე კონვენცია, მე-6 მუხლი
მონაცემთა დაცვის დირექტივა, მე-8 მუხლის მე-5 პუნქტი	მონაცემთა დამუშავება სასამართლოების შესახებ	108-ე კონვენცია, მე-6 მუხლი
მონაცემთა დაცვის დირექტივა, მე-8 მუხლის მე-7 პუნქტი	საიდენტიფიკაციო ნომრების დამუშავება	
უსაფრთხო დამუშავების წესები		
მონაცემთა დაცვის დირექტივა, მე-17 მუხლი	უსაფრთხო დამუშავების წარმოების ვალდებულება	108-ე კონვენცია, მე-7 მუხლი
		ადამიანის უფლებათა ევროპული სასამართლო, I. v. Finland, No. 20511/03, 17 ივლისი 2008 წელი
პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ დირექტივის მე-4 მუხლის მე-2 პუნქტი	წესების დარღვევის შესახებ შეტყობინება	
მონაცემთა დაცვის დირექტივა, მე-16 მუხლი	კონფიდენციალურობის ვალდებულება	
წესები დამუშავების გამჭვირვალობის თაობაზე		
	გამჭვირვალობა ზოგადად	108-ე კონვენცია, მე-8 მუხლის -ა- ქვეპუნქტი
მონაცემთა დაცვის დირექტივა, მე-10 და მე-11 მუხლები	ინფორმირება	108-ე კონვენცია, მე-8 მუხლის -ა- ქვეპუნქტი
მონაცემთა დაცვის დირექტივა, მე-10 და მე-11 მუხლები	გამონაკლისები ინფორმირების ვალდებულებისგან	108-ე კონვენცია, მე-9 მუხლი
მონაცემთა დაცვის დირექტივა, მე-18 და მე-19 მუხლები	შეტყობინება	რეკომენდაცია პროფილების შესახებ, მე-9 მუხლის მე-2 პუნქტის -ა- ქვეპუნქტი
წესები შესაბამისობის ხელშეწყობის თაობაზე		
მონაცემთა დაცვის დირექტივა, მე-20 მუხლი	წინასწარი შემოწმება	

მონაცემთა დაცვის დირექტივა, მე-18 მუხლის მე-2 პუნქტი	პერსონალური მონაცემთა დაცვის პასუხისმგებელი პირები	რეკომენდაცია პროფილირების შესახებ, მე-8 მუხლის მე-3 პუნქტი
მონაცემთა დაცვის დირექტივა, 27-ე მუხლი	ქცევის კოდექსები	

პრინციპები არის ზოგადი აუცილებლობის შემცველი. მათი გავრცელება კონკრეტულ შემთხვევებზე ხდება ინტერპრეტაციის გარკვეული ფარგლებითა და მნიშვნელობის შერჩევით. ევროპის საბჭოს კანონმდებლობის მიხედვით, ინტერპრეტაციის ფარგლების განსაზღვრა ნებადართულია 108-ე კონვენციის ნეკრი ქვეყნების ეროვნული კანონმდებლობებით. ევროპული კავშირის კანონმდებლობის მიხედვით მოცემულობა სხვაგვარია: ევროპული კავშირის დონეზე, შიდა ბაზრის ფარგლებში მონაცემთა დაცვის უზრუნველსაყოფად, აუცილებელი იყო მეტად დეტალური წესების დადგენა ევროპული კავშირის ნეკრი ქვეყნების შიდასახელმწიფოებრივი კანონმდებლობებით, მონაცემთა დაცვის დონის ჰარმონიზების უზრუნველსაყოფად. მონაცემთა დაცვის დირექტივა, მე-6 მუხლით განსაზღვრული პრინციპებით, ადგენს წესების დეტალური ჩამონათვალს, რომელიც ჯეროვნად უნდა იქნეს იმპლემენტირებული შიდასახელმწიფოებრივ კანონმდებლობაში. შესაბამისად, ევროპულ დონეზე, მონაცემთა დაცვის დეტალური დებულებების თაობაზე მითითება ვრცელდება ევროპული კავშირის კანონმდებლობაზე.

4.1. კანონიერი დამუშავების წესები

საკანძო დებულებები

- პერსონალური მონაცემები შესაძლებელია დამუშავდეს კანონიერად თუ:
 1. დამუშავება ხორციელდება მონაცემთა სუბიექტის თანხმობის საფუძველზე; ან
 2. მონაცემთა სუბიექტის სასიცოცხლო ინტერესები მოითხოვს მის მონაცემთა დამუშავებას; ან
 3. სხვათა ლეგიტიმური ინტერესები წარმოადგენს დამუშავების საფუძველს, მაგრამ მხოლოდ იმ შემთხვე-

ვაში თუ მონაცემთა სუბიექტის ძირითადი უფლებების დაცვის ინტერესი არ არის აღმატებული.

- განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავება ექვემდებარება სპეციალურ, მკაცრ რეჟიმს.

მონაცემთა დაცვის დირექტივა შეიცავს მონაცემთა კანონიერი დამუშავების წესების შესახებ ორი სახის განსხვავებულ რეგულირებას: პირველი ეხება არასენსიტიური კატეგორიის მონაცემებს, რომელიც მე-7 მუხლით არის მოცემული და მეორე – სენსიტიური კატეგორიის მონაცემებს, მე-8 მუხლით.

4.1.1. არასენსიტიური კატეგორიის მონაცემთა კანონიერი დამუშავება

95/46 დირექტივის მე-2 თავი, „პერსონალურ მონაცემთა კანონიერი დამუშავების ძირითადი წესები,“ ადგენს, რომ გარდა მე-13 მუხლით გათვალისწინებული გამონაკლისების, პერსონალურ მონაცემთა ნებისმიერი დამუშავება, უპირველესად, უნდა იყოს შესაბამისობაში მონაცემთა დაცვის დირექტივის მე-6 მუხლით დადგენილ მონაცემთა ხარისხის პრინციპებთან, ხოლო მეორე მხრივ – მე-7 მუხლით დადგენილ მონაცემთა დამუშავების ლეგიტიმურობის რომელიმე საფუძველთან.¹³⁰ ეს ეხება შემთხვევებს, რომელიც ლეგიტიმურს ხდის არასენსიტიური კატეგორიის ინფორმაციის დამუშავებას.

თანხმობა

ევროპის საბჭოს კანონმდებლობის მიხედვით, თანხმობა არ არის ნახსენები ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლით ან 108-ე კონვენციით. თუმცა, იგი მითითებულია

¹³⁰ მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები C-465/00, C-138/01 და C-139/01 *Rechnungshof v. Österreichischer Rundfunk and Others*, 20 მაისი 2003 წელი, პარაგ. 65; მართლმსაჯულების ევროპული კავშირის სასამართლო, C-524/06, *Huber v. Germany*, 16 დეკემბერი 2008 წელი, პარაგ. 48; მართლმსაჯულების ევროპული კავშირის სასამართლო, 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*, 24 ნოემბერი 2011 წელი, პარაგ. 26.

ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკაში და ევროპის საბჭოს რამოდენიმე რეკომენდაციაში. ევროპული კავშირის კანონმდებლობის მიხედვით, თანხმობა, როგორც მონაცემთა დამუშავების სამართლებრივი საფუძველი, მკაფიოდ დადგენილია მონაცემთა დაცვის დირექტივის მე-7 მუხლის -a- ქვეპუნქტით, ასევე მკაფიოდ არის მითითებული ქარტიის მე-8 მუხლში.

სახელშეკრულებო ურთიერთობა

ევროპული კავშირის კანონმდებლობის მიხედვით, პერსონალურ მონაცემთა ლეგიტიმური დამუშავების მორიგი საფუძველი მოცემულია მონაცემთა დაცვის დირექტივის მე-7 მუხლის -b- ქვეპუნქტით, კერძოდ, თუ დამუშავება „აუცილებელია ხელშეკრულების შესრულებისთვის, რომლის მხარეს წარმოადგენს მონაცემთა სუბიექტი.“ ეს დებულება, ასევე, ვრცელდება წინასახელშეკრულებო ურთიერთობებზე. მაგალითად, მხარე განიზრახავს ხელშეკრულების გაფორმებას, მაგრამ ჯერ არ ახორციელებს ამას, საბოლოო გადამოწმების აუცილებლობიდან გამომდინარე. თუ მხარეს სჭირდება ამ მიზნისთვის მონაცემთა დამუშავება, ეს ლეგიტიმურია, რამდენადაც განხორციელებულია იმისათვის, რათა ხელშეკრულების დადებამდე გადაიდგას ნაბიჯები მონაცემთა სუბიექტის მოთხოვნის საფუძველზე.

ევროპის საბჭოს კანონმდებლობის თანახმად, „სხვათა უფლებებისა და თავისუფლებების დაცვა“ მოცემულია კონვენციის მე-8 მუხლის მე-2 პუნქტით, რაც წარმოადგენს ლეგიტიმური ჩარევის საფუძველს მონაცემთა დაცვის უფლებაში.

დამმუშავებლის სამართლებრივი ვალდებულებები

ევროპული კავშირის კანონმდებლობა მკაფიოდ ადგენს მონაცემთა დამუშავების პროცესის ლეგიტიმურობის მორიგ კრიტერიუმს, კერძოდ, თუ „იგი არის აუცილებელი იმ ვალდებულების შესასრულებლად, რომელიც აკისრია მონაცემთა დამმუშავებელს“ (მონაცემთა დაცვის დირექტივის მე-7 მუხლის -c- ქვეპუნქტი). ეს დებულება ეხება დამმუშავებლებს, რომლებიც

მოქმედებენ კერძო სექტორში; საჯარო სექტორის მონაცემთა დამმუშავებლების სამართლებრივი ვალდებულებები მოცემულია დირექტივის მე-7 მუხლის -e- ქვეპუნქტით. არსებობს ბევრი შემთხვევა, როდესაც კერძო სექტორის დამმუშავებლები კანონით ვალდებული არიან დაამუშავონ სხვათა მონაცემები. მაგალითად, ექიმებს და ჰოსპიტალს აქვთ სამართლებრივი ვალდებულება, რომ შეინახონ პაციენტის მკურნალობის შესახებ მონაცემები რამოდენიმე წლით; დამსაქმებლებმა უნდა დაამუშავონ მონაცემები მათი დასაქმებულების შესახებ სოციალური უსაფრთხოებისა და საგადასახადო მიზნებისთვის; ასევე, საწარმოებმა უნდა დაამუშავონ მონაცემები მათი კლიენტების შესახებ საგადასახადო მიზნებისთვის.

ავიახაზების მიერ მგზავრთა მონაცემების საზღვარგარეთის საიმიგრაციო კონტროლის ორგანოებისთვის სავალდებულო გადაცემის კონტექსტში დაისვა საკითხი, იყო თუ არა უცხოური კანონმდებლობით გათვალისწინებული სამართლებრივი ვალდებულებები, ევროპული კავშირის კანონმდებლობის მიხედვით, დამმუშავების სამართლებრივი საფუძვლის მქონე (საკითხი დეტალურად განხილულია 6.2 პარაგრაფში).

დამმუშავებლის სამართლებრივი ვალდებულებები, ასევე, წარმოადგენს მონაცემთა დამმუშავების ლეგიტიმურ საფუძველს ევროპის საბჭოს კანონმდებლობის მიხედვით. როგორც ზემოთ აღინიშნა, კერძო სექტორის მონაცემთა დამმუშავებლის სამართლებრივი ვალდებულებები წარმოადგენს სხვათა ლეგიტიმური ინტერესების გათვალისწინების ერთ-ერთ კონკრეტულ შემთხვევას, როგორც მითითებულია კონვენციის მე-8 მუხლის მეორე პუნქტით. შესაბამისად, მოცემული მაგალითი, რელევანტურია ევროპის საბჭოს სამართლებრივი სისტემისთვისაც.

მონაცემთა სუბიექტის სასიცოცხლო ინტერესები

ევროპული კავშირის კანონმდებლობის მიხედვით, მონაცემთა დაცვის დირექტივის მე-7 მუხლის -d- ქვეპუნქტი ადგენს, რომ პერსონალურ მონაცემთა დამმუშავება კანონიერია თუ იგი „არის აუცილებელი მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად.“ მსგავსი ინტერესები, რომელიც მჭიდროდ

არის დაკავშირებული მონაცემთა სუბიექტის გადარჩენასთან, შესაძლებელია, მაგალითად, იყოს ჯანმრთელობის შესახებ არსებული მონაცემების ან დაკარგული პირების შესახებ არსებული მონაცემების გამოყენების ლეგიტიმურობის საფუძველი.

ევროპის საბჭოს კანონმდებლობის მიხედვით, მონაცემთა სუბიექტის სასიცოცხლო ინტერესები არ არის მოცემული კონვენციის მე-8 მუხლით, როგორც მონაცემთა დაცვის უფლებაში ლეგიტიმური ჩარევის საფუძველი. ევროპის საბჭოს ზოგიერთ რეკომენდაციაში, რომელიც ავსებს 108-ე კონვენციას კონკრეტულ სფეროებში, მონაცემთა სუბიექტის სასიცოცხლო ინტერესები მკაფიოდ არის მოცემული მონაცემთა დამუშავების ლეგიტიმურობის საფუძველად.¹³¹ მიჩნეულია, რომ მონაცემთა სუბიექტების სასიცოცხლო ინტერესები ჩართულია მონაცემთა დამუშავების მართლზომიერების საფუძველებში: ძირითად უფლებათა დაცვამ არასდროს უნდა შეუქმნას საფრთხე იმ პირის სასიცოცხლო ინტერესებს, რომელიც უნდა იქნეს დაცული.

საჯარო ინტერესი და საჯარო უფლებამოსილების განხორციელება

საზოგადო ურთიერთობათა მონესრიგების შესაძლო მრავალი საშუალებიდან, მონაცემთა დაცვის დირექტივის მე-7 მუხლის -e- ქვეპუნქტი ადგენს, რომ პერსონალური მონაცემები შესაძლოა კანონიერად დამუშავდეს თუ ის „არის აუცილებელი საჯარო ინტერესის ფარგლებში შესასრულებელი მოქმედებისთვის ან სახელმწიფო ორგანოს უფლებამოსილების განსახორციელებლად, რისი შესრულებაც დაკისრებული აქვს დამმუშავებელს ან მესამე პირს, რომელსაც გადაეცა მონაცემები.“¹³²

მაგალითი: საქმეზე *Huber v. Germany*,¹³³ ჰუბერმა, ეროვნებით ავსტრიელმა და მცხოვრებმა გერმანიაში, სთხოვა მიგრაციისა და ლტოლვილთა ფედერალურ ოფისს წაეშალათ მის შესახებ არსებული მონაცემები ეროვნებით უცხოელთა ცენტრალური რეესტრიდან. რეესტრი, რომელიც შეიცავს გერმანიაში სამ თვეზე მეტი ვადით

131 რეკომენდაცია პროფილირების შესახებ, მე-3 მუხლის მე-4 პუნქტის -b- ქვეპუნქტი.

132 იხ. ასევე, მონაცემთა დაცვის დირექტივა, პრეამბულის 32-ე პუნქტი.

133 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-524/06, *Huber v. Germany*, 16 დეკემბერი 2008 წელი.

ევროპულ კავშირში მცხოვრებ არაგერმანელთა პერსონალურ მონაცემებს, გამოიყენება სამართალდამცავი და კანონის აღმასრულებელი ორგანოების მიერ სტატისტიკური მიზნებისთვის, გამოძიებისა და სისხლისსამართლებრივი დევნისას იმ პირთა მიმართ, რომლებიც საფრთხეს უქმნიან საზოგადოებრივ უსაფრთხოებას. საქმის განმხილველმა სასამართლომ დასვა საკითხი, იყო თუ არა ევროპული კავშირის სამართალთან შესაბამისი იმ პირების პერსონალური მონაცემების დამუშავება, რომლებიც მოიპოვებოდა უცხოელ მცხოვრებთა ცენტრალურ რეესტრში და რაზეც ჰქონდათ ნდომა სახელმწიფო ორგანოებსაც, იმის გათვალისწინებით, რომ ამგვარი რეესტრი არ არსებობდა გერმანელი მაცხოვრებლებისთვის.

პირველ რიგში, მართლმსაჯულების ევროპული კავშირის სასამართლომ აღნიშნა, რომ დირექტივის მე-7 მუხლის -e- ქვეპუნქტით პერსონალური მონაცემები შესაძლებელია დამუშავდეს მხოლოდ იმ შემთხვევაში თუ ემსახურება საჯარო ინტერესის მიზნებს ან სახელმწიფო დანესებულების მიერ მოვალეობების შესრულებას.

სასამართლოს მსჯელობაზე დაყრდნობით, „წევრ ქვეყნებში მონაცემთა დაცვის ექვივალენტური დონის მიღწევის გათვალისწინებით, 95/46 დირექტივის მე-7 მუხლის -e- ქვეპუნქტით მოცემული აუცილებლობის კონცეფციას არ შეიძლება ჰქონდეს განსხვავებული მნიშვნელობა წევრ ქვეყნებს შორის. შესაბამისად, ეს არის საკითხი, რომელსაც აქვს თავისი დამოუკიდებელი მნიშვნელობა და, გაერთიანების კანონმდებლობის თანახმად, უნდა იქნეს განმარტებული იმგვარად, რომ სრულად დააკმაყოფილოს დირექტივის პირველი მუხლის პირველი პუნქტით დადგენილი მიზნები.“¹³⁴

სასამართლო აღნიშნავს, რომ გაერთიანების მოქალაქის თავისუფალი გადაადგილების უფლება იმ წევრი ქვეყნის ტერიტორიაზე, რომლის ეროვნების მქონე იგი არ არის, არ არის უპირობო და შესაძლებელია დაექვემდებაროს ხელშეკრულებით მოცემულ შეზღუდვებს, პირობებს და მისგან გამომდინარე მიღებულ ზომებს. შესაბამისად, თუ წევრი ქვეყნებისთვის ლეგიტიმურია გერმანული რეესტრის მსგავსი ბაზის გამოყენება, რათა მოხდეს იმ ორგანოების დახმარება, რომლებიც არიან პაუსიხმგებელნი ბინადრობასთან დაკავშირებული კანონმდებლობის შესრულებაზე, იგი არ უნდა შეიცავდეს იმაზე მეტ ინფორმაციას, რაც აუცილებელია მოცემული კონკრეტული მიზნისთვის. სასამართლო ასკვნის, რომ პერსონალურ მონაცემთა დამუშავების აგვარი სისტემა შესაბამისობაშია ევროპული კავშირის კანონმდებლობასთან, თუ იგი შეიცავს მხოლოდ იმ მონაცემებს, რომელიც აუცილებელია კანონმდებლობის მოქმედებისთვის და თუ მისი ორგანიზებული ბუნება ხელს უწყობს კანონმდებლობის მეტად ეფექტურ გამოყენებას. ეროვნულმა სასამართლომ უნდა დაადგინოს თუ რამდენად არის ეს პირობები სახეზე ამ კონკრეტულ შემთხვევაში. თუ არ არის, პერსონალურ მონაცემ-

თა შენახვა და დამუშავება ისეთ რეესტრში, როგორიც გერმანულია, სტატისტიკური მიზნებისთვის, ვერც ერთ შემთხვევაში ვერ იქნება მიჩნეული მართლზომიერად 95/46/EC დირექტივის მე-7 მუხლის -e ქვეპუნქტის მიხედვით.¹³⁵

საბოლოოდ, რაც შეეხება საკითხს დანაშაულის წინააღმდეგ ბრძოლის მიზნებისთვის რეესტრში განთავსებულ მონაცემთა გამოყენებას, სასამართლომ აღნიშნა, რომ ეს მიზანი „აუცილებლად გულისხმობს ჩადენილი დანაშაულებებისა და მართლსაწინააღმდეგო ქმედებების დევნას, მისი ჩამდენის ეროვნების მიუხედავად.“ მოცემული რეესტრი არ შეიცავს გერმანული ეროვნების მქონე პირთა მონაცემებს და ეს განხვავება ქმნის დისკრიმინაციას, რომელიც აკრძალულია ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულების მე-18 მუხლით. შესაბამისად, ეს დებულება, როგორც იქნა განმარტებული სასამართლოს მიერ, გამოირიცხავს წევრი ქვეყნების მხრიდან, დანაშაულთან ბრძოლის მიზნებისთვის, პერსონალურ მონაცემთა დამუშავების იმგვარი სისტემის დანერგვას, რაც მხოლოდ გაერთიანების იმ მოქალაქეებს ეხება, რომლებიც არ არიან მოცემული წევრი ქვეყნის ეროვნების მქონენი.¹³⁶

სახელმწიფო ორგანოების მიერ პერსონალურ მონაცემთა საჯარო მიზნებისთვის გამოყენებაზე, ასევე, ვრცელდება კონვენციის მე-8 მუხლი.

დამუშავების ან მესამე პირის ლეგიტიმური ინტერესის დაკმაყოფილება

მონაცემთა სუბიექტი არ არის ერთადერთი ლეგიტიმური ინტერესის მქონე. მონაცემთა დაცვის დირექტივის მე-7 მუხლის -f- ქვეპუნქტი ადგენს, რომ პერსონალური მონაცემები შესაძლებელია კანონიერად დამუშავდეს თუ ეს „აუცილებელია დამუშავების ან მესამე პირის ან იმ პირების ლეგიტიმური ინტერესის მიზნებისთვის, რომელთაც გადაეცათ მონაცემები, გარდა იმ შემთხვევისა, როდესაც მონაცემთა სუბიექტის ძირითადი უფლებებისა და თავისუფლებების ინტერესი აღმატებულია და მოითხოვს დაცვას.“

მოცემულ საკმეზე, მართლმსაჯულების ევროპული კავში-

¹³⁵ იქვე, პარაგ. 54, 58, 59, 66-68.

¹³⁶ იქვე, პარაგ. 78 და 81.

რის სასამართლომ გადაწყვეტილება გამოიტანა უშუალოდ დირექტივის მე-7 მუხლის -f ქვეპუნქტზე დაყრდნობით:

მაგალითი: საქმეზე ASNEF და FECEMD,¹³⁷ მართლმსაჯულების ევროპული კავშირის სასამართლომ განმარტა, რომ შიდასახელმწიფოებრივი კანონმდებლობით არ არის ნებადართული განისაზღვროს მონაცემთა კანონიერი დამუშავების დამატებითი პირობები, დირექტივის მე-7 მუხლის -f ქვეპუნქტთან მიმართებით. ეს დაკავშირებული იყო ესპანეთის მონაცემთა დაცვის კანონის დებულებასთან, რომლის თანახმადაც სხვა კერძო პირებს შეეძლოთ პერსონალურ მონაცემთა დამუშავებისას თავიანთი ლეგიტიმური ინტერესის დაყენება, მხოლოდ იმ შემთხვევაში თუ ინფორმაცია უკვე იქნა განთავსებული საჯარო წყაროებში.

სასამართლომ, პირველ რიგში აღნიშნა, რომ დირექტივა 95/46 ისწრაფვის უზრუნველყოს ინდივიდთა უფლებებისა და თავისუფლებების დაცვის ექვივალენტური დონე ევროპული კავშირის ყველა წევრ ქვეყანაში პერსონალურ მონაცემთა დამუშავების მხრივ. ამ სფეროში შიდასახელმწიფოებრივი კანონმდებლობების ჰარმონიზაცია არ უნდა იწვევდეს დადგენილი დაცვის დონის დაქვეითებას, პირიქით, იგი უნდა ცდილობდეს დაცვის მაღალი დონის დამკვიდრებას ევროპულ კავშირში.¹³⁸ შესაბამისად, სასამართლომ აღნიშნა, რომ „წევრ ქვეყნებში დაცვის ექვივალენტური დონის დადგენის მიზნიდან გამომდინარე, 95/46 დირექტივის მე-7 მუხლი აყალიბებს იმ საფუძვლების ამომწურავ და შეზღუდულ ჩამონათვალს, როდესაც პერსონალურ მონაცემთა დამუშავება შესაძლებელია იქნეს მიჩნეული კანონიერად.“ ამასთან, „წევრ ქვეყნებს არ შეუძლიათ დაამატონ ახალი პრინციპები 95/46 დირექტივის მე-7 მუხლს, რომელიც ეხება პერსონალურ მონაცემთა დამუშავების კანონიერებას ან დაადგინონ დამატებითი მოთხოვნები, რომლებსაც გააჩნიათ მე-7 მუხლით დადგენილი ექვსი პრინციპთან რომელიმესთვის შემცვლელი გავლენა.“¹³⁹ სასამართლომ დასძინა: იმ ბალანსის მისაღწევად, რომელიც აუცილებელია 95/46/EC დირექტივის მე-7 მუხლის -f ქვეპუნქტის თანახმად, „შესაძლებელია მიღებულ იქნეს მხედველობაში ის ფაქტი, რომ დამუშავებით გამოწვეული მონაცემთა სუბიექტის ძი-

137 მართლმსაჯულების ევროპული კავშირის სასამართლო, 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, 24 ნოემბერი 2011 წელი.

138 იქვე, პარაგ. 28. იხ. მონაცემთა დაცვის დირექტივა, პრეამბულის მე-8 და მე-10 პუნქტები.

139 მართლმსაჯულების ევროპული კავშირის სასამართლო, 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, 24 ნოემბერი 2011 წელი, პარაგ. 30 და 32.

რითადი უფლებების დარღვევის სერიოზულობა, შესაძლოა განსხვავდებოდეს იმის მიხედვით, თუ რამდენად არის მონაცემები განთავსებული საჯარო წყაროებში.“

თუმცა, „დირექტივის მე-7 მუხლის -f- ქვეპუნქტი არ აძლევს ნეერ ქვეყნებს იმის შესაძლებლობას, რომ, კონკრეტული ან ზოგადი ფორმით, განსაზღვრონ პერსონალურ მონაცემთა გარკვეული კატეგორიების დამუშავება იმგვარად, რომ არ მისცენ საშუალება საპირისპირო უფლებებსა და ინტერესებს იქნენ ერთმანეთის წინაშე განონასწორებული, კონკრეტული სიტუაციის გათვალისწინებით.“

აღნიშნული მსჯელობის გათვალისწინებით, სასამართლომ დაასკვნა, რომ 95/46 დირექტივის მე-7 მუხლის -f- ქვეპუნქტი უნდა განიმარტოს შემდეგი სახით: იგი არ იძლევა საშუალებას შიდა-სახელმწიფოებრივი წესებით, მონაცემთა სუბიექტის თანხმობის არარსებობისას, დამუშავებლის, მესამე პირის ან იმ პირთა ლეგიტიმური ინტერესის დაცვის მიზნით, ვისაც გადაეცა მონაცემები, სუბიექტის პერსონალური მონაცემების დამუშავებისთვის დადგინდეს არა მხოლოდ მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის მოთხოვნა, არამედ ისიც, რომ მონაცემები უნდა იყოს მოცემული საჯარო წყაროებში, რაც, თავის მხრივ, გამორიცხავს, კონკრეტული და ზოგადი ფორმით, იმ მონაცემთა დამუშავების შესაძლებლობას, რომელიც არ ჩნდება ასეთ წყაროებში.“¹⁴⁰

მსგავსი ფორმულირებები შესაძლებელია ინახოს ევროპის საბჭოს რეკომენდაციებშიც. რეკომენდაცია პროფილირების შესახებ ლეგიტიმურად მიიჩნევს პერსონალურ მონაცემთა დამუშავებას პროფილირების მიზნებისთვის, თუ ეს აუცილებელია სხვათა ლეგიტიმური ინტერესების დასაცავად, „გარდა იმ შემთხვევისა თუ ასეთი ინტერესები არ არის აღმატებული მონაცემთა სუბიექტების ფუნდამენტურ უფლებებსა და თავისუფლებებზე.“¹⁴¹

4.1.2. განსაკუთრებული კატეგორიის მონაცემთა კანონიერი დამუშავება

ევროპის საბჭოს კანონმდებლობა ნებას რთავს შიდასახელმწიფოებრივ კანონმდებლობას განსაზღვროს შესაბამისი დაცვის ზომები განსაკუთრებული კატეგორიის მონაცემთა გამო-

¹⁴⁰ იქვე, პარაგ. 40, 44, 48 და 49.

¹⁴¹ რეკომენდაცია პროფილირების შესახებ, მე-4 მუხლის მე-4 პუნქტის -b- ქვეპუნქტი.

ყენებისთვის, მაშინ, როდესაც ევროპული კავშირის კანონმდებლობის მიხედვით, მონაცემთა დაცვის დირექტივის მე-8 მუხლი შეიცავს დეტალურ წესებს იმ კატეგორიის მონაცემთა დამუშავებისთვის, რომელიც ავლენს: რასობრივ ან ეთნიკურ წარმომავლობას, პოლიტიკურ შეხედულებებს, რელიგიურ და ფილოსოფიურ მრწამსს, სავაჭრო გაერთიანების წევრობის შესახებ ინფორმაციას ან ინფორმაციას ჯანმრთელობის ან სექსობრივი ცხოვრების შესახებ. ზოგადად, განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავება აკრძალულია.¹⁴² თუმცა, არსებობს მოცემული აკრძალვის გამონაკლისთა ამომწურავი ჩამონათვალი, რომელიც დადგენილია დირექტივის მე-8 მუხლის მე-2 და მე-3 პუნქტებით. ეს გამონაკლისები შეიცავს მონაცემთა სუბიექტის აშკარა თანხმობას, მონაცემთა სუბიექტის სასიცოცხლო ინტერესებს, სხვათა ლეგიტიმურ ინტერესებსა და საჯარო ინტერესს.

არასენსიტიური კატეგორიის მონაცემთა დამუშავებისგან განსხვავებით, მონაცემთა სუბიექტთან სახელშეკრულებო ურთიერთობა არ არის განხილული, როგორც განსაკუთრებული კატეგორიის მონაცემთა ლეგიტიმური დამუშავების საფუძველი. შესაბამისად, თუ განსაკუთრებული მონაცემები უნდა იქნეს დამუშავებული მონაცემთა სუბიექტთან დადებული ხელშეკრულების ფარგლებში, ხელშეკრულების დადების შესახებ თანხმობასთან ერთად, ეს მოითხოვს მონაცემთა სუბიექტის ცალკე მკაფიო თანხმობას. მონაცემთა სუბიექტის მიერ განხორციელებული მკაფიო მოთხოვნა საქონლისა და მომსახურების მიღების შესახებ, რომელიც აუცილებელი წესით ავლენს მის განსაკუთრებულ მონაცემებს, თავის მხრივ, მიჩნეული იქნება იმავე ძალის მქონედ, როგორც მკაფიო თანხმობა.

142 მონაცემთა დაცვის დირექტივა, მე-8 მუხლის პირველი პუნქტი.

მაგალითი: თუ ავიახაზების მგზავრი, ფრენის დაჯავშნისას, მოითხოვს რომ ავიახაზებმა მისთვის უზრუნველყოს ეტლი და რელიგიური ნესებით გათვალისწინებული საკვები, ავიახაზები უფლებამოსილია გამოიყენოს ეს მონაცემები იმ შემთხვევაშიც კი, თუ მგზავრმა არ მოაწერა ხელი დამატებითი თანხმობის პირობას იმ მონაცემთა გამოყენების თაობაზე, რომელიც ავლენს ინფორმაციას მისი ჯანმრთელობის მდგომარეობისა და რელიგიური შეხედულებების შესახებ.

მონაცემთა სუბიექტის მკაფიო თანხმობა

მონაცემთა კანონიერი დამუშავების უპირველესი პირობა, მიუხედავად იმისა, განსაკუთრებულია თუ არა იგი, არის მონაცემთა სუბიექტის თანხმობა. განსაკუთრებული კატეგორიის მონაცემის შემთხვევაში, თანხმობა უნდა იყოს მკაფიო. შიდა-სახელმწიფოებრივი კანონით შესაძლებელია განისაზღვროს, რომ განსაკუთრებული მონაცემების გამოყენებაზე თანხმობა არ არის საკმარისი საფუძველი მათი დამუშავებისთვის,¹⁴³ მაგალითად, თუ, განსაკუთრებულ შემთხვევებში, დამუშავება მოიცავს დიდ რისკებს მონაცემთა სუბიექტისთვის.

ზოგიერთ შემთხვევაში, შინაარსობრივი თანხმობაც კი შესაძლებელია აღიარებული იყოს განსაკუთრებული კატეგორიის მონაცემთა დამუშავების სამართლებრივ საფუძვლად: დირექტივის მე-8 მუხლის მე-2 პუნქტი ადგენს, რომ დამუშავება არ არის აკრძალული თუ იგი მოიცავს მონაცემებს, რომელიც მონაცემთა სუბიექტმა აშკარად საჯარო გახადა. ეს დებულება თვალნათლივ გულისხმობს, რომ მონაცემთა სუბიექტის ქმედება საკუთარი მონაცემის საჯაროდ ხელმისაწვდომობის შესახებ უნდა იქნეს განმარტებული, როგორც მონაცემთა სუბიექტის ნაგულისხმევი თანხმობა ამ მონაცემის გამოყენების თაობაზე.

მონაცემთა სუბიექტის სასიცოცხლო ინტერესები

არასენსიტიური მონაცემების მსგავსად, განსაკუთრებული კატეგორიის მონაცემები შესაძლებელია დამუშავებული იქნეს მონაცემთა სუბიექტის სასიცოცხლო ინტერესებისთვის.¹⁴⁴

ამ საფუძვლით განსაკუთრებული კატეგორიის მონაცემთა

¹⁴³ იქვე, მე-8 მუხლის მე-2 პუნქტის -a- ქვეპუნქტი.

¹⁴⁴ იქვე, მე-8 მუხლის მე-2 პუნქტის -c- ქვეპუნქტი.

კანონიერი დამუშავებისთვის აუცილებელია, რომ შეუძლებელი იყოს მონაცემთა სუბიექტისთვის საკითხის დასმა მის გადასაწყვეტად, მაგალითად, მონაცემთა სუბიექტის უგონო მდგომარეობის ან მისი მიუწვდომლობის გამო.

სხვათა ლეგიტიმური ინტერესები

არასენსიტიური მონაცემების მსგავსად, სხვათა ლეგიტიმური ინტერესების დაცვა შესაძლოა წარმოადგენდეს განსაკუთრებული კატეგორიის მონაცემების დამუშავების საფუძველს. მათი დამუშავება, მონაცემთა დაცვის დირექტივის მე-8 მუხლის მე-2 პუნქტის მიხედვით, ნებადართულია მხოლოდ შემდეგ შემთხვევებში:

- თუ დამუშავება აუცილებელია სხვა პირის სასიცოხლლო ინტერესებისთვის,¹⁴⁵ როდესაც მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად არ შესწევს უნარი განაცხადოს თანხმობა;
- თუ განსაკუთრებული კატეგორიის მონაცემთა დამუშავება, როგორცაა ჯანმრთელობის შესახებ მონაცემები, ხორციელდება შრომით-სამართლებრივი მიზნებისთვის, განსაკუთრებით სახიფათო სამუშაო ადგილის გათვალისწინებით; ან რელიგიური მრწამსის შესახებ მონაცემები – დასვენების დღეების განსასაზღვრად;¹⁴⁶
- როდესაც ფონდები, ასოციაციები ან სხვა არასამეწარმეო ორგანოები პოლიტიკური, ფილოსოფიური, რელიგიური ან სავაჭრო კავშირის მიზნებიდან გამომდინარე, ამუშავებენ მონაცემებს მათი წევრების, სპონსორების ან სხვა დაინტერესებული პირების შესახებ (ამგვარი მონაცემები განსაკუთრებული კატეგორიისაა, ვინაიდან ისინი შესაძლებელია ავლენდეს კონკრეტული ინდივიდის რელიგიურ ან პოლიტიკურ შეხედულებებს);¹⁴⁷
- თუ განსაკუთრებული კატეგორიის მონაცემები არის გამოყენებული სასამართლოში პროცესისთვის ან ადმი-

145 *ibid.*

146 იქვე, მე-8 მუხლის მე-2 პუნქტის -ბ- ქვეპუნქტი.

147 იქვე, მე-8 მუხლის მე-2 პუნქტის -დ- ქვეპუნქტი.

ნისტრაციულ ორგანოში სამართლებრივი მოთხოვნით მიმართვისთვის, მისი განხილვისთვის ან დაცვისთვის.¹⁴⁸

- ამასთან, მონაცემთა დაცვის დირექტივის მე-8 მუხლის მე-3 პუნქტის თანახმად, თუ ჯანმრთელობის შესახებ მონაცემები გამოიყენება სამედიცინო გამოკვლევისა და მკურნალობისთვის შესაბამისი ჯანდაცვის დაწესებულების მომსახურე პირის მიერ, ამ მომსახურებათა მართვა, ასევე, გათვალისწინებულია დადგენილი განმარტებით. განსაკუთრებული უსაფრთხოებისთვის, პირები მიიჩნევიან „ჯანდაცვის დაწესებულების მომსახურე პირებად“ იმ შემთხვევაში, თუ ისინი ექვემდებარებიან კონფიდენციალურობის სპეციალურ, პროფესიულ ვალდებულებას.

საჯარო ინტერესი

მონაცემთა დაცვის დირექტივის მე-8 მუხლის მე-4 პუნქტის თანახმად, ნევრ ქვეყნებს შეუძლიათ დაადგინონ დამატებითი მიზნები, რომლისთვისაც შესაძლებელია დამუშავდეს განსაკუთრებული მონაცემები, კერძოდ:

- მონაცემთა დამუშავება აუცილებელია არსებითი საჯარო ინტერესისთვის; და
- იგი განსაზღვრულია შიდასახელმწიფოებრივი კანონით, ან ზედამხედველი ორგანოს გადაწყვეტილებით; და
- შიდასახელმწიფოებრივი კანონი ან ზედამხედველი ორგანოს გადაწყვეტილება შეიცავს უსაფრთხოების აუცილებელ ზომებს მონაცემთა სუბიექტის ინტერესთა ეფექტური დაცვისთვის.¹⁴⁹

თვალსაჩინო მაგალითია ჯანმრთელობის ელექტრონული ფაილური სისტემები, რომლის შექმნაც იგეგმება ევროპული კავშირის ბევრ ქვეყანაში. ამგვარი სისტემით შესაძლებელია ჯანმრთელობის მდგომარეობის შესახებ მონაცემები, რომელიც შეგროვებულ იქნა ჯანდაცვის დაწესებულების მომსახურე პირის მიერ პაციენტის მკურნალობის პროცესში, ფართოდ გახდეს

¹⁴⁸ იქვე, მე-8 მუხლის მე-2 პუნქტის -e- ქვეპუნქტი.

¹⁴⁹ იქვე, მე-8 მუხლის მე-4 პუნქტი.

ხელმისაწვდომი ჯანდაცვის სხვა დაწესებულების მომსახურეთათვის, ძირითადად, მთელი ქვეყნის მასშტაბით.

მუხლი 29 სამუშაო ჯგუფმა დაასკვნა, რომ ამგვარი სისტემების დანერგვა ვერ მოხერხდება პაციენტის მონაცემების დამუშავებისთვის განკუთვნილი არსებული სამართლებრივი წესების საფუძველზე, რაც დადგენილია მონაცემთა დაცვის დირექტივის მე-8 მუხლის მე-3 პუნქტით. იმის გათვალისწინებით, რომ ჯანმრთელობის შესახებ მოცემული ელექტრონული ფაილური სისტემის არსებობა წარმოადგენს არსებით საჯარო ინტერესს, იგი შესაძლებელია დაეყრდნოს დირექტივის მე-8 მუხლის მე-4 პუნქტს, რაც მოითხოვს მკაფიო სამართლებრივ საფუძველს მისი განხორციელებისთვის, და უსაფრთხოების აუცილებელ ზომებს სისტემის დაცული ფუნქციონირებისთვის.¹⁵⁰

4.2. დამუშავების უსაფრთხოების წესები

საკვანძო დებულებები

- დამუშავების უსაფრთხოების წესები მოიცავს დამმუშავებლისა და უფლებამოსილი პირის ვალდებულებას მოახდინონ შესაბამისი ტექნიკური და ორგანიზაციული ზომების იმპლემენტირება მონაცემთა დამუშავების პროცესში ნებისმიერი არაავტორიზებული ჩარევის პრევენციისთვის.
- მონაცემთა უსაფრთხოების მოთხოვნის დონე განისაზღვრება:
 1. კონკრეტული დამუშავების სახის გათვალისწინებით, ბაზარზე არსებული უსაფრთხოების ხელმისაწვდომი ზომებით; და
 2. ხარჯებით; და
 3. დამუშავებულ მონაცემთა ხასიათით.
- მონაცემთა უსაფრთხო დამუშავება, ასევე, უზრუნველყოფილია მასში ჩართული ყველა პირის, დამმუშავებლებისა და უფლებამოსილი პირების ვალდებულებით, რომ მონაცემები დარჩეს კონფიდენციალური.

150 მუხლი 29 სამუშაო ჯგუფი (2007), სამუშაო დოკუმენტი ჯანმრთელობის ელექტრონულ რეესტრში (EHR) ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დამუშავების თაობაზე, WP 131, ბრიუსელი, 15 თებერვალი 2007 წელი.

დამმუშავებელთა და უფლებამოსილ პირთა ვალდებულება დანერგონ ადეკვატური ზომები მონაცემთა უსაფრთხოებისთვის, განსაზღვრულია როგორც ევროპის საბჭოს მონაცემთა დაცვის, ისე ევროპული კავშირის მონაცემთა დაცვის კანონმდებლობის მიხედვით.

4.2.1. მონაცემთა უსაფრთხოების ელემენტები

ევროპული კავშირის კანონმდებლობით:

„წევრმა ქვეყნებმა უნდა განსაზღვრონ, რომ დამმუშავებელმა დანერგოს შესაბამისი ტექნიკური და ორგანიზაციული ზომები პერსონალურ მონაცემთა შემთხვევითი ან უკანონო განადგურებისგან, შემთხვევითი დაკარგვისგან, შეცვლისგან, არაავტორიზებული გამჟღავნების ან წვდომისგან დასაცავად, ძირითადად მაშინ, როდესაც დამმუშავებამ მოიცავს მონაცემთა გადაცემას ქსელის მეშვეობით და, ასევე, სხვა დანარჩენი უკანონო დამმუშავების ფორმებისგან დასაცავად.“¹⁵¹

მსგავსი დებულება მოცემულია ევროპის საბჭოს კანონმდებლობით:

„უსაფრთხოების შესაბამისი ზომები უნდა იქნეს მიღებული პერსონალურ მონაცემთა დასაცავად, რომელიც შენახულია ავტომატიზებულ მონაცემთა ფაილებში, შემთხვევითი ან არაავტორიზებული განადგურებისგან, შემთხვევითი დაკარგვისგან, ისევე როგორც არაავტორიზებული წვდომისგან, შეცვლისგან და გავრცელებისგან დასაცავად.“¹⁵²

ხშირ შემთხვევაში, არსებობს ინდუსტრიული, შიდასახელმწიფოებრივი და საერთაშორისო სტანდარტები, რომლებიც შემუშავებულ იქნა მონაცემთა უსაფრთხო დამმუშავებისთვის. მაგალითად, EuroPriSe, წარმოადგენს ევროპული კავშირის ტრანს-ევროპული სატელეკომუნიკაციო ქსელის (eTEN) პროექტს, რომელმაც დაადგინა პროდუქტთა სერტიფიცირების საშუალებები, მეტწილად, პროგრამული უზრუნველყოფების ევროპული კავშირის მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის კუთხით. ევროპული კავშირის წევრი ქვეყნების

151 მონაცემთა დაცვის დირექტივა, მე-17 მუხლის პირველი პუნქტი.

152 108-ე კონვენცია, მე-7 მუხლი.

და ბიზნეს გაერთიანებების მიერ ქსელისა და ინფორმაციის უსაფრთხოების პრობლემათა პრევენციის, გამოვლენისა და რეაგირების გაძლიერების მიზნით შეიქმნა ქსელისა და ინფორმაციული უსაფრთხოების ევროპული სააგენტო (ENISA).¹⁵³ სააგენტო რეგულარულად აქვეყნებს უსაფრთხოების წინაშე არსებული რისკების ანალიზებსა და რჩევებს თუ როგორ განხორციელდეს მათი მართვა.

მონაცემთა უსაფრთხოება არ არის მიღწეული მხოლოდ სწორი აღჭურვილობის, კერძოდ, ტექნოლოგიური და პროგრამული მხარდაჭერის დანერგვით. იგი, ასევე, მოითხოვს შესაბამის შიდა ორგანიზაციულ წესებს. ამგვარი შიდა წესები სრულად ვრცელდება შემდეგ საკითხებზე:

- ყველა თანამშრომლისთვის მონაცემთა უსაფრთხოების წესებისა და მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული ვალდებულებების, განსაკუთრებით, კონფიდენციალურობის პირობის შესახებ ინფორმაციის რეგულარულ მიწოდებას;
- მონაცემთა დამუშავების საკითხებში პასუხისმგებლობათა ნათელი გადანაწილება და კომპეტენციათა მკაფიო ხაზგასმა, განსაკუთრებით, პერსონალურ მონაცემთა დამუშავებისა და მათი მესამე მხარეებისთვის გადაცემის თაობაზე გადაწყვეტილების მიღებისას;
- პერსონალურ მონაცემთა გამოყენება მხოლოდ კომპეტენტური პირების მიერ დადგენილი ინსტრუქციების ან ზოგადად დადგენილი წესების მიხედვით;
- დამმუშავებლის ან უფლებამოსილი პირის ადგილმდებარეობაზე წვდომისგან დაცვა და, ასევე, ტექნოლოგიური და პროგრამული უზრუნველყოფის დაცვა, მათ შორის წვდომისას ავტორიზების შემოწმება;
- კომპეტენტური პირის მიერ პერსონალურ მონაცემებთან წვდომის ავტორიზაციის დადგენის უზრუნველყოფა და შესაბამისი დოკუმენტაციის არსებობა;
- ელექტრონული საშუალებებით პერსონალურ მონა-

153 ევროპული პარლამენტისა და საბჭოს 2004 წლის 10 მარტის რეგულაცია No. 460/2004 ქსელისა და ინფორმაციული უსაფრთხოების ევროპული სააგენტოს შექმნის თაობაზე, OJ 2004 L 77.

ცემებთან წვდომის ავტომატიზებული წესები და შიდა საზედამხებდველო ორგანოს მიერ მათი რეგულარული შემოწმება;

- მონაცემთა ავტომატიზებული წვდომის გარდა, მონაცემებთან წვდომის სხვა ფორმების საგულდაგულო დოკუმენტირება, მათი გადაცემის უკანონო ფორმების არ არსებობის დასაბუთების მიზნით.

თანამშრომელთათვის მონაცემთა დაცვის სათანადო ტრენინგი და ცოდნის გაზიარება, ასევე, მნიშვნელოვანი ელემენტია უსაფრთხოების ეფექტური ზომების მხრივ. ნამდვილობის დადასტურების პროცედურები, ასევე, უნდა იქნეს დაწესებული, რათა შესაბამისი ზომების არსებობა უზრუნველყოფილ იქნეს არა მხოლოდ ქალაქში, არამედ მოხდეს მათი სამუშაო პროცესში იმპლემენტირებაც (როგორიცაა შიდა და გარე აუდიტი).

დამმუშავებლის ან უფლებამოსილი პირის მიერ უსაფრთხოების დონის ასამაღლებელი ზომები მოიცავს ინსტრუმენტებს, როგორიცაა პერსონალურ მონაცემთა დაცვის პასუხისმგებელი პირები, უსაფრთხოების გაცნობა დასაქმებულთათვის, რეგულარული აუდიტი, სიღრმისეული ტესტირებები და ხარისხის ბეჭდები.

მაგალითი: საქმეზე I. v. Finland,¹⁵⁴ განმცხადებელმა ვერ დაადასტურა მისი ჯანმრთელობის მდგომარეობის შესახებ ჩანაწერზე უკანონო წვდომის განხორციელება იმ ჰოსპიტალის თანამშრომელთა მიერ, სადაც იგი მუშაობდა. შესაბამისად, მისი საჩივარი მონაცემთა დაცვის უფლების დარღვევაზე იქნა უარყოფილი ეროვნული სასამართლოების მიერ. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ ადგილი ჰქონდა ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის დარღვევას, რამდენადაც ჰოსპიტალის ჯანმრთელობის მდგომარეობის შესახებ ფაილური რეესტრის სისტემა „იყო იმგვარი, რომ შეუძლებელ ხდიდა პაციენტთა მონაცემების გამოყენების რეტროაქტიულ დადგენას, რამდენადაც იგი ავლენდა მხოლოდ განხორციელებული წვდომის ბოლო ხუთ ფაქტს და ეს ინფორმაცია იყო წაშლილი მათი არქივში გადაცემისთანავე.“ სასამართლოსთვის გადამწყვეტი იყო ის, რომ ჰოსპიტალში მოცემული ჩანაწერების სისტემა არ იყო შესაბამისობაში შიდასახელმწიფოებრივი კანონმდებლობით დადგენილ მოთხოვნებთან, რა ფაქტიც არ იქნა ჯეროვნად შეფასებული ადგილობრივი სასამართლოების მიერ.

154 ადამიანის უფლებათა ევროპული სასამართლო, I. v. Finland, No. 20511/03, 17 ივლისი 2008 წელი.

შეტყობინებები მონაცემთა წესების დარღვევის შესახებ

მონაცემთა უსაფრთხოების დარღვევის წინააღმდეგ მიმართული ახალი ინსტრუმენტი შემოთავაზებულ იქნა რამოდენიმე ევროპული ქვეყნის მონაცემთა დაცვის კანონმდებლობით: ელექტრონული კომუნიკაციების მომსახურებათა მწარმოებლების ვალდებულება აცნობონ მონაცემთა დარღვევის შესახებ შესაძლო დაზარალებულებსა და ზედამხედველ ორგანოებს. ევროპული კავშირის კანონმდებლობით, სატელეკომუნიკაციო პროვაიდერებისთვის ეს სავალდებულო მოთხოვნაა.¹⁵⁵ მონაცემთა სუბიექტებისთვის მონაცემთა დამუშავების წესების დარღვევის შეტყობინებების მიზანი არის ზიანის თავიდან აცილება: შეტყობინებები და მათი შესაძლო შედეგები ამცირებს მონაცემთა სუბიექტებისთვის ნეგატიური ეფექტის რისკს. აშკარა დაუდევრობის შემთხვევაში, მომსახურების მიმწოდებლები შესაძლოა, ასევე, იქნენ სანქცირებულნი.

შიდა პროცედურების წინასწარ დანერგვა აუცილებელია უსაფრთხოების დარღვევის ეფექტური მართვისა და შეტყობინებისთვის, რამდენადაც მონაცემთა სუბიექტებისთვის ან/და ზედამხედველი ორგანოებისთვის შეტყობინების ვადა, შიდა-სახელმწიფოებრივი კანონმდებლობის მიხედვით, ძირითადად მცირეა.

4.2.2. კონფიდენციალურობა

ევროპული კავშირის კანონმდებლობით, მონაცემთა უსაფრთხო დამუშავების ვალდებულება დაკისრებულია ყველა პირისთვის, კერძოდ, დამუშავებელისა და უფლებამოსილი პირის-

155 იხ. ევროპული პარლამენტისა და საბჭოს 2002 წლის 12 ივლისის დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ (პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ დირექტივა), OJ 2002 L 201, მე-4 მუხლის მე-3 პუნქტი, შეცვლილი ევროპული პარლამენტისა და საბჭოს 2009 წლის 25 ნოემბრის დირექტივის 2009/136/EC მიერ, რომელსაც ცვლილებები შეაქვს 2002/22/EC დირექტივაში ელექტრონულ საკომუნიკაციო ქსელებსა და მომსახურებებთან დაკავშირებით უნივერსალური მომსახურებისა და მომხმარებელთა უფლებების თაობაზე; იხ. ასევე, დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ და რეგულაცია (EC) No. 2006/2004 მომხმარებელთა დაცვის კანონმდებლობის აღსრულებაზე პასუხისმგებელი ეროვნული საზედამხედველო ორგანოების შესახებ, OJ 2009 L 337.

თვის დადგენილი მოვალეობით, დაიცვან მონაცემთა კონფიდენციალურობა.

მაგალითი: სადაზღვევო კომპანიის თანამშრომელი იღებს სატელეფონო ზარს საკუთარ სამუშაო ადგილას, პირი თავს აცხადებს კლიენტად და ითხოვს ინფორმაციას მისი სადაზღვევო კონტრაქტის შესახებ.

კლიენტის მონაცემთა კონფიდენციალურად შენახვის ვალდებულება მოითხოვს, რომ დასაქმებულმა მიიღოს უსაფრთხოების მინიმალური ზომები მაინც, პერსონალურ მონაცემთა გამჟღავნებამდე. ეს უზრუნველყოფილი იქნება თუ, მაგალითად, იგი გადაურეკავს კლიენტს მის ფაილში მითითებულ სატელეფონო ნომერზე.

კონფიდენციალურობის ვალდებულება არ ვრცელდება იმ შემთხვევებზე, სადაც მონაცემები ცნობილი გახდა პირისათვის პირადად და არა როგორც დამმუშავებლის ან უფლებამოსილი პირის დასაქმებულის სტატუსით. ამ მხრივ, მონაცემთა დაცვის დირექტივის მე-16 მუხლი არ ვრცელდება, რამდენადაც, ფიზიკური პირების მიერ პერსონალურ მონაცემთა გამოყენება კერძო პირებს შორის სრულიად თავისუფალია დირექტივის რეგულირებისგან, ვინაიდან ამგვარი გამოყენება ექცევა ე.წ. პირადი მიზნებისთვის გამოყენების ფარგლებში.¹⁵⁶ ეს გამონაკლისი წარმოადგენს პერსონალურ მონაცემთა გამოყენებას „ფიზიკური პირების მიერ აშკარად პირადი ან საშინაო საქმიანობის მიზნებისთვის.“¹⁵⁷ მართლმსაჯულების ევროპული კავშირის სასამართლოს გადაწყვეტილებიდან გამომდინარე, საქმეზე *Bodil Lindqvist*,¹⁵⁸ ეს გამონაკლისი უნდა იყოს განმარტებული ვიწროდ, განსაკუთრებით, მონაცემთა გამჟღავნების მხრივ. კერძოდ, პირადი მიზნებისთვის არსებული გამონაკლისი არ უნდა გავრცელდეს ინტერნეტში პერსონალურ მონაცემთა პუბლიკაციაზე მიმღებთა შეუზღუდავი წრისათვის (მეტად დაწვრილებით, იხილეთ პარაგრაფები 2.1.2, 2.2, 2.3.1 და 6.1).

ევროპის საბჭოს კანონმდებლობის მიხედვით, კონფიდენ-

¹⁵⁶ მონაცემთა დაცვის დირექტივა, მე-3 მუხლის მე-2 პუნქტი, მეორე აბზაცი.

¹⁵⁷ *ibid.*

¹⁵⁸ მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, *Lindqvist*, 6 ნოემბერი 2003 წელი.

ციალურობის ვალდებულება ჩართულია 108-ე კონვენციის მე-7 მუხლში, რომელიც ეხება მონაცემთა უსაფრთხოებას.

უფლებამოსილი პირებისთვის კონფიდენციალურობა ნიშნავს, რომ მათ უნდა გამოიყენონ დამმუშავებლისგან გადაცემული პერსონალური მონაცემები მხოლოდ დამმუშავებლის მიერ დადგენილი ინსტრუქციის ფარგლებში. დამმუშავებლის ან უფლებამოსილი პირის დასაქმებულებისთვის, კონფიდენციალურობა მოითხოვს, რომ მათ გამოიყენონ პერსონალური მონაცემები მხოლოდ იმ ინსტრუქციების შესაბამისად, რაც განსაზღვრულია მათი უშუალო ზემდგომების მიერ.

კონფიდენციალურობის პირობა უნდა იქნეს გათვალისწინებული დამმუშავებელსა და უფლებამოსილ პირს შორის არსებულ ნებისმიერ ხელშეკრულებაში. ამასთან, დამმუშავებლებსა და უფლებამოსილ პირებს ექნებათ ვალდებულება მიიღონ სპეციალური ზომები მათი დასაქმებულების მიერ კონფიდენციალურობის სამართლებრივი მოთხოვნის უზრუნველსაყოფად, ძირითადად, დამსაქმებელსა და დასაქმებულს შორის არსებულ ხელშეკრულებაში კონფიდენციალურობის პირობების ჩართვით.

ევროპული კავშირისა და 108-ე კონვენციის ხელმომწერ ბევრ სახელმწიფოებში კონფიდენციალურობის პროფესიული მოვალეობის დარღვევა დასჯადია სისხლის სამართლის წესით.

4.3. დამუშავების გამჭვირვალობის წესები

საკვანძო დებულებები

- პერსონალურ მონაცემთა დამუშავების დაწყებამდე, დამმუშავებელმა, სულ მცირე, უნდა მოახდინოს მონაცემთა სუბიექტების ინფორმირება დამმუშავებლის ვინაობისა და მონაცემთა დამუშავების მიზნის შესახებ, გარდა იმ შემთხვევისა, თუ მონაცემთა სუბიექტს უკვე აქვს ამგვარი ინფორმაცია.
- თუ მონაცემები შეგროვებულია მესამე პირებისგან, ინფორმაციის მიწოდების ვალდებულება აღარ არსებობს თუ:

1. მონაცემთა დამუშავება გათვალისწინებულია კანონით; ან
 2. ინფორმაციის მიწოდება შეუძლებელია ან დაკავშირებულია არაპროპორციულ ძალისხმევასთან.
- პერსონალურ მონაცემთა დამუშავების დაწყებამდე, მონაცემთა დამუშავებელს დამატებით ევალება:
 1. შეატყობინოს საზედამხედველო ორგანოს დაგეგმილი დამუშავების მოქმედებათა შესახებ; ან
 2. განეროს დამუშავება შიდა დონეზე, პერსონალურ მონაცემთა დაცვის პასუხისმგებელი დამოუკიდებელი პირის მიერ, თუ შიდასახელმწიფოებრივი კანონმდებლობა ადგენს ამგვარ წესს.

სამართლიანი დამუშავების პრინციპი მოითხოვს დამუშავების გამჭვირვალობას. ევროპის საბჭოს კანონმდებლობა ადგენს, რომ ნებისმიერ პირს უნდა შეეძლოს მონაცემთა დამუშავების ფაილების არსებობის, მათი მიზნისა და პასუხისმგებელი დამუშავებლის დადგენა,¹⁵⁹ ხოლო მისი მიღწევის გზების განსაზღვრა ნებადართულია შიდასახელმწიფოებრივი კანონმდებლობით. ევროპული კავშირის კანონმდებლობა მეტად კონკრეტულია, უზრუნველყოფს რა, გამჭვირვალობას მონაცემთა სუბიექტების წინაშე, დამუშავებლისთვის ინფორმირების ვალდებულების დაკისრებით და, მთლიანობაში, საზოგადოებისთვის შეტყობინების გზით.

ორივე სამართლებრივი სისტემის მიხედვით, გამონაკლისები და შეზღუდვები დამუშავებლისთვის დადგენილი გამჭვირვალობის ვალდებულებისგან შესაძლებელია მოცემული იყოს შიდასახელმწიფოებრივი კანონით, როდესაც ასეთი შეზღუდვა წარმოადგენს აუცილებელ ზომას კონკრეტული საჯარო ინტერესების, მონაცემთა სუბიექტის ან სხვათა უფლებებისა და თავისუფლებების დასაცავად, თუ ეს აუცილებელია დემოკრატიულ საზოგადოებაში.¹⁶⁰ მსგავსი გამონაკლისები, შესაძლებელია აუცილებელი იყოს დანაშაულის გამოძიების პროცესში, ასევე, იყოს მართლზომიერი სხვა პირობების არსებობისას.

159 108-ე კონვენცია, მე-8 მუხლის -a- ქვეპუნქტი.

160 იქვე, მე-9 მუხლის მე-2 პუნქტი; მონაცემთა დაცვის დირექტივა, მე-13 მუხლის პირველი პუნქტი.

4.3.1. ინფორმირება

ევროპის საბჭოსა და ევროპული კავშირის კანონმდებლობის მიხედვით, დამმუშავებლები ვალდებული არიან წინასწარ მოახდინონ მონაცემთა სუბიექტის ინფორმირება დაგეგმილი დამუშავების შესახებ.¹⁶¹ ეს ვალდებულება არ არის დამოკიდებული მონაცემთა სუბიექტის მიერ მოთხოვნის წარდგენაზე, არამედ, უნდა იყოს განხორციელებული დამმუშავებლის მიერ პრაქტიულად, მიუხედავად იმისა იჩენს თუ არა მონაცემთა სუბიექტი ინტერესს ინფორმაციის მიმართ.

ინფორმაციის შინაარსი

ინფორმაცია უნდა შეიცავდეს დამუშავების მიზანს, ასევე დამმუშავებლის ვინაობასა და საკონტაქტო მონაცემებს.¹⁶² მონაცემთა დაცვის დირექტივა ითხოვს დამატებით ინფორმაციას, რომელიც უნდა იქნეს მიწოდებული თუ „ეს აუცილებელია მონაცემთა შეგროვების სპეციალური გარემოებების გათვალისწინებით, მონაცემთა სამართლიანი დამუშავების უზრუნველსაყოფად მონაცემთა სუბიექტთან მიმართებით.“ დირექტივის მე-10 და მე-11 მუხლები, სხვა საკითხებთან ერთად, განსაზღვრავს დასამუშავებელ მონაცემთა კატეგორიებსა და ამ მონაცემთა მიმღებებს, ასევე, მათზე წვდომისა და მონაცემთა შესწორების უფლებას. თუ მონაცემები შეგროვებულია მონაცემთა სუბიექტებისგან, ინფორმაცია უნდა იქნეს მიწოდებული შეგროვების სავალდებულო თუ ნებაყოფლობითი ხასიათის შესახებ, ასევე, ინფორმაციის გაცემაზე უარის თქმის შედეგები.¹⁶³

ევროპის საბჭოს სამართლებრივი სისტემის პერსპექტივიდან გამომდინარე, ამგვარი ინფორმაციის მიწოდების განსაზღვრა შესაძლებელია ჩაითვალოს კარგი პრაქტიკის მაგალითად მონაცემთა სამართლიანი დამუშავების პრინციპის ჭრილში, და, ამდენად, მიიჩნევა ევროპის საბჭოს სამართლის სისტემის შემა-

161 108-ე კონვენცია, მე-8 მუხლის -a- ქვეპუნქტი; მონაცემთა დაცვის დირექტივა, მე-10 და მე-11 მუხლები.

162 108-ე კონვენცია, მე-8 მუხლის -a- ქვეპუნქტი; მონაცემთა დაცვის დირექტივა, მე-10 მუხლის -a- და -b- ქვეპუნქტები.

163 მონაცემთა დაცვის დირექტივა, მე-10 მუხლის -c- ქვეპუნქტი.

დგენელ ნაწილად.

სამართლიანი დამუშავების პრინციპი მოითხოვს, რომ ინფორმაცია უნდა იყოს ადვილად გასაგები მონაცემთა სუბიექტებისთვის. უნდა იქნეს გამოყენებული ის ენა, რომელიც გასაგებია ადრესატებისთვის. თუ სამიზნე აუდიტორია არის ბავშვები ან ზრდასრულები, ასევე, მთლიანად საზოგადოება ან ექსპერტები, გამოყენებული ენის დონე და ტიპი უნდა იყოს თითოეულისთვის შესაბამისი ფორმის.

ზოგიერთი მონაცემთა სუბიექტი მოისურვებს მათ შესახებ არსებულ მონაცემთა დამუშავების შესახებ იყოს მოკლედ ინფორმირებული, მაშინ როდესაც სხვა პირებმა, შესაძლოა, მოითხოვონ დეტალური განმარტება. თუ როგორ უნდა იქნეს დაბალანსებული ინფორმაციის სამართლიანობის ეს ასპექტი მოცემულია მუხლი 29 სამუშაო ჯგუფის მოსაზრებაში, რომელიც მხარს უჭერს ე.წ. არჩევითი შეტყობინებების იდეას,¹⁶⁴ რითაც საშუალებას აძლევს მონაცემთა სუბიექტს გადაწყვიტოს აირჩიოს ინფორმირების სასურველი მოცულობა.

ინფორმაციის მიწოდების ვადა

მონაცემთა დაცვის დირექტივა შეიცავს მცირედ განსხვავებულ დებულებებს, რომელიც ეხება ინფორმაციის მიწოდების ვადას, რაც დამოკიდებულია იმაზე, თუ ვისგან არის მონაცემები შეგროვებული – მონაცემთა სუბიექტისგან (მე-10 მუხლი) თუ მესამე პირისგან (მე-11 მუხლი). როდესაც მონაცემები შეგროვებულია უშუალოდ მონაცემთა სუბიექტისგან, ინფორმაცია უნდა იქნეს მიწოდებული შეგროვების დროს მაინც. როდესაც მონაცემები შეგროვებულია მესამე პირებისგან, ინფორმაცია უნდა იქნეს მიწოდებული მონაცემთა დამუშავებლის მიერ მონაცემთა შენახვის მომენტში ან იქამდე, სანამ მონაცემები პირველად გადაეცემა მესამე მხარეს.

164 მუხლი 29 სამუშაო ჯგუფი (2004), მოსაზრება 10/2004 ინფორმაციის მიწოდების მეთად ჰარმონიზების თაობაზე, WP 100, ბრიუსელი, 25 ნოემბერი 2004 წელი.

გამონაკლისი ინფორმირების ვალდებულებისგან

ევროპული კავშირის კანონმდებლობის მიხედვით, მონაცემთა სუბიექტისთვის ინფორმირების ვალდებულებისგან ძირითადი გამონაკლისია ფაქტი, როდესაც მონაცემთა სუბიექტი უკვე ინფორმირებულია.¹⁶⁵ ეს ეხება შემთხვევებს, როდესაც არსებული ვითარებიდან გამომდინარე, მონაცემთა სუბიექტი უკვე ინფორმირებული იქნება მისი მონაცემების სამომავლო დამუშავების შესახებ კონკრეტული მიზნისთვის, კონკრეტული დამუშავებლის მიერ.

დირექტივის მე-11 მუხლი, რომელიც ეხება მონაცემთა სუბიექტის ინფორმირების ვალდებულებას, როდესაც მონაცემები არ არის უშუალოდ მისგან მოპოვებული, ადგენს, რომ ინფორმირების ვალდებულება არ არსებობს მონაცემთა სტატისტიკური მიზნებისთვის ან ისტორიული და სამეცნიერო მიზნებისთვის დამუშავებისას, თუ:

- ამგვარი ინფორმაციის მიწოდება შეუძლებელია; ან
- იგი დაკავშირებულია არაპროპორციულ ძალისხმევასთან; ან
- მონაცემთა ჩანერა ან გამჟღავნება მკაფიოდ დადგენილია კანონით.¹⁶⁶

მონაცემთა დაცვის დირექტივის მხოლოდ მე-11 მუხლის მე-2 პუნქტი ადგენს, რომ მონაცემთა სუბიექტები აღარ საჭიროებენ დამუშავების ოპერაციითა შესახებ ინფორმირებას თუ დამუშავება განსაზღვრულია კანონით. ზოგადი სამართლებრივი ვარაუდიდან გამომდინარე, რომლის თანახმად კანონი ცნობილია მისი სუბიექტებისთვის, შესაძლებელია იმის მტკიცება, რომ თუ მონაცემები შეგროვებულია მონაცემთა სუბიექტისგან, დირექტივის მე-10 მუხლის მიხედვით, მონაცემთა სუბიექტს აქვს ინფორმაცია. მაგრამ იმის გათვალისწინებით, რომ კანონის ცოდნა მხოლოდ ვარაუდია, სამართლიანი დამუშავების პრინციპი მოითხოვს, რომ მე-10 მუხლის მიხედვით დამუშავებისას მონაცემთა სუბიექტი იქნეს ინფორმირებული იმ შემთხვევაშიც კი, თუ დამუშავება გათვალისწინებულია კანონით, რამდენადაც

¹⁶⁵ მონაცემთა დაცვის დირექტივა, მე-10 მუხლი და მე-11 მუხლის პირველი პუნქტი.

¹⁶⁶ იქვე, პრეამბულის მე-40 პუნქტი და მე-11 მუხლის მე-2 პუნქტი.

მონაცემთა სუბიექტების ინფორმირება არ წარმოადგენს დამატებით ტვირთს მონაცემთა უშუალოდ მონაცემთა სუბიექტისგან შეგროვების დროს.

რაც შეეხება ევროპის საბჭოს კანონმდებლობას, 108-ე კონვენცია ადგენს მკაფიო გამოთქმას მე-8 მუხლით დადგენილი წესებისგან. ისევ და ისევ, მონაცემთა დაცვის დირექტივის მე-10 და მე-11 მუხლებით დადგენილი გამოთქმისგან შესაძლებელია დანახული იქნეს, როგორც კარგი პრაქტიკის მაგალითი იმ გამოთქმისგან, რაც დადგენილია 108-ე კონვენციის მე-9 მუხლით.

ინფორმაციის მინოდების სხვადასხვა გზები

ინფორმაციის მინოდების საუკეთესო გზა არის თითოეული მონაცემთა სუბიექტის შეტყობინება, ვერბალურად ან წერილობით. თუ მონაცემები არის შეგროვებული მონაცემთა სუბიექტებისგან, ინფორმაციის მინოდება უნდა განხორციელდეს მოპოვების პარალელურად, განსაკუთრებით იმ შემთხვევაში, თუ მონაცემები შეგროვებულია მესამე პირებისგან, თუმცა, მონაცემთა სუბიექტებთან დაკავშირების შესაძლო სირთულეების გათვალისწინებით, ინფორმირება შესაძლებელია განხორციელდეს სათანადო პუბლიკაციითაც.

ინფორმაციის მინოდების ერთ-ერთი ყველაზე ეფექტური გზა არის ის, რომ დამმუშავებელმა განათავსოს ინფორმირების პირობები, როგორიცაა კონფიდენციალურობის პოლიტიკა, ვებ-გვერდზე. თუმცა, არსებობს მოსახლეობის საკმაოდ ნაწილი, რომელიც არ იყენებს ინტერნეტს, რაც კომპანიის ან სახელმწიფო დაწესებულების ინფორმირების პოლიტიკით უნდა იყოს გათვალისწინებული.

4.3.2. შეტყობინება

შიდასახელმწიფოებრივი კანონით შესაძლებელია გათვალისწინებულ იქნეს დამმუშავებლების მიერ საზედამხედველო ორგანოსთვის შეტყობინების ვალდებულება დამმუშავების პროცესის თაობაზე იმგვარად, რომ შესაძლებელი იყოს მისი გამო-

ქვეყნება. ასევე, შიდასახელმწიფოებრივი კანონით შესაძლებელია განისაზღვროს დამუშავებლების მიერ მონაცემთა დაცვის პასუხისმგებელი პირის დანიშვნა, რომელიც პასუხისმგებელი იქნება დამუშავებლის მიერ დამუშავების მოქმედებათა რეესტრის წარმოებაზე.¹⁶⁷ აღნიშნული შიდა რეესტრი, მოთხოვნის შემთხვევაში, უნდა იქნეს ხელმისაწვდომი საზოგადოებისთვის.

მაგალითი: პერსონალურ მონაცემთა დაცვის შიდა მაკონტროლების შეტყობინება, ისევე როგორც დოკუმენტაცია, უნდა აღწერდეს მოცემულ მონაცემთა დამუშავების ძირითად თავისებურებებს. ეს მოიცავს დამუშავებლის, დამუშავების მიზნის, დამუშავების სამართლებრივი საფუძვლის, დასამუშავებელ მონაცემთა კატეგორიების, შესაძლო მიმღები მესამე პირების შესახებ ინფორმაციას და, ასევე, ინფორმაციას იმის თაობაზე იგვემება თუ არა მონაცემთა საერთაშორისო გადაცემა, თუ კი – მაშინ, რა მონაცემთა გადაცემა.

საზედამხედველო ორგანოს მიერ შეტყობინებათა გამოქვეყნება უნდა იყოს მოცემული სპეციალური რეესტრით. დასახული მიზნის გათვალისწინებით, ამგვარ რეესტრთან წვდომა უნდა იყოს მარტივი და უფასო. იგივე ეხება დოკუმენტებს, რომელიც წარმოებულია დამუშავებლის პერსონალურ მონაცემთა დაცვის პასუხისმგებელი პირის მიერ.

კომპეტენტური საზედამხედველო ორგანოსთვის შეტყობინების ვალდებულებისგან ან მონაცემთა დაცვის შიდა პასუხისმგებელი პირის დანიშვნასთან დაკავშირებული გამონაკლისები შესაძლებელია განისაზღვროს შიდასახელმწიფოებრივი კანონმდებლობით დამუშავების იმ მოქმედებებზე, რომელიც ნაკლებად სავარაუდოა, რომ წარმოშვას რისკები მონაცემთა სუბიექტებისთვის, რაც განსაზღვრულია მონაცემთა დაცვის დირექტივის მე-18 მუხლის მე-2 პუნქტით.¹⁶⁸

4.4. წესები შესაბამისობის მხარდაჭერის შესახებ

საკვანძო დებულებები

- ანგარიშვალდებულების პრინციპის განვითარებისთვის,

¹⁶⁷ იქვე, მე-18 მუხლის მე-2 პუნქტის მე-2 აბზაცი.

¹⁶⁸ იქვე, მე-18 მუხლის მე-2 პუნქტის პირველი აბზაცი.

მონაცემთა დაცვის დირექტივა განსაზღვრავს რამოდენიმე ინსტრუმენტს შესაბამისობის მხარდასაჭერად:

1. ეროვნული საზედამხედველო ორგანოს მიერ დამუშავების დაგეგმილი მოქმედებების წინასწარი შემოწმება;
 2. პერსონალურ მონაცემთა დაცვის პასუხისმგებელი პირები, რომლებიც დამმუშავებლისთვის განახორციელებენ შესაბამის ექსპერტიზას მონაცემთა დაცვის მხრივ;
 3. ქცევის კოდექსები, რომელიც განსაზღვრავს მონაცემთა დაცვის არსებულ წესებს, ძირითადად, ბიზნეს-გაერთიანებებზე გასავრცობად.
- ევროპის საბჭო; პროფილირების შესახებ რეკომენდაციით, აყალიბებს შესაბამისობის ნახალისების მსგავს ინსტრუმენტებს.

4.4.1. წინასწარი შემოწმება

მონაცემთა დაცვის დირექტივის მე-20 მუხლის თანახმად, საზედამხედველო ორგანომ დამუშავების დაწყებამდე უნდა შეამოწმოს დამუშავების ოპერაციები, რომლებიც შესაძლებელია წარმოშობდეს რისკებს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებებისთვის, დამუშავების პირობების ან მიზნის გათვალისწინებით. შიდასახელმწიფოებრივმა კანონმა უნდა განსაზღვროს, თუ რომელი დამუშავების სახეობა ექვემდებარება წინასწარ შემოწმებას. ამგვარი შემოწმების შედეგად, შესაძლებელია მოხდეს დამუშავების სახეობის აკრძალვა ან დამუშავების მოცემულ სახეობათა თავისებურებების შეცვლა. დირექტივის მე-20 მუხლი განსაზღვრავს, რომ სარისკო და აუცილებლობის არმქონე დამუშავება საერთოდ არ უნდა დაიწყოს, ხოლო ზედამხედველი ორგანო უფლებამოსილია აკრძალოს მსგავსი ოპერაციები. ამ მექანიზმის ეფექტურობის წინაპირობა არის ის, რომ ზედამხედველი ორგანო იქნეს ინფორმირებული. იმისათვის, რათა უზრუნველყოფილ იქნეს დამმუშავებელთა მიერ შეტყობინების ვალდებულების შესრულება, ზედამხედველ ორგანოს დასჭირდება იძულებითი მექანიზმები, ისეთი, როგორიცაა დამმუშავებლების დაჯარიმების შესაძლებლობა.

მაგალითი: თუ კომპანია აწარმოებს იმგვარ დამუშავებას, რომელიც შიდასახელმწიფოებრივი კანონმდებლობის მიხედვით, ექვემდებარება წინასწარ შემოწმებას, ამ კომპანიამ ზედამხედველ ორგანოს უნდა მიაწოდოს დოკუმენტაცია დაგეგმილი დამუშავების მოქმედებათა შესახებ. კომპანია არ არის უფლებამოსილი დაიწყოს დამუშავება ზედამხედველი ორგანოდან დადებითი პასუხის მიღების გარეშე.

ევროპული კავშირის ზოგიერთ წევრ ქვეყანაში კანონმდებლობა აწესებს, რომ დამუშავების ოპერაციები შესაძლებელია დაიწყოს თუ ზედამხედველი ორგანოს მიერ დროის კონკრეტულ ვადაში არ განხორციელდა გამოხმაურება, მაგალითად, სამი თვის განმავლობაში.

4.4.2. პერსონალურ მონაცემთა დაცვის პასუხისმგებელი პირები

მონაცემთა დაცვის ღირექტივა განსაზღვრავს შესაძლებლობას, რომ დამუშავებლებისთვის შიდასახელმწიფოებრივი კანონმდებლობით დადგინდეს პერსონალურ მონაცემთა დაცვაზე პასუხისმგებელი პირის განსაზღვრის უფლებამოსილება.¹⁶⁹ ამ მოცემულობის მიზანია მოხდეს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დაცვა დამუშავებით გათვალისწინებული ნეგატიური ზეგავლენისგან.¹⁷⁰

მაგალითი: გერმანიის მონაცემთა დაცვის ფედერალური კანონის მე-4f პარაგრაფის პირველი ქვე-პარაგრაფის თანახმად, კერძო საკუთრებაში არსებულ კომპანიებს ევალებათ დანიშნონ პერსონალური მონაცემთა დაცვის შიდა პასუხისმგებელი პირი, თუ კომპანიები მუდმივად ახორციელებენ პერსონალურ მონაცემთა დამუშავების ავტომატიზებულ მოქმედებებს ათი ან მეტი პირის მეშვეობით.

მოცემული მიზნის მისაღწევად აუცილებელია პასუხისმგებელი პირის პოზიციის დამოუკიდებლობის გარკვეული დონით უზრუნველყოფა დამუშავებლის ორგანიზაციაში, რაც მკაფიოდ არის დადგენილი ღირექტივით. გარდა ამისა, მძლავრი შრომითი უფლებების არსებობა, როგორცაა დაუსაბუთებელი დათხოვნის წინააღმდეგ დაცვის უფლება, ასევე, იქნება აუცი-

169 იქვე, მე-18 მუხლის მე-2 პუნქტის მე-2 აბზაცი.

170 *ibid.*

ლებელი მოცემული პასუხისმგებელი პირის (სამსახურის) ეფექტური ფუნქციონირებისთვის.

მონაცემთა დაცვის შიდასახელმწიფოებრივ კანონთან შესაბამისობის ხელშეწყობისთვის, პერსონალურ მონაცემთა დაცვის შიდა პასუხისმგებელი პირების კონცეფცია, ასევე, დადგენილ იქნა ევროპის საბჭოს ზოგიერთი რეკომენდაციით.¹⁷¹

4.4.3. ქცევის კოდექსები

შესაბამისობის მხარდასაჭერად, ბიზნესისა და სხვა სექტორების წარმომადგენლებს, საუკეთესო პრაქტიკის კოდიფიკაციის გზით შეუძლიათ განსაზღვრონ დეტალური წესები, რაც დაარეგულირებს დამუშავების ჩვეულ მოქმედებებს. კონკრეტული სექტორის წევრთა მიერ განხორციელებული ექსპერტიზა ხელს შეუწყობს პრაქტიკული გადაწყვეტიების მოიძიებას და, შესაბამისად, სამომავლო შესრულებას. აქედან გამომდინარე, ევროპული კავშირის წევრი ქვეყნები, ისევე როგორც ევროპული კომისია, ხელს უწყობს ქცევის კოდექსების შემუშავებას, რომელიც მიზნად ისახავს შიდასახელმწიფოებრივი დებულებების სწორი იმპლემენტირების მხარდაჭერას, რაც განსაზღვრულია წევრი ქვეყნების მიერ დირექტივის შესაბამისად, სხვადასხვა სექტორის თავისებურებების გათვალისწინებით.¹⁷²

იმისათვის, რათა უზრუნველყოფილ იქნეს აღნიშნული ქცევის კოდექსების შესაბამისობა შიდასახელმწიფოებრივ დებულებებთან, რომელიც მიღებულ იქნა, თავის მხრივ, მონაცემთა დაცვის დირექტივიდან გამომდინარე, წევრმა ქვეყნებმა უნდა დაადგინონ მათი შეფასების პროცედურები. ამ პროცედურამ უნდა განსაზღვროს შიდასახელმწიფოებრივი საზედამხებელო ორგანოს, სავაჭრო ასოციაციებისა და იმ პირების ჩართვა, რომელიც წარმოადგენენ სხვა კატეგორიის მონაცემთა დამმუშავებლებს.¹⁷³

გაერთიანების კოდექსის პროექტები და ცვლილებები ან გაერთიანების არსებული კოდექსებით დადგენილი დამატებე-

171 იხ. მაგალითად, რეკომენდაცია პროფილირების შესახებ, მე-8 მუხლის მე-3 პუნქტი.

172 იხ. მონაცემთა დაცვის დირექტივა, 27-ე მუხლის პირველი პუნქტი.

173 იქვე, 27-ე მუხლის მე-2 პუნქტი.

ბი შესაძლებელია იქნეს გაგზავნილი შეფასებისთვის მუხლი 29 სამუშაო ჯგუფისთვის. აღნიშნული სამუშაო ჯგუფის მიერ დადასტურების შემთხვევაში, ევროპულ კომისიას შეუძლია უზრუნველყოს მოცემულ კოდექსთა სათანადო გამოქვეყნება.¹⁷⁴

მაგალითი: პირდაპირი და ინტერაქტიული მარკეტინგის ევროპულ-მა ფედერაციამ შეიმუშავა ქცევის ევროპული კოდექსი პირდაპირი მარკეტინგისას პერსონალურ მონაცემთა გამოყენების შესახებ. ეს კოდექსი მონონებული იქნა მუხლი 29 სამუშაო ჯგუფის მიერ. დანართი, რომელიც ეხება ელექტრონულ მარკეტინგულ კომუნიკაციას, დამატებულ იქნა კოდექსში 2010 წელს.¹⁷⁵

174 იქვე, 27-ე მუხლის მე-3 პუნქტი.

175 მუხლი 29 სამუშაო ჯგუფი (2010), მოსაზრება 4/2010 FEDMA-ს ქცევის ევროპული კოდექსის შესახებ პირდაპირი მარკეტინგისთვის პერსონალურ მონაცემთა გამოყენების თაობაზე, WP 174, ბრიუსელი, 13 ივლისი 2010 წელი.

5. მონაცემთა სუბიექტის უფლებები და მათი რეალიზაცია

ევროპული კავშირი	განხილული საკითხები	ევროპის საბჭო
წდომის უფლება		
მონაცემთა დაცვის დირექტივა, მე-12 მუხლი მართლმსაჯულების ევროპული კავშირის სასამართლო, C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkboer, 7 მაისი 2009 წელი	პირის მიერ საკუთარ მონაცემებზე წდომის უფლება	108-ე კონვენცია, მე-8 მუხლის -b- ქვეპუნქტი
	შეცვლის, წაშლის ან დაბლოკვის უფლება	108-ე კონვენცია, მე-8 მუხლის -c- ქვეპუნქტი ადამიანის უფლებათა ევროპული სასამართლო, Cemalettin Canli v. Turkey, No. 22427/04, 18 ნოემბერი 2008 წელი ადამიანის უფლებათა ევროპული სასამართლო, Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 6 ივნისი 2006 წელი ადამიანის უფლებათა ევროპული სასამართლო, Ciubotaru v. Moldova, No. 27138/04, 27 ივლისი 2010 წელი
გასაჩივრების უფლება		
მონაცემთა დაცვის დირექტივა, მე-14 მუხლის პირველი პუნქტის -a- ქვეპუნქტი	გასაჩივრების უფლება მონაცემთა სუბიექტის კონკრეტული ვითარების გათვალისწინებით	რეკომენდაცია პროფილირების შესახებ, მე-5 მუხლის მე-3 პუნქტი
მონაცემთა დაცვის დირექტივა, მე-14 მუხლის პირველი პუნქტის -b- ქვეპუნქტი	გასაჩივრების უფლება პირდაპირი მარკეტინგისთვის მონაცემთა შემდგომი გამოყენების თაობაზე	რეკომენდაცია პირდაპირი მარკეტინგის შესახებ, მე-4 მუხლის პირველი პუნქტი

მონაცემთა დაცვის დირექტივა, მე-15 მუხლი	გასაჩივრების უფლება ავტომატიზებული გადწყვეტილებების შესახებ	რეკომენდაცია პროფილირების შესახებ, მე-5 მუხლის მე-5 პუნქტი
დამოუკიდებელი ზედამხედველობა		
ქარტია, მე-8 მუხლის მესამე პუნქტი მონაცემთა დაცვის დირექტივა, 28-ე მუხლი ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის რეგულაცია, მე-5 თავი მონაცემთა დაცვის რეგულაცია მართლმსაჯულების ევროპული კავშირის სასამართლო, C-518/07, European Commission v. Federal Republic of Germany, 9 მარტი 2010 წელი მართლმსაჯულების ევროპული კავშირის სასამართლო, C-614/10, European Commission v. Republic of Austria, 16 ოქტომბერი 2012 წელი მართლმსაჯულების ევროპული კავშირის სასამართლო C-288/12, European Commission v. Hungary, 8 ივნისი 2012 წელი	შიდასახელმწიფოებრივი საზედამხედველო ორგანოები	108-ე კონვენცია, დამატებითი ოქმი, პირველი მუხლი
სამართლებრივი დაცვის საშუალებები და სანქციები		
მონაცემთა დაცვის დირექტივა, მე-12 მუხლი	მიმართვა დამმუშავებელს	108-ე კონვენცია, მე-8 მუხლის -ბ- ქვეპუნქტი
მონაცემთა დაცვის დირექტივა, 28-ე მუხლის მე-4 პუნქტი ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის რეგულაცია, 32-ე მუხლის მე-2 პუნქტი	საზედამხედველო ორგანოში შეტანილი საჩივარი	108-ე კონვენცია, დამატებითი ოქმი, პირველი მუხლის მე-2 პუნქტის -ბ- ქვეპუნქტი

ქარტია, 47-ე მუხლი	სასამართლო (ზოგადად)	ადამიანის უფლებათა ევროპული კონვენცია, მე-13 მუხლი
მონაცემთა დაცვის დირექტივა, 28-ე მუხლის მე-3 პუნქტი	შიდასახელმწიფოებრივი სასამართლოები	108-ე კონვენცია, დამატებითი ოქმი, პირველი მუხლის მე-4 პუნქტი
ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულება, 263-ე მუხლის მე-4 პუნქტი	მართლმსაჯულების ევროპული კავშირის სასამართლო	
ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის რეგულაცია, 32-ე მუხლის პირველი პუნქტი		
ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულება, 267-ე მუხლი		
	ადამიანის უფლებათა ევროპული სასამართლო	ადამიანის უფლებათა ევროპული კონვენცია, 34-ე მუხლი
ქარტია, 47-ე მუხლი	მონაცემთა დაცვის შიდასახელმწიფოებრივი კანონმდებლობის დარღვევებისთვის	ადამიანის უფლებათა ევროპული სასამართლო, მე-13 მუხლი (მხოლოდ ევროპის საბჭოს წევრი ქვეყნებისთვის)
მონაცემთა დაცვის დირექტივა, 22-ე და 23-ე მუხლები		108-ე კონვენცია, მე-10 მუხლი
მართლმსაჯულების ევროპული კავშირის სასამართლო, C-14/83, Sabine von Colson and Elisabeth Kamann v. Land Nordrhein-Westfalen, 10 აპრილი 1984 წელი		ადამიანის უფლებათა ევროპული სასამართლო, K.U. v. Finland, No. 2872/02, 2 დეკემბერი 2008 წელი
მართლმსაჯულების ევროპული კავშირის სასამართლო, C-152/84, M.H. Marshall v. Southampton and South- West Hampshire Area Health Authority, 26 თებერვალი 1986 წელი		ადამიანის უფლებათა ევროპული სასამართლო, Bir-iuk v. Lithuania, No. 23373/03, 25 თებერვალი 2009 წელი

ევროპული კავშირის დანესებულებათა მონაცემთა დაცვის რეგულაცია 34-ე და 49-ე მუხლები მართლმსაჯულების ევროპული კავშირის სასამართლო C-28/08 P, European Commission v. The Bavarian Lager Co. Ltd, 29 ივნისი 2010 წელი	ევროპული კავშირის დანესებულებებისა და ორგანოების მიერ ევროპული კავშირის კანონმდებლობის დარღვევა	
---	---	--

ზოგადად, ძირითადი სამართლებრივი ნორმების ეფექტურობა, კერძოდ, მონაცემთა სუბიექტების უფლებების ეფექტურობა, მნიშვნელოვნად დამოკიდებულია მათი აღსრულების შესაბამისი მექანიზმების არსებობაზე. მონაცემთა დაცვის ევროპულ სამართალში, მონაცემთა სუბიექტი შიდასახელმწიფოებრივი კანონმდებლობის მიერ უნდა იყოს აჭურვილი გარკვეული უფლებებით, საკუთარი მონაცემების დასაცავად. დამოუკიდებელი საზედამხედველო ორგანოები, ასევე, უნდა იქნეს დაფუძნებული შიდასახელმწიფოებრივი კანონმდებლობით, რათა მხარი დაუჭირონ მონაცემთა სუბიექტებს მათი უფლებების რეალიზაციისას და განახორციელონ პერსონალურ მონაცემთა დამუშავების ზედამხედველობა. ამასთან, ეფექტური სამართლებრივი დაცვის უფლება, რაც გარანტირებულია ადამიანის უფლებათა ევროპული კონვენციითა და ძირითად უფლებათა ქარტიით, მოითხოვს, რომ სამართლებრივი დაცვის საშუალებები იყოს ხელმისაწვდომი ნებისმიერი პირისთვის.

5.1. მონაცემთა სუბიექტის უფლებები

საკვანძო დებულებები

- შიდასახელმწიფოებრივი კანონმდებლობით ყველას უნდა ჰქონდეს უფლება ნებისმიერი დამმუშავებლისგან მოითხოვოს ინფორმაცია მის შესახებ არსებულ მონაცემთა დამუშავების თაობაზე.
- შიდასახელმწიფოებრივი კანონმდებლობით მონაცემთა სუბიექტებს უნდა ჰქონდეთ უფლება, რომ:

1. ჰქონდეთ წვდომა საკუთარ მონაცემებზე იმ დამმუშავებელთან, რომელიც ამუშავებს მონაცემებს;
 2. მოახდინონ საკუთარი მონაცემების შესწორება (ან დაბლოკვა, შესაბამის შემთხვევებში) იმ დამმუშავებელთან, რომელიც ამუშავებს მონაცემებს, თუ ისინი არაზუსტია;
 3. საჭიროების შემთხვევაში, მოახდინონ დამმუშავებელთან საკუთარ მონაცემთა წაშლა ან დაბლოკვა თუ დამმუშავებელი უკანონოდ ამუშავებს მონაცემს.
- დამატებით, მონაცემთა სუბიექტებს უნდა ჰქონდეთ უფლება დამმუშავებელთან გაასაჩივრონ:
 1. ავტომატიზებული გადაწყვეტილებები (მიღებული პერსონალურ მონაცემთა მხოლოდ ავტომატიზებული დამუშავების საშუალებებით);
 2. მონაცემთა დამუშავება თუ ეს წარმოშობს არაპროპორციულ შედეგებს;
 3. მონაცემთა გამოყენება პირდაპირი მარკეტინგის მიზნებისთვის.

5.1.1. წვდომის უფლება

ევროპული კავშირის კანონმდებლობის მიხედვით, მონაცემთა დაცვის დირექტივის მე-12 მუხლი შეიცავს მონაცემთა სუბიექტების წვდომის უფლების ელემენტებს, მათ შორის უფლებას, რომ მონაცემთა დამმუშავებლისგან მიიღონ ინფორმაცია, მუშავდება თუ არა მის შესახებ მონაცემები და, ასევე, ინფორმაცია დამუშავების მიზნის, მონაცემთა კატეგორიების და მათი მიმღებების ან მიმღებთა კატეგორიების შესახებ, ვისთვისაც ხდება მონაცემთა გადაცემა, ასევე მოითხოვონ იმ მონაცემთა შეცვლა, წაშლა ან დაბლოკვა, რომელთა დამუშავებაც არ არის შესაბამისობაში დირექტივის დებულებებთან, მონაცემთა ნაკლებობის ან უზუსტობის გამო.

მსგავსი უფლებებია დადგენილი ევროპის საბჭოს კანონმდებლობის მიხედვით, რაც, ასევე, იდენტურად უნდა იყოს განსაზღვრული შიდასახელმწიფოებრივი კანონმდებლობით (108-ე

კონვენციის მე-8 მუხლი). ევროპის საბჭოს ზოგიერთი რეკომენდაციით, გამოყენებულია ცნება „წვდომა“, ხოლო წვდომის უფლების განსხვავებული ასპექტები აღწერილია და განსაზღვრულია შიდასახელმწიფოებრივ კანონმდებლობაში იმპლემენტირებისთვის იმგვარად, როგორც მოცემულია აღნიშნული პარაგრაფით.

108-ე კონვენციის მე-9 მუხლით და მონაცემთა დაცვის დირექტივის მე-13 მუხლით, დამმუშავებლების ვალდებულება – მოახდინონ მონაცემთა სუბიექტების წვდომის მოთხოვნაზე რეაგირება, შესაძლებელია იქნეს შეზღუდული სხვათა აღმატებული სამართლებრივი ინტერესების საფუძველზე. აღმატებული სამართლებრივი ინტერესები შეიძლება მოიცავდეს როგორც საჯარო ინტერესს, როგორიცაა ეროვნული თავდაცვა, საზოგადოებრივი უსაფრთხოება და დანაშაულთა გამოძიება, ასევე, იმ კერძო ინტერესებს, რომელიც უფრო აღმატებულია მონაცემთა დაცვის ინტერესებთან შედარებით. ნებისმიერი გამონაკლისი ან შეზღუდვა უნდა იყოს აუცილებელი დემოკრატიულ საზოგადოებაში და დასახული მიზნის პროპორციული. ძალიან იშვიათ შემთხვევებში, მაგალითად, სამედიცინო ჩვენებების დროს, მონაცემთა სუბიექტის დაცვა შესაძლოა მოითხოვდეს გამჭვირვალობის შეზღუდვას; ეს, ძირითადად, ეხება მონაცემებზე წვდომის უფლების შეზღუდვას ნებისმიერი მონაცემთა სუბიექტისთვის.

როდესაც მონაცემები მუშავდება მხოლოდ სამეცნიერო ან სტატისტიკური კვლევის მიზნებისთვის, მონაცემთა დაცვის დირექტივა დასაშვებად მიიჩნევს წვდომის უფლების შეზღუდვას შიდასახელმწიფოებრივი კანონმდებლობის მიხედვით; თუმცა, სამართლებრივი დაცვის ადეკვატური მექანიზმები უნდა იქნეს მიღებული. კერძოდ, უზრუნველყოფილ უნდა იქნეს, რომ არც ერთი ზომა ან გადაწყვეტილება არ არის მიღებული რომელიმე ინდივიდის შესახებ მონაცემთა ამგვარი დამუშავების კონტექსტში და „ნამდვილად არ არსებობს მონაცემთა სუბიექტების პირადი ცხოვრების დარღვევის რისკი.“¹⁷⁶ მსგავსი დებულებები მოცემულია 108-ე კონვენციის მე-9 მუხლის მესამე პუნქტით.

176 მონაცემთა დაცვის დირექტივა, მე-13 მუხლის მე-2 პუნქტი.

პირის მიერ საკუთარ მონაცემებზე წვდომის უფლება

ევროპის საბჭოს კანონმდებლობის მიხედვით, პირის მიერ საკუთარ მონაცემებზე წვდომის უფლება მკაფიოდ აღიარებულია 108-ე კონვენციის მე-8 მუხლით. ადამიანის უფლებათა ევროპულმა სასამართლომ არაერთგზის აღნიშნა, რომ პირს გააჩნია უფლება მიიღოს ინფორმაცია საკუთარი პერსონალური მონაცემების შესახებ, რომელსაც ფლობს ან იყენებს სხვა, ხოლო ეს უფლება გამომდინარეობს პირადი ცხოვრების დაცვის აუცილებლობიდან.¹⁷⁷ ლენდერის საქმეზე,¹⁷⁸ ადამიანის უფლებათა ევროპულმა სასამართლომ დაასკვნა, რომ იმ პერსონალურ მონაცემებთან წვდომის უფლება, რომელიც შენახული აქვთ საჯარო ორგანოებს, გარკვეულ შემთხვევებში, შესაძლებელია იქნეს შეზღუდული.

ევროპული კავშირის კანონმდებლობის მიხედვით, პირის უფლება განახორციელოს წვდომა საკუთარ მონაცემებზე, მკაფიოდ დადგენილია მონაცემთა დაცვის დირექტივის მე-12 მუხლით და, როგორც ძირითადი უფლება, ქარტიის მე-8 მუხლის მე-2 პუნქტით.

დირექტივის მე-12 მუხლის -a- ქვეპუნქტი ადგენს, რომ ევროპული კავშირის წევრმა ქვეყნებმა უნდა მოახდინონ თითოეული მონაცემთა სუბიექტისთვის მათ პერსონალურ მონაცემებზე წვდომისა და ინფორმირების უფლების უზრუნველყოფა. კერძოდ, მონაცემთა თითოეულ სუბიექტს აქვს უფლება, რომ მიიღოს დამმუშავებლისგან ინფორმაცია იმის შესახებ, მუშავდება თუ არა მისი მონაცემები და ინფორმაცია, რომელიც მოიცავს, სულ მცირე:

- დამუშავების მიზნებს;
- დასამუშავებელ მონაცემთა კატეგორიებს;
- მონაცემებს, რომელიც დამუშავების პროცესშია;

¹⁷⁷ ადამიანის უფლებათა ევროპული სასამართლო, *Gaskin v. the United Kingdom*, No. 10454/83, 7 ივლისი 1989 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *Odièvre v. France* [GC], No. 42326/98, 13 თებერვალი 2003 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *K.H. and Others v. Slovakia*, No. 32881/04, 28 აპრილი 2009 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *Godelli v. Italy*, No. 33783/09, 25 სექტემბერი 2012 წელი.

¹⁷⁸ ადამიანის უფლებათა ევროპული სასამართლო, *Leander v. Sweden*, No. 9248/81, 26 მარტი 1987 წელი.

- მიმღებების ან მიმღებთა კატეგორიებს, რომლებსაც გადაეცათ მონაცემები;
- ნებისმიერ არსებულ ინფორმაციას, რაც უკავშირდება დამუშავების პროცესში არსებული მონაცემების წყაროს;
- ნებისმიერი ავტომატიზებული გადაწყვეტილებების შემთხვევაში, თითოეული ავტომატიზებული დამუშავების ლოგიკის შესახებ ინფორმაციას.

შიდასახელმწიფოებრივი კანონმდებლობით შესაძლებელია დამატებულ იქნეს ინფორმაცია, რაც უნდა მიაწოდოს დამმუშავებელმა, მაგალითად, მონაცემთა დამუშავების სამართლებრივი საფუძვლის შესახებ ინფორმაცია.

მაგალითი: პირის მიერ მონაცემთა წვდომის შემთხვევაში, მას შეუძლია შეაფასოს არის თუ არა ეს მონაცემები სწორი. შესაბამისად, აუცილებელია მონაცემთა სუბიექტი იქნეს ინფორმირებული დამუშავებულ მონაცემთა კატეგორიების შესახებ, ისევე როგორც მისი მინაარსის შესახებ. აქედან გამომდინარე, საკმარისი არ იქნება თუ მონაცემთა დამმუშავებელი აცნობებს მონაცემთა სუბიექტს, რომ იგი ამუშავებს მის სახელს, მისამართს, დაბადების თარიღსა და ინტერესის სფეროს. დამმუშავებელმა უნდა წარუდგინოს მონაცემთა სუბიექტს, რომ იგი ამუშავებს „სახელს: ნ.ნ; მისამართს: შვარცენბერგპლატზი 11, 1040, ვენა, ავსტრია; დაბადების თარიღი: 10.10.1977; და ინტერესის სფერო (გაცხადებული მონაცემთა სუბიექტის მიერ): კლასიკური მუსიკა.“ ეს უკანასკნელი, დამატებით, მოიცავს ინფორმაციას მონაცემთა წყაროს შესახებ.

მონაცემთა სუბიექტისთვის მონაცემთა მიმდინარე დამუშავების პროცესის შესახებ შეტყობინება და ყოველი ხელმისაწვდომი წყაროს შესახებ ინფორმაციის მიწოდება უნდა განხორციელდეს გასაგები ფორმით, რაც ნიშნავს, რომ შესაძლოა დამმუშავებელმა დეტალურად განუმარტოს მონაცემთა სუბიექტს თუ რისი დამუშავება მიმდინარეობს. მაგალითად, წვდომის მოთხოვნაზე საპასუხოდ მხოლოდ ტექნიკური აბრევიატურის ან სამედიცინო ტერმინოლოგიის მიწოდება, როგორც წესი, არ იქნება საკმარისი იმ შემთხვევაშიც კი, თუ მხოლოდ მსგავსი აბრევიატურები ან ცნებები არის შენახული.

მონაცემთა იმ წყაროს შესახებ ინფორმაცია, რომელიც მუ-

შავდება დამმუშავებლის მიერ, უნდა იქნეს მიწოდებული წვდომის მოთხოვნაზე საპასუხოდ თუ არსებობს ამგვარი ინფორმაცია. ეს დებულება გაგებულ უნდა იქნეს სამართლიანობისა და ანგარიშვალდებულების პრინციპის ქრილში. დამმუშავებელმა არ უნდა გაანადგუროს ინფორმაცია მონაცემთა წყაროს შესახებ, იმ მიზნით, რომ აღარ იყოს პასუხისმგებელი მის გაცემაზე, ასევე, არ უნდა განახორციელოს მისი მოქმედებების დასაბუთების ჩვეული და აღიარებული სტანდარტის იგნორირება. დამმუშავებულ მონაცემთა წყაროს შესახებ ინფორმაციის განადგურება, ძირითადად, წვდომის უფლების ქრილში, არ უზრუნველყოფს დამმუშავებლის ვალდებულებების შესრულებას.

ავტომატური შეფასებების წარმოებისას, მათი ძირითადი ლოგიკა უნდა იქნეს განმარტებული იმ კრიტერიუმების გათვალისწინებით, რაც მონაცემთა სუბიექტის შეფასებისას იქნა გამოყენებული.

დირექტივა კონკრეტულად არ ადგენს, თუ რამდენად ვრცელდება ინფორმაციაზე წვდომის უფლება წარსულში და, თუ ვრცელდება, რა პერიოდს მოიცავს. ამ მხრივ, როგორც ხაზგასმულია მართლმსაჯულების ევროპული კავშირის სასამართლოს პრეცედენტებში, პირის უფლება მონაცემთა წვდომაზე არ უნდა იქნეს არაგონივრულად დროში შეზღუდული. მონაცემთა სუბიექტებს უნდა ჰქონდეთ არსებითი შესაძლებლობა მიიღონ ინფორმაცია მონაცემთა დამმუშავების წარსულში არსებულ მოქმედებათა შესახებ.

მაგალითი: საქმეზე *Rijkeboer*,¹⁷⁹ მართლმსაჯულების ევროპული კავშირის სასამართლოს წინაშე დაისვა საკითხი, დაედგინა დირექტივის მე-12 მუხლის -a- ქვეპუნქტის თანახმად, იყო თუ არა შესაძლებელი პირის წვდომის უფლების განსაზღვრა ერთ წლამდე ვადით იმ ინფორმაციაზე, რომელიც ეხება პერსონალურ მონაცემთა მიმღებებს ან მიმღებთა კატეგორიებს და გადაცემულ მონაცემთა შინაარსს.

იმისათვის, რათა განესაზღვრა თუ რამდენად იძლევა დირექტივის მე-12 მუხლის -a- ქვეპუნქტი დროში შეზღუდვის ამგვარ საშუალებას, სასამართლომ გადანყვიტა განემარტა მოცემული მუხლი დირექტივის მიზნებიდან გამომდინარე. სასამართლომ, პირველ

179 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 7 მაისი 2009 წელი.

რიგში, აღნიშნა, რომ წვდომის უფლება აუცილებელია მონაცემთა სუბიექტებისთვის იმ უფლების რეალიზაციის მხრივ, რომლის საფუძველზეც დამუშავებული შეასწორებს, წაშლის ან დაბლოკავს მის მონაცემებს (მუხლი 12, -b- ქვეპუნქტი), ან მესამე პირებისთვის, ვისაც გადაეცა მონაცემები, მიმართვის განსახორციელებლად, შესწორების, წაშლის ან დაბლოკვის მოთხოვნით (მუხლი 12 -c- ქვეპუნქტი). წვდომის უფლება, ასევე, აუცილებელია, რათა მონაცემთა სუბიექტებს მიეცეს უფლება პერსონალურ მონაცემთა დამუშავების გასაჩივრების თაობაზე (მუხლი 14) ან ზიანის მიღების შემდეგ რეაგირების უფლების უზრუნველყოფისთვის (მუხლი 22 და 23).

განხილული დებულებებისთვის პრაქტიკული მნიშვნელობის მისაცემად, სასამართლომ დაადგინა, რომ „ეს უფლება აუცილებელი წესით უნდა ეხებოდეს წარსულს. წინააღმდეგ შემთხვევაში, მონაცემთა სუბიექტი ვეღარ მოახდენს მისი უფლების, სავარაუდო უკანონო ან არაზუსტი მონაცემების შესწორების, წაშლის ან დაბლოკვის რეალიზაციას ან სამართლებრივი პროცედურების წარმოებას და კომპენსაციის მიღებას მიყენებული ზიანისთვის.“

მონაცემთა შეცვლის, წაშლისა და დაბლოკვის უფლება

„ნებისმიერ პირს უნდა ჰქონდეს შესაძლებლობა მოახდინოს მის შესახებ არსებულ მონაცემებზე წვდომის უფლების რეალიზაცია, რათა შეეძლოს მონაცემთა სისწორისა და მისი დამუშავების კანონიერების დადასტურება.“¹⁸⁰ ამ პრინციპებთან ერთად, მონაცემთა სუბიექტებს, შიდასახელმწიფოებრივი კანონმდებლობით, უნდა შეეძლოს მონაცემები შეცვლის, წაშლის ან დაბლოკვის რეალიზაცია დამუშავებელთან, თუ მიაჩნიათ, რომ დამუშავება არ არის შესაბამისობაში დირექტივის დებულებებთან, მონაცემთა უზუსტობის ან არასრული ბუნების გამო.¹⁸¹

მაგალითი: საქმეზე *Cemalettin Canli v. Turkey*,¹⁸² ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა, რაც ეხებოდა პოლიციის მცდარ შეტყობინებებს საგამოძიებო მოქმედების დროს.

180 მონაცემთა დაცვის დირექტივა, პრეამბულის 41-ე პუნქტი.

181 იქვე, მე-12 მუხლის -b- ქვეპუნქტი.

182 ადამიანის უფლებათა ევროპული სასამართლო, ჩეპალეტტინ ჩანლი ვ. თურქეთი, ო. 22427/04, 18 ნოემბერი 2008 წელი, პარაგ. 33, 42 და 43; ადამიანის უფლებათა ევროპული სასამართლო ალვა ვ. რანცე, ო. 964/07, 2 თებერვალი 2010 წელი.

უკანონო ორგანიზაციებში შესაძლო წევრობისთვის განმცხადებელზე ორჯერ განხორციელდა საგამოძიებო მოქმედებები, თუმცა არასდროს იქნა დამნაშავედ ცნობილი. როდესაც განმცხადებელი დაკავებულ იქნა სხვა დანაშაულისთვის და წარედგინა ბრალდება, პოლიციამ სასამართლოს გაუგზავნა შეტყობინება სათაურით „ინფორმაცია სხვა დანაშაულებზე“, სადაც განმცხადებელი მოხსენიებულ იქნა ორი უკანონო ორგანიზაციის წევრად. განმცხადებლის მოთხოვნა შეტყობინებისა და პოლიციის ჩანაწერების შეცვლის შესახებ არ იქნა დაკმაყოფილებული. ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ პოლიციის შეტყობინებაში მოცემული ინფორმაცია ეხებოდა კონვენციის მე-8 მუხლით გათვალისწინებულ ფარგლებს, რამდენადაც საჯარო ინფორმაცია შესაძლოა მოექცეს პირადი ცხოვრების ფარგლებში, როდესაც იგი სისტემადურად შეგროვებული და შენახულია ფაილებში სახელმწიფო ორგანოების მიერ. თუმცა, პოლიციის ანგარიში იყო არასწორი და მისი ჩამოყალიბება და მიწოდება სისხლის სამართლის საქმის განმხილველი სასამართლოსთვის არ იყო შესაბამისობაში კანონთან. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა მე-8 მუხლის დარღვევა.

მაგალითი: საქმეზე *Segerstedt-Wiberg and Others v. Sweden*,¹⁸³ განმცხადებლები დაკავშირებულნი იყვნენ კონკრეტულ ლიბერალურ და კომუნისტურ პოლიტიკურ პარტიებთან. ისინი ეჭვობდნენ, რომ მათ შესახებ ინფორმაცია შეტანილ იქნა დაცვის პოლიციის ჩანაწერებში. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ მონაცემთა შენახვას გააჩნდა სამართლებრივი საფუძველი და ემსახურებოდა ლეგიტიმურ მიზანს. ზოგიერთი განმცხადებლის შემთხვევაში, სასამართლომ დაადგინა, რომ მონაცემთა შემდგომი შენახვა წარმოადგენდა არაპროპორციულ ჩარევას მათ პირად ცხოვრებაში. მაგალითად, შმიდის შემთხვევაში, სახელმწიფო დაწესებულებებს შენახული ჰქონდათ ინფორმაცია, რომლის თანახმად 1969 წელს დემონსტრაციების მიმდინარეობისას იგი მხარს უჭერდა პოლიციის წინააღმდეგ მიმართულ ძალადობრივ ქმედებას. სასამართლომ აღნიშნა, რომ ეს ინფორმაცია, მისი ისტორიული ბუნებიდან გამომდინარე, არ ემსახურებოდა ეროვნული უსაფრთხოების რომელიმე რელევანტურ ინტერესს. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა ხუთი განმცხადებლისგან ოთხის შემთხვევაში.

183 ადამიანის უფლებათა ევროპული სასამართლო *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 6 ივნისი 2006, პარაგ. 89 და 90; იხ. ასევე, მაგ. ადამიანის უფლებათა ევროპული სასამართლო, *M.K. v. France*, No. 19522/09, 18 აპრილი 2013 წელი.

ზოგიერთ შემთხვევაში, მონაცემთა სუბიექტის მიერ საკმარისი იქნება მხოლოდ მოთხოვნა მონაცემის, მაგალითად, სახელის წარმოთქმის, მისამართის ან ტელეფონის ნომერის შეცვლის შესახებ. თუ, მოთხოვნა დაკავშირებულია სამართლებრივ საკითხებთან, როგორიცაა მონაცემთა სუბიექტის რეგისტრირებული ვინაობა, ან საცხოვრებლის ზუსტი ადგილი სამართლებრივი დოკუმენტაციის გადასაცემად, მხოლოდ შეცვლის მოთხოვნა არ იქნება საკმარისი და დამუშავებელი უფლებამოსილია მოითხოვოს გაცხადებული უზუსტობის დამტკიცება. ამგვარმა მოთხოვნებმა მონაცემთა სუბიექტს არ უნდა დააკისროს არაგონივრული მტკიცებების ტვირთი, რაც გამორიცხავს მონაცემთა სუბიექტების შესახებ მონაცემთა შეცვლას. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევები საქმეებზე, სადაც განმცხადებლებს არ ჰქონდათ საშუალება განესაზღვრათ საიდუმლო რეესტრებში შენახული ინფორმაციის სისწორე.¹⁸⁴

მაგალითი: საქმეზე *Ciubotaru v. Moldova*,¹⁸⁵ განმცხადებელმა ვერ შეცვალა სახელმწიფო რეესტრში მისი ეთნიკური წარმომავლობის შესახებ ჩანაწერი მოლდოველიდან რუმინელზე, იმ ფაქტის გამო, რომ მან ვერ დაასაბუთა მოთხოვნა. ადამიანის უფლებათა ევროპულმა სასამართლომ დასაშვებად მიიჩნია სახელმწიფოების მხრიდან ინდივიდის ეთნიკური წარმომავლობის რეგისტრაციისთვის ობიექტური მტკიცებულების მოთხოვნა. როდესაც მოთხოვნა დაფუძნებული იყო მხოლოდ სუბიექტურ და დაუსაბუთებელ გარემოებებზე, ორგანოებს შეეძლოთ უარის თქმა. თუმცა, განმცხადებლის მოთხოვნა დაფუძნებული არ იყო მხოლოდ მის სუბიექტურ ვარაუდზე; მან წარმოადგინა ობიექტურად დამადასტურებელი კავშირები რუმინულ ეთნიკურ ჯგუფებთან, როგორიცაა ენა, სახელი, გამომეტყველება და სხვა. თუმცა, შიდასახელმწიფოებრივი კანონმდებლობით, განმცხადებელს მოეთხოვებოდა წარმოედგინა მტკიცებულება მისი მშობლების რუმინულ ეთნიკურ ჯგუფთან კუთვნილების თაობაზე. მოლდოვის ისტორიული რეალობის გათვალისწინებით, ამ მოთხოვნამ წარმოშვა დაუძლეველი ბარიერი ეთნიკური წარმომავლობის დასარეგისტრირებლად და იმ ჩანაწერის შესაცვლელად, რაც მისი მშობლების შესახებ იქნა დარეგისტრირებული საბჭოთა ორგა-

184 ადამიანის უფლებათა ევროპული სასამართლო, *Rotaru v. Romania*, No. 28341/95, 4 მაისი 2000 წელი.

185 ადამიანის უფლებათა ევროპული სასამართლო, *Ciubotaru v. Moldova*, No. 27138/04, 27 ივლისი 2010 წელი, პარაგ. 51 და 59.

ნოს მიერ. მიუხედავად ობიექტური მტკიცებულების არსებობისა, განცხადების განხილვის პრევენციის გამო, სახელმწიფომ ვერ უზრუნველყო შეესრულებინა განმცხადებლისთვის პოზიტიური ვალდებულება, მისი პირადი ცხოვრების ეფექტურად დაცვისათვის. სამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

სამოქალაქო საქმისწარმოების ან სახელმწიფო ორგანოებში პროცედურების მიმდინარეობისას, რომელიც ეხება მონაცემთა სისწორის დასადგენას, მონაცემთა სუბიექტს შეუძლია მოითხოვოს შენიშვნის მითითება მისი მონაცემის ფაილზე, სადაც მიეთითება მონაცემთა სისწორის შემოწმებისა და ოფიციალური გადაწყვეტილების მომზადების პროცესის თაობაზე. ამ პერიოდის განმავლობაში, მონაცემთა დამმუშავებელმა არ უნდა წარუდგინოს მონაცემები, როგორც ზუსტი ან საბოლოო, განსაკუთრებით, მესამე მხარეებს.

მონაცემთა სუბიექტის მოთხოვნა მონაცემთა წაშლის ან განადგურების თაობაზე ხშირად ეფუძნება განცხადებას, რომლის მიხედვით მონაცემთა დამუშავებას არ გააჩნია ლეგიტიმური საფუძველი. ამგვარი მოთხოვნები ხშირად წარმოიშობა, როდესაც თანხმობა იქნა გამოთხოვნილი ან კონკრეტული მონაცემი აღარ არის საჭირო მონაცემთა შეგროვების მიზნის მისაღწევად. მტკიცების ტვირთი მონაცემთა დამუშავების ლეგიტიმურობის თაობაზე აკისრია მონაცემთა დამმუშავებელს, რამდენადაც იგი არის მონაცემთა დამუშავების კანონიერებაზე პასუხისმგებელი. ანგარიშვალდებულების პრინციპის თანახმად, დამმუშავებელმა ნებისმიერ დროს უნდა შეძლოს მკაფიო სამართლებრივი საფუძვლის არსებობის დასაბუთება მონაცემთა დამუშავებისთვის, სხვა შემთხვევაში დამუშავება შესაძლებელია იქნეს შეწყვეტილი.

თუ გასაჩივრებულია მონაცემთა დამუშავება, მონაცემთა სავარაუდო უზუსტობის ან უკანონო დამუშავების გამო, სამართლიანობის პრინციპიდან გამომდინარე, მონაცემთა სუბიექტს შეუძლია მოითხოვოს სადავო მონაცემების დაბლოკვა. ეს ნიშნავს იმას, რომ მონაცემები არ არის წაშლილი, თუმცა დამმუშავებელმა თავი უნდა შეიკავოს მონაცემთა გამოყენებისგან ბლოკირების პერიოდის განმავლობაში. ეს, ძირითადად, აუცილებელი იქნება მაშინ, როდესაც არაზუსტი ან უკანონოდ მოპოვებული მონაცემების განგრძობითმა დამუშავებამ შესაძლოა

ზიანი მიაყენოს მონაცემთა სუბიექტს. შიდასახელმწიფოებრივი კანონმდებლობა დეტალურად უნდა განაზღვრავდეს, თუ როდის შეიძლება წარმოიშვას მონაცემთა დაბლოკვის ვალდებულება და როგორ უნდა იქნეს იგი შესრულებული.

მონაცემთა სუბიექტებს, დამატებით, აქვთ უფლება მოსთხოვონ მონაცემთა დამმუშავებლებს მონაცემთა დაბლოკვის, შეცვლის ან წაშლის თაობაზე მიმართონ შეტყობინებით მესამე მხარეებს, თუ მათ მიიღეს მონაცემები დამმუშავების მოცემული მოქმედებების წარმოებამდე. რამდენადაც მესამე პირებისთვის მონაცემთა გადაცემა უნდა იქნეს დასაბუთებული მონაცემთა დამმუშავებლის მიერ, შესაძლებელი უნდა იყოს მონაცემთა მიმღებების ვინაობის დადგენა და წაშლის მოთხოვნის დაყენება. თუ, მაგალითად, მონაცემები ამ დროის განმავლობაში იქნა გამოქვეყნებული ინტერნეტით, მონაცემთა წაშლა სრულად შესაძლებელია ვერ იქნეს უზრუნველყოფილი მონაცემთა მიმღებების დაუდგენლობის გამო. მონაცემთა დაცვის დირექტივის თანახმად, მონაცემთა მიმღებებთან დაკავშირება შეცვლის, წაშლის ან დაბლოკვის თაობაზე სავალდებულოა, „გარდა იმ შემთხვევისა, თუ ეს შეუძლებელია ან მოიცავს არაპროპორციულ ძალისხმევას.“¹⁸⁶

5.1.2. გასაჩივრების უფლება

გასაჩივრების უფლება მოიცავს ცალკეული ავტომატიზებული გადანაცვეტილებების გასაჩივრების, მონაცემთა სუბიექტის კონკრეტული ვითარებიდან გამომდინარე გასაჩივრებისა და პირდაპირი მარკეტინგის მიზნებისთვის მონაცემთა შემდგომი გამოყენების გასაჩივრების უფლებას.

გასაჩივრების უფლება კონკრეტულ ავტომატიზებულ გადანაცვეტილებებზე

ავტომატიზებული გადანაცვეტილებები მიღებულია მხოლოდ პერსონალურ მონაცემთა ავტომატიზებული საშუალებებით დამმუშავებისგან. ამგვარ გადანაცვეტებს გააჩნიათ საკმაო გა-

¹⁸⁶ მონაცემთა დაცვის დირექტივა, მე-12 მუხლის -c- ქვეპუნქტის უკანასკნელი წინადადების მეორე ნახევარი.

ვლენა ინდივიდთა ცხოვრებაზე, რამდენადაც ეს შეიძლება შეეხოს, მაგალითად, გადახდისუნარიანობას, სამუშაოს წარმოებას, შესრულებას ან სანდოობას; აუცილებელია განსაკუთრებული დაცვა შეუსაბამო შედეგების თავიდან ასაცილებლად. მონაცემთა დაცვის დირექტივა ადგენს, რომ ავტომატიზებული გადაწყვეტილებები არ უნდა იძლეოდეს განმარტებებს იმ საკითხებზე, რომელიც მნიშვნელოვანია ინდივიდებისთვის და, ამასთან, მოითხოვს, რომ ინდივიდს უნდა ჰქონდეს ავტომატიზებული გადაწყვეტილების განხილვის უფლება.¹⁸⁷

მაგალითი: ავტომატიზებული გადაწყვეტილების მიღების გავრცელებული და პრაქტიკული მაგალითია საკრედიტო შეფასება. სავარაუდო მომხმარებლის გადახდისუნარიანობის შესახებ საკითხის სწრაფი გადაწყვეტისთვის, მონაცემები, როგორიცაა პროფესია და ოჯახური მდგომარეობა შეგროვებულია მომხმარებლისგან და დაკავშირებულია იმ მონაცემებთან, რომელიც ხელმისაწვდომია სუბიექტის შესახებ სხვა წყაროებიდან, როგორიცაა საკრედიტო საინფორმაციო სისტემები. ეს მონაცემები ავტომატურად გამოითვლება შეფასების ალგორითმით, რომელიც ითვლის საბოლოო ქულას პოტენციური მომხმარებლის გადახდისუნარიანობის თაობაზე. შესაბამისად, კომპანიის თანამშრომელს შეუძლია უმოკლეს ვადაში გადანაცვითს არის თუ არა მონაცემთა სუბიექტი მისაღები, როგორც მომხმარებელი.

მიუხედავად ამისა, დირექტივის თანახმად, ევროპული კავშირის წევრმა ქვეყნებმა შეიძლება დაადგინონ, რომ პირის თაობაზე მიღებულ იქნეს კონკრეტული ავტომატიზებული გადაწყვეტილება, როდესაც მონაცემთა სუბიექტის ინტერესების შესახებ სახეზე არ არის, თუ გადაწყვეტილება მიღებულ იქნა მონაცემთა სუბიექტის თხოვნით, ან, თუ დაცულია უსაფრთხოების შესაბამისი ზომებით.¹⁸⁸ ავტომატიზებულ გადაწყვეტილებებზე გასაჩივრების უფლება, ასევე, გათვალისწინებულია ევროპის საბჭოს კანონმდებლობით, რაც დადგენილია პროფილირების შესახებ რეკომენდაციით.¹⁸⁹

187 იქვე, მე-15 მუხლის პირველი პუნქტი.

188 იქვე, მე-15 მუხლის მე-2 პუნქტი.

189 რეკომენდაცია პროფილირების შესახებ, მე-5 მუხლის მე-5 პუნქტი.

გასაჩივრების უფლება მონაცემთა სუბიექტის კონკრეტული ვითარების გათვალისწინებით

მონაცემთა სუბიექტებისთვის მონაცემთა დამუშავების გასაჩივრების ერთიანი უფლება არ არსებობს.¹⁹⁰ თუმცა, მონაცემთა დაცვის დირექტივის მე-14 მუხლის -a- ქვეპუნქტი უფლებას ანიჭებს მონაცემთა სუბიექტს წარადგინოს საჩივარი, სათანადო ლეგიტიმური საფუძვლებით, რომელიც ეხება მონაცემთა სუბიექტის კონკრეტულ შემთხვევას. მსგავსი უფლება აღიარებული იქნა ევროპის საბჭოს პროფილირების შესახებ რეკომენდაციითაც.¹⁹¹ აღნიშნული დებულებები მიზნად ისახავს სწორი ბალანსის მოძიებას მონაცემთა სუბიექტის მონაცემების დაცვის ინტერესებსა და სხვათა ლეგიტიმურ ინტერესებს შორის, მონაცემთა სუბიექტის მონაცემების დამუშავებისას.

მაგალითი: ბანკი, იმ მომხმარებლების შესახებ მონაცემებს, რომლებიც ვერ იხდიან სასესხო თანხას, ინახავს შვიდი წლით. მომხმარებელი, რომლის მონაცემები არის მოცემული ამ ბაზაში, აკეთებს განაცხადს სხვა სესხზე. მონაცემთა ბაზა მოწმდება, ფინანსური მდგომარეობის შესახებ შეფასება განხორციელდა და მომხმარებელს უარი ეთქვა სესხის გაცემაზე. თუმცა, მონაცემთა სუბიექტს შეუძლია გაასაჩივროს პერსონალური მონაცემების შენახვა მონაცემთა ბაზაში და მოითხოვოს მათი წაშლა თუ იგი დაადასტურებს, რომ სესხის გადაუხდელობა დაფიქსირდა ხარვეზის საფუძველზე, რომელიც დაუყოვნებლივ შესწორდა მას შემდეგ, რაც მომხმარებელმა შეიტყო ამის თაობაზე.

წარმატებული გასაჩივრების შედეგი არის ის, რომ მონაცემები შესაძლებელია აღარ დამუშავდეს დამმუშავებლის მიერ. მონაცემთა სუბიექტის მონაცემებზე განხორციელებული დამუშავების მოქმედებები, რომელიც იქნა განხორციელებული გასაჩივრებამდე, რჩება ძალაში.

190 იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლო, *M.S. v. Sweden*, No. 20837/92, 27 აგვისტო 1997 წელი, სადაც სამედიცინო მონაცემები გადაცემულ იქნა თანხმობის ან გასაჩივრების შესაძლებლობის გარეშე; ან ადამიანის უფლებათა ევროპული სასამართლო, *Leander v. Sweden*, No. 9248/81, 26 მარტი 1987 წელი; ან ადამიანის უფლებათა ევროპული სასამართლო *Mosley v. the United Kingdom*, No. 48009/08, 10 მაისი 2011 წელი.

191 რეკომენდაცია პროფილირების შესახებ, მე-5 მუხლის მე-3 პუნქტი.

გასაჩივრების უფლება პირდაპირი მარკეტინგის მიზნებისთვის მონაცემთა შემდგომი გამოყენების თაობაზე

მონაცემთა დაცვის დირექტივის მე-14 მუხლის -b- ქვეპუნქტი ადგენს სპეციალურ უფლებას პირდაპირი მარკეტინგის მიზნებისთვის მონაცემთა გამოყენების თაობაზე. მსგავსი უფლება, ასევე, მოცემულია ევროპის საბჭოს პირდაპირი მარკეტინგის შესახებ რეკომენდაციით.¹⁹² ამგვარი საჩივარი უნდა იქნეს წარდგენილი იქამდე, სანამ მონაცემები გახდება ხელმისაწვდომი მესამე პირთათვის პირდაპირი მარკეტინგის მიზნებისთვის. თავის მხრივ, მონაცემთა სუბიექტს უნდა გააჩნდეს გასაჩივრების შესაძლებლობა მონაცემთა გადაცემამდე.

5.2. დამოუკიდებელი ზედამხედველობა

საკვანძო დებულებები

- მონაცემთა დაცვის ეფექტურობის უზრუნველსაყოფად, შიდასახელმწიფოებრივი კანონმდებლობით, უნდა შეიქმნას დამოუკიდებელი საზედამხედველო ორგანო.
- საზედამხედველო ორგანო უნდა მოქმედებდეს სრული დამოუკიდებლობით, რაც უნდა იქნეს უზრუნველყოფილი სადამფუძნებლო კანონით და ასახული საზედამხედველო ორგანოს სპეციალურ ორგანიზაციულ სტრუქტურაში.
- საზედამხედველო ორგანოს გააჩნია სპეციალური ამოცანები, მათ შორის:
 1. შიდასახელმწიფოებრივ დონეზე მონაცემთა დაცვის მონიტორინგი და ხელშეწყობა;
 2. კონსულტაციის გაწევა მონაცემთა სუბიექტებისა და დამმუშავებლებისთვის, ისევე, როგორც ხელისუფლებისა და მთლიანად საზოგადოებისთვის;

¹⁹² ევროპის საბჭო, მინისტრთა კომიტეტი (1985), რეკომენდაცია Rec(85)20 წევრი ქვეყნებისთვის პირდაპირი მარკეტინგის მიზნებისთვის გამოყენებულ პერსონალურ მონაცემთა დაცვის შესახებ, 1985 წლის 25 ოქტომბერი, მე-4 მუხლის პირველი პუნქტი.

3. საჩივრების განხილვა და მონაცემთა სუბიექტისთვის დახმარების აღმოჩენა მონაცემთა დაცვის უფლების შესაძლო დარღვევებისას;
4. დამმუშავებლებისა და უფლებამოსილი პირების ზედამხედველობა;
5. აუცილებლობისას, ჩარევის განხორციელება: 1. გაფრთხილებით, მოთხოვნის დაყენებით ან დამმუშავებლებისა და უფლებამოსილი პირების დაჯარიმებით; 2. მონაცემთა შესწორების, დაბლოკვის ან წაშლის შესახებ ბრძანების გაცემით; 3. მონაცემთა დამუშავების აკრძალვით.
6. წარადგინოს საკითხები სასამართლოში განსახილველად.

მონაცემთა დაცვის დირექტივა დამოუკიდებელ ზედამხედველობას, როგორც მექანიზმს მონაცემთა დაცვის ეფექტური უზრუნველყოფისთვის, განიხილავს სავალდებულოდ. მონაცემთა დაცვის გასაძლიერებლად დირექტივამ წარადგინა ინსტრუმენტი, რომელიც თავდაპირველად არ აისახა 108-ე კონვენციაში და არც OECD პირადი ცხოვრების სახელმძღვანელოში.

იმის გათვალისწინებით, რომ დამოუკიდებელი ზედამხედველობა აღიარებულ იქნა აუცილებლად მონაცემთა დამუშავების ეფექტური განვითარებისთვის, OECD პირადი ცხოვრების სახელმძღვანელოს 2013 წელს მიღებული, გადასინჯული ვერსია, მოუწოდებს წევრ ქვეყნებს „დააფუძნონ და აღჭურვონ პირადი ცხოვრების საზედამხედველო ორგანოები მართვის, რესურსებისა და ტექნიკური ექსპერტიზისთვის აუცილებელი ზომებით, თავიანთი უფლებამოსილების ეფექტურად შესრულებისთვის და გადაწყვეტილებების ობიექტურად, მიუკერძოებლად და შესაბამისი საფუძვლით მიღებისთვის.“¹⁹³

ევროპის საბჭოს კანონმდებლობის მიხედვით, 108-ე კონვენციის დამატებითმა ოქმმა სავალდებულოდ განსაზღვრა საზედამხედველო ორგანოების შექმნა. ამ დოკუმენტის პირველი მუხლით მოცემულია დამოუკიდებელი საზედამხედველო ორგა-

193 OECD (2013), სახელმძღვანელო პირადი ცხოვრების დაცვისა და მონაცემთა საერთაშორისო გადაცემის შესახებ, პარაგ. 19 -c- ქვეპუნქტი.

ნობის სამართლებრივი მოწესრიგება, რისი იმპლემენტირებაც შიდასახელმწიფოებრივი კანონმდებლობით უნდა მოახდინონ ხელშემკვრელმა მხარეებმა. იგი იყენებს მონაცემთა დაცვის დირექტივის მსგავს ფორმულირებას ამ ორგანოთა ფუნქციებისა და უფლებამოსილებების განსამარტად. ზოგადად, საზედამხედველო ორგანოები ევროპულ კავშირსა და ევროპის საბჭოში ერთმანეთის მსგავსად უნდა ფუნქციონირებდნენ.

ევროპული კავშირის კანონმდებლობით, პირველად საზედამხედველო ორგანოების კომპეტენცია და ორგანიზაციული სტრუქტურა მოცემულ იქნა მონაცემთა დაცვის დირექტივის 28-ე მუხლის პირველი პუნქტით. ევროპული კავშირის დანესებულებათა მონაცემთა დაცვის რეგულაცია¹⁹⁴ აყალიბებს EDPS-ს, როგორც მონაცემთა დამუშავების საზედამხედველო ორგანოს ევროპული კავშირის ორგანოებისა და დანესებულებებისთვის. როდესაც საუბარია საზედამხედველო ორგანოს დანიშნულებასა და პასუხისმგებლობაზე, რეგულაცია ყურადღებას ამახვილებს მონაცემთა დაცვის დირექტივის მიღების პერიოდიდან არსებულ გამოცდილებაზე.

მონაცემთა დაცვის საზედამხედველო ორგანოების დამოუკიდებლობა გარანტირებულია ევროპული კავშირის ფუნქციონირების შესახებ შეთანხმების მე-16 მუხლის მე-2 პუნქტით და ქარტიის მე-8 მუხლის მე-3 პუნქტით. ეს უკანასკნელი კონკრეტულად გამოყოფს დამოუკიდებელი ორგანოს კონტროლს, როგორც მონაცემთა დაცვის ძირითადი უფლების არსებით ელემენტს. დამატებით, დირექტივის შესრულების მონიტორინგისთვის, მონაცემთა დაცვის დირექტივა მოითხოვს ევროპული კავშირის წევრი ქვეყნებისგან სრული დამოუკიდებლობის მქონე საზედამხედველო ორგანოების შექმნას.¹⁹⁵ კანონი, რომელიც განსაზღვრავს საზედამხედველო ორგანოს შექმნას, ასევე, უნდა შეიცავდეს სპეციალურ დებულებებს დამოუკიდებლობის უზრუნველსაყოფად, ამასთან, ასევე, ორგანოს სპეციალური

194 ევროპული პარლამენტისა და საბჭოს 2000 წლის 18 დეკემბრის რეგულაცია (EC) No. 45/2001 გაერთიანების დანესებულებებისა და ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ, OJ 2001 L 8, 41–48 მუხლები.

195 მონაცემთა დაცვის დირექტივა, 28-ე მუხლის პირველი პუნქტის უკანასკნელი წინადადება; 108-ე კონვენცია, დამატებითი ოქმი, პირველი მუხლის მე-3 პუნქტი.

ორგანიზაციული სტრუქტურაც უნდა ახდენდეს დამოუკიდებლობის დემონსტრირებას.

2010 წელს, მართლმსაჯულების ევროპული კავშირის სასამართლოს წინაშე პირველად დაისვა საკითხი მონაცემთა დაცვის საზედამხებდველო ორგანოებისთვის მოთხოვნილი დამოუკიდებლობის ფარგლების თაობაზე.¹⁹⁶ მომდევნო მაგალითები ასახავს სასამართლოს მსჯელობას.

მაგალითი: საქმეში *Commission v. Germany*,¹⁹⁷ ევროპულმა კომისიამ სთხოვა მართლმსაჯულების ევროპული კავშირის სასამართლოს გამოეცხადებინა, რომ გერმანიამ მონაცემთა დაცვის უზრუნველყოფაზე პასუხისმგებელი ორგანოებისთვის „სრული დამოუკიდებლობის“ მოთხოვნა არ შეასრულა მართებულად და ვერ უზრუნველყო მისი ვალდებულებების შესრულება დირექტივის 28-ე მუხლით პირველი პუნქტის მიხედვით. კომისიის აზრით, სირთულეს ქმნიდა ის, რომ გერმანიამ სახელმწიფო ზედამხებდველობის ქვეშ მოაქცია საჯარო სექტორს მიღმა არებული დაწესებულებების მონაცემთა დაცვის ზედამხებდველი ორგანოების საქმიანობა, სხვადასხვა ფედერალურ ერთეულში.

ქმედების არსებითი მხარის შეფასება, სასამართლოს თანახმად, დამოკიდებული იყო მოცემულ დებულებაზე, დამოუკიდებლობის მოთხოვნის ფარგლებზე და, შესაბამისად, მის განმარტებაზე.

სასამართლომ ხაზი გაუსვა, რომ სიტყვები „სრული დამოუკიდებლობით“ დირექტივის 28-ე მუხლის პირველი პუნქტის მიხედვით, უნდა იყოს განმარტებული ამ მოცემულობის რეალური გაგებით და მონაცემთა დაცვის დირექტივის მიზნებისა და სტრუქტურის საფუძველზე.¹⁹⁸ სასამართლომ ხაზი გაუსვა, რომ საზედამხებდველო ორგანოები არიან დირექტივით განმტკიცებული პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული უფლებების დამცველები და, შესაბამისად, მათი წარმოქმნა ევროპული კავშირის წევრ ქვეყნებში მიჩნეულია „როგორც მნიშვნელოვანი კომპონენტი ინდივიდთა დაცვისათვის, პერსონალურ მონაცემთა დამუშავების მხრივ.“¹⁹⁹ სასამართლომ დაასკვნა, რომ „უფლებამოსილებათა შესრულებისას, საზედამხებდველო ორგანოები უნდა მოქმედებდნენ ობიექტურად

196 იხ. FRA (2010), ფუნდამენტური უფლებები: გამოწვევები და მიღწევები 2010 წელს, ყოველწლიური ანგარიში 2010, გვ. 59. FRA-მ განიხილა ეს საკითხი დეტალურად ანგარიშში – მონაცემთა დაცვა ევროპულ კავშირში: შიდასახელმწიფოებრივი მონაცემთა დაცვის საზედამხებდველო ორგანოების როლი – რომელიც გამოქვეყნდა 2010 წლის მაისში.

197 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-518/07, *European Commission v. Federal Republic of Germany*, 9 მარტი 2010 წელი, პარაგ. 27.

198 იქვე, პარაგ. 17 და 29.

199 იქვე, პარაგ. 23.

და მიუკერძოებლად. საამისოდ, ისინი უნდა იყვნენ თავისუფალნი ნებისმიერი გარე გავლენისგან, მათ შორის, სახელმწიფოს ან ფედერალური ერთეულის პირდაპირი ან არაპირდაპირი გავლენისგან, და არა მხოლოდ ზედამხედველი ორგანოს გავლენისგან.²⁰⁰

სასამართლომ ასევე დაადგინა, რომ „სრული დამოუკიდებლობის“ ცნება უნდა იქნეს განმარტებული EDPS-ის დამოუკიდებლობის პერსპექტივიდან გამომდინარე, რაც განსაზღვრულია ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის რეგულაციით. როგორც სასამართლოს მიერ არის ხაზგასმული, რეგულაციის 44-ე მუხლის მე-2 პუნქტი განმარტავს დამოუკიდებლობის კონცეფციას იმის დამატებით, რომ ფუნქციების შესრულებისას, EDPS-მა არ უნდა მიმართოს ან მიიღოს ინსტრუქციები რომელიმე პირისგან. ეს გამოირიცხავს სახელმწიფო ზედამხედველობას მონაცემთა დაცვის დამოუკიდებელ საზედამხედველო ორგანოზე.²⁰¹

შესაბამისად, სასამართლომ დაადგინა, რომ მონაცემთა დაცვის გერმანული დაწესებულებები ფედერალური ერთეულის დონეზე, რომლებიც იყვნენ პასუხისმგებლები კერძო დაწესებულებების მიერ პერსონალურ მონაცემთა დამუშავების მონიტორინგზე არ იყვნენ საკმარისად დამოუკიდებლები, რამდენადაც ისინი იყვნენ სახელმწიფოს ზედამხედველობის ქვეშ.

მაგალითი: საქმეზე *Commission v. Austria*,²⁰² მართლმსაჯულების ევროპული კავშირის სასამართლომ ხაზი გაუსვა მსგავს პრობლემებს, რომელიც ეხებოდა ავსტრიის მონაცემთა დაცვის ორგანიზაციის (მონაცემთა დაცვის კომისია) კონკრეტული წევრების პოზიციებსა და თანამშრომლებს. სასამართლომ დაადგინა, რომ მონაცემთა დაცვის დირექტივის განმარტებიდან გამომდინარე, ავსტრიული კანონმდებლობა გამორიცხავდა ავსტრიის მონაცემთა დაცვის ორგანოს მიერ ფუნქციების სრული დამოუკიდებლობით შესრულებას. მონაცემთა დაცვის ავსტრიული საზედამხედველო ორგანოს დამოუკიდებლობა არ იყო საკმარისად უზრუნველყოფილი, რამდენადაც სახელმწიფო კანცელარია აწვდიდა დაწესებულებას საკუთარ ადამიანურ რესურსს, აკვირდებოდა და ნებისმიერ დროს ჰქონდა უფლება ყოფილიყო ინფორმირებული მათი საქმიანობის შესახებ.

მაგალითი: საქმეზე *European Commission v. Hungary*,²⁰³ მართლმსაჯულების ევროპული კავშირის სასამართლომ აღნიშნა, რომ „თითოეულ საზედამხედველ ორგანოზე დაკისრებული უფლება-

200 იქვე, პარაგ. 25.

201 იქვე, პარაგ. 27.

202 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-614/10, *European Commission v. Republic of Austria*, 16 ოქტომბერი 2012, პარაგ. 59 და 63.

203 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-288/12, *European Commission v. Hungary*, 8 აპრილი 2014 წელი, პარაგ. 50 და 67.

მოსილების განხორციელებისას, სრული დამოუკიდებლობით მოქმედების უზრუნველყოფის მოთხოვნა მოიცავს წევრი ქვეყნების ვალდებულებას იმოქმედონ უფლებამოსილების სრული ვადით.“ სასამართლომ ასევე აღნიშნა, რომ „პერსონალურ მონაცემთა დაცვის საზედამხებველო ორგანოს უფლებამოსილების ვადის ნაადრევით შეწყვეტით, უნგრეთმა ვერ უზრუნველყო 95/46/EC დირექტივით გათვალისწინებული ვალდებულებების შესრულება.“

შიდასახელმწიფოებრივი კანონმდებლობით საზედამხებველო ორგანოებს მინიჭებული აქვთ გარკვეული უფლებამოსილებები, მათ შორის:²⁰⁴

- დამმუშავებლებისა და უფლებამოსილი პირებისთვის მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე კონსულტაციის გაწევა;
- დამმუშავების მოქმედებების გამოკვლევა და შესაბამისი ჩარევის განხორციელება;
- დამმუშავებელთა გაფრთხილება, მოთხოვნით მიმართვა;
- მონაცემთა შეცვლის, დაბლოკვის, წაშლის ან განადგურების მოთხოვნა;
- დამმუშავებაზე დროებითი ან სამუდამო აკრძალვის დაწესება;
- სასამართლოსთვის მიმართვა.

საკუთარი ფუნქციების განხორციელებისთვის, საზედამხებველო ორგანოს უნდა ჰქონდეს წვდომის უფლება ნებისმიერ პერსონალურ მონაცემებსა და ინფორმაციაზე, რომელიც აუცილებელია გამოძიებისთვის, ასევე, უნდა შეეძლოს შევიდეს ნებისმიერ დაწესებულებაში, სადაც დამმუშავებელი ინახავს შესაბამის ინფორმაციას.

არსებობს საგრძნობი განსხვავება შიდასახელმწიფოებრივ მონესრიგებას შორის, რომელიც ეხება პროცედურებს და ზედამხებველი ორგანოს მიერ განსაზღვრული რეაგირების სასამართლებრივ ეფექტს შორის. ისინი შესაძლებელია იცვლებოდეს ომბუცმენის ტიპის რეკომენდაციებიდან – დაუყოვნებლივ აღსასრულებელ გადაწყვეტილებებამდე. შესაბამისად, როდეს-

204 მონაცემთა დაცვის დირექტივა, 28-ე მუხლი; იხ. ასევე, 108-ე კონვენცია, დამატებითი ოქმი, პირველი მუხლი.

აც ხდება კონკრეტული იურისდიქციის ფარგლებში სამართლებრივი დაცვის ეფექტურობის ანალიზი, მოცემული სამართლებრივი დაცვის ინსტრუმენტები უნდა იქნეს განხილული კონკრეტულ კონტექსტში.

5.3. სამართლებრივი დაცვა და სანქციები

საკვანძო დებულებები

- 108-ე კონვენციის და მონაცემთა დაცვის დირექტივის მიხედვით, შიდასახელმწიფოებრივი კანონმდებლობა უნდა განსაზღვრავდეს სამართლებრივი დაცვის შესაბამის საშუალებებს და აცალიბებდეს სანქციებს მონაცემთა დაცვის უფლების დარღვევებისთვის.
- უფლება ეფექტური სამართლებრივი დაცვის საშუალებაზე, ევროპული კავშირის კანონმდებლობით, მოითხოვს, რომ განისაზღვროს სამართლებრივი დაცვის მექანიზმები მონაცემთა დაცვის უფლებათა დარღვევისთვის, საზედამხედველო ორგანოსთვის მიმართვის შესაძლებლობის მიუხედავად.
- სანქციები უნდა იქნეს დადგენილი შიდასახელმწიფოებრივი კანონმდებლობით, რომელიც უნდა იყოს ეფექტური, ექვივალენტური, პროპორციული და ქმედითი.
- სასამართლოსთვის მიმართვამდე, პირმა ჯერ უნდა მიმართოს დამმუშავებელს. იქნება თუ არა სასამართლოსთვის მიმართვამდე საზედამხედველო ორგანოსთვის მიმართვა სავალდებულო, განსასაზღვრია შიდასახელმწიფოებრივი კანონმდებლობით.
- მონაცემთა სუბიექტებს, კონკრეტული პირობების გათვალისწინებით, შეუძლიათ მონაცემთა დაცვის კანონის დარღვევის გამო, როგორც დაცვის უკანასკნელ საშუალებას, მიმართონ ადამიანის უფლებათა ევროპულ სასამართლოს.
- დამატებით, მართლმსაჯულების ევროპული კავშირის სასამართლო, ასევე, ხელმისაწვდომია მონაცემთა სუბიექტებისთვის, თუმცა მხოლოდ ძალზედ შეზღუდულ შემთხვევებში.

მონაცემთა დაცვის კანონმდებლობით დადგენილი უფლებები შესაძლებელია რეალიზებულ იქნეს მხოლოდ იმ პირის მიერ, ვის უფლებებსაც ეხება საქმე; ეს იქნება პირი, რომელიც, სულ მცირე, აცხადებს, რომ არის მონაცემთა სუბიექტი. აღნიშნული პირები, თავიანთი უფლებების რეალიზაციისას, შესაძლებელია წარმოდგენილ იქნენ წარმომადგენლების მიერ, რომლებიც, შიდასახელმწიფოებრივი კანონმდებლობის მიხედვით, აკმაყოფილებენ აუცილებელ მოთხოვნებს. არასრულწლოვნები უნდა იქნენ წარმოდგენილნი მათი მშობლების ან მეურვეების მიერ. საზედამხედველო ორგანოში პირი, ასევე, შესაძლოა წარმოდგენილ იქნეს გაერთიანების მიერ, რომლის კანონიერ მიზანს წარმოადგენს მონაცემთა დაცვის უფლებების მხარდაჭერა.

5.3.1. დამმუშავებლის წინაშე დაყენებული მოთხოვნები

3.2.1 პარაგრაფში მოცემული უფლებები, უპირველესად, რეალიზებულ უდნა იქნეს უშუალოდ დამმუშავებლის წინაშე. პირდაპირ საზედამხედველო ორგანოსთვის ან სასამართლოსთვის მიმართვა არ იქნება შედეგის მომტანი, რამდენადაც საზედამხედველო ორგანო რჩევას მისცემს, პირველ რიგში, დამმუშავებელთან დაკავშირების თაობაზე, ხოლო სასამართლო სარჩელს დაუშვებლად ცნობს. დამმუშავებელთან სამართლებრივი მიმართვის ფორმალური მოთხოვნები უნდა დარეგულირდეს შიდასახელმწიფოებრივი კანონმდებლობით, კერძოდ, უნდა დადგინდეს იყოს თუ არა მოთხოვნა წერილობითი.

პირმა, რომელსაც მიმართეს როგორც დამმუშავებელს, უნდა მოახდინოს მოთხოვნაზე რეაგირება, იმ შემთხვევაშიც კი, თუ იგი არ არის დამმუშავებელი. პასუხი, ნებისმიერ შემთხვევაში, უნდა იქნეს მიწოდებული მონაცემთა სუბიექტისთვის იმ ვადაში, რაც დადგენილია შიდასახელმწიფოებრივი კანონით, მაშინაც, თუ მომთხოვნის შესახებ არანაირი მონაცემი არ მუშავდება. მონაცემთა დაცვის დირექტივის მე-12 მუხლის -a- ქვეპუნქტის და 108-ე კონვენციის მე-8 მუხლის -b- ქვეპუნქტის თანახმად, მოთხოვნაზე რეაგირება უნდა განხორციელდეს „გადამეტებული დაყოვნების გარეშე.“ შესაბამისად, შიდასახელმწიფოებრივმა კანონმდებლობამ უნდა განსაზღვროს პასუხის ის ვადა, რომე-

ლიც საკმაოდ მოკლეა, თუმცა დამმუშავებელს აძლევს რეაგირების ადეკვატურად განხორციელების საშუალებას.

პასუხის გაცემამდე, პირმა, რომელსაც მიმართეს როგორც დამმუშავებელს, უნდა დაადგინოს მომთხოვნის ვინაობა, რათა განხორციელოს იდენტიფიცირება, კონფიდენციალურობის მნიშვნელოვანი დარღვევის თავიდან ასაცილებლად. თუ ვინაობის დადგენის წესები არ არის სპეციალურად დარეგულირებული შიდასახელმწიფოებრივი კანონმდებლობით, გადანაცვლებები უნდა იქნეს მიღებული დამმუშავებლის მიერ. შესაბამისად, სამართლიანი დამმუშავების პრინციპი, მოითხოვს, რომ დამმუშავებლებმა არ განსაზღვრონ არაპროპორციული ტვირთის მატარებელი პირობები ვინაობის (და, ასევე მოთხოვნის ნამდვილობის, რაც განხილულია 2.1.1. პარაგრაფში) დადგენისთვის.

შიდასახელმწიფოებრივი კანონმდებლობა, ასევე, უნდა არეგულირებდეს საკითხს, თუ რამდენად შეუძლიათ დამმუშავებლებს, პასუხის გაცემამდე, მოსთხოვონ განმცხადებელს მოსაკრებლის გადახდა: ღირექტივის მე-12 მუხლის -a- ქვეპუნქტი და 108-ე კონვენციის მე-8 მუხლის -b- ქვეპუნქტი ადგენს, რომ მოთხოვნაზე გამომხაურება უნდა განხორციელდეს „გადაამტებული დანახარჯების გარეშე.“ ბევრი ევროპული ქვეყნის კანონმდებლობა ადგენს, რომ მონაცემთა დაცვის კანონმდებლობის საფუძველზე განხორციელებული მიმართვა უფასოდ უნდა იქნეს რეაგირებული, თუ გამომხაურება არ წარმოშობს გადამეტებულ ან დიდ ძალისხმევას; თავის მხრივ, დამმუშავებლები, ძირითადად, დაცულნი არიან შიდასახელმწიფოებრივი კანონმდებლობით მოთხოვნაზე გამომხაურების განხორციელების უფლების ბოროტად გამოყენების წინააღმდეგ.

თუ პირმა, დანესებულებამ ან ორგანომ, რომელსაც მიმართეს როგორც დამმუშავებელს, არ უარყოფს დამმუშავებლად არსებობის ფაქტს, ამ პირს, ეროვნული კანონით განსაზღვრულ ვადაში, შეუძლია:

- დაეთანხმოს მოთხოვნას და შეატყობინოს მომთხოვნს თუ როგორ ხდება მოთხოვნის შესრულება; ან
- მოახდინოს მომთხოვნის ინფორმირება, თუ რატომ ვერ იქნება მისი მოთხოვნა შესრულებული.

5.3.2. საზედამხედველო ორგანოში შეტანილი მოთხოვნები

თუ პირი, რომელსაც დამმუშავებელთან შეტანილი აქვს მოთხოვნა ან საჩივარი, არ მიიღებს დროულ და დამაკმაყოფილებელ პასუხს, მას შეუძლია მიმართოს მონაცემთა დაცვის შიდასახელმწიფოებრივ საზედამხედველო ორგანოს დახმარებისთვის. საზედამხედველო ორგანოში წარმოებისას, უნდა დადგინდეს თუ რამდენად, პირს, დაწესებულებას ან ორგანოს, რომელსაც მიმართა მომთხოვნმა, გააჩნდა რეაგირების ვალდებულება და რამდენად იყო აღნიშნული რეაგირება სწორი და სათანადო. განმცხადებელი უნდა იყოს ინფორმირებული საზედამხედველო ორგანოს მიერ საჩივართან დაკავშირებული წარმოების შედეგების შესახებ.²⁰⁵ საზედამხედველო ორგანოში არსებული წარმოებიდან გამომდინარე შედეგის სამართლებრივი ეფექტი დამოკიდებულია შიდასახელმწიფოებრივ კანონმდებლობაზე: საზედამხედველო ორგანოს გადაწყვეტილებები შესაძლებელია იქნეს სამართლებრივად აღსრულებული, რაც ნიშნავს, რომ იგი უნდა აღასრულოს უფლებამოსილმა დაწესებულებამ ან, შესაძლებელია, აუცილებელი იყოს სასამართლოსთვის მიმართვა დამმუშავებლის მიერ საზედამხედველო ორგანოს გადაწყვეტილებით (მოსაზრებით, მოთხოვნით, ა.შ) დადგენილი მოთხოვნის შეუსრულებლობის გამო.

იმ შემთხვევაში თუ მონაცემთა დაცვის უფლებები, უზრუნველყოფილი ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულების მე-16 მუხლით, დაირღვა ევროპული კავშირის დაწესებულებებისა და ორგანოების მიერ, მონაცემთა სუბიექტს შეუძლია საჩივრის შეტანა EDPS-ში²⁰⁶ - ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის რეგულაციით დადგენილ მონაცემთა დაცვის დამოუკიდებელ საზედამხედველო ორგანოში. ექვსი თვის განმავლობაში EDPS-ისგან გამოხმაურების მიუღებლობის შემთხვევაში, საჩივარი მიიჩნევა უარყოფილად.

²⁰⁵ მონაცემთა დაცვის დირექტივა, 28-ე მუხლის მე-4 პუნქტი.

²⁰⁶ ევროპული პარლამენტისა და საბჭოს 2000 წლის 18 დეკემბრის რეგულაცია (EC) No. 45/2001 გაერთიანების დაწესებულებებისა და ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისა ფიზიკურ პირთა დაცვის შესახებ, OJ 2001 L 8.

ეროვნული საზედამხედველო ორგანოს გადაწყვეტილებების წინააღმდეგ უნდა იყოს გათვალისწინებული სასამართლოსთვის მიმართვის შესაძლებლობა. ეს ეხება, როგორც მონაცემთა სუბიექტებს ისე დამმუშავებლებს, რომლებიც იყვნენ მხარეები საზედამხედველო ორგანოში საქმის განხილვისას.

მაგალითი: 2013 წლის 24 ივლისს გაერთიანებული სამეფოს ინფორმაციის კომისარმა გამოსცა გადაწყვეტილება, რითაც მიმართავდა ჰერტფორდშირის პოლიციას შეეწყვიტა სანომრე ნიშნის მიდევნების სისტემის გამოყენება, მისი უკანონობის გამო. კამერების მიერ შეგროვებული მონაცემები შენახული იყო ადგილობრივი პოლიციის განყოფილების მონაცემთა ბაზაში და ცენტრალიზებულ ბაზაში. სანომრე ნიშნის ფოტოსურათები ინახებოდა ორი წლის მანძილზე, ხოლო ავტომანქანის ფოტოსურათები – 90 დღის განმავლობაში. დადგენილ იქნა, რომ კამერებისა და თვალთვალის სხვა ფორმების მსგავსი გრძელვადიანი გამოყენება არ იყო პროპორციული მოცემული პრობლემის გადასაჭრელად.

5.3.3. სასამართლოში შეტანილი სარჩელი

მონაცემთა დაცვის დირექტივის თანახმად, თუ პირი, რომელმაც მონაცემთა დაცვის კანონმდებლობის შესაბამისად, დააყენა მოთხოვნა დამმუშავებლის წინაშე, არ მიიჩნევს სათანადოდ დამმუშავებლის გამომხაურებას, მას უნდა შეეძლოს მიმართოს სასამართლოს.²⁰⁷

არის თუ არა სავალდებულო სასამართლომდე საზედამხედველო ორგანოსთვის მიმართვა, განსასაზღვრია შიდასახელმწიფოებრივი კანონმდებლობით. ბევრ შემთხვევაში, პირის მონაცემთა დაცვის უფლებების რეალიზაციისთვის ხელსაყრელი იქნება უპირველესად საზედამხედველო ორგანოსთვის მიმართვა, რამდენადაც მათ მოთხოვნებთან დაკავშირებული საქმის განხილვა იქნება უფასო და არ იქნება ბიუროკრატიული. დასკვნა, რომელიც მოცემული იქნება საზედამხედველო ორგანოს გადაწყვეტილებით (მოსაზრება, მოთხოვნა და ა.შ.) შესაძლოა დაეხმაროს მონაცემთა სუბიექტს მისი უფლებების დაცვის უზრუნველყოფაში სასამართლოს წინაშე.

²⁰⁷ მონაცემთა დაცვის დირექტივა, 22-ე მუხლი.

ევროპის საბჭოს კანონმდებლობით, მონაცემთა დაცვის უფლების დარღვევები, განხორციელებული შიდასახელმწიფოებრივ დონეზე, ადამიანის უფლებათა ევროპული კონვენციის ხელშემკვრელი მხარის მიერ, რაც, იმავდროულად, წარმოშობს კონვენციის მე-8 მუხლის დარღვევას, შესაძლებელია გასაჩივრდეს ადამიანის უფლებათა ევროპულ სასამართლოში ყველა ხელმისაწვდომი შიდასახელმწიფოებრივი საშუალებების ამონურვის შემდეგ. კონვენციის მე-8 მუხლის დარღვევის თაობაზე შეტანილი საჩივარი, ასევე, უნდა აკმაყოფილებდეს დასაშვებობის სხვა კრიტერიუმებსაც (კონვენციის 34-37 მუხლები).²⁰⁸

მიუხედავად იმისა, რომ საჩივრები სასამართლოში შესაძლებელია მიმართულ იქნეს მხოლოდ ხელშემკვრელი სახელმწიფოს მიმართ, ის, ასევე, შესაძლებელია არაპირდაპირ ეხებოდეს კერძო პირთა ქმედებებს, თუ ხელშემკვრელმა მხარემ, კონვენციის თანახმად, ვერ შეასრულა მისი პოზიტიური ვალდებულება და არ უზრუნველყო შიდასახელმწიფოებრივი კანონმდებლობით საკმარისი დაცვა მონაცემთა დაცვის უფლებაში ჩარევის წინააღმდეგ.

მაგალითი: საქმეზე *K.U. v. Finland*,²⁰⁹ არასრულწლოვანმა განმცხადებელმა აღნიშნა, რომ მის შესახებ ინტერნეტ-პაემნების გვერდზე იქნა განთავსებული სექსუალური ხასიათის რეკლამა. ფინეთის კანონმდებლობით, კონფიდენციალურობის მოთხოვნებიდან გამომდინარე პირის ვინაობა, რომელმაც გამოაქვეყნა ინფორმაცია, არ იყო გამოვლენილი სერვის-პროვაიდერის მიერ. განმცხადებელი აღნიშნავდა, რომ ფინური კანონმდებლობა არ ადგენდა დაცვის საკმარის მექანიზმებს იმ ქმედებების წინააღმდეგ, როდესაც კერძო პირი ათავსებდა ინტერნეტში მამხილებელ მონაცემებს განმცხადებლის შესახებ. ადამიანის უფლებათა ევროპულმა სასამართლომ განაცხადა, რომ სახელმწიფოები არა მხოლოდ ვალდებული იყვნენ თავი შეეკავებინათ ინდივიდის პირად ცხოვრებაში ჩარევისგან, არამედ, ასევე, გააჩნდათ პოზიტიური ვალდებულება, რაც მოიცავს „პირადი ცხოვრების პატივისცემის დასაცავად ზომების მიღებას ინდივიდთა შორის არსებულ ურთიერთობათა სფეროშიც კი.“ განმცხადებლის შემთხვევაში, მისი ქმედითი და ეფექტური დაცვა მოითხოვდა, რომ დამრღვევის ვინაობის დადგენისთვის და პასუხისმგებლობაში მის-

208 ადამიანის უფლებათა ევროპული კონვენცია, 34–37 მუხლები, ხელმისაწვდომია: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 ადამიანის უფლებათა ევროპული სასამართლო, *K.U. v. Finland*, No. 2872/02, 2 დეკემბერი 2008 წელი.

აცემად მიღებული ყოფილიყო ეფექტური ზომები. თუმცა, ამგვარი ზომა არ იყო განსაზღვრული სახელმწიფოს მიერ და სასამართლომ დაასკვნა, რომ სახეზე იყო კონვენციის მე-8 მუხლის დარღვევა.

მაგალითი: საქმეზე *Köpke v. Germany*,²¹⁰ განმცხადებელი ექვმიტანილი იქნა ქურდობაში თავის სამუშაო ადგილზე და, შესაბამისად, დაექვემდებარა ფარულ ვიდეოთვალთვალს. ადამიანის უფლებათა ევროპულმა სასამართლომ დაასკვნა, რომ „ვერ დადგინდა ადგილობრივი ორგანოების მიერ დაცვის სამართლიანი ბალანსის დარღვევა, არსებული დისკრეციის გათვალისწინებით, მე-8 მუხლით დადგენილი განმცხადებლის პირადი ცხოვრების უფლების პატივისცემას, მისი დამსაქმებლის საკუთრების დაცვის უფლების ინტერესსა და, ასევე, სამართლიანობის სწორი ადმინისტრირების საჯარო ინტერესს შორის.“ შესაბამისად, სარჩელი იქნა დაუშვებლად ცნობილი.

თუ ადამიანის უფლებათა ევროპული სასამართლო დაადგენს, რომ წევრმა სახელმწიფომ დაარღვია კონვენციით დაცული რომელიმე უფლება, წევრი სახელმწიფო ვალდებულია აღასრულოს სასამართლოს გადაწყვეტილება. აღსრულების ზომებით, პირველ რიგში, უნდა შეწყდეს უფლების დარღვევა და განისაზღვროს სამართლებრივი დაცვა, შესაძლებლობის ფარგლებში, განმცხადებლის ნეგატიური შედეგების მიმართ. გადანაცვებილებათა აღსრულება შესაძლოა, ასევე, მოითხოვდეს ზოგადი ზომების გატარებას იმ დარღვევათა პრევენციისთვის, რომელიც მსგავსია სასამართლოს მიერ დადგენილის, კანონმდებლობის ცვლილების მეშვეობით, სასამართლო პრაქტიკით ან სხვა ზომებით.

თუ სასამართლო დაადგენს კონვენციის დარღვევას, მისი 41-ე მუხლი განსაზღვრავს, რომ განმცხადებელს შესაძლოა აუზნალაურდეს ზიანი წევრი სახელმწიფოს ხარჯზე.

ევროპული კავშირის სამართლით,²¹¹ შიდასახელმწიფოებრივი მონაცემთა დაცვის კანონმდებლობის მიხედვით, რომელიც

210 ადამიანის უფლებათა ევროპული სასამართლო, *Köpke v. Germany* (dec.), No. 420/07, 5 ოქტომბერი 2010 წელი.

211 ევროპული კავშირი (2007), ლისაბონის ხელშეკრულება, რომელიც ცვლის ევროპული კავშირის შესახებ ხელშეკრულებას და ევროპული გაერთიანების შესახებ ხელშეკრულებას, ხელმოწერილი ლისაბონში, 2007 წლის 13 დეკემბერს, OJ 2007 C 306. იხ. ასევე, ევროპული კავშირის ხელშეკრულების OJ 2012 C 326 და ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულების კონსოლიდირებული ვერსია, OJ 2012 C 326.

ახორციელებს ევროპული კავშირის მონაცემთა დაცვის ნორმების იმპლემენტირებას, დაზარალებულ პირებს შეუძლიათ, ზოგიერთ შემთხვევაში, წარადგინონ თავიანთი საჩივრები მართლმსაჯულების ევროპული კავშირის სასამართლოში. არსებობს ორი შესაძლო გზა, თუ როგორ შეუძლია მონაცემთა სუბიექტს მიმართოს მართლმსაჯულების ევროპული კავშირის სასამართლოს, მისი მონაცემთა დაცვის უფლების დარღვევს თაობაზე.

პირველი ვარიანტის თანახმად, მონაცემთა სუბიექტი უნდა იყოს ევროპული კავშირის იმ ადმინისტრაციული ან მომწესრიგებელი აქტის გამო დაზარალებული, რომელიც არღვევს ინდივიდის უფლებას მონაცემთა დაცვაზე. ევროპული კავშირის ფუნქციონირების შესახებ შეთანხმების 263-ე მუხლის მე-4 ნაწილის თანახმად:

„ნებისმიერ ფიზიკურ ან იურიდიულ პირს შეუძლია წამოიწყოს პროცესი აქტის წინააღმდეგ, რომელიც ეხება უშუალოდ პიროვნებას ან აქვს პირდაპირი და კონკრეტული გავლენა მასზე, და, ასევე, მომწესრიგებელი აქტის წინააღმდეგ, რომელიც უშუალოდ ეხება მას და არ განსაზღვრავს იმპლემენტირების ზომებს.“

შესაბამისად, ევროპული კავშირის დანესებულებების მიერ მონაცემთა უკანონოდ დამუშავებით დაზარალებულებს შეუძლიათ პირდაპირ მიმართონ მართლმსაჯულების ევროპული კავშირის სასამართლოს მთავარ სასამართლოს, რომელიც უფლებამოსილია გამოიტანოს გადაწყვეტილებები ევროპული კავშირის დანესებულებათა მონაცემთა დაცვის რეგულაციის დებულებებთან მიმართებით. მართლმსაჯულების ევროპული კავშირის სასამართლოსთვის პირდაპირ მიმართვის შესაძლებლობა არსებობს, ასევე, იმ შემთხვევაში თუ ევროპული კავშირის სამართლებრივი ნორმა კონკრეტულ გავლენას ახდენს პირის სამართლებრივ მდგომარეობაზე.

მეორე ვარიანტი ეხება მართლმსაჯულების ევროპული კავშირის სასამართლოს კომპეტენციას გამოიტანოს წინასწარი გადაწყვეტილება ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულების 267-ე მუხლის თანახმად.

მონაცემთა სუბიექტებს, შიდასახელმწიფოებრივი სა-

ქმისწარმოების მიმდინარეობისას, შეუძლიათ მიმართონ ეროვნულ სასამართლოს მოთხოვნით - მიიღონ განმარტებები მართლმსაჯულების სასამართლოსგან ევროპული კავშირის ხელშეკრულებების ინტერპრეტაციის და ევროპული კავშირის დანესებულებების, ორგანოების, სამსახურებისა და სააგენტოების ქმედებათა ინტერპრეტაციისა და კანონიერების შესახებ. ამგვარი დასკვნები, ცნობილია როგორც წინასწარი გადაწყვეტილებები. ეს არ არის სამართლებრივი დაცვის პირდაპირი საშუალება განმცხადებლისთვის, თუმცა საშუალებას აძლევს შიდასახელმწიფოებრივ სასამართლოებს დარწმუნდნენ ევროპული კავშირის კანონმდებლობის სწორ ინტერპრეტაციაში.

თუ შიდასახელმწიფოებრივ სასამართლოებში საქმისწარმოებისას მხარე მოითხოვს მართლმსაჯულების ევროპული კავშირის სასამართლოს დასკვნას საკითხზე, მხოლოდ ის სასამართლოები, რომლებიც არიან საბოლოო ინსტანციის და რომელთა შემდგომ აღარ არსებობს სამართლებრივი დაცვის საშუალებები, არიან ვალდებული შეასრულონ მოთხოვნა.

მაგალითი: საქმეზე *Kärntner Landesregierung and Others*,²¹² ავსტრიის საკონსტიტუციო სასამართლომ შეკითხვით მიმართა მართლმსაჯულების ევროპული კავშირის სასამართლოს, რომელიც ეხებოდა 2006/24/EC დირექტივის (მონაცემთა შენახვის დირექტივა) მე-3 და მე-9 მუხლების შესაბამისობას ქარტიის მე-7, მე-9 და მე-11 მუხლებთან და იყო თუ არა ტელეკომუნიკაციების შესახებ ავსტრიის ფედერალური კანონის კონკრეტული დებულებები, რომელიც ახდენდა მონაცემთა შენახვის დირექტივის იმპლემენტირებას, მონაცემთა დაცვის დირექტივასთან და ევროპული კავშირის დანესებულებათა მონაცემთა დაცვის რეგულაციასთან შესაბამისი.

სეიტლინგერმა, საკონსტიტუციო სასამართლოს განხილვაში მონაწილე ერთ-ერთმა განმცხადებელმა, აღნიშნა, რომ იგი იყენებს ტელეფონს, ინტერნეტსა და ელ-ფოსტას, როგორც სამუშაო მიზნებისთვის, ისე პირადი მიზნებისთვის. შესაბამისად, ინფორმაცია, რომელსაც იგი აგზავნის და იღებს ხორციელდება საჯარო სატელეკომუნიკაციო ქსელის მეშვეობით. ავსტრიის 2003 წლის ტელეკომუნიკაციების შესახებ აქტის მიხედვით, სატელეკომუნიკაციო პროვაიდერი სამართლებრივად ვალდებულია შეაგროვოს და შეინ-

212 მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები C-293/12 და C-594/12, *Digital Rights Ireland and Seitling and Others*, 8 აპრილი 2014 წელი.

ახოს მონაცემები მის მიერ ქსელის გამოყენების თაობაზე. სეიტლინგერმა დაასკვნა, რომ მისი პერსონალური მონაცემების ამგავრი შეგროვება და შენახვა არ იყო აუცილებელი ტექნიკური მიზნებისთვის ქსელში ინფორმაციის „ა“ პუნქტიდან „ბ“ პუნქტში გადაგზავნისთვის. არც ამ მონაცემთა შეგროვება და შენახვა წარმოადგენდა ირიბ აუცილებლობას ანგარიშსწორების მიზნებისთვის. სეიტლინგერს აშკარად არ განუცხადებია თანხმობა მისი პერსონალური მონაცემების გამოყენების შესახებ. აღნიშნული დამატებითი მონაცემების შეგროვებისა და შენახვის ერთადერთი მიზეზი იყო ავსტრიის 2003 წლის ტელეკომუნიკაციების შესახებ აქტი.

შესაბამისად სეიტლინგერმა, ავსტრიის საკონსტიტუციო სასამართლოში წამოიწყო პროცესი, სადაც განაცხადა, რომ მისი სატელეკომუნიკაციო პროვაიდერისთვის დადგენილი საკანონმდებლო მოთხოვნები არღვევდა ქარტიის მე-8 მუხლით დადგენილ მის ძირითად უფლებებს.

მართლმსაჯულების ევროპული კავშირის სასამართლოს გამოაქვს დასკვნები მხოლოდ წინასწარი გადანყვეტილების თაობაზე მიმართვით მოთხოვნილი კონკრეტული საკითხების შესახებ. შიდასახელმწიფოებრივი სასამართლო ინარჩუნებს კომპეტენციას დაწყებულ განხილვაზე გამოიტანოს გადანყვეტილება.

ძირითადად, სასამართლომ უნდა გასცეს პასუხი მის წინაშე დასმულ საკითხს. მას არ შეუძლია უარი განაცხადოს წინასწარი გადანყვეტილების გამოტანაზე იმ მიზეზით, რომ ეს მოთხოვნა არ არის საქმესთან დაკავშირებული ან ხანდაზმულია კონკრეტული საქმიდან გამომდინარე. თუმცა, მას შეუძლია უარი განაცხადოს განხილვაზე თუ შეკითხვა სცდება მისი კომპეტენციის ფარგლებს.

საბოლოოდ, თუ მონაცემთა დაცვის უფლებები, აღიარებული ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულებით, დარღვეულია ევროპული კავშირის დაწესებულებების ან ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებისას, მონაცემთა სუბიექტმა შესაძლებელია მიმართოს მართლმსაჯულების ევროპული კავშირის სასამართლოს მთავარ სასამართლოს (ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის რეგულაციის 32-ე მუხლის პირველი და მე-4 პუნქტები). იგივე წესი ვრცელდება EDPS-ის გადანყვეტილებებზე, რომელიც

ინვეს ამგვარ დარღვევებს (ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის დირექტივის 32-ე მუხლის მე-3 პუნქტი).

მართლმსაჯულების ევროპული კავშირის სასამართლოს მთავარი სასამართლო უფლებამოსილია გამოიტანოს გადაწყვეტილებები ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის რეგულაციის ფარგლებში, მაგრამ თუ პირს სურს ისარგებლოს სამართლებრივი დაცვის საშუალებებით ევროპული კავშირის დაწესებულების ან მისი ორგანოს მომსახურეთაგან, მან უნდა მიმართოს ევროპული კავშირის სამოქალაქო სამსახურის ტრიბუნალს.

მაგალითი: საქმე The European Commission v. The Bavarian Lager Co. Ltd,²¹³ ახდენს სამართლებრივი დაცვის იმ საშუალებების ილუსტრირებას, რაც დაკავშირებულია ევროპული კავშირის დაწესებულებებისა და ორგანოების ქმედებებისა და გადაწყვეტილებების წინააღმდეგ, მონაცემთა დაცვის კუთხით.

Bavarian Lager-მა ევროპულ კომისიას მიმართა განცხადებით კომისიის მიერ გამართული შეხვედრების ჩანაწერებზე წვდომის მინიჭების შესახებ, კომპანიის საკითხებთან შესაძლო კავშირის მქონე სამართლებრივი საკითხების არსებობის გამო. კომისიამ უარყო კომპანიის მოთხოვნა წვდომის თაობაზე მონაცემთა დაცვის აღმატებული ინტერესის გამო.²¹⁴ ამ გადაწყვეტილების საწინააღმდეგოდ, კომპანიამ ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის რეგულაციის 32-ე მუხლზე დაყრდნობით, შეიტანა საჩივარი მართლმსაჯულების ევროპული კავშირის სასამართლოში; უფრო ზუსტად, მის პირველ ინსტანციაში (მთავარი სასამართლოს წინამორბედი). თავის გადაწყვეტილებაში T-194/04, Bavarian Lager v. Commission, პირველი ინსტანციის სასამართლომ გააუქმა კომისიის გადაწყვეტილება წვდომის მოთხოვნაზე უარის შესახებ. ევროკომისიამ გაასაჩივრა ეს გადაწყვეტილება მთავარ სასამართლოში. მთავარმა სასამართლომ (დიდმა პალატამ) გამოიტანა გადაწყვეტილება, რომლითაც გააუქმა პირველი ინსტანციის სასამართლოს გადაწყვეტილება და დაადსტურა ევროპული კომისიის მოთხოვნის უარყოფის მართლზომიერება.

213 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-28/08 P, European Commission v. The Bavarian Lager Co. Ltd, 29 ივნისი 2010 წელი.

214 მსჯელობის ანალიზისთვის, იხ. EDPS (2011), პერსონალური მონაცემების შემცველ დოკუმენტებთან საჯარო წვდომა Bavarian Lager-ის გადაწყვეტილების შემდეგ, ბრიუსელი EDPS, ხელმისაწვდომია: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

5.3.4. სანქციები

ევროპის საბჭოს კანონმდებლობის მიხედვით, 108-ე კონვენციის მე-10 მუხლი ადგენს, რომ ყოველი ხელშემკვრელი მხარის მიერ წესების დარღვევისთვის შიდასახელმწიფოებრივი კანონმდებლობით უნდა იქნეს მიღებული შესაბამისი სანქციები და დაცვის საშუალებები, რომელიც თანხვედრაშია 108-ე კონვენციით მოცემულ მონაცემთა დაცვის მთავარ პრინციპებთან.²¹⁵ ევროპული კავშირის კანონმდებლობით, მონაცემთა დაცვის დირექტივის 24-ე მუხლი ადგენს, რომ წევრმა ქვეყნებმა „უნდა მიიღონ შესაბამისი ზომები, რათა უზრუნველყოფილ იქნეს ამ დირექტივის დებულებათა სრული იმპლემენტაცია და უნდა განისაზღვროს სანქციები, რომელთა დაკისრება ხდება დადგენილ დებულებათა დარღვევის შემთხვევაში.“

ორივე ინსტრუმენტი ანიჭებს წევრ ქვეყანას ფართო დისკრეციას შესაბამისი სანქციებისა და სამართლებრივი დაცვის საშუალებათა არჩევისთვის. არც ერთი სამართლებრივი ინსტრუმენტი არ მიუთითებს შესაბამისი სანქციების სახეობის ან ბუნების შესახებ და არც მის მაგალითებს განსაზღვრავს.

თუმცა:

„მიუხედავად იმისა, რომ ევროპული კავშირის წევრი ქვეყნები სარგებლობენ ფართო დისკრეციით ევროპული კავშირის კანონმდებლობიდან გამომდინარე ინდივიდების უფლებათა დასაცავად გათვალისწინებული ზომების არჩევაში, ევროპული კავშირის შესახებ ხელშეკრულების მე-4 მუხლის მე-3 პუნქტით დადგენილი ლოიალური თანამშრომლობის პრინციპის თანახმად, ეფექტურობის, ექვივალენტურობის, პროპორციულობისა და ქმედითობის მინიმალური მოთხოვნები უნდა იყოს დაცული.“²¹⁶

მართლმსაჯულების ევროპული კავშირის სასამართლომ არაერთხელ აღნიშნა, რომ შიდასახელმწიფოებრივი სამართალი სანქციების განსაზღვრაში არ არის სრულიად თავისუფალი.

215 ადამიანის უფლებათა ევროპული სასამართლო, I. v. Finland, No. 20511/03, 17 ივლისი 2008 წელი; ადამიანის უფლებათა ევროპული სასამართლო, K.U. v. Finland, No. 2872/02, 2 დეკემბერი 2008 წელი.

216 FRA (2012), ევროპული კავშირის ძირითადი უფლებების სააგენტოს მოსაზრება მონაცემთა დაცვის ინიცირებული რეფორმის პაკეტის შესახებ, 2/2012, ვენა, 1 ოქტომბერი 2012 წელი, გვ. 27.

მაგალითი: საქმეზე Von Colson and Kamann v. Land Nordrhein-Westfalen,²¹⁷ მართლმსაჯულების ევროპული კავშირის სასამართლომ აღნიშნა, რომ ევროპული კავშირის ყველა წევრი ქვეყანა, რომელზეც ვრცელდება დირექტივა, ვალდებულია შიდასახელმწიფოებრივი კანონმდებლობით მიიღოს ყველა აუცილებელი ზომა, რათა იგი სრულად ეფექტური იყოს დადგენილი მიზნიდან გამომდინარე. სასამართლოს აზრით, მიუხედავად იმისა, რომ დირექტივის იმპლმენტირების უზრუნველსაყოფად გზებისა და საშუალებების არჩევა წევრ ქვეყნებზეა დამოკიდებული, ეს თავისუფლება არ ცვლის მათზე დაკისრებულ ვალდებულებებს. კერძოდ, ეფექტური სამართლებრივი დაცვის მექანიზმი უნდა აძლევდეს ინდივიდს საშუალებას იმოქმედოს და მოახდინოს უფლების სრული რეალიზაცია. ამგვარი არსებითი და ეფექტური დაცვის მისაღწევად, სამართლებრივი დაცვის საშუალებები უნდა განსაზღვრავდეს საჯარიმო ან/და კომპენსაციის პროცედურებს, რაც ადგენს შემაკავებელი ეფექტის მქონე სანქციებს.

ევროპული კავშირის დანესებულებების ან ორგანოების მიერ ევროპული კავშირის სამართლის დარღვევისთვის გათვალისწინებული სანქციების მხრივ, ევროპული კავშირის დანესებულებათა მონაცემთა დაცვის რეგულაციის სპეციალური მონესრიგების გათვალისწინებით, სანქციები დადგენილია მხოლოდ დისციპლინური ზომების სახით. რეგულაციის 49-ე მუხლის თანახმად, „იმ ვალდებულებების ნებისმიერი შეუსრულებლობა, რაც დადგენილია რეგულაციით, პირის განზრახვით ან გაუფრთხილებლობით, თანამდებობის პირს ან ევროპული გაერთიანების სხვა მოსამსახურეს გახდის დისციპლინარული ღონისძიებებისადმი დაქვემდებარებულს.“

217 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-14/83, Sabine von Kolson and Elisabeth Kamann v. Land Nordrhein-Westfalen, 10 აპრილი 1984 წელი.

6. მონაცემთა საერთაშორისო გადაცემა

ევროპული კავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა საერთაშორისო გადაცემა		
მონაცემთა დაცვის დირექტივა, 25-ე მუხლის პირველი პუნქტი მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, Bodil Lindqvist, 6 ნოემბერი 2003 წელი	ცნება	108-ე კონვენცია, დამატებითი ოქმი, მე-2 მუხლის პირველი პუნქტი
მონაცემთა თავისუფალი გადაადგილება		
მონაცემთა დაცვის დირექტივა, პირველი მუხლის მე-2 პუნქტი	ევროპული კავშირის წევრ ქვეყნებს შორის	
	108-ე კონვენციის ხელმომწერ მხარეებს შორის	108-ე კონვენცია, მე-12 მუხლის მე-2 პუნქტი
მონაცემთა დაცვის დირექტივა, 25-ე მუხლი	მონაცემთა დაცვის ადეკვატური დონის მქონე მესამე ქვეყნებში	108-ე კონვენცია, დამატებითი ოქმი, მე-2 მუხლის პირველი პუნქტი
მონაცემთა დაცვის დირექტივა, 26-ე მუხლის პირველი პუნქტი	მესამე ქვეყნებში კონკრეტული შემთხვევების გათვალისწინებით	108-ე კონვენცია, დამატებითი ოქმი, მე-2 მუხლის მე-2 პუნქტის -a- ქვეპუნქტი
მონაცემთა შეზღუდული გადაადგილება მესამე ქვეყნებში		
მონაცემთა დაცვის დირექტივა, 26-ე მუხლის მე-2 პუნქტი მონაცემთა დაცვის დირექტივა, 26-ე მუხლის მე-4 პუნქტი	სახელშეკრულებო პირობები	108-ე კონვენცია, დამატებითი ოქმი, მე-2 მუხლის მე-2 პუნქტის -b- ქვეპუნქტი სახელშეკრულებო პირობების მომზადების სახელმძღვანელო
მონაცემთა დაცვის დირექტივა, 26-ე მუხლის მე-2 პუნქტი	სავალდებულო საკორპორაციო წესები	
მაგალითები: EU-US PNR შეთანხმება EU-US SWIFT შეთანხმება	სპეციალური საერთაშორისო შეთანხმებები	

მონაცემთა დაცვის დირექტივა წევრ ქვეყნებს შორის არა მარტო ადგენს მონაცემთა თავისუფალი გადაადგილების შესაძლებლობას, არამედ, ასევე, შეიცავს დებულებებს პერსონალურ მონაცემთა გადაცემისთვის მესამე ქვეყნებში, ევროპული კავშირის გარეთ. ევროპის საბჭომ, ასევე, აღიარა მონაცემთა მესამე ქვეყნებისთვის საერთაშორისო გადაცემის წესების იმპლემენტირების აუცილებლობა და 2001 წელს მიიღო 108-ე კონვენციის დამატებითი ოქმი. აღნიშნულმა ოქმმა გაითავისა კონვენციის წევრი სახელმწიფოებისგან და ევროპული კავშირის წევრი ქვეყნებისგან მთავარი მარეგულირებელი წესები მონაცემთა საერთაშორისო გადაცემის თაობაზე.

6.1. მონაცემთა საერთაშორისო გადაცემის არსი

საკვანძო დებულება

- მონაცემთა საერთაშორისო გადაცემა არის პერსონალურ მონაცემთა გადაცემა მიმღებისთვის, რომელიც ექვემდებარება სხვა ქვეყნის კანონმდებლობას.

108-ე კონვენციის დამატებითი ოქმის მე-2 მუხლის პირველი პუნქტი მონაცემთა საერთაშორისო გადაცემას განმარტავს, როგორც პერსონალურ მონაცემთა გადაცემას იმ მიმღებისთვის, რომელიც ექვემდებარება უცხო ქვეყნის კანონმდებლობას. მონაცემთა დაცვის დირექტივის 25-ე მუხლის პირველი პუნქტი არეგულირებს „დამუშავების პროცესში არსებულ ან გადაცემის შემდეგ დამუშავებისთვის გამიზნულ პერსონალურ მონაცემთა გადაცემას მესამე ქვეყნისთვის.“ მონაცემთა ამგვარი გადაცემა ნებადართულია მხოლოდ 108-ე კონვენციის დამატებითი ოქმის მე-2 მუხლით დადგენილი წესების თანახმად, ხოლო ევროპული კავშირის ქვეყნებისთვის, ასევე, მონაცემთა დაცვის დირექტივის 25-ე და 26-ე მუხლებით გათვალისწინებულ შემთხვევებში.

მაგალითი: საქმეზე Bodil Lindqvist,²¹⁸ მართლმსაჯულების ევროპული კავშირის სასამართლომ აღნიშნა, რომ „ვებ-გვერდის მეშვეობით სხვადასხვა პირებისთვის მიმართვა და მათი იდენტიფიცირება

218 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-101/01, Bodil Lindqvist, 6 ნოემბერი 2003 წელი, პარაგ. 27, 68 და 69.

სახელით ან სხვა საშუალებით, მაგალითად, მათი ტელეფონის ნომრის ან მათი საშუალო პირობების ან ჰობის შესახებ ინფორმაციით, წარმოადგენს პერსონალურ მონაცემთა დამუშავებას სრულად ან ნაწილობრივ ავტომატური საშუალებებით 95/46 დირექტივის მესამე მუხლის პირველი ნაწილის თანახმად.“

შემდეგ სასამართლომ აღნიშნა, რომ დირექტივა ადგენს სპეციალურ ნებსებას, რომელიც წევრ ქვეყნებს უფლებას აძლევს მონიტორინგი გაუწიონ მესამე ქვეყნებისთვის მონაცემთა გადაცემას.

თუმცა, პირველ რიგში, დირექტივის შედგენის დროს ინტერნეტის განვითარების დონის გათვალისწინებით, და, ასევე, იქიდან გამომდინარე, რომ ინტერნეტის გამოყენებაზე მოქმედი კრიტერიუმი არ არის მოცემული დირექტივით, „ნაკლებად სავარაუდოა, რომ ცნების - „მონაცემთა გადაცემა მესამე ქვეყნისთვის“ - ქვეშ გაერთიანების კანონმდებლობამ განიზრახა მოეცვა მონაცემთა ჩატვირთვა ინტერნეტ გვერდზე, იმ შემთხვევაშიც კი, თუ მონაცემები ხელმისაწვდომია პირებისთვის მესამე ქვეყნებში, წვდომის ტექნიკური საშუალებების გამოყენებით.“

წინააღმდეგ შემთხვევაში, თუ დირექტივა იქნებოდა „განმარტებული, იმგვარად, რომ მონაცემთა გადაცემა მესამე ქვეყნისთვის სახეზე იქნებოდა ყველა შემთხვევაში, როდესაც პერსონალური მონაცემები არის ჩატვირთული ვებ-გვერდზე, მოქმედება აუცილებლად ჩაითვლებოდა გადაცემად ყველა იმ მესამე ქვეყანაში, სადაც არსებობს ტექნიკური საშუალებები ინტერნეტთან წვდომისთვის. დირექტივის მიერ დადგენილი სპეციალური რეჟიმი, შესაბამისად, მოგვევლინებოდა, როგორც ინტერნეტ-ოპერაციებთან დაკავშირებული ზოგადი რეგულირების წესი. აქედან გამომდინარე, თუ კომისია დაადგენდა, რომ ერთ-ერთი მესამე ქვეყანა მაინც არ აკმაყოფილებს ადეკვატურ დაცვის დონეს, წევრი ქვეყნები იქნებოდნენ ვალდებული არ განეთავსებინათ რაიმე სახის პერსონალური მონაცემები ინტერნეტში.“

პრინციპი, რომლის თანახმად, პერსონალურ მონაცემთა მხოლოდ გამოქვეყნება არ არის მიჩნეული მონაცემთა საერთაშორისო გადაცემად ვრცელდება, ასევე, საჯარო ონლაინ-რეესტრებზე ან მასობრივი მედიის საშუალებებზე, როგორიცაა ელექტრონული გაზეთები და ტელევიზია. მხოლოდ იმგვარი გადაცემა, რომელიც მიმართულია კონკრეტულ მიმღებებზე, თავსებადია მონაცემთა საერთაშორისო გადაცემის კონცეფციასთან.

6.2. მონაცემთა თავისუფალი გადაადგილება ევროპული კავშირის წევრ ქვეყნებს ან 108-ე კონვენციის ხელმომწერ მხარეებს შორის

საკვანძო დებულება

- პერსონალურ მონაცემთა გადაცემა ევროპული ეკონომიკური ზონის წევრი ქვეყნისთვის ან 108-ე კონვენციის ხელმომწერ ქვეყნებს შორის თავისუფალი უნდა იყოს შეზღუდვებისგან.

ევროპის საბჭოს კანონმდებლობით, კერძოდ, 108-ე კონვენციის მე-12 მუხლის მე-2 პუნქტით, შესაძლებელი უნდა იყოს პერსონალურ მონაცემთა თავისუფალი გადაადგილება კონვენციის ხელმომწერ მხარეებს შორის. შიდასახელმწიფოებრივი კანონმდებლობა არ უნდა კრძალავდეს პერსონალურ მონაცემთა ექსპორტს ხელშემკრელ სახელმწიფოსთან, გარდა იმ შემთხვევისა თუ:

- ეს საჭიროა მონაცემთა განსაკუთრებული ბუნებიდან გამომდინარე;²¹⁹ ან
- შეზღუდვა აუცილებელია, რათა თავიდან იქნეს აცილებული ადგილობრივი კანონმდებლობის გვერდის ავლა მონაცემთა საერთაშორისო გადაცემის თაობაზე მესამე ქვეყნებში.²²⁰

ევროპული კავშირის კანონმდებლობით, შეზღუდვები ან აკრძალვები წევრ ქვეყნებს შორის მონაცემთა თავისუფალ გადაადგილებაზე, მონაცემთა დაცვის მიზნებიდან გამომდინარე, აკრძალულია მონაცემთა დაცვის დირექტივის პირველი მუხლის მეორე პუნქტით. მონაცემთა თავისუფალი გადაადგილების ფარგლები ევროპული ეკონომიკური ზონის შეთანხმების²²¹ თანახმად გაფართოვდა და შიდა ბაზრის ფარგლებში მოიცავს ისლანდიას, ლიხტენშტაინსა და ნორვეგიას.

219 108-ე კონვენცია, მე-12 მუხლის მე-3 პუნქტის -a- ქვეპუნქტი.

220 იქვე, მე-12 მუხლის მე-3 პუნქტის -b- ქვეპუნქტი.

221 საბჭოსა და კომისიის 1993 წლის 13 დეკემბრის გადამწყვეტილება ევროპული ეკონომიკური ზონის შესახებ ევროპულ გაერთიანებას, მათ წევრ ქვეყნებსა და ავსტრიის რესპუბლიკას, ფინეთის რესპუბლიკას, ისლანდიის რესპუბლიკას, ლიხტენშტაინის სამეფოს, ნორვეგიის გაერთიანებულ სამეფოს, შვედეთის სამეფოსა და შვეიცარიის კონფედერაციას შორის, OJ 1994 L 1.

მაგალითი: თუ საერთაშორისო კომპანიათა ჯგუფის წევრი, დაფუძნებული ევროპული კავშირის სხვადასხვა წევრ ქვეყანაში, მათ შორის სლოვენიასა და საფრანგეთში, აგზავნის პერსონალურ მონაცემებს სლოვენდიიდან საფრანგეთში, მონაცემთა ამგვარი გადაცემა არ უნდა იქნეს შეზღუდული ან აკრძალული სლოვენიის კანონმდებლობით.

თუ იგივე სლოვენიური კომპანია მოინდომებს გადასცეს იგივე პერსონალური მონაცემები სათავო კომპანიას აშშ-ში, სლოვენიურმა მონაცემთა გამამცემმა უნდა გაითვალისწინოს სლოვენიური კანონმდებლობით დადგენილი წესები მონაცემთა საერთაშორისო გადაცემისთვის იმ ქვეყნებში, რომლებსაც არ გააჩნიათ მონაცემთა დაცვის ადეკვატური დონე, გარდა იმ შემთხვევისა თუ სათავო კომპანია არ შეუერთდა Safe Harbor-ის პირადი ცხოვრების პრინციპებს – ქვეყნის ნებაყოფლობით კოდექსს, რომელიც ადგენს მონაცემთა დაცვის ადეკვატურ დონეს (იხ. პარაგრაფი 6.3.1).

ევროპული ეკონომიკური ზონის წევრ ქვეყნებთან მონაცემთა საერთაშორისო გადაცემა შიდა ბაზრის მიღმა არსებული მიზნებისთვის, როგორიცაა დანაშაულთა გამოძიება, არ ექვემდებარება მონაცემთა დაცვის დირექტივის დებულებებს და, შესაბამისად, არ ექვემდებარება მონაცემთა თავისუფალი გადაადგილების პრინციპს. რაც შეეხება ევროპის საბჭოს კანონმდებლობას, 108-ე კონვენციისა და მისი დამატებითი ოქმის ფარგლებში მოქცეულია ყველა სფერო, მიუხედავად ამისა, გამონაკლისები შესაძლებელია დადგენილ იქნეს ხელმომწერი მხარეების მიერ. ევროპული ეკონომიკური ზონის ყველა წევრი ქვეყანა, ასევე, არის 108-ე კონვენციის ხელმომწერი მხარე.

6.3. მონაცემთა თავისუფალი გადაადგილება მესამე ქვეყნებში

საკვანძო დებულებები

- მონაცემთა გადაცემა მესამე ქვეყნებითვის თავისუფალი უნდა იყოს შეზღუდვებისგან მონაცემთა დაცვის შიდასახელმწიფოებრივი კანონმდებლობით, თუ:
 1. მიმღებთან დასტურდება მონაცემთა დაცვის ადეკვატურობა; ან

2. ეს აუცილებელია მონაცემთა სუბიექტის განსაზღვრული ინტერესებისთვის ან სხვათა აღმატებული ლეგიტიმური მიზნებისთვის, განსაკუთრებით, მნიშვნელოვანი საჯარო ინტერესისთვის.
- მესამე ქვეყანაში მონაცემთა დაცვის ადეკვატურობა ნიშნავს, რომ მონაცემთა დაცვის მთავარი პრინციპები ეფექტურად იქნა იმპლემენტირებული ქვეყნის ეროვნულ კანონმდებლობაში.
- ევროპული კავშირის კანონმდებლობის თანახმად, მესამე ქვეყნებში მონაცემთა დაცვის ადეკვატურობა დგინდება ევროპული კომისიის მიერ. ევროპის საბჭოს კანონმდებლობით, მონაცემთა დაცვის ადეკვატურობის განსაზღვრა ნებადართულია შიდასახელმწიფოებრივი კანონმდებლობებისთვის.

6.3.1. მონაცემთა თავისუფალი გადაადგილება ადეკვატური დაცვის არსებობის საფუძველზე

ევროპის საბჭოს კანონმდებლობა ნებას რთავს შიდასახელმწიფოებრივ კანონმდებლობას დაადგინოს მონაცემთა თავისუფალი გადაადგილება არანეგრ სახელმწიფოებში, თუ მიმღები სახელმწიფო ან ორგანიზაცია უზრუნველყოფს დაცვის ადეკვატურ დონეს მონაცემთა დაგეგმილი გადაცემისთვის.²²² შიდასახელმწიფოებრივი კანონმდებლობა ნყვეტს თუ როგორ იქნება მონაცემთა დაცვის დონე შეფასებული უცხო ქვეყანაში და თუ ვინ უნდა შეაფასოს იგი.

ევროპული კავშირის კანონმდებლობით, მონაცემთა ადეკვატური დაცვის მქონე მესამე ქვეყნებში მონაცემთა თავისუფალი გადაადგილება დადგენილია მონაცემთა დაცვის დირექტივის 25-ე მუხლის პირველი პუნქტით. ადეკვატურობის მოთხოვნა, განსხვავებით ექვივალენტურობისგან, ქმნის შესაძლებლობას მოხდეს მონაცემთა დაცვის იმპლემენტირების სხვადასხვა გზების დადგენა. დირექტივის 25-ე მუხლის მე-6 პუნქტის მიხედვით, ევროპული კომისია კომპეტენტურია შეაფასოს მონაცემთა დაცვის დონე უცხო ქვეყნებში ადეკვატურობის შეფასებით და ამ

²²² 108-ე კონვენცია, დამატებითი ოქმი, მე-2 მუხლის პირველი პუნქტი.

მიზნით მიმართავს მუხლი 29 სამუშაო ჯგუფს, რომელმაც არსებითი წვლილი შეიტანა 25-ე და 26-ე მუხლების განმარტებაში.²²³

ევროპული კომისიის მიერ ადეკვატურობის დადგენას გააჩნია სავალდებულო ხასიათი. თუ ევროპული კომისია ევროპული კავშირის ოფიციალურ ჟურნალში გამოაქვეყნებს კონკრეტულ ქვეყანაში ადეკვატურობის დადგენას, ევროპული ეკონომიკური ზონის ყველა წევრი ქვეყანა და სხვა ორგანოები ვალდებული არიან დაემორჩილონ გადაწყვეტილებას, რაც ნიშნავს იმას, რომ ამ ქვეყანაში მონაცემები შეიძლება გადაიცეს შიდასახელმწიფოებრივი ორგანოების მიერ ლიცენზირების პროცესის ან შემონმების გარეშე.²²⁴

ევროპული კომისია, ასევე, უფლებამოსილია შეაფასოს, როგორც ქვეყნის სამართლებრივი სისტემის ნაწილი, ისე, შემოიფარგლოს მხოლოდ კონკრეტული საკითხებით. მაგალითად, კომისიამ დაადგინა ადეკვატურობა მხოლოდ კანადის კერძო კომერციულ კანონმდებლობაზე დაყრდნობით.²²⁵ არსებობს კიდევ რამოდენიმე ადეკვატურობის დადგენა ტრანსფერებისთვის, რომელიც დაფუძნებულია ევროპულ კავშირსა და უცხო სახელმწიფოებს შორის არსებულ შეთანხმებებზე. ეს გადაწყვეტილებები ეხება მონაცემთა გადაცემის კონკრეტულ სახეს, როგორიცაა ავიახაზების მიერ მგზავრთა სახელების ჩანაწერების გადაცემა საზღვარგარეთის სასაზღვრო კონტროლის ზედამხედველებისთვის, როდესაც ავიახაზები დაფრინავს ევროპული კავშირიდან კონკრეტული მიმართულებით (იხ. პარაგრაფი 6.4.3). მონაცემთა გადაცემის უკანასკნელი შემთხვევები, რომელიც

223 იხ. მაგალითად, მუხლი 29 სამუშაო ჯგუფი (2003), სამუშაო დოკუმენტი პერსონალურ მონაცემთა მესამე ქვეყნებში გადაცემის შესახებ: ევროპული კავშირის მონაცემთა დაცვის დირექტივის 26-ე მუხლის მოქმედება სავალდებულო საკორპორაციო წესებზე მონაცემთა საერთაშორისო გადაცემისთვის, WP 74, ბრიუსელი, 3 ივნისი 2003 წელი; და მუხლი 29 სამუშაო ჯგუფი (2005), სამუშაო დოკუმენტი 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივის 26-ე მუხლის პირველი პუნქტის ერთგვაროვანი განმარტების შესახებ, WP 114, ბრიუსელი, 25 ნოემბერი 2005 წელი.

224 იმ ქვეყნების განახლებადი სიის სანახავად, სადაც დადგენილია ადეკვატური დონე, იხ. ევროპული კომისიის, მართლმსაჯულების გენერალური დირექტორატის ვებ-გვერდი, ხელმისაწვდომია: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 ევროპული კომისია (2002), 2001 წლის 20 დეკემბრის გადაწყვეტილება 2002/2/EC ევროპული პარლამენტისა და საბჭოს 95/46/EC დირექტივის შესაბამისად კანადის პერსონალური ინფორმაციისა და ელექტრონული დოკუმენტების აქტის მიხედვით პერსონალურ მონაცემთა ადეკვატური დაცვის შესახებ, OJ 2002 L 2.

დაფუძნებულია სპეციალურ შეთანხმებებზე ევროპულ კავშირსა და მესამე ქვეყნებს შორის ხორციელდება ადეკვატურობის დადგენის საჭიროების გარეშე, იმის გათვალისწინებით, რომ თავად შეთანხმება განსაზღვრავს მონაცემთა დაცვის ადეკვატურ დონეს.²²⁶

ადეკვატურობის დადგენის ერთ-ერთი ყველაზე მნიშვნელოვანი გადანყვეტილება არ უკავშირდება მრავალ სამართლებრივ დებულებათა ერთობლიობას,²²⁷ პირიქით, იგი მოიცავს წესებს, რომელიც მეტად მსგავსია ქვეყნის კოდექსის, ცნობილი როგორც Safe Harbor პირადი ცხოვრების პრინციპები. ეს პრინციპები შემუშავებულ იქნა ევროპულ კავშირსა და აშშ-ს შორის აშშ-ის კომერციული კომპანიებისთვის. Safe Harbor-ის წევრობა მიიღწევა ნებაყოფლობითი დეკლარირებით აშშ-ის სავაჭრო დეპარტამენტში და ასახულია დოკუმენტში, რომელსაც აქვეყნებს დეპარტამენტი. რამდენადაც ადეკვატურობის ერთ-ერთი მნიშვნელოვანი ელემენტია მონაცემთა დაცვის იმპლემენტირების ეფექტურობა, Safe Harbor შეთანხმება, ასევე, ადგენს სახელმწიფო ზედამხედველობის განსაზღვრულ დონეს: მხოლოდ იმ კომპანიებს შეუძლიათ შეუერთდნენ Safe Harbor-ს, რომლებიც იმყოფებიან აშშ-ის ფედერალური სავაჭრო კომისიის ზედამხედველობის ქვეშ.

6.3.2. მონაცემთა თავისუფალი გადაადგილება კონკრეტულ შემთხვევებში

ევროპის საბჭოს კანონმდებლობით, 108-ე კონვენციის დამატებითი ოქმის მე-2 მუხლის მეორე პუნქტი დასაშვებად მიიჩნე-

226 მაგ. შეთანხმება ამერიკის შეერთებულ შტატებსა და ევროპულ კავშირს შორის მგზავრთა სახელების ჩანაწერების ამერიკის შეერთებული შტატების სახელმწიფო უსაფრთხოების დეპარტამენტისთვის გადაცემის შესახებ (OJ 2012 L 215, გვ. 5–14) ან ევროპულ კავშირსა და ამერიკის შეერთებულ შტატებს შორის შეთანხმება ტერორიზმის დაფინანსების გამოვლენის პროგრამის მიზნებისთვის ევროპული კავშირიდან ამერიკის შეერთებულ შტატებში ფინანსური გზავნილების მონაცემთა დამუშავებისა და ტრანსფერის თაობაზე, OJ 2010 L 8, გვ. 11–16.

227 ევროპული კომისია (2000), კომისიის 2000 წლის 26 ივლისის გადანყვეტილება 2000/520/EC ევროპული პარლამენტისა და საბჭოს 95/46/EC დირექტივის შესაბამისად Safe Harbor პირადი ცხოვრების პრინციპებით დადგენილი დაცვის ადეკვატურობისა და აშშ-ის სავაჭრო დეპარტამენტის მიერ გამოცემულ ხშირად დასმული შეკითხვების თაობაზე, OJ 2000 L 215.

ნებს პერსონალურ მონაცემთა გადაცემას იმ მესამე ქვეყნებში, სადაც არ არსებობს მონაცემთა ადეკვატური დაცვის დონე, თუ გადაცემა დადგენილია შიდასახელმწიფოებრივი კანონმდებლობით და აუცილებელია:

- მონაცემთა სუბიექტის კონკრეტული ინტერესების გათვალისწინებით; ან
- სხვათა აღმატებული ინტერესების საფუძველზე, განსაკუთრებით მნიშვნელოვანი საჯარო ინტერესის მიზნებისთვის.

ევროპული კავშირის კანონმდებლობის მიხედვით, მონაცემთა დაცვის დირექტივის 26-ე მუხლის პირველი პუნქტი შეიცავს დებულებას, რომელიც მსგავსია 108-ე კონვენციის დამატებით ოქმში არსებულთან.

დირექტივის თანახმად, მონაცემთა სუბიექტის ინტერესებს შეუძლია მართლზომიერი გახადოს მონაცემთა თავისუფალი გადაადგილება მესამე ქვეყანაში, თუ:

- მონაცემთა სუბიექტმა განაცხადა აშკარა თანხმობა მონაცემთა გადაცემის შესახებ; ან
- მონაცემთა სუბიექტმა დაამყარა ან ემზადება დაამყაროს სახელშეკრულებო ურთიერთობა, რომელიც აშკარად მოითხოვს მონაცემთა გადაცემას საზღვარგარეთ მიმღებისთვის; ან
- მონაცემთა დამმუშავებელსა და მესამე პირს შორის ხელშეკრულება შედგა მონაცემთა სუბიექტის ინტერესების სასარგებლოდ; ან
- გადაცემა აუცილებელია მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად.
- ხორციელდება საჯარო რეესტრიდან მონაცემთა გადაცემა; იგი არის მაგალითი აღმატებული საზოგადოებრივი ინტერესის, რათა შესაძლებელი იყოს საჯარო რეესტრში მოცემულ ინფორმაციაზე წვდომა.

სხვათა ლეგიტიმური ინტერესები შესაძლებელია მართლზომიერს ხდიდეს მონაცემთა საერთაშორისო გადაცემას.²²⁸

- მნიშვნელოვანი საჯარო ინტერესის გამო, გარდა ეროვნული უსაფრთხოების ან საზოგადოებრივი უსაფრ-

228 მონაცემთა დაცვის დირექტივა, 26-ე მუხლის პირველი პუნქტის -d- ქვეპუნქტი.

თხოვბის ინტერესებისა, რამდენადაც მათ არ მოიცავს მონაცემთა დაცვის დირექტივა; ან

- სამართლებრივი მოთხოვნების წარდგენის, რეალიზების ან დაცვისათვის.

ზემოხსენებული შემთხვევები უნდა იქნეს გაგებული, როგორც არსებული გამონაკლისები იმ წესიდან, რომლის თანახმად სხვა ქვეყნებში მონაცემთა თავისუფალი გადაცემა მოითხოვს მონაცემთა დაცვის ადეკვატური დონის არსებობას ადრესატ სახელმწიფოში. გამონაკლისები ყოველთვის უნდა იქნეს განმარტებული ვიწროდ. აღნიშნული მრავალჯერ იქნა ხაზგასმული მუხლი 29 სამუშაო ჯგუფის მიერ მონაცემთა დაცვის დირექტივის 26-ე მუხლის პირველი პუნქტის კონტექსტში, ძირითადად მაშინ, როდესაც მონაცემთა გადაცემის საფუძველი არის თანხმობა.²²⁹ მუხლი 29 სამუშაო ჯგუფმა დაასკვნა, რომ თანხმობის სამართლებრივ მნიშვნელობასთან დაკავშირებული ძირითადი წესები, ასევე, ვრცელდება დირექტივის 26-ე მუხლის პირველ პუნქტზე. თუ შრომითი ურთიერთობის კონტექსტში ნათელი არ არის დასაქმებულების მიერ გაცემული თანხმობის ნებაყოფლობითი ხასიათი, მონაცემთა გადაცემა ვერ დაეყრდნობა დირექტივის 26-ე მუხლის პირველი პუნქტის -a- ქვეპუნქტს. ასეთ შემთხვევებში, გამოიყენება 26-ე მუხლის მე-2 პუნქტი, რომელიც ითხოვს შიდასახელმწიფოებრივი მონაცემთა დაცვის საზედამხედველო ორგანოებისგან ლიცენზიის გაცემას მონაცემთა გადაცემისთვის.

6.4. მონაცემთა გადაცემის შეზღუდვა მესამე ქვეყნებში

საკვანძო დებულებები

- მონაცემთა მესამე ქვეყნებში გადაცემამდე, სადაც არ ხდება მონაცემთა დაცვის ადეკვატური დონის უზრუნველყოფა, მონაცემთა დამმუშავებელმა საზედამხედველო ორგანოში განსახილველად უნდა წარადგინოს მონა-

²²⁹ ძირითადად, იხ. მუხლი 29 სამუშაო ჯგუფი (2005), სამუშაო დოკუმენტი 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივის 26-ე მუხლის პირველი პუნქტის ერთგვაროვანი განმარტების შესახებ, WP 114, ბრიუსელი, 25 ნოემბერი 2005 წელი.

ცემთა დაგეგმილი გადაცემის საკითხი.

- დამმუშავებელი, რომელსაც სურს მონაცემთა ექსპორტი, უნდა ასაბუთებდეს ორ საკითხს ამ განხილვის დროს:
 1. არსებობს მონაცემთა გადაცემის სამართლებრივი საფუძველი მიმღებისთვის; და
 2. მიღებულია ზომები მონაცემთა მიმღებთან მონაცემთა ადეკვატური დაცვის უზრუნველსაყოფად.
- მიმღებთან მონაცემთა დაცვის ადეკვატურობის დამდგენი ზომები შესაძლებელია მოიცავდეს:
 1. მონაცემთა ექსპორტიორ დამმუშავებელსა და მონაცემთა მიმღებს შორის სახელშეკრულებო დებულებების განსაზღვრას; ან
 2. სავალდებულო საკორპორაციო წესებს, რომელიც ძირითადად მოქმედებს მონაცემთა გადაცემაზე საერთაშორისო კომპანიის ჯგუფის ფარგლებში.
- მონაცემთა გადაცემა საზღვარგარეთის სახელმწიფო ორგანოებისთვის შესაძლებელია დარეგულირდეს სპეციალური საერთაშორისო შეთანხმებითაც.

მონაცემთა დაცვის დირექტივა და 108-ე კონვენციის დამატებითი ოქმი ნებას რთავს შიდასახელმწიფოებრივ კანონმდებლობას განსაზღვროს წესები მონაცემთა საერთაშორისო გადაცემისთვის იმ მესაქმე ქვეყნებთან, რომლებიც არ უზრუნველყოფენ მონაცემთა დაცვის ადეკვატურ დონეს, იმ შემთხვევაში თუ დამმუშავებელს მიღებული აქვს სპეციალური შეთანხმება მიმღებთან მონაცემთა დაცვის ადეკვატური უსაფრთხოების უზრუნველსაყოფად და თუ დამმუშავებელს შეუძლია აღნიშნულის დასაბუთება კომპეტენტური ორგანოსთვის. ეს მოთხოვნა მკაფიოდ არის დადგენილი მხოლოდ 108-ე კონვენციის დამატებითი ოქმით, თუმცა, მიჩნეულია, როგორც სტანდარტული პროცედურა მონაცემთა დაცვის დირექტივის თანახმად.

6.4.1. სახელშეკრულებო პირობები

როგორც ევროპის საბჭოს, ისე ევროპული კავშირის კანონმდებლობა მოიხსენიებს სახელშეკრულებო პირობებს მონაცემთა ექსპორტიორ დამმუშავებელსა და მიმღებს შორის მესამე

ქვეყანაში, როგორც მონაცემთა მიმღებთან მონაცემთა დაცვის შესაბამისი დონის განსაზღვრის საშუალებად.

ევროპული კავშირის ფარგლებში, ევროპულმა კომისიამ მუხლი 29 სამუშაო ჯგუფის დახმარებით შეიმუშავა სტანდარტული სახელშეკრულებო პირობები, რომელიც ოფიციალურად სერტიფიცირებულ იქნა კომისიის გადანყვეტილებით, როგორც მონაცემთა დაცვის ადეკვატურობის დადასტურების საშუალება.²³⁰ რამდენადაც კომისიის გადანყვეტილებები სრულად სავალდებულოა მის ნეერ ქვეყნებში, შიდასახელმწიფოებრივმა ორგანოებმა, რომლებიც ახორციელებენ მონაცემთა საერთაშორისო გადაცემის ზედამხედველობას, უნდა აღიარონ მოცემული სტანდარტული სახელშეკრულებო პირობები მათ პროცედურებში.²³¹ შესაბამისად, თუ მონაცემთა ექსპორტიორი დამმუშავებელი და მიმღები მესამე ქვეყანა დათანხმდებიან და მოაწერენ ხელს ამ პირობებს, აღნიშნული უნდა იყოს საკმარისი მტკიცებულება ზედამხედველი ორგანოსთვის, ადეკვატური დაცვის ზომების გათვალისწინებულის მხრივ.

ევროპული კავშირის სამართლებრივ სისტემაში სტანდარტული სახელშეკრულებო პირობების არსებობა არ უკრძალავს დამმუშავებლებს მოახდინონ სხვა სპეციალური სახელშეკრულებო პირობების ფორმულირება. თუმცა, ამ პირობებმაც უნდა წარმოქმნან დაცვის იგივე დონე, რაც მიიღება სტანდარტული სახელშეკრულებო პირობებით. სტანდარტული სახელშეკრულებო პირობების ყველაზე მნიშვნელოვანი მახასიათებლებია:

- ბენეფიციარი მესამე მხარის პირობა, რომელიც ნებას რთავს მონაცემთა სუბიექტებს გააჩნდეთ სახელშეკრულებო უფლებები, იმ შემთხვევაშიც კი, თუ ისინი არ არიან ხელშეკრულების მხარეები;
- მონაცემთა მიმღები ან იმპორტიორი, რომელიც თანხმდება იყოს მონაცემთა ექსპორტიორი დამმუშავებლის შიდასახელმწიფოებრივი საზედამხედველო ორგანოს პროცედურებს დაქვემდებარებული ან/და სასამართლო განხილვისას დავის მონაწილე.

არსებობს სტანდარტული სახელშეკრულებო პირობების

230 მონაცემთა დაცვის დირექტივა, 26-ე მუხლის მე-4 პუნქტი.

231 ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულება, 288-ე მუხლი.

ორი ვარიანტი დამმუშავებელიდან დამმუშავებლის მიმართ ტრანსფერისთვის, რომელთაგან მონაცემთა დამმუშავებელ ექსპორტიორს შეუძლია აირჩიოს ერთ-ერთი.²³² დამმუშავებელიდან უფლებამოსილი პირის მიმართ ტრანსფერებისთვის, არსებობს მხოლოდ ერთი სახის სტანდარტული სახელშეკრულებო პირობები.²³³

ევროპის საბჭოს სამართლებრივ კონტექსტში, 108-ე კონვენციის საკონსულტაციო კომიტეტმა შეადგინა სახელმძღვანელო სახელშეკრულებო პირობების მომზადების თაობაზე.²³⁴

6.4.2. სავალდებულო საკორპორაციო წესები (BCRs)

მრავალხმრივი სავალდებულო საკორპორაციო წესები ყველაზე ხშირად მოიცავს რამოდენიმე ევროპულ მონაცემთა დაცვის ზედამხედველს ერთდროულად.²³⁵ იმისათვის, რათა სავალდებულო საკორპორაციო წესები იქნეს დამტკიცებული, სტანდარტიზებულ საგანცხადო ფორმასთან ერთად მათი პირველადი ტექსტი უნდა იქნეს გაგზავნილი წამყვან ზედამხედველ ორგანოსთან.²³⁶ წამყვანი საზედამხედველო ორგანო განისაზღ-

232 პირველი ვარიანტი მოცემულია ევროპული კომისიის (2001) 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) 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.

233 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.

234 ევროპის საბჭო, 108-ე კონვენციის საკონსულტაციო კომიტეტი (2002), პერსონალურ მონაცემთა ადეკვატური დაცვის დონის არმქონე მესამე ქვეყნებში გადაცემისთვის დადგენილი მოსამზადებელი სახელმძღვანელო.

235 შესაბამისი სავალდებულო საკორპორაციო წესების შინაარსი და სტრუქტურა განხილულია მუხლი 29 სამუშაო ჯგუფის მიერ (2008), სავალდებულო საკორპორაციო წესების სტრუქტურის შესახებ მოცემულ სამუშაო დოკუმენტში, WP 154, ბრიუსელი, 24 ივნისი 2008 წელი; და მუხლი 29 სამუშაო ჯგუფის (2008) სამუშაო დოკუმენტში, რომელიც განსაზღვრავს სავალდებულო საკორპორაციო წესების პრინციპებისა და ელემენტების შემცველ ცხრილს, WP 153, ბრიუსელი, 24 ივნისი 2008 წელი.

236 მუხლი 29 სამუშაო ჯგუფი (2007), რეკომენდაცია 1/2007 პერსონალურ მონაცემთა გადაცემისთვის სავალდებულო საკორპორაციო წესების თაობაზე თანხმობის სტანდარტული გაცემის შესახებ, WP 133, ბრიუსელი, 10 იანვარი 2007 წელი.

ვრება სტანდარტიზებული საგანაცხადო ფორმის საფუძველზე. შემდეგ, ეს ორგანო აცნობებს ყველა საზედამხედველო ორგანოს ევროპული ეკონომიკური ზონის ქვეყნებში, სადაც ჯგუფის წარმომადგენელი არის დაუძნებელი, თუმცა, მათი მონაწილეობა სტანდარტული საკორპორაციო წესების შეფასების პროცესში ნებაყოფლობითია. მიუხედავად იმისა, რომ ეს არ არის სავალდებულო, მონაცემთა დაცვის თითოეულმა ჩართულმა ზედამხედველმა უნდა მოახდინოს შეფასების შედეგის დანერგვა ლიცენზირების თავიანთ ფორმალურ პროცედურებში.

6.4.3. სპეციალური საერთაშორისო შეთანხმებები

ევროპულმა კავშირმა შეადგინა სპეციალური შეთანხმებები ორი სახის მონაცემთა გადამცემისთვის:

მგზავრის სახელის ჩანაწერები (PNRs)

მგზავრის სახელის ჩანაწერები არის მონაცემები შეგროვებული საჰაერო გადამზიდავების მიერ დაჯავშნის პროცესში და მოიცავს სახელებს, მისამართებს, საკრედიტო ბარათის დეტალებს და მგზავრების ადგილების ნომრებს. აშშ-ის კანონმდებლობის მიხედვით, საჰაერო გადამზიდავი კომპანიები ვალდებული არიან გახადონ ეს მონაცემები ხელმისაწვდომი სახელმწიფო უსაფრთხოების დეპარტამენტისათვის მათ გამგზავრებამდე. ეს ეხება ფრენებს როგორც აშშ-ს მიმართულებით, ისე აშშ-დან.

PNR მონაცემების ადეკვატური დაცვის უზრუნველსაყოფად, 95/46/EC დირექტივის საფუძველზე, 2004 წელს მიღებულ იქნა PNR-ის პაკეტი.²³⁷ იგი მოიცავდა აშშ-ის სახელმწიფო უსაფრ-

237 2004 წლის 17 მაისის საბჭოს გადაწყვეტილება 2004/496/EC შეთანხმების თაობაზე ევროპულ გაერთიანებასა და ამერიკის შეერთებულ შტატებს შორის PNR მონაცემების დამუშავებისა და გადამცემის შესახებ საჰაერო გადამზიდავების მიერ ამერიკის შეერთებული შტატების სახელმწიფო უსაფრთხოების დეპარტამენტისთვის, საბაჟო და სასაზღვრო დაცვის ბიუროსთვის, OJ 2004 L 183, გვ. 83; და 2004 წლის 14 მაისის 2004/535/EC გადაწყვეტილება ამერიკის შეერთებული შტატების საბაჟო და სასაზღვრო ბიუროსთვის გადამცემული საჰაერო მგზავრების PNR-ით მოცემული პერსონალური მონაცემების ადეკვატური დაცვის შესახებ, OJ 2004 L 235, გვ. 11-22.

თხოვების დეპარტამენტის მონაცემთა დამუშავების ადეკვატურობის საკითხს.

მართლმსაჯულების ევროპული კავშირის მიერ PNR პაკეტის გაუქმების შემდეგ,²³⁸ ევროპულმა კავშირმა და შეერთებულმა შტატებმა გააფორმეს ორი დამოუკიდებელი შეთანხმება ორი მიზნით: პირველი - დადგენილი ყოფილიყო სამართლებრივი საფუძველი აშშ-ის სახელმწიფო ორგანოებისთვის PNR მონაცემთა გადასაცემად და, მეორე - მიმღებ სახელმწიფოში მონაცემთა დაცვის ადეკვატური დონის დასადგენად.

პირველ შეთანხმებას, გაფორმებულს 2012 წელს, ევროპის ქვეყნებსა და შეერთებულ შტატებს შორის მონაცემთა გაზიარებასა და მართვაზე, გააჩნდა გარკვეული ხარვეზები და ჩანაცვლებულ იქნა იმავე წელს სხვა შეთანხმებით, უკეთესი სამართლებრივი სიზუსტის მისაღწევად.²³⁹ ახალი შეთანხმება ხასიათდება საგრძნობი გაუმჯობესებით. იგი ზღუდავს და ადგენს მიზნებს, რისთვისაც შესაძლებელია გამოყენებულ იქნეს ინფორმაცია, როგორიცაა მნიშვნელოვანი საერთაშორისო დანაშაულები და ტერორიზმი, და ადგენს მონაცემთა შენახვის ვადას: ექვსი თვის შემდეგ მონაცემები უნდა იყოს დეპერსონალიზებული და დაშიფრული. მონაცემთა უკანონო გამოყენების შემთხვევაში, აშშ-ის კანონმდებლობის მიხედვით, ყველას აქვს უფლება ადმინისტრაციულ და სასამართლო დაცვაზე. ასევე, განსაზღვრულია საკუთარ PNR მონაცემებზე წვდომის უფლება და აშშ-ის სახელმწიფო უსაფრთხოების დეპარტამენტის წინაშე შეცვლის, ასევე, ნაშლის მოთხოვნის უფლება, თუ ინფორმაცია არაზუსტია.

შეთანხმება, რომელიც ძალაში შევიდა 2012 წლის 1 ივლისს, იმოქმედებს შვიდი წლის განმავლობაში, 2019 წლამდე.

238 მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები C-317/04 და C-318/04, *European Parliament v. Council of the European Union*, 30 მაისი 2006 წელი, პარაგ. 57, 58 და 59, სადაც სასამართლომ გადაწყვიტა, რომ ადეკვატურობის გადაწყვეტილება და პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული შეთანხმება არის დირექტივის ფარგლებს მიღმა.

239 კომისიის 2012 წლის 26 აპრილის გადაწყვეტილება 2012/472/EU შეერთებულ შტატებსა და ევროპულ კავშირს შორის შეთანხმების თაობაზე მგზავრთა სახელების ჩანაწერთა გამოყენებასა და გადაცემაზე შეერთებული შტატების სახელმწიფო უსაფრთხოების დეპარტამენტისთვის OJ 2012 L 215/4. შეთანხმების ტექსტი, რომელმაც ჩაანაცვლა 2008 წლის შეთანხმება, მიმაგრებულია გადაწყვეტილებაზე OJ 2012 L 215, გვ. 4-16.

2011 წლის დეკემბერში ევროპული კავშირის საბჭომ მიიღო შეთანხმება ევროპულ კავშირსა და ავსტრალიას შორის PNR მონაცემების დამუშავებისა და გადაცემის შესახებ.²⁴⁰ ეს შეთანხმება არის მორიგი წინგადადგმული ნაბიჯი ევროპული კავშირის დღის წესრიგში, რომელიც მოიცავს გლობალურ PNR სახელმძღვანელოს,²⁴¹ აყალიბებს ევროპული კავშირისა და PNR გეგმას²⁴² და მოლაპარაკებას შეთანხმებების თაობაზე მესამე ქვეყნებთან.²⁴³

მონაცემები ფინანსური გზავნილების შესახებ

ბელგიური საზოგადოება SWIFT, რომელიც არის ევროპული ბანკებიდან გლობალური ფულადი ტრანსფერების დიდი ნაწილის განმახორციელებელი, ამუშავებდა მის ერთ-ერთ კომპიუტერულ ცენტრს აშშ-ში, რა დროსაც დადგა მონაცემთა გამჟღავნების საკითხის წინაშე აშშ-ის სახელმწიფო ხაზინის დეპარტამენტისთვის, ტერორიზმის გამოძიების მიზნებისთვის.²⁴⁴

240 საბჭოს 2011 წლის 13 დეკემბრის გადაწყვეტილება 2012/381/EU ევროპულ კავშირსა და ავსტრალიას შორის შეთანხმების შესახებ PNR ჩანაწერების დამუშავებისა და ტრანსფერის თაობაზე საპაეო გადამზიდავების მიერ ავსტრალიის საბაჟო და სასაზღვრო დაცვის სამსახურისთვის, OJ 2012 L 186/3. შეთანხმების ტექსტი მიმაგრებულია გადაწყვეტილებაზე, OJ 2012 L 186, გვ. 4–16.

241 იხ. კომისიის 2010 წლის 21 სექტემბრის მიმართვა PNR მონაცემების მესამე ქვეყნებში ტრანსფერის გლობალური მიდგომის თაობაზე, COM(2010) 492 final, ბრიუსელი, 21 სექტემბერი 2010. იხ. ასევე, მუხლი 29 სამუშაო ჯგუფი (2010), მოსაზრება 7/2010 ევროპული კომისიის მიმართვის შესახებ PNR მონაცემების მესამე ქვეყნებში ტრანსფერის გლობალური მიდგომის თაობაზე, WP 178, ბრიუსელი, 12 ნოემბერი 2010 წელი.

242 ევროპული პარლამენტისა და საბჭოს დირექტივის კანონპროექტი PNR მონაცემების გამოყენების თაობაზე ტერორისტული ქმედებებისა და მნიშვნელოვანი დანაშაულების აღკვეთის, გამოვლენის, გამოძიებისა და დევნისთვის, COM(2011) 32 final, ბრიუსელი, 2 თებერვალი 2011 წელი. 2011 წლის აპრილში, ევროპულმა პარლამენტმა სთხოვა FRA-ს წარედგინა მოსაზრება ამ კანონპროექტისა და მისი შესაბამისობის შესახებ ევროპული კავშირის ძირითად უფლებათა ქარტიასთან. იხ. FRA (2011), მოსაზრება 1/2011 – მგზავრთა სახელის ჩანაწერები, ვენა, 14 ივნისი 2011 წელი.

243 ევროპული კავშირი ამ ეტაპზე მართავს მოლაპარაკებებს PNR შეთანხმების თაობაზე კანადასთან, რაც ჩანაცვლებს 2006 წლის დღემდე მოქმედ შეთანხმებას.

244 ამ მხრივ, იხ. მუხლი 29 სამუშაო ჯგუფი (2011), მოსაზრება 14/2011 ფულის გათვტობასთან და ტერორიზმის ფინანსირებასთან დაკავშირებულ პერსონალურ მონაცემთა საკითხების თაობაზე, WP 186, ბრიუსელი, 13 ივნისი 2011 წელი; მუხლი 29 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), გად-

ევროპული კავშირის პერსპექტივიდან, მხოლოდ იმიტომ, რომ SWIFT-ის ერთ-ერთი მონაცემთა მომსახურების, დამუშავების ცენტრი მდებარეობდა აშშ-ში, არ არსებობდა საკმარისი სამართლებრივი საფუძველი არსებითად ევროპული მონაცემების გამჟღავნებისთვის, რაც განთავსებული იყო აშშ-ში.

სპეციალური შეთანხმება ევროპული კავშირისა და აშშ-ს შორის, ცნობილი როგორც SWIFT-ის შეთანხმება, გაფორმდა 2010 წელს, მონაცემთა დაცვის ადეკვატურობისა და აუცილებელი სამართლებრივი საფუძვლის უზრუნველსაყოფად.²⁴⁵

ამ შეთანხმებით, SWIFT-ის მიერ შენახული ფინანსური მონაცემები მიეწოდება აშშ-ის სახელმწიფო ხაზინის დეპარტამენტს, ტერორიზმის ან ტერორიზმის ფინანსირების აღკვეთის, გამოძიების, გამოვლენის და დევნის მიზნებისთვის. აშშ-ის სახელმწიფო ხაზინის დეპარტამენტს შეუძლია გამოითხოვოს SWIFT-ისგან ფინანსური მონაცემები, იმის გათვალისწინებით რომ მოთხოვნა:

- ახდენს ფინანსური მონაცემების იდენტიფიცირებას შესაძლებლობის ფარგლებში;
- მკაფიოდ ასაბუთებს მონაცემთა აუცილებლობას;
- მოთხოვნილია კონკრეტულად, მონაცემთა მოთხოვნის მინიმიზაციის გათვალისწინებით;
- არ ითხოვს ევროთი ანგარიშსწორების საერთო სივრცესთან (SEPA) დაკავშირებულ მონაცემებს.

Europol-მა უნდა მიიღოს აშშ-ს სახელმწიფო ხაზინის დეპარტამენტისგან თითოეული მოთხოვნის ასლი და განსაზღვროს რამდენად არის SWIFT-ის შეთანხმების პრინციპები დაცული.²⁴⁶ თუ დადასტურდება რომ ისინი დაცულია, SWIFT-მა უნდა მიაწოდოს

ანგვეტილება, 9 დეკემბერი 2008 წელი SWIFT scl-სთან დაკავშირებით ინიცირებული კონტროლისა და რეკომენდაციის პროცედურა.

245 საბჭოს 2010 წლის 13 ივლისის გადაწყვეტილება 2010/412/EU ევროპულ კავშირსა და ამერიკის შეერთებულ შტატებს შორის შეთანხმების შესახებ ფინანსური გზავნილების მონაცემთა ტრანსფერისა და დამუშავების თაობაზე ევროპული კავშირიდან ამერიკის შეერთებული შტატებისთვის ტერორიზმის დაფინანსების გამომვლენის პროგრამის მიზნებისთვის, OJ 2010 L 195, გვ. 3 და 4. შეთანხმების ტექსტი მიმაგრებულია გადაწყვეტილებაზე, OJ 2010 L 195, გვ. 5-14.

246 Europol-ის საერთო საზედამხედველო ორგანო ამ სფეროში განახორციელა Europol-ის მოქმედებათა შემოწმება, რომლის შედეგები ხელმისაწვდომია მისამართზე: <http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en>.

დოს ფინანსური მონაცემები უშუალოდ აშშ-ის სახელმწიფო ხაზინის დეპარტამენტს. დეპარტამენტმა უნდა შეინახოს მონაცემები უსაფრთხო ადგილას, სადაც ისინი არის ხელმისაწვდომი მხოლოდ ტერორიზმის ან მათი დამფინანსებლების ანალიტიკოსი გამოძიებლების მიერ და მონაცემები არ უნდა იყოს დაკავშირებული რომელიმე სხვა მონაცემთა ბაზასთან. ზოგადად, SWIFT-ისგან მოწოდებული ფინანსური მონაცემები უნდა იყოს ნაშლილი მისი მიღებიდან არაუგვიანეს ხუთი წლის განმავლობაში. ფინანსური მონაცემები, რომელიც არის საჭირო კონკრეტული გამოძიებებისთვის ან დევნისთვის, შესაძლებელია იქნეს შენახული იმ ვადით, რაც აუცილებელია ამ გამოძიებების ან დევნისთვის.

აშშ-ის სახელმწიფო ხაზინის დეპარტამენტს შეუძლია გადასცეს SWIFT-ისგან მიღებული მონაცემები სამართალდამცავ ორგანოებს, საზოგადოებრივი უსაფრთხოების ან ტერორიზმის წინააღმდეგ ბრძოლის ორგანოებს აშშ-ის ან მის ფარგლებს გარეთ მხოლოდ ტერორიზმის ან მისი დაფინანსების გამოძიების, გამოვლენის, პრევენციის ან დევნის მიზნებისთვის. თუ ფინანსური მონაცემების მიმდინარე ტრანსფერი მოიცავს ევროპული კავშირის წევრი ქვეყნის მოქალაქეს ან რეზიდენტს, მონაცემთა ნებისმიერი გადაცემა მესამე ქვეყნის სახელმწიფო ორგანოებისთვის, დაექვემდებარება ევროპული კავშირის წევრი ქვეყნების კომპეტენტური სახელმწიფო ორგანოების წინასწარ თანხმობას. გამონაკლისები შესაძლებელია დაშვებულ იქნეს თუ მონაცემთა გადაცემა არის აუცილებელი საზოგადოებრივი უსაფრთხოებისთვის, მომეტებული და მყისიერი საშიშროების პრევენციის მიზნებისთვის.

დამოუკიდებელი ზედახმედველები, მათ შორის ევროპული კომისიის მიერ დანიშნულები პირები, მონიტორინგს უწევენ SWIFT-ის შეთანხმების პრინციპების შესრულებას.

მონაცემთა სუბიექტებს უფლება აქვთ ევროპული კავშირის მონაცემთა დაცვის კომპეტენტური ზედამხედველებისგან მოიპოვონ ინფორმაცია მათი პერსონალური მონაცემების უფლებათა დაცვის თაობაზე. მონაცემთა სუბიექტებს, ასევე, უფლება აქვთ იმ მონაცემების შეცვლაზე, ნაშლასა ან დაბლოკვაზე, რომელიც შეგროვებულია და შენახულია აშშ-ის სახელმწიფო ხაზი-

ნის დეპარტამენტის მიერ SWIFT-ის შეთანხმების საფუძველზე. თუმცა, მონაცემთა სუბიექტის წვდომის უფლებები, შესაძლებელია, დაექვემდებაროს კონკრეტულ სამართლებრივ შეზღუდვებს. როდესაც წვდომა უარყოფილია, მონაცემთა სუბიექტი უნდა იქნეს წერილობით ინფორმირებული უარყოფის შესახებ და უფლების შესახებ – მოითხოვოს ადმინისტრაციული ან სასამართლო განხილვა აშშ-ში.

SWIFT-ის შეთანხმება ძალაშია ხუთი წლის მანძილზე, 2015 წლის აგვისტომდე. მისი მოქმედება ავტომატურად გრძელდება ერთი წლით, გარდა იმ შემთხვევისა, როდესაც ერთ-ერთი მხარე შეატყობინებს მეორეს, სულ მცირე 6 თვით ადრე, მისი ნების შესახებ, რომ ხელშეკრულება არ იქნეს გაგრძელებული.

7. მონაცემთა დაცვა პოლიციის სექტორსა და სისხლისსამართლებრივი მართლმსაჯულების სფეროში

ევროპული კავშირი	განხილული საკითხები	ევროპის საბჭო
	ზოგადად	108-ე კონვენცია
	პოლიცია	რეკომენდაცია პოლიციის შესახებ
		ადამიანის უფლებათა ევროპული სასამართლო, B.B. v. France, No. 5335/06, 17 დეკემბერი 2009 წელი
		ადამიანის უფლებათა ევროპული სასამართლო, S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 დეკემბერი 2008 წელი
		ადამიანის უფლებათა ევროპული სასამართლო, Vetter v. France, No.59842/00, 31 მაისი 2005 წელი
	კიბერდანაშაული	კონვენცია კიბერდანაშაულის შესახებ
მონაცემთა დაცვა პოლიციისა და სამართალდამცავი ორგანოების საერთაშორისო თანამშრომლობის კონტექსტში		
მონაცემთა დაცვის ჩარჩო შეთანხმება	ზოგადად	108-ე კონვენცია რეკომენდაცია პოლიციის შესახებ
Prüm-ის გადაწყვეტილება	განსაკუთრებული მონაცემებისთვის: თითის ანაბეჭდი, დნმ, ხულიგნობა და ა.შ.	108-ე კონვენცია რეკომენდაცია პოლიციის შესახებ
Europol-ის აწყვეტილება	სპეციალური სააგენტოებისთვის	108-ე კონვენცია
Eurojust-ის აწყვეტილება		რეკომენდაცია პოლიციის შესახებ
Frontex-ის რეგულაცია		

Schengen II-ის გად- ანყვეტილება VIS რეგულაცია Eurodac რეგულაცია CIS გადანყვეტილება	სპეციალური საერთო საინფორმაციო სისტემები	108-ე კონვენცია რეკომენდაცია პოლიციის შესახებ ადამიანის უფლებათა ევ- როპული სასამართლო, Dalea v. France, No. 964/07, 2 თებერვალი 2010 წელი
--	---	--

დანაშაულთან ბრძოლის, ეროვნული და საზოგადოებრივი უსაფრთხოების უზრუნველყოფის მიზნით ინდივიდის მონაცემთა დაცვის ინტერესებისა და მონაცემთა შეგროვებისას საზოგადოების ინტერესების გასაწონასწორებლად, ევროპის საბჭომ და ევროპულმა კავშირმა აამოქმედა კონკრეტული სამართლებრივი ინსტრუმენტები.

7.1. ევროპის საბჭოს კანონმდებლობა მონაცემთა დაცვის შესახებ პოლიციის სექტორსა და სისხლისსამართლებრივი მართლმსაჯულების კონტექსტში

საკვანძო დებულებები

- 108-ე კონვენცია და ევროპის საბჭოს რეკომენდაცია პოლიციის შესახებ ვრცელდება მონაცემთა დაცვაზე პოლიციის საქმიანობის ყველა სფეროში.
- კონვენცია კიბერდანაშაულის შესახებ (ბუდაპეშტის კონვენცია) არის სავალდებულო საერთაშორისო სამართლებრივი ინსტრუმენტი, რომელიც ეხება ელექტრონული ქსელების მეშვეობით და მათ წინააღმდეგ ჩადენილ დანაშაულებს.

ევროპის დონეზე, 108-ე კონვენცია ვრცელდება პერსონალურ მონაცემთა დამუშავების ყველა სფეროზე და მისი დებულებები მიმართულია პერსონალურ მონაცემთა საერთო დამუშავების რეგულირებისკენ. შესაბამისად, 108-ე კონვენცია ვრცელდება მონაცემთა დაცვაზე პოლიციის სექტორსა და სისხლისსამართლებრივი მართლმსაჯულების სფეროში, თუმცა ხელმომწერ სახელმწიფოებს შეუძლიათ შეზღუდონ მისი გავრცელება.

პოლიციისა და სისხლისსამართლებრივი მართლმსაჯულების ორგანოთა მოვალეობები ხშირად მოითხოვს პერსონალურ მონაცემთა დამუშავებას, რაც შესაძლოა ინვესტირდეს საგრძნობ შედეგებს შესაბამისი ინდივიდებისთვის. 1987 წელს ევროპის საბჭოს მიერ მიღებული რეკომენდაცია იძლევა მითითებებს ხელშემრკველი მხარეებისთვის, თუ როგორ უნდა უზრუნველყონ 108-ე კონვენციის პრინციპების დანერგვა პოლიციის მიერ პერსონალურ მონაცემთა დამუშავების კონტექსტში.²⁴⁷

7.1.1. რეკომენდაცია პოლიციის შესახებ

ადამიანის უფლებათა ევროპულმა სასამართლომ არაერთხელ აღნიშნა, რომ პოლიციის ან ეროვნული უსაფრთხოების ორგანოების მიერ პერსონალურ მონაცემთა ჩანერა და შენახვა წარმოადგენს ჩარევას კონვენციის მე-8 მუხლი პირველი პუნქტით დადგენილ უფლებაში. სასამართლოს მრავალი გადაწყვეტილება ეხება ამგვარი ჩარევის მართლზომიერების საკითხს.²⁴⁸

მაგალითი: საქმეზე *B.B. v. France*,²⁴⁹ ადამიანის უფლებათა ევროპულმა სასამართლომ გადანყვიტა, რომ სექსობრივი დანაშაულისთვის მსჯავრდებულის მონაცემების შენახვა ეროვნულ მონაცემთა ბაზაში მოექცა კონვენციის მე-8 მუხლის ფარგლებში. იმის გათვალისწინებით, რომ იმპლემენტირებულ იქნა მონაცემთა დაცვის საკმარისი ზომები, როგორიცაა მონაცემთა სუბიექტის მონაცემთა ნაშლის მოთხოვნის უფლება, მონაცემთა შენახვის ლიმიტირებული ვადა და ამ მონაცემებთან ლიმიტირებული წვდომა - დადგინდა სამართლიანი ბალანსი დაპირისპირებულ პირად და საჯარო ინტერესებს შორის. სასამართლომ დაადგინა, რომ სახეზე არ იყო კონვენციის მე-8 მუხლის დარღვევა.

მაგალითი: საქმეზე *S. and Marper v. the United Kingdom*,²⁵⁰ ორივე გან-

247 ევროპის საბჭო, მინისტრთა კომიტეტი (1987), რეკომენდაცია Rec(87)15 წევრი ქვეყნებისთვის პოლიციის სექტორში პერსონალურ მონაცემთა გამოყენების რეგულირების თაობაზე, 17 სექტემბერი 1987 წელი.

248 იხ. მაგ. ადამიანის უფლებათა ევროპული სასამართლო, *Leander v. Sweden*, No. 9248/81, 26 მარტი 1987 წელი; ადამიანის უფლებათა ევროპული სასამართლო *M.M. v. the United Kingdom*, No. 24029/07, 13 ნოემბერი 2012 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *M.K. v. France*, No. 19522/09, 18 აპრილი 2013 წელი.

249 ადამიანის უფლებათა ევროპული სასამართლო, *B.B. v. France*, No. 5335/06, 17 დეკემბერი 2009 წელი.

250 ადამიანის უფლებათა ევროპული სასამართლო, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 დეკემბერი 2008 წელი, პარაგ. 119 და 125.

მცხადებელი იქნა ბრალდებული, მაგრამ არა მსჯავრდებული, სისხლისსამართლებრივი დანაშაულებისთვის. მიუხედავად ამისა, მათი თითის ანებეჭდები, დნმ-ის პროფილი და უჯრედული მონაცემები იქნა შენახული პოლიციის მიერ. ბიომეტრიული მონაცემების განუსაზღვრელი ვადით შენახვა კანონით ნებდართული იყო იმ შემთხვევაშიც კი, თუ პირი იყო ექვმიტანილი სისხლისსამართლებრივი ქმედებისთვის და მოგვიანებით იქნა გამართებული ან მოეხსნა ბრალდება. ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ პერსონალური მონაცემების ყოველმხრივი და განუსაზღვრელი შენახვა, რომელიც არ იყო ვადებში განსაზღვრული და როდესაც გამართლებულ ინდივიდებს გააჩნდათ მხოლოდ ლიმიტირებული შესაძლებლობა მოეთხოვათ წაშლა, წარმოადგენდა არაპროპორციულ ჩარევას განმცხადებლის პირადი ცხოვრების უფლებაში. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

ადამიანის უფლებათა ევროპული სასამართლოს სხვა გადწყვეტილებები ეხება მონაცემთა დაცვის უფლებაში თვალთვალის მეშვეობით ჩარევის მართლზომიერებას.

მაგალითი: საქმეზე *Allan v. the United Kingdom*,²⁵¹ შესაბამისი ორგანოს მიერ საიდუმლოდ იქნა ჩანერილი პატიმრის პირადი საუბრები ციხეში მის მეგობართან შეხვედრებისთვის გამოყოფილ ტერიტორიაზე და, ასევე, მისი საუბრები თანამესაკნესთან. ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ განმცხადებლის საკანში აუდიო და ვიდეო ჩანაწერების გამოყენება შეხვედრებისთვის გამოყოფილ ადგილას და თანამესაკნესთან საუბრის დროს წარმოადგენდა ჩარევას განმცხადებლის პირადი ცხოვრების უფლებაში. რამდენადაც არ არსებობდა საკანონმდებლო სისტემა, რომელიც შესაბამის დროს დაარეგულირებდა პოლიციის მიერ ჩამწერი მონაცემების ფარულ გამოყენებას, აღნიშნული ჩარევა არ იყო კანონის შესაბამისი. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

მაგალითი: საქმეზე *Klass and Others v. Germany*,²⁵² გამცხადებლები აღნიშნავენ, რომ რამოდენიმე გერმანული სამართლებრივი აქტი, რომელიც დასაშვებად აღიარებდა ფოსტისა და ტელეკომუნიკაციების ფარულ თვალთვალს, არღვევდა კონვენციის მე-8 მუხლს იქიდან გამომდინარე, რომ პირი, რომელზეც მიმდინარეობდა თვალთვალი არ იყო ინფორმირებული თვალთვალის მიზნით მიღებული ზომების შესახებ და არ შეეძლო მიემართა სასამართლოსთ-

251 ადამიანის უფლებათა ევროპული სასამართლო, *Allan v. the United Kingdom*, No. 48539/99, 5 ნოემბერი 2002 წელი.

252 ადამიანის უფლებათა ევროპული სასამართლო, *Klass and Others v. Germany*, No. 5029/71, 6 სექტემბერი 1978 წელი.

ვის მისი შეწყვეტის შემდეგ. ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ თვალთვალის საშიშროება საჭიროების ფარგლებში იჭრებოდა მოხმარებლებს შორის კომუნიკაციის თავისუფლებაში, საფოსტო და სატელეკომუნიკაციო მომსახურების დროს. ამასთან, აღმოჩნდა, რომ უსაფრთხოების საკმარისი ზომები იქნა მიღებული უფლების ბოროტად გამოყენების წინააღმდეგ. გერმანული კანონმდებლობა მიჩნეულ იქნა მართლზომიერად, იმ მხრივ, რომ დაადგინა ეს ზომები აუცილებლად დემოკრატიულ საზოგადოებაში ეროვნული უსაფრთხოების ინტერესების დაცვისთვის, დანაშაულისა და არეულობის პრევენციისთვის. სასამართლომ დაასკვნა, რომ სახეზე არ იყო კონვენციის მე-8 მუხლის დარღვევა.

რამდენადაც პოლიციის მიერ მონაცემთა დამუშავებას შესაძლოა ჰქონდეს საკმაო ზეგავლენა მოცემულ პირებზე, ამ სფეროში აუცილებელია მონაცემთა ბაზების შექმნისთვის მონაცემთა დაცვის დეტალური წესების არსებობა. ევროპის საბჭოს რეკომენდაცია პოლიციის შესახებ ცდილობს მოაწესრიგოს პოლიციის მუშაობის დროს მონაცემთა შეგროვების საკითხი მითითებების მიცემით, თუ როგორ უნდა იქნეს შენახული მონაცემთა ფაილები ამ სფეროში; ვინ არის უფლებამოსილი მოახდინოს წვდომა ამ ფაილებზე, მათ შორის, პირობები, რომელიც ეხება მონაცემთა გადაცემას საზღვარგარეთის პოლიციის ორგანოებისთვის; როგორ შეუძლია მონაცემთა სუბიექტს საკუთარ მონაცემთა დაცვასთან დაკავშირებული უფლებების რეალიზაცია; როგორ უნდა იყოს იმპლმენტირებული კონტროლი დამოუკიდებელი ორგანოების მიერ. ასევე, გათვალისწინებულია მონაცემთა უსაფრთხოების ადეკვატურობის ვალდებულება.

რეკომენდაცია არ ადგენს მონაცემთა განუსაზღვრელ, განურჩეველ შეგროვებას პოლიციის მიერ. იგი ზღუდავს პერსონალურ მონაცემთა დამუშავების ფარგლებს პოლიციის ორგანოების მიერ იმ დონემდე, რაც აუცილებელია რეალური საფრთხის ან სპეციალური დანაშაულებრივი ქმედების პრევენციისთვის. ნებისმიერი დამატებითი მონაცემთა დამუშავება შესაძლებელია დაფუძნებული იყოს ეროვნულ სპეციალურ კანონმდებლობაზე. განსაკუთრებული კატეგორიის მონაცემთა დამუშავება უნდა იყოს ლიმიტირებული იმ დონემდე, რაც წარმოადგენს აუცილებლობას კონკრეტული გამოძიების მიმდინარეობისას.

თუ პერსონალური მონაცემები შეგროვებულია მონაცემთა სუბიექტის ინფომირების გარეშე, იგი უნდა იქნეს ინფორმირებული მონაცემთა შეგროვების შესახებ მაშინვე, როდესაც ამგვარ ინფომირებას აღარ ზღუდავს გამოძიება. მონაცემთა შეგროვება ტექნიკური ან სხვა ავტომატიზებული საშუალებებით, ასევე, უნდა იყოს დაფუძნებული სპეციალურ სამართლებრივ დებულებებზე.

მაგალითი: საქმეზე *Vetter v. France*,²⁵³ ანონიმურმა მონმეებმა ბრალი დასდეს განმცხადებელს მკვლელობაში. რამდენადაც განმცხადებელი რეგულარულად მიდიოდა მეგობრის სახლში, პოლიციამ მის სახლში დააყენა მოსასმენი მოწყობილობები მოსამართლის ნებართვის საფუძველზე. ჩანერილ საუბრებზე დაყრდნობით, განმცხადებელი იქნა დაკავებული და ბრალდებული მკვლელობისთვის. მან მოითხოვა ჩანანერის დაუშვებელ მტკიცებულებად ცნობა, იმის გათვალისწინებით, რომ ის არ იყო კანონმდებლობით დადგენილი. ადამიანის უფლებათა ევროპული სასამართლოს თანახმად, საკითხი ეხებოდა მოსასმენი მოწყობილობების გამოყენებას „კანონის შესაბამისად.“ პირადი საცხოვრებლის მოსასმენი საშუალებებით აღჭურვა მკაფიოდ არ იყო მოცემული სისხლის სამართლის საპროცესო კოდექსის შესაბამის ნორმებში, რამდენადაც კოდექსის დებულებები მოიცავდა სატელეფონო ხაზების მოსმენას. კოდექსის 81-ე მუხლი საკმარისი სიცხადით არ ადგენდა ორგანოების დისკრეციის აღსრულების ფარგლებსა და ხასიათს პირადი საუბრების მონიტორინგის ჭრილში. შესაბამისად, განმცხადებელი ვერ სარგებლობდა დაცვის მინიმალური დონით, რომლითაც მოქალაქეები სარგებლობდნენ დემოკრატიულ საზოგადოებაში კანონის უზენაესობიდან გამომდინარე. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

რეკომენდაცია ადგენს, რომ პერსონალურ მონაცემთა შენახვისას, უნდა იქნეს დაგენილი მკაფიო განსხვავება: ადმინისტრაციულ მონაცემებსა და პოლიციის მონაცემებს შორის; მონაცემთა სუბიექტების სხვადასხვა სახეებს შორის, როგორიცაა ეჭვმიტანილები, პატიმრები, დაზარალებულები და მონმეები; ასევე განსხვავება მონაცემებს შორის, რომელიც დაფუძნებულია უტყუარ მტკიცებულებებზე, ვარაუდებსა და მოსაზრებებზე.

253 ადამიანის უფლებათა ევროპული სასამართლო, *Vetter v. France*, No. 59842/00, 31 მაისი 2005 წელი.

პოლიციის მონაცემები უნდა იყოს მკაცრად ლიმიტირებული მიზნის გათვალისწინებით. აღნიშნულს გააჩნია შედეგი პოლიციის მონაცემების მესამე პირებთან კომუნიკაციისას: ამგვარი მონაცემების გადაგზავნა ან მიწოდება პოლიციის სექტორს შიგნით უნდა იყოს რეგულირებული იმის მიხედვით, თუ რამდენად არსებობს ლეგიტიმური ინტერესი ინფორმაციის გაზიარებისას. ამგვარი მონაცემების გადაცემა პოლიციის სექტორს გარეთ უნდა იყოს ნებადართული მხოლოდ კანონით გათვალისწინებული ვალდებულებიდან გამომდინარე ან შესაბამისი ნებართვის საფუძველზე. საერთაშორისო ტრანსფერი ან გადაცემა უნდა იყოს შეზღუდული მხოლოდ საზღვარგარეთის პოლიციის ორგანოებისთვის და იყოს დაფუძნებული სპეციალურ სამართლებრივ დებულებებზე, მათ შორის, საერთაშორისო შეთანხმებებზე, გარდა იმ შემთხვევისა, როდესაც ეს აუცილებელია მნიშვნელოვანი და მყისიერი საფრთხის პრევენციისთვის.

პოლიციის მიერ მონაცემთა დამუშავება უნდა დაექვემდებაროს დამოუკიდებელი საზედამხედველო ორგანოს კონტროლს, რათა უზრუნველყოფილ იქნეს მონაცემთა დაცვის შიდასახელმწიფოებრივ კანონმდებლობასთან შესაბამისობა. მონაცემთა სუბიექტებს უნდა გააჩნდეთ წვდომის ყველა უფლება, რაც მოცემულია 108-ე კონვენციით. თუ პოლიციის გამოძიების ეფექტურობის ინტერესებისთვის მონაცემთა სუბიექტის წვდომის უფლებები იქნა შეზღუდული 108-ე კონვენციის მე-9 მუხლით, მონაცემთა სუბიექტს შიდასახელმწიფოებრივი კანონმდებლობით უნდა ჰქონდეს შესაძლებლობა მიმართოს მონაცემთა დაცვის საზედამხედველო ან სხვა დამოუკიდებელ ორგანოს.

7.1.2. ბუდაპეშტის კონვენცია კიბერდანაშაულის შესახებ

რამდენადაც დანაშაულებრივი ქმედებებისას სულ უფრო მეტად გამოიყენება მონაცემთა დამუშავების ელექტრონულ სისტემები და გავლენა აქვს მასზე, აუცილებელია ახალი სამართლებრივი ნორმები ამ გამოწვევის დასარეგულირებლად. თავის მხრივ, ევროპის საბჭომ მიიღო საერთაშორისო სამართლებრივი ინსტრუმენტი, კონვენცია კიბერდანაშაულის შესახებ – ცნობილი როგორც ბუდაპეშტის კონვენცია, რათა დაერეგულირებინა

ელექტრონული საშუალებების წინააღმდეგ და მათი გამოყენებით ჩადენილი დანაშაულები.²⁵⁴ ეს კონვენცია ღიაა ხელმოწერისთვის ევროპის საბჭოს არაწევრი ქვეყნებისთვისაც, 2013 წლის შუა პერიოდისთვის, ევროპის საბჭოს მიღმა არსებული ოთხი სახელმწიფო – ავსტრალია, დომინიკის რესპუბლიკა, იაპონია და აშშ იყვნენ კონვენციის ხელმომწერი მხარეები, ხოლო თორმეტმა სხვა არაწევრმა სახელმწიფომ, ასევე, მოაწერა ხელი ან იქნა მოწვეული ხელმოწერისთვის.

კონვენცია კიბერდანაშაულის შესახებ რჩება ყველაზე გავლენიან საერთაშორისო შეთანხმებად, რომელიც ეხება კანონის დარღვევებს ინტერნეტში ან ინფორმაციის სხვა ქსელებში. იგი მოითხოვს მხარეებისგან მოახდინონ მათი სისხლისსამართლებრივი ნორმების განახლება და ჰარმონიზება ჰაკერობისა და უსაფრთხოების სხვა დარღვევების წინააღმდეგ, მათ შორის, საავტორო უფლებების დარღვევების წინააღმდეგ, კომპიუტერულად განხორციელებული დანაშაულის წინააღმდეგ, ბავშვთა პორნოგრაფიისა და სხვა არაკანონიერი კიბერ-ქმედებების წინააღმდეგ. კონვენცია, ასევე, განსაზღვრავს პროცედურულ უფლებამოსილებებს, რომელიც ეხება კომპიუტერული ქსელების გამოძიებასა და კომუნიკაციების თვალთვალს კიბერდანაშაულთან ბრძოლის პროცესში. და ბოლოს, იგი განსაზღვრავს საერთაშორისო კოოპერაციის ეფექტურ შესაძლებლობას. კონვენციის დამატებითი ოქმი ეხება რასისტული და ქსენოფობიური პროპაგანდის კრიმინალიზაციას კომპიუტერულ ქსელებში.

მიუხედავად იმისა, რომ კონვენცია, ძირითადად, არ არის მონაცემთა დაცვის მხარდამჭერი ინსტრუმენტი, იგი ახდენს იმ ქედებათა კრიმინალიზაციას, რომელიც შესაძლოა არღვევდეს მონაცემთა სუბიექტის უფლებას მონაცემთა დაცვაზე. კონვენციის იმპლემენტირებისას, იგი, ასევე, ავალდებულებს ხელშემკვრელ მხარეებს გააანალიზონ ადამიანის უფლებათა და თავისუფლებათა ადეკვატური დაცვა, მათ შორის იმ უფლებების, რომელიც გარანტირებულია ადამიანის უფლებათა ევროპული კონვენციით, როგორიცაა მონაცემთა დაცვის უფლება.²⁵⁵

254 ევროპის საბჭო, მინისტრთა კომიტეტი (2001), კონვენცია კიბერდანაშაულის შესახებ, CETS No. 185, ბუდაპეშტი, 23 ნოემბერი 2001 წელი, ძალაში შევიდა 2004 წლის პირველ ივლისს.

255 იქვე, მე-15 მუხლის პირველი პუნქტი.

7.2. მონაცემთა დაცვის ევროპული კავშირის კანონმდებლობა პოლიციის და სისხლისსამართლებრივ საკითხებში

საკვანძო დებულებები

- ევროპული კავშირის დონეზე, მონაცემთა დაცვა პოლიციისა და სისხლისსამართლებრივ სექტორში რეგულირებულია მხოლოდ პოლიციისა და სამართალდამცავი ორგანოების საერთაშორისო კოოპერაციის კონტექსტში.
- მონაცემთა დაცვის სპეციალური წესები დადგენილია პოლიციის ევროპული სამსახურის (Europol) და ევროპული კავშირის სამართლებრივი თანამშრომლობის გაერთიანებისთვის (Eurojust), რომლებიც არიან კანონის აღსრულებისას საერთაშორისო თანამშრომლობისა და ხელშეწყობის ევროპული კავშირის ორგანოები.
- მონაცემთა დაცვის სპეციალური წესები დადგენილია საერთო საინფორმაციო სისტემებისთვისაც, რომელიც დაფუძნებულია ევროპული კავშირის დონეზე ინფორმაციის საერთაშორისო გაცვლისათვის პოლიციისა და კომპეტენტურ სამართალდამცავ ორგანოებს შორის. მნიშვნელოვანი მაგალითებია Schengen II, სავიზო საინფორმაციო სისტემა (VIS) და Eurodac – ცენტრალიზებული სისტემა, რომელიც შეიცავს მესამე ქვეყნის იმ მაცხოვრებელთა თითის ანაბეჭდების მონაცემებს, რომლებმაც თავშესაფრისთვის მიმართეს ევროპული კავშირის რომელიმე წევრ ქვეყანას.

მონაცემთა დაცვის დირექტივა არ ვრცელდება პოლიციისა და სისხლისსამართლებრივ სექტორზე, პარაგრაფი 7.2.1. აღწერს ამ სფეროში ყველაზე მნიშვნელოვან სამართლებრივ ინსტრუმენტებს.

7.2.1. მონაცემთა დაცვის ჩარჩო გადანყვეტილება

საბჭოს ჩარჩო გადანყვეტილების 2008/977/JHA, სისხლისსამართლებრივ საქმეებში პოლიციისა და სამართლებრივი თანამშრომლობის ფარგლებში დამუშავებულ პერსონალურ

მონაცემთა დაცვის შესახებ (მონაცემთა დაცვის ჩარჩო გადაწყვეტილება),²⁵⁶ მიზანს წარმოადგენს ფიზიკური პირების პერსონალურ მონაცემთა დაცვის უზრუნველყოფა, როდესაც მათი პერსონალური მონაცემები დამუშავებულია დანაშაულებრივ ქმედებათა აღკვეთის, გამოძიების, გამოვლენის, დევნის მიზნებისთვის ან სასჯელთა აღსრულებისთვის. ამ მიმართულებით ევროპული კავშირისთვის ან მისი წევრი ქვეყნებისთვის მოქმედებს კომპეტენტური ორგანოები, რომელიც მუშაობენ პოლიციისა და კრიმინალური მართლმსაჯულების კონტექსტში. ეს ორგანოები მოქმედებენ ევროპული კავშირის წევრი ქვეყნებისთვის ან ევროპული კავშირისთვის, პოლიციისა და სისხლის სამართლებრივ სფეროში. ეს ორგანოებია ევროპული კავშირის ან მისი წევრი ქვეყნების სააგენტოები ან დანესებულებები.²⁵⁷ ჩარჩო გადაწყვეტილების მოქმედება ვრცელდება ამ ორგანოთა შორის თანამშრომლობაზე საერთაშორისო მონაცემთა დაცვის კუთხით და არ ვრცელდება სახელმწიფო უსაფრთხოებაზე.

მონაცემთა დაცვის ჩარჩო გადაწყვეტილება მეტწილად ეყრდნობა იმ პრინციპებსა და ცნებებს, რომელიც მოცემულია 108-ე კონვენციითა და მონაცემთა დაცვის დირექტივით.

მონაცემები უნდა იქნეს გამოყენებული მხოლოდ კომპეტენტური ორგანოს მიერ და მხოლოდ იმ მიზნისთვის, რომლისთვისაც იგი გადაიცა ან ხელმისაწვდომი გახდა. მიმღებმა წევრმა სახელმწიფომ უნდა დაიცვას მონაცემთა გაცვლისთვის დანესებული ნებისმიერი შეზღუდვა, რაც გათვალისწინებულია გადმოცემი სახელმწიფოს კანონით. მიუხედავად ამისა, მიმღები ქვეყნის მიერ მონაცემთა გამოყენება განსხვავებული მიზნისთვის ნებადართულია კონკრეტული პირობების არსებობისას. გადაცემათა აღრიცხვა და დოკუმენტირება კომპეტენტური ორგანოების სპეციალური მოვალეობაა, საჩივრების არსებობის შემთხვევაში სიცხადის უზრუნველსაყოფად. საერთაშორისო გადაცემის კოოპერაციისას მიღებულ მონაცემთა გადაცემა მესამე მხარეებისთვის საჭიროებს იმ წევრი ქვეყნის თანხმობას,

256 ევროპული კავშირის საბჭო (2008), საბჭოს 2008 წლის 27 ნოემბრის ჩარჩო გადაწყვეტილება 2008/977/JHA პოლიციისა და სამართლებრივი თანამშრომლობის ფარგლებში სისხლის სამართლებრივ კონტექსტში დამუშავებულ პერსონალურ მონაცემთა დაცვის შესახებ (მონაცემთა დაცვის ჩარჩო გადაწყვეტილება), OJ 2008 L 350.

257 იქვე, მე-2 მუხლის -h- ქვეპუნქტი.

რომელი ქვეყნიდანაც პირველად მოხდა მონაცემთა გადმოცემა, მიუხედავად ამისა, გადაუდებელი შემთხვევისას არსებობს გამონაკლისები.

კომპეტენტურმა ორგანოებმა უნდა მიიღონ აუცილებელი ზომები უსაფრთხოებისთვის, პერსონალურ მონაცემთა ნებისმიერი უკანონო დამუშავებისგან დასაცავად.

ევროპული კავშირის თითოეულმა წევრმა ქვეყანამ უნდა უზრუნველყოს ერთი ან მეტი დამოუკიდებელი ეროვნული ზედამხედველი ორგანოს არსებობა, რომელიც პასუხისმგებელია მონაცემთა დაცვის ჩარჩო გადანაცვების საფუძველზე მიღებული დებულებების მონიტორინგსა და მოქმედებაზე. მათ, ასევე, უნდა განიხილონ საჩივრები, რომელიც შეტანილია ნებისმიერი პირის მიერ მათი უფლებებისა და თავისუფლებების დაცვის თაობაზე, კომპეტენტური ორგანოების მიერ პერსონალურ მონაცემთა დამუშავების კუთხით.

მონაცემთა სუბიექტს უფლება აქვს მიიღოს ინფორმაცია მისი პერსონალური მონაცემის დამუშავების შესახებ და მისი წვდომის, შეცვლის, ნაშლის ან დაბლოკვის უფლებების შესახებ. როდესაც ამ უფლებათა რეალიზაცია უარყოფილია შესაბამისი მიზეზის საფუძველზე, მონაცემთა სუბიექტს უნდა ჰქონდეს უფლება საჩივრით მიმართოს კომპეტენტურ შიდასახელმწიფოებრივ საზედამხედველო ორგანოს ან/და სასამართლოს. თუ პირი მიიღებს ზიანს, მონაცემთა დაცვის ჩარჩო გადანაცვების მაიმპლემენტირებელი ეროვნული კანონმდებლობის დარღვევების გამო, იგი უფლებამოსილია დამუშავებისგან მოითხოვოს კომპენსაცია.²⁵⁸ ძირითადად, მონაცემთა სუბიექტებს უნდა ჰქონდეთ უფლება სამართლებრივ დაცვაზე, მონაცემთა დაცვის ჩარჩო გადანაცვების მაიმპლემენტირებელი შიდასახელმწიფოებრივი კანონმდებლობით აღიარებული უფლებების დარღვევის გამო.²⁵⁹

ევროპულმა კომისიამ წარადგინა რეფორმა, რომელიც მოიცავს მონაცემთა დაცვის გენერალურ რეგულაციას²⁶⁰ და მონა-

258 იქვე, მე-19 მუხლი.

259 იქვე, მე-20 მუხლი.

260 ევროპული კომისია (2012), ევროპული პარლამენტისა და საბჭოს რეგულაციის პროექტი პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ (მონაცემთა დაცვის ძირითადი რეგულაცია), COM (2012) 11 final, ბრიუსელი, 2012 წლის 25 იანვარი.

ცემთა დაცვის გენერალურ დირექტივას.²⁶¹ ახალი დირექტივა ჩანაცვლებს არსებულ მონაცემთა დაცვის ჩარჩო გადაწყვეტილებას და დაადგენს ძირითად პრინციპებსა და წესებს პოლიციისა და სამართლებრივი თანამშრომლობის შესახებ სისხლისმართლებრივ საქმეებზე.

7.2.2. მონაცემთა დაცვის მეტად სპეციფიკური სამართლებრივი ინსტრუმენტები პოლიციისა და კანონის აღმასრულებელი ორგანოების საერთაშორისო კოოპერაციისას

მონაცემთა დაცვის ჩარჩო გადაწყვეტილებასთან ერთად, ევროპული კავშირის წევრი ქვეყნების ხელთ არსებული ინფორმაციის გაცვლა, კონკრეტულ შემთხვევებში, რეგულირებულია არაერთი სამართლებრივი ინსტრუმენტით, მათ შორისაა, საბჭოს ჩარჩო გადაწყვეტილება 2009/315/JHA წევრ ქვეყნებს შორის დანაშაულების თაობაზე ჩანაწერების გაცვლის დროს ამოღებული ინფორმაციის ორგანიზაციასა და შინაარსზე და საბჭოს გადაწყვეტილება, რომელიც ეხება წევრი ქვეყნების ფინანსური სადაზვერვო განყოფილებების კოოპერაციის შეთანხმებას ინფორმაციის გაცვლის მხრივ.²⁶²

დიდწილად, კომპეტენტურ ორგანოებს შორის საერთაშორისო თანამშრომლობა,²⁶³ სულ უფრო და უფრო, ითვალისწინებს

261 ევროპული კომისია (2012), ევროპული პარლამენტისა და საბჭოს დირექტივის პროექტი კომპეტენტური ორგანოების მიერ დანაშაულის აღკვეთის, გამოძიების, გამოვლენის, დევნის ან სასჯელების აღსრულებისას პერსონალურ მონაცემთა დამუშავების და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ (მონაცემთა დაცვის ძირითადი დირექტივა), COM (2012) 10 final, ბრიუსელი, 2012 წლის 25 იანვარი.

262 ევროპული კავშირის საბჭო (2009), საბჭოს 2009 წლის 26 თებერვლის ჩარჩო გადაწყვეტილება 2009/315/JHA წევრ ქვეყნებს შორის სისხლისმართლებრივი ჩანაწერების გაცვლის დროს ამოღებული ინფორმაციის ორგანიზაციასა და შინაარსზე, OJ 2009 L 93; ევროპული კავშირის საბჭო (2000), საბჭოს 2000 წლის 17 ოქტომბრის გადაწყვეტილება 2000/642/JHA წევრი ქვეყნების ფინანსური სადაზვერვო განყოფილებების მიერ ინფორმაციის გაცვლის მხრივ კოოპერაციის თაობაზე შეთანხმება, OJ 2000 L 271.

263 ევროპული კომისია (2012), კომისიის მიმართვა ევროპულ პარლამენტსა და საბჭოს – სამართალდამცავი თანამშრომლობის გაძლიერება ევროპულ კავშირში: საინფორმაციო გაცვლის ევროპული მოდელი (EIXM), COM(2012) 735 final, ბრიუსელი, 7 დეკემბერი 2012 წელი.

საიმიგრაციო მონაცემების გაცვლას. სამართლის ეს სფერო არ მიეკუთვნება პოლიციისა და სისხლისსამართლებრივი მართლმსაჯულების სფეროს, მაგრამ მოიცავს ბევრ საკითხს, რომელიც რელევანტურია პოლიციისა და სამართალდამცავი ორგანოების საქმიანობისთვის, ასევე, საქონლის შესახებ მონაცემებისთვის, რომელიც არის ევროპულ კავშირში იმპორტირებული ან ექსპორტირებული. ევროპულ კავშირში შიდა სასაზღვრო კონტროლის გაუქმებამ გაზარდა მართლსაწინააღმდეგო ქმედების რისკი, რამაც აუცილებელი გახადა წევრი ქვეყნების მიერ თანამშრომლობის გაძლიერება, ძირითადად, საერთაშორისო საინფორმაციო გაცვლის განმტკიცებით, ცალკეული ქვეყნისა და ევროპული კავშირის საბაჟო კანონმდებლობით დადგენილი დარღვევების ეფექტური გამოვლენისთვის.

Prüm-ის გადაწყვეტილება

სახელმწიფოში შენახული მონაცემების გაცვლის საერთაშორისო ინსტიტუციური თანამშრომლობის მნიშვნელოვან მაგალითს წარმოადგენს საბჭოს გადაწყვეტილება 2008/615/JHA საერთაშორისო კოოპერაციის გაძლიერების თაობაზე, ძირითადად, ტერორიზმთან ბრძოლისა და საერთაშორისო დანაშაულის (The Prüm Decision) კუთხით, რომლითაც Prüm-ის შეთანხმება ჩართულ იქნა ევროპული კავშირის კანონმდებლობაში 2008 წელს.²⁶⁴ ეს შეთანხმება იყო პოლიციის საერთაშორისო თანამშრომლობის შეთანხმება, რომელიც 2005 წელს ხელმოწერა იქნა ავსტრიის, ბელგიის, საფრანგეთის, გერმანიის, ლუქსემბურგის, ნიდერლანდებისა და ესპანეთის მიერ.²⁶⁵

გადაწყვეტილების მიზანია ევროპული კავშირის წევრი ქვეყნების დახმარება, რათა გაუმჯობესდეს ინფორმაციის გა-

²⁶⁴ ევროპული კავშირის საბჭო (2008), საბჭოს 2008 წლის 23 ივნისის გადაწყვეტილება 2008/615/JHA საერთაშორისო თანამშრომლობის გაძლიერების თაობაზე, ტერორიზმთან ბრძოლისა და საერთაშორისო დანაშაულის (The Prüm Decision) მხრივ, OJ 2008 L 210.

²⁶⁵ კონვენცია ბელგიის სამეფოს, გერმანიის ფედერაციულ რესპუბლიკას, ესპანეთის სამეფოს, საფრანგეთის რესპუბლიკას, ლუქსემბურგის დიდ საჰერცოგოს, ნიდერლანდების სამეფოსა და ავსტრიის რესპუბლიკას შორის საერთაშორისო კოოპერაციის გაძლიერების შესახებ, ტერორიზმთან, საერთაშორისო დანაშაულთან და არალეგალურ მიგრაციასთან ბრძოლის მხრივ; ხელმისაწვდომია: <http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf>.

ზიარება დანაშაულის პრევენციისა და ბრძოლის მიზნებისთვის შემდეგ სფეროებში: ტერორიზმი, საერთაშორისო დანაშაული და არალეგალური მიგრაცია. ამ მიზნებისთვის, გადანყვეტილება ადგენს დებულებებს, რომელიც ეხება:

- დნმ-ის, თითის ანაბეჭდებისა და კონკრეტულ შიდა-სახელმწიფოებრივ სატრანსპორტო სარეგისტრაციო მონაცემებზე ავტომატიზებულ წვდომას;
- მონაცემთა მიწოდებას, რომელიც ხორციელდება გარკვეული პირობების გათვალისწინებით და გააჩნია საერთაშორისო ფარგლები;
- ინფორმაციის მიწოდებას ტერორისტული აქტების პრევენციისთვის;
- სხვა ზომებს, რომელიც აძლიერებს პოლიციის კოოპერაციას საერთაშორისო კონტექსტში.

მონაცემთა ბაზები, რომლებიც ხელმისაწვდომია Prüm-ის გადანყვეტილების ფარგლებში არის რეგულირებული მთლიანად შიდასახელმწიფოებრივი კანონმდებლობით, თუმცა მონაცემთა გაცვლა დამატებით რეგულირებულია გადანყვეტილებით და, შემდგომ, მონაცემთა დაცვის ჩარჩო გადანყვეტილებით. ამგვარ მონაცემთა გადაადგილებაზე ზედახმედველი კომპეტენტური ორგანოები არიან შიდასახელმწიფოებრივი მონაცემთა დაცვის საზედამხედველო ორგანოები.

7.2.3. მონაცემთა დაცვა Europol-სა და Eurojust-ში

Europol

ევროპული კავშირის სამართალდამცავი სააგენტოს - Europol-ის სათავეს ოფისი მდებარეობს ჰააგაში, ასევე გააჩნია შიდასახელმწიფოებრივი ერთეულები (ENUs) ევროპული კავშირის თითოეულ წევრ ქვეყანაში. Europol შეიქმნა 1998 წელს; მისი დღევანდელი სამართლებრივი სტატუსი, როგორც ევროპული კავშირის ორგანო, მოცემულია საბჭოს გადანყვეტილებით პოლიციის ევროპული სამსახურის შექმნის შესახებ (Europol-ის გადანყვეტილება).²⁶⁶ ევროპოლის მიზანია ხელი შეუწყოს ორ-

²⁶⁶ ევროპული კავშირის საბჭო (2009), საბჭოს 2009 წლის 6 აპრილის გადანყვეტილება პოლიციის ევროპული სამსახურის შექმნის თაობაზე, OJ 2009 L 121 (Europol). იხ.

განიზებული დანაშაულის, ტერორიზმისა და მნიშვნელოვანი დანაშაულის სხვა ფორმების პრევენციასა და გამოძიებას, რაც მოცემულია Europol-ის გადანყვეტილების დანართით, როდესაც ჩართულია ევროპული კავშირის ორი ან მეტი წევრი სახელმწიფო.

საკუთარი მიზნების მისაღწევად, Europol-მა დააფუძნა საინფორმაციო სისტემა, რომელიც ქმნის მონაცემთა ბაზას ევროპული კავშირის წევრი ქვეყნებისთვის დანაშაულთა დაზვერვისა და ინფორმაციის გაცვლის მიზნით, Europol-ის შიდასახელმწიფოებრივი ერთეულების მეშვეობით. საინფორმაციო სისტემა შესაძლებელია გამოყენებულ იქნეს მონაცემთა ხელმისაწვდომობისთვის, რომელიც ეხება: პირებს, რომლებიც არიან ეჭვმიტანილები ან მსჯავრდებულები დანაშაულში, რაც განეკუთვნება Europol-ის კომპეტენციას; პირებს, რომლებზეც მიიჩნევა, რომ არსებობს ფაქტიური საფუძვლები მათ მიერ დანაშაულის ჩადენის თაობაზე. Europol-ს და მის შიდასახელმწიფოებრივ ერთეულებს შეუძლიათ განახორციელონ წვდომა მონაცემებზე უშუალოდ საინფორმაციო სისტემაში და გადმოწერონ ინფორმაცია. მხოლოდ იმ პირს, რომელმაც მოახდინა მონაცემთა შეყვანა სისტემაში, შეუძლია შეცვალოს, გაასწოროს ან წაშალოს იგი.

მისი მოვალეობების შესრულებისთვის, Europol-ს შეუძლია შეინახოს, შეცვალოს და გამოიყენოს დანაშაულების შესახებ არსებული მონაცემები ანალიტიკურ სამუშაო ფაილებში. ანალიტიკური სამუშაო ფაილები გათვალისწინებულია იმ მონაცემთა შეგროვების, დამუშავების ან გამოყენებისთვის, რომელიც მიზნად ისახავს კონკრეტული დანაშაულების გამოძიების ხელშეწყობას და ხორციელდება Europol-ის მიერ ევროპული კავშირის წევრ ქვეყნებთან ერთად.

არსებული განვითარების საპაუხოდ, Europol-ში, 2013 წლის 1 იანვარს, შეიქმნა კიბერდანაშაულის ევროპული ცენტრი.²⁶⁷ იგი

ასევე, კომისიის პროექტი რეგულაციის შესახებ, რომელიც ადგენს სამართლებრივ მოწესრიგებას განახლებული Europol-ისთვის – ევროპული პოლიციის სამსახური (Europol) და ცვლის 2009 წლის 6 აპრილის საბჭოს 2009/371/JHA გადანყვეტილებით დაფუძნებულ Europol-სა და CEPOL-ს, რომელიც დაფუძნდა საბჭოს 2005/681/JHA გადანყვეტილებით პოლიციის ევროპული კოლეგიის შექმნის შესახებ, (CEPOL), COM(2013) 173 final.

267 იხ. ასევე, EDPS (2012), მონაცემთა დაცვის ზედამხედველის მოსაზრება ევროპული კომისიის მიმართვაზე საბჭოსა და ევროპული პარლამენტისთვის, კიბერდან-

ფუნქციონირებს, როგორც ევროპული კავშირის ინფორმაციული ცენტრი კიბერდანაშაულის შესახებ და წვლილი შეაქვს ონლაინ-დანაშაულებებზე სწრაფ რეაგირებაში, ასევე, ავითარებს და ნერგავს ციფრული ექსპერტიზის საშუალებებს და აწვდის საუკეთესო პრაქტიკას კიბერდანაშაულის გამოძიებებზე. ცენტრი ფოკუსირებულია კიბერდანაშაულზე, რომელიც:

- ჩადენილია ორგანიზებული ჯგუფების მიერ უკანონო დიდი შემოსავლის მიღების მიზნით, როგორიცაა ონლაინ-დანაშაულები;
- იწვევს მნიშვნელოვან ზიანს დაზარალებულისთვის, როგორიცაა ინტერნეტით ბავშვთა სექსუალური ექსპლუატაცია;
- გავლენას ახდენს ევროპულ კავშირში კრიტიკულ ინფრასტრუქტურასა და ინფორმაციულ სისტემებზე.

მონაცემთა დაცვის წესები, რომელიც ვრცელდება Europol-ზე გაძლიერებულია. Europol-ის შესახებ გადანყვეტილების 27-ე მუხლი ადგენს, რომ მოქმედებს 108-ე კონვენციით და პოლიციის შესახებ რეკომენდაციით მოცემული პრინციპები ავტომატური და არავტომატური მონაცემთა დამუშავების თაობაზე. მონაცემთა გადაცემა Europol-სა და ევროპული კავშირის წევრ ქვეყანას შორის უნდა აკმაყოფილებდეს მოთხოვნებს, რომელიც მოცემულია მონაცემთა დაცვის ჩარჩო გადანყვეტილებით.

მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის უზრუნველსაყოფად და, კერძოდ, პერსონალურ მონაცემთა დამუშავებისას ინდივიდის უფლებების დარღვევის თავიდან ასაცილებლად, Europol-ის დამოუკიდებელი საერთო საზედამხედველო ორგანო (JSB) ახორციელებს მისი საქმიანობის მონიტორინგსა და ზედამხედველობას.²⁶⁸ ნებისმიერ ინდივიდს აქვს უფლება განახორციელოს წვდომა მის შესახებ მონაცემებზე, რომელსაც ფლობს Europol-ი, დამატებით, მას აქვს უფლება მოითხოვოს აღნიშნული პერსონალური მონაცემების შემოწმება, შეცვლა ან წაშლა. თუ პირი არ ეთანხმება Europol-ის გადანყვეტილებას ამ უფლებათა რეალიზაციის თაობაზე, მას შეუძლია მიმართოს საჩივრით Europol-ის საერთო საზედამხედველო ორგანოს სააპელაციო კომიტეტს.

აშუალის ევროპული ცენტრის შექმნის თაობაზე, ბრიუსელი, 29 ივნისი 2012 წელი.

268 გადანყვეტილება Europol-ის შესახებ, 34-ე მუხლი.

თუ Europol-ის მიერ მონაცემთა შენახვის ან დამუშავების შედეგად, სამართლებრივი ან ფაქტობრივი შეცდომის გამო, დადგა ზიანი, დაზარალებულ მხარეს შეუძლია მიმართოს ზიანის ანაზღაურების მოხოვნით მხოლოდ ევროპული კავშირის წევრი ქვეყნის უფლებამოსილ სასამართლოს, სადაც დადგა ზიანის წარმომშობი ქმედება.²⁶⁹ Europol აუნაზღაურებს ზიანს ევროპული კავშირის წევრ სახელმწიფოს თუ იგი გამოწვეულია Europol-ის მიერ ვალდებულებების შეუსრულებლობით.

Eurojust

Eurojust შეიქმნა 2002 წელს და წარმოადგენს ევროპული კავშირის დაწესებულებას, რომლის სათავე ოფისი ჰააგაშია. იგი ხელს უწყობს სამართლებრივ თანამშრომლობას გამოძიებებისა და დევნის განხორციელებისას ევროპული კავშირის ორ წევრ სახელმწიფოს შორის, რომელიც ეხება მნიშვნელოვან დანაშაულებს.²⁷⁰ Eurojust უფლებამოსილია:

- ევროპის სხვადასხვა წევრ სახელმწიფოს შორის მოახდინოს გამოძიებებისა და დევნისას თანამშრომლობის ხელშეწყობა და გაუმჯობესება;
- უზრუნველყოს მოთხოვნათა და გადაწყვეტილებათა აღსრულების გამარტივება, რომელიც უკავშირდება სამართლებრივ თანამშრომლობას.

Eurojust-ის უფლებამოსილებები ხორციელდება შიდა-სახელმწიფოებრივი წევრების მიერ. ევროპული კავშირის თითოეული წევრი სახელმწიფო წარადგენს ერთ მოსამართლეს ან პროკურორს Eurojust-ში, რომელთა სტატუსი განისაზღვრე-

269 იქვე, 52-ე მუხლი.

270 ევროპული კავშირის საბჭო (2002), საბჭოს 2002 წლის 28 თებერვლის გადაწყვეტილება 2002/187/JHA მნიშვნელოვანი დანაშაულის წინააღმდეგ ბრძოლის გაძლიერებისთვის Eurojust-ის შექმნის შესახებ OJ 2002 L 63; ევროპული კავშირის საბჭო (2003), საბჭოს 2003 წლის 18 ივნისის გადაწყვეტილება 2003/659/JHA, რომელსაც შეაქვს ცვლილებები საბჭოს გადაწყვეტილებაში 2002/187/JHA მნიშვნელოვანი დანაშაულის წინააღმდეგ ბრძოლის გაძლიერებისთვის Eurojust-ის შექმნის შესახებ, OJ 2003 L 44; ევროპული კავშირის საბჭო (2009), საბჭოს 2008 წლის 16 დეკემბრის გადაწყვეტილება 2009/426/JHA Eurojust-ის გაძლიერების თაობაზე და გადაწყვეტილებაში 2002/187/JHA მნიშვნელოვანი დანაშაულის წინააღმდეგ ბრძოლის გაძლიერებისთვის Eurojust-ის შექმნის შესახებ ცვლილებების თაობაზე, OJ 2009 L 138 (გადაწყვეტილებები Eurojust-ის შესახებ).

ბა შიდასახელმწიფოებრივი კანონმდებლობის მიხედვით და აღჭურვილია აუცილებელი უფლებამოსილებით იმ დავალებების შესასრულებლად, რაც აუცილებელია სამართლებრივი თანამშრომლობის ხელშეწყობისა და გაუმჯობესებისთვის. ამასთან, Eurojust-ის სპეციალური უფლებამოსილებების შესრულებისთვის წევრები მოქმედებენ ერთობლივად, როგორც კოლეგები.

Eurojust-ს შეუძლია დაამუშავოს პერსონალური მონაცემები თუ ეს აუცილებელია მისი მიზნების მისაღწევად. თუმცა, შეგროვება შეზღუდულია კონკრეტულ ინფორმაციამდე, რომელიც ეხება ექვმიტანილ პირებს, ასევე, მათ, რომლებსაც მონაწილეობა აქვთ მიღებული ან იყვნენ ბრალდებულნი დანაშაულისთვის, რომელიც განეკუთვნება Eurojust-ის კომპეტენციას. Eurojust, ასევე, უფლებამოსილია დაამუშავოს კონკრეტული ინფორმაცია იმ დანაშაულთა მონმეების ან დაზარალებულების შესახებ, რომელიც განეკუთვნება მის კომპეტენციას.²⁷¹ გამონაკლის შემთხვევებში, Eurojust უფლებამოსილია ხანმოკლე ვადით დაამუშავოს ვრცელი პერსონალური მონაცემები, რომელიც ეხება დანაშაულებრივი ქმედების მახასიათებლებს, თუ ეს მონაცემები წარმოადგენს გადაუდებელ აუცილებლობას მიმდინარე გამოძიებისთვის. მისი უფლებამოსილების ფარგლებში, Eurojust შესაძლებელია თანამშრომლობდეს ევროპული კავშირის სხვა დაწესებულებებთან, ორგანოებთან ან სააგენტოებთან და გაცვალოს პერსონალური მონაცემები მათთან. იგი ასევე უფლებამოსილია თანამშრომლობდეს და გაცვალოს პერსონალური მონაცემები მესამე ქვეყნებთან და ორგანიზაციებთან.

მონაცემთა დაცვის კუთხით, Eurojust-მა უნდა უზრუნველყოს მონაცემთა დაცვის დონე, რომელიც სულ მცირე ექვმინტურია 108-ე კონვენციით და მისი თანმდევი ცვლილებებით დადგენილი პრინციპების. მონაცემთა გაცვლის შემთხვევაში, კონკრეტული წესები და შეზღუდვები უნდა იქნეს დადგენილი, რომელიც გათვალისწინებულია თანამშრომლობის შესახებ შეთანხმებით ან სამუშაო შეთანხმებით საბჭოს გადაწყვეტილებე-

271 საბჭოს გადაწყვეტილების 2002/187/JHA კონსოლიდირებული ვერსია საბჭოს გადაწყვეტილების 2003/659/JHA და 2009/426/JHA გათვალისწინებით, მე-15 მუხლის მე-2 პუნქტი.

ბის Eurojust-ის შესახებ და Eurojust-ის მონაცემთა დაცვის წესების შესაბამისად.²⁷²

Eurojust-ში შეიქმნა დამოუკიდებელი საერთო საზედამხებ-ველო ორგანო, რომლის მოვალეობაა Eurojust-ის მიერ წარმოებული პერსონალური მონაცემების დამუშავების მონიტორინგი. ინდივიდებს შეუძლიათ შეიტანონ საჩივარი საზედამხებველო ორგანოში თუ ისინი არ ეთანხმებიან Eurojust-ის პასუხს წვდომის, შეცვლის, დაბლოკვის ან პერსონალურ მონაცემთა წაშლის შესახებ მოთხოვნის თაობაზე. თუ Eurojust უკანონოდ დაამუშავებს პერსონალურ მონაცემებს, იგი იქნება პასუხისმგებელი ევროპული კავშირის იმ წევრი ქვეყნის შიდასახელმწიფოებრივი კანონმდებლობით, სადაც არის დაფუძნებული მისი სათავო ოფისი, კერძოდ ნიდერლანდური კანონმდებლობით, ნებისმიერი ზიანისთვის, რაც მიადგა მონაცემთა სუბიექტს.

7.2.4. მონაცემთა დაცვა ევროპული კავშირის საერთო საინფორმაციო სისტემებში

ევროპული კავშირის წევრ ქვეყნებს შორის მონაცემთა გაცვლასთან და ევროპული კავშირის სპეციალიზებულ საერთაშორისო დანაშაულის წინააღმდეგ ბრძოლის ორგანოების შექმნასთან ერთად, ევროპული კავშირის დონეზე დაფუძნდა რამოდენიმე საერთო საინფორმაციო სისტემა, რომელიც ევროპულ კავშირსა და შიდასახელმწიფოებრივ კომპეტენტურ ორგანოებს შორის წარმოადგენს პლატფორმას მონაცემთა გაცვლისათვის კანონის აღსრულების კონკრეტული მიზნებისთვის, მათ შორის, საიმეგრაციო და საბაჟო კანონმდებლობისთვის. ამ სისტემათაგან ზოგიერთმა შექმნა მრავალმხრივი შეთანხმებები, რომელიც შემდეგ სრულყოფილ იქნა ევროპული კავშირის სამართლებრივი ინსტრუმენტებითა და სისტემებით, როგორიცაა შენგენის საინფორმაციო სისტემა, სავიზო საინფორმაციო სისტემა, Eurodac, Eurosur და საბაჟო საინფორმაციო სისტემა.

ფართომასშტაბიანი ინფორმაციული ტექნოლოგიების სის-

272 Eurojust-ში პერსონალურ მონაცემთა დამუშავებისა და დაცვის შესახებ პროცედურული წესები, OJ 2005 C 68/01, 19 მარტი 2005 წელი, გვ. 1.

ტემების ევროპული სააგენტო (eu-LISA),²⁷³ დაფუძნებული 2012 წელს, პასუხისმგებელია მეორე თაობის შენგენის საინფორმაციო სისტემის (SIS II) გრძელვადიან ოპერაციულ მართვაზე, სა-ვიზო საინფორმაციო სისტემასა (VIS) და Eurodac-ზე. eu-LISA-ს ძირითადი მოვალეობაა უზრუნველყოს ინფორმაციული ტექნოლოგიების სისტემების ეფექტური, დაცული და მუდმივი ოპერირება. იგი, ასევე, პასუხისმგებელია აუცილებელი ზომების მიღებაზე, რომელიც უზრუნველყოფს სისტემებისა და მონაცემების დაცულობას.

შენგენის საინფორმაციო სისტემა

1985 წელს, ევროპული კავშირის რამოდენიმე წევრი ქვეყანა ყოფილი ევროპული გაერთიანებიდან, კერძოდ, გერმანია და საფრანგეთი, შეუერთდა შეთანხმებას ბენილუქსის ეკონომიკური კავშირის ქვეყნებთან საერთო სასაზღვრო კონტროლის თანმიმდევრული გაუქმების შესახებ (შენგენის შეთანხმება), რომელიც მიზნად ისახავდა პირების თავისუფალი გადაადგილებისთვის შეექმნა ზონა შენგენის ტერიტორიაზე, სასაზღვრო კონტროლის გარეშე.²⁷⁴ იმისათვის, რათა მომხდარიყო საზოგადოებრივი უსაფრთხოების უზრუნველყოფა, რომელიც შესაძლოა დარღვეულიყო ღია საზღვრებით, შენგენის ზონის გარე საზღვრებზე დაფუძნდა გაძლიერებული სასაზღვრო კონტროლი, ასევე, გამყარდა ახლო თანამშრომლობა შიდასახელმწიფოებრივ პოლიციასა და სამართალდამცავ ორგანოებს შორის.

შენგენის შეთანხმებაში სხვა სახელმწიფოების შესვლის გამო, შენგენის სისტემა საბოლოოდ ინტეგრირებულ იქნა ევროპული კავშირის სამართლებრივ სისტემაში ამსტერდამის ხელშეკრულების საფუძველზე.²⁷⁵ ამ გადანყვებილების იმპლე-

273 ევროპული პარლამენტისა და საბჭოს 2011 წლის 25 ოქტომბრის რეგულაცია (EU) No. 1077/2011 ფართომასშტაბიანი ინფორმაციული ტექნოლოგიების სისტემების ევროპული სააგენტოს დაფუძნების შესახებ თავისუფლების, უსაფრთხოებისა და მართლმსაჯულების სფეროში, OJ 2011 L 286.

274 შეთანხმება ბენილუქსის ეკონომიკური კავშირის ქვეყნების მთავრობას, გერმანიის ფედერაციულ რესპუბლიკასა და საფრანგეთის რესპუბლიკას შორის საერთო საზღვრებზე შემონების თანმიმდევრული გაუქმების შესახებ, OJ 2000 L 239.

275 ევროპული გაერთიანება (1997), ამსტერდამის ხელშეკრულება, რომელსაც ცვლილება შეაქვს ევროპული კავშირის ხელშეკრულებაში, ევროპული გაერთიანების შექმნისა და დაკავშირებულ აქტებში, OJ 1997 C 340.

მენტაცია განხორციელდა 1999 წელს. შენგენის საინფორმაციო სისტემის უახლესი ვერსია, ე.წ. SIS II, ამოქმედდა 2013 წლის 9 აპრილს. ამჟამად, იგი ემსახურება ევროპული კავშირის ყველა წევრ ქვეყანას, ასევე, ისლანდიას, ლიხტენშტაინს, ნორვეგიასა და შვეიცარიას.²⁷⁶ Europol-სა და Eurojust-ს, ასევე, წვდომა აქვთ SIS II-თან.

SIS II შედგება ცენტრალური სისტემისგან (C-SIS), შიდასახელმწიფოებრივი სისტემისგან (N-SIS) ევროპული კავშირის თითოეულ წევრ ქვეყანაში და საკომუნიკაციო ინფრასტრუქტურისგან ცენტრალურ სისტემასა და შიდასახელმწიფოებრივ სისტემას შორის. C-SIS მოიცავს ევროპული კავშირის წევრი სახელმწიფოების მიერ შეყვანილ კონკრეტულ მონაცემებს პირებისა და ობიექტების შესახებ. C-SIS გამოიყენება შიდასახელმწიფოებრივი სასაზღვრო კონტროლის, პოლიციის, საბაჟო, სავიზო და სამართალდაცავი ორგანოების მიერ შენგენის ზონის ფარგლებში. ევროპული კავშირის თითოეულ წევრ ქვეყანაში ფუნქციონირებს C-SIS-ის შიდასახელმწიფოებრივი ასლი, ცნობილი როგორც შენგენის შიდასახელმწიფოებრივი საინფორმაციო სისტემა (N-SIS). იგი მუდმივად განახლებადია და, თავის მხრივ, ანახლებს C-SIS-საც. N-SIS-თან წვდომა დაიშვება და აუცილებელია შემდეგ შემთხვევებში:

- პირს არ აქვს უფლება შევიდეს ან დარჩეს შენგენის ტერიტორიაზე; ან
- პირი ან ობიექტი არის ძებნაში კანონის აღმასრულებელი ან სამართალდამცავი ორგანოების მიერ; ან
- პირი დაკარგულად იქნა გამოცხადებული; ან
- საქონელი, როგორცაა ბანკნოტები, ავტომანქანები, სატვირთოები, იარაღი და საიდენტიფიკაციო დოკუმენტები, აღიარებული იქნა მოპარულად ან დაკარგულ საკუთრებად.

შესაბამისი შემთხვევის არსებობისას, შენგენის შიდასახელ-

²⁷⁶ 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 ევროპული კავშირის საბჭო (2007), საბჭოს 2007 წლის 12 ივნისის გადაწყვეტილება 2007/533/JHA შენგენის საინფორმაციო სისტემის მეორე თაობის შექმნის, ოპერირებისა და გამოყენების თაობაზე, (SIS II), OJ 2007 L 205.

მნიფობრივი საინფორმაციო სისტემის მეშვეობით მიიღება თანმდევი მოქმედებები.

SIS II-ს გააჩნია ახალი ფუნქციები, როგორცაა შესაძლებლობა შეყვანილ იქნეს: ბიომეტრიული მონაცემები – თითის ანაბეჭდი და ფოტოსურათი; ასევე, ახალი კატეგორიები, როგორცაა მოპარული ნავეები, მფრინავი საშუალებები, კონტეინერები ან გადახდის საშუალებები; გაძლიერებული დაცვა პირებსა და ობიექტებზე; დაკავების ევროპული ბრძანების (EAW) ასლები ძებნილი პირების დაკავების, ჩაბარებისა და ექსტრადირებისთვის.

საბჭოს გადანყვეტილება 2007/533/JHA შენგენის საინფორმაციო სისტემის მეორე თაობის შექმნის, ოპერირებისა და გამოყენების შესახებ (გადანყვეტილება შენგენი II) ახდენს 108-ე კონვენციის იმპლემენტირებას: „ამ გადანყვეტილების გამოყენებისას დამუშავებული პერსონალური მონაცემები იქნება დაცული ევროპის საბჭოს 108-ე კონვენციის მიხედვით.“²⁷⁷ როდესაც პერსონალური მონაცემები გამოიყენება შიდასახელმწიფობრივი პოლიციის ორგანოების მიერ შენგენი II-ის გადანყვეტილების საფუძველზე, 108-ე კონვენციის დებულებები, ისევე როგორც რეკომენდაცია პოლიციის მონაცემთა შესახებ, უნდა იქნეს იმპლემენტირებული შიდასახელმწიფობრივი კანონმდებლობით.

ევროპული კავშირის თითოეულ წევრ ქვეყანაში არსებული კომპეტენტური საზედამხედველო ორგანო მართავს ადგილობრივ N-SIS-ს. ძირითადად, უნდა შემონმდეს ევროპული კავშირის წევრი ქვეყნის მიერ შეყვანილი მონაცემის ხარისხი N-SIS-ის მეშვეობით C-SIS-ში. საზედამხედველო ორგანომ უნდა უზრუნველყოს მონაცემთა დამუშავების ოპერაციათა აუდიტი ადგილობრივ N-SIS-ში ოთხ წელიწადში ერთხელ მაინც. შიდასახელმწიფობრივი საზედამხედველო ორგანოები და EDPS თანამშრომლობენ SIS-ის კოორდინირებული ზედამხედველობის უზრუნველსაყოფად, მაშინ, როდესაც EDPS პასუხისმგებელია C-SIS-ის ზედამხედველობაზე. გამჭვირვალობის უზრუნველსაყოფად, ქმედებათა საერთო ანგარიში უნდა იქნეს გაგზავნილი

277 ევროპული კავშირის საბჭო (2007), საბჭოს 2007 წლის 12 ივნისის გადანყვეტილება 2007/533/JHA შენგენის საინფორმაციო სისტემის მეორე თაობის შექმნის, ოპერირებისა და გამოყენების შესახებ, OJ 2007 L 205, 57-ე მუხლი.

ევროპული პარლამენტის, საბჭოსა და eu-LISA-სთვის ყოველ ორ ნელინადში ერთხელ.

ინდივიდების წვდომის უფლებები, რომელიც ეხება SIS II-ს შესაძლებელია რეალიზებულ იქნეს ევროპული კავშირის ნებისმიერ წევრ ქვეყანაში, რამდენადაც ყოველი N-SIS არის C-SIS-ის ზუსტი ასლი.

მაგალითი: საქმეზე *Dalea v. France*,²⁷⁸ განმცხადებელს უარი ეთქვა ვიზის გაცემაზე საფრანგეთში ვიზიტისთვის, რამდენადაც საფრანგეთის შესაბამის ორგანოებს შეტანილი ჰქონდათ ინფორმაცია შენგენის საინფორმაციო სისტემაში შესვლაზე მისთვის უარის გაცხადების შესახებ. განმცხადებლის მიერ ამ მონაცემთა წვდომის, შეცვლის ან წაშლის მოითხოვნა არ დაკმაყოფილდა საფრანგეთის მონაცემთა დაცვის კომისიის მიერ და, საბოლოოდ, სახელმწიფო საბჭოს წინაშე. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ განმცხადებლის შესახებ ჩანაწერი შენგენის საინფორმაციო სისტემაში შესაბამისობაში იყო კანონმდებლობასთან და ემსახურებოდა ეროვნული უსაფრთხოების დაცვის ლეგიტიმურ მიზანს. რამდენადაც განმცხადებელმა ვერ დაასაბუთა ზიანის რეალური მიღება შენგენის ზონაში შესვლაზე უარის თქმის გამო და, რამდენადაც საკმარისი ზომები იქნა მიღებული დაუსაბუთებელი გადაწყვეტილებებისგან დასაცავად, მისი პირადი ცხოვრების დაცვის უფლებაში ჩარევა იყო პროპორციული, შესაბამისად, განმცხადებლის საჩივარი მე-8 მუხლის საფუძველზე დაუშვებლად იქნა აღიარებული.

სავიზო საინფორმაციო სისტემა

სავიზო საინფორმაციო სისტემა (VIS), რომელიც მართულია eu-LISA-ს მიერ, შეიქმნა ევროპული კავშირის საერთო სავიზო პოლიტიკის იმპლემენტირების ხელშეწყობისთვის.²⁷⁹ VIS საშუა-

²⁷⁸ ადამიანის უფლებათა ევროპული სასამართლო, *Dalea v. France* (dec.), No. 964/07, 2 თებერვალი 2010 წელი.

²⁷⁹ ევროპული კავშირის საბჭო (2004), საბჭოს 2004 წლის 8 ივნისის გადაწყვეტილება სავიზო საინფორმაციო სისტემის (VIS) შექმნის შესახებ, OJ 2004 L 213; ევროპული პარლამენტისა და საბჭოს 2008 წლის 9 ივლისის რეგულაცია (EC) No. 767/2008 სავიზო საინფორმაციო სისტემისა (VIS) და წევრ ქვეყნებს შორის მოკლევადიანი ვიზების თაობაზე მონაცემთა გაცვლის შესახებ, OJ 2008 L 218 (VIS Regulation); ევროპული კავშირის საბჭო (2008), საბჭოს 2008 წლის 23 ივნისის გადაწყვეტილება 2008/633/JHA წევრი ქვეყნებისა და Europol-ის მიერ განსაზღვრული უფლებამოსილი ორგანოების მიერ სავიზო საინფორმაციო სისტემასთან (VIS) წვდომის შესახებ ტერორისტული ქმედებებისა და სხვა მნიშვნელოვანი დანაშაულებრივი ქმედებების პრევენციის, გამოვლენისა და გამოძიების მიზნებისთვის, OJ 2008 L 218.

ლებას აძლევს შენგენის სახელმწიფოებს გაცვალონ სავიზო მონაცემები სისტემის მეშვეობით, რომელიც აკავშირებს შენგენის ქვეყნების ევროპული კავშირის არაწევრ ქვეყანაში მდებარე საკონსულოებსა და შენგენის გარე სასაზღვრო კვეთის კონტროლის პუნქტებს – შენგენის ყველა ქვეყანაში. VIS ამუშავებს მონაცემებს, რომელიც ეხება მოკლევადიან სავიზო განაცხადებს შენგენის ზონაში ვიზიტისთვის ან ტრანზიტული გავლის მიზნით. VIS საშუალებას აძლევს სასაზღვრო ორგანოებს, ბიომეტრიული მონაცემების მეშვეობით, განსაზღვრონ არის თუ არა ვიზის წარმდგენი პირი მისი მართლზომიერი მფლობელი და მოახდინონ პირების იდენტიფიცირება დოკუმენტების არ ქონის ან მათი გაყალბების შემთხვევაში.

ევროპული პარლამენტისა და საბჭოს სავიზო საინფორმაციო სისტემისა (VIS) და ევროპული კავშირის წევრ ქვეყნებს შორის მოკლევადიანი ვიზების თაობაზე მონაცემთა გაცვლის შესახებ რეგულაციის (EC) No. 767/2008 (VIS რეგულაცია) თანახმად, მხოლოდ განმცხადებლის მონაცემები, მისი ვიზები, ფოტოსურათები, თითის ანაბეჭდები, კავშირები წინა განაცხადებთან და მათი თანმხლები პირების საგანაცხადო ფალები შეიძლება იქნეს შენახული VIS-ში.²⁸⁰ VIS-თან წვდომა მონაცემთა შეყვანის, შეცვლის ან წაშლის მიზნით დასაშვებია მხოლოდ ევროპული კავშირის წევრი ქვეყნების სავიზო ორგანოებისთვის გარე სასაზღვრო კვეთის წერტილებში შემოწმებისთვის, საიმიგრაციო და თავშესაფრის კონტროლისთვის. კონკრეტული პირობების გათვალისწინებით, შიდასახელმწიფოებრივი პოლიციის კომპეტენტურმა ორგანოებმა და Europol-მა შეიძლება მოითხოვოს VIS-ში შეყვანილ მონაცემებზე წვდომა ტერორისტული და დანაშაულებრივი ქმედებების პრევენციის, გამოვლენის და გამოძიების მიზნებისთვის.²⁸¹

280 ევროპული პარლამენტისა და საბჭოს 2008 წლის 9 ივლისის რეგულაცია (EC) No. 767/2008 სავიზო საინფორმაციო სისტემისა (VIS) და წევრ ქვეყნებს შორის მოკლევადიანი ვიზების თაობაზე მონაცემთა გაცვლის შესახებ, OJ 2008 L 218 (VIS Regulation).

281 ევროპული კავშირის საბჭო (2008), საბჭოს 2008 წლის 23 ივნისის გადანაცვლებით 2008/633/JHA წევრი ქვეყნებისა და Europol-ის მიერ განსაზღვრული უფლებამოსილი ორგანოების მიერ სავიზო საინფორმაციო სისტემასთან (VIS) წვდომის შესახებ ტერორისტული ქმედებებისა და სხვა მნიშვნელოვანი დანაშაულებრივი ქმედებების პრევენციის, გამოვლენისა და გამოძიების მიზნებისთვის, OJ 2008 L 218.

Eurodac

Eurodac-ის სახელწოდება ეხება დაქტილოგრამებს ანუ თითის ანაბეჭდებს. ეს არის ცენტრალიზებული სისტემა, რომელიც მოიცავს მესამე ქვეყნების მცხოვრებთა თითის ანაბეჭდებს, რომლებმაც თავშესაფრის მოთხოვნით მიმართეს ევროპული კავშირის ერთ-ერთ წევრ ქვეყანას.²⁸² სისტემა ფუნქციონირებს 2003 წლის იანვრიდან და მისი მიზანია დაეხმაროს წევრ ქვეყნებს იმის განსაზღვრაში, თუ რომელი მათგანი არის ვალდებული განიხილოს კონკრეტული განაცხადი თავშესაფრის თაობაზე საბჭოს 343/2003 რეგულაციის მიხედვით, რომელიც ადგენს კრიტერიუმებს და მექანიზმებს თავშესაფრის განაცხადის განხილვაზე პასუხისმგებელი წევრი ქვეყნის განსაზღვრისთვის თუ მოთხოვნა შეტანილია ევროპული კავშირის ერთ-ერთ წევრ ქვეყანაში მესამე ქვეყანაში მცხოვრები პირის მიერ (რეგულაცია დუბლინი II).²⁸³ Eurodac-ში არსებული პერსონალური მონაცემები შესაძლებელია გამოყენებულ იქნეს მხოლოდ დუბლინი II რეგულაციის გამოყენების გამარტივების მიზნით, ნებისმიერი სხვა გამოყენება ექვემდებარება სანქციებს.

Eurodac შედგება ცენტრალური განყოფილებისგან, მართული eu-LISA-ს მიერ, თითის ანაბეჭდის შენახვისა და შედარებისთვის, ასევე, ელექტრონული მონაცემთა გადაცემის სისტემისგან ევროპული კავშირის წევრ ქვეყნებს შორის და ცენტრალური მონაცემთა ბაზისგან. წევრი ქვეყნები იღებენ და ინახავენ, სულ მცირე, 14 წლის მანძილზე, ევროპული კავშირის თითოეული არარეზიდენტის ან მოქალაქეობის არ მქონე პირის თითის ანაბეჭდებს, რომლებიც ითხოვენ თავშესაფარს გარე საზღ-

282 საბჭოს 2000 წლის 11 დეკემბრის რეგულაცია (EC) No. 2725/2000 Eurodac-ის შექმნის თაობაზე თითის ანაბეჭდების შედარებისთვის დუბლინის კონვენციის ეფექტური მოქმედების მიზნით, OJ 2000 L 316; საბჭოს 2002 წლის 28 თებერვლის რეგულაცია (EC) No. 407/2002 კონკრეტული წესების განსაზღვრის შესახებ რეგულაციის (EC) No. 2725/2000 - Eurodac-ის შექმნის თაობაზე თითის ანაბეჭდების შედარებისთვის დუბლინის კონვენციის ეფექტური მოქმედების მიზნით - იმპლემენტირებისთვის, OJ 2002 L 62 (Eurodac-ის რეგულაციები).

283 საბჭოს 2003 წლის 18 თებერვლის რეგულაცია (EC) No. 343 თავშესაფრის განაცხადის განხილვაზე პასუხისმგებელი წევრი ქვეყნის დადგენის კრიტერიუმებისა და მექანიზმების განსაზღვრის თაობაზე, როდესაც მოთხოვნა შეტანილია ერთ-ერთ წევრ ქვეყანაში მესამე ქვეყანაში მცხოვრები პირის მიერ, OJ 2003 L 50 (რეგულაცია Dublin II).

ვრებთან. ევროპული კავშირის წევრ ქვეყნებს, ასევე, შეუძლიათ ევროპული კავშირის არაწევრი მოქალაქეების ან მოქალაქეობის არ მქონე პირთა თითის ანაბეჭდების გადაცემა, რომლებიც დარჩნენ ტერიტორიაზე შესაბამისი ნებართვის გარეშე.

თითის ანაბეჭდების მონაცემები შენახულია Eurodac-ის მონაცემთა ბაზაში მხოლოდ ფსევდონიმირებული ფორმით. დამთხვევის შემთხვევაში, ფსევდონიმი, იმ ქვეყნის სახელწოდებასთან ერთად, რომელმაც პირველად შეიყვანა თითის ანაბეჭდის მონაცემები, ხელმისაწვდომი ხდება მეორე წევრი ქვეყნისთვის. ამის შემდეგ, მეორე წევრი ქვეყანა მიმართავს პირველს, ვინაიდან, დუბლინი II რეგულაციით, პირველი წევრი ქვეყანა ვალდებულია დაამუშავოს თავშესაფრის შესახებ განაცხადი.

პერსონალური მონაცემები, რომელიც შენახულია Eurodac-ში და ეხება თავშესაფრის მომთხოვნებს შენახულია 10 წლით, იმ თარიღიდან, როდესაც თითის ანაბეჭდები იქნა აღებული, გარდა იმ შემთხვევისა თუ მონაცემთა სუბიექტი მიიღებს ევროპული კავშირის წევრი ქვეყნის მოქალაქეობას. ამ შემთხვევაში, მონაცემები დაუყოვნებლივ უნდა წაიშალოს. მონაცემები, რომელიც ეხება უცხოელ მოქალაქეებს, დაკავებულებს გარე საზღვრის უნებართვო გადაკვეთისთვის, შენახულია ორი წლით. ეს მონაცემები უნდა იქნეს დაუყოვნებლივ წაშლილი თუ მონაცემთა სუბიექტი მიიღებს ბინადრობის ნებართვას, დატოვებს ევროპული კავშირის ტერიტორიას ან მიიღებს ევროპული კავშირის წევრი ქვეყნის მოქალაქეობას.

ევროპული კავშირის ყველა წევრ ქვეყანასთან ერთად, ისლანდია, ნორვეგია, ლიხტენშტაინი და შვეიცარია, ასევე, მიმართავს Eurodac-ს საერთაშორისო შეთანხმებების საფუძველზე.

Eurosur

ევროპული სასაზღვრო სათვალთვალო სისტემა (Eurosur)²⁸⁴ შექმნილია შენგენის გარე საზღვრების კონტროლის გაძლიერებისთვის, არალეგალური მიგრაციისა და საერთაშორისო დანაშაულის გამოვლენის, პრევენციისა და მის წინააღმდეგ

284 ევროპული პარლამენტისა და საბჭოს 2013 წლის 22 ოქტომბრის რეგულაცია (EU) No. 1052/2013 ევროპული სასაზღვრო სათვალთვალო სისტემის შექმნის თაობაზე (Eurosur), OJ 2013 L 295.

ბრძოლისთვის. იგი მოქმედებს საინფორმაციო გაცვლისა და ოპერაციული კოოპერაციის გაძლიერებისთვის შიდასახელმწიფოებრივ საკოორდინაციო ცენტრებსა და ევროპული კავშირის სააგენტოს – Frontex-ს შორის, რომელსაც ევალება ინტეგრირებული სასაზღვრო მართვის ახალი კონცეფციების შემუშავება და ამოქმედება.²⁸⁵ მისი ძირითადი მიზნებია:

- ევროპულ კავშირში აღურიცხავად შესული არალეგალი მიგრანტების რაოდენობის შემცირება;
- არალეგალი მიგრანტების სიკვდილიანობის რაოდენობის შემცირება, ზღვაში მეტი სიცოცხლის გადასარჩენად;
- ევროპული კავშირის შიდა უსაფრთხოების ერთიანი გაძლიერება, საერთაშორისო დანაშაულის პრევენციის მეშვეობით.²⁸⁶

ორგანომ საქმიანობა დაიწყო 2013 წლის 2 დეკემბერს ევროპული კავშირის გარე საზღვრის მქონე ყველა წევრ ქვეყანაში და დაიწყებს 2014 წლის 1 დეკემბრიდან სხვა წევრ ქვეყნებშიც. რეგულაცია გავრცელდება წევრი ქვეყნების მიწის, ზღვის გარე საზღვრებისა და საჰაერო საზღვრების თვალთვალზე.

საბაჟო საინფორმაციო სისტემა

მორიგი მნიშვნელოვანი საერთო საინფორმაციო სისტემა, რომელიც შექმნილია ევროპული კავშირის დონეზე არის საბაჟო საინფორმაციო სისტემა (CIS).²⁸⁷ შიდა ბაზრის შექმნის პრო-

285 ევროპული პარლამენტისა და საბჭოს 2011 წლის 25 ოქტომბრის რეგულაცია (EU) No. 1168/2011, რომელსაც ცვლილება შეაქვს საბჭოს რეგულაციაში (EC) No. 2007/2004 ევროპული კავშირის წევრი ქვეყნების გარე საზღვრებთან მართვისა და ოპერაციული თანამშრომლობის ევროპული სააგენტოს შექმნის შესახებ, OJ 2011 L 394 (Frontex რეგულაცია).

286 იხ. ასევე, ევროპული კომისია (2008), ევროპული კომისიის მიმართვა ევროპული პარლამენტის, საბჭოს, ევროპული ეკონომიკური და სოციალური კომიტეტისა და რეგიონული კომიტეტის მიმართ: ევროპული სასაზღვრო სათვალთვალ სისტემის (Eurosur) შექმნის განხილვა, COM(2008) 68 final, ბრიუსელი, 13 თებერვალი 2008 წელი; ევროპული კომისია (2011), ევროპული პარლამენტისა და საბჭოს ევროპული სასაზღვრო სათვალთვალ სისტემის (Eurosur) შექმნის თაობაზე რეგულაციის პროექტის გავლენის შეფასება, შიდა სამუშაო დოკუმენტი, SEC(2011) 1536 final, ბრიუსელი, 12 დეკემბერი 2011 წელი, გვ. 18.

287 ევროპული კავშირის საბჭო (1995), საბჭოს 1995 წლის 26 ივლისის აქტი საბაჟო მიზნებისთვის ინფორმაციული ტექნოლოგიების თაობაზე კონვენციის შექმნის შესახებ, OJ 1995 C 316, რომელიც შეცვლილია ევროპული კავშირის საბჭოს მიერ (2009),

ცესში გაუქმდა ყოველი შემონმება და ფორმალობა, რომელიც უკავშირდებოდა ევროპული კავშირის ტერიტორიაზე მოძრავ საქონელს, რამაც გაზრდა დანაშაულებრივი ქმედების რისკი. ეს რისკი დაბალნასებულ იქნა ევროპული კავშირის ქვეყნების საბაჟო ადმინისტრაციებს შორის ინტენსიური თანამშრომლობით. CIS-ის მიზანია ხელი შეუწყოს ევროპული კავშირის ქვეყნებს ევროპული კავშირის საბაჟო და აგრარული კანონმდებლობის მნიშვნელოვანი დარღვევების პრევენციაში, გამოძიებასა და დევნაში.

ინფორმაცია, რომელიც განთავსებულია CIS-ში მოიცავს საქონელთან, ტრანსპორტირების საშუალებებთან, საწარმოებთან, პირებთან, საქონელთან, ამოღებულ ან ჩამორთმეულ ფულთან დაკავშირებულ პერსონალურ მონაცემებს. ეს ინფორმაცია შესაძლებელია გამოყენებულ იქნეს მხოლოდ დათვალიერების, ანგარიშგების ან კონკრეტული შემონმების ჩატარების დროს ან სტრატეგიული და ოპერაციული ანალიზისას, რომელიც უკავშირდება საბაჟო წესების დარღვევაში ეჭვმიტანილ პირებს.

CIS-თან წვდომა შეუძლია შიდასახელმწიფოებრივ საბაჟო, საგადასახადო, აგრარულ, საზოგადოებრივი ჯანდაცვისა და პოლიციის ორგანოებს, ასევე, Europol-სა და Eurojust-ს.

პერსონალურ მონაცემთა დამუშავება თანხვედრაში უნდა იყოს 515/97 რეგულაციისა CIS-ის კონვენციის²⁸⁸ მიერ დადგენილ კონკრეტულ წესებთან, ისევე, როგორც მონაცემთა დაცვის დირექტივასთან, ევროპული კავშირის დაწესებულებათა მონაცემთა დაცვის რეგულაციასთან, 108-ე კონვენციასთან და პოლიციის შესახებ რეკომენდაციის დებულებებთან. EDPS პასუხისმგებელია CIS-ის შესაბამისობის ზედამხედველობაზე 45/2001 რეგულაციის დებულებებთან და იწვევს კრებას წელიწადში ერთხელ მაინც, მონაცემთა დაცვის ყველა იმ შიდასახელმწიფოებრივი საზედამხედველო ორგანოების მონაწილეობით, რომლებსაც გააჩნიათ უფლებამოსილება CIS-თან დაკავშირებულ საზედამხედველო საკითხებში.

1997 წლის 13 მარტის რეგულაცია No. 515/97 წევრი ქვეყნების ადმინისტრაციული ორგანოების ურთიერთდახმარებისა და წევრ ქვეყნებსა და კომისიას შორის თანამშრომლობის შესახებ, საბაჟო და აგრარულ სფეროში კანონმდებლობის სწორი მოქმედების უზრუნველსაყოფად, საბჭოს 2009 წლის 30 ნოემბრის გადაწყვეტილება 2009/917/JHA საბაჟო მიზნებისთვის ინფორმაციული სისტემების გამოყენების თაობაზე, OJ 2009 L 323 (CIS გადანაცვტილება).

288 ibid.

8. მონაცემთა დაცვის სხვა სპეციალური ევროპული კანონები

ევროპული კავშირი	განხილული საკითხები	ევროპის საბჭო
მონაცემთა დაცვის დირექტივა დირექტივა პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ	ელექტრონული კომუნიკაციები	108-ე კონვენცია რეკომენდაცია სატელეკომუნიკაციო სერვისების შესახებ
მონაცემთა დაცვის დირექტივა, მე-8 მუხლის მე-2 პუნქტის -b- ქვეპუნქტი	შრომითი ურთიერთობები	108-ე კონვენცია რეკომენდაცია დასაქმების შესახებ აღამიანის უფლებათა ევროპული სასამართლო, Copland v. the United Kingdom, No. 62617/00, 3 აპრილი 2007 წელი
მონაცემთა დაცვის დირექტივა, მე-8 მუხლის მე-3 პუნქტი	სამედიცინო მონაცემები	108-ე კონვენცია რეკომენდაცია სამედიცინო მონაცემების შესახებ აღამიანის უფლებათა ევროპული სასამართლო, Z. v. Finland, No. 22009/93, 25 თებერვალი 1997 წელი
დირექტივა კლინიკური ცდების შესახებ	კლინიკური ცდები	
მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის -b- ქვეპუნქტი, მე-13 მუხლის მე-2 პუნქტი	სტატისტიკა	108-ე კონვენცია რეკომენდაცია სტატისტიკის მონაცემთა შესახებ
რეგულაცია (EC) No. 223/2009 ევროპული სტატისტიკის შესახებ მართლმსაჯულების ევროპული კავშირის სასამართლო, C-524/06, Huber v. Germany, 16 დეკემბერი 2008 წელი	ოფიციალური სტატისტიკა	108-ე კონვენცია რეკომენდაცია სტატისტიკის მონაცემთა შესახებ

დირექტივა 2004/39/EC ფინანსური ინსტრუმენტებში არსებული ბაზრის შესახებ რეგულაცია (EU) No. 648/2012 OTC დერივატივების, ცენტრალური მხარეებისა და სავაჭრო საცაგების შესახებ რეგულაცია (EC) No. 1060/2009 საკრედიტო სარეგულირგო სააგენტოების შესახებ დირექტივა 2007/64/EC შიდა ბაზარზე არსებული საგადახდო სერვისების შესახებ	ფინანსური მონაცემები	108-ე კონვენცია რეკომენდაცია 90(19) გადახდებისა და სხვა დაკავშირებული ოპერაციების გამოყენების შესახებ ადამიანის უფლებათა ევროპული სასამართლო, Michaud v. France, No. 12323/11, 6 დეკემბერი 2012 წელი
---	------------------------------------	---

ზოგიერთ სფეროში, ევროპის მასშტაბით შემუშავდა სპეციალური სამართლებრივი ინსტრუმენტები, რომელიც დეტალურად განაწარმოებს 108-ე კონვენციისა და მონაცემთა დაცვის დირექტივის ძირითად წესებს კონკრეტულ შემთხვევებზე.

8.1. ელექტრონული კომუნიკაციები

საკანძო დებულებები

- სატელეკომუნიკაციო სექტორში მონაცემთა დაცვის სპეციალური ინსტრუმენტები, ძირითადად სატელეფონო მომსახურებებთან დაკავშირებით, მოცემულია 1995 წლის ევროპის საბჭოს რეკომენდაციაში.
- პერსონალურ მონაცემთა დამუშავება, რომელიც ეხება ევროპული კავშირის დონეზე საკომუნიკაციო მომსახურებათა წარმოებას რეგულირებულია დირექტივით პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ.
- ელექტრონული კომუნიკაციების კონფიდენციალურობა ვრცელდება არა მხოლოდ კომუნიკაციის შინაარსზე, არამედ ტრაფიკის მონაცემებზე, როგორცაა ინფორმაცია იმის თაობაზე, თუ ვინ ვის დაუკავშირდა, როდის და რა ხანგრძლივობით, და, ასევე მონაცემებზე ადგილმდებ-

ბარეობის შესახებ, როგორცაა მონაცემთა გადაცემის სანყისი ადგილმდებარეობა.

საკომუნიკაციო ქსელები შეიცავს მომხმარებელთა პერსონალურ სფეროში არამართლზომიერი ჩარევის მომეტებულ რისკს, რამდენადაც გამოიყენება დამატებითი ტექნიკური შესაძლებლობები მოსმენებისთვის და ამგვარ ქსელებში განხორციელებული კომუნიკაციის თავლთვალისთვის. შესაბამისად, მონაცემთა დაცვის სპეციალური რეგულაციები აუცილებლობად იქნა მიჩნეული იმ რისკების წინააღმდეგ, რაც წარმოშობილია საკომუნიკაციო მომსახურების მომხმარებლებისთვის.

1995 წელს ევროპის საბჭომ გამოსცა რეკომენდაცია მონაცემთა დაცვის შესახებ სატელეკომუნიკაციო სფეროში, რომელიც, ძირითადად, ეხებოდა სატელეფონო მომსახურებებს.²⁸⁹ ამ რეკომენდაციის თანახმად, სატელეკომუნიკაციო სფეროში პერსონალურ მონაცემთა შეგროვებისა და დამუშავების მიზნები უნდა ეხებოდეს მხოლოდ: მომხმარებელს, რომელიც მიერთებულია ქსელთან კონკრეტული სატელეკომუნიკაციო მომსახურებების ხელმისაწვდომობის მიზნით, გადახდის, დამონების, ოპტიმალური ტექნიკური ოპერაციების უზრუნველსაყოფად, ქსელისა და მომსახურების განსავითარებლად.

განსაკუთრებული ყურადღება დაეთმო საკომუნიკაციო ქსელების გამოყენებით პირდაპირი მარკეტინგის შემცველი შეტყობინებების გაგზავნას. ზოგადად, პირდაპირი მარკეტინგის შემცველი შეტყობინებები არ უნდა იქნეს გაგზავნილი იმ მომხმარებლისთვის, რომელმაც აშკარა უარი განაცხადა სარეკლამო შეტყობინებების მიღებაზე. ავტომატიზებული ზარის განმახორციელებელი მოწყობილობები, რომელიც განკუთვნილია წინასწარ ჩანერილი საკრელამო შეტყობინებების გაგზავნისთვის, შესაძლებელია გამოყენებულ იქნეს მხოლოდ მაშინ, თუ მომხმარებელმა გასცა მკაფიო თანხმობა. შიდასახელმწიფოებრივი კანონმდებლობა ამ სფეროში უნდა განსაზღვრავდეს დეტალურ ნესებს.

რაც შეეხება ევროპული კავშირის საკანონმდებლო მოწეს-

289 ევროპის საბჭო, მინისტრთა კომიტეტი (1995), რეკომენდაცია Rec(95)4 წევრი ქვეყნებისთვის სატელეკომუნიკაციო მომსახურების, ძირითადად, სატელეფონო მომსახურების სფეროში პერსონალურ მონაცემთა დაცვის შესახებ, 7 თებერვალი 1995 წელი.

რიგებას, 1997 წელს პირველი მცდელობის შემდეგ, 2002 წელს მიღებულ იქნა დირექტივა პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ და შეიცვალა 2009 წელს, მონაცემთა დაცვის დირექტივის იმ დებულებების მხარდაჭერისა და დაკონკრეტებისთვის, რომელიც ეხება სატელეკომუნიკაციო სექტორს.²⁹⁰ პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ დირექტივის მოქმედება შეზღუდულია საჯარო ელექტრონული ქსელების მეშვეობით საკომუნიკაციო მომსახურებაზე.

დირექტივა პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ განასხვავებს სამი სახის მონაცემთა კატეგორიას, რომელიც შეგროვებულია კომუნიკაციის პროცესში:

- მონაცემები, რომელიც შეიცავს კომუნიკაციის პროცესში გაგზავნილი შეტყობილებების შინაარსს; ეს მონაცემები არის მკაცრად კონფიდენციალური;
- მონაცემები, რომელიც აუცილებელია კომუნიკაციის წარმოშობისა და მიმდინარეობისთვის, ე.წ. ტრაფიკის მონაცემები, როგორიცაა ინფორმაცია კომუნიკაციის მხარეებს შორის, კომუნიკაციის დრო და ხანგრძლივობა;
- ტრაფიკის მონაცემებს შორის არსებობს მონაცემები, რომელიც უშუალოდ ეხება საკომუნიკაციო მოწყობილობის ადგილმდებარეობას, ე.წ. ადგილმდებარეობის შესახებ მონაცემები; ეს, ამავდროულად, არის საკომუნიკაციო მოწყობილობების მომხმარებელთა ადგილსამყოფელის შესახებ არსებული მონაცემები, რაც კავშირშია მობილური კავშირგაბმულობის მოწყობილობის მომხმარებლებთან.

ტრაფიკის მონაცემები შესაძლებელია გამოყენებულ იქნეს

290 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 ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ), რომელიც შეცვლილ იქნა ევროპული პარლამენტისა და საბჭოს 2009 წლის 25 ნოემბრის დირექტივით 2009/136/EC, რომელიც ცვლის დირექტივას 2002/22/EC უნივერსალური მომსახურებისა და ელექტრონულ საკომუნიკაციო ქსელებსა და მომსახურებებთან დაკავშირებული მომხმარებლების უფლებების შესახებ და რეგულაციას (EC) No. 2006/2004 მომხმარებელთა დაცვის კანონმდებლობის მოქმედებაზე პასუხისმგებელი შიდასახელმწიფოებრივი ორგანოების თანამშრომლობის შესახებ, OJ 2009 L 337.

სერვისის მიმწოდებლის მიერ მხოლოდ ანგარიშსწორების და მომსახურების ტექნიკური მხარდაჭერის მიზნებისთვის. მონაცემთა სუბიექტის თანხმობით, ეს მონაცემები შესაძლებელია გადაცემულ იქნეს სხვა დამმუშავებლებისთვის, რომლებიც სთავაზობენ დამატებით მომსახურებებს, როგორცაა მომდევნო მეტრო სადგურის შესახებ ინფორმაციის მიწოდება მომხმარებლის ადგილმდებარეობის გათვალისწინებით, ასევე, აფთიაქის ან ამინდის პროგნოზის შესახებ ინფორმაციის მიწოდება მდებარეობის მიხედვით.

ელექტრონულ ქსელებში არსებული კომუნიკაციის მონაცემთა სხვა მიზნით წვდომა, როგორცაა დანაშაულებათა გამოძიება, პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების დირექტივის მე-15 მუხლის თანახმად, უნდა იქნეს განხორციელებული იმ მოთხოვნების სრული დაკმაყოფილებით, რომელიც აუცილებელია მონაცემთა დაცვის უფლებაში მართლზომიერი ჩარევისთვის და მოცემულია კონვენციის მე-8 მუხლის მე-2 პუნქტით და ქარტიის მე-8 და 52-ე მუხლებით.

პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების დირექტივის 2009 წელს განხორციელებული ცვლილებების თანახმად²⁹¹ შემოთავაზებულ იქნა:

- შეზღუდვები, დაწესებული ელ-ფოსტის გაგზავნაზე პირდაპირი მარკეტინგის მიზნებისთვის, გავრცელდა მოკლე ტექსტურ შეტყობინებებზე, მულტიმედიურ შეტყობინებათა მომსახურებაზე და სხვა მსგავსი სახის სერვისებზე; მარკეტინგული ელ-ფოსტები აკრძალულია წინასწარი თანხმობის მოპოვების გარეშე. ამგვარი თანხმობის გარეშე, მარკეტინგული ელ-ფოსტის გაგზავნა ნებადართულია მხოლოდ არსებულ მომხმარებლებთან, თუ მათ ხელმისაწვდომი გახადეს მათი ელ-ფოსტის მისამართი და არ ეწინააღმდეგებიან გამოყენებას.

291 ევროპული პარლამენტისა და საბჭოს 2009 წლის 25 ნოემბრის დირექტივა 2009/136/EC, რომელიც ცვლის დირექტივას 2002/22/EC უნივერსალური მომსახურებისა და ელექტრონულ საკომუნიკაციო ქსელებსა და მომსახურებებთან დაკავშირებული მომხმარებლების უფლებების შესახებ, დირექტივას 2002/58/EC ელექტრონულ საკომუნიკაციო 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.

- ვალდებულება წევრ ქვეყნებზე – უზრუნველყონ სამართლებრივი დაცვის საშუალება იმ დარღვევების წინააღმდეგ, რომელიც სახეზეა თავისუფალი კომუნიკაციის აკრძალვიდან გამომდინარე.²⁹²
- ე.წ. cookies-ის დანერგვა – პროგრამული უზრუნველყოფა, რომელიც მონიტორინგს უწევს და აფიქსირებს კომპიუტერის მომხმარებლის აქტივობას – აღარ არის ნებადართული კომპიუტერის მომხმარებლის თანხმობის გარეშე. შიდასახელმწიფოებრივი კანონმდებლობა დეტალურად უნდა არეგულირებდეს, თუ როგორ უნდა იქნეს თანხმობა გამოხატული და მოპოვებული, რათა სუბიექტი საკმარისად იქნეს დაცული.²⁹³

თუ სახეზეა მონაცემთა დამუშავების წესების დარღვევა უნებართვო წვდომის, მონაცემთა დაკარგვის ან განადგურების სახით, კომპეტენტური საზედამხედველო ორგანო უნდა იქნეს დაუყოვნებლივ ინფორმირებული. აბონენტები უნდა იყვნენ ინფორმირებულები, თუ მათ შესაძლოა მიაღდგეს ზიანი მონაცემთა დამუშავების წესების დარღვევდან გამომდინარე.²⁹⁴

დირექტივა მონაცემთა შენახვის შესახებ²⁹⁵ (ძალადაკარგული 2014 წლის 8 აპრილს, იხ. ქვემოთ მოყვანილი მაგალითი) ავალდებულებდა კომუნიკაციების მომსახურების მიმწოდებლებს გაეხადათ ტრაფიკის მონაცემები ხელმისაწვდომი მნიშვნელოვანი დანაშაულების წინააღმდეგ ბრძოლის მიზნებისთვის, სულ მცირე 6 თვის და არა უმეტეს 24 თვის მანძილზე, მიუხედავად იმისა სჭირდებოდა თუ არა პროვაიდერს ეს მონაცემები ანგარიშსწორების ან მომსახურების ტექნიკური მხარდაჭერის მიზნებისთვის.

292 იხ. შეცვლილი დირექტივა, მე-13 მუხლი.

293 იხ. იქვე, მე-5 მუხლი; იხ. ასევე, მუხლი 29 სამუშაო ჯგუფი (2012), მოსაზრება 04/2012 cookie-ის თაობაზე თანხმობის გამონაკლისის შესახებ, WP 194, ბრიუსელი, 7 ივნისი 2012 წელი.

294 იხ. ასევე, მუხლი 29 სამუშაო ჯგუფი (2011), სამუშაო დოკუმენტი 01/2011 ევროპული კავშირის პერსონალურ მონაცემთა დამუშავების არსებული წესების დარღვევის მონესრიგებისა და სამომავლო პოლიტიკის განვითარების რეკომენდაციების თაობაზე, WP 184, ბრიუსელი, 5 აპრილი 2011 წელი.

295 ევროპული პარლამენტისა და საბჭოს 2006 წლის 15 მარტის დირექტივა 2006/24/EC საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების მომსახურებისას ან საჯარო კომუნიკაციების ქსელებში წარმოშობილი ან დამუშავებული მონაცემების შენახვის შესახებ, რომელიც ცვლის დირექტივას 2002/58/EC, OJ 2006 L 105.

ევროპული კავშირის წევრმა ქვეყნებმა უნდა განსაზღვრონ დამოუკიდებელი საჯარო ორგანო, რომელიც პასუხისმგებელია შენახული მონაცემების უსაფრთხოების მონიტორინგზე.

ტელეკომუნიკაციის მონაცემთა შენახვა წარმოადგენს აშკარა ჩარევას მონაცემთა დაცვის უფლებაში.²⁹⁶ ამგვარი ჩარევის მართლზომიერების საკითხი განხილულ იქნა რამოდენიმე სასამართლო პროცესზე ევროპული კავშირის წევრ ქვეყნებში.²⁹⁷

მაგალითი: საქმეზე Digital Rights Ireland and Seitlinger and Others,²⁹⁸ მართლმსაჯულების ევროპული კავშირის სასამართლომ ძალადაკარგულად გამოაცხადა დირექტივა მონაცემთა შენახვის შესახებ. სასამართლოს აზრით, „დირექტივის ფართო ხასიათი და საგრძნობი ჩარევა მასში მოცემულ ძირითად უფლებებში არ არის საკმარისად შეზღუდული, რათა უზრუნველყოს ჩარევა იმ ოდენობით, რაც მკაცრად აუცილებელია.“

ელექტრონული კომუნიკაციების კონტექსტში მნიშვნელოვანი საკითხია ჩარევა საჯარო ორგანოების მიერ. კომუნიკაციის კონტროლის ან მოსმენის საშუალებები, როგორცაა მოსასმენი ან ჩამწერი მოწყობილობები, ნებადართულია თუ ეს განსაზღვრულია კანონმდებლობით და წარმოადგენს აუცილებელ ზომას დემოკრატიულ საზოგადოებაში სახელმწიფო უსაფრთხოების, საზოგადოებრივი უსაფრთხოების, სახელმწიფოს ფულადი ინტერესების, დანაშაულთა შემცირების მიზნებისთვის, მონაცემთა სუბიექტის ან სხვათა უფლებებისა და თავისუფლებების დასაცავად.

მაგალითი: საქმეზე Malone v. the United Kingdom,²⁹⁹ განმცხა-

296 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.

297 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.

298 მართლმსაჯულების ევროპული კავშირის სასამართლო, გაერთიანებული საქმეები C-293/12 და C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 აპრილი 2014 წელი, პარაგ. 65.

299 ადამიანის უფლებათა ევროპული სასამართლო, Malone v. the United Kingdom, No. 8691/79, 2 აგვისტო 1984 წელი.

დებელი ბრალდებულ იქნა რამოდენიმე დანაშაულში, რომელიც ეხებოდა მოპარული ნივთების არამართლზომიერ ფლობას. სასამართლო პროცესის განმავლობაში გაირკვა, რომ განმცხადებლის სატელეფონო საუბრები ისმინებოდა სახელმწიფო ორგანოს მიერ გაცემული ნებართვის საფუძველზე. მიუხედავად იმისა, რომ შიდასახელმწიფოებრივი კანონმდებლობის მიხედვით განმცხადებლის კომუნიკაციის მოსმენის ფორმა იყო კანონიერი, ადამიანის უფლებათა ევროპულმა სასამართლომ დაასკვნა, რომ არ არსებობდა სამართლებრივი ნორმები, რომელიც ეხებოდა სახელმწიფო ორგანოებისთვის ამ სფეროში მინიჭებული დისკრეციით სარგებლობის ფარგლებსა და ხასიათს და ჩარევა, რომელიც სახეზე იყო არსებული პრაქტიკიდან გამომდინარე, არ იყო „კანონმდებლობასთან შესაბამისი.“ სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

8.2. დასაქმების შესახებ მონაცემები

საკვანძო დებულებები

- შრომით ურთიერთობებში მონაცემთა დაცვისთვის სპეციალური წესები მოცემულია ევროპის საბჭოს რეკომენდაციაში დასაქმების მონაცემთა შესახებ.
- მონაცემთა დაცვის დირექტივაში, შრომითი ურთიერთობები კონკრეტულად მოხსენიებულია მხოლოდ განსაკუთრებული მონაცემების დამუშავების კონტექსტში.
- ნებაყოფლობით გაცემული თანხმობის კანონიერი ძალის არსებობა, როგორც დასაქმებულების შესახებ მონაცემთა დამუშავების სამართლებრივი საფუძველი, შესაძლებელია იყოს საეჭვო, თუ გავითვალისწინებთ ეკონომიკურ დისბალანსს დასაქმებულსა და დამსაქმებელს შორის. თანხმობის პირობები უნდა იყოს ყურადღებით დარეგულირებული.

ევროპულ კავშირში არ არსებობს რაიმე კონკრეტული სამართლებრივი რეგულირება, რომელიც აწესრიგებს მონაცემთა დამუშავებას შრომით კონტექსტში. მონაცემთა დაცვის დირექტივაში, შრომითი ურთიერთობები კონკრეტულად მოხსენიე-

ბულია მხოლოდ დირექტივის მე-8 მუხლის მე-2 პუნქტით, რომელიც ეხება განსაკუთრებული კატეგორიის მონაცემთა დამუშავებას. რაც შეეხება ევროპის საბჭოს, რეკომენდაცია დასაქმების მონაცემთა შესახებ გამოქვეყნებულ იქნა 1989 წელს და ამჟამად მიმდინარეობს მისი განახლება.³⁰⁰

დასაქმების კონტექსტთან დაკავშირებული მონაცემთა დაცვის ყველაზე გავრცელებული პრობლემატიკის განხილვა მოცემულია მუხლი 29 სამუშაო ჯგუფის სამუშაო დოკუმენტში.³⁰¹ სამუშაო ჯგუფმა გააანალიზა თანხმობის მნიშვნელობა, როგორც დასაქმების შესახებ მონაცემთა დამუშავების სამართლებრივი საფუძველი.³⁰² მან აღნიშნა, რომ ეკონომიკური დისბალანსი თანხმობის მომთხოვნ დაშლას დასაქმებულსა და თანხმობის გამცემ დასაქმებულს შორის ხშირად წარმოშობს ეჭვებს თანხმობის ნებაყოფლობით გაცემის თაობაზე. პირობები, რისი გათვალისწინებითაც თანხმობა არის მოთხოვნილი უნდა იყოს ყურადღებით განხილული, როდესაც ხდება თანხმობის კანონიერების შეფასება დასაქმების კონტექსტში.

დღევანდელ ჩვეულ სამუშაო გარემოში მონაცემთა დაცვის გავრცელებული პრობლემა სამუშაო ადგილზე დასაქმებულთა ელექტრონული კომუნიკაციების მონიტორინგის განხორციელების დასაშვები ფარგლები. მიიჩნევა, რომ ეს პრობლემა შესაძლებელია მარტივად იქნეს გადაწყვეტილი სამსახურში კომუნიკაციების საშუალებების პირადი მიზნებისთვის გამოყენების აკრძალვით. თუმცა, ამგვარი ზოგადი აკრძალვა შესაძლებელია იყოს არაპროპორციული და არარეალური. ამ მხრივ საყურადღებოა ადამიანის უფლებათა ევროპული სასამართლოს მოცემული გადაწყვეტილება:

300 ევროპის საბჭო, მინისტრთა კომიტეტი (1989), რეკომენდაცია Rec(89)2 ნევრი ქვეყნებისთვის პერსონალურ მონაცემთა დასაქმების მიზნებისთვის გამოყენების თაობაზე, 18 იანვარი 1989 წელი. იხ. შემდგომ, 108-ე კონვენციის საკონსულტაციო კომიტეტი, პერსონალურ მონაცემთა დასაქმების მიზნებისთვის გამოყენების თაობაზე რეკომენდაციის No. R (89) 2 კვლევა და პროექტის შეთავაზება მოცემული რეკომენდაციის გადასინჯვის თაობაზე, 9 სექტემბერი 2011 წელი.

301 მუხლი 29 სამუშაო ჯგუფი (2001), მოსაზრება 8/2001 პერსონალურ მონაცემთა დამუშავების შესახებ დასაქმების კონტექსტში, WP 48, ბრიუსელი, 13 სექტემბერი 2001 წელი.

302 მუხლი 29 სამუშაო ჯგუფი (2005), სამუშაო დოკუმენტი 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივის 26-ე მუხლის პირველი პუნქტის ერთგვაროვანი განმარტების თაობაზე, WP 114, ბრიუსელი, 25 ნოემბერი 2005 წელი.

მაგალითი: საქმეზე *Copland v. UK*,³⁰³ კოლეჯში დასაქმებულის მიმართ ხორციელდებოდა ტელეფონის, ელ-ფოსტის და ინტერნეტის გამოყენების ფარული მონიტორინგი, რათა დამტკიცებულიყო თუ რამდენად ახორციელებდა განმცხადებელი კოლეჯის საშუალებების გამოყენებას პირადი მიზნებისთვის. ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ სამსახურის შეობიდან განხორციელებული სატელეფონო ზარები ექცეოდა პირადი ცხოვრებისა და მიმოწერის ცნებათა ფარგლებში. შესაბამისად, სამსახურიდან განხორციელებული ზარები და გაგზავნილი ელ-ფოსტები, ისევე როგორც მიღებული ინფორმაცია ინტერნეტის პირადი გამოყენების მონიტორინგის შესახებ დაცული იყო კონვენციის მე-8 მუხლით. მოცემულ საქმეზე არ არსებობდა დებულებები, რომელიც არეგულირებდა პირობებს, რის ფარგლებშიც დამსაქმებლები მოახდენდნენ დასაქმებულების მიერ ტელეფონის, ელ-ფოსტისა და ინტერნეტის გამოყენების მონიტორინგს. შესაბამისად, ჩარევა არ იყო კანონის შესაბამისი. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

ევროპის საბჭოს დასაქმების შესახებ რეკომენდაციის თანახმად, დასაქმების მიზნებისთვის შეგროვებული პერსონალური მონაცემები უნდა იყოს მიღებული უშუალოდ კონკრეტული დასაქმებულიდან.

შერჩევის პროცესში შეგროვებული პერსონალური მონაცემები უნდა იყოს შეზღუდული იმ ინფორმაციამდე, რომელიც აუცილებელია კანდიდატისა და მისი კარიერული პოტენციალის შესაბამისობის შეფასებისთვის.

რეკომენდაცია, ასევე, ცალკე ეხება კონრეტული ინდივიდების მუშაობის შესრულების ან პოტენციალის შეფასებით მონაცემებს. ეს მონაცემები უნდა იყოს დაფუძნებული სამართლიან და ღირსეულ შეფასებებზე და არ უნდა იყოს შეურაცხყოფელი მისი ფორმულირების გათვალისწინებით. ეს მოთხოვნა მომდინარეობს მონაცემთა სამართლიანი დამუშავებისა და მათი სისწორის პრინციპებიდან.

მონაცემთა დაცვის სამართალში დამსაქმებელსა და დასაქმებულს შორის ურთიერთობის სპეციფიკურ ასპექტს წარმოადგენს დასაქმებულთა წარმომადგენლების ფუნქცია. ამგვარი წარმომადგენლები შესაძლოა იღებდნენ დასაქმებულების პერ-

303 ადამიანის უფლებათა ევროპული სასამართლო, *Copland v. the United Kingdom*, No. 62617/00, 3 აპრილი 2007 წელი.

სონალურ მონაცემებს, თუ ეს აუცილებელია დასაქმებულების ინტერესების წარმოდგენისთვის.

დასაქმების მიზნებისთვის შეგროვებული სენსიტიური პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ კონკრეტულ შემთხვევებში და დაცვის იმ მექანიზმების თანახმად, რაც დადგენილია შიდასახელმწიფოებრივი კანონმდებლობით. დამსაქმებლებმა შესაძლოა ჰკითხონ დასაქმებულებს ან განმცხადებლებს მათი ჯანმრთელობის მდგომარეობის შესახებ ან, შესაძლოა, გამოიკვლიონ სამედიცინო წესით, თუ ეს აუცილებელია: სამუშაოსთან შესაბამისობის დადგენისთვის; პრევენციული მედიცინით გათვალისწინებული მოთხოვნების შესრულებისთვის; ან სოციალური შეღავათების გამოყოფისთვის. ჯანმრთელობის შესახებ მონაცემები არ უნდა იქნეს შეგროვებული სხვა წყაროდან გარდა უშუალოდ დასაქმებულისა, გარდა იმ შემთხვევისა თუ მისგან იქნა მიღებული აშკარა და ინფორმირებული თანხმობა ან, როდესაც ამის შესაძლებლობას განსაზღვრავს შიდასახელმწიფოებრივი კანონმდებლობა.

დასაქმების შესახებ რეკომენდაციის თანახმად, დასაქმებულები უნდა იყვნენ ინფორმირებულები მათი პერსონალური მონაცემების დამუშავების მიზნის შესახებ, შენახულ პერსონალურ მონაცემთა სახის შესახებ, იმ პირების შესახებ, რომელთაც რეგულარულად გადაეცემთ მონაცემები და ამგვარი გადაცემის მიზნისა და სამართლებრივ საფუძვლის შესახებ. დამსაქმებლებმა, ასევე, წინასწარ უნდა მოახდინონ მათი დასაქმებულების ინფორმირება დასაქმებულთა პერსონალური მონაცემების დამუშავების ან დასაქმებულთა შედეგიანობის მაჩვენებლების მონიტორინგის მიზნით ავტომატიზებული სისტემების შეთავაზების ან დანერგვის ეტაპზე.

დასაქმებულებს უნდა ჰქონდეთ უფლება განახორციელონ წვდომა მათი დასაქმების შესახებ მონაცემებთან, ისევე, როგორც უნდა ჰქონდეთ უფლება შესწორებასა და წაშლაზე. თუ დამუშავებულია შეფასებითი მონაცემები, დასაქმებულებს, დამატებით, უნდა ჰქონდეთ უფლება გაასაჩივრონ ის. მიუხედავად ამისა, ეს უფლებები, შესაძლოა, დროებით იქნეს შეზღუდული შიდა გამოძიების მიზნებისთვის. თუ დასაქმებულს უარი ეთქვა დასაქმების პერსონალურ მონაცემთა წვდომაზე, შესწორებასა

ან წაშლაზე, შიდასახელმწიფოებრივი კანონმდებლობა უნდა ადგენდეს შესაბამის პროცედურებს ამგვარი გადაწყვეტილების გასაჩივრებისთვის.

8.3. სამედიცინო მონაცემები

საკვანძო დებულება

- სამედიცინო მონაცემები არის სენსიტიური, შესაბამისად, სარგებლობს სპეციალური დაცვით.

პერსონალური მონაცემები, რომელიც ეხება მონაცემთა სუბიექტის ჯანმრთელობის მდგომარეობას მიიჩნევა განსაკუთრებულ მონაცემებად მონაცემთა დაცვის დირექტივის მე-8 მუხლის პირველი პუნქტის მიხედვით და 108-ე კონვენციის მე-6 მუხლის თანახმად. შესაბამისად, სამედიცინო მონაცემები ექვემდებარება მონაცემთა დამუშავების გამკაცრებულ რეჟიმს არასენსიტიურ მონაცემებთან შედარებით.

მაგალითი: საქმეზე *Z. v. Finland*,³⁰⁴ განმცხადებლის ყოფილმა მეუღლემ, რომელიც ინფიცირებული იყო აივ-ით, ჩაიდინა რამოდენიმე სქესობრივი დანაშაული. შესაბამისად, იგი იქნა ბრალდებული მკვლელობის მცდელობისთვის, იმ საფუძველით, რომ მან გაცნობიერებულად დააყენა მისი მსხვერპლები აივ-ით ინფიცირების რისკის წინაშე. შიდასახელმწიფოებრივმა სასამართლომ გასცა ბრძანება მთლიანი განაჩენისა და საქმის მასალების 10 წლის ვადით კონფიდენციალურად შენახვის თაობაზე, მიუხედავად განმცხადებლის მიერ კონფიდენციალურად შენახვის მეტი ვადის მოთხოვნისა. ეს მოთხოვნა უარყოფილ იქნა სააპელაციო სასამართლოს მიერ, ხოლო მისი გადაწყვეტილება შეიცავდა განმცხადებლისა და მისი ყოფილი მეუღლის სრულ სახელებს. ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ ჩარევა არ იყო აუცილებელი დემოკრატიულ საზოგადოებაში, ვინაიდან სამედიცინო მონაცემების დამუშავება იყო ფუნდამენტური მნიშვნელობის მატარებელი პირადი და ოჯახური

304 ადამიანის უფლებათა ევროპული სასამართლო, *Z. v. Finland*, No. 22009/93, 25 თებერვალი 1997 წელი, პარაგ. 94 და 112; იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლო, *M.S. v. Sweden*, No. 20837/92, 27 აგვისტო 1997 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *L.L. v. France*, No. 7508/02, 10 ოქტომბერი 2006 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *I. v. Finland*, No. 20511/03, 17 ივლისი 2008 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *K.H. and others v. Slovakia*, No. 32881/04, 28 აპრილი 2009 წელი; ადამიანის უფლებათა ევროპული სასამართლო, *Szuluk v. the United Kingdom*, No. 36936/05, 2 ივნისი 2009 წელი.

ცხოვრების დაცვის უფლებით სარგებლობისთვის, განსაკუთრებით კი მაშინ, როდესაც ინფორმაცია ეხებოდა აივ-ს, რომელსაც გააჩნია სტიგმატიზაციის ეფექტი სხვადასხვა საზოგადოებაში. შესაბამისად, სასამართლომ დაასკვნა, რომ განმცხადებლის ვინაობასა და ჯანმრთელობის მდგომარეობაზე წვდომის განხორციელება, როგორც აღინიშნა სააპელაციო სასამართლოს გადაწყვეტილებაში, გადაწყვეტილების გამოტანიდან მხოლოდ 10 წლის გასვლის შემდეგ წარმოადგენდა კონვენციის მე-8 მუხლის დარღვევას.

მონაცემთა დაცვის დირექტივის მე-8 მუხლის მე-3 პუნქტი დასაშვებად აღიარებს სამედიცინო მონაცემების დამუშავებას, როდესაც ეს მოითხოვება პრევენციული მედიცინის, სამედიცინო დიაგნოზის, მკურნალობის კურსის ან ჯანდაცვის მომსახურებათა მართვის მიზნებისთვის. დამუშავება დასაშვებია, თუ წარმოებულია მხოლოდ სამედიცინო პერსონალის მიერ, რომელიც ექვემდებარება პროფესიული საიდუმლოს დაცვის ვალდებულებას, ან სხვა პირის მიერ ექვივალენტური ვალდებულების არსებობის შემთხვევაში.³⁰⁵

ევროპის საბჭოს 1997 წლის სამედიცინო მონაცემების შესახებ რეკომენდაცია დეტალურად განაგრცობს 108-ე კონვენციის პრინციპებს მონაცემთა დამუშავებაზე სამედიცინო სფეროში.³⁰⁶ მოცემული წესები თანხვედრაშია იმ წესებთან, რომელიც დადგენილია მონაცემთა დაცვის დირექტივით, რამდენადაც ეხება სამედიცინო მონაცემების ლეგიტიმური დამუშავების მიზნებს, აუცილებელი პროფესიული საიდუმლოების დაცვის ვალდებულებას იმ პირებისთვის, რომლებიც იყენებენ სამედიცინო მონაცემებს, და მონაცემთა სუბიექტის უფლებებს გამჭვირვალობაზე, წვდომაზე, შესწორებასა და წაშლაზე. მეტიც, სამედიცინო მონაცემები, რომლებიც კანონიერად არის დამუშავებული სამედიცინო პერსონალის მიერ არ უნდა იქნეს გადაცემული სამართალდამცავი ორგანოებისთვის თუ „არ იქნება გარანტირებული დაცვის საკმარისი მექანიზმები იმგვარი გამჟღავნების პრევენციისთვის, რომელიც არ არის შესაბამის-

305 იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლო, *Biriuk v. Lithuania*, No. 23373/03, 25 თებერვალი 2009 წელი.

306 ევროპის საბჭო, მინისტრთა კომიტეტი (1997), რეკომენდაცია Rec(97)5 ნევრი ქვეყნებისთვის სამედიცინო მონაცემების დაცვის შესახებ, 13 თებერვალი 1997 წელი.

ობაში კონვენციის მე-8 მუხლით გარანტირებულ პირადი ცხოვრების პატივისცემის უფლებასთან.³⁰⁷

ამასთან, რეკომენდაცია სამედიცინო მონაცემების შესახებ შეიცავს სპეციალურ დებულებებს ჯერ კიდევ არშობილი ბავშვებისა და უნარწარმეული პირების სამედიცინო მონაცემების შესახებ, ასევე გენეტიკური მონაცემების დამუშავებაზე. სამეცნიერო კვლევა მკაფიოდ აღიარებულია, როგორც მიზეზი მონაცემთა კონსერვაციისთვის საჭიროზე მეტი ვადით, თუმცა, აღნიშნული ძირითადად მოითხოვს ანონიმიზაციას. სამედიცინო მონაცემების შესახებ რეკომენდაციის მე-12 მუხლი ადგენს დეტალურ რეგულირებას იმ შემთხვევებისთვის, სადაც მკვლევარებს სჭირდებათ პერსონალური მონაცემები და ანონიმიზებული მონაცემები არ არის საკმარისი.

ფსევდონიმიზება, ასევე, შესაძლებელია იყოს შესაბამისი ზომა სამეცნიერო საჭიროებების დასაკმაყოფილებლად და, ამავე დროს, პაციენტთა ინტერესების დასაცავად. ფსევდონიმიზების კონცეფცია მონაცემთა დაცვის კონტექსტში უფრო დეტალურად არის განხილული 2.1.3. პარაგრაფში.

ინტენსიური დისკუსია მიმდინარეობს შიდასახელმწიფოებრივ და ევროპულ დონეზე პაციენტის სამედიცინო მკურნალობის შესახებ მონაცემთა ელექტრონული ჯანმრთელობის ფაილში შენახვის ინიციატივის შესახებ.³⁰⁸ ეროვნული მასშტაბის ელექტრონული ჯანმრთელობის ფაილების სპეციალური დანიშნულება მდგომარეობს მის ხელმისაწვდომობაში საზღვრებს მიღმა, რაც განსაკუთრებული ინტერესის საგანია ევროპულ კავშირში საერთაშორისო ჯანდაცვის კონტექსტის გათვალისწინებით.³⁰⁹

განხილვის მორიგი სფერო ეხება კლინიკურ ცდებთან დაკავშირებულ ახალ დებულებებს, სხვა სიტყვებით, დოკუმენტირებულ კვლევით გარემოში ახალი მედიკამენტების გამოცდას

307 ადამიანის უფლებათა ევროპული სასამართლო, *Avilkina and Others v. Russia*, No. 1585/09, 6 ივნისი 2013 წელი, პარაგ. 53 (დაუსრულებელი).

308 მუხლი 29 სამუშაო ჯგუფი (2007), სამუშაო დოკუმენტი ჯანმრთელობის ელექტრონულ რეესტრში (EHR) პერსონალური მონაცემების დამუშავების შესახებ, WP 131, ბრიუსელი, 15 თებერვალი 2007 წელი.

309 ევროპული პარლამენტისა და საბჭოს 2011 წლის 9 მარტის დირექტივა 2011/24/EU საერთაშორისო ჯანდაცვისას პაციენტთა უფლებების განსაზღვრის შესახებ, OJ 2011 L 88.

პაციენტებზე; ეს მიმართულება მოიცავს მონაცემთა დაცვის სხვადასხვა საკითხებს. კლინიკური ცდები, სამედიცინო პროდუქტების ადამიანის მიერ გამოყენების მიზნით, რეგულირებულია ევროპის პარლამენტისა და საბჭოს 2001 წლის 4 აპრილის 2001/20/EC დირექტივის მიერ წევრი ქვეყნების კანონების, რეგულაციებისა და ადმინისტრაციულ პროცედურათა დაახლოვების შესახებ კარგი კლინიკური პრაქტიკის იმპლემენტაციისთვის ადამიანების სამედიცინო პროდუქტებთან დაკავშირებული კლინიკური ცდების თაობაზე (კლინიკური ცდების დირექტივა).³¹⁰ 2012 წლის დეკემბერში, ევროპულმა კომისიამ წარადგინა რეგულაციის კანონპროექტი, რომელმაც უნდა ჩაანაცვლოს კლინიკური ცდების დირექტივა, პროცედურის უნიფიცირებისა და ეფექტურობის მიზნით.³¹¹

ევროპული კავშირის დონეზე არსებობს ბევრი სხვა საკანონმდებლო და სხვა სახის ინიციატივები, რომელიც განხილვის რეჟიმშია და ეხება პერსონალურ მონაცემებს ჯანდაცვის სექტორში.³¹²

8.4. მონაცემთა დამუშავება სტატისტიკური მიზნებისთვის

საკვანძო დებულებები

- სტატისტიკური მიზნებისთვის შეგროვებული მონაცემები არ უნდა იქნეს გამოყენებული ნებისმიერი სხვა მიზნისთვის.
- ნებისმიერი მიზნისთვის კანონიერად შეგროვებული მო-

310 ევროპული პარლამენტისა და საბჭოს 2001 წლის 4 აპრილის 2001/20/EC დირექტივა წევრი ქვეყნების კანონების, რეგულაციებისა და ადმინისტრაციულ პროცედურათა დაახლოვების შესახებ კარგი კლინიკური პრაქტიკის იმპლემენტაციისთვის ადამიანების სამედიცინო პროდუქტებთან დაკავშირებული კლინიკური ცდების თაობაზე, OJ 2001 L 121.

311 ევროპული კომისია (2012), ევროპული პარლამენტისა და საბჭოს რეგულაციის პროექტი ადამიანების სამედიცინო პროდუქტებთან დაკავშირებული კლინიკური ცდების შესახებ, რომელიც აუქმებს 2001/20/EC დირექტივას, COM(2012) 369 final, ბრიუსელი, 17 ივლისი 2012 წელი.

312 EDPS (2013), მონაცემთა დაცვის ევროპული ზედამხედველის მოსაზრება კომისიის მიმართვაზე „ელ-ჯანდაცვის სამოქმედო გეგმა 2012-2020 – ინოვაციური ჯანდაცვა 21-ე საუკუნეში“, ბრიუსელი, 27 მარტი 2013 წელი.

ნაცემები შესაძლებელია გამოყენებულ იქნეს სტატისტიკური მიზნებისთვის, თუ შიდასახელმწიფოებრივი კანონმდებლობა ადგენს დაცვის ადეკვატურ მექანიზმებს, რაც უზრუნველყოფილია მათი მომხმარებლების მიერ. ამ მიზნისთვის, მესამე პირთათვის გადაცემამდე, ანონიმირება ან ფსევდონიმირება უნდა იქნეს გათვალისწინებული.

მონაცემთა დაცვის დირექტივით, მონაცემთა დამუშავება სტატისტიკური მიზნებისთვის მოცემულია მონაცემთა დაცვის პრინციპებისგან შესაძლო გამონაკლისების კონტექსტში. დირექტივის მე-6 მუხლის პირველი პუნქტის -b- ქვეპუნქტით, შიდასახელმწიფოებრივი კანონმდებლობით მონაცემების შემდგომი სტატისტიკური მიზნებისთვის გამოყენებაზე შესაძლებელია არ გავრცელდეს მიზნის ლიმიტირების პრინციპი, თუმცა კანონმდებლობა უნდა ადგენდეს დაცვის ყველა აუცილებელ მექანიზმს. დირექტივის მე-13 მუხლის მე-2 პუნქტი, შიდასახელმწიფოებრივი კანონმდებლობის მიხედვით, დასაშვებად მიიჩნევა შეზღუდვების დაწესებას წვდომის უფლებებზე თუ მონაცემები დამუშავებულია კონკრეტულად სტატისტიკური მიზნებისთვის; ისევ და ისევ, დაცვის ადეკვატური ზომები უნდა იყოს მოცემული შიდასახელმწიფოებრივი კანონმდებლობით. ამ კონტექსტში, მონაცემთა დაცვის დირექტივა აყალიბებს კონკრეტულ მოთხოვნას, რომლის თანახმად, სტატისტიკური კვლევის დროს არც ერთი მოპოვებული ან შექმნილი მონაცემი არ არის დასაშვები, რომ იქნეს გამოყენებული მონაცემთა სუბიექტების თაობაზე კონკრეტული გადანაცვების მიღებისთვის.

მონაცემები, რომელიც იქნა კანონიერად შეგროვებული დამუშავების მიერ ნებისმიერი მიზნისთვის, შესაძლებელია გამოყენებულ იქნეს აღნიშნული დამუშავების მიერ მისი საკუთარი სტატისტიკური მიზნებისთვის – ე.წ. მეორადი სტატისტიკისთვის, მონაცემები უნდა იქნეს ანონიმირებული ან ფსევდონიმირებული, კონკრეტული ვითარების გათვალისწინებით, სანამ იგი გადაეცემა მესამე მხარეს სტატისტიკური მიზნებისთვის, გარდა იმ შემთხვევისა თუ მონაცემთა სუბიექტმა თანხმობა განაცხადა ან თუ ეს კონკრეტულად დადგენილია ში-

დასახელმწიფოებრივი კანონმდებლობით. ეს გამომდინარეობს უსაფრთხოების შესაბამისი ზომების მიღების მოთხოვნიდან, მონაცემთა დაცვის დირექტივის მე-6 მუხლის პირველი პუნქტის -b- ქვეპუნქტის თანახმად.

მონაცემთა სტატისტიკური მიზნებისთვის გამოყენების ყველაზე მნიშვნელოვანი შემთხვევებია ოფიციალური სტატისტიკა, წარმოებული შიდასახელმწიფოებრივი და ევროპული კავშირის სტატისტიკის სამსახურების მიერ, რომელიც ეფუძნება შიდასახელმწიფოებრივ და ევროპული კავშირის კანონმდებლობებს ოფიციალური სტატისტიკის შესახებ. ამ კანონებზე დაყრდნობით, მოქალაქეები და ორგანიზაციები, ჩვეულებრივ, ვალდებული არიან გაამჟღავნონ მონაცემები სტატისტიკური სამსახურებისთვის. პირები, რომლებიც მუშაობენ სტატისტიკის სამსახურებში გააჩნიათ პროფესიული საიდუმლოების სპეციალური ვალდებულება, რომელსაც განსაკუთრებით ეთმობა ყურადღება, რამდენადაც ეს არსებითია მოქალაქეთა ნდობის მაღალი დონის არსებობისთვის, რაც აუცილებელია არსებობდეს თუ მონაცემები უნდა გახდეს ხელმისაწვდომი სტატისტიკის ორგანოებისთვის.

სტატისტიკის შესახებ ევროპული რეგულაცია 223/2009 (სტატისტიკის ევროპული რეგულაცია) შეიცავს მნიშვნელოვან წესებს ოფიციალური სტატისტიკაში მონაცემთა დაცვისათვის და შესაბამისად, შესაძლოა იყოს რელევანტური ოფიციალური სტატისტიკის შესახებ დებულებებისთვის შიდასახელმწიფოებრივ დონეზე.³¹³ რეგულაცია შეიცავს პრინციპს, რომლის თანახმად, ოფიციალური სტატისტიკის ოპერაციებს ესაჭიროებათ საკმარისად ზუსტი სამართლებრივი საფუძველი.³¹⁴

313 ევროპული პარლამენტისა და საბჭოს 2009 წლის 11 მარტის რეგულაცია (EC) No. 223/2009 ევროპული სტატისტიკის შესახებ, რომელიც აუქმებს პარლამენტისა და საბჭოს რეგულაციას (EC, Euratom) No. 1101/2008 ევროპული გაერთიანების სტატისტიკური სამსახურისთვის სტატისტიკურ კონფიდენციალურობას დაქვემდებარებულ მონაცემთა გადაცემის შესახებ, საბჭოს რეგულაციას (EC) No. 322/97 გაერთიანების სტატისტიკის შესახებ და საბჭოს გადანყვევტილებას 89/382/EEC ევროპული გაერთიანების სტატისტიკური პროგრამების Euratom-ის კომიტეტის შექმნის შესახებ, OJ 2009 L 87.

314 ეს პრინციპი დეტალურად განვრცობილია Eurostat-ის ქცევის კოდექსში, რომელიც, ევროპული სტატისტიკის რეგულაციის მე-11 მუხლის თანახმად, ადგენს ეთიკის სახელმძღვანელო დებულებებს, თუ როგორ უნდა იქნეს განხორციელებული ოფიციალური სტატისტიკა, მათ შორის, პერსონალურ მონაცემთა სწორი გამოყენება;

მაგალითი: საქმეზე *Huber v. Germany*,³¹⁵ მართლმსაჯულების ევროპული კავშირის სასამართლომ დაადგინა, რომ ორგანოს მიერ პერსონალურ მონაცემთა შეგროვება და შენახვა სტატისტიკური მიზნებისთვის არ იყო სათანადო მიზეზი მონაცემთა დამუშავების კანონიერებისთვის. კანონი, რომელიც ადგენდა პერსონალურ მონაცემთა დამუშავებას, ასევე, საჭიროებდა აუცილებლობის მოთხოვნების დაკმაყოფილებას, რაც არ იყო სახეზე მოცემულ კონტექსტში.

ევროპის საბჭოს კონტექსტში, 1997 წელს გამოცემულ იქნა რეკომენდაცია სტატისტიკის მონაცემთა შესახებ, რომელიც ვრცელდება საჯარო და კერძო სექტორში სტატისტიკის წარმოებაზე.³¹⁶ ამ რეკომენდაციამ წარადგინა პრინციპები, რომელიც თანხვედრაშია მონაცემთა დაცვის დირექტივის განხილულ საკვანძო წესებთან. მოცემულია მეტად დეტალური წესები, რომელიც ეხება დაკავშირებულ საკითხებს.

დამმუშავებლის მიერ სტატისტიკური მიზნებისთვის შეგროვებული მონაცემები არ უნდა იქნეს გამოყენებული ნებისმიერი სხვა მიზნისთვის, მონაცემები, რომელიც არ იქნა შეგროვებული სტატისტიკური მიზნებისთვის შესაძლებელია იქნეს გამოყენებული სტატისტიკური მიზნებისთვის. რეკომენდაცია სტატისტიკის მონაცემთა შესახებ დასაშვებად მიიჩნევს მონაცემთა გადაცემას მესამე მხარეებისთვის მხოლოდ სტატისტიკის მიზნებისთვის. ამ შემთხვევებში, მხარეები უნდა შეთანხმდნენ და წერილობით განსაზღვრონ სტატისტიკის შემდგომი ლეგიტიმური გამოყენების ფარგლები. რამდენადაც ეს ვერ დაექვემდებარება მონაცემთა სუბიექტის თანხმობას, ითვლება, რომ შიდასახელმწიფოებრივი კანონმდებლობით უნდა იყოს განსაზღვრული უსაფრთხოების დამატებითი ზომები, როგორიცაა მონაცემთა ანონიმიზაციის ან ფსევდონიმიზაციის ვალდებულება მის გადაცემამდე, პერსონალურ მონაცემთა არასწორი გამოყენების რისკის მინიმუმამდე დასაყვანად.

ხელმისაწვდომია: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 მართლმსაჯულების ევროპული კავშირის სასამართლო, C-524/06, *Huber v. Germany*, 16 დეკემბერი 2008 წელი; იხ. ძირითადად, პარაგ. 68.

316 ევროპის საბჭო, მინისტრთა კომიტეტი (1997), რეკომენდაცია Rec(97)18 წევრი ქვეყნებისთვის სტატისტიკური მიზნებისთვის შეგროვებულ და დამუშავებულ პერსონალურ მონაცემთა შესახებ, 30 სექტემბერი 1997 წელი.

ადამიანები, რომლებსაც პროფესიულად ეხებათ სტატისტიკური კვლევა, შიდასახელმწიფოებრივი კანონმდებლობით უნდა გააჩნდეთ საიდუმლოების დაცვის სპეციალური პროფესიული ვალდებულება, რაც დამახასიათებელია ოფიციალური სტატისტიკისთვის. ეს, ასევე, უნდა გავრცელდეს გამომკითხავებზე, თუ ისინი არიან ჩართულნი მონაცემთა შეგროვებაში მონაცემთა სუბიექტებისგან ან სხვა პირებისგან.

თუ სტატისტიკური კვლევა, პერსონალურ მონაცემთა გამოყენებით, არ არის გათვალისწინებული კანონით, მონაცემთა სუბიექტებმა უნდა განაცხადონ თანხმობა მათი მონაცემების გამოყენებაზე, რათა ეს იყოს ლეგიტიმური, ან, სულ მცირე, მათ უნდა მიეცეთ გასაჩივრების შესაძლებლობა. თუ პერსონალური მონაცემები სტატისტიკური მიზნებისთვის შეგროვებულია პირების გამოკითხვის გზით, ეს პირები უნდა იყვნენ მკაფიოდ ინფორმირებულები იმის შესახებ, არის თუ არა მონაცემთა მიწოდება აუცილებელი შიდასახელმწიფოებრივი კანონმდებლობით. განსაკუთრებული მონაცემები არ უნდა იქნეს შეგროვებული ინდივიდის იდენტიფიცირებადი ფორმით, გარდა იმ შემთხვევისა თუ ეს კანონით აშკარად ნებადართულია.

თუ სტატისტიკური კვლევა ვერ იქნება განხორციელებული ანონიმირებული მონაცემების გარეშე და პერსონალური მონაცემები აშკარად აუცილებელია, ამ მიზნისთვის შეგროვებული მონაცემები უნდა იქნეს ანონიმირებული მაშინვე, როგორც კი იქნება ამის შესაძლებლობა. სტატისტიკური კვლევის შედეგები, სულ მცირე, არ უნდა იძლეოდეს რომელიმე მონაცემთა სუბიექტის იდენტიფიცირების შესაძლებლობას, გარდა იმ შემთხვევისა, თუ ეს აშკარად არ წარმოშობს რაიმე რისკს.

სტატისტიკური ანალიზის შემდეგ, გამოყენებული პერსონალური მონაცემები უნდა იქნეს ნაშლილი ან ანონიმირებული. ამ შემთხვევაში, რეკომენდაცია სტატისტიკის მონაცემთა შესახებ ადგენს, რომ პირის მაიდენტიფიცირებელი ინფორმაცია უნდა იქნეს შენახული განცალკევებულად სხვა პერსონალური მონაცემებისგან. ეს ნიშნავს, რომ, მაგალითად, მონაცემები უნდა იყოს ფსევდონიმირებული ან შიფრის კოდი, მაიდენტიფიცირებელი სინონიმების სია, უნდა იქნეს შენახული ფსევდონიმირებული მონაცემებისგან ცალკე.

8.5. ფინანსური მონაცემები

საკვანძო დებულებები

- მიუხედავად იმისა, რომ 108-ე კონვენციის მიხედვით ან მონაცემთა დაცვის დირექტივის თანახმად ფინანსური მონაცემები არ არის სენსიტიური, მათი დამუშავება საჭიროებს უსაფრთხოების გარკვეულ ზომებს, რათა უზრუნველყოფილი იქნეს მონაცემთა სისწორე და უსაფრთხოება.
- ელექტრონული ანგარიშსწორების სისტემები საჭიროებს თანდართულ მონაცემთა დაცვას, ე.წ. Privacy by Design-ს.
- ამ სფეროში მონაცემთა დაცვის კონკრეტული პრობლემები წარმოიშობა ავთენტურობის შესაბამისი მექანიზმების არსებობის საჭიროებიდან გამომდინარე.

მაგალითი: საქმეზე *Michaud v. France*,³¹⁷ განმცხადებელმა, ფრანგმა იურისტმა, გაასაჩივრა ფრანგული კანონმდებლობის მიხედვით არსებული ვალდებულება განეხორციელებინა საეჭვოობის შესახებ შეტყობინება მისი კლიენტების მიერ ფულის გათეთრების შესაძლო ქმედების თაობაზე. ადამიანის უფლებათა ევროპულმა სასამართლომ გამოიკვლია, რომ იურისტებისთვის დაწესებული მოთხოვნა - განეხორციელებინათ შეტყობინება ადმინისტრაციული ორგანოებისთვის, რაც შეიცავდა ინფორმაციას მეორე პირის შესახებ და რომელიც მათ ხელთ ჩაუვარდათ ამ პირთან ინფორმაციის გაცვლისას, წარმოადგენდა იურისტის მიმოწერისა და პირადი ცხოვრების პატივისცემის უფლებაში ჩარევას, კონვენციის მე-8 მუხლის საფუძველზე, რამდენადაც ეს კონცეფცია მოიცავს პროფესიული ან საქმიანი ხასიათის მოქმედებებს. თუმცა, ჩარევა იყო კანონთან შესაბამისი და ემსახურებოდა ლეგიტიმურ მიზანს, კერძოდ, არეულობისა და დანაშაულის პრევენციას. რამდენადაც იურისტები ექვემდებარებოდნენ ვალდებულებას განეხორციელებინათ საეჭვოობის შესახებ შეტყობინება მხოლოდ ძალზედ შეზღუდულ შემთხვევებში, სასამართლომ დაადგინა, რომ ეს ვალდებულება იყო პროპორციული, მიიჩნია რა, რომ მე-8 მუხლის დარღვევა არ იყო სახეზე.

317 ადამიანის უფლებათა ევროპული სასამართლო, *Michaud v. France*, No. 12323/11, 6 დეკემბერი 2012 წელი; იხ. ასევე, ადამიანის უფლებათა ევროპული სასამართლო, *Niemietz v. Germany*, No. 13710/88, 16 დეკემბერი 1992 წელი, პარაგ. 29 და ადამიანის უფლებათა ევროპული სასამართლო, *Halford v. the United Kingdom*, No. 20605/92, 25 ივნისი 1997 წელი, პარაგ. 42.

108-ე კონვენციით მოცემული მონაცემთა დაცვის ძირითადი სამართლებრივი მოწესრიგების გავრცელება ანგარიშსწორების კონტექსტში განსაზღვრულ იქნა ევროპის საბჭოს 1990 წლის რეკომენდაციით Rec(90)19.³¹⁸ ეს რეკომენდაცია ადგენს ანგარიშსწორების კონტექსტში მონაცემთა კანონიერი შეგროვებისა და გამოყენების ფარგლებს, განსაკუთრებით, საკრედიტო ბარათების მეშვეობით. იგი, ასევე, ადგენს შიდასახელმწიფოებრივი კანონმდებლებისთვის დეტალურ რეგულაციებს იმ შეზღუდვების შესახებ, რომელიც ეხება ანგარიშსწორების მონაცემთა მიწოდების შეზღუდვას მესამე პირებისთვის, მონაცემთა კონსერვაციის ვადებს, გამჭვირვალობას, მონაცემთა უსაფრთხოებას და მონაცემთა საერთაშორისო გადაცემას, საბოლოოდ კი, ზედამხედველობასა და დაცვის მექანიზმებს. მოცემული წესები თანხვედრაშია ევროპული კავშირის მიერ შემდგომ დადგენილ მონაცემთა დაცვის ძირითადი მოწესრიგებით არსებულ სტრუქტურასთან მონაცემთა დაცვის დირექტივაში.

რიგი სამართლებრივი ინსტრუმენტები იქმნება ფინანსური ინსტრუმენტების ბაზრის, საკრედიტო დაწესებულებებისა და საინვესტიციო ფირმების ქმედებების დასარეგულირებლად.³¹⁹ სხვა სამართლებრივი ინსტრუმენტები ხელს უწყობს ინსაიდერული გარიგებებისა და ბაზრის მანიპულაციის წინააღმდეგ ბრძოლას.³²⁰ ამ სფეროში მეტად კრიტიკული საკითხები, რომე-

318 ევროპის საბჭო, მინისტრთა კომიტეტი (1990), რეკომენდაცია No. R(90)19 გადახდებისა და სხვა დაკავშირებული ოპერაციებისთვის გამოყენებულ პერსონალურ მონაცემთა დაცვის შესახებ, 13 სექტემბერი 1990 წელი.

319 ევროპული კომისია (2011), ევროპული პარლამენტისა და საბჭოს დირექტივის პროექტი ფინანსურ ინსტრუმენტებში არსებული ბაზრის შესახებ, რომელიც აუქმებს ევროპული პარლამენტისა და საბჭოს დირექტივას 2004/39/EC, COM(2011) 656 final, ბრიუსელი, 20 ოქტომბერი 2011 წელი; ევროპული კომისია (2011), ევროპული პარლამენტისა და საბჭოს რეგულაციის პროექტი ფინანსურ ინსტრუმენტებში არსებული ბაზრის შესახებ, რომელიც ცვლის რეგულაციას [EMIR] OTC დერივატივების, ცენტრალური მხარეებისა და სავაჭრო საცავების შესახებ, COM(2011) 652 final, ბრიუსელი, 20 ოქტომბერი 2011 წელი; ევროპული კომისია (2011), ევროპული პარლამენტისა და საბჭოს დირექტივის პროექტი საკრედიტო ინსტიტუტების ქმედებათა ხელმისაწვდომობის და ამ ინსტიტუტებისა და საინვესტიციო ფირმების ჯეროვანი ზედამხედველობის შესახებ, რომელიც ცვლის ევროპული პარლამენტისა და საბჭოს დირექტივას 2002/87/EC ფინანსურ კონგლომერატში არსებული საკრედიტო ინსტიტუტების, სადაზღვევო კომპანიებისა და საინვესტიციო ფირმების დამატებითი ზედამხედველობის შესახებ, COM(2011) 453 final, ბრიუსელი, 20 ივლისი 2011 წელი.

320 ევროპული კომისია (2011), ევროპული პარლამენტისა და საბჭოს რეგულაციის პროექტი ინსაიდერთა გარიგებისა და ბაზრის მანიპულირების შესახებ (ბაზრის ბოროტად გამოყენება), COM(2011) 651 final, ბრიუსელი, 20 ოქტომბერი 2011 წელი; ევროპული კომისია (2011), ევროპული პარლამენტისა და საბჭოს დირექტივის პრო-

ლიც გავლენას ახდენს მონაცემთა დაცვაზე არის:

- ფინანსური ტრანზაქციების შესახებ მონაცემთა შენახვა;
- პერსონალური მონაცემების გადაცემა მესამე ქვეყნებში;
- სატელეფონო საუბრების ან ელექტრონული კომუნიკაციების ჩანერა, მათ შორის, კომპეტენტური ორგანოების უფლებამოსილება - მოითხოვონ ჩანერილი სატელეფონო და ტრაფიკის მონაცემები;
- პერსონალურ მონაცემთა გამჟღავნება, მათ შორის, სანქციების გამოქვეყნება;
- კომპეტენტური ორგანოების საზედამხედველო და საგამოძიებო უფლებამოსილებები, მათ შორის, ადგილობრივი შემომნებები და დოკუმენტების ხელმისაწვდომობისთვის კერძო დანესებულებებში შესვლა;
- დარღვევების ანგარიშგების მექანიზმები, მხილების სქემები; და
- წევრი ქვეყნების კომპეტენტურ ორგანოებსა და ევროპული ფასიანი ქაღალდებისა და ბაზრის ოფიციალურ ორგანოს (ESMA) შორის თანამშრომლობა.

ამ სფეროში არსებობს, ასევე, სხვა საკითხები, რომელიც კონკრეტულად რეგულირებულია, მათ შორის, მონაცემთა სუბიექტების ფინანსური სტატუსის შესახებ მონაცემთა შეგროვება³²¹ ან საბანკო ტრანსფერისას საერთაშორისო ანგარიშსწორება, რომელიც გარდაუვლად იწვევს პერსონალურ მონაცემთა გადაცემას.³²²

ექტი ინსაიდერთა გარიგებისა და ბაზრის მანიპულირებისთვის სასჯელის განსაზღვრის შესახებ, COM(2011) 654 final, ბრიუსელი, 20 ოქტომბერი 2011 წელი.

321 ევროპული პარლამენტისა და საბჭოს 2009 წლის 16 სექტემბრის რეგულაცია (EC) No. 1060/2009 საკრედიტო სარეიტინგო სააგენტოების შესახებ, OJ 2009 L 302; ევროპული კომისია, ევროპული პარლამენტისა და საბჭოს რეგულაციის პროექტი, რომელიც ცვლის რეგულაციას (EC) No. 1060/2009 საკრედიტო სარეიტინგო სააგენტოების შესახებ, COM(2010) 289 final, Brussels, 2 ივნისი 2010 წელი.

322 ევროპული პარლამენტისა და საბჭოს 2007 წლის 13 ნოემბრის დირექტივა 2007/64/EC შიდა ბაზარში არსებული საგადახდო მომსახურებების შესახებ, რომელიც ცვლის დირექტივებს 97/7/EC, 2002/65/EC, 2005/60/EC და 2006/48/EC და აუქმებს დირექტივას 97/5/EC, OJ 2007 L 319.

დამატებითი ლიტერატურა

პირველი თავი

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.

EDRI, An introduction to data protection, Brussels, available at: www.edri.org/files/paper06_datap.pdf.

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, available at:

<http://www.english.illinois.edu/-people/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>.

White, R. and Ovey, C. (2010), The European Convention on Human Rights, Oxford, Oxford University Press.

80-2 0530

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.

Desgens-Pasanau, G. (2012), *La protection des données a caractere personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

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.

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*, available at: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

80-3-80-5 053030

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*, Saarbrücken, Éditions universitaires européennes.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Data Protection*

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.

Simitis, S. (2011), Bundesdatenschutzgesetz, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, Privacy Impact Assessment, available at: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

ᐃᐅ-6 ᐅᐃᓂᐅ

Gutwirth, S., Pouillet, 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.

ᐃᐅ-7 ᐅᐃᓂᐅ

Europol (2012), Data Protection at Europol, Luxembourg, Publications Office, available at: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, Data protection at Eurojust: A robust, effective and tailor-made regime, The Hague, Eurojust.

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.

Gutwirth, S., Pouillet, Y. and De Hert, P. (2010), Data protection in a profiled world, Dordrecht, Springer.

Gutwirth, S., Pouillet, 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, available at: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

ᐃᐃ-8 ᐅᐅᐅᐅ

Büllesbach, A., Gijrath, S., Pouillet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. and Pouillet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Pouillet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Pouillet, 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.

სასამართლო გადაწყვეტილებები

**ადამიანის უფლებათა ევროპული სასამართლოს
შერჩეული გადაწყვეტილებები**

პერსონალურ მონაცემებთან წვდომა

Gaskin v. the United Kingdom, No. 10454/83, 7 July 1989
Godelli v. Italy, No. 33783/09, 25 September 2012
K.H. and Others v. Slovakia, No. 32881/04, 28 April 2009
Leander v. Sweden, No. 9248/81, 26 March 1987
Odievre v. France [GC], No. 42326/98, 13 February 2003

პერსონალური მონაცემებისა და გამოსატვის თავისუფლების ბალანსი

Axel Springer AG v. Germany [GC], No. 39954/08, 7 February 2012
Von Hannover v. Germany, No. 59320/00, 24 June 2004
Von Hannover v. Germany (No. 2) [GC], Nos. 40660/08 and 60641/08,
7 February 2012

გამონვევები მონაცემთა დაცვისთვის ონლაინ-სივრცეში

K.U. v. Finland, No. 2872/02, 2 December 2008

მიმონერა

Amann v. Switzerland [GC], No. 27798/95, 16 February 2000
Bernh Larsen Holding AS and Others v. Norway, No. 24117/08,
14 March 2013
Cemalettin Canli v. Turkey, No. 22427/04, 18 November 2008
Dalea v. France, No. 964/07, 2 February 2010
Gaskin v. the United Kingdom, No. 10454/83, 7 July 1989
Haralambie v. Romania, No. 21737/03, 27 October 2009
Khelili v. Switzerland, No. 16188/07, 18 October 2011
Leander v. Sweden, No. 9248/81, 26 March 1987
Malone v. the United Kingdom, No. 8691/79, 2 August 1984

McMichael v. the United Kingdom, No. 16424/90, 24 February 1995
M.G. v. the United Kingdom, No. 39393/98, 24 September 2002
Rotaru v. Romania [GC], No. 28341/95, 4 May 2000
S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04,
4 December 2008
Shimovolos v. Russia, No. 30194/09, 21 June 2011
Turek v. Slovakia, No. 57986/00, 14 February 2006

დანაშაულებრივ ქმედებათა მონაცემთა ბაზები

B.B. v. France, No. 5335/06, 17 December 2009
M.M. v. the United Kingdom, No. 24029/07, 13 November 2012

დნმ-ის მონაცემთა ბაზები

S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04,
4 December 2008.

GPS მონაცემები

Uzun v. Germany, No. 35623/05, 2 September 2010

ჯანმრთელობის შესახებ მონაცემები

Biriuk v. Lithuania, No. 23373/03, 25 November 2008
I. v. Finland, No. 20511/03, 17 July 2008
L.L. v. France, No. 7508/02, 10 October 2006
M.S. v. Sweden, No. 20837/92, 27 August 1997
Szuluk v. the United Kingdom, No. 36936/05, 2 June 2009
Z. v. Finland, No. 22009/93, 25 February 1997

ვინაობა

Ciubotaru v. Moldova, No. 27138/04, 27 April 2010
Godelli v. Italy, No. 33783/09, 25 September 2012
Odievre v. France [GC], No. 42326/98, 13 February 2003

ინფორმაცია პროფესიული საქმიანობის შესახებ

Michaud v. France, No. 12323/11, 6 December 2012

Niemietz v. Germany, No. 13710/88, 16 December 1992

კომუნიკაციის კონტროლი

Amann v. Switzerland [GC], No. 27798/95, 16 February 2000

Copland v. the United Kingdom, No. 62617/00, 3 April 2007

Cotlet v. Romania, No. 38565/97, 3 June 2003

Kruslin v. France, No. 11801/85, 24 April 1990

Lambert v. France, No. 23618/94, 24 August 1998

Liberty and Others v. the United Kingdom, No. 58243/00, 1 July 2008

Malone v. the United Kingdom, No. 8691/79, 2 August 1984

Halford v. the United Kingdom, No. 20605/92, 25 June 1997

Szuluk v. the United Kingdom, No. 36936/05, 2 June 2009

პასუხისმგებელი პირების ვალდებულებები

B.B. v. France, No. 5335/06, 17 December 2009

I. v. Finland, No. 20511/03, 17 July 2008

Mosley v. the United Kingdom, No. 48009/08, 10 May 2011

ფოტოსურათები

Sciacca v. Italy, No. 50774/99, 11 January 2005

Von Hannover v. Germany, No. 59320/00, 24 June 2004

უფლება იყო დავინწყებული

Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 6 June 2006

გასაჩივრების უფლება

Leander v. Sweden, No. 9248/81, 26 March 1987

Mosley v. the United Kingdom, No. 48009/08, 10 May 2011

M.S. v. Sweden, No. 20837/92, 27 August 1997

Rotaru v. Romania [GC], No. 28341/95, 4 May 2000

მონაცემთა განსაკუთრებული კატეგორიები

I. v. Finland, No. 20511/03, 17 July 2008
Michaud v. France, No. 12323/11, 6 December 2012
S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04,
4 December 2008

ზედამხედველობა და აღსრულება (სხვადასხვა მონაწილეთა დანიშნულება, მათ შორის, მონაცემთა დაცვის ზედამხედველების)

I. v. Finland, No. 20511/03, 17 July 2008
K.U. v. Finland, No. 2872/02, 2 December 2008
Von Hannover v. Germany, No. 59320/00, 24 June 2004
Von Hannover v. Germany (No. 2) [GC], Nos. 40660/08 and 60641/08,
7 February 2012

თვალთვალის მეთოდები

Allan v. the United Kingdom, No. 48539/99, 5 November 2002
Association “21 Décembre 1989” and Others v. Romania,
Nos. 33810/07 and
18817/08, 24 May 2011
Bykov v. Russia [GC], No. 4378/02, 10 March 2009
Kennedy v. the United Kingdom, No. 26839/05, 18 May 2010
Klass and Others v. Germany, No. 5029/71, 6 September 1978
Rotaru v. Romania [GC], No. 28341/95, 4 May 2000
Taylor-Sabori v. the United Kingdom, No. 47114/99, 22 October 2002
Uzun v. Germany, No. 35623/05, 2 September 2010
Vetter v. France, No. 59842/00, 31 May 2005

ვიდეოთვალთვალი

Köpke v. Germany, No. 420/07, 5 October 2010
Peck v. the United Kingdom, No. 44647/98, 28 January 2003

ხმოვანი ნიშნები

P.G. and J.H. v. the United Kingdom, No. 44787/98, 25 September 2001

Wisse v. France, No. 71611/01, 20 December 2005

მართლმსაჯულების ევროპული კავშირის სასამართლოს შერჩეული გადაწყვეტილებები

მონაცემთა დაცვის დირექტივასთან დაკავშირებული პრეცედენტები

C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, 16 December 2008 [„ჟურნალისტური ქმედებების“ კონცეფცია მონაცემთა დაცვის დირექტივის მე-9 მუხლის მიხედვით]

Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010 [ევროპული კავშირის კონკრეტული აგრარული ფონდების ბენეფიციართა პერსონალურ მონაცემთა გამოქვეყნების სამართლებრივი ვალდებულების პროპორციულობა]

C-101/01, Bodil Lindqvist, 6 November 2003 [ინდივიდის მიერ ინტერნეტში სხვათა პირადი ცხოვრების შესახებ მონაცემების გამოქვეყნების ლეგიტიმურობა]

C-131/12, Google Spain, S.L., Google Inc. v. Agencia Espanola de Protección de Datos, Mario Costeja González, Reference for a preliminary ruling from the Audiencia Nacional (Spain) lodged on 9 March 2012, 25 May 2012, pending [საძიებო სისტემების პროვაიდერების ვალდებულება, მონაცემთა სუბიექტის მოთხოვნის საფუძველზე, შეწყვიტონ პერსონალური მონაცემების ჩვენება ძიების შედეგებში]

C-270/11, European Commission v. Kingdom of Sweden, 30 May 2013 [ჯარიმა დირექტივის იმპლემენტირების არ შესრულებაზე]

C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 January 2008 [ინტერნეტ-წვდომის პროვაიდერების ვალდებულება გასცენ KaZaA ფაილური გაცვლის პროგრამის მომხმარებელთა ვინაობა ინტელექტუალური საკუთრების დაცვის ასოციაციისთვის]

C-288/12, European Commission v. Hungary, 8 April 2014 [მონაცემთა დაცვის ეროვნული ზედამხედველის სამსახურის დათხოვნის ლეგიტიმურობა]

C-291/12, Michael Schwarz v. Stadt Bochum, Opinion of the Advocate General, 13 June 2013 [ევროპული კავშირის პირველადი კა-

ნონმდებლობის დარღვევა (EC) 2252/2004 რეგულაციის მიერ, რის საფუძველზეც თითის ანაბეჭდები უნდა იქნეს შენახული პასპორტებში]

Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitling and Others v. Ireland, 8 April 2014 [ევროპული კავშირის პირველადი კანონმდებლობის დარღვევა მონაცემთა შენახვის დირექტივის მიერ]

C-360/10, SABAM v. Netlog N.V., 16 February 2012 [სოციალური ქსელის პროვaidერთა ვალდებულება მოახდინონ მუსიკალური და აუდიოვიზუალური ნამუშევრების უკანონო გამოყენების პრევენცია ქსელის მომხმარებელთა მიერ]

Joined cases C-465/00, C-138/01 and C-139/01, Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauer mann v. Österreichischer Rundfunk, 20 May 2003 [საჯარო სექტორთან დაკავშირებული დანესებულებების დასაქმებულთა შემოსავლების შესახებ პერსონალური მონაცემების გამოქვეყნების სამართლებრივი ვალდებულების პროპორციულობა]

Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECMD) v. Administración del Estado, 24 November 2011 [მონაცემთა დაცვის დირექტივის მე-7 მუხლის -f- ქვეპუნქტის – „სხვათა ლეგიტიმური ინტერესები“ - სწორი იმპლემენტაცია შიდასახელმწიფოებრივ კანონმდებლობაში]

C-518/07, European Commission v. Federal Republic of Germany, 9 March 2010 [ეროვნული საზედამხედველო ორგანოს დამოუკიდებლობა]

C-524/06, Huber v. Bundesrepublik Deutschland, 16 December 2008 [სტატისტიკურ რეესტრში უცხოელთა მონაცემების ფლობის ლეგიტიმურობა]

C-543/09, Deutsche Telekom AG v. Bundesrepublik Deutschland, 5 May 2011 [განახლებული თანხმობის აუცილებლობა]

C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, 7 May 2009 [მონაცემთა სუბიექტის წვდომის უფლება]

C-614/10, European Commission v. Republic of Austria, 16 October 2012 [ეროვნული საზედამხედველო ორგანოს დამოუკიდებლობა]

**ევროპული კავშირის დანესებულებათა მონაცემთა
დაცვის რეგულაციასთან დაკავშირებული
პრეცედენტები**

C-28/08 P, European Commission v. The Bavarian Lager Co. Ltd., 29 June 2010 [დოკუმენტებთან წვდომა]

C-41/00 P, Interporc Im- und Export GmbH v. Commission of the European Communities, 6 March 2003 [დოკუმენტებთან წვდომა]

F-35/08, Dimitrios Pachtitis v. European Commission, 15 June 2010 [პერსონალური მონაცემების გამოყენება დასაქმების კონტექსტში ევროპული კავშირის დანესებულებებში]

F-46/09, V v. European Parliament, 5 July 2011 [პერსონალური მონაცემების გამოყენება დასაქმების კონტექსტში ევროპული კავშირის დანესებულებებში]

ძირითადი უფლებების ევროპული კავშირის სააგენტო
ევროპის საბჭო – ადამიანის უფლებათა ევროპული სასამართლო

მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო

ISBN (ქართულენოვანი) 978-9941-9406-3-7

ძირითადი უფლებების ევროპული კავშირის სააგენტოს (FRA) შესახებ დაწვრილებითი ინფორმაცია ხელმისაწვდომია ინტერნეტში. იგი ხელმისაწვდომია ძირითადი უფლებების ევროპული კავშირის სააგენტოს ვებ-გვერდზე fra.europa.eu.

ევროპის საბჭოს შესახებ დამატებითი ინფორმაცია ხელმისაწვდომია ინტერნეტში, ვებ-გვერდზე hub.coe.int.

ადამიანის უფლებათა ევროპული სასამართლოს შესახებ დამატებითი ინფორმაცია ხელმისაწვდომია სასამართლოს ვებ-გვერდზე echr.coe.int. HUDOC-ის საძიებო პორტალით შესაძლებელია განხორციელდეს წვდომა გადაწყვეტილებებზე ინგლისურად ან ფრანგულად, სხვა ენებზე თარგმანებზე, სამართლებრივ რეზიუმეებზე, პრეს-რელიზებსა და სასამართლოს საქმიანობის შესახებ დამატებით ინფორმაციასზე.

როგორ მივიღოთ ევროპული კავშირის პუბლიკაციები

უფასო პუბლიკაციები:

- ერთი ეგზემპლარი: ევროპული კავშირის წიგნების მაღაზიის მეშვეობით (<http://bookshop.europa.eu>)
- ერთზე მეტი ეგზემპლარი ან პოსტერი/რუქები: ევროპული კავშირის წარმომადგენლობისგან (http://ec.europa.eu/represent_en.htm); ევროპული კავშირის არანევრ ქვეყნებში წარმომადგენლობისგან (http://eeas.europa.eu/delegations/index_en.htm); Europe Direct-თან პირდაპირ დაკავშირებით (http://europa.eu/europeirect/index_en.htm) ან 00 800 6 7 8 9 10 11 (უფასო სატელეფონო ნომერი ევროპული კავშირის ნებისმიერი ადგილიდან) (*).

ფასიანი პუბლიკაციები:

- ევროპული კავშირის წიგნების მაღაზიის მეშვეობით (<http://bookshop.europa.eu>);

ფასიანი გამომწერა:

- ევროპული კავშირის საგამომცემლო სამსახურის ერთ-ერთი გაყიდვების აგენტის მეშვეობით (http://publications.europa.eu/others/agents/index_en.htm).

(*) ინფორმაცია, ისევე როგორც ზარების უმეტესობა, არის უფასო (თუმცა ზოგიერთმა ოპერატორმა, სატელეფონო ჯიხურმა ან სასტუმრომ შესაძლებელია დაადგინოს საფასური)

როგორ მივიღოთ ევროპული საბჭოს პუბლიკაციები

ევროპის საბჭოს გამომცემლობა საქმიანობს ორგანიზაციასთან დაკავშირებული საკითხების ყველა სფეროში, მათ შორის, ადამიანის უფლებებში, სამართლებრივ მეცნიერებებში, ჯანდაცვაში, ეთიკაში, სოციალურ ურთიერთობებში, გარემოში, განათლებაში, კულტურაში, სპორტში, ახალგაზრდობასა და ძეგლთა დაცვაში. ვრცელ კატალოგში არსებული წიგნები და ელექტრონული პუბლიკაციები შესაძლებელია შეკვეთილ იქნეს ინტერნეტით (<http://book.coe.int/>). ვირტუალური საკითხავი ოთახი საშუალებას აძლევს მომხმარებლებს გაეცნონ გამოქვეყნებული ნაშრომების ამონაწილებს ან კონკრეტული ოფიციალური დოკუმენტების მთლიან ტექსტებს უფასოდ. ინფორმაცია ევროპის საბჭოს კონვენციების შესახებ, ისევე, როგორც მათი მთლიანი ტექსტი ხელმისაწვდომია ვებ-გვერდზე: <http://conventions.coe.int/>.

საინფორმაციო და საკომუნიკაციო ტექნოლოგიების სწრაფი განვითარება ხაზს უსვამს პერსონალურ მონაცემთა დაცვის აუცილებლობას – უფლებას, რომელიც დაცულია ევროპული კავშირისა და ევროპის საბჭოს ინსტრუმენტებით. ტექნოლოგიური წინსვლა, კერძოდ, თვალთვალის, კომუნიკაციის კონტროლი და მონაცემთა შენახვა, ხსნის საზღვრებს; ყველა მათგანი წარმოშობს საგრძნობ გამოწვევებს მონაცემთა დაცვის უფლების წინაშე. ეს სახელმძღვანელო შექმნილია იმ სამართალმცოდნეებისთვის, რომლებიც არ არიან სპეციალიზებული მონაცემთა დაცვის სამართლის მოცემულ სფეროში. იგი წარმოადგენს ევროპული კავშირისა და ევროპის საბჭოს მოქმედი სამართლებრივი მოწესრიგების აღწერას. იგი განმარტავს საკვანძო პრეცედენტებს, როგორც ადამიანის უფლებათა ევროპული სასამართლოს, ისე მართლმსაჯულების ევროპული კავშირის სასამართლოს უმეტეს გადწყვეტილებათა რეზუმირებით. შესაბამისი გადწყვეტილების არარსებობისას, წარდგენილია სავარაუდო შინაარსის მქონე პრაქტიკული მაგალითები. ძირითადად, ეს სახელმძღვანელო მიზნად ისახავს უზრუნველყოფის მონაცემთა დაცვის უფლების მდგრადობა და სიმტკიცე.

ძირითადი უფლებების ევროპული კავშირის სააგენტო

Schwarzenbergplatz 11 - 1040, Vienna, Austria

ტელ. +43 (1) 580 30-60 - ფაქსი +43 (1) 580 30-693

fra.europa.eu – info@fra.europa.eu

ევროპის საბჭო

ადამიანის უფლებათა ევროპული სასამართლო

67075 Strasbourg Cedex - France

ტელ. +33 (0) 3 88 41 20 00 - ფაქსი +33 (0) 3 88 41 27 30

echr.coe.int – publishing@echr.coe.int

ISBN (ქართულენოვანი) 978-9941-94 06-3-7



გამომცემლობა „იურისტების სამყარო“

თბილისი, მ. კოსტავას ქ. №75

ტელ.: 238 35 99; 557 51 51 34

E-mail: Lawyers.world@yahoo.com;

<https://www.facebook.com/PublishingHouselawyersworld>

