ნინო ცაგარეიშვილი*

პერსონალურ მონაცემთა საერთაშორისო გადაცემის სამართლებრივი მოწესრიგება (საერთაშორისო და ეროვნული სტანდარტები)

პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემა როგორც საქართველოს, ისე საერთაშორისო რეალობაში კომპლექსურ საკითხს წარმოადგენს. აღსანიშნავია, რომ სახელმწიფოთა თანამშრომლობის ფარგლებში, სხვადასხვა სფეროში გადაიცემა დიდი რაოდენობის პერსონალური მონაცემი, რაც საჭიროებს ეფექტიან რეგულირებას მონაცემთა სუბიექტის უფლებების დაცვის თვალსაზრისით.

საკვანძო სიტყვები: *პერსონალურ მონაცემთა საერთაშორისო/ტრანსსასაზღვრო გადაცემა, პერსონალურ მონაცემთა დაცვის სამსახური, შესაბამისობის გადაწყვეტილება, მონაცემთა დაცვის სათანადო გარანტიები, მონაცემთა სუბიექტის უფლებები.*

1. შესავალი

თანამედროვე სამყაროში საერთაშორისო დონეზე პერსონალური მონაცემების გადაცემის საკითხი დღითიდღე აქტუალური ხდება. სახელმწიფოთა/საერთაშორისო ორგანიზაციათა შორის, სხვადასხვა სფეროში თანამშრომლობის გაღრმავების მიზნით, უწყვეტ რეჟიმში, ხორციელდება პერსონალური მონაცემების მიმოცვლა, რაც, ერთი მხრივ, სარგებლის მომტანია, თუმცა, მეორე მხრივ, წარმოშობს გარკვეულ რისკებს პერსონალურ მონაცემთა დაცვის თვალსაზრისით.

უპირველეს ყოვლისა, გასაანალიზებელია სახელმწიფოთა შორის პერსონალურ მონაცემთა დაცვის კანონმდებლობის თავსებადობა. რიგი საკითხების განსხვავებული მოწესრიგებით შეიძლება, დაირღვეს მონაცემთა სუბიექტის უფლებები და პერსონალურ მონაცემთა დაცვის სტანდარტები. შესაბამისად, ჩნდება კითხვები: რა ეროვნული და საერთაშორისოსამართლებრივი მექანიზმები არსებობს პერსონალურ მონაცემთა საერთაშორისო გადაცემის მიმართულებით? თუ კონკრეტულ სახელმწიფოში სათანადოდ არ არის დაცული პერსონალური მონაცემები, რამდენად გამოირიცხება პერსონალურ მონაცემთა გადაცემის შესაძლებლობა? სათანადო სამართლებრივი რეგულირების არარსებობის პირობებში, როგორ უნდა იქნას უზრუნველყოფილი პერსონალურ მონაცემთა დაცულობა? რა ბერკეტები გააჩნია პერსონალურ მონაცემთა დაცვის სამსახურს

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის საერთაშორისო სამართლის მაგისტრი, პერსონალურ მონაცემთა დაცვის სამსახურის საერთაშორისო ურთიერთობების, ანალიტიკისა და სტრატეგიული განვითარების დეპარტამენტის მკვლევარ-ანალიტიკოსი.

პერსონალურ მონაცემთა საერთაშორისო გადაცემის რეგულირების თვალსაზრისით?

წინამდებარე სტატიის ფარგლებში შეფასდება პერსონალურ მონაცემთა საერთაშორისო გადაცემის სამართლებრივი ასპექტები. განიხილება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის[1] V თავით გათვალისწინებული მოთხოვნები მონაცემთა საერთაშორისო გადაცემის თაობაზე. წარმოდგენილი იქნება საერთაშორისო საკანონმდებლო ჩარჩო და სტანდარტები, ევროპული კომისიისა[2] და მონაცემთა დაცვის ევროპული საბჭოს (“EDPB”[3]) მიერ შემუშავებული სარეკომენდაციო დოკუმენტები, საზღვარგარეთის მონაცემთა დაცვის საზედამხედველო ორგანოთა პრაქტიკა, რომელთა ანალიზის საფუძველზეც პასუხი გაეცემა დასმულ კითხვებს.

2. მონაცემთა საერთაშორისო გადაცემის ეროვნული მოწესრიგება

2024 წლის პირველ მარტს, ძალაში შევიდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი (კანონი),[4] რომლის ძირითადი მიზანი პერსონალური მონაცემების დაცვის სტანდარტებისა და გარანტიების უზრუნველყოფაა. ახალი კანონით ახლებურად რეგულირდება პერსონალურ მონაცემთა დაცვის სფეროში მნიშვნელოვანი საკითხები, მათ შორის, მონაცემთა საერთაშორისო გადაცემის მიმართულებით.

პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა მოწესრიგებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 37-ე მუხლით, რომლის შესაბამისადაც მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვებია, თუ არსებობს მონაცემთა დამუშავების ამ კანონით გათვალისწინებული მოთხოვნები და შესაბამის სახელმწიფოში ან საერთაშორისო ორგანიზაციაში უზრუნველყოფილია მონაცემთა დაცვისა და მონაცემთა სუბიექტის უფლებების დაცვის სათანადო გარანტიები.[5]

გარდა აღნიშნულისა, 37-ე მუხლის მე-2 პუნქტის თანახმად, მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვებია, თუ:

- საქართველოს საერთაშორისო ხელშეკრულება და შეთანხმება ითვალისწინებს მონაცემთა გადაცემას;
- დამუშავებისთვის პასუხისმგებელი პირი უზრუნველყოფს მონაცემთა დაცვის სათანადო გარანტიებს;
- მონაცემთა გადაცემა ხორციელდება „გ“ ქვეპუნქტით გათვალისწინებული კანონმდებლობის საფუძველზე (სისხლის სამართლის საპროცესო კოდექსი; „უცხოელთა და მოქალაქეობის არმქონე პირთა სამართლებრივი მდგომარეობის შესახებ“ საქართველოს კანონი; „სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის შესახებ“ საქართველოს კანონი; „სამართალდაცვით სფეროში საერთაშორისო თანამშრომლობის

[1] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
[2] European Commission, the Executive Body of the European Union, <https://commission.europa.eu/about-european-commission_en> [03.08.2024].
[3] The European Data Protection Board, <https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en> [03.08.2024].
[4] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
[5] იქვე, 37-ე მუხლის პირველი პუნქტი.

შესახებ“ საქართველოს კანონი; „საქართველოს ეროვნული ბანკის შესახებ“ საქართველოს ორგანული კანონი; „ფულის გათეთრებისა და ტერორიზმის დაფინანსების აღკვეთის ხელშეწყობის შესახებ“ საქართველოს კანონის საფუძველზე მიღებული ნორმატიული აქტი);

- შესაბამის სახელმწიფოში მონაცემთა დაცვის სათანადო გარანტიების არარსებობისა და შესაძლო საფრთხეების შესახებ ინფორმაციის მიღების შემდეგ მონაცემთა სუბიექტი განაცხადებს წერილობით თანხმობას;
- მონაცემთა გადაცემა აუცილებელია მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად და მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად უნარი არ აქვს, მონაცემთა დამუშავებაზე თანხმობა განაცხადოს;
- არსებობს კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესი (მათ შორის, დანაშაულის თავიდან აცილება, გამოძიება, გამოვლენა და სისხლისსამართლებრივი დევნა, სასჯელის აღსრულება და ოპერატიულ-სამძებრო ღონისძიებების განხორციელება) და მონაცემთა გადაცემა აუცილებელი და პროპორციული ზომაა დემოკრატიულ საზოგადოებაში.[6]

გასათვალისწინებელია, რომ დამუშავებისთვის პასუხისმგებელი პირის მიერ ხელშეკრულების შესაბამისად სათანადო გარანტიების უზრუნველყოფის შემთხვევაში,[7] მონაცემთა გადაცემა შეიძლება მხოლოდ პერსონალურ მონაცემთა დაცვის სამსახურის ნებართვის მიღების შემდეგ, რომლის გაცემის წესი დგინდება პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტით.[8] აღნიშნულ შემთხვევაში, მონაცემთა გადაცემის შესახებ შეთანხმება სავალდებულო სამართლებრივი ძალის მქონე შესასრულებელ პირობებს უნდა ითვალისწინებდეს.[9] ამასთან, ჩამოთვლილი საფუძვლებით მონაცემთა გადაცემის შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირი/დამუშავებაზე უფლებამოსილი პირი ვალდებულია, მიიღოს მონაცემთა უსაფრთხო გადაცემისთვის აუცილებელი ორგანიზაციული და ტექნიკური ზომები.[10]

ამავე მუხლის მე-6 პუნქტის გათვალისწინებით, მესამე მხარისთვის სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემული მონაცემების შემდგომი გადაცემა დასაშვებია მხოლოდ იმ შემთხვევაში, თუ ამგვარი გადაცემა თავდაპირველი მიზნებითაა განპირობებული და აკმაყოფილებს მონაცემთა გადაცემისთვის ამ მუხლით გათვალისწინებულ საფუძვლებსა და მონაცემთა დაცვის სათანადო გარანტიებს.

3. პერსონალურ მონაცემთა დაცვის სამსახურის საზედამხედველო ბერკეტები მონაცემთა ტრანსსასაზღვრო გადაცემის მიმართულებით

პერსონალურ მონაცემთა დაცვის სამსახურის (შემდგომში - სამსახური) ერთ-ერთ ძირითად ფუნქციას პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემის

[6] იქვე, 37-ე მუხლის მე-2 პუნქტი.
[7] იქვე, 37-ე მუხლის მე-2 პუნქტის „ბ“ ქვეპუნქტი.
[8] იქვე, 37-ე მუხლის მე-3 პუნქტი.
[9] იქვე, 37-ე მუხლის მე-5 პუნქტი.
[10] იქვე, 37-ე მუხლის მე-4 პუნქტი.

კონტექსტში კანონიერების ზედამხედველობა წარმოადგენს. კერძოდ, როდესაც საქართველოს სახელით დასადები საერთაშორისო ხელშეკრულებისა და შეთანხმებების პროექტები ითვალისწინებს პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემის შესაძლებლობას, შესაბამისი უწყების მომართვის საფუძველზე, სამსახური ატარებს აღნიშნული დოკუმენტების სამართლებრივ ექსპერტიზას.

სამსახური ხელშეკრულების სამართლებრივი ექსპერტიზის განხორციელებისას ითვალისწინებს შესაბამის სახელმწიფოში/საერთაშორისო ორგანიზაციაში მონაცემთა დაცვის სათანადო გარანტიების არსებობას. აღნიშნულის გათვალისწინებით, სამართლებრივი ექსპერტიზის ფარგლებში, სამსახური შეისწავლის წარმოდგენილი ხელშეკრულებების/შეთანხმებების პროექტებს, მხარე სახელმწიფოში პერსონალურ მონაცემთა დაცვის სფეროში არსებულ საკანონმდებლო და ინსტიტუციურ მექანიზმებს, რომლის საფუძველზეც, საჭიროებისამებრ, გაიცემა შეთანხმების/ხელშეკრულების პროექტში ცვლილებების რეკომენდაცია.

პერსონალურ მონაცემთა დაცვის სამსახური, სხვა სახელმწიფოში ან/და საერთაშორისო ორგანიზაციაში მონაცემთა დაცვის სათანადო გარანტიების არსებობას აფასებს მონაცემთა დაცვასთან დაკავშირებით ნაკისრი საერთაშორისო ვალდებულებებისა და მარეგულირებელი კანონმდებლობის, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის გარანტიების (მათ შორის, ეფექტიანი სამართლებრივი დაცვის მექანიზმების), მონაცემთა შემდგომი საერთაშორისო გადაცემის წესების, მონაცემთა დაცვის დამოუკიდებელი საზედამხედველო ორგანოს არსებობის, უფლებამოსილებებისა და საქმიანობის ანალიზის საფუძველზე.[11]

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის №23 ბრძანებით დამტკიცებულია პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხა,[12] რომლებშიც მონაცემთა გადაცემა, სათანადო საფუძვლების არსებობის შემთხვევაში, მიიჩნევა უსაფრთხოდ. აღნიშნულ სიაში ასახულია როგორც ევროკავშირის წევრი, ასევე, ის ქვეყნები, რომლებთან მიმართებითაც ევროპული კომისიის მიერ მიღებულია შესაბამისობის გადაწყვეტილება.[13]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 38-ე მუხლის მე-3 პუნქტის შესაბამისად, განსაზღვრული ნუსხა მინიმუმ 3 წელიწადში ერთხელ უნდა გადაიხედოს. თუ სახელმწიფო ან/და საერთაშორისო ორგანიზაცია აღარ აკმაყოფილებს კანონის მოთხოვნებს, ნორმატიული აქტით განსაზღვრულ ნუსხაში შეტანილი უნდა იქნეს შესაბამისი ცვლილებები, რომლებსაც უკუქცევითი ძალა არ ექნება.

ამასთანავე, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის პირველი მარტის №33 ბრძანების საფუძველზე, შემუშავებულია პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე ნებართვის გაცემის წესი და დამტკიცებულია განაცხადის ფორმა, რომელიც

[11] იქვე, 38-ე მუხლის პირველი პუნქტი.

[12] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის №23 ბრძანება „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“.

[13] იხ. 3.2. თავი: „პერსონალური მონაცემების გადაცემა ევროკავშირის არაწევრ სახელმწიფოში, ევროპული კომისიის მიერ მიღებული შესაბამისობის გადაწყვეტილების საფუძველზე“.

განსაზღვრავს განაცხადისა და შესაბამისი დოკუმენტაციის წარდგენის, მათი განხილვის, გადაწყვეტილების მიღების, ნებართვის გაცემის წესსა და პირობებს.[14]

4. საერთაშორისო სტანდარტები პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემის შესახებ

4.1. საერთაშორისო საკანონმდებლო ჩარჩოს ზოგადი მიმოხილვა

„პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ“ ევროპის საბჭოს 108-ე კონვენციის[15] (შემდგომში - 108-ე კონვენცია) მე-12 მუხლი არეგულირებს პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემების საკითხს. მასში წარმოდგენილია დებულებები, რომლებიც უნდა იქნეს გამოყენებული სახელმწიფო საზღვარზე პერსონალური მონაცემების ნებისმიერი საშუალებით გადაცემის მიმართ. ამავე მუხლის მე-3 პუნქტის თანახმად, მხარეს მხოლოდ კონფიდენციალობის დაცვის მოტივით, უფლება არ აქვს ხელი შეუშალოს პერსონალური მონაცემების გადაცემას სხვა მხარის ტერიტორიაზე ან მოითხოვოს ამისათვის სპეციალური ნებართვა. თუმცა, კონვენციის მე-3 პუნქტი შეიცავს გამონაკლისებს, რა შემთხვევაშიც მხარე უფლებამოსილია არ დაეთანხმოს მე-2 პუნქტის დებულებას:

- თუ მისი კანონმდებლობა შეიცავს განსაკუთრებულ დებულებებს პერსონალური მონაცემების ავტომატიზებული ფაილების განსაზღვრული კატეგორიებისათვის. აღნიშნულში არ მოიაზრება ისეთი შემთხვევა, როდესაც სხვა მხარის კანონმდებლობა ითვალისწინებს ეკვივალენტურ დაცვას;
- როდესაც გადაცემა ხორციელდება სხვა ქვეყნის ტერიტორიაზე არსებული შუამავლის მეშვეობით მისი ტერიტორიიდან იმ სახელმწიფოს ტერიტორიაზე, რომელიც არ წარმოადგენს ხელშეკრულების მონაწილეს.

ევროპის საბჭოს 108-ე კონვენციის დამატებითი ოქმი[16] საზედამხედველო ორგანოებისა და მონაცემთა ტრანსსასაზღვრო მიმოცვლის საკითხებს შეეხება. პრეამბულაში ყურადღება მახვილდება სახელმწიფოთა შორის პერსონალური მონაცემების მიმოცვლის ინტენსივობის ზრდის პირობებში ადამიანის უფლებებისა და ძირითადი თავისუფლებების, განსაკუთრებით პირადი ცხოვრების ხელშეუხებლობის დაცვის მნიშვნელობაზე. სამართლებრივი დოკუმენტის მე-2 მუხლი აწესრიგებს პერსონალური მონაცემების საერთაშორისო გადაცემას ისეთი მიმღებისთვის, რომელზეც კონვენციის მხარის იურისდიქცია არ ვრცელდება. პირველი პუნქტის გათვალისწინებით, მონაცემთა გადაცემისას სახელმწიფოსა თუ ორგანიზაციის მიერ სათანადო დონეზე უნდა იქნას დაცული პერსონალური

[14] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის პირველი მარტის №33 ბრძანება „პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე ნებართვის გაცემის წესის და პერსონალურ მონაცემთა სხვა სახელმწიფოს ან/და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე განაცხადის ფორმის დამტკიცების შესახებ“.

[15] CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, 1981.

[16] CoE, Additional Protocol to the Convention for The Protection Of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, European Treaty Series - No. 181, 2001, <https://rm.coe.int/1680080626> [03.08.2024].

მონაცემები. მე-2 პუნქტის შესაბამისად, ყოველ მხარეს შეუძლია პერსონალური მონაცემების გადაცემა, თუ:

- აღნიშნულის საფუძველია შიდასახელმწიფოებრივი კანონმდებლობა (მონაცემთა შინაარსისადმი არსებული კონკრეტული ინტერესების ან ლეგიტიმური უპირატესი ძალის მქონე ინტერესების არსებობა);
- პერსონალურ მონაცემთა გადაცემაზე დამუშავებისთვის პასუხისმგებელი პირი სახელშეკრულებო დებულებებიდან გამომდინარე უზრუნველყოფს უსაფრთხოების ზომებს, რომლებიც შესაბამისობაში უნდა იყოს კომპეტენტური ორგანოების შიდასახელმწიფოებრივ კანონმდებლობასთან.

ევროპის საბჭოს მოდერნიზებული 108-ე კონვენციის[17] მე-14 მუხლში წარმოდგენილია დებულებები პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემის თაობაზე. აღნიშნული მუხლის მიზანია ინფორმაციის თავისუფალი მიმოცვლის ხელშეწყობა. მონაცემთა საერთაშორისო მიმოცვლა ნიშნავს პერსონალური მონაცემების გადაცემას იმ მიმღებთათვის, რომლებიც სხვა იურისდიქციას ექვემდებარებიან. მონაცემთა საერთაშორისო მიმოცვლა მიმღებთან, რომელზეც ხელშემკვრელი სახელმწიფოს იურისდიქცია არ ვრცელდება, ნებადართულია მხოლოდ იმ შემთხვევაში, თუ მონაცემები დაცულია სათანადო დონეზე.[18]

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”)[19] მე-5 თავი აწესრიგებს მესამე სახელმწიფოსთვის[20] ან საერთაშორისო ორგანიზაციისთვის პერსონალური მონაცემების გადაცემის საკითხებს. მესამე ქვეყნისთვის ან საერთაშორისო ორგანიზაციისთვის პერსონალური მონაცემების გადაცემისას უნდა იქნას უზრუნველყოფილი მონაცემთა დაცვის სტანდარტები.[21] მოცემულ შემთხვევაში, გასათვალისწინებელია ე.წ. „ორსაფეხურიანი მიდგომა“:[22] პირველ ეტაპზე, მონაცემების გადაცემა უნდა შეესაბამებოდეს ევროკავშირის მონაცემთა დაცვის მოთხოვნებს და ეფუძნებოდეს მონაცემთა სუბიექტის თანხმობას ან სხვა სავალდებულო ნებართვას; მეორე ეტაპზე, გადაცემა თანხვედრაში უნდა იყოს რეგულაციით გათვალისწინებულ მოთხოვნებთან. მონაცემთა დაცვის სათანადო გარანტიების არარსებობის შემთხვევაში, პერსონალური მონაცემები არ უნდა გადაიცეს.[23]

ევროკავშირის კანონმდებლობის თანახმად, ევროპის ეკონომიკური ზონის ქვეყნებთან პერსონალური მონაცემების მიმოცვლა ისეთი მიზნებით, როგორიცაა სისხლის სამართლის დანაშაულების პრევენცია, გამოძიება, გახსნა, დამნაშავეთა

[17] CoE, Convention 108 +, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018.

[18] CoE, Council of Europe Treaty Series - No. 223, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, §102 <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> [03.08.2024].

[19] EU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [03.08.2024].

[20] მესამე სახელმწიფოებში მოიაზრება ევროკავშირის არაწევრი ქვეყნები.

[21] იქვე, Article 44.

[22] The EU General Data Protection Regulation (GDPR), A Practical Guide, 117.

[23] იქვე.

დასჯა ან სისხლისსამართლებრივი სასჯელის აღსრულება, საპოლიციო სექტორში პერსონალური მონაცემების დამუშავების შესახებ დირექტივას ექვემდებარება.[24] აღნიშნულის მიზანია, პერსონალური მონაცემების გაცვლა უფლებამოსილი ორგანოების მიერ ევროკავშირის ფარგლებში არ აიკრძალოს/შეიზღუდოს მონაცემთა დაცვასთან დაკავშირებული მიზეზებით.[25]

4.2. პერსონალური მონაცემების გადაცემა ევროკავშირის არაწევრ სახელმწიფოში, ევროპული კომისიის მიერ მიღებული შესაბამისობის გადაწყვეტილების საფუძველზე

ევროპულ კომისიას, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 45-ე მუხლის საფუძველზე, მინიჭებული აქვს უფლებამოსილება, განსაზღვროს ევროკავშირის არაწევრ სახელმწიფოში მონაცემთა დაცვის სათანადო დონის არსებობა. შესაბამისობის გადაწყვეტილების მიღება მოიცავს შემდეგ ეტაპებს:

- ევროპული კომისიის წინადადება;
- მონაცემთა დაცვის ევროპული საბჭოს (“EDPB”) მოსაზრება;
- ევროკავშირის წევრი სახელმწიფოების წარმომადგენელთა თანხმობა;
- ევროპული კომისიის მიერ გადაწყვეტილების მიღება.

შესაბამისობის გადაწყვეტილების საფუძველზე, შესაძლებელია მესამე ქვეყნებში პერსონალური მონაცემების გადაცემა სხვა დამატებითი გარანტიების არსებობის გარეშე. კონკრეტულად, მოცემულ შემთხვევაში გავრცელდება იგივე სტანდარტები, რაც ევროკავშირის წევრ ქვეყნებში მოქმედებს.

ევროპული კომისია ვალდებულია, პერიოდულად გადახედოს შესაბამისობის გადაწყვეტილებას და ანალიზის შედეგების შესახებ აცნობოს ევროპულ პარლამენტსა და საბჭოს. ევროპულ პარლამენტსა და საბჭოს, ნებისმიერ დროს, შეუძლია მოსთხოვოს ევროპულ კომისიას შესაბამისობის გადაწყვეტილების ძალაში დატოვება, შესწორება ან გამოხმობა, თუკი დაირღვევა “GDPR”-ით გათვალისწინებული მოთხოვნები.[26]

4.3. პერსონალურ მონაცემთა გადაცემა ევროკავშირის არაწევრ ქვეყნებში, მონაცემთა დაცვის სათანადო გარანტიების საფუძველზე

ევროკავშირის არაწევრ ქვეყნებში, რომლებთან მიმართებითაც არ არის მიღებული შესაბამისობის გადაწყვეტილება, აპრიორი არ გამოირიცხება პერსონალური მონაცემების გადაცემის შესაძლებლობა. მოცემულ შემთხვევაში,

[24] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and repealing Council Framework Decision 2008/977/JHA.
[25] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 287.
[26] European Commission, Adequacy decisions, <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> [03.08.2024].

დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს პერსონალური მონაცემების სათანადო დაცულობა ალტერნატიული საშუალებებით. ამავდროულად, ფიზიკურ პირებს უნდა შეეძლოთ მათთვის მინიჭებული უფლებებით სარგებლობა.[27]

"GDPR"-ის 46-ე მუხლში წარმოდგენილია სხვადასხვა საშუალება, რომლის მეშვეობით, კერძო ორგანიზაციების მიერ, შესაბამისობის გადაწყვეტილების არარსებობის პირობებში, შესაძლებელია სათანადო გარანტიების დაცვა. კერძოდ, უნდა იქნას შემუშავებული:

- მონაცემთა დაცვის სტანდარტული დებულებები;[28]
- შესასრულებლად სავალდებულო კორპორაციული წესები;[29]
- ქცევის კოდექსები;
- სერტიფიცირების მექანიზმები;
- ხელშეკრულების სტანდარტული პირობები უშუალოდ მონაცემთა გადაცემის შესახებ[30].[31]

დამატებით, მესამე ქვეყნებში პერსონალური მონაცემების გადაცემა შესაბამისობის გადაწყვეტილების არარსებობისას შეიძლება, დასაშვები იყოს მონაცემთა სუბიექტის თანხმობის საფუძველზე, რომელიც უნდა გაიცეს თავისუფალი ნებით, ასევე, ხელშეკრულებით გათვალისწინებული ვალდებულების შესასრულებლად, მნიშვნელოვანი საჯარო ინტერესის დასაცავად და სხვა.[32]

წარმოდგენილ საკითხთან მიმართებით, უნდა აღინიშნოს ევროკავშირის მართლმსაჯულების სასამართლოს ("CJEU") გადაწყვეტილება "*Maximillian Schrems*"[33]-ის საქმეზე, რომლის ფარგლებშიც ხაზი გაესვა ევროპის ეკონომიკური ზონის ფარგლებს გარეთ პერსონალური მონაცემების გადაცემისას, სათანადო გარანტიების არსებობასთან ერთად, დამატებითი ზომების მიღების საჭიროებას. სასამართლოს შეფასებით, მონაცემთა გადაცემისას დამუშავებისთვის პასუხისმგებელმა და დამუშავებაზე უფლებამოსილმა პირებმა უნდა შეაფასონ ევროკავშირის არაწევრ ქვეყანაში არსებული კანონმდებლობისა და პრაქტიკის პოტენციური გავლენა სათანადო გარანტიების მოქმედების ეფექტიანობაზე.[34]

მონაცემთა დაცვის ევროპულმა საბჭომ შეიმუშავა სახელმძღვანელო რეკომენდაციები ევროკავშირის წევრ ქვეყნებსა და ორგანიზაციებს და არაწევრ ქვეყნებსა და ორგანიზაციებს შორის პერსონალური მონაცემების გადაცემის შესახებ. აღნიშნული დოკუმენტის შემუშავების მიზანს წარმოადგენდა, "GDPR"-ით დადგენილი მოთხოვნების გათვალისწინებით, შესაბამისობის გადაწყვეტილების არარსებობის პირობებში მონაცემთა საერთაშორისო გადაცემის რეგულირება. ხელშეკრულების მხარეები არ იზღუდებიან შეთანხმებაში დამატებითი გარანტიების ასახვის თვალსაზრისით. დოკუმენტში წარმოდგენილია ხელშეკრულებაში გასათვალისწინებელი ძირითადი საკითხები, მათ შორის: ტერმინები; მონაცემთა

[27] GDPR, Third Countries, <gdpr-info.eu> [03.08.2024].
[28] Standard data protection clauses (SCCs).
[29] Binding corporate rules (BCRs).
[30] Ad hoc contractual clauses.
[31] EDPB, International Data Transfers, <edpb.europa.eu> [03.08.2024].
[32] იქვე.
[33] CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.
[34] EDPB, International Data Transfers, <edpb.europa.eu> [03.08.2024].

დამუშავების პრინციპები; მონაცემთა სუბიექტის უფლებები; მხარეთა ვალდებულებები; მონაცემთა გადაცემასთან დაკავშირებული შეზღუდვები და სხვა.[35]

ევროპულმა კომისიამ გამოაქვეყნა მესამე ქვეყნებში პერსონალური მონაცემების გადაცემისას ხელშეკრულების სტანდარტული პირობების შესახებ დოკუმენტი,[36] რომელიც ეყრდნობა „მონაცემთა დაცვის ძირითადი რეგულაციის" მოთხოვნებს. მასში ხაზგასმულია, რომ თანამედროვე ტექნოლოგიების პირობებში, საერთაშორისო თანამშრომლობისა და ვაჭრობის ხელშესაწყობად, იზრდება მონაცემთა ტრანსსასაზღვრო გადაცემის საჭიროება, რა პროცესშიც, არსებითად მნიშვნელოვანია პერსონალურ მონაცემთა სათანადო დაცვა.[37]

"GDPR"-ის 46-ე მუხლის პირველი პუნქტის შესაბამისად, შესაბამისობის გადაწყვეტილების არარსებობისას, პერსონალური მონაცემების გადაცემა დასაშვებია, თუ უზრუნველყოფილია მონაცემთა დაცვის სათანადო გარანტიები, მათ შორის, მონაცემთა სუბიექტის უფლებები და სამართლებრივი დაცვის საშუალებები. ამგვარი გარანტიები მიზანშეწონილია, ითვალისწინებდეს ევროპული კომისიის მიერ მიღებულ მონაცემთა დაცვის სტანდარტულ პირობებს, 46-ე მუხლის მე-2 პუნქტის „გ" ქვეპუნქტის შესაბამისად.[38]

ევროპული კომისიის მიერ შედგენილი მონაცემთა დაცვის სტანდარტული პირობების მიზანია მონაცემთა საერთაშორისო გადაცემისას სათანადო გარანტიების უზრუნველყოფა. ხელშეკრულების მხარეები არ არიან შეზღუდულნი, შეთანხმებაში ასახონ დამატებითი სტანდარტები პერსონალურ მონაცემთა დაცვის ხელშესაწყობად. აღნიშნულ დოკუმენტს თან ახლავს დანართი, რომელშიც წარმოდგენილია ხელშეკრულების სტანდარტული პირობები საერთაშორისო გადაცემის მიმართულებით.[39]

დამატებით, მონაცემთა დაცვის ევროპულმა საბჭომ შეიმუშავა დოკუმენტი, რომელიც შეეხება მონაცემთა დაცვის სათანადო გარანტიებს ევროპის ეკონომიკური ზონისა და მესამე ქვეყნების მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის თანამშრომლობის განხორციელებისას. სახელმძღვანელოში ასახული სტანდარტები ეფუძნება "GDPR"-ის 70-ე (1)(u) და 50(a)-ე მუხლებს.[40]

4.4. მონაცემთა საერთაშორისო გადაცემის შესახებ საზღვარგარეთის ქვეყნების მონაცემთა დაცვის საზედამხედველო ორგანოთა პრაქტიკის მიმოხილვა

საზღვარგარეთის ქვეყნების მონაცემთა დაცვის საზედამხედველო ორგანოებს არაერთ საქმეში უმსჯელიათ პერსონალურ მონაცემთა საერთაშორისო გადაცემის საკითხებზე. წინამდებარე თავის ფარგლებში საილუსტრაციოდ წარმოდგენილია

[35] EDPB, Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and non-EEA Public Authorities and Bodies, 15/12/2020, <edpb.europa.eu> [03.08.2024].

[36] European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, <eur-lex.europa.eu> [03.08.2024].

[37] იქვე.

[38] იქვე.

[39] იქვე.

[40] EDPB, Toolbox on Essential Data Protection Safeguards for Enforcement Cooperation between EEA Data Protection Authorities and Competent Data Protection Authorities of Third Countries, 14/03/2022, <edpb.europa.eu> [03.08.2024].

რამდენიმე ქვეყნის პრაქტიკა, რომელიც მონაცემთა საერთაშორისო გადაცემასთან დაკავშირებით არსებულ მიდგომებზე ზოგად წარმოდგენას ქმნის.

ა. შვედეთი

შვედეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ("IMY") დამუშავებისთვის პასუხისმგებელი პირის მიერ "Google Analytics"-ის საშუალებით პერსონალური მონაცემების დამუშავების მართლზომიერებაზე იმსჯელა. საქმის ფაქტობრივი გარემოებების შესაბამისად, პლატფორმის საშუალებით, პერსონალური მონაცემები შეერთებულ შტატებში გადაიცემოდა.

საზედამხედველო ორგანომ შეაფასა მონაცემთა გადაცემის თავსებადობა "GDPR"-ის V თავით გათვალისწინებულ მოთხოვნებთან და, ამავდროულად, 44-ე მუხლთან. "*Schrems II*"-ის საქმეზე დაყრდნობით, აღინიშნა, რომ მხოლოდ ხელშეკრულების სტანდარტული პირობების არსებობა მონაცემთა სათანადო დაცვის უზრუნველყოფის თვალსაზრისით საკმარისი არ არის. მოცემულ შემთხვევაში, აუცილებელია ეროვნული საკანონმდებლო ჩარჩოს ანალიზი.

საზედამხედველო ორგანოს გადაწყვეტილებით, მონაცემთა გადაცემა არ იყო თავსებადი "GDPR"-ის V თავით დადგენილ მოთხოვნებთან. დამუშავებისთვის პასუხისმგებელმა პირმა ვერ უზრუნველყო მონაცემთა სუბიექტთა უფლებების დაცულობა, რის საფუძველზეც დაირღვა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის" 44-ე მუხლი.[41]

ბ. ესპანეთი

ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ შეისწავლა სატელეფონო კომპანია - "Vodafone"-ის მიერ პერსონალური მონაცემების დამუშავების კანონიერება, მათ შორის, მონაცემთა საერთაშორისო გადაცემის კონტექსტში.

ფაქტობრივი გარემოებების თანახმად, სატელეფონო კომპანიას ხელშეკრულება ჰქონდა გაფორმებული დამუშავებაზე უფლებამოსილ პირთან, რომელსაც, თავის მხრივ, მონაცემები უნდა დაემუშავებინა პერუში. შესაბამისად, პერსონალური მონაცემები გადაიცემოდა მესამე სახელმწიფოში. ხელშეკრულებით პერსონალურ მონაცემთა საერთაშორისო გადაცემის საკითხები არ რეგულირდებოდა. ამდენად, მონაცემთა დაცვის სათანადო გარანტიები არ იყო უზრუნველყოფილი.

წარმოდგენილი გარემოების გათვალისწინებით, საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირის მიერ "GDPR"-ის 44-ე მუხლის დარღვევა დაადგინა.[42]

გ. ავსტრია

ავსტრიის მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება ერთ-ერთი კომპანიის მიერ "Facebook"-ის საშუალებით, შესაბამისი სამართლებრივი საფუძვლის არარსებობის პირობებში, პერსონალური მონაცემების შეერთებულ შტატებში გადაცემას უკავშირდება.

საზედამხედველო ორგანომ იმსჯელა პერსონალურ მონაცემთა საერთაშორისო გადაცემის კანონიერებასა და "GDPR"-ის V თავით დადგენილ მოთხოვნებთან შესაბამისობაზე. მსგავსად სხვა საზედამხედველო ორგანოებისა, აღნიშნულ

[41] Decision of the Swedish DPA (IMY), 30/06/2023, <gdprhub.eu> [03.08.2024].
[42] Decision of Spanish DPA, 10/03/2021, <gdprhub.eu> [03.08.2024].

შემთხვევაშიც მითითება გაკეთდა "CJEU"-ს გადაწყვეტილებაზე.[43] საქმის შესწავლის შედეგად დადგინდა, რომ არ არსებობდა პერსონალურ მონაცემთა გადაცემის სამართლებრივი საფუძველი. კერძოდ, "Schrems II"-ის საქმეზე ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილებით ძალადაკარგულად გამოცხადდა ევროპული კომისიის მიერ მიღებული შესაბამისობის გადაწყვეტილება ევროკავშირიდან შეერთებულ შტატებში პერსონალური მონაცემების გადაცემების შესახებ. ამდენად, მონაცემთა მიმღები და გადამცემი ვერ დაეყრდნობოდა "GDPR"-ის 45-ე მუხლს.

საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია "GDPR"-ის V თავით გათვალისწინებული მოთხოვნები შეერთებულ შტატებში მონაცემთა სუბიექტის პერსონალური მონაცემების უკანონო გადაცემის გამო.[44]

დ. იტალია

იტალიის მონაცემთა დაცვის საზედამხედველო ორგანომ ("Garante") ვებგვერდის ოპერატორის მიერ "Google Analytics"-ის გამოყენებით შეერთებულ შტატებში პერსონალურ მონაცემთა გადაცემის კანონიერებაზე იმსჯელა.

საზედამხედველო ორგანოს შეფასებით, შეერთებული შტატების ორგანოების მხრიდან პერსონალურ ინფორმაციაზე წვდომის მცირე ალბათობა არსებობდა, რაც ვერ იქნებოდა დამუშავებისთვის პასუხისმგებელი პირის პასუხისმგებლობისგან გათავისუფლების საფუძველი სათანადო გარანტიების უზრუნველყოფის თვალსაზრისით. საქმის ფაქტობრივი გარემოებების შესაბამისად, პერსონალური მონაცემების დაშიფვრა, წარმოადგენდა არასაკმარის ტექნიკური უსაფრთხოების ზომას.

აღნიშნულიდან გამომდინარე, დაირღვა "GDPR"-ის 44-ე და 46-ე მუხლები. დამუშავებისთვის პასუხისმგებელ პირს საზედამხედველო ორგანომ შენიშვნა გამოუცხადა და 90 დღის განმავლობაში 46-ე მუხლთან შესაბამისობის უზრუნველყოფა დაავალა. წინააღმდეგ შემთხვევაში, უნდა შეეწყვიტა პერსონალური მონაცემების გადაცემა.[45]

ე. ფინეთი

პლატფორმა "Google Analytics"-ის გამოყენებით პერსონალური მონაცემების დამუშავების მართლზომიერება ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანომაც შეაფასა. ფაქტობრივი გარემოებების თანახმად, დამუშავებისთვის პასუხისმგებელი პირის (მეტეოროლოგიური ინსტიტუტი) მიერ პერსონალური მონაცემები გადაიცემოდა შეერთებულ შტატებში. საზედამხედველო ორგანომ *"Schrems II"*-ის გადაწყვეტილებაზე დაყრდნობით იმსჯელა მონაცემთა გადაცემის კანონიერებაზე.

საზედამხედველო ორგანოს გადაწყვეტილებით, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის" V თავის თანახმად, დამუშავებისთვის პასუხისმგებელი პირის მიერ პერსონალური მონაცემების გადაცემა არ ეფუძნებოდა შესაბამის სამართლებრივ საფუძველს. ამასთან, მონაცემთა დაცვის სათანადო გარანტიები არ იყო უზრუნველყოფილი. ამდენად, დამუშავებისთვის

[43] CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.
[44] Decision of Austrian DPA, 06/03/2023, <gdprhub.eu> [03.08.2024].
[45] Decision of Italian DPA, 9/06/2022, <gdprhub.eu> [03.08.2024].

პასუხისმგებელი პირი შეერთებულ შტატებს, "Google Analytics"-ის გამოყენებით, მონაცემთა სუბიექტების პერსონალურ მონაცემებს უკანონოდ გადასცემდა.

აღნიშნულის გათვალისწინებით, დაირღვა "GDPR"-ის 44-ე და 46-ე მუხლები. საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს შენიშვნა გამოუცხადა და შეერთებულ შტატებში სამართლებრივი საფუძვლის გარეშე გადაცემული პერსონალური მონაცემების წაშლა დაავალა.[46]

5. დასკვნა

სახელმწიფოთა/საერთაშორისო ორგანიზაციათა შორის პერსონალური მონაცემების ინტენსიური მიმოცვლა საჭიროებს ეფექტიან რეგულირებას, რათა შესაბამისად იქნას დაცული მონაცემთა სუბიექტის უფლებები. სტატიაში განხილული საკითხები, მათ შორის, ევროკავშირის მართლმსაჯულების სასამართლოსა და საზღვარგარეთის მონაცემთა დაცვის საზედამხედველო ორგანოთა პრაქტიკა მიუთითებს პერსონალურ მონაცემთა საერთაშორისო გადაცემის აქტუალობაზე და წარმოაჩენს ამ მიმართულებით არსებულ გამოწვევებს.

როგორც გამოიკვეთა, თუ ევროკავშირის არაწევრ ქვეყანასთან მიმართებით არ არის მიღებული შესაბამისობის გადაწყვეტილება და, ამავდროულად, არ არის მონაცემთა დაცვის სათანადო გარანტიები უზრუნველყოფილი, პერსონალურ მონაცემთა გადაცემა არ გამოირიცხება, რამდენადაც შესაძლებელია საკითხის ხელშეკრულებით მოწესრიგება. მოცემულ შემთხვევაში, მიზანშეწონილია, ხელშეკრულებაში აისახოს: ძირითად ტერმინთა განმარტებები, მონაცემთა დამუშავების პრინციპები, მონაცემთა სუბიექტის უფლებები, მხარეთა ვალდებულებები და ა.შ.

პერსონალური მონაცემების გადაცემამდე, მნიშვნელოვანია კონკრეტულ სახელმწიფოში ეროვნული კანონმდებლობისა და მონაცემთა დაცვის სტანდარტების შეფასება. ამასთან, სათანადო გარანტიების არსებობის დადგენა. აღნიშნული მიზნით, გასათვალისწინებელია სტატიაში განხილული საერთაშორისო საკანონმდებლო ჩარჩო და სტანდარტები და, ასევე, „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის V თავით დადგენილი მოთხოვნები.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", 14/06/2023.
2. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის №23 ბრძანება „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე", 29/02/2024.
3. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის №33 ბრძანება „პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე ნებართვის გაცემის წესის და პერსონალურ მონაცემთა სხვა სახელმწიფოს ან/და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე განაცხადის ფორმის დამტკიცების შესახებ", 01/03/2024.
4. მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი, 2018, 287.

[46] Decision of Finnish DPA, 24/03/2023, <gdprhub.eu> [03.08.2024].

5. CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, 1981.
6. CoE, Additional Protocol to the Convention for The Protection Of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, European Treaty Series - No. 181, 2001.
7. CoE, Convention 108 +, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018.
8. CoE, Council of Europe Treaty Series - No. 223, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018.
9. EU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).
10. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and repealing Council Framework Decision 2008/977/JHA.
11. The EU General Data Protection Regulation (GDPR), a Practical Guide.
12. European Commission, Information Regarding the Adequacy Decisions.
13. GDPR, Information Regarding the Third Countries.
14. EDPB, Overview of International Data Transfers.
15. CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.
16. EDPB, Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, 15 December 2020.
17. European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
18. EDPB, Toolbox on Essential Data Protection Safeguards for Enforcement Cooperation between EEA Data Protection Authorities and Competent Data Protection Authorities of Third Countries, 14 March 2022.
19. Case of the Data Protection Authority (Sweden), 30/06/2023.
20. Case of the Data Protection Authority (Spain), 10/03/2021.
21. Case of the Data Protection Authority (Austria), 06/03/2023.
22. Case of the Data Protection Authority (Italy), 09/06/2022.
23. Case of the Data Protection Authority (Finland), 24/03/2023.