პერსონალურ მონაცემთა
დაცვის სამსახური

პერსონალურ მონაცემთა დაცვის სამსახურის ანგარიში

საქართველოში მონაცემთა დაცვის მდგომარეობის, ფარული საგამოძიებო მოქმედებების ჩატარებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობის კონტროლის შესახებ

2024

WWW.PDPS.GE

წლიური ანგარიში მომზადებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 48-ე მუხლის პირველი პუნქტისა და საქართველოს პარლამენტის რეგლამენტის 169-ე მუხლის პირველი პუნქტის შესაბამისად, რომელთა თანახმად, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი წელიწადში ერთხელ, არაუგვიანეს 31 მარტისა, საქართველოს პარლამენტს წარუდგენს ანგარიშს საქართველოში მონაცემთა დაცვის მდგომარეობის, ფარული საგამოძიებო მოქმედებების ჩატარებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობის კონტროლის შესახებ; ასევე, საქართველოს პარლამენტის რეგლამენტის 169-ე მუხლის მე-2 პუნქტის შესაბამისად, რომლის თანახმად, სამსახურის უფროსი საქართველოს პარლამენტს ასევე წელიწადში ერთხელ წარუდგენს საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე – 138-ე მუხლებით გათვალისწინებული საგამოძიებო მოქმედებებისა და ამავე კოდექსის 143¹ მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული ფარული საგამოძიებო მოქმედებების ჩატარების კონტროლის შედეგების შესახებ ანგარიშს. აღნიშნულ ანგარიშს პარლამენტის ბიურო გადასცემს პარლამენტის შესაბამის კომიტეტსა და ნდობის ჯგუფს.

წინამდებარე ანგარიში მოიცავს ინფორმაციას პერსონალურ მონაცემთა დაცვის სამსახურის მიერ განხორციელებული აქტივობების შესახებ 2024 წლის 1-ელი იანვრიდან 2024 წლის 31 დეკემბრის ჩათვლით საანგარიშო პერიოდში.

შინაარსი

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მიმართვა

პერსონალურ მონაცემთა დაცვის სამსახურის სახელით მოხარული ვარ, წარმოგიდგინოთ სამსახურის 2024 წლის საქმიანობის წლიური ანგარიში. გასული წელი გამორჩეული იყო მონაცემთა დაცვის მომწესრიგებელი ეროვნული კანონმდებლობის ევროპულ სტანდარტებთან დაახლოების თვალსაზრისით. 2024 წლის მარტიდან ამოქმედდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, რომელიც ითვალისწინებს მონაცემთა სუბიექტის უფლებათა და თავისუფლებათა ეფექტიანი დაცვის სათანადო გარანტიებს, ასევე – პერსონალურ მონაცემთა დაცვის დამოუკიდებელი საზედამხედველო ორგანოს საქმიანობისთვის აუცილებელი მექანიზმებითა და უფლებამოსილებებით აღჭურვას. ევროპული ინტეგრაციის პროცესში აღსანიშნავია პერსონალურ მონაცემთა დაცვის ეროვნული კანონმდებლობის ჰარმონიზაციის მნიშვნელობა ევროკავშირის კანონმდებლობასთან და, შესაბამისად, ახალი საკანონმდებლო სტანდარტის დანერგვის შედეგად პერსონალურ მონაცემთა დაცვის ქართული სამართლის განვითარება.

მსოფლიო მასშტაბით პერსონალური მონაცემების დაცვა და პირადი ცხოვრების ხელშეუხებლობა კვლავ რჩება გლობალური დღის წესრიგის მნიშვნელოვან საკითხად. ციფრული განვითარება და სწრაფი ტექნოლოგიური პროგრესი ყოველდღიურად ახალი გამოწვევების წინაშე გვაყენებს. აღნიშნული წარმოაჩენს საერთაშორისო თანამშრომლობისა და საუკეთესო სტანდარტების დანერგვის საჭიროებას, რათა უზრუნველყოფილი იყოს ადამიანის ფუნდამენტური უფლებების დაცვა ციფრულ ეპოქაში.

დღესდღეობით განსაკუთრებით აქტუალურია ხელოვნური ინტელექტის მომწესრიგებელი სამართლებრივ ნორმათა ზეგავლენა მონაცემთა სუბიექტების პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის უფლებებზე. ხელოვნური ინტელექტის მეშვეობით გადაწყვეტილებების მიღების პროცესი თანამედროვე რეალობის ყოველდღიური ნაწილია, რაც, თავის მხრივ, ქმნის არაერთ სირთულეს სამართლიანობის, გამჭვირვალობისა და პერსონალურ მონაცემთა დამუშავების ძირითადი პრინციპებისა თუ სტანდარტების დაცვის თვალსაზრისით. განსაკუთრებით საყურადღებოა ისეთი საკითხები, როგორებიცაა: პროფაილინგი, დისკრიმინაციის რისკები, მონაცემთა მინიმიზაციის პრინციპი და ალგორითმების პასუხისმგებლიანი გამოყენება. ამ მიმართულებით აუცილებელია მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვაზე თანამედროვე ტექნოლოგიების ზეგავლენის თანმიმდევრული შეფასება და მონაცემთა დამუშავების პროცესების თანმდევი რისკების შემცირება. სამსახური აქტიურად ეცნობა პერსონალურ მონაცემთა დაცვის სფეროს აქტუალურ ტენდენციებს, რათა ჩვენს საქმიანობაში უზრუნველყოფილ იქნეს საერთაშორისო პრაქტიკის იმპლემენტაცია და მონაცემთა სუბიექტის უფლებების დაცვა საუკეთესო სტანდარტების მიხედვით. ასევე, განვაგრძობთ მუშაობას პერსონალურ მონაცემთა დაცვის საერთაშორისო სტანდარტებთან ჰარმონიზაციის საკითხზე ციფრულ

ეპოქაში ხელოვნური ინტელექტის ეთიკური და უსაფრთხო გამოყენების უზრუნველსაყოფად.

შესაბამისად, წინამდებარე ანგარიშში განხილულია მონაცემთა დამუშავების კანონიერების კონტროლის ცალკეული აქტუალური საკითხები, მათ შორის – საჯარო და კერძო სექტორში მონაცემთა დამუშავების მნიშვნელოვანი მიმართულებები და ტენდენციები, პრეცედენტული გადაწყვეტილებები, გაცემული დავალებები და რეკომენდაციები, რომელთა მიზანია პერსონალური მონაცემების დაცვის ეფექტიანობის ზრდა. აგრეთვე, წარმოდგენილია ინფორმაცია სამართალდამცავი ორგანოების მიერ მონაცემთა დამუშავების პროცესებისა და ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობის კონტროლის შესახებ.

სამსახურის საქმიანობის ერთ-ერთი ძირითადი მიმართულებაა საზოგადოებრივი ცნობიერების ამაღლება. შესაბამისად, ანგარიშში ასახულია საზოგადოების ცნობიერების ამაღლების მიზნით სამსახურის მიერ განხორციელებული საინფორმაციო ხასიათის არაერთი ღონისძიება. ამასთან, წარმოდგენილია სამსახურის საქმიანობის სტატისტიკური მონაცემი, რომელიც, სხვა მაჩვენებლებთან ერთად, მიუთითებს სამსახურისადმი გაზრდილ მიმართვიანობას, პერსონალურ მონაცემთა დაცვის კანონიერების შესწავლის მასშტაბურობასა და მის შედეგებს.

აღსანიშნავია, რომ პერსონალურ მონაცემთა დაცვის სამსახურმა გამოსცა ორი მნიშვნელოვანი სპეციალური ანგარიში: „პერსონალურ მონაცემთა დაცვის სამსახურის სპეციალური ანგარიში პერსონალურ მონაცემთა დაცვის სამართლის საუკეთესო საერთაშორისო და ევროპული პრაქტიკისა და სტანდარტის დანერგვის მიზნით 2022-2024 წლებში სამსახურის მიერ განხორციელებული საერთაშორისო აქტივობების შესახებ“, რომელიც ასახავს სამსახურის მონაწილეობას საერთაშორისო პლატფორმებში და ჩვენს კოლეგა პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებთან თანამშრომლობას. ასევე, გამოქვეყნდა „პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის სპეციალური ანგარიში „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის იმპლემენტაციის შესახებ“, რომელშიც წარმოდგენილია სამსახურის მიერ განხორციელებული აქტივობები და უახლესი პრაქტიკა ახალი კანონმდებლობის ამოქმედების შემდგომ.

ანგარიშს დანართის სახით ერთვის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ევროკავშირის კანონმდებლობასთან შესაბამისობის საკითხი. წარმოდგენილია კანონით გათვალისწინებულ ცალკეულ ნორმათა ანალიზი ევროკავშირის კანონმდებლობით დადგენილ სტანდარტთან მიმართებით. საგულისხმოა, რომ სამსახურმა შეიმუშავა „პერსონალურ მონაცემთა დაცვის სამსახურის 2025-2028 წლების საქმიანობის სტრატეგია“, რომელიც აყალიბებს ჩვენი საქმიანობის სტრატეგიულ ხედვასა და პრიორიტეტულ ამოცანებს — საზოგადოებაში პერსონალურ მონაცემთა დაცვის კულტურისა და ცნობიერების ამაღლებას, საზოგადოების ინფორმირებას პერსონალური მონაცემების დაცვის საშუალებებისა და მნიშვნელობის შესახებ, პერსონალურ მონაცემთა დაცვის სამსახურის ცნობადობის გაზრდას, პერსონალურ მონაცემთა დაცვის სამსახურის

საზედამხედველო, მათ შორის, პრევენციული მექანიზმების გაძლიერებასა და ინსტიტუციურ განვითარებას, ევროკავშირის წევრი სახელმწიფოებისა და სხვა ქვეყნების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებთან, ევროკავშირის დარგობრივ ინსტიტუციებთან და საერთაშორისო ორგანიზაციებთან თანამშრომლობის გაფართოებას.

დაბოლოს, მსურს აღვნიშნო, პერსონალურ მონაცემთა დაცვის სამსახური განაგრძობს მონაცემთა დაცვის თანამედროვე ევროპული სტანდარტების მხარდაჭერასა და ინიცირებას. ამ მიზნით აქტიურად ვთანამშრომლობთ ევროპის კოლეგა მონაცემთა დაცვის საზედამხედველო ორგანოებთან და საერთაშორისო აქტორებთან. სამსახურის საქმიანობის უალტერნატივო მიზანია, ევროპული ფასეულობების დაცვით, ქვეყანაში პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა დაცვის კულტურის ამაღლება. ამ თვალსაზრისით 2024 წელი იყო გარდამტეხი პერსონალურ მონაცემთა დაცვის ეროვნული კანონმდებლობის *de lege ferenda-სა* და პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ეფექტიანი საზედამხედველო ფუნქციის განხორციელების თვალსაზრისით. აღნიშნული მყარ საფუძველს ქმნის ციფრული განვითარების თანმდევი რისკების შესამცირებლად და საქართველოში მონაცემთა დაცვის სტანდარტების კიდევ უფრო გასაუმჯობესებლად.

დოქტ., დოქტ. ლელა ჯანაშვილი

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი
ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის
ასოცირებული პროფესორი
ბარსელონის ავტონომიური უნივერსიტეტის ასოცირებული პროფესორი

I თავი. პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში

1. მონაცემთა დამუშავება საჯარო სექტორში

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის იმპლემენტაციის პროცესის გათვალისწინებით, 2024 წლის საანგარიშო პერიოდი მრავალი გამოწვევით ხასიათდება. განცხადებებისა და შეტყობინებების რაოდენობა წინა წლებთან შედარებით არსებითად გაიზარდა და პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი მონაცემთა დამუშავების შემთხვევები კანონით გათვალისწინებულ არაერთ საკითხს შეეხო. საჯარო უწყებები მონაცემების უკანონო დამუშავების ფაქტებზე სამსახურისთვის შეტყობინების მექანიზმს აქტიურად იყენებდნენ. საგულისხმოა, რომ კანონის ზოგიერთი სიახლე უშუალოდ საჯარო სექტორს მიემართება, მაგალითად, 2024 წლის პირველი ივნისიდან სავალდებულოა, ნებისმიერ საჯარო დაწესებულებას პერსონალურ მონაცემთა დაცვის ოფიცერი ჰყავდეს. გარდა ამისა, თითოეულ უწყებაში მონაცემთა დამუშავების პროცესების მოცულობამ კანონით გათვალისწინებული არაერთი წერილობითი დოკუმენტის შექმნის აუცილებლობა განაპირობა (მაგალითად, წესი ვიდეომონიტორინგის განხორციელების თაობაზე, კანონის 28-ე მუხლით განსაზღვრული მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვის დოკუმენტი და ა.შ.). გარდა ამისა, საჯარო სექტორში მიმდინარე ერთსა და იმავე მონაცემთა დამუშავების პროცესში ხშირად სხვადასხვა დაწესებულებაა ჩართული, ხოლო კანონი მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისათვის ინფორმაციის კანონიერად დამუშავების დასაბუთების ვალდებულებას ითვალისწინებს. ამასთან, საჯარო უწყებებს, ხშირ შემთხვევაში, ორგანიზაციულ-ტექნიკურ მხარდაჭერას სხვა ორგანიზაციები უწევენ, ამ მხრივ კი მონაცემთა უსაფრთხოება კანონით დამუშავების ერთ-ერთ პრინციპად განისაზღვრა და, შესაბამისად, მისი მნიშვნელობა კიდევ უფრო გაიზარდა. ამავდროულად, მონაცემთა უსაფრთხოების დარღვევისთვის პასუხისმგებლობა მონაცემთა დამუშავებაზე უფლებამოსილ პირსაც შეეხო, რამაც დამუშავებაზე უფლებამოსილი საჯარო უწყებების მიერ ჩადენილ სამართალდარღვევების გამოვლენას შეუწყო ხელი.

განცხადებებისა და შეტყობინებების, ასევე, სამსახურის ინიციატივის საფუძველზე შეფასებულმა მონაცემთა დამუშავების პროცესებმა საანგარიშო პერიოდში მოიცვა ინციდენტის (მონაცემთა უსაფრთხოების დარღვევა) გამოვლენის, მართვისა და მასთან დაკავშირებული შეტყობინების ვალდებულებების შესრულების, ადმინისტრაციული სამართალდარღვევის გამოვლენისა და ადმინისტრირების პროცესში მონაცემების მოპოვების, ამ მიზნით ვიდეომონიტორინგის სისტემის გამოყენების, შრომით ურთიერთობებში და ჯანდაცვის სისტემაში მონაცემების კონფიდენციალურობის, მომსახურების სივრცესთან დაკავშირებული მონაცემთა დამუშავების, სააღმზრდელო-საგანმანათლებლო დაწესებულებების ფარგლებში ბავშვების მონაცემების დამუშავების, პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნისა და

ინტერესთა კონფლიქტის საკითხები, მონაცემთა სუბიექტების უფლებების რეალიზების სხვადასხვა ასპექტი, გამჭვირვალობის პრინციპთან მონაცემების დამუშავების პროცესების თავსებადობა, გარდაცვლილი პირის მონაცემების დამუშავების კანონიერება და სხვა.

საანგარიშო პერიოდში შესწავლილ იქნა პაციენტების, ბაგა-ბაღის აღსაზრდელების, დისციპლინური წარმოების მხარეების, უწყებების მოქმედი და ყოფილი თანამშრომლების, სოციალურად დაუცველი ოჯახის წევრების, საგადასახადო ვალდებულების მქონე პირების, მოვალეების, სახელმწიფო ზრუნვაში მყოფი პირების, შშმ ბავშვების, ადმინისტრაციულ სახდელდადებული პირების და სხვა მონაცემთა სუბიექტების პერსონალურ მონაცემთა დამუშავების კანონიერება. ინსპექტირებებისა და განცხადებების განხილვის შედეგად განხორციელებული კანონით გათვალისწინებული სხვადასხვა ღონისძიება (დავალება, რეკომენდაცია, სამართალდარღვევის ოქმი) გამოყენებულ იქნა საქართველოს განათლების, მეცნიერებისა და ახალგაზრდობის, საქართველოს იუსტიციის, საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის, საქართველოს ფინანსთა სამინისტროების სისტემის ორგანოების, ასევე, მართლმსაჯულების, მუნიციპალიტეტების დაწესებულებებისა და სხვათა მიმართ.

1.1. მნიშვნელოვანი მიმართულებები და ტენდენციები

ა. ინციდენტი — მონაცემების უსაფრთხოების დარღვევა

საანგარიშო პერიოდში განსაკუთრებული ყურადღება დაეთმო მონაცემთა უსაფრთხოების დარღვევასთან (ინციდენტთან) დაკავშირებული ვალდებულებების შესრულებას. კანონით განსაზღვრულია ინციდენტის აღრიცხვის, სამსახურისათვის შეტყობინებისა და მონაცემთა სუბიექტის ინფორმირების ვალდებულებები. ინციდენტი, თავისი ბუნებისა და შედეგების მიუხედავად, უნდა აღირიცხოს, თუმცა მის შესახებ სამსახურისათვის შეტყობინებისა და მონაცემთა სუბიექტის ინფორმირების ვალდებულება მხოლოდ მაშინ წარმოიშობა, თუ საშუალო ან მაღალი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და ადამიანის ძირითად უფლებებსა და თავისუფლებებს მნიშვნელოვან საფრთხეს შეუქმნის.

შესწავლილი საქმეების გათვალისწინებით დადგინდა, რომ მონაცემთა ბაზებიდან არასტანდარტული რაოდენობის ინფორმაციის გამოთხოვის შემთხვევაში ცალკეული დაწესებულებები პერსონალურ მონაცემებზე საეჭვო მოქმედებების გავლენას პროაქტიულად არ აფასებენ; უსაფრთხოების დაცვის მიზნით გარკვეულ ნაბიჯებს დგამენ, თუმცა, ამავდროულად, განმარტავენ, რომ დაზუსტებით არ იციან, მოხდა თუ არა ინციდენტი.

მსგავს შემთხვევებში უწყებები სავარაუდო დანაშაულის თაობაზე ინფორმაციას საგამოძიებო ორგანოებში აგზავნიან, ხოლო სამსახურის მიერ ფაქტით დაინტერესების შემთხვევაში განმარტავენ, რომ გამოძიების დასრულებისა

და გარემოებების დადგენის შემდეგ მოახდენენ რეაგირებას. საგულისხმოა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირებისთვის კანონით დაკისრებული ვალდებულებების არაჯეროვანი შესრულება გამოძიების დაწყების არგუმენტით ვერ გამართლდება. მონაცემების უსაფრთხოებისთვის მნიშვნელოვანია დაყოვნების გარეშე ინციდენტის აღმოჩენა და მონაცემთა სუბიექტების უფლებებისთვის ზიანის შესამცირებლად აუცილებელი ღონისძიებების დროულად გატარება მაშინ, როდესაც ეს შესაძლებელია გონივრული, რისკების ადეკვატური ორგანიზაციულ-ტექნიკური ზომების გამოყენების შემთხვევაში.

კიბერშეტევა და ინციდენტი განსხვავებული ცნებებია. ინციდენტი მონაცემთა უსაფრთხოების დარღვევაა, რომელიც მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე, უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას/მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას იწვევს. შესაბამისად, მნიშვნელოვანია, რომ პასუხისმგებელმა საჯარო უწყებებმა ერთმანეთისაგან მკვეთრად გამიჯნონ ზემოაღნიშნული ცნებები და სამსახურში ინციდენტის თაობაზე შეტყობინება წარმოადგინონ არა ზოგადად კიბერშეტევის, არამედ მონაცემების უსაფრთხოების დარღვევის შემთხვევაში.

თავის მხრივ, ინციდენტთან დაკავშირებულ პროცესში სამსახურის ჩართულობისთვის რიგი ინფორმაციის წარმოდგენა არის საჭირო, რასაც სამსახურის უფროსის ნორმატიული აქტი განსაზღვრავს. ამასთან, უზრუნველყოფილია სამსახურის ვებგვერდზე შესაბამისი ფორმის შევსების შესაძლებლობა. საანგარიშო პერიოდში გამოვლინდა შემთხვევები, როდესაც ინციდენტის თაობაზე სამსახურს შეატყობინა არა მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა, არამედ ფაქტის თაობაზე ინფორმირებულმა სხვა დაწესებულებამ. ამ შემთხვევაში ინციდენტის შეტყობინების ვალდებულება შესრულებულად ვერ მიიჩნევა, ვინაიდან მსგავსი პირები, როგორც წესი, მონაცემთა უსაფრთხოების დარღვევაზე არ ფლობენ ისეთ ინფორმაციას, როგორიცაა: მონაცემების მოცულობა, კატეგორია, ინციდენტის შედეგები, მისი სტატუსი (მაგალითად, დასრულებული, მიმდინარე), უკავშირდება თუ არა ინციდენტის შედეგი არასრულწლოვანს, შეზღუდული შესაძლებლობების მქონე პირს და სხვა.

ინციდენტის შეტყობინებაზე სამსახური მყისიერ რეაგირებას ახდენს. არის შემთხვევები, როდესაც ინციდენტის შეტყობინების ფორმით სამსახურს მონაცემების არაკანონიერი დამუშავების იმგვარ ფაქტებზე მომართავენ, რომლებიც უსაფრთხოების დარღვევას არ წარმოადგენს (მაგალითად, პედაგოგის მიერ, საკუთარი გადაწყვეტილებით და საზოგადოებისგან რჩევების, მოსაზრებების მიღების მიზნით, მოსწავლის პერსონალური მონაცემების სოციალურ ქსელში გასაჯაროების შემთხვევა). შესაბამისად, ინციდენტთან დაკავშირებით როგორც საზოგადოების ცნობიერება, ასევე საჯარო დაწესებულებების პრაქტიკა მნიშვნელოვანი გამოწვევების წინაშე დგას.

ბ. პერსონალურ მონაცემთა დაცვის ოფიცერი

პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნა/განსაზღვრა და კანონის 33-ე მუხლით განსაზღვრული სხვა ვალდებულებების ჯეროვანი შესრულება ერთ-ერთი პრობლემური საკითხია. 2024 წელს, როგორც ინსპექტირებების, ასევე მომართვების საფუძველზე, ათეულობით მონაცემთა დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირი შემოწმდა, მათ შორის, ზოგადსაგანმანათლებლო დაწესებულებები, მუნიციპალიტეტების ორგანოები (საკრებულო და მერია). სამსახურის უფროსის გადაწყვეტილებები შეეხო აღმასრულებელი ხელისუფლების ორგანოებს, საჯარო სამართლის იურიდიულ პირებსა და ა.შ. ძირითად შემთხვევებში შეფასების საგანს წარმოადგენდა: პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის/განსაზღვრის ვალდებულების შესრულება; თანამდებობრივი ინტერესთა კონფლიქტი; მონაცემთა დაცვის სფეროს სათანადო ცოდნა; ოფიცრის საიდენტიფიკაციო/საკონტაქტო მონაცემების სამსახურში წარმოდგენა, მათი სხვადასხვა საშუალებით პროაქტიულად გამოქვეყნება და სხვა.

საანგარიშო პერიოდში ოფიცრის დანიშვნის ვალდებულების შეუსრულებლობის ათზე მეტი შემთხვევა გამოიკვეთა. ასევე, საკანონმდებლო ვალდებულების[1] მიუხედავად, ცალკეულ შემთხვევებში სამსახური არ იყო ინფორმირებული პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის შესახებ. დაწესებულებების უმრავლესობას მოქმედ ვებგვერდზე არ ჰქონდა მითითებული ოფიცრის ვინაობა ან საზოგადოებისთვის რთულად ხელმისაწვდომი ფორმით იყო აღნიშნული ინფორმაცია განთავსებული; ხოლო უწყებები, რომლებსაც ვებგვერდები არ ჰქონდათ, ოფიცრის თაობაზე მონაცემებს არც სხვა გზით აქვეყნებდნენ.

სამსახურის მიერ შემოწმებულ დაწესებულებებს შორის, რომლებმაც პერსონალურ მონაცემთა დაცვის ოფიცრის განსაზღვრის, მისი ფუნქციების მოქმედი თანამშრომლისთვის შეთავსების გადაწყვეტილება მიიღეს, ერთ-ერთი ყველაზე ხელშესახები პრობლემა თანამდებობრივი ინტერესთა კონფლიქტი აღმოჩნდა. უმეტესწილად აღნიშნული პოზიცია მოქმედმა თანამშრომლებმა მათ ფუნქციებთან ერთად შეითავსეს. სამსახურმა არაერთი შემთხვევა შეისწავლა, რომელთა ფარგლებშიც გამოვლინდა, რომ პერსონალურ მონაცემთა დაცვის ოფიცრის უფლება-მოვალეობები გადაწყვეტილების მიმღები სტრუქტურული ერთეულის ხელმძღვანელს ან/და იმ თანამშრომელს ჰქონდა შეთავსებული, რომელსაც ევალებოდა ადამიანური რესურსების მართვა, პედაგოგიური საქმიანობის განხორციელება, საქმისწარმოების ორგანიზება, საორგანიზაციო საკითხების, სახელმწიფო შესყიდვების, ინვენტარიზაციის პროცედურების წარმართვა, დამსაქმებლის წარმომადგენლობა სასამართლოში და სხვა. მსგავსი საქმიანობები თავისთავად დაკავშირებულია პერსონალური მონაცემების დამუშავების მიზნებისა და საშუალებების თაობაზე გადაწყვეტილებების

[1] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 33-ე მუხლის მე-8 პუნქტი.

მიღებასთან ან/და მასში მონაწილეობასთან, რაც ოფიცრის მოვალეობებთან ინტერესთა კონფლიქტს იწვევს.

ოფიცერი მონაცემთა დამუშავების პროცესების კანონიერად წარმართვას უზრუნველყოფს, შესაბამისად, მას უნდა ჰქონდეს სათანადო ცოდნა მონაცემთა დაცვის სფეროში. კომპეტენტური კადრების მოძიების სირთულესთან დაკავშირებით აღსანიშნავია, რომ სამსახურის ვებგვერდზე ხელმისაწვდომია არაერთი სახელმძღვანელო რეკომენდაცია, წესი და ინსტრუქცია, რომლებიც დაინტერესებულ პირებს მონაცემთა დაცვის სფეროში სათანადო ცოდნის შეძენის საშუალებას აძლევს. გარდა ამისა, კონსულტაციები სამსახურში სხვადასხვა ფორმატში მიმდინარეობს, ასევე, არაერთი ნორმატიული აქტი საჯაროდ არის ხელმისაწვდომი.

ამასთან, მიუხედავად იმისა, რომ ოფიცერი დაწესებულებას სამსახურთან ურთიერთობაში წარმოადგენს, მონაცემთა დამუშავების კონკრეტული ფაქტების კანონიერების შესწავლისას გამოვლინდა, რომ შესაფასებელი პროცესების შესახებ ტექნიკური, ორგანიზაციული თუ სამართლებრივი ხასიათის ინფორმაციის სწორად და ეფექტიანად წარმოსადგენად მნიშვნელოვანია, დაწესებულებებმა, სამსახურში მიმდინარე განხილვებისა და ინსპექტირებების ფარგლებში, ოფიცერთან ერთად შესაბამისი კომპეტენციის/გამოცდილების მქონე თანამშრომლების წარმომადგენლობა ან/და საქმისწარმოებაში მათი მოწმის სახით ჩართულობა უზრუნველყონ.

გ. მონაცემთა უსაფრთხოება

„მონაცემების უსაფრთხოების დაცვის მიზნით მონაცემთა დამუშავებისას მიღებული უნდა იქნეს ისეთი ტექნიკური და ორგანიზაციული ზომები, რომლებიც სათანადოდ უზრუნველყოფს მონაცემთა დაცვას, მათ შორის, უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვისგან, განადგურებისგან ან/და დაზიანებისგან“[2]. ამასთან, მნიშვნელოვანია წინასწარ იქნეს გათვალისწინებული მონაცემთა შემთხვევითი გამჟღავნების საფრთხეები, ხოლო საჭირო ზომები რისკების ადეკვატურად შეირჩეს. ამ კუთხით, ერთ-ერთი გამოწვევა მოქალაქეთა მომსახურების სივრცის ორგანიზაციულ-ტექნიკური მოწყობაა. ხშირად, მომსახურების სივრცეებში, ე. წ. ცოცხალი რიგის პირობებში, სენსიტიური მონაცემების გამოყენებით მიმდინარეობს კომუნიკაცია, ამდენად, ინფორმაციის შემთხვევითი გამჟღავნების რისკები მაღალია; ხოლო, სათანადო ძალისხმევისა და მომსახურების პროცესის დაგეგმვის პირობებში, მონაცემების შემთხვევითი გამჟღავნების პრევენცია, მაგალითად, სივრცის შეცვლით, სხვაგვარად მოწყობით, რიგის მართვის ეფექტიანი მექანიზმის დანერგვით, თანამშრომლებისათვის ცხადი და კონკრეტული ინსტრუქციების მიცემით არის შესაძლებელი.

მონაცემთა დამუშავების პროცესებს ნაკლებად აქვს სრულად ავტომატიზებული სახე. მნიშვნელოვანია მათი წარმართვა დაწესებულებებში

[2] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „ვ“ ქვეპუნქტი.

დასაქმებული პირების ჩართულობით. წინა წლების მსგავსად, საანგარიშო პერიოდში მონაცემთა უკანონო დამუშავების შემთხვევებს დაწესებულებები ხშირად უკავშირებენ თანამშრომლების ქმედებებს. მონაცემთა დამუშავებაში ჩართული უწყებების მიერ თანამშრომლებისთვის მხოლოდ ზოგადი ხასიათის მითითებების მიცემა, სათანადო ორგანიზაციულ-ტექნიკური უზრუნველყოფისა და მონაცემების დაცვის საკითხების თაობაზე მათი ინფორმირების გარეშე, სამართალდარღვევების ჩადენას ხშირად იწვევს; ამასთან, დაწესებულებებისთვის პასუხისმგებლობის მოხსნის საფუძველი თანამშრომლის მიმართ დისციპლინური ზომების გატარება ვერ გახდება. სწორედ დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირები არიან ვალდებულნი, რომ საკადრო ცვლილებებისას და პროცესების დაგეგმვისას გაითვალისწინონ პოტენციური რისკები, შესაძლო საფრთხეები და მონაცემთა დამუშავების კანონიერად წარმართვისათვის ადეკვატური ზომები მიიღონ.

სამსახურის მიერ განხორციელებული შემოწმებების ფარგლებში გამოიკვეთა ელექტრონულ სისტემაში დაცულ მონაცემებზე თანამშრომლებისათვის მინიჭებული წვდომის არასამსახურებრივი მიზნებისათვის გამოყენება, ასევე, მონაცემებზე იმ თანამშრომლის წვდომა, რომელსაც ელექტრონულ სისტემაში განპიროვნებული მომხმარებელი არ აქვს შექმნილი. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის თანახმად, მონაცემთა უსაფრთხოების მიზნით, ნებისმიერი თანამშრომელი ვალდებულია, არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს, დაიცვას მონაცემთა საიდუმლოება და კონფიდენციალურობა. მსგავსი გამოწვევების არსებობა ძირითადად მონიტორინგის/კონტროლის ეფექტიანი მექანიზმის არარსებობასთან არის დაკავშირებული. შესაბამისად, მონაცემების დაცვისა და ამ მიზნით შესასრულებლად აუცილებელი ზომების შესახებ თანამშრომლების ზედმიწევნით ინფორმირებულობის უზრუნველყოფის გარდა, მნიშვნელოვანია საჯარო უწყებებს მონაცემთა დამუშავების პროცესების სათანადო მონიტორინგის მექანიზმი ჰქონდეთ დანერგილი, რაც ეფექტიანია მონაცემთა უკანონო დამუშავების ფაქტების გამოვლენისა და პრევენციისათვის.

ერთ-ერთი შემოწმების ფარგლებში დადგინდა, რომ საჯარო დაწესებულების თანამშრომლების მიერ პირადი ელექტრონული ფოსტის მისამართების სამსახურებრივი მიზნებისთვის გამოყენებამ არაუფლებამოსილი პირისათვის ჯანმრთელობის შესახებ მოცულობითი მონაცემების შემთხვევითი გამჟღავნება გამოიწვია. პირადი დანიშნულების ელექტრონული ფოსტის მისამართების (მაგალითად, „Google“-ის ელექტრონული ფოსტის) გამოყენება მონაცემთა უკანონო დამუშავების რისკებს ზრდის, ხოლო შესაძლო უარყოფითი შედეგების მასშტაბი და ხარისხი ისეთ ფაქტორებზეა დამოკიდებული, როგორებიცაა: მონაცემების ტიპი, ინფორმაციის გაცვლის სიხშირე და სხვა. პირადი ელექტრონული ფოსტა, მონაცემთა უსაფრთხოების დაცვის თვალსაზრისით, სამსახურებრივი ელექტრონული ფოსტის სპეციფიკისაგან განსხვავებულია. მაგალითად, პირად ელექტრონულ ფოსტას დამსაქმებელი ვერ აკონტროლებს, რის გამოც დაწესებულება ამ გზით მიღებული პერსონალური ინფორმაციის შემდგომი შენახვისა და შესაძლო გამოყენების საწინააღმდეგოდ (თანამშრომლის სამსახურიდან გათავისუფლების შემთხვევაშიც) ეფექტიან ზომებს ვერ მიიღებს.

შესაბამისად, საჯარო უწყებების მითითება სამსახურებრივ ელექტრონულ ფოსტასთან დაკავშირებულ ისეთ გამოწვევებზე, როგორებიცაა ტექნიკური გაუმართაობა ან/და მეხსიერების სიმცირე, კანონმდებლობით დაკისრებული ვალდებულებების შეუსრულებლობის შემთხვევაში მხედველობაში მისაღებ ობიექტურ გარემოებად ვერ აღიქმება.

უმეტეს შემთხვევაში, თანამედროვე ტექნოლოგიური მიღწევების პირობებში, მონაცემთა დამუშავება ელექტრონული სისტემების მეშვეობით ხორციელდება. წინა წლის მსგავსად, მიმდინარე საანგარიშო პერიოდში, არაერთი საქმის შესწავლის ფარგლებში სხვადასხვა უწყების მართვისა და ადმინისტრირებების ქვეშ არსებულ ელექტრონულ სისტემებში მონაცემთა მიმართ განხორციელებული მოქმედებების აღრიცხვის (ე. წ. „ლოგირების“) მეთოდის პრობლემა გამოიკვეთა. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებულნი არიან სრულყოფილი „ლოგირება“ უზრუნველყონ. შედეგად შესაძლებელი ხდება როგორც არასანქცირებული წვდომის დროულად და ეფექტიანად გამოვლენა, ასევე – განხორციელებული ქმედების შინაარსის, დროის, განმახორციელებელი პირის ვინაობის სწორად იდენტიფიცირება და ფაქტებზე სათანადო რეაგირება.

სამიზნე აუდიტორიისათვის გარკვეული ინფორმაციის მისაწოდებლად საჯარო დაწესებულებები ოფიციალურ ვებგვერდებს იყენებენ. საანგარიშო პერიოდში სამსახურმა ერთ-ერთ გამოწვევად, სწორედ საჯარო გამოქვეყნების გზით მონაცემთა დამუშავების პროცესები შეაფასა. გასაჯაროება მონაცემთა დამუშავების იმდენად მძიმე ფორმაა, რომ ამგვარ შემთხვევებში მონაცემების არაკანონიერი დამუშავება ხშირად შეუქცევად ზიანს იწვევს. ამ კუთხით, სიფრთხილით უნდა შეირჩეს მონაცემების გასაჯაროების ვადა, რაც ხშირად პრობლემურია პროაქტიულად გამოქვეყნებული პერსონალური მონაცემების შემთხვევაში. მონაცემთა დამუშავების დაწყების სამართლებრივი საფუძვლის არსებობა არ განაპირობებს იმავე საფუძვლის ლეგიტიმურობას დამუშავების მთელი პროცესის განმავლობაში. ვებგვერდებზე მოძველებული მონაცემების ხელმისაწვდომობას დაწესებულებები ხშირად ელექტრონული რესურსების ტექნიკურ გაუმართაობას, სისტემების განახლების საჭიროებას ან/და განხორციელებულ საკადრო ცვლილებებს უკავშირებენ. მონაცემების არაკანონიერი დამუშავების თავიდან ასაცილებლად მნიშვნელოვანია, რომ პასუხისმგებელმა პირებმა პერიოდული მონიტორინგი გაუწიონ ვებგვერდებზე განთავსებულ მასალას, შეაფასონ პერსონალური მონაცემების შემცველი თითოეული დოკუმენტის საჯაროდ გამოქვეყნების ლეგიტიმური ინტერესები და, მიუხედავად ორგანიზაციულ-ტექნიკური სირთულეებისა, წაშალონ არაკანონიერად გავრცელებული მონაცემები.

დ. გამჭვირვალობის პრინციპის დაცვით მონაცემების დამუშავება

გამჭვირვალობის პრინციპის დაცვა მონაცემთა სუბიექტების ეფექტიანი ინფორმირებით მიიღწევა, რასაც ხშირად მონაცემთა დამუშავებისთვის

პასუხისმგებელი პირები პროაქტიულ პროცესად არ აღიქვამენ. მონაცემთა სუბიექტებისათვის ნათელი უნდა იყოს, რომ მათთან დაკავშირებული მონაცემები მუშავდება. ისინი დამუშავების მიზნების, მოცულობის, გზების, მეთოდების თაობაზე ინფორმაციას უნდა ფლობდნენ, რათა გააცნობიერონ რისკები და საჭიროების შემთხვევაში უზრუნველყონ საკუთარი უფლებების რეალიზება.

მონაცემთა დამუშავების შესახებ ინფორმაცია კონკრეტული, ადვილად შესამჩნევ ადგილზე განთავსებული, პირთა მაქსიმალურად ფართო წრისთვის გასაგები და ხელმისაწვდომი უნდა იყოს. საჭიროების შემთხვევაში შესაძლებელია, გამოყენებულ იქნეს ვიზუალური მასალა, ოფიციალური ვებგვერდი, როგორც ინფორმაციის ხელმისაწვდომის საშუალება და სხვა. ზემოაღნიშნული პრინციპის დაცვა განსაკუთრებით მნიშვნელოვანია, როდესაც მონაცემთა სუბიექტთა/პოტენციურ მონაცემთა სუბიექტთა ოდენობა დიდია, ხოლო დამუშავების პროცესები მრავალფეროვნებით ხასიათდება. ამგვარ შემთხვევებში გამჭვირვალობის პრინციპის სათანადო რეალიზების პრობლემა არაერთ შემოწმებაში გამოიკვეთა.

მიუხედავად იმისა, რომ საჯარო დაწესებულებებში მონაცემთა დამუშავების საფუძვლები უმეტესად კანონმდებლობით არის მოწესრიგებული, ხშირად სამართლებრივ აქტებში მოცემული ინფორმაცია გამჭვირვალობის პრინციპის დასაცავად საკმარისი არ არის. შესაბამისად, კანონით დადგენილი ახალი პრინციპის პრაქტიკაში იმპლემენტაციის გამოწვევაა იმ მექანიზმების იდენტიფიცირება, რომლებითაც მონაცემთა სუბიექტების სათანადო და პროაქტიული ინფორმირება მოხდება. აღნიშნული ხშირად სამართლებრივ აქტებში ცვლილებების შეტანასთან, სხვა დოკუმენტების შექმნასთან ან/და საზოგადოებისთვის ინფორმაციის შესაფერისი მეთოდებით მიწოდებასთან არის დაკავშირებული.

სამსახურის მიერ განხორციელებული ღონისძიებების საპასუხოდ, საჯარო დაწესებულებებმა გამჭვირვალობის პრინციპის დასაცავად შესაბამისი დოკუმენტაცია შექმნეს, რაზეც ინფორმაცია საზოგადოებას სხვადასხვა მეთოდით მიეწოდა.

თბილისის მუნიციპალიტეტში დამონტაჟდა მრავალი სპეციალური ვიზუალის გამაფრთხილებელი ნიშანი თბილისის მუნიციპალიტეტის მიერ ვიდეომონიტორინგის განხორციელების თაობაზე. ამდენად, საზოგადოებისთვის მოულოდნელი აღარ იქნება, გარკვეული ადმინისტრაციული სამართალდარღვევის ჩადენის შემთხვევაში ვიდეოკამერების ჩანაწერების მტკიცებულებებად გამოყენება.

ერთ-ერთი გარემოება, რამაც საანგარიშო პერიოდში ყურადღება მიიქცია, მონაცემთა დამუშავებისთვის ორი, ერთმანეთისგან განსხვავებული ინსტიტუტის - მონაცემთა სუბიექტის ინფორმირებისა და მონაცემთა სუბიექტის თანხმობის ერთმანეთში აღრევაა. ინფორმირება გამჭვირვალობის პრინციპის დასაცავად სხვადასხვა პროცედურით შეიძლება განხორციელდეს. მაგალითად, როდესაც მონაცემები უშუალოდ სუბიექტისგან გროვდება, პასუხისმგებელ პირებს განსხვავებული ვალდებულებები აქვთ, ხოლო როდესაც მათგან არ გროვდება, სუბიექტებამდე ინფორმაცია მაინც უნდა მივიდეს, ცალკეული გამონაკლისების გარდა. ინფორმირების მიზნით გაზიარებულ წერილობით დოკუმენტებზე

სუბიექტმა შეიძლება ხელი არც მოაწეროს, თუმცა ეს არ ნიშნავს, რომ მის წინაშე ინფორმირების ვალდებულება არ შესრულებულა. რაც შეეხება თანხმობას, ის მონაცემთა დამუშავების საფუძველია, ცალმხრივი ნების გამოვლენაა, მასზე ხელმოწერა ან/და ნების სხვაგვარად გამოხატვა აუცილებელია. თანხმობის ნამდვილობისთვის პრიორიტეტული დატვირთვა აქვს იმ შინაარსს, რომელზეც პირი თანხმობას აცხადებს. მეტიც, მოცულობითი დოკუმენტების ერთ-ერთ ნაწილად თანხმობის გათვალისწინების შემთხვევაში, მაგალითად, მომსახურების, სესხისა და სხვა ხელშეკრულებების მრავალპუნქტიანმა იურიდიულმა ტექსტმა ნებაყოფლობითი თანხმობის საფუძველი არ უნდა შთანთქას. საანგარიშო პერიოდში გამოიკვეთა, რომ დამუშავებისთვის პასუხისმგებელი პირები კარგად არ იცნობენ კანონის მოქმედი რედაქციით გათვალისწინებულ, მონაცემთა სუბიექტის თანხმობის სავალდებულო კომპონენტებს და თანხმობას ხშირ შემთხვევაში არასწორად მოიაზრებენ მონაცემთა დამუშავების სამართლებრივ საფუძვლად.

ე. მონაცემთა სუბიექტის უფლებების რეალიზება

პერსონალური მონაცემის ცნების ფართო შინაარსის გათვალისწინებით, როგორც მონაცემთა სუბიექტებისათვის, ასევე დამუშავებისთვის პასუხისმგებელი პირებისათვის, გარკვეული ინფორმაციის პერსონალურად იდენტიფიცირება კვლავ გამოწვევად რჩება. პერსონალური მონაცემის ცნების ქვეშ, გარდა პირის მაიდენტიფიცირებელი, საკონტაქტო, საბანკო თუ სხვა სახის ინფორმაციისა, მონაცემთა სუბიექტის ქცევა, მასთან დაკავშირებული მოსაზრებები და შეფასებები, ასევე, პირის ფსიქო-სოციალური თუ ფიზიკური თავისებურებებიც მოიაზრება. თავის მხრივ, პერსონალური მონაცემის ცნების სწორად იდენტიფიცირება, მონაცემთა დამუშავების პროცესების კანონიერად წარმართვისა და მონაცემთა სუბიექტების უფლებების ჯეროვნად რეალიზებისთვის არსებითად მნიშვნელოვანია.

ხშირია შემთხვევები, როდესაც ფიზიკური პირები სამსახურისთვის მომართვის გზით იმედოვნებენ, რომ მესამე პირების თაობაზე ინფორმაციას, სუბიექტის ინფორმირების უფლების რეალიზებით მოიპოვებენ. მსგავს საკითხებზე რეაგირება სამსახურის კომპეტენციის ფარგლებს სცდება ისეთ შემთხვევაში, როდესაც მესამე პირების შესახებ ინფორმაცია იმავდროულად არ წარმოადგენს სუბიექტის პერსონალურ მონაცემს.

საანგარიშო პერიოდში, მონაცემთა სუბიექტებმა კანონის მე-13 და მე-14 მუხლით გათვალისწინებული ინფორმაციის მიღების, მონაცემთა გაცნობისა და ასლის გამოთხოვის უფლებებით არაერთხელ ისარგებლეს; ხოლო საპასუხო რეაგირებების მართლზომიერების შეფასებისას გამოვლინდა, რომ საჯარო დაწესებულებების მხრიდან ინფორმაციის/დოკუმენტაციის არასრულად მოძიების/მიწოდების პრობლემები ძირითადად ელექტრონული სისტემების ძიების მექანიზმის არასრულყოფილი პარამეტრებით იყო გამოწვეული. ცალკეულ შემთხვევებში მონაცემთა სუბიექტის უფლებების ჯეროვანი დაცვის მიმართ

დაბალი ორგანიზაციული კულტურაც გამოიკვეთა, რამაც უფლების რეალიზების პროცესი შეაფერხა.

მონაცემთა სუბიექტის უფლებების რეალიზების ქმედითი მექანიზმების შემუშავების ჭრილში მნიშვნელოვანია, აღინიშნოს კანონის 26-ე მუხლით[3] დადგენილი ვალდებულება, რომელიც გულისხმობს მომსახურების პროცესში მონაცემთა დაცვის სტანდარტის გათვალისწინებას, როგორც მონაცემთა სუბიექტის უფლებების ეფექტიანი რეალიზების საშუალებას.

მონაცემთა სუბიექტის ინფორმირების უფლება აბსოლუტურ უფლებათა კატეგორიას არ მიეკუთვნება, თუმცა ხშირად სხვა უფლებების რეალიზების წინაპირობებს ქმნის და ინფორმაციული თვითგამორკვევის კონსტიტუციური უფლების განხორციელების საშუალებაა. შესაბამისად, მონაცემთა დაცვის სფეროში მოქმედი კანონმდებლობა ამ უფლების შეზღუდვის მოცულობას/გზებს და აღნიშნულის თაობაზე ფიზიკური პირისათვის ინფორმაციის სწრაფად, გასაგებად, ეფექტიანად მიწოდებას დიდ მნიშვნელობას ანიჭებს. თავის მხრივ, უფლების ჯეროვანი რეალიზება ძირითადად მოწესრიგებული მონაცემთა დამუშავების სისტემების, სათანადო ცოდნის მქონე თანამშრომლებისა და პერსონალური მონაცემების დაცვის მიმართ დამკვიდრებული ორგანიზაციული კულტურის პირობებშია შესაძლებელი, რაც, წინსვლის მიუხედავად, კვლავ გამოწვევაა.

ცალკეულ შემთხვევებში საჯარო დაწესებულებები დარგობრივ სამართლებრივ აქტებზე (მაგალითად, საგადასახადო კანონმდებლობაზე) მითითებით მიიჩნევენ, რომ, თუკი მონაცემების გამოქვეყნების შესაძლებლობა რეგლამენტირებულია, თუმცა წაშლის გზით დამუშავება — არა, მათ არ აქვთ წაშლის უფლებამოსილება. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით და ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ აღიარებულია მონაცემთა წაშლის უფლება (ე. წ. „დავიწყების უფლება“), რომლის შეზღუდვა მხოლოდ კანონმდებლობით პირდაპირ გათვალისწინებულ შემთხვევებშია შესაძლებელი. რა თქმა უნდა, მონაცემთა წაშლის, მისი განხორციელების თაობაზე თითოეული სფეროს მომწესრიგებელ კანონმდებლობაში ჩანაწერის არარსებობა, მონაცემთა წაშლის მოთხოვნის დაკმაყოფილებაზე უარის თქმის საფუძვლად ვერ იქნება მიჩნეული. არსებითი მნიშვნელობისაა, საჯარო უწყებებმა მონაცემთა დამუშავების თითოეული პროცესი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ჭრილში შეაფასონ.

ვ. არასრულწლოვანის მონაცემების დამუშავება

ბავშვის საუკეთესო ინტერესებისათვის უპირატესობის მინიჭება მნიშვნელოვანი პრინციპია და იგი ბავშვთან დაკავშირებული ნებისმიერი გადაწყვეტილების მიღების პროცესზე ვრცელდება. შესაბამისად, მონაცემების

[3] მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი, ახალი პროდუქტის ან მომსახურების შექმნისას.

დამუშავების დროს დამუშავებისთვის პასუხისმგებელმა და დამუშავებაზე უფლებამოსილმა პირებმა არასრულწლოვანის საუკეთესო ინტერესის განსაზღვრისათვის ინდივიდუალური და სათანადო მიდგომები უნდა გამოიყენონ. მათ შორის: შესაძლებლობის შემთხვევაში ჩართონ არასრულწლოვანი გადაწყვეტილების მიღების პროცესში; ბავშვს გაესაუბრონ მისი ლექსიკური მარაგისა და სოციალურ-კულტურული მახასიათებლების გათვალისწინებით შესაბამისი სპეციალიზაციის მქონე პირების დახმარებით შეაფასონ ბავშვის მიერ გამოხატული ნება და მხედველობაში მიიღონ ისეთი ფაქტორები, როგორებიცაა ასაკი და შეზღუდული შესაძლებლობის სტატუსი (ასეთის არსებობის შემთხვევაში). მსგავსი მიდგომები, ერთი მხრივ, ხელს შეუწყობს ბავშვის, როგორც მონაცემთა სუბიექტის, უფლებების ჯეროვნად განხორციელებას, ხოლო, მეორე მხრივ, მონაცემთა უკანონო დამუშავების პრევენციას მოახდენს. ხშირია შემთხვევები, როდესაც, ბავშვის მონაცემების დამუშავების ფაქტებთან დაკავშირებული ინსპექტირებების ფარგლებში, ორგანიზაციები ნაკლებად წარმოაჩენენ თავიანთ პოზიციებს ბავშვის საუკეთესო ინტერესების უპირატესად გათვალისწინებიდან გამომდინარე. საყურადღებოა, რომ, არასრულწლოვნის მონაცემების დამუშავების შემთხვევაში, კანონით გათვალისწინებულ თითოეულ საფუძველთან ერთად, სამსახური ბავშვის საუკეთესო ინტერესების უპირატესობის საკითხებსაც აფასებს.

საგანმანათლებლო დაწესებულებების რაოდენობის, საქმიანობის სპეციფიკის მრავალფეროვნების, დასაქმებულ და განათლების მიმღებ პირთა რიცხოვნობის გათვალისწინებით, ამ სფეროში მონაცემთა დამუშავების პროცესებთან დაკავშირებული არაერთი გამოწვევა გამოიკვეთა. სკოლებში, ბაგა-ბაღებში დასაქმებული პირები, ყოველდღიური, საქმიანი და პირადი ურთიერთობებიდან გამომდინარე, ფორმალურ და არაფორმალურ გარემოში პროფესიული ხასიათის არაერთ მონაცემს მოიპოვებენ და გასცემენ. თავის მხრივ, პროფესიული საქმიანობისას მონაცემთა დამუშავება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედების სფეროში ექცევა. შესაბამისად, დაწესებულებებმა, დირექციის თანამშრომლებმა, პედაგოგებმა როგორც კოლეგებთან, ასევე მოსწავლეებთან ან/და სხვა პირებთან დაკავშირებული ინფორმაციის სოციალურ ქსელებში გამოქვეყნებამდე, სპეციალური დანიშნულების ე. წ. „ჩათებში“ განთავსებამდე მონაცემების დამუშავების საფუძვლის არსებობა უნდა შეაფასონ.

კანონის იმპლემენტაციის საწყის ეტაპზე საჯარო სკოლები მონაცემთა სუბიექტის თანხმობის მოპოვებას არასწორად ცდილობდნენ. როგორც წესი, თანხმობის ფორმებს თავად სკოლები ადგენენ, ხოლო ბავშვების წარმომადგენლები დოკუმენტზე ხელმოწერას აფიქსირებენ. თავის მხრივ, საჯარო სკოლებში მიმდინარე სტანდარტულ მონაცემთა დამუშავების პროცესები კანონმდებლობით არის მოწესრიგებული. გარდა ამისა, განათლებით უზრუნველყოფა სახელმწიფოს მიერ შეთავაზებული მომსახურებაა. კონკრეტულ სკოლაში ჩარიცხვის საკითხზე არსებობს მშობლების განაცხადი, შესაბამისად, მონაცემთა სუბიექტის თანხმობა, როგორც საფუძველი, გამოსადეგია მხოლოდ ცალკეულ შემთხვევებში. ამასთან, მნიშვნელოვანი საკითხია თანხმობის სწორად მოპოვებაც. სუბიექტმა თანხმობა უნდა განაცხადოს კონკრეტული და მკაფიო, კანონიერი მიზნით მონაცემების

დამუშავებაზე. სკოლების მიერ ზემოხსენებული თანხმობების მოპოვების მცდელობისას დოკუმენტის სტანდარტული ტექსტი ამ ინფორმაციას არ შეიცავდა და ასევე ბუნდოვანებას იწვევდა დოკუმენტში ასახული იმგვარი მონაცემების საჭიროება, როგორებიცაა ბიომეტრიული და განსაკუთრებული კატეგორიის ინფორმაცია. მნიშვნელოვანია, თანხმობის ტექსტის იმგვარად ჩამოყალიბება, რომ არ იწვევდეს ბუნდოვანებასა და არაგონივრულად ფართო ინტერპრეტირების შესაძლებლობას.

გასათვალისწინებელია ისიც, რომ ბავშვებისთვის, როგორც იმ პირებისთვის, რომელთაც ფიზიკური და ფსიქოლოგიური სიმწიფისთვის არ მიუღწევიათ, პერსონალური მონაცემების დამუშავებასთან დაკავშირებული რისკები, შედეგები, დაცვის მექანიზმები და მათი უფლებების ფარგლები შესაძლოა ნაკლებად იყოს ცნობილი. აქედან გამომდინარე, ბავშვების მონაცემების კანონიერად დამუშავებისთვის, მათი სიზუსტისთვის, განახლებისთვის, პროაქტიული ზომების მიღება კრიტიკულად მნიშვნელოვანია. განსაკუთრებით მაშინ, როდესაც ოჯახის სრულწლოვან წევრებთან ერთად ბავშვები სხვადასხვა პროგრამის ან/და პროცესის მონაწილენი ხდებიან, შესაძლოა მხოლოდ კანონიერი წარმომადგენლის ინფორმირებულობა საკმარისი არ იყოს. საანგარიშო პერიოდში გამოვლინდა შემთხვევა, როდესაც ბავშვის მონაცემები წლების განმავლობაში სოციალურად დაუცველი ოჯახის წევრის სტატუსით მუშავდებოდა, თუმცა ბავშვის მშობლები განქორწინებულნი იყვნენ, სოციალურად დაუცველ ოჯახში ბავშვის ბებია და მამა აღირიცხებოდა, ხოლო ბავშვი მრავალი წლის განმავლობაში დედასთან ცხოვრობდა. თავის მხრივ, მოქმედი კანონმდებლობით სოციალურად დაუცველი ოჯახი განმარტებულია, როგორც ერთ მისამართზე მცხოვრები საერთო მეურნეობის მქონე ფიზიკურ პირთა ერთობა. შესწავლილ შემთხვევაში დადგინდა, რომ ბავშვი თავდაპირველად მამასთან ერთად მის საცხოვრებელ მისამართზე იმყოფებოდა, ხოლო შემდეგ, წლების განმავლობაში, სხვა რეგიონში დედასთან ერთად დიდი ხნით ცხოვრობდა. აღნიშნულის მიუხედავად, არ გადამოწმებულა და შეცვლილა სოციალურად დაუცველი ოჯახის წევრების შემადგენლობა და ბავშვის შესახებ ხანგრძლივი პერიოდით მუშავდებოდა მისი სოციალური სტატუსის თაობაზე არაზუსტი მონაცემები. მსგავსი შემთხვევების გამოსავლენად სოციალური მუშაობის სხვადასხვა ღონისძიების გამოყენება შესაძლოა ეფექტიანი და პრევენციული იყოს.

ზ. შრომით ურთიერთობასთან დაკავშირებული მონაცემების დამუშავება

შრომითი ურთიერთობები მონაცემთა დამუშავების პროცესების მრავალფეროვნებით ხასიათდება, რაც ხშირ შემთხვევაში ურთიერთობის ხანგრძლივობის, მასშტაბისა და დამუშავებული მონაცემების დიდი მოცულობით არის განპირობებული. სამსახურმა ერთ-ერთი საჯარო დაწესებულების მიერ ყოფილ დასაქმებულთან დაკავშირებული დისციპლინური წარმოების მასალების საქმისწარმოების ელექტრონულ სისტემაში იმგვარი ფორმით განთავსება

გამოავლინა, რამაც დოკუმენტზე არასანქცირებული წვდომები განაპირობა. დისციპლინური წარმოების მასალები სენსიტიური ბუნების მქონეა, რამდენადაც, დასაქმებულისათვის დამდგარი სამართლებრივი შედეგის სიმძიმის მიუხედავად, ისინი უარყოფითი კონტექსტისა და დატვირთვის მატარებელია. აქედან გამომდინარე, დამუშავების პროცესში მონაწილე პირებმა დისციპლინურ წარმოებასთან დაკავშირებული მონაცემების შემცველი მასალის უსაფრთხოებისათვის ორგანიზაციულ-ტექნიკური ზომები სიფრთხილით უნდა შეარჩიონ და ეფექტიანად დაიცვან მათი კონფიდენციალობა.

მონაცემთა არაკანონიერი დამუშავების შემთხვევები ხშირად დასაქმებულების შეცდომებით არის გამოწვეული. ინსპექტირებების ფარგლებში, ასეთ დროს დამსაქმებლები უმეტესად დისციპლინურ სამართალწარმოებას წარმართავენ და თანამშრომლების სამსახურებრივ გადაცდომებზე სახდელების დაკისრების გზით რეაგირებენ. აღნიშნული არ გამორიცხავს ფაქტების სამსახურის მიერ შეფასების შესაძლებლობას; ხოლო საზედამხედველო ორგანოს მიერ ჩატარებული შემოწმებების ფარგლებში განსაკუთრებული ყურადღება დამსაქმებლის მიერ მიღებულ იმ ორგანიზაციულ-ტექნიკურ პროცესებს ექცევა, რომლებმაც დასაქმებული ადამიანების მხრიდან მონაცემების შეცდომით, არაკანონიერად დამუშავების რისკები უნდა შეამციროს.

დისციპლინური წარმოების მასალების, განსაკუთრებით მოწმეების ვინაობისა და მათი ჩვენებების თაობაზე დიდი დაინტერესება სამსახურში წარმოდგენილ მომართვებშიც შეინიშნება. მონაცემთა სუბიექტები ხშირად აპროტესტებენ მათთვის გადაცემულ მასალებში სხვა ფიზიკური პირების მონაცემების დაშტრიხვას. ასეთ შემთხვევებში სამსახურის კომპეტენცია მონაცემთა სუბიექტის უფლების (საკუთარი მონაცემების დამუშავების, მასალების შესახებ ინფორმირებულობის თაობაზე) რეალიზების კონტროლით შემოიფარგლება. თავის მხრივ, სხვა პირთა მონაცემების შემცველი დოკუმენტების, ვიდეოჩანაწერების, აუდიოჩანაწერების მონაცემთა სუბიექტებისთვის გადასაცემ ეფექტიან მეთოდს, გარეშე სუბიექტების შესახებ მონაცემების დაფარვა, ე. წ. „დაშტრიხვა“, წარმოადგენს. შესაბამისად, სამსახურის კომპეტენციისა და საკუთარი უფლებების შესახებ მონაცემთა სუბიექტების ცნობიერების ამაღლება კვლავ აქტუალური საკითხია.

საანგარიშო პერიოდში შესწავლილი საქმეების მიხედვით, მონაცემთა სუბიექტებს ხშირად აქვთ განცდა, რომ მათ, როგორც ფიზიკურ პირებს, შრომითი ურთიერთობის დეტალებისა და ნიუანსების საჯარო წყაროებში მიმოხილვის უფლება აქვთ, ხოლო დამსაქმებლებს - არა. თავის მხრივ, ინფორმაციის ღიაობა სახელმწიფო დაწესებულებების ანგარიშვალდებულების ამაღლებასა და საქმიანობის ეფექტიანობის ზრდას უწყობს ხელს. აქტიური ზრუნვა განსაკუთრებით იმ საჯარო დაწესებულებებს უწევთ, რომლებიც დიდი რაოდენობით მოქალაქეებს სხვადასხვა ტიპის მომსახურებას უწევენ, რათა ეფექტიანად შეასრულონ დაკისრებული მოვალეობები, საზოგადოებაში მოიპოვონ/შეინარჩუნონ ნდობა და საქმიანი რეპუტაცია. აღნიშნულის მისაღწევად, ცალკეულ შემთხვევებში, ისინი ყოფილ/მოქმედ დასაქმებულებთან დაკავშირებული ფაქტების თაობაზე საზოგადოების წინაშე იმ ინფორმაციას პასუხობენ, რაც პირთა განუსაზღვრელი წრის წინაშე თავად თანამშრომლებმა

გაავრცელეს და დაწესებულების რეპუტაციას საფრთხეს უქმნის. მსგავს შემთხვევებში კრიტიკულად მნიშვნელოვანია გასაჯაროებული მონაცემების მინიმიზებული მოცულობის შერჩევა.

თ. აუდიო- და ვიდეომონიტორინგი

საჯარო დაწესებულებების მიერ აუდიომონიტორინგის განხორციელება მონაცემთა დამუშავების გავრცელებული ფორმაა. საანგარიშო პერიოდში შესწავლილი საქმეების მიხედვით, აუდიომონიტორინგის მიზნები მომსახურების ხარისხის მონიტორინგს, ჩატარებული ადმინისტრაციული წარმოებების ეფექტიანობასა და გამჭვირვალობას უკავშირდება.

საგულისხმოა, რომ აუდიომონიტორინგის თაობაზე არაჯეროვანი ინფორმირების არაერთი შემთხვევა გამოვლინდა. დამუშავებისთვის პასუხისმგებელი პირი აუდიომონიტორინგის მიმდინარეობის თაობაზე ინფორმაციის მიწოდების ვალდებულებას სათანადოდ ვერ შეასრულებს, თუ მისი თანამშრომლები მონაცემთა დამუშავების გარემოებებს არასათანადოდ ფლობენ (მაგალითად, არ იციან ამ გზით ხდება თუ არა მონაცემთა შეგროვება, თუ ხდება - რა მიზნით, საფუძვლით და ა. შ.). ფიზიკური პირების სწორად ინფორმირების მნიშვნელობა იზრდება, როდესაც განმცხადებელს აუდიომონიტორინგის შესახებ ობიექტური მოლოდინი აქვს, რასაც შეიძლება დაწესებულებების ცხელ ხაზზე მიღებული განმარტებები ან ვებგვერდებზე არსებული ინფორმაცია ქმნიდეს.

გამოვლენილი შემთხვევების მიხედვით, მონაცემთა სუბიექტების ინფორმირების საკითხის (მაგალითად, მისაწოდებელი ინფორმაციის შინაარსის) მხოლოდ პრაქტიკით მოწესრიგება უფლების არათანმიმდევრულ და არაჯეროვან რეალიზებას ხშირად განაპირობებს. საჯარო დაწესებულებების ნაწილს არ აქვს შემუშავებული კანონით გათვალისწინებული სპეციალური წერილობითი წესი ან იგი მხოლოდ ფრაგმენტულად ასახავს აუდიომონიტორინგის მიზანსა და მოცულობას, ხანგრძლივობას, აუდიოჩანაწერზე წვდომის, მისი შენახვისა და განადგურების წესსა და პირობებს, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმებს.

ვიდეომონიტორინგი, როგორც მონაცემთა დამუშავების ერთ-ერთი ყველაზე ფართოდ გავრცელებული ფორმა, კანონის მოთხოვნების ზედმიწევნით დაცვით უნდა წარიმართოს. სამსახურმა საჯარო დაწესებულებების მიერ ვიდეომონიტორინგის თაობაზე გამაფრთხილებელი ნიშნების როგორც არარსებობის, ასევე არასათანადო, რთულად შესამჩნევ ადგილებზე განთავსების რამდენიმე ფაქტი გამოავლინა. შესაბამისად, არაერთ საქმეში განიმარტა გამაფრთხილებელი ნიშნის თვალსაჩინო ადგილზე განთავსების სპეციფიკა. კერძოდ, გამაფრთხილებელი ნიშანი ისეთ სივრცეში უნდა განთავსდეს, რომ მასზე დატანილი წარწერა და გამოსახულება აღქმადი იყოს ვიდეომონიტორინგის სივრცეში მოხვედრილი ნებისმიერი ადამიანისთვის. ამასთან, ვიდეომონიტორინგის განმახორციელებელი დაწესებულების თაობაზე ინფორმაცია მონაცემთა სუბიექტებისათვის უნდა იყოს ნათელი, რათა სწრაფად და ეფექტიანად უზრუნველყონ საკუთარი უფლებების რეალიზება.

საანგარიშო პერიოდში საგზაო მოძრაობის წესებთან დაკავშირებული ადმინისტრაციული სამართალდარღვევების ფარგლებში შეინიშნებოდა თბილისში, შუქნიშნის ბოძებზე, დამონტაჟებული თბილისის მუნიციპალიტეტის სარგებლობაში არსებული ვიდეოკამერების გამოყენების ფაქტები, ხოლო მონაცემთა სუბიექტები ხშირად ასაჩივრებდნენ აღნიშნული ფორმით მოპოვებული პერსონალური მონაცემების (ფოტოსურათების, ვიდეოჩანაწერების) კანონიერებას. შესწავლილი საქმეების ნაწილში გამოვლინდა გამაფრთხილებელი ნიშნების თვალსაჩინო ადგილზე არარსებობის შემთხვევები, ხოლო ამ მიმართულებით გაცემული დავალებები უმოკლეს ვადებში შესრულდა.

1.2. პრეცედენტული გადაწყვეტილებები

ა. ინციდენტთან დაკავშირებული ვალდებულებების შეუსრულებლობა

— ქალაქ თბილისის მუნიციპალიტეტის მერიის და ა(ა)იპ — „მუნიციპალური სერვისების განვითარების სააგენტოს“ ელექტრონული სისტემის მეშვეობით მონაცემთა ბაზაზე არასანქცირებული წვდომა და მონაცემების მოპოვება

სამსახურმა, ანონიმური შეტყობინების საფუძველზე, ინციდენტთან დაკავშირებული ვალდებულებების შეუსრულებლობის ფაქტი გამოავლინა. შეტყობინება შეიცავდა ბმულს, რომელშიც ასახული იყო ინგლისურენოვანი ტერმინები, რაც ა(ა)იპ — „მუნიციპალური სერვისების განვითარების სააგენტოდან“ მოპოვებული მონაცემების გაყიდვის შეთავაზებაზე მიუთითებდა. დაწესებულებიდან მონაცემების გამჟღავნების თაობაზე გარკვეული სახის ინფორმაციას ქართულენოვანი წყაროებიც შეიცავდა.

შემოწმების ფარგლებში გამოვლინდა, რომ სააგენტო ერთ-ერთი ელექტრონული სისტემის მართვასა და ადმინისტრირებას ახორციელებდა, რომელშიც, სხვადასხვა მუნიციპალური სერვისის მიღების მიზნით, დაინტერესებული ფიზიკური და იურიდიული პირები რეგისტრირდებოდნენ. აღნიშნული სისტემის მეშვეობით, სსიპ — „სახელმწიფო სერვისების განვითარების სააგენტოს“ მონაცემთა ელექტრონულ ბაზაზე რეალურ დროში დაშვებისა და ფიზიკურ პირებზე ინფორმაციის მიღების შესაძლებლობა ჰქონდა. საქმეში არსებული მტკიცებულებებით დადგინდა, რომ ზემოაღნიშნული ელექტრონული სისტემის მეშვეობით მონაცემთა დამუშავების პროცესში ა(ა)იპ — „მუნიციპალური სერვისების განვითარების სააგენტო“ დამუშავებაზე უფლებამოსილი პირის სტატუსით მონაწილეობდა, ხოლო ქალაქ თბილისის მუნიციპალიტეტის მერია — დამუშავებისთვის პასუხისმგებელი პირის სტატუსით.

სააგენტო და მერია განმარტავდნენ, რომ ელექტრონულ სისტემაში ფიქსირდებოდა „ანომალიური“, არასტანდარტული ქცევა, რის თაობაზეც საგამოძიებო ორგანოს მიმართეს, თუმცა თავად არ შეუფასებიათ დასახელებული

ქცევის გავლენა სისტემაში დაცულ პერსონალურ მონაცემებზე. ასევე, დაზუსტებით არ იცოდნენ, მოხდა თუ არა ინციდენტი. სააგენტო ინფორმირებული იყო ერთ-ერთ ვებგვერდზე განთავსებული პერსონალური მონაცემების გაყიდვის შესახებ, ხოლო მყიდველისთვის საილუსტრაციოდ, ღიად ფიქსირდებოდა ათეულობით ადამიანის შესახებ ინფორმაცია, რაც ინციდენტის განმახორციელებელი პირის მიერ არასანქცირებული მოქმედებების დროს გამოყენებულ მონაცემთა ბაზაში ასახულს ემთხვეოდა. საქმის შესწავლის ფარგლებში დადგინდა ინციდენტის არსებობა, რაც სააგენტოს ადმინისტრირების ქვეშ არსებული ელექტრონული სისტემის მეშვეობით მონაცემთა ბაზაზე არასანქცირებულ წვდომასა და მონაცემების მოპოვებაში გამოიხატა; ხოლო ინციდენტის ადამიანის უფლებებსა და თავისუფლებაზე გავლენის მასშტაბი/ხარისხი სამსახურისათვის შეტყობინებისა და მონაცემთა სუბიექტის ინფორმირების ვალდებულებას წარმოშობდა. ინსპექტირების შედეგად მოპოვებული მტკიცებულებებით გამოვლინდა, რომ სააგენტომ და მერიამ არ დაადგინეს ინციდენტის არსებობა და, შესაბამისად, არ აღრიცხეს იგი. გარდა ამისა, მერიას ინციდენტის თაობაზე სამსახურისთვის და მონაცემთა სუბიექტებისთვის ინფორმაცია არ მიუწოდებია. აღნიშნული საქმის შესწავლისას ყურადღება შემდეგ საკითხებზე გამახვილდა:

ელექტრონულ სისტემაში მომხმარებლის რეგისტრაციის მეთოდი იძლეოდა სხვა პირის საიდენტიფიკაციო მონაცემებით რეგისტრაციის შესაძლებლობას. კერძოდ, მომხმარებლის ანგარიშის შესაქმნელად საჭირო იყო ორი ზუსტი, ამასთან (საჯაროდ ხელმისაწვდომი ინფორმაციიდან გამომდინარე), ადვილად მოპოვებადი მონაცემი — გვარი და პირადი ნომერი, ხოლო ელექტრონული ფოსტის მისამართად და სატელეფონო ნომრად შეიძლებოდა მონაცემების გამოყენება, რომლებსაც რეგისტრაციის განმახორციელებელი პირი ფლობდა. შესწავლის შედეგად დადგინდა, რომ, ზემოაღნიშნულ ელექტრონულ სისტემაში რამდენიმე მომხმარებლის ანგარიშის რეგისტრაციის მიზნით, ინციდენტის განმახორციელებელმა სუბიექტმა, სავარაუდოდ, საჯაროდ ხელმისაწვდომი წყაროებიდან მიითვისა მონაცემთა სუბიექტების პერსონალური მონაცემები (გვარი და პირადი ნომერი). თავის მხრივ, აღნიშნული პირები სამეწარმეო სუბიექტების დირექტორები/ხელმძღვანელები იყვნენ.

ინციდენტის განმახორციელებელმა პირმა ზემოაღნიშნულ ელექტრონულ სისტემაში შექმნა მეწარმე სუბიექტების დირექტორების/ხელმძღვანელების მომხმარებლები, ხოლო რეგისტრაციის პროცესში გამოიყენა ერთჯერადი „Email“ სერვისის პროვაიდერების დომენზე რეგისტრირებული ელექტრონული ფოსტის მისამართები, რომელთა მეშვეობითაც მიიღო სხვა პირების მომხმარებლების რეგისტრაციის პროცესის წარმატებით დასრულებისათვის საჭირო ინფორმაცია. აღნიშნულის შემდეგ, მითითებული ელექტრონული სისტემის ერთ-ერთი ფუნქციონალის მეშვეობით, სხვადასხვა გვარისა და პირადი ნომრის ასახვით, რამდენიმე დღის განმავლობაში მოთხოვნები გააგზავნა სსიპ — „სახელმწიფო სერვისების განვითარების სააგენტოს“ მონაცემთა ელექტრონულ ბაზაში, რომელსაც მოთხოვნის წარმატებულად გაგზავნის შემთხვევაში შესაბამისი ინფორმაციის უკან დაბრუნების ვალდებულება ხელშეკრულებით ჰქონდა აღებული.

ელექტრონული სისტემის ტექნიკური მოწყობიდან გამომდინარე, ინციდენტის განმახორციელებელ პირს სხვა პირების პერსონალური მონაცემების მოპოვების შესაძლებლობა ჰქონდა მხოლოდ მაშინ, თუ კონკრეტული გვარი და პირადი ნომერი რეგისტრირებული იქნებოდა როგორც სსიპ — „სახელმწიფო სერვისების განვითარების სააგენტოს“ მონაცემთა ელექტრონულ ბაზაში, ისე – თავად სააგენტოს მართვის/ადმინისტრირების ქვეშ არსებულ ელექტრონულ სისტემაში. გაგზავნილი ასიათასობით მოთხოვნიდან ათეულობით ათას შემთხვევაში ორივე ბაზაში ერთმანეთს დაემთხვა ფიზიკური პირების გვარები და პირადი ნომრები. შესაბამისად, ინციდენტის განმახორციელებელმა პირმა მოიპოვა რამდენიმე ათეულობით ათასი პირის სხვადასხვა პერსონალური მონაცემი (მაგალითად: ტელეფონის ნომერი, მისამართი, ელექტრონული ფოსტის მისამართი და სხვა).

შეფასებული უსაფრთხოების ზომების მიხედვით, ინციდენტი რამდენიმე ფაქტორმა გამოიწვია, მათ შორის: ელექტრონული სისტემა იძლეოდა უცხო ფიზიკური პირის პირადი ნომრის, ასევე – გვარის მითითებითა და ნებისმიერი აქტიური ელექტრონული ფოსტის მისამართისა და მობილური ტელეფონის ნომრით ვერიფიცირების შესაძლებლობას. ამასთან, სსიპ — „სახელმწიფო სერვისების განვითარების სააგენტოს“ მონაცემთა ბაზიდან ინფორმაციის გამოთხოვის პროცესში გათვალისწინებული არ იყო კომპიუტერისა და ადამიანის განმასხვავებელი სრულად ავტომატური „ტურინგის ტესტი“ („Re Capture“ ფუნქციონალი), რაც მნიშვნელოვანია მავნე პროგრამული საშუალებების არამართლზომიერი ქმედებების თავიდან ასაცილებლად. გარდა ამისა, ინციდენტამდე პერიოდში პერსონალური მონაცემების ავტომატური გამოთხოვის მეთოდით სსიპ — „სახელმწიფო სერვისების განვითარების სააგენტოდან“ შესაძლებელი იყო ერთდროულად ყველა იმ მონაცემის მოპოვება, რომლებიც გათვალისწინებული იყო შესაბამისი ხელშეკრულებით, თუმცა ამ მონაცემებიდან სხვადასხვა სერვისს განსხვავებული მოცულობის ინფორმაცია სჭირდებოდა. ასევე, უწყებას შემუშავებული არ ჰქონდა ელექტრონულ სისტემაში მონაცემების მიმართ განხორციელებული მოქმედებების აღრიცხვის (ე. წ. „ლოგირების“) სრულყოფილი მექანიზმი და გათვალისწინებული არ იყო ინციდენტის დროული გამოვლენისთვის მნიშვნელოვანი ორგანიზაციულ-ტექნიკური ზომები, რაც არსებითია ინციდენტის შეწყვეტისა და მავნე შედეგების შემსუბუქებისათვის.

საქმის შესწავლის ფარგლებში მოპოვებულ მტკიცებულებებსა და ინციდენტის გამოვლენისა და შეფასების მარეგულირებელ ნორმატიულ აქტებზე დაყრდნობით, სამსახურმა განსაზღვრა გამოვლენილი ინციდენტის თავისებურებები და დაადგინა, რომ ადამიანის უფლებებისა და თავისუფლებებისათვის ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის მაღალი ალბათობა არსებობდა; მოცემული საკითხის შეფასებისას კი მხედველობაში სხვადასხვა ფაქტორი იქნა მიღებული — მაგალითად: ინციდენტის სახე, მონაცემთა სუბიექტების რაოდენობა, დამუშავებისათვის პასუხისმგებელი სუბიექტის საქმიანობის განსაკუთრებული ხასიათი და მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობის ხარისხი. შესწავლის ფარგლებში დადგინდა სააგენტოს მიერ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე და 28-ე მუხლის, ხოლო მერიის მიერ — კანონის 28-ე, 29-ე და 30-ე მუხლების

დარღვევა. შესაბამისად, დამუშავებაზე უფლებამოსილი პირი სამართალდამრღვევად იქნა ცნობილი ამავე კანონის 76-ე და 77-ე მუხლებით გათვალისწინებული სამართალდარღვევისთვის, ხოლო დამუშავებისთვის პასუხისმგებელი პირი — 77-ე, 78-ე და 79-ე მუხლებით გათვალისწინებული სამართალდარღვევებისთვის.

— **ერთ-ერთმა სამედიცინო დაწესებულებამ სიმსივნის დიაგნოზის მქონე ათეულობით პირის მონაცემები სახელმწიფო შესყიდვების ვებგვერდზე შემთხვევით გაამჟღავნა**

პერსონალურ მონაცემთა დაცვის სამსახურში წარმოდგენილი ინფორმაციის საფუძველზე საზედამხედველო ორგანომ, გენეტიკურ მუტაციებზე ჩატარებული ანალიზების სახელმწიფო შესყიდვების საჯარო ვებგვერდზე განთავსებით, მონაცემთა გამჟღავნების კანონიერება და სავარაუდო ინციდენტის შესახებ სამსახურისათვის შეტყობინების ვალდებულების შესრულება შეისწავლა.

საწყის ეტაპზე გამოვლინდა, რომ გასაჯაროებული დოკუმენტი 200-ამდე ფიზიკური პირის სახელს, გვარს, პირად ნომერს, ჩატარებული სამედიცინო კვლევების დასახელებას, თარიღს შეიცავდა და მასში მითითებული კვლევების სახელწოდებები პაციენტების სიმსივნის დიაგნოზზე მიუთითებდა. თავის მხრივ, სახელმწიფო შესყიდვების პორტალი, რომლის ადმინისტრირებასაც სსიპ — „სახელმწიფო შესყიდვების სააგენტო“ ახორციელებს, საჯარო დაწესებულებების მიერ შესყიდვების ღია და გამჭვირვალე ელექტრონული ტენდერების მეშვეობით განხორციელებას უზრუნველყოფს. საკითხის მნიშვნელობასა და შესაძლო საფრთხეებს ელექტრონულ ტენდერებთან დაკავშირებით სისტემაში განთავსებული ინფორმაციის საჯარო ხასიათი განაპირობებდა. შესაბამისად, დოკუმენტში ასახული ფიზიკური პირებისათვის მიყენებული ზიანის არსებითად შემცირების მიზნით, სამსახურმა მონაცემების დაბლოკვის გადაწყვეტილება შესწავლის დასრულებამდე მიიღო, რაც სააგენტომ დაუყოვნებლივ შეასრულა.

პაციენტების პერსონალური მონაცემების შემცველი დოკუმენტი სატენდერო დოკუმენტაციის ნაწილს არ წარმოადგენდა და იგი სისტემაში პრეტენდენტი კომპანიის ერთ-ერთმა თანამშრომელმა შეცდომით ატვირთა. კომპანიამ ელექტრონულ ტენდერთან დაკავშირებული დოკუმენტების სისტემაში ატვირთვა იმ პირს დაავალა, რომელსაც სახელმწიფო შესყიდვების მიმართულებით გამოცდილება არ ჰქონია და რაიმე სახის დამატებითი კვალიფიკაციის ასამაღლებელი კურსი არ გაუვლია. ამასთან, იგი სისტემაში განთავსებული მონაცემების საჯარო ბუნებასა და სახელმწიფო შესყიდვების ზოგადი პრინციპების თაობაზე ინფორმირებული არ ყოფილა.

ტენდერში მონაწილე ორგანიზაცია და ელექტრონულ ტენდერებზე პასუხისმგებელი პირი შესყიდვების პროცესში მონაცემების დამუშავების სპეციფიკასა და შესაძლო რისკებს სრულად უნდა აცნობიერებდეს. ეს საკითხი მით უფრო აქტუალურია, როდესაც პრეტენდენტი სამედიცინო დაწესებულებაა, სადაც დიდი რაოდენობის ფიზიკურ პირთა შესახებ ჯანმრთელობასთან დაკავშირებული

სხვადასხვა შინაარსის მონაცემი იყრის თავს. სწორედ დამუშავებისთვის პასუხისმგებელი პირია ვალდებული, მათ შორის საკადრო ცვლილებების შემთხვევაში, გაითვალისწინოს თანამშრომლების გამოცდილებიდან მომდინარე საფრთხეები და მონაცემთა უსაფრთხოების უზრუნველსაყოფად ადეკვატური ზომები მიიღოს. სათანადო სიფრთხილის გამოჩენის საჭიროებაზე მიანიშნებს, რომ სისტემაში ატვირთული ინფორმაცია/დოკუმენტაცია პირთა განუსაზღვრელი წრისთვის ხდება ხელმისაწვდომი და ტენდერის მხარეებს მათი შეცვლის, დამატების, წაშლის ტექნიკური შესაძლებლობა არ აქვთ.

ამდენად, მონაცემთა უსაფრთხოების დასაცავად სათანადო ორგანიზაციულ-ტექნიკური ზომების მიუღებლობით კომპანიამ დაარღვია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის (მონაცემთა უსაფრთხოება) მოთხოვნები და 76-ე მუხლის შესაბამისად, სამართალდამრღვევად იქნა ცნობილი.

გარდა ამისა, კომპანიის თანამშრომლის მიერ ზემოაღნიშნული დოკუმენტის შემთხვევით უკანონოდ გასაჯაროების ფაქტი ინციდენტად იქნა მიჩნეული, რის გამოც დამუშავებისთვის პასუხისმგებელი პირის მიერ სპეციფიკური ვალდებულებების შესრულება შეფასდა.

კომპანიამ პაციენტების პერსონალური მონაცემების შემცველი დოკუმენტის საჯაროდ გამოქვეყნება მართებულად მიიჩნია ინციდენტად და შეადგინა ოქმი, თუმცა ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა და სიმძიმე არ შეუფასებია. ამასთან, კომპანიას სამსახურისთვის არ შეუტყობინებია ინციდენტის თაობაზე და სააგენტოსათვის მიმართვის გზით შეეცადა, მოეგვარებინა პრობლემა.

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტით (2024 წლის 28 თებერვლის №19 ბრძანებით) დამტკიცებული კრიტერიუმების შესაბამისად, პერსონალურ მონაცემთა დაცვის სამსახურმა ინციდენტის სახე და სიმძიმე შეაფასა. მიიჩნია, რომ დაირღვა მონაცემთა კონფიდენციალურობა, ხოლო ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა შეფასებული იქნა, როგორც — საშუალო. შეფასებისას მხედველობაში იქნა მიღებული მონაცემთა სუბიექტების რაოდენობა, მონაცემების ხასიათი, დოკუმენტის ნახვის ოდენობა და ინციდენტის მოკლე ვადაში აღმოჩენის ფაქტი.

ამასთან, კომპანიის მიერ სააგენტოსათვის ინფორმაციის მიწოდება არ შეფასდა სამსახურისთვის შეტყობინების ვალდებულების შესრულების ტოლფასად, რამდენადაც სააგენტო ვერ უზრუნველყოფდა საზედამხედველო ორგანოსთვის დამუშავებისთვის პასუხისმგებელი პირის მიერ კანონითა და ნორმატიული წესით განსაზღვრული ფორმისა და შინაარსის მქონე ინფორმაციის მოწოდებას. სამსახურისთვის ინციდენტის შეტყობინების პროცესი არ არის ფორმალური და მონაცემთა დაცვის საზედამხედველო ორგანოს, საკუთარი მანდატის ფარგლებში, აქვს ისეთი ეფექტიანი მექანიზმების (მაგალითად, დაბლოკვის) გამოყენების უფლებამოსილება, რომლითაც შესაძლოა არსებითად შემსუბუქდეს ინციდენტის შედეგები.

ამდენად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 29-ე მუხლის შესაბამისად, კომპანიამ ვერ უზრუნველყო ადამიანის

უფლებებისთვის საშუალო საფრთხის შემცველი ინციდენტის შესახებ სამსახურისთვის შეტყობინების ვალდებულების შესრულება, რის გამოც, კანონის 78-ე მუხლის შესაბამისად, იგი სამართალდამრღვევად იქნა ცნობილი.

ბ. პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული გამოწვევები

პერსონალურ მონაცემთა დაცვის სამსახურმა არაგეგმურად შეისწავლა მუნიციპალიტეტების ოცზე მეტი ორგანოს, რამდენიმე სკოლის, უნივერსიტეტის, სხვადასხვა საჯარო სამართლის იურიდიული პირის, საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს, საქართველოს იუსტიციის სამინისტროსა და სხვა უწყებებს დაქვემდებარებული საჯარო სამართლის, ასევე – არასამეწარმეო არაკომერციული იურიდიული პირების მიერ პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის/განსაზღვრის ვალდებულების ჯეროვანი შესრულების ფაქტები. მათ შორის:

— ერთ-ერთი მუნიციპალიტეტის საკრებულოს შემოწმების ფარგლებში დადგინდა, რომ დაწესებულებამ პერსონალურ მონაცემთა დაცვის ოფიცრად განსაზღვრა საკრებულოს აპარატის უფროსი, რომელსაც ახალი ფუნქციები თავის ძირითად სამსახურებრივ უფლებამოსილებებზე დამატებით დააკისრა. შესაბამისად, ის ხელმძღვანელობდა აპარატს და ადამიანურ რესურსებს, საორგანიზაციო საკითხებს, ადმინისტრაციულ საქმისწარმოებასა და სხვა მიმართულებებს. ამასთან, მონაცემთა დამუშავების მიზნებისა და საშუალებების განსაზღვრაში გადაწყვეტილების მიმღებ პირად მონაწილეობდა. მაგალითად, ითანხმებდა კორესპონდენციების შინაარსს და მათ ვიზირებას ახდენდა დოკუმენტბრუნვის ელექტრონულ სისტემაში, სასამართლო დავებთან დაკავშირებით გადაწყვეტილებას იღებდა წარსადგენი მტკიცებულებების შესახებ და წყვეტდა სხვა მენეჯერულ საკითხებს. მოქმედი კანონმდებლობის გარდა, სამსახური ასევე დაეყრდნო „მონაცემთა დაცვის ევროპული საბჭოს“ განმარტებებს, რომელთა მიხედვით ინტერესთა კონფლიქტის არარსებობა მჭიდროდ არის დაკავშირებული პერსონალურ მონაცემთა დაცვის ოფიცრის მიერ მიუკერძოებლად და დამოუკიდებლად საქმიანობის განხორციელების შესაძლებლობასთან.[4] შესაბამისად, ოფიცერი თავად არ უნდა იყოს დაწესებულებაში დასაქმებული პირი, რომელიც პერსონალურ მონაცემთა დამუშავების მიზნებსა და საშუალებებს განსაზღვრავს ანდა მონაწილეობს მათ განსაზღვრაში.[5] ზემოაღნიშნულიდან გამომდინარე, სამსახურმა დაადგინა კანონის 33-ე

[4] Guidelines on Data Protection Officers (‘DPOs’), European Commission, endorsed by EDBP, 2017, 16.

[5] Guidelines on Data Protection Officers (‘DPOs’), European Commission, endorsed by EDBP, 2017, 16. აქვე აღსანიშნავია, რომ, პერსონალურ მონაცემთა დაცვის ოფიცრისთვის ინტერესთა კონფლიქტის საკითხთან დაკავშირებით, მართლმსაჯულების ევროპული სასამართლოც ანალოგიურ განმარტებას აკეთებს იხ., Judgment of the Court, ECJ, Case C-453/21, 09/02/2024, par. 44, 46.2.

მუხლის მე-5 პუნქტის (პერსონალურ მონაცემთა დაცვის ოფიცერს უფლება აქვს, შეასრულოს სხვა ფუნქციაც, თუ ეს არ წარმოშობს ინტერესთა კონფლიქტს) არაჯეროვანი შესრულების ფაქტი.

— ერთ-ერთ სკოლასთან მიმართებით მიღებულ გადაწყვეტილებაში სამსახურმა შეაფასა პერსონალურ მონაცემთა დაცვის ოფიცრის სათანადო ცოდნისა და ინტერესთა კონფლიქტის საკითხი. შესწავლის შედეგად დადგინდა, რომ სკოლას განსაზღვრული ჰყავდა პერსონალურ მონაცემთა დაცვის ოფიცერი, რომელიც იმავდროულად დასაქმებული იყო სკოლის პედაგოგისა და კონცერტმაისტერის პოზიციაზე. პედაგოგი გაწევრიანებული იყო სკოლის კოლეგიურ ორგანოში — პედაგოგიურ საბჭოში. საბჭო გადაწყვეტილებას იღებს სკოლაში მიმდინარე/განსახორციელებელ მნიშვნელოვან ღონისძიებებზე, როგორიცაა, მაგალითად, სამუშაო და სასწავლო გეგმები; მითითებული საქმიანობა კი, თავის მხრივ, მონაცემთა დამუშავების მრავალმხრივ პროცესებს მოიცავს. როდესაც დაწესებულების მოქმედი თანამშრომელი ოფიცრად განისაზღვრება, ის მხოლოდ ოფიცრის უფლებამოსილებას უნდა ასრულებდეს ან დამატებით ითავსებდეს სხვა ისეთ ფუნქციებს, რომელთა განხორციელებისას არ წარმოიშობა ინტერესთა კონფლიქტი. ფუნქციებს შორის ინტერესთა კონფლიქტის არარსებობა მნიშვნელოვანია იმისათვის, რომ ოფიცერმა სათანადოდ შეძლოს ვითარების ობიექტური აღქმა, საჭირო მექანიზმების პრაქტიკაში ინტეგრირება და შემდგომი რეაგირება. შესაბამისად, გადაწყვეტილების მიხედვით, ვინაიდან პედაგოგი უშუალოდ მონაწილეობს სკოლის მიზნების შესრულებასა და სკოლაში მონაცემთა დამუშავებასთან დაკავშირებული კონკრეტული პროცესების დაგეგმვაში, ასევე, განგრძობადი და პირდაპირი შეხება აქვს საგანმანათლებლო დაწესებულების ძირითად მონაცემთა სუბიექტებთან (მოსწავლეებთან), ის ვერ შეითავსებს პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციას. რაც შეეხება მონაცემთა დაცვის სფეროში ოფიცრის სათანადო ცოდნის საკითხის შეფასებას, იგი უნდა ფლობდეს კანონის სიღრმისეულ ცოდნას; მონაცემთა დაცვის ოფიცრისთვის განსაზღვრული კონკრეტული დავალებების შესასრულებლად აუცილებელ უნარებს; პიროვნულ თვისებებს, რათა ხელი შეუწყოს, მხარი დაუჭიროს და მიაღწიოს დაწესებულების შესაბამისობას კანონის მოთხოვნებთან; ასევე უნდა ფლობდეს კანონთან შესაბამისობის დასადასტურებლად საჭირო დოკუმენტაციის ცოდნას. ამასთან, ოფიცერს საბაზისო ცოდნა უნდა ჰქონდეს საინფორმაციო ტექნოლოგიების, მონაცემთა უსაფრთხოების მიმართულებით და უნდა იცნობდეს დაწესებულების საქმიანობის მარეგულირებელ საკანონმდებლო და კანონქვემდებარე აქტებს.[6] თავის მხრივ, მონაცემთა დამუშავების სფეროში სათანადო ცოდნის შეძენის სხვადასხვა საშუალება არსებობს. მაგალითად, შესაძლებელია, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესწავლა და სამსახურისაგან შესაბამისი

[6] იხ. პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაცია - „მინიმალური სტანდარტი პერსონალურ მონაცემთა დაცვის ოფიცრებისთვის“, 6-7.

კონსულტაციების მიღება; ხელმისაწვდომ სხვადასხვა საინფორმაციო შეხვედრასა და შესაბამის სასწავლო კურსზე/ტრენინგზე დასწრება; სამსახურის ვებგვერდზე განთავსებული სხვადასხვა სარეკომენდაციო შინაარსის დოკუმენტის გაცნობა მონაცემთა დამუშავებასთან დაკავშირებულ არაერთ საკითხზე, მათ შორის – არასრულწლოვნების მონაცემების დაცვის წესების თაობაზე და სხვა. განხილულ შემთხვევაში დადგინდა, რომ პედაგოგი, რომელიც ამავდროულად პერსონალურ მონაცემთა დაცვის ოფიცრის პოზიციას იკავებდა, არ ფლობდა პერსონალურ მონაცემთა დაცვის სფეროს მარეგულირებელი კანონმდებლობის საბაზისო ცოდნას. მას დაწესებულებიდან არ მიეწოდა სათანადო ინფორმაცია და არც სხვა საშუალებით გადამზადებულა. ზემოაღნიშნულიდან გამომდინარე, სამსახურმა დაადგინა კანონის 33-ე მუხლის მე-5 პუნქტის (პერსონალურ მონაცემთა დაცვის ოფიცერს უნდა ჰქონდეს სათანადო ცოდნა მონაცემთა დაცვის სფეროში) არაჯეროვანი შესრულების ფაქტი.

— საანგარიშო პერიოდში გამოვლინდა, რომ რამდენიმე მუნიციპალიტეტის საკრებულოსა და მერიას დანიშნული ჰყავდა პერსონალურ მონაცემთა დაცვის ოფიცერი, თუმცა მისი საიდენტიფიკაციო და საკონტაქტო მონაცემები პროაქტიულად არ ჰქონდა გამოქვეყნებული. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებულნი არიან, პერსონალურ მონაცემთა დაცვის ოფიცრის ვინაობა და საკონტაქტო ინფორმაცია პროაქტიულად გამოაქვეყნონ ვებგვერდზე (ასეთის არსებობის შემთხვევაში) ან სხვა ხელმისაწვდომი საშუალებით. სამსახურმა შეაფასა საზოგადოებისთვის ხელმისაწვდომი ფორმით ინფორმაციის გამოქვეყნების მეთოდები და მსგავსი მნიშვნელობა მიენიჭა მოქმედ ვებგვერდებს, რომლებზეც დაწესებულებები სისტემატურად აახლებენ ინფორმაციას, ასევე – ადმინისტრაციულ შენობებში არსებულ საინფორმაციო დაფებს. შესაბამისად, საჯარო უწყებებს მიეცათ დავალებები და რეკომენდაციები, მათ შორის უკვე გამოქვეყნებულ მონაცემებთან დაკავშირებით (სხვა ინფორმაციისგან განცალკევებულად), რომ იგი ყველასთვის ხელმისაწვდომად და მარტივად გამოქვეყნებულიყო.

— საანგარიშო პერიოდში გამოვლინდა რამდენიმე შემთხვევა, როდესაც დაწესებულებებმა სამსახურის გადაწყვეტილებით პერსონალურ მონაცემთა დაცვის ოფიცერთან დაკავშირებით დადგენილი დავალებები არ შეასრულეს ან/და მათ შესასრულებლად მხოლოდ ნაწილობრივი ღონისძიებები გაატარეს. მსგავს შემთხვევებში სამსახურმა დავალების შეუსრულებლობის ფაქტებზე ინსპექტირებები (ე. წ. „რეინსპექტირებები“) ჩაატარა. ცალკეულ დაწესებულებებთან მიმართებით „რეინსპექტირების“ ფარგლებში გამოიკვეთა, რომ განსაზღვრული პერსონალურ მონაცემთა დაცვის ოფიცრები ვერ აკმაყოფილებდნენ სათანადო ცოდნის თაობაზე კანონით დადგენილ სტანდარტს. გარდა ამისა, გამოვლინდა ისეთი შემთხვევები, როდესაც, პერსონალურ მონაცემთა დაცვის სამსახურის გადაწყვეტილებით მიღებული

დავალების მიუხედავად, დაწესებულებებმა არ დანიშნეს პერსონალურ მონაცემთა დაცვის ოფიცერი, რაც სამსახურის მიერ კანონის 87-ე მუხლის (სამსახურის კანონიერი მოთხოვნის შეუსრულებლობა) დარღვევად შეფასდა.

გ. პირის სახელისა და გვარის შემცველი საფინანსო დეკლარაციის უცხოური ძალის ინტერესების გამტარებელ ორგანიზაციათა რეესტრში გამოქვეყნების გზით დამუშავება

„უცხოური ძალის გამჭვირვალობის შესახებ“ საქართველოს კანონი და „უცხოური ძალის ინტერესების გამტარებელ ორგანიზაციათა რეესტრის წარმოების, საფინანსო დეკლარაციის წარდგენისა და მონიტორინგის წესი“ მონაცემების დამუშავების პროცესების განმსაზღვრელი ახალი ნორმატიული რეგულაციებია. სამსახურმა, შეტყობინების საფუძველზე, „უცხოური ძალის ინტერესების გამტარებელ ორგანიზაციათა რეესტრში“ გამოქვეყნებულ ერთ-ერთ საფინანსო დეკლარაციაში მომართვის ავტორის პერსონალური მონაცემების დამუშავების კანონიერება შეისწავლა.

საქმის გარემოებების მიხედვით, შეტყობინების ავტორმა მომსახურების ხელშეკრულების საფუძველზე ერთ-ერთი ორგანიზაციიდან ფულადი ანაზღაურება რამდენჯერმე მიიღო, გარკვეული დროის გასვლის შემდეგ კი ორგანიზაციათა რეესტრში მისი სახელის, გვარისა და სხვა მონაცემების შემცველი საფინანსო დეკლარაცია გამოქვეყნდა.

კანონმდებლობის თანახმად, თუ სუბიექტი უცხოური ძალის ინტერესების გამტარებელ ორგანიზაციად მიჩნევის კრიტერიუმებს აკმაყოფილებს (მაგალითად, თუ ორგანიზაციის მთლიანი შემოსავლის 20%-ზე მეტის წყარო უცხოური ძალაა), იგი ვალდებულია, ორგანიზაციათა რეესტრში რეგისტრაციის მიზნით სააგენტოს მიმართოს და ნორმატიული აქტით დადგენილი ფორმების შესაბამისად შევსებული საფინანსო დეკლარაცია წარადგინოს. აღნიშნულის შემდეგ სააგენტოში საფინანსო დეკლარაციის შესწავლისა და გამოკვლევის ეტაპი იწყება, რომლის ფარგლებში შესაძლებელია სხვადასხვა სუბიექტისგან საჭირო ინფორმაციის გამოთხოვა. თუ ორგანიზაცია კრიტერიუმებს აკმაყოფილებს, თუნდაც მის მიერ წარდგენილი დეკლარაცია არ იყოს ფორმის შესაბამისად სრულად შევსებული, სუბიექტი ორგანიზაციათა რეესტრში რეგისტრირდება და საფინანსო დეკლარაცია ვებგვერდზე ქვეყნდება.

მოცემული საქმის განხილვის ფარგლებში დადგინდა, რომ ორგანიზაციის მიერ სააგენტოში წარდგენილ საფინანსო დეკლარაციაში შეტყობინების ავტორის სახელთან, გვართან და ხელფასის სახით მიღებული თანხის ოდენობასთან ერთად, მითითებული იყო მისი პირადი ნომერი. საფინანსო დეკლარაციაში აღნიშნული იყო, რომ შეტყობინების ავტორის მიერ მიღებული ხელფასი საშემოსავლო გადასახადით არ დაიბეგრა, ხოლო „ხარჯების გაწევის მიზნის“ გრაფაში მითითებული იყო, რომ მან „ისარგებლა 6000 ლარამდე საშემოსავლო შეღავათით (შშმ პირი)“. ვინაიდან საფინანსო დეკლარაციის წარდგენის შემდეგ განხორციელებული ნორმატიული ცვლილებების გამო დეკლარაციის ფორმაში

საჭირო აღარ იყო პირადი ნომრის მითითება, სააგენტომ სპეციალური პროგრამული კოდის გამოყენებით შეტყობინების ავტორის პირადი ნომერი დეკლარაციაში დამალა. ამასთან, საფინანსო დეკლარაციის ფორმაში ასახული შენიშვნის თანახმად, „ხარჯების გაწევის მიზანი“ ისე უნდა ჩამოყალიბებულიყო, რომ მასში განსაკუთრებული კატეგორიის პერსონალური მონაცემები არ აღნიშნულიყო. აქედან გამომდინარე, სააგენტომ დეკლარაციაში ასახული ტერმინი „შშმ პირი“ წაშალა და მომართვის ავტორის სახელისა და გვარის შემცველი საფინანსო დეკლარაცია ვებგვერდზე გამოაქვეყნა.

სააგენტოსა და საქართველოს იუსტიციის სამინისტროს მიერ განხილვის ფარგლებში წარმოდგენილი განმარტებების მიხედვით, სახელისა და გვარის შემცველი საფინანსო დეკლარაციის გამოქვეყნება საჭირო იყო ორგანიზაციათა საქმიანობის გამჭვირვალობის მიზნის მისაღწევად; ამასთან, კანონის თანახმად, საფინანსო დეკლარაცია საჯაროა, ხოლო კანონქვემდებარე აქტით დამტკიცებულ მის ფორმაში შესავსებ ერთ-ერთ გრაფას თანხის მიმღები პირის სახელი და გვარი წარმოადგენდა; გარდა ამისა, საფინანსო დეკლარაციაში თანხის მიმღები პირების სახელებისა და გვარების მითითება შეფასებისა და გამოკვლევის ეტაპის სრულყოფილად წარმართვის მიზანს ემსახურებოდა; ხოლო დეკლარაციის სადავო ფორმით გამოქვეყნების საფუძვლებად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლის პირველი პუნქტის „გ“ (კანონით გათვალისწინებული შემთხვევა) და „დ“ (კანონმდებლობით დაკისრებული მოვალეობის შესასრულებლად საჭიროება) ქვეპუნქტები დასახელდა.

აღსანიშნავია, რომ სამართლებრივი საფუძვლების თაობაზე წარმოდგენილი პოზიცია სამსახურმა არ გაიზიარა. გადაწყვეტილებაში ყურადღება გამახვილდა შემდეგ გარემოებაზე: სააგენტოს მიერ გამოქვეყნებულ არაერთ საფინანსო დეკლარაციაში ასახული არ იყო იმ პირის სახელი და გვარი, რომელმაც ორგანიზაციის მიერ გაწეული ხარჯი მიიღო; კანონი და მის საფუძველზე მიღებული კანონქვემდებარე აქტი დეკლარაციის საშუალებით, ორგანიზაციის მიერ გაწეული ხარჯის ნაწილში, გამოსაქვეყნებელ ინფორმაციად ასახელებდა მხოლოდ ფულადი თანხის ოდენობასა და მიზანს (განსხვავებით მიღებული შემოსავლების მიმართ წარსადგენი ინფორმაციისაგან, რომელზეც წყაროც უნდა დასახელებულიყო); ასევე, მართალია, კანონმდებლობა საფინანსო დეკლარაციის საჯაროობაზე მიუთითებდა, თუმცა საფინანსო დეკლარაცია საჯარო ხდებოდა სააგენტოს მიერ სათანადო გამოკვლევისა და შეფასების შემდეგ (აღნიშნული პროცესი კი, სააგენტოს პრაქტიკის მიხედვით, მათ შორის მოიცავდა სპეციალური პროგრამული კოდით მონაცემების დამალვას ან სააგენტოს თანამშრომლის მხრიდან მონაცემის წაშლას). შესაბამისად, კანონმდებლობა არ ადგენდა ზუსტად იმგვარი ფორმით დოკუმენტის გასაჯაროების ვალდებულებას, როგორითაც ის წარდგენილი იყო. სააგენტოს საფინანსო დეკლარაციის ის რედაქცია უნდა გამოექვეყნებინა, რომელიც უცხოური გავლენის გამჭვირვალობის უზრუნველსაყოფად ფართო საზოგადოების ლეგიტიმურ ინტერესებს პასუხობდა.

ამასთან, გამოვლინდა, რომ უცხოური ძალის ინტერესების გამტარებელ ორგანიზაციათა რეესტრში რეგისტრაციამდე მონაცემები სხვადასხვა ფორმით მუშავდებოდა, მაგალითად: ორგანიზაციებიდან ან/და სხვა პირებიდან ინფორმაციის მოპოვება, მოპოვებული ინფორმაციის გამოყენება ახალი

რეგულაციებით დადგენილი კომპეტენციის ფარგლებში, საჭიროების შემთხვევაში ხარვეზის დადგენა ან ინფორმაციის მესამე პირებისგან გამოთხოვა, მათი მიღება, შენახვა, მონიტორინგი და სხვა. არსებულ ნორმატიულ აქტებსა და მათ ექსპლიციტურ ჩანაწერებზე დაყრდნობით სამსახურმა განმარტა, რომ წესით დადგენილი საფინანსო დეკლარაციის ფორმა არ არის ის დოკუმენტი, რომლითაც კანონმდებლობა ორგანიზაციათა რეესტრში გამოსაქვეყნებელი და საჯაროდ გასავრცელებელი ინფორმაციის ჩამონათვალს განსაზღვრავს, არამედ ეს არის ფორმა/ნიმუში, რომელმაც უნდა უზრუნველყოს სააგენტოსათვის იმ ინფორმაციის წარდგენა, რომელიც საფინანსო დეკლარაციის სათანადო შესწავლასა და გამოკვლევაში დაეხმარება. შესაბამისად, კანონმდებლობა არ ითვალისწინებდა ორგანიზაციიდან ხარჯის მიმღები პირის სახელისა და გვარის შემცველი სახით დეკლარაციის გამოქვეყნებას და, ამდენად, მოცემულ შემთხვევას არ შეესაბამებოდა სააგენტოს მიერ დასახელებული მონაცემების დამუშავების არცერთი საფუძველი.

ზემოაღნიშნულიდან გამომდინარე, დადგინდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლის (მონაცემთა დამუშავების საფუძვლები) დარღვევა, რის გამოც სააგენტო ცნობილ იქნა სამართალდამრღვევად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 67-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული სამართალდარღვევისთვის.

შემოწმების ფარგლებში გამოვლინდა, რომ შეტყობინების ავტორის დამსაქმებელმა ორგანიზაციამ სათანადო ყურადღება არ მიაქცია საფინანსო დეკლარაციაში არსებულ განმარტებას, რომლის მიხედვით ხარჯების გაწევის მიზანი ისეთი ფორმით უნდა ჩამოყალიბებულიყო, რომ მასში თანხის მიმღები ფიზიკური პირის განსაკუთრებული კატეგორიის პერსონალური მონაცემები არ ასახულიყო. ამასთან, შეტყობინების ავტორს მისი შშმ სტატუსისა და სტატუსის მინიჭების კონკრეტული საფუძვლის თაობაზე ინფორმაცია საჯაროდ ხელმისაწვდომი წყაროებით თავად ჰქონდა გავრცელებული. შესაბამისად, ორგანიზაციის მიერ სააგენტოსათვის შშმ პირის სტატუსის გამო საშემოსავლო შეღავათის თაობაზე ინფორმაციის მიწოდება შეფასდა მონაცემების მინიმიზაციის პრინციპის დარღვევად („პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „გ“ ქვეპუნქტი), რის გამოც იგი ცნობილ იქნა სამართალდამრღვევად კანონის 66-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებულ სამართალდარღვევაში.

დ. სსიპ — „საჯარო რეესტრის ეროვნული სააგენტოს“ მიერ თანამშრომლის დისციპლინური საქმისწარმოების ფარგლებში მონაცემების დამუშავება

გადაცდომის ჩამდენი თანამშრომლის მონაცემები დისციპლინური საქმისწარმოების ფარგლებში განსაკუთრებული სიფრთხილით უნდა დამუშავდეს. მსგავს შემთხვევებში მონაცემების უსაფრთხოების საკითხი უაღრესად მნიშვნელოვანია. პერსონალურ მონაცემთა დაცვის სამსახურმა სსიპ საჯარო რეესტრის ეროვნული სააგენტოს ყოფილი თანამშრომლის მომართვის

საფუძველზე დისციპლინური წარმოების მასალების არაუფლებამოსილი პირებისთვის ხელმისაწვდომობის ფაქტი შეისწავლა.

განცხადების განხილვის ფარგლებში დადგინდა, რომ სააგენტოს ყოფილმა თანამშრომელმა სსიპ — „იუსტიციის სახლში“ წარდგენილი მიმართვით სააგენტოდან გამოითხოვა შრომით ურთიერთობასთან დაკავშირებული მოცულობითი ინფორმაცია, მათ შორის – დისციპლინური წარმოების მასალები. მოთხოვნილი მასალის ისეთი ნაწილები, როგორებიცაა: თანამდებობაზე დანიშვნის ბრძანებები, ხელშეკრულება და ა. შ., სატელეფონო ნომერზე მისული მოკლეტექსტური შეტყობინების გზით გახდა ხელმისაწვდომი, თუმცა მას დისციპლინური წარმოების მასალები არ გადასცემია. საკითხის მოკვლევის შედეგად განმცხადებელმა შეიტყო, რომ მის მიმართვაზე რეაგირების მიზნით სხვა წერილი მომზადდა, რომელიც, დისციპლინური წარმოების მასალებთან ერთად, დოკუმენტბრუნვის ელექტრონული სისტემის საშუალებით იუსტიციის სახლის თანამშრომლისთვის იყო ხელმისაწვდომი.

შესწავლის ფარგლებში გამოვლინდა, რომ წერილების შინაარსობრივი სეგრეგაციის მიზნით სააგენტოს დოკუმენტბრუნვის სისტემაში შესული, შესრულებული და შიდა მოძრაობის კორესპონდენციის ორი ტიპი აისახებოდა — „საჯარო“, რომელიც პროგრამის ყველა მომხმარებლისთვის იყო ხელმისაწვდომი და „მკაცრად არასაჯარო“, რომელიც პროგრამის მხოლოდ ექსკლუზიური უფლების მქონე პირებისთვის იყო ხილვადი. სააგენტოს მიერ დამტკიცებული წესით „მკაცრად არასაჯარო“ კორესპონდენციების მახასიათებლები (პერსონალური მონაცემების, თანამშრომელთა სამუშაო ადგილისა და თანამდებობრივი სარგოს შესახებ ინფორმაციის შემცველი წერილები და ა. შ.) და მასზე წვდომის მქონე პირთა შეზღუდული წრე იყო განსაზღვრული. სააგენტომ დაადასტურა, რომ ყოფილი თანამშრომლის მიერ წარდგენილი განცხადება, ასევე მასზე საპასუხოდ მომზადებული ორივე წერილი „მკაცრად არასაჯარო“ კორესპონდენციის ტიპს მიეკუთვნებოდა და მათზე წვდომის შესაძლებლობა მხოლოდ სააგენტოს თანამშრომელთა მცირე წრეს უნდა ჰქონოდა. მიუხედავად ამისა, სააგენტოს თანამშრომლის შეცდომის გამო, დისციპლინური წარმოების შემცველი წერილი „საჯარო“ ტიპის დოკუმენტად მომზადდა.

შეცდომით მომზადებულ წერილზე დართული იყო დასაქმებულ პირთან დაკავშირებული დისციპლინური დასკვნა, რომელიც წარმოების პროცესში გამოკითხული სააგენტოს თანამშრომლების დეტალურ განმარტებებსა და შრომით ურთიერთობებში ყველაზე მძიმე სახდელის (სამსახურიდან გათავისუფლება) შეფარდების შესახებ ინფორმაციას შეიცავდა. სამსახურის შეფასებით, წერილის შინაარსისა და თანდართული დოკუმენტაციის ბუნების გათვალისწინებით, დისციპლინური წარმოების მასალების სააგენტოს ყველა თანამშრომლისა და იუსტიციის სახლის დაახლოებით რვაასი მიმღები ოპერატორისათვის ხელმისაწვდომობა შესაძლოა განმცხადებლისთვის მნიშვნელოვანი რეპუტაციული და მორალური ზიანის მატარებელი ყოფილიყო. ამასთან, სააგენტომ ზემოხსენებულ წერილზე წვდომა მხოლოდ და მხოლოდ მას შემდეგ შეზღუდა, რაც განცხადების განხილვის დაწყებასთან დაკავშირებით სამსახურის კორესპონდენციები მიიღო.

სამსახურმა გაითვალისწინა ის გარემოება, რომ განმცხადებლის მოთხოვნაზე პასუხის მომზადების პროცესში სააგენტოს არაერთი, მათ შორის მაღალი რგოლის, მენეჯერი მონაწილეობდა, ხოლო მომზადებული წერილის ტიპი და სათაური დოკუმენტის „საჯარო“ ხასიათზე მიუთითებდა. აღნიშნულის მიუხედავად, დოკუმენტის ვიზირების/ხელმოწერის პროცესში ზემდგომმა თანამდებობის პირებმა ვერ შენიშნეს კორესპონდენციის მახასიათებლები. შესაბამისად, მათ თავიდან ვერ აიცილეს წერილის არასწორი ფორმით მომზადების თანმდევი შედეგები.

ყოველივე ზემოხსენებული მიუთითებდა „პერსონალურ მონაცემთა დაცვის შესახებ“[7] საქართველოს კანონის მე-17 მუხლის (მონაცემების უსაფრთხოება, კანონის მოქმედი რედაქციის 27-ე მუხლი) დარღვევაზე, რის გამოც, ამავე კანონის 46-ე მუხლის (კანონის მოქმედი რედაქციის 76-ე მუხლი მუხლი) საფუძველზე, სსიპ — „საჯარო რეესტრის ეროვნული სააგენტო“ სამართალდამრღვევად იქნა ცნობილი.

ე. სსიპ — „გ. აბრამიშვილის სახელობის საქართველოს თავდაცვის სამინისტროს სამხედრო ჰოსპიტალისა“ და ამავე ჰოსპიტალის თანამშრომლის მიერ ელექტრონული სისტემა „მედსერვისის“ მეშვეობით მონაცემების დამუშავება

როგორც წესი, მონაცემთა დამუშავების პროცესები თანამშრომლების მეშვეობით წარიმართება, ხოლო მონაცემების უსაფრთხოებისთვის დასაქმებულების მიერ უფლებამოსილების არამართლზომიერად გამოყენება მნიშვნელოვანი რისკია. თავის მხრივ, მონაცემთა ბაზების მიმართ ორგანიზაციული და ტექნიკური ზომების სწორად შერჩევის მნიშვნელობა იზრდება, როცა საკითხი ჯანმრთელობასთან დაკავშირებულ ინფორმაციას ეხება, ვინაიდან მსგავსი ინფორმაციის კონფიდენციალურობა განსაკუთრებით მნიშვნელოვანია.

შეტყობინების საფუძველზე სამსახურმა ერთ-ერთი პაციენტის გარდაცვალების შემდეგ მისი პერსონალური მონაცემების შემცველი სამედიცინო დოკუმენტაციის სამხედრო ჰოსპიტალიდან სავარაუდო გამჟღავნების კანონიერება შეისწავლა. შემოწმების ფარგლებში დადგინდა, რომ პაციენტი სამხედრო ჰოსპიტალში სტაციონარულ მკურნალობას გადიოდა, რა დროსაც სხვადასხვა სამედიცინო მანიპულაცია ჩაუტარდა. მისი გარდაცვალების შემდეგ, პაციენტის მიერ უძრავი ქონების გასხვისებასთან დაკავშირებული გარემოებების გამორკვევის მიზნით, შეტყობინების ავტორმა, როგორც გარდაცვლილი პირის მემკვიდრის წარმომადგენელმა, საქართველოს შინაგან საქმეთა სამინისტროს მიმართა და განმარტა, რომ შესაძლებელია ქონების გასხვისება პაციენტის ნებას არ შეესაბამებოდა; ხოლო ქონების გასხვისების შეთანხმების მონაწილედ სამხედრო ჰოსპიტალში დასაქმებული მედდა დაასახელა. საქმის მასალით დასტურდებოდა,

[7] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი (დოკუმენტის №5669-რს, მიღების თარიღი, 28/12/2011, გამოქვეყნების თარიღი: 16/01/2012, ძალადაკარგულია 2023 წლის 14 ივნისიდან).

რომ აღნიშნული მედდა სამინისტროს სამხედრო ჰოსპიტალის მიერ გარდაცვლილთან დაკავშირებით წარმოებულ სამედიცინო დოკუმენტაციას ფლობდა.

სამხედრო ჰოსპიტალი სამედიცინო საქმიანობის ფარგლებში ელექტრონულ სისტემას იყენებს, რომელშიც, მაგალითად, პაციენტებისათვის გაწეული სამედიცინო მომსახურების ამსახველი დოკუმენტები მუშავდება და ინახება. დასაქმებულთა ფუნქცია-მოვალეობებიდან გამომდინარე, ელექტრონულ სისტემაში განსაზღვრული იყო სხვადასხვა ჯგუფი (მაგალითად, ექიმები, ეპიდემიოლოგები და სხვა), რომლებსაც მონაცემებზე წვდომის განსხვავებული ფარგლები ჰქონდათ მინიჭებული. ამასთან, ცალკეული კატეგორიის დასაქმებულებს (მაგალითად, მედდებს) ელექტრონულ სისტემაში შექმნილი არ ჰქონდათ მომხმარებლები, თუმცა ისინი ექიმებს სამედიცინო დოკუმენტაციის შედგენაში ეხმარებოდნენ და ამ მიზნით უშუალოდ ექიმებისგან ფლობდნენ მათ მომხმარებლებსა და პაროლებს.

ინსპექტირების ფარგლებში მოპოვებული მტკიცებულებებიდან დადგინდა, რომ მედდა პაციენტის გარდაცვალების შემდეგ შევიდა ელექტრონულ სისტემაში სხვადასხვა ექიმის მომხმარებლისა და პაროლის გამოყენებით და პირადი საჭიროებისთვის მოიძია გარდაცვლილი პირის სისხლის საერთო ანალიზების პასუხები, გლუკოზის ანალიზისა და მუცლის ღრუს კომპიუტერული ტომოგრაფიის შედეგის ამსახველი სამედიცინო დოკუმენტაცია და სხვა. კანონის 27-ე მუხლის მე-5 პუნქტის დარღვევის ფაქტზე (დამუშავებისთვის პასუხისმგებელი პირის ნებისმიერი თანამშრომელი, რომელიც მონაცემთა დამუშავების პროცესი მონაწილეობს, ვალდებულია მისთვის მინიჭებული უფლებამოსილების ფარგლებს არ გასცდეს) მედდა ცნობილი იქნა სამართალდამრღვევად კანონის 76-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული სამართალდარღვევისთვის.

ამავე შემოწმების ფარგლებში დადგინდა, რომ სამსახურებრივი საქმიანობის დროს მედდების მიერ ექიმების მომხმარებლებისა და პაროლების გამოყენება პრაქტიკას წარმოადგენდა, რაზეც ინფორმაციას სამხედრო ჰოსპიტალიც ფლობდა, თუმცა არსებული მდგომარეობის შეცვლის მიზნით რაიმე სახის ეფექტიანი ნაბიჯი არ გადაუდგამს. გარდა ამისა, გარდაცვლილი პირის პერსონალური მონაცემების დამუშავების ყველა რელევანტური ფაქტის იდენტიფიცირების მიზნით სამსახურმა „მედსერვისი“ დაათვალიერა, რის შედეგადაც გამოვლინდა, რომ სისტემაში და მის მონაცემთა ბაზაში არ აღირიცხებოდა პაციენტების მოძიების, ასევე – კონკრეტული დოკუმენტის დათვალიერების, გადმოწერისა და ამობეჭდვის ფაქტები. აღსანიშნავია, რომ კონკრეტული დასაქმებულისათვის მომხმარებლისა და პაროლის გაწერა მოიაზრებს მის კონფიდენციალურობას, რაც სამომავლო რისკების პრევენციას ემსახურება; ერთი მომხმარებლის რამდენიმე პირის მიერ გამოყენება კი ართულებს ან შეუძლებელს ხდის იმ პირის იდენტიფიცირება, რომელმაც ელექტრონულ სისტემაში გარკვეული მოქმედება განახორციელა. ამასთან, კანონის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებულნი არიან, უზრუნველყონ ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა, რაც მათ შორის მიზნად ისახავს ელექტრონულ სისტემაში

განხორციელებული ქმედების შინაარსის, დროისა და განმახორციელებელი პირის ვინაობის სწორად იდენტიფიცირებას.

ამასთან, ვინაიდან ელექტრონულ სისტემაში ჯანმრთელობასთან დაკავშირებული მონაცემები მუშავდებოდა, სამსახურმა ყურადღება კანონის მე-6 მუხლზეც გაამახვილა და განმარტა, რომ, კანონის თანახმად, მონაცემთა დამუშავების კონკრეტული საფუძვლის გარდა, თავად მონაცემთა დამუშავების ფაქტობრივი პროცესი კანონთან შესაბამისი უნდა ყოფილიყო, რაც მედდების მიერ ექიმების მომხმარებლების გამოყენების პრაქტიკის გათვალისწინებით უზრუნველყოფილი არ იყო.

ზემოაღნიშნული გარემოებები მიუთითებდა სამხედრო ჰოსპიტალის მიერ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის (მონაცემთა უსაფრთხოება) დარღვევაზე, რის გამოც დაწესებულება სამართალდამრღვევად იქნა ცნობილი კანონის 76-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული სამართალდარღვევისთვის.

ვ. სსიპ — „ლ. საყვარელიძის სახელობის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნულ ცენტრში“ სამედიცინო დაწესებულებების მიერ წარმოებული პერსონალური მონაცემების დამუშავება პირადი ელექტრონული ფოსტის მეშვეობით

დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირი ვალდებულნი არიან დამუშავების პროცესში გამოიყენონ მონაცემებისთვის უსაფრთხო მეთოდები და საშუალებები. შეტყობინების საფუძველზე სამსახურმა შეისწავლა ცენტრში სამსახურებრივი საქმიანობის ფარგლებში დასაქმებული პირების მიერ პირადი ელექტრონული ფოსტის მეშვეობით პერსონალური მონაცემების დამუშავების კანონიერება.

შეტყობინების ავტორს წლების განმავლობაში საკუთარ ელექტრონულ ფოსტაზე სხვადასხვა სამედიცინო დაწესებულებიდან ეგზავნებოდა ინფორმაცია უცნობ პირთა სამედიცინო მანიპულაციების თაობაზე. შეტყობინებებში ასახული იყო პაციენტების სახელი, გვარი, პირადი ნომერი, ასევე – ინფორმაცია მშობიარობის თარიღის, გარე ორსულობის, B და C ჰეპატიტის ტესტების ჩატარების თაობაზე და სხვა. კომუნიკაციის შინაარსიდან ირკვეოდა, რომ ინფორმაცია ცენტრის თანამშრომლისათვის იყო განკუთვნილი, ხოლო შეცდომა ელექტრონული ფოსტების მისამართებს შორის არსებითმა მსგავსებამ გამოიწვია — ისინი ერთმანეთისგან მხოლოდ ერთი ასოთი განსხვავდებოდნენ. თითოეული ელექტრონული ფოსტა „Google“-ის ელექტრონული ფოსტის მისამართს მიეკუთვნებოდა.

შესწავლის ფარგლებში დადგინდა, რომ ცენტრი „დაბადების რეგისტრის“ ადმინისტრირებასა და მონაცემთა პროგრამულ დამუშავებას ახორციელებდა, რაც სამედიცინო დაწესებულებების მიერ ელექტრონულ სისტემაში შეყვანილი მონაცემების სისწორის კონტროლსა და მონაცემთა შესწორებას გულისხმობდა. მოცემული რეგისტრის წარმოებაში ასეულობით სამედიცინო დაწესებულება იყო ჩართული და მათ ელექტრონულ სისტემაში ორსულებისა და ახალშობილების

თაობაზე სხვადასხვა სახის ინფორმაცია (მაგალითად: საიდენტიფიკაციო მონაცემები, კვლევებისა და ანალიზების შედეგები) შეჰყავდათ; ხოლო სისტემაში ასახული მონაცემების კორექტირების მიზნით ისინი ცენტრის უფლებამოსილ თანამშრომლებს მიმართავდნენ და ელექტრონულ ფოსტაზე ფიზიკური პირების ჯანმრთელობასთან დაკავშირებულ ინფორმაციასა და დოკუმენტაციას უგზავნიდნენ. თავის მხრივ, ცენტრის თანამშრომლები, სამედიცინო დაწესებულებებთან კომუნიკაციის პროცესში, სამსახურებრივ ელექტრონულ ფოსტასთან ერთად პირად ელექტრონულ ფოსტას იყენებდნენ. აღნიშნულის შესახებ ცენტრი ინფორმირებული იყო და პირადი საკონტაქტო მონაცემის გამოყენება სამსახურებრივ ელექტრონულ ფოსტასთან დაკავშირებული გამოწვევებით (მეხსიერების სიმცირე და „ru“-ზე დაბოლოებული ელექტრონული ფოსტის მისამართებზე კომუნიკაციის ტექნიკური შეუძლებლობა) ახსნა. თავის მხრივ, საქმეში დაცული მტკიცებულებებით დადასტურდა სამსახურებრივი ელექტრონული ფოსტის მეხსიერების გაზრდის შესაძლებლობა. ამასთან, დადგინდა, რომ ცენტრს ეფექტიანი მეთოდებით სამედიცინო დაწესებულებებისათვის არ მიუწოდებია ინფორმაცია „ru“-ზე დაბოლოებული ელექტრონული ფოსტების გამოყენების შეზღუდვისა და მხოლოდ ცენტრის სამსახურებრივ ელექტრონულ ფოსტაზე კომუნიკაციის თაობაზე. საქმის შესწავლისას გამოვლინდა, რომ მომართვის ავტორთან შეცდომით გაგზავნილი შეტყობინებების თაობაზე ცენტრი საწყისი ეტაპიდანვე იყო ინფორმირებული, თუმცა მხოლოდ შეცდომის დამშვებ ცალკეულ სამედიცინო დაწესებულებასთან კომუნიკაციით შემოიფარგლა და არ გაუტარებია სათანადო პრევენციული ღონისძიებები.

მითითებულ საქმეში სამსახურმა პირადი და სამსახურებრივი ელექტრონული ფოსტის მისამართების სამსახურებრივი მიზნებისთვის გამოყენების გარკვეული ასპექტები შეაფასა. მაგალითად, გადაწყვეტილებაში აღინიშნა, რომ სამსახურებრივი ელექტრონული ფოსტის შექმნის შემთხვევაში დამსაქმებელი არსებითად მსგავსი მისამართების რეგისტრაციის რისკს ითვალისწინებს; ხოლო პირადი ელექტრონული ფოსტის მისამართის შექმნისას პირი სიმბოლოებს/დასახელებას თავად ირჩევს, რაც სხვა პირის პირადი ელექტრონული ფოსტის მისამართის მსგავსი შეიძლება იყოს. ამასთან, პირადი ელექტრონული ფოსტის მფლობელი უსაფრთხოების ზომების მიღებას საკუთარი შეხედულებით წყვეტს, რაც შესაძლებელია, სამსახურებრივი ელექტრონული ფოსტის ადმინისტრირების პროცესში უსაფრთხოების მიზნით განსახორციელებელი მოქმედებებისგან არსებითად განსხვავდებოდეს. გარდა ამისა, ვინაიდან პირადი ელექტრონული ფოსტა უწყების სერვერზე არ იყო განთავსებული, ცენტრი პროცესის მონიტორინგს ვერ ახორციელებდა, რაც მნიშვნელოვნად ამცირებდა დაწესებულების ეფექტიანი ჩარევის შესაძლებლობას პირად ელექტრონულ ფოსტაზე არსებული მონაცემების უსაფრთხოების, მათ შორის – დასაქმებული პირის მიერ მონაცემების შესაძლო გამოყენების (მაგალითად, სამსახურიდან განთავისუფლების შემთხვევაში) თვალსაზრისით.

ამასთან, ვინაიდან პირადი ელექტრონული ფოსტის მეშვეობით ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავებაც ხორციელდებოდა, სამსახურმა ყურადღება კანონის მე-6 მუხლზე გაამახვილა და განმარტა, რომ

ცენტრის მიერ შერჩეული საშუალება მონაცემების დამუშავებასთან შეუთავსებელი იყო. ამასთან, მიუხედავად იმისა, რომ არსებობდა მონაცემთა დამუშავების საფუძველი, მონაცემთა დამუშავების ფაქტობრივი პროცესი კანონს არ შეესაბამებოდა.

ზემოაღნიშნული გარემოებები მიუთითებდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის (მონაცემთა უსაფრთხოება) დარღვევაზე, რის გამოც სსიპ — „ლ. საყვარელიძის სახელობის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნული ცენტრი“ სამართალდამრღვევად იქნა ცნობილი კანონის 76-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტის საფუძველზე.

ზ. სსიპ — „ლევან სამხარაულის სახელობის სასამართლო ექსპერტიზის ეროვნული ბიუროს“ მხრიდან მომსახურების გაწევისას, ვერბალური კომუნიკაციის პროცესში მონაცემების დამუშავება

მონაცემთა უსაფრთხოების უზრუნველსაყოფად მნიშვნელოვანია გათვალისწინებულ იქნეს მომსახურების სივრცე და მისი მოწყობა, ასევე – ვერბალური კომუნიკაციის სპეციფიკა და სერვისის შინაარსობრივი მახასიათებლები. პერსონალურ მონაცემთა დაცვის სამსახურმა ბიუროს მიერ სერვისის მიწოდებისას, ვერბალური კომუნიკაციის პროცესში, გამოთხოვისა და მოპოვების გზით მონაცემების დამუშავების კანონიერება შეისწავლა.

შემოწმების შედეგად დადგინდა, რომ ბიუროს ნარკოლოგიური ექსპერტიზის სამმართველოს თანამშრომლებს მოქალაქეთა მომსახურების საერთო სივრცეში, ოთხი სხვადასხვა მომსახურების გაწევის პროცესში, დაინტერესებულ პირებთან ვერბალური კომუნიკაცია ჰქონდათ. აღნიშნული ელექტრონულ სისტემაში ინფორმაციის მოძიებასა და შესაბამისი დასკვნის მომზადებასთან იყო დაკავშირებული, მომსახურების სახეებს კი წარმოადგენდა: ნარკოლოგიური აღრიცხვიანობის შესახებ ცნობის მიღება, ნარკოტიკული და ფსიქოტროპული საშუალებების ზემოქმედების ფაქტის დადგენა, ალკოჰოლური თრობის ფაქტის დადგენა და დინამიური ნარკოლოგიური გამოკვლევა.

მოქალაქეთა მომსახურების სივრცის ფართობი დაახლოებით 15მ^2 იყო, რომელშიც ყოველდღიურად მომსახურების მიღების მსურველი 100-ზე მეტი პირი შედიოდა. რიგის მართვის პოლიტიკის არარსებობის გამო ზემოაღნიშნული პირები, ზოგიერთ შემთხვევაში თანმხლებ პირებთან ერთად (მაგალითად, მეგობარი), ე. წ. „ცოცხალ რიგში“ იდგნენ და ყოველგვარი ძალისხმევის გარეშე შეეძლოთ ბიუროს თანამშრომლებსა და მომსახურების მიღების მსურველ სხვა პირებს შორის ვერბალური კომუნიკაციის შინაარსი მოესმინათ. მინის გამყოფი ბარიერის შიდა მხარეს მყოფი ბიუროს თანამშრომელი შეკითხვას სვამდა, პასუხად კი სერვისის მსურველი მომსახურების სახეს ასახლებდა, ხოლო თანამშრომელი ზეპირსიტყვიერი კომუნიკაციის გზით მასთან დამატებით ინფორმაციას აზუსტებდა.

მომსახურების თითოეული სახე ინდივიდუალური სპეციფიკით ხასიათდებოდა, რაც ვერბალური კომუნიკაციის განსხვავებულ შინაარსს განაპირობებდა. მაგალითად:

— ნარკოლოგიური აღრიცხვიანობის შესახებ ცნობის გაცემის პროცესში ბიუროს თანამშრომელი ასახელებდა მომსახურების მიღების მსურველი პირის სახელს, გვარსა და დასაქმების ადგილს, სადაც პირს ცნობა უნდა წარედგინა;
— ნარკოტიკული და ფსიქოტროპული საშუალებების ზემოქმედების დადგენასთან დაკავშირებით ვერბალური კომუნიკაციის პროცესში ჩართული პირები ცვლიდნენ ინფორმაციას გარკვეული მედიკამენტების მიღებისა და სხეულზე ნანემსარის არსებობის, ასევე – კვლევის შედეგად კონკრეტული ნარკოტიკული ნივთიერების მოხმარების ფაქტის დადგენის თაობაზე;
— თუ პირს ალკოჰოლური თრობის ფაქტის დადგენა სურდა, მიუთითებდა აღნიშნული კვლევის ჩატარების საჭიროებაზე. შესაბამისად, ასახელებდა მომსახურების კონკრეტულ სახეს;
— დინამიურ ნარკოლოგიურ გამოკვლევას ის პირები გადიან, რომლებსაც ნარკოტიკული საშუალების მოხმარების ფაქტი აქვთ დადგენილი ან დამოკიდებულნი არიან ნარკოტიკულ საშუალებებზე. თავის მხრივ, ნარკოტიკულ საშუალებებზე დამოკიდებული პირები „მეტადონით“ ან „სუბოქსონით“ ჩანაცვლებით თერაპიაში მონაწილეობენ. ვერბალური კომუნიკაციის პროცესში მომსახურების მიღების მსურველი პირი მიუთითებდა კვლევის ჩატარების სურვილზე და ასახელებდა, თუ მერამდენე ვიზიტზე იმყოფებოდა, ხოლო ბიუროს თანამშრომლები სვამდნენ შეკითხვებს და იღებდნენ შესაბამის პასუხებს, მათ შორის – ზემოაღნიშნულ თერაპიებში/პროგრამებში პირის მონაწილეობასთან დაკავშირებით.

თითქმის ყოველთვის სივრცეში რამდენიმე ადამიანი ერთდროულად იმყოფებოდა, ზოგიერთ შემთხვევაში კი იქ მყოფთა რაოდენობა 15-ს აჭარბებდა. არსებული მდგომარეობის გამო ნებისმიერ ვიზიტორს უწევდა, რომ ბიუროს თანამშრომლისათვის საკუთარი პერსონალური მონაცემები სხვა პირების თანდასწრებით მიეწოდებინა. თავის მხრივ, გარეშე პირებისთვის გამჟღავნებული ინფორმაციის ნაწილი, როგორიცაა ნარკოტიკული ნივთიერების მოხმარების ან/და ნარკოტიკულ ნივთიერებებზე დამოკიდებულთა პროგრამაში ჩართვის ფაქტი, სენსიტიური ინფორმაციაა, ხოლო მისმა გამჟღავნებამ შესაძლოა მონაცემთა სუბიექტის სტიგმატიზება ან/და სხვა არასასურველი შედეგი გამოიწვიოს.

ხელშესახები პრობლემის მიუხედავად, მის მოსაგვარებლად ბიუროს აქტიური ქმედებები ინსპექტირების დაწყებამდე არ განუხორციელებია. შემოწმების მიმდინარეობისას ვერბალური კომუნიკაციის ფარგლებში გარკვეული შეკითხვების დასმა შეწყდა. სამსახურმა ყურადღება გაამახვილა შესაბამისი წესის შემუშავებისა და დანერგვის საჭიროებაზე, რომელიც ნარკოლოგიური ექსპერტიზის სამმართველოს მომსახურების გამწევ პირებს, თითოეული მომსახურების სპეციფიკის გათვალისწინებით, ცხად და გასაგებ ინსტრუქციებს

მისცემდა მომსახურების მიმღები პირის მონაცემთა მოპოვებისა თუ გადამოწმების პროცესის თაობაზე. გარდა ამისა, არსებულ ფიზიკურ სივრცეში შექმნილი პირობები მონაცემთა უსაფრთხოებისთვის მნიშვნელოვანი რისკის შემცველად შეფასდა.

ამდენად, საქმის შესწავლის ფარგლებში დადგენილი გარემოებები მიუთითებდა სსიპ — „ლევან სამხარაულის სახელობის სასამართლო ექსპერტიზის ეროვნული ბიუროს“ მიერ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის (მონაცემთა უსაფრთხოება) დარღვევაზე, რის გამოც ბიურო სამართალდამრღვევად იქნა ცნობილი 76-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული სამართალდარღვევისთვის.

თ. პერსონალური მონაცემების შემცველი მინისტრის ბრძანებების ვებგვერდზე ხანგრძლივად გამოქვეყნება

თანამედროვე ტექნოლოგიური პროგრესის პირობებში მონაცემების ელექტრონული რესურსების გამოყენებით, მათ შორის ვებგვერდებზე განთავსების გზით, დამუშავება უფრო და უფრო საფრთხილო ხდება; ხოლო მონაცემთა განგრძობადი დამუშავებისას დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დამუშავების საფუძვლის არსებობის პერიოდული შეფასება და პოტენციური რისკების იდენტიფიცირება განსაკუთრებით მნიშვნელოვანია.

პერსონალურ მონაცემთა დაცვის სამსახურში წარმოდგენილ შეტყობინებაზე რეაგირების მიზნით საქართველოს განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტროს ვებგვერდზე გამოქვეყნებული მინისტრის 2012-2014 წლების ბრძანებების განთავსების გზით სხვადასხვა დაფინანსების/გრანტის მიმღებ ფიზიკურ პირთა ფართო წრის, მათ შორის ახალგაზრდების, დიდი მოცულობის პერსონალური მონაცემების დამუშავების კანონიერება იქნა შესწავლილი. სამინისტროს ვებგვერდზე 2012-2014 წლებში გამოქვეყნებული მინისტრის რამდენიმე ათეული ბრძანება ჯამურად 2500-ზე მეტი პირის ისეთ მონაცემებს შეიცავდა, როგორებიცაა: სახელი, გვარი, პირადი ნომერი, მოქალაქეობა, უმაღლესი საგანმანათლებლო დაწესებულება, სწავლის საფასური, გრანტი და სხვა. ცალკეული ბრძანებების სახელწოდებებით/გაცემული გრანტების ტიპით ირკვეოდა, რომ დაფინანსება ობოლ (უდედმამო), სახელმწიფო ზრუნვის ქვეშ მყოფ, სოციალურად დაუცველი ოჯახების წევრ, საქართველოს ოკუპირებულ ტერიტორიებთან გამყოფი ხაზის მიმდებარე სოფლებში დაზარალებულ აბიტურიენტებს/სტუდენტებს ჰქონდათ მოპოვებული.

მონაცემების გამოქვეყნების საჭიროებასთან დაკავშირებით, მოცემულ საქმეში სამინისტრომ ისეთ ლეგიტიმურ ინტერესებზე მიუთითა, როგორებიცაა: ეროვნული გამოცდებისადმი მაღალი საზოგადოებრივი ინტერესი, უწყების მიერ თემატური ინფორმაციის გამჭვირვალობის/ობიექტურობის უზრუნველყოფა, აქტების ადრესატებისათვის ჩაბარება და სხვა. თუმცა განხილვის ფარგლებში გამოვლინდა, რომ აღნიშნული ინტერესები ბრძანებების გამოქვეყნების დროს და მომდევნო გარკვეულ პერიოდში არსებობდა; ხოლო საწყის ეტაპზე მონაცემების

სათანადო საფუძვლით გამოქვეყნება თავისთავად იმას არ გულისხმობს, რომ დამუშავების საფუძვლები, დოკუმენტების ვებგვერდზე განთავსების გრძელვადიან პერიოდში უწყვეტად შენარჩუნდებოდა. ამასთან, 2015 წლიდან სამინისტრომ თავად დაიწყო ვებგვერდზე გამოსაქვეყნებელ დოკუმენტებში პერსონალური მონაცემების დაშტრიხვა, რაც ეროვნული გამოცდების გზით ჩარიცხვისა და დაფინანსების მოპოვების შესახებ საზოგადოებრივი ინტერესის კლებით ახსნა. ამავე პერიოდიდან ვებგვერდი აღარ წარმოადგენდა აბიტურიენტებისთვის/სტუდენტებისთვის ინფორმაციის მიღების აუცილებელ წყაროს და იგი საგანმანათლებლო სფეროში დანერგილმა სისტემებმა ჩაანაცვლა.

არსებული ფაქტობრივ-სამართლებრივი გარემოებებიდან გამომდინარე, ინსპექტირების შედეგად დადგინდა, რომ ათი და მეტი წლის წინანდელ ბრძანებებთან მიმართებით, 2024 წლის მდგომარეობით გასული იყო ის გონივრული პერიოდი, რომლის განმავლობაშიც ადრესატებისა და ფართო საზოგადოების ინფორმირების სამართლებრივი ვალდებულება ან/და მომეტებული საზოგადოებრივი ინტერესი იარსებებდა. ყურადღება გამახვილდა 2012-2014 წლების ბრძანებების გასაჩივრების ვადების ამოწურვაზე, გრანტების დაგეგმილი წესით განაწილებასა და შესაბამისი წლების სასწავლო პროცესის შეუფერხებლად დაწყებაზე. გარდა ამისა, სამსახურის მიერ ინსპექტირების პროცესის დასრულებამდე, სამინისტრომ პერსონალური მონაცემების შემცველი შესაფასებელი პერიოდის ბრძანებები ვებგვერდიდან თავად წაშალა.

ამდენად, 2024 წლის მდგომარეობით სამინისტროს ვებგვერდზე მინისტრის 2012-2014 წლების ბრძანებების გამოქვეყნების სამართლებრივი საფუძვლის არსებობა არ დადასტურდა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 67-ე მუხლის საფუძველზე, საქართველოს განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტრო სამართალდამრღვევად იქნა ცნობილი.

ი. სსიპ — „საჯარო რეესტრის ეროვნული სააგენტოს“ მიერ უძრავი ქონების რეესტრში უფლებების რეგისტრაციასთან დაკავშირებული დაინტერესებული პირების სატელეფონო ნომრების ძიების პარამეტრად გამოყენების გზით დამუშავება

უძრავ ნივთებზე უფლებათა რეესტრის საჯაროდ ხელმისაწვდომობა, როგორც სამართლებრივი ურთიერთობის მონაწილეთა კანონიერი ინტერესების დაცვას, ასევე, მარეგისტრირებელი ორგანოს საქმიანობის გამჭვირვალობას და მასზე ეფექტიანი საზოგადოებრივი კონტროლის განხორციელებას ემსახურება. უძრავ ნივთებზე უფლებათა რეესტრი გასაჯაროებული პერსონალური მონაცემების ერთ-ერთი ყველაზე დიდი ბაზაა. თავის მხრივ, მარეგისტრირებელი ორგანო თავად განსაზღვრავს იმ პრაქტიკულ და ტექნიკურ საშუალებებს, რომელთა მეშვეობით რეესტრის საჯაროობა მიიღწევა. აღნიშნული ზომების შერჩევისას პერსონალური მონაცემების დამუშავების წესების ზედმიწევნით

გათვალისწინება, პოტენციური საფრთხეების პროგნოზირება და პრევენცია, არსებითად მნიშვნელოვანია.

როდესაც პირი სსიპ — „საჯარო რეესტრის ეროვნული სააგენტოს“ ვებგვერდის გამოყენებით უძრავი ქონების რეესტრში ინფორმაციის მოძიებას ცდილობს, სისტემა მას ელექტრონული სერვისების ერთიან პორტალზე ამისამართებს, რომელიც ვიზიტორს ამცნობს, რომ უძრავ ნივთთან დაკავშირებული მასალა პიროვნების სახელით, გვარითა და პირადი ნომრით შეუძლია მოიძიოს. სამსახურში წარმოდგენილ შეტყობინებაზე რეაგირების მიზნით განხორციელებული სატესტო მოქმედებების შედეგად დადგინდა, რომ რეესტრში რეგისტრირებულ გარკვეულ ინფორმაციაზე/დოკუმენტაციაზე წვდომის შესაძლებლობას ფიზიკური პირის ტელეფონის ნომერიც იძლეოდა, თუმცა ტელეფონის ნომრის მფლობელის სისტემის მეშვეობით იდენტიფიცირება არ იყო შესაძლებელი. აღნიშნულის გათვალისწინებით, სამსახურმა ამ პროცესში მონაცემთა დამუშავების კანონიერება შეისწავლა.

შემოწმების ფარგლებში გამოვლინდა, რომ პორტალი დაკავშირებულია სარეგისტრაციო პროგრამასთან, ხოლო საზოგადოებისთვის ხელმისაწვდომი განაცხადების ძიების პარამეტრი — „პიროვნება/ორგანიზაცია“ — სარეგისტრაციო პროგრამაში არსებული „დაინტერესებული პირის“ მონაცემებთან არის ინდექსირებული (დაკავშირებული). შემოწმების ფარგლებში სარეგისტრაციო წარმოების მიზნებისთვის „დაინტერესებული პირი“ განმარტებულ იქნა, როგორც ნებისმიერი პირი, რომელსაც სააგენტოს გადაწყვეტილების ან ქმედების მიმართ შესაძლოა იურიდიული ინტერესი ჰქონდეს. „დაინტერესებული პირი“ ხშირ შემთხვევაში თავად არის სარეგისტრაციო წარმოების ინიციატორი და შეიძლება იგი როგორც უძრავი ნივთის შემძენი, ასევე გამსხვისებელი ან/და სხვა უფლების მქონე პირი იყოს. შემოწმების ფარგლებში გამოვლინდა, რომ „პიროვნება/ორგანიზაციის“ სახელწოდების მქონე საძიებო ველი, „დაინტერესებული პირის“ სახელის, გვარის, პირადი ნომრის გარდა, განაცხადის რეგისტრაციის პროცესში დაფიქსირებულ მის ტელეფონის ნომერთანაც იყო დაკავშირებული (ინდექსირებული).

ასევე, გამოვლინდა, რომ „დაინტერესებული პირის“ ტელეფონის ნომრის სააგენტოს მიერ მიღება და სარეგისტრაციო პროგრამაში ასახვა საჯარო უწყებისთვის კანონმდებლობით დაკისრებული ვალდებულებებით არ იყო განპირობებული და თავად მონაცემთა სუბიექტის ნებაზე იყო დამოკიდებული. სატელეფონო ნომრის მოპოვების თავდაპირველ მიზნად გამოიკვეთა სარეგისტრაციო წარმოების პროცესში მიღებულ გადაწყვეტილებასთან დაკავშირებით „დაინტერესებული პირის“ მყისიერი ინფორმირება, განაცხადთან დაკავშირებით დამატებითი ინფორმაციის (მაგალითად, წარსადგენი დოკუმენტაციის აუცილებლობის, მიღებული გადაწყვეტილების თაობაზე) მიწოდება და, შესაბამისად, მისთვის სერვისის ეფექტიანად გაწევა. რაც შეეხება „დაინტერესებული პირის“ ტელეფონის ნომრის შემდგომ, პორტალზე ძიების პარამეტრად გამოყენების გზით დამუშავებას, იგი სარეგისტრაციო პროგრამის 2016-2017 წლების სისტემურმა განახლებამ განაპირობა. სააგენტომ დაადასტურა, რომ ხსენებული ფუნქციონალის დამატება უწყების მიერ დასახულ ამოცანას არ წარმოადგენდა. რაც შეეხება მის საჭიროებას — დაწესებულებამ ელექტრონულ

პორტალზე განაცხადების „დაინტერესებული პირის“ ტელეფონის ნომრებით ძიება საგამონაკლისო შემთხვევებად დააიდენტიფიცირა, სამოქალაქო ბრუნვის სტაბილურობის მიზანს დაუკავშირა და მიუთითა, რომ სხვა პარამეტრებით ძიების გართულების პროცესში იქნებოდა ის გამოსადეგი საშუალება (მაგალითად: როდესაც სუბიექტის მიერ შეცვლილია სახელი/გვარი, სარეგისტრაციო პროგრამაში არასწორადაა მითითებული სახელი/გვარი/პირადი ნომერი ან სუბიექტი უცხოელია).

შესაბამისად, დადგინდა, რომ „დაინტერესებული პირის“ ტელეფონის ნომრის მოპოვების მიზნისგან (ადმინისტრაციული წარმოების პროცესზე და შედეგებზე პირის ინფორმირება) განსხვავდებოდა მონაცემის შემდგომი დამუშავების მიზნები (კონკრეტული ადმინისტრაციული წარმოების დასრულებიდან ნებისმიერ დროს, ელექტრონული პორტალის მეშვეობით განცხადების/მასში მითითებული, მათ შორის – უძრავ ქონებასთან დაკავშირებული სხვა მონაცემების ხელმისაწვდომობის მიზანი). აქედან გამომდინარე, სამსახურმა სატელეფონო ნომრებთან დაკავშირებით თავად მონაცემთა სუბიექტების გონივრული მოლოდინები შეაფასა, რის შედეგადაც დადგინდა, რომ არც სააგენტოს ვებგვერდზე/პორტალზე განთავსებული ინფორმაცია და არც განაცხადის რეგისტრაციის პროცესი, „დაინტერესებული პირების“ საკონტაქტო ტელეფონის ნომრების შემდგომ, განსხვავებული მიზნით დამუშავებაზე პირთა პროაქტიულ და სათანადო ინფორმირებას ვერ უზრუნველყოფდა. შეფასებულ იქნა ის შედეგები, რომლებიც ელექტრონულ პორტალზე პირთა განუსაზღვრელ წრეს მოცულობითი ინფორმაციის მოძიების საშუალებას მხოლოდ ტელეფონის ნომრის მეშვეობით აძლევდა. ყოველდღიური ადამიანური ურთიერთობების მრავალფეროვნების გათვალისწინებით, არცთუ იშვიათია შემთხვევები, როდესაც პირისათვის ცნობილი ხდება სხვა პირის მხოლოდ ტელეფონის ნომერი, ან ტელეფონის ნომერი და სახელი. სხვა საძიებო მონაცემებისგან (სახელი, გვარი, პირადი ნომერი) განსხვავებით, ტელეფონის ნომრის შემთხვევაში, გაცილებით მეტია ალბათობა იმისა, რომ ელექტრონული პორტალის ვიზიტორი სააგენტოს ვებგვერდს იყენებდეს ტელეფონის ნომრით პირის იდენტიფიცირების ან/და დამატებითი მონაცემების მოპოვების მიზნით; ზემოხსენებული კი მესამე პირებს აძლევს განაცხადთან დაკავშირებული პირების პირად სივრცეში შეჭრისა და მათი ნებართვისა და გონივრული მოლოდინების გარეშე სხვადასხვა სახის მონაცემზე წვდომის შესაძლებლობას. შესაბამისად, გადაწყვეტილებით დადგინდა, რომ მონაცემთა შემდგომი დამუშავების შედეგებმა შეიძლება მნიშვნელოვნად იმოქმედოს მონაცემთა სუბიექტების პირადი ცხოვრების ხელშეუხებლობის უფლებაზე.

„დაინტერესებული პირის“ სატელეფონო ნომრის თავდაპირველ მიზანთან შეუთავსებელი მიზნით დამუშავების გამო, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 66-ე მუხლის საფუძველზე, სსიპ — „საჯარო რეესტრის ეროვნული სააგენტო“ სამართალდამრღვევად იქნა ცნობილი.

კ. სსიპ — „შრომის ინსპექციის სამსახურის“ მიერ ინსპექტირების პროცესში სამხრე კამერების საშუალებით მონაცემთა დამუშავება

ვიდეო- და აუდიომონიტორინგის მეშვეობით მონაცემთა დამუშავების მასშტაბის, სპეციფიკის და მისგან მომდინარე საფრთხეების გათვალისწინებითა და პერსონალურ მონაცემთა დაცვის სამსახურში წარმოდგენილ შეტყობინებაზე რეაგირების მიზნით სამსახურმა სსიპ — „შრომის ინსპექციის სამსახურის“ მიერ სამხრე კამერების მეშვეობით აუდიოჩაწერისა და ვიდეოჩაწერის გზით პერსონალური მონაცემების დამუშავების კანონიერება შეისწავლა.

შრომის ინსპექციის პრაქტიკის თანახმად, ინსპექტირების განმახორციელებელი პირები ობიექტზე ყოფნისას იყენებენ სამუშაო ფორმაზე დამაგრებულ სამხრე კამერებს, რომლებიც ვიდეოგამოსახულებასა და აუდიოსიგნალს უწყვეტად აფიქსირებენ. შრომის ინსპექციის, როგორც საჯაროსამართლებრივი უფლებამოსილების განმახორციელებელი ორგანოს, მიზანი შრომითი ნორმების ეფექტიანი გამოყენების უზრუნველყოფაა. თავის მხრივ, სახელმწიფო კონტროლის მიზანი, დამსაქმებელთა, დასაქმებულთა თუ ობიექტზე მყოფ სხვა პირთა მიმართ შრომითი ნორმების ეფექტიანი დამკვიდრების, ხელშეწყობისა და გამოყენების მიზნით, შრომითი ნორმების დადგენილი წესების შესრულების უზრუნველყოფაა. ინსპექტირების პროცესში მონაცემების ვიდეომონიტორინგის გზით დამუშავებას სფეროს მარეგულირებელი აქტები სავალდებულოდ ადგენენ, ხოლო, შრომის ინსპექციის პოზიციით, მსგავს ნორმატიულ ჩანაწერებში აუდიომონიტორინგი ავტომატურად იგულისხმება. აღნიშნულ მოსაზრებას დაწესებულება უკავშირებდა იმ გარემოებას, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის წინა რედაქცია აუდიომონიტორინგის წესს დამოუკიდებლად არ ითვალისწინებდა.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი აუდიომონიტორინგის რამდენიმე სამართლებრივ საფუძველს ასახელებს, მათ შორის, გარდა კანონმდებლობით პირდაპირ გათვალისწინებული შემთხვევისა, საოქმო ჩანაწერის წარმოებისა და დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური ინტერესის დაცვის საჭიროებაც მოიაზრება. ამასთან, აუდიომონიტორინგი, როგორც მონაცემების დამუშავების ერთ-ერთი და ამასთან ვიდეომონიტორინგისგან განსხვავებული ფორმა, დასახელებული იყო კანონის წინა რედაქციაშიც.

შესწავლის შედეგად გამოვლინდა, რომ სამხრე კამერების საშუალებით შექმნილი ვიდეო-აუდიოჩანაწერები გამოიყენება როგორც ობიექტზე არსებული სიტუაციის აღწერისათვის ვიზუალურ, ისე – ობიექტის მიერ შრომითი ნორმების დაცვის საქართველოს კანონმდებლობასთან შესაბამისობის ან შეუსაბამობის დასადგენ მტკიცებულებებად. თავის მხრივ, ინსპექტირებისას გადაღებული ჩანაწერები ობიექტზე არსებულ მდგომარეობას შრომის ინსპექციის თანამშრომლების შესვლის მომენტში უნდა ასახავდეს, ხოლო შრომითი ნორმების დაცვა მხოლოდ ვიზუალური გამოსახულებებიდან არ შეიძლება გამომდინარეობდეს. პროცესის ვიდეოჩანაწერებზე დაფიქსირება ობიექტის ფიზიკური მდგომარეობის, სამუშაო სივრცისა და პირობების,

უსაფრთხოებისათვის მიღებული ზომების ფიქსაციისათვის არის მნიშვნელოვანი; ხოლო ხმოვანი სიგნალის დამუშავება დასაქმებულებთან/დამსაქმებლებთან წარმოებული კომუნიკაციის შემდგომი ინტერპრეტაციის გარეშე ფიქსაციას, გაბმული ხმაურისა და ობიექტზე მყოფი პირების სპეციფიკური ინტონაციების (ყვირილი, კამათი, მიმანიშნებელი ხმოვანი სიგნალი და სხვა) გამოვლენას ემსახურება. სამსახურის მიერ სამხრე კამერების საშუალებით ვიდეო- და აუდიომონიტორინგის განხორციელების ისეთი მიზნები იქნა დანახული, როგორებიცაა ეფექტიანი და გამჭვირვალე წარმოება, რაც, შრომის ინსპექციის გარდა, წარმოების მხარეებისათვისაც არის სარგებლიანი.

ვიდეო- და აუდიომონიტორინგის განხორციელების კანონიერების დასადგენად, გარდა სათანადო საფუძვლების და ლეგიტიმური ინტერესებისა, სამსახურმა კანონით გათვალისწინებული სხვა მოთხოვნების შესრულების ხარისხიც შეაფასა. კერძოდ, შემოწმების ფარგლებში გამოკვლეულ იქნა დამუშავებული მონაცემების მოცულობა, ჩანაწერების შენახვის ვადა, მონაცემთა სუბიექტთა ინფორმირების მიზნით შერჩეული მეთოდები, მონაცემთა უსაფრთხოებისთვის მიღებული ორგანიზაციულ-ტექნიკური ზომები, კანონით პირდაპირ განსაზღვრული წერილობითი წესების არსებობა/სისრულე და მონაცემთა დამუშავების პრინციპების დაცვა.

შესწავლის შედეგად დადგინდა, რომ სამხრე კამერების საშუალებით ვიდეო-აუდიომონიტორინგის თაობაზე ფიზიკური პირების ინფორმირების ძირითადი მეთოდებია შრომის ინსპექტორების მიერ ჩაწერის თაობაზე ზეპირსიტყვიერი ინფორმაციის გაჟღერება და ინსპექტორის სხეულზე მოწყობილობის თვალსაჩინო ადგილას განთავსება. სანიმუშოდ წარმოდგენილი 15-ამდე ვიდეო-აუდიოჩანაწერის გამოკვლევის შედეგად გამოვლინდა, რომ ჩაწერის თაობაზე პირთა ინფორმირება პრაქტიკაში განსხვავებული ფორმულირებებით, არათანმიმდევრულად მიმდინარეობდა. კერძოდ, რიგ შემთხვევებში ინსპექტორები პირებს მხოლოდ იმას განუმარტავდნენ, რომ სხეულზე კამერა ჰქონდათ დამაგრებული, ზოგ შემთხვევაში მხოლოდ ვიდეომონიტორინგზე ხდებოდა მითითება. შესაბამისად, აუდიოჩაწერის წარმოება ყურადღების მიღმა რჩებოდა და ა. შ. თავის მხრივ, კამერის თვალსაჩინოება ფიზიკურ პირს ჩაწერის მიმდინარეობის ან/და ფარგლების (მათ შორის, ვერც აუდიოჩაწერის) თაობაზე სათანადო ინფორმაციას ვერ მიაწვდის. აქედან გამომდინარე, მონაცემთა სუბიექტების ინფორმირების მეთოდი ნაკლოვანად იქნა შეფასებული. გარდა ამისა, მოპოვებული მტკიცებულებებით დადასტურდა, რომ შრომის ინსპექციას სამხრე კამერების საშუალებით განხორციელებული აუდიომონიტორინგის წესი არ ჰქონდა შემუშავებული და აღნიშნული არც მოქმედი კანონმდებლობის ჩანაწერებით იყო რეგულირებული, რითაც დაირღვა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-11 მუხლის მე-2 პუნქტის (აუდიომონიტორინგის წესი) მოთხოვნები და სსიპ — „შრომის ინსპექციის სამსახური“, ამავე კანონის 69-ე მუხლის შესაბამისად, სამართალდამრღვევად იქნა ცნობილი.

შემოწმების ფარგლებში როგორც სამხრე კამერების გამოყენებისა და ფუნქციონირების წესები, ასევე უშუალოდ ვიდეო-აუდიოჩანაწერების შენახვის, მათზე წვდომის პროცესები იქნა შესწავლილი, რის შედეგადაც მონაცემთა

უსაფრთხოების მიმართ მიღებული ზომების რიგი ნაკლოვანებები გამოვლინდა. მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვა უსაფრთხოების ერთ-ერთი უმნიშვნელოვანესი გარანტია, რომელიც მონაცემთა უკანონო დამუშავების პრევენციის მიზანს ემსახურება. დადგენილი გარემოებების მიხედვით, სსიპ — „ინფორმაციული ტექნოლოგიების სააგენტოს“ მიერ (რომელიც შრომის ინსპექციის მონაცემთა დამუშავებაზე უფლებამოსილი პირია), ვიდეო-აუდიოჩანაწერების შენახვის/ორგანიზების მიზნით შექმნილი ელექტრონული სისტემა მონაცემების მიმართ განხორციელებულ მოქმედებებს (ჩაწერა, წაშლა, გაზიარება, დათვალიერება, გადმოწერა) არ აღრიცხავდა; ხოლო ელექტრონული სისტემის მომხმარებლებით შრომის ინსპექციის ასზე მეტი თანამშრომელი სარგებლობდა, ინსპექტირების პროცესის ამსახველი ჩანაწერები კი განსაკუთრებული სენსიტიურობით და მტკიცებულებითი მნიშვნელობით ხასიათდებოდა. გარდა ამისა, ვიდეოა-უდიოჩანაწერების შემნახველი ელექტრონული რესურსის ოპერაციული სისტემის მომხმარებელი და პაროლი არ იყო განპიროვნებული. მისი გამოყენების შესაძლებლობა, სააგენტოს რამდენიმე სისტემურ ადმინისტრატორს ჰქონდა, რაც, თავის მხრივ, მონაცემთა მიმართ შესრულებული მოქმედებების განმახორციელებელი პირის უტყუარად იდენტიფიცირებას შეუძლებელს ხდიდა. აღნიშნულიდან გამომდინარე, დადგინდა სსიპ — „ინფორმაციული ტექნოლოგიების სააგენტოს“, როგორც ინფორმაციული ტექნოლოგიების გამართულ ფუნქციონირებაზე პასუხისმგებელი პირის, მიერ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლით (მონაცემთა უსაფრთხოება) დადგენილი მოთხოვნების დარღვევის ფაქტი და, კანონის 76-ე მუხლის შესაბამისად, იგი სამართალდამრღვევად იქნა ცნობილი.

გარდა ზემოხსენებულისა, გამოვლინდა, რომ შრომის ინსპექციას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლის[8] მოთხოვნები შესრულებული არ ჰქონდა. კერძოდ, ის არ აღრიცხავდა სამხრე კამერების საშუალებით ვიდეო-აუდიომონიტორინგის გზით მონაცემთა დამუშავებასთან დაკავშირებულ ინფორმაციას. ამ საკითხთან დაკავშირებით არ იქნა გაზიარებული დაწესებულების პოზიცია, რომელიც ინსპექტორების მიერ შესრულებული სამუშაოს პერიოდულ ანგარიშგებას, კანონის მითითებული ნორმის შესრულებისთვის საკმარისად მიიჩნევდნენ. ხსენებული მუხლი კანონის მოქმედი რედაქციის სიახლეა და ის არ გულისხმობს პერსონალური მონაცემების შემცველი მასალის ან კონკრეტულ მონაცემთა დამუშავების შემთხვევების შესახებ, ზემდგომი თანამდებობის პირების ინფორმირებიდან თუ მათ წინაშე ანგარიშვალდებულებიდან გამომდინარე, ცალკეული დოკუმენტების (მაგალითად, ყოველთვიური ანგარიშების) შექმნას; არამედ საჭიროა მონაცემების დამუშავების პროცესების თაობაზე განზოგადებული ინფორმაციის აღრიცხვა, რომელიც მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს პრაქტიულ საშუალებას აძლევს, ერთგვაროვან ინფორმაციას ფლობდეს ყველა იმ მონაცემის დამუშავების თაობაზე, რომელთა კანონიერების დადასტურების ვალდებულებაც აქვს. აღნიშნულ მექანიზმს პრევენციული დატვირთვა აქვს და დამუშავებისთვის

[8] მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინება.

პასუხისმგებელ პირებს თავიანთი ვალდებულებების შესრულებაში და, შესაბამისად, მონაცემების არაკანონიერი დამუშავების შემთხვევების შემცირებასა და აღმოფხვრაში ეხმარება. მითითებული ვალდებულების შეუსრულებლობის გამო, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 77-ე მუხლის შესაბამისად, სსიპ — „შრომის ინსპექციის სამსახური“ სამართალდამრღვევად იქნა ცნობილი.

ლ. სსიპ — „შემოსავლების სამსახურის“ მიერ საგადასახადო დავალიანების მქონე პირის შესახებ საჯარო შეტყობინებების ვებგვერდზე გამოქვეყნების გზით მონაცემთა დამუშავება

სამართლებრივი აქტის ადრესატისათვის ჩაბარებას არსებითი მნიშვნელობა აქვს, თუმცა აღნიშნულის შეუძლებლობის შემთხვევაში, კანონმდებლობა დოკუმენტის საჯაროდ გავრცელების მექანიზმს ითვალისწინებს. ამასთან, ინფორმაციის გასაჯაროება მონაცემთა დამუშავების სპეციფიკური სახეა და მნიშვნელოვანია, მონაცემების ამ გზით დამუშავების პროცესი განსაკუთრებული სიფრთხილით წარიმართოს.

პერსონალურ მონაცემთა დაცვის სამსახურმა განცხადების საფუძველზე შემოსავლების სამსახურის ვებგვერდზე დოკუმენტების საჯაროდ გავრცელების გზით განმცხადებლის პერსონალური მონაცემების დამუშავების კანონიერება შეისწავლა. შემოსავლების სამსახურში მომართვის ავტორის საგადასახადო შემოწმება მიმდინარეობდა, ხოლო შემოწმების ფარგლებში უწყების ვებგვერდზე სხვადასხვა დოკუმენტი განთავსდა, რომლებიც თვეების განმავლობაში იყო საჯაროდ გავრცელებული; მასალა შეიცავდა მის სახელს, გვარს, პირად ნომერს, ტელეფონის ნომრებს, ჯარიმების ოდენობას, ინფორმაციას საგადასახადო დავალიანების თაობაზე და სხვა.

საგადასახადო კანონმდებლობით ფიზიკური პირისათვის დოკუმენტის ჩაბარების რამდენიმე გზა არსებობს: დოკუმენტის მისამართზე გაგზავნა, „rs.ge“-ის პორტალის ავტორიზებული მომხმარებლის გვერდზე განთავსება და საჯაროდ გავრცელება. დოკუმენტის საჯაროდ გავრცელება დასაშვებია, თუ, მისამართზე ორჯერ გაგზავნის მიუხედავად, ის ადრესატს ვერ ჩაბარდება და ამავდროულად დოკუმენტის განთავსების შემდეგ ავტორიზებული მომხმარებლის გვერდზე (ასეთის არსებობის შემთხვევაში) მას ადრესატი არ გაეცნობა. თავის მხრივ, დოკუმენტის საჯაროდ გავრცელების თაობაზე წერილობით გადაწყვეტილებას უწყების უფლებამოსილი პირი იღებს.

მოცემულ საქმეში უფლებამოსილი პირის ბრძანებების მიხედვით, მხოლოდ ის დოკუმენტები უნდა გასაჯაროებულიყო, რომლებიც ადრესატს გაეგზავნა და ვერ ჩაბარდა, კერძოდ: წერილი, შემოწმების ფარგლებში მიღებული ბრძანებები და საგადასახადო მოთხოვნა; თუმცა, მათ გარდა, საჯაროდ გავრცელდა ფოსტის უკუგზავნილები, რომლებიც დამატებით მონაცემებს შეიცავდა (მაგალითად, ტელეფონის ნომრებს, ასევე, კონკრეტულ თარიღში მისამართზე არყოფნის და მისთვის წერილის ჩაუბარებლობის ფაქტებს). საჯარო შეტყობინებებში ასახული

მასალა მათი გამოქვეყნების შემდეგ განმცხადებლის მიერ შექმნილ ავტორიზებული მომხმარებლის გვერდზეც განთავსდა, რომელსაც ადრესატი გაეცნო, ხოლო აღნიშნულის თაობაზე დაწესებულებაც ინფორმირებული იყო. განმცხადებელმა საგადასახადო წარმოების ფარგლებში მიღებული საბოლოო აქტი (რომელიც ასევე გამოქვეყნებული იყო) ამავე უწყებაში გაასაჩივრა, რაც დოკუმენტის გაცნობის ფაქტზე მიუთითებდა. გარდა ამისა, განმცხადებელმა ორჯერ მიმართა უწყებას, დაადასტურა საჯაროდ გამოქვეყნებული მასალის გაცნობა და მათი წაშლა მოითხოვა, თუმცა მოთხოვნა არ დაკმაყოფილდა.

უწყების განმარტების თანახმად, დოკუმენტების საჯაროდ გავრცელების მიზანი მათი ადრესატისათვის ჩაბარება იყო, რათა სამართლებრივი შედეგები (მაგალითად, გასაჩივრების ვადის ათვლა) წარმოეშვა. თავის მხრივ, კანონმდებლობის მიხედვით, დოკუმენტის ვებგვერდზე განთავსებიდან მე-20 დღეს ის ადრესატისათვის ჩაბარებულად ითვლება. დაწესებულების პოზიციით, 20 დღის გასვლის შემდეგ გამოქვეყნებული მასალის საჯაროდ ხელმისაწვდომობა რამდენიმე გარემოებით იყო განპირობებული, მაგალითად, სფეროს მარეგულირებელი კანონმდებლობა საჯარო შეტყობინებას წაშლას, წაშლის პროცედურას არ ითვალისწინებდა, ასევე შესაძლებელი იყო ადრესატს მასალა მითითებული ვადის გასვლის შემდეგ ენახა და შემდგომი სამართლებრივი რეაგირება განეხორციელებინა. ამასთან აღინიშნა, რომ დავის დაწყების შემთხვევაში დაწესებულებას შესაძლებლობა უნდა ჰქონოდა, დაემტკიცებინა, თუ როდის გაავრცელა საჯაროდ დოკუმენტები, ხოლო ფოსტის უკუგზავნილის საჯაროდ გავრცელება ემსახურებოდა ადრესატის ინფორმირებას დოკუმენტის მისამართზე გაგზავნის შესახებ.

სამსახურმა უწყების პოზიცია არ გაიზიარა და მიუთითა, რომ დოკუმენტების გამოქვეყნების ლეგიტიმური მიზანი მიღწეული იყო, ვინაიდან საჯარო შეტყობინებების ვებგვერდზე განთავსებიდან 20 დღე იყო გასული და ამავდროულად უტყუარად დგინდებოდა მისი ინფორმირების ფაქტები ადრესატის მიერ მასალის რეალურად ჩაბარებისა და შეტყობინებების გამოქვეყნების თაობაზე. ამასთან, სამსახურმა განმარტა, რომ, კანონის თანახმად, მონაცემთა სუბიექტს აქვს მასთან დაკავშირებული მონაცემების წაშლის უფლება, ხოლო მოცემულ შემთხვევაში არ არსებობდა უფლების შეზღუდვისთვის საკმარისი საფუძველი. რაც შეეხება ფოსტის უკუგზავნილების გამოქვეყნებას — ზოგადად, უწყებამ შესაძლებელია მიზანშეწონილად მიიჩნიოს მასთან სამართლებრივ ურთიერთობაში მყოფი პირის არაერთ საკითხზე დარწმუნება. თუმცა, როდესაც ინფორმაცია ქვეყნდება არა ფართო საზოგადოებისთვის, არამედ მხოლოდ ერთი ინდივიდისთვის, მნიშვნელოვანია, გამოსაქვეყნებელი მონაცემების მინიმიზებული მოცულობა შეირჩეს.

ზემოაღნიშნული გარემოებებით დადასტურდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „გ“ (მინიმიზაციის პრინციპი) და „ე“ (ვადის შეზღუდვის) ქვეპუნქტებით გათვალისწინებული პრინციპების დარღვევა, რის გამოც სსიპ — „შემოსავლების სამსახური“ სამართალდამრღვევად იქნა ცნობილი კანონის 66-ე მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული სამართალდარღვევისთვის.

1.3. დავალებები და რეკომენდაციები

დარღვევების შემდგომი პრევენციისა და მონაცემთა სუბიექტის უფლების დასაცავად სამსახურმა საჯარო უწყებებს არაერთი რეკომენდაცია და შესასრულებლად სავალდებულო დავალება მისცა. გარდა ამისა, საანგარიშო პერიოდში, დავალების შესრულების მონიტორინგის მიზნით, აქტიურად იყო გამოყენებული დავალების შეუსრულებლობის სავარაუდო ფაქტებზე ინსპექტირების ჩატარების მექანიზმები. მათი განზოგადების შედეგად შემუშავებულ იქნა ძირითადი მითითებები, რომლებიც დამუშავებისთვის პასუხისმგებელმა და დამუშავებაზე უფლებამოსილმა პირებმა უნდა გაითვალისწინონ:

— გამჭვირვალობის პრინციპის დასაცავად პერსონალურ მონაცემთა დამუშავების კონკრეტული პროცესების, დასამუშავებელი მონაცემების მოცულობის, მონაცემთა დამუშავების გზებისა და ფორმების თაობაზე საზოგადოებისათვის ინფორმაციის გონივრული საშუალებებით მიწოდება;
— მონაცემთა დამუშავების ნამდვილობის, გამჭვირვალობისა და სიზუსტის უზრუნველყოფის მიზნით მონაცემთა დამუშავების პროცესში გამოსაყენებელ სტანდარტულ წერილობით დოკუმენტში ცვლილებების შეტანა/ახალი ფორმის შემუშავება;
— მოქმედი საქმისწარმოების პროგრამის საძიებო პარამეტრების იმგვარად მოწესრიგება, რომ სამომავლოდ შესძლებოდა სუბიექტის უფლების რეალიზების მიზნებისთვის მასთან დაკავშირებული მასალის მოძიება/მიგნება;
— საქმისწარმოების პროცესში გამოყენებული წესების იმგვარად მოდიფიცირების მითითება, რომ უწყების თანამშრომლები დაევალდებულებინა, ელექტრონული პროგრამის ველებში პერსონალური მონაცემები ერთგვაროვნად შეევსოთ. აღნიშნულ საჯარო უწყებას სამომავლოდ მონაცემთა სუბიექტების უფლებების რეალიზებისთვის საჭირო ყველა დოკუმენტის მოძიების საშუალებას მისცემდა;
— მონაცემთა სუბიექტებისთვის საკუთარი მონაცემების შემცველი ინფორმაციის/დოკუმენტაციის სრულყოფილად მიწოდება; მონაცემების გასწორებისა და განადგურების მოთხოვნაზე საპასუხოდ დასაბუთებული გადაწყვეტილების/პოზიციის მონაცემთა სუბიექტებისთვის მიწოდება; რიგ შემთხვევებში კი საჯარო სექტორს მიკუთვნებულ პირებს ინფორმირების უფლების შეზღუდვის შემთხვევაში ამგვარი გადაწყვეტილების წინაპირობებისა და სამართლებრივი საფუძვლების მონაცემთა სუბიექტისთვის განმარტება;
— მონაცემების შემცველი მასალების სამართლებრივი საფუძვლის გარეშე, საჭიროზე მეტი ვადით, კონკრეტული და მკაფიო მიზნის გარეშე ან/და ორგანიზაციულ-ტექნიკური ზომების დაუცველობის გამო უკანონოდ დამუშავების ფაქტების გამოვლენის შემთხვევაში, დაწესებულებებს მონაცემების დამუშავების შეწყვეტა;

— სამსახურის მიერ დაწყებული შემოწმების დასრულებამდე, მონაცემთა შემდგომი გავრცელების/გამჟღავნების თავიდან აცილების მიზნით, დაწესებულებას ვებგვერდზე გამოქვეყნებული დოკუმენტაციის გასაჯაროების შეჩერება; ხოლო შემოწმების დასრულების შემდეგ ხსენებული დოკუმენტის წაშლის დავალება;
— მონაცემების შემცველი დოკუმენტაციის არათანმიმდევრული მიდგომის მოწესრიგება;
— ელექტრონულ ბაზაში ასახული არასრულწლოვანების მონაცემების სანდოობის, სიზუსტისა და მოძველებული ინფორმაციის დროულად განახლების მიზნით კომპლექსური ორგანიზაციულ-ტექნიკური ზომების მიღება;
— აუდიომონიტორინგსა და ვიდეომონიტორინგთან დაკავშირებით — დამუშავების მიზნის, მოცულობის, ხანგრძლივობის, ჩანაწერებზე წვდომის, მათი შენახვის, განადგურების წესის/პირობებისა და მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმების წერილობით განსაზღვრა;
— ვიდეომონიტორინგის კანონიერად წარმართვის მიზნით გამაფრთხილებელი ნიშნების თვალსაჩინო ადგილზე განთავსება, მონაცემთა სუბიექტთა ზეპირსიტყვიერი ინფორმირების ფორმის/მეთოდის უნიფიცირება, ვიდეოჩამწერ/შემნახველ სისტემებში მონაცემების მიმართ განხორციელებული ყველა მოქმედების აღრიცხვისა და ოპერაციულ სისტემაზე განპიროვნებული მომხმარებლებით წვდომის უზრუნველყოფა;
— საჯარო უწყებას მიეცა თანამშრომლების პირადი ელექტრონული ფოსტების გამოყენების შეწყვეტისა და შენახული პერსონალური მონაცემების წაშლა;
— ელექტრონულ სისტემაში მომხმარებლის დროებითი უმოქმედობის შემთხვევაში, მონაცემების უსაფრთხოებისა და არასანქცირებული წვდომების რისკის შესამცირებლად ბმულის ავტომატური დეაქტივაციის (სესიის გათიშვის) ფუნქციის დამატება; გარდა ამისა, სამსახურებრივ კომპიუტერებზე განპიროვნებული, პაროლით დაცული მომხმარებლის შექმნა. მსგავსი მითითებები გათვალისწინებულ იქნა ელექტრონულ მონაცემთა ბაზებთან დაკავშირებითაც, ვინაიდან გამოვლინდა შემთხვევები, რომელთა ფარგლებში სისტემის ერთი და იმავე მომხმარებლით სარგებლობდა სხვადასხვა თანამშრომელი;
— ელექტრონულ სისტემებში არსებულ პერსონალურ მონაცემთა მიმართ განხორციელებული ყველა მოქმედების აღრიცხვას უზრუნველყოფა და ორგანიზაციული და ტექნიკური ზომების მიღება;
— მომსახურების ფიზიკური სივრცის ფარგლებში ვერბალური კომუნიკაციის დროს მონაცემების არაკანონიერი გამჟღავნების რისკების შესამცირებლად, სათანადო ორგანიზაციული და ტექნიკური ზომების მიღება;
— პერსონალური მონაცემების შემცველი დოკუმენტაციის ადრესატისთვის ჩაბარების პროცესში, მონაცემების მესამე პირისათვის გამჟღავნების შესაძლო რისკების თავიდან აცილების მიზნით, ტექნიკური და ორგანიზაციული ზომების მიღების რეკომენდაცია;

— კანონის 28-ე მუხლით[9] გათვალისწინებული ვალდებულების შესასრულებლად, ვიდეო-აუდიომონიტორინგის გზით მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა;
— საანგარიშო პერიოდში მონაცემთა უკანონო დამუშავების პრევენციის, გამოვლენისა და აღკვეთის მიზნით ელექტრონული ფორმით დამუშავებულ მონაცემებზე წვდომის ფაქტების სათანადო მონიტორინგის მექანიზმის შემუშავება და დანერგვა;
— პასუხისმგებელი საჯარო უწყებებისათვის, ინციდენტთან დაკავშირებული ვალდებულებების შესრულების მიზნით, ინციდენტის აღრიცხვის, ინციდენტის თაობაზე სამსახურისათვის შეტყობინებისა და მონაცემთა სუბიექტების ინფორმირება;
— მონაცემთა დაცვის ოფიცრის დაუყოვნებლივ დანიშვნა, მისი საქმიანობის ინტერესთა კონფლიქტის გარეშე უზრუნველყოფა, კანონის 33-ე მუხლით დადგენილ სტანდარტებსა და მოთხოვნებთან (მათ შორის სათანადო ცოდნის თაობაზე) ოფიცრის საქმიანობის შესაბამისობაში მოყვანა, ასევე – მონაცემთა სუბიექტების მიერ თავიანთი უფლებების მარტივად განხორციელების მიზნით, პერსონალურ მონაცემთა დაცვის ოფიცრის საიდენტიფიკაციო და საკონტაქტო მონაცემების პროაქტიული გამოქვეყნება;
— რამდენადაც უწყება სხვა საჯარო დაწესებულების მონაცემთა ბაზებიდან ლეგიტიმური მიზნის მიღწევისათვის საჭიროზე მეტ ინფორმაციას მოიპოვებდა, მას კანონიერი მიზნის ადეკვატური და პროპორციული მოცულობის მონაცემების განსაზღვრა და მასზე დაყრდნობით სამომავლო საქმიანობის წარმართვა დაევალა.

[9] მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინება.

2. მონაცემთა დამუშავება კერძო სექტორში

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირებს არაერთი ვალდებულების შესრულება დაეკისრათ, რაც მონაცემთა დამუშავების პროცესში ევროპული კანონმდებლობის მოთხოვნების დაცვასა და საქართველოში მონაცემთა დაცვის სამართლებრივი კულტურის გაღრმავებას ემსახურება.

მონაცემთა დამუშავების კანონიერების კონტროლის მიზნით, საკუთარი ინიციატივით (არაგეგმური შემოწმების (ინსპექტირების)) და მონაცემთა სუბიექტების/დაინტერესებული პირების განცხადებებისა და შეტყობინებების საფუძველზე შეისწავლა კერძო ორგანიზაციებისა და ფიზიკური პირების მიერ მონაცემთა დამუშავების კანონიერების არაერთი ფაქტი. გამოიკვეთა მთელი რიგი პრობლემური საკითხები, რომლებიც უკავშირდება: მონაცემთა სუბიექტის საკუთარ მონაცემებზე ხელმისაწვდომობას; გამჭვირვალობის პრინციპის დაცვით მონაცემთა დამუშავებას; მონაცემთა უსაფრთხოების დარღვევას (ინციდენტი); მონაცემთა დამუშავებას პირდაპირი მარკეტინგის მიზნით; მონაცემების დაცვას შრომით ურთიერთობებში; ვიდეომონიტორინგის განხორციელებას და ა. შ.

2.1. მნიშვნელოვანი მიმართულებები და ტენდენციები

ა. მონაცემთა სუბიექტის ხელმისაწვდომობა საკუთარ მონაცემებზე

საკუთარ მონაცემებზე მონაცემთა სუბიექტის ხელმისაწვდომობა მონაცემთა დაცვის კანონმდებლობის ერთ-ერთი მთავარი მიზანი და არაერთი უფლების რეალიზაციის წინაპირობაა. მონაცემთა სუბიექტის უფლება, წვდომა ჰქონდეს საკუთარ მონაცემებზე, ერთი მხრივ, ემსახურება მონაცემთა სუბიექტის ინფორმირებას მის შესახებ მონაცემების დამუშავების თაობაზე, ხოლო, მეორე მხრივ, მას კანონით განსაზღვრული სხვა უფლებების რეალიზებისთვის დამხმარე ფუნქცია აქვს. მონაცემებზე წვდომის უფლება აუცილებელია, რათა მონაცემთა სუბიექტს მიეცეს მონაცემების დამუშავების შეწყვეტის, წაშლის, განადგურების ან დაბლოკვის მოთხოვნის საშუალება. შესაბამისად, მონაცემთა სუბიექტის უფლებების რეალიზაციის ხელშეწყობა, მის ინფორმირებასთან დაკავშირებული ქმედითი მექანიზმების დანერგვა და მათი ეფექტიანი გამოყენება სამსახურის ერთ-ერთ მთავარ გამოწვევას წარმოადგენდა.

მონაცემთა სუბიექტის მიერ საკუთარ მონაცემებზე წვდომის უზრუნველყოფის პროცესში გამოიკვეთა დამუშავებისთვის პასუხისმგებელი პირების მიერ კანონმდებლობით ნაკისრი ვალდებულებების შეუსრულებლობის ან ნაკლოვანი შესრულების შემდეგი ფაქტები:

— მონაცემთა სუბიექტებისთვის მათი მონაცემების შემცველი დოკუმენტაციის/ინფორმაციის მიუწოდებლობის ან კანონით განსაზღვრული ვადის დარღვევით გადაცემის შემთხვევები. აღნიშნული არ

შეიძლება გახდეს დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა სუბიექტის საკუთარ მონაცემებზე წვდომის უფლების შეზღუდვის საფუძველი. შესაბამისად, მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა მონაცემთა სუბიექტებს მოთხოვნილი დოკუმენტაცია/ინფორმაცია მიაწოდონ კანონით განსაზღვრული 10 სამუშაო დღის ვადაში, რომელიც საჭიროა მოთხოვნილი მასალის ხასიათისა და მოცულობის გათვალისწინებით, დოკუმენტაციის მოსამზადებლად და მონაცემთა სუბიექტისთვის გადასაცემად;[10]

— შესწავლილი პროცესების საფუძველზე გამოიკვეთა მონაცემთა სუბიექტის კანონით დადგენილი ათდღიანი ვადის დარღვევით ინფორმირების ფაქტები. ამასთან, ზოგიერთ შემთხვევაში, მოთხოვნილი ინფორმაცია/დოკუმენტაცია მონაცემთა სუბიექტს არ მიეწოდა. ასევე, არ განემარტა უარის თქმის საფუძვლების არსებობის შესახებ, რის გამოც დამუშავებისთვის პასუხისმგებელ პირს სამსახურმა შესასრულებლად სავალდებულო დავალება მისცა. გარდა ამისა, კანონით განსაზღვრული ვადის დასაცავად მნიშვნელოვანია, დამუშავებისთვის პასუხისმგებელმა პირებმა უზრუნველყონ დასაქმებულ პირებზე უფლებამოსილებების იმგვარი დელეგირება, რომ ადამიანური რესურსის ნაკლებობა არ გახდეს მონაცემთა სუბიექტისთვის ინფორმაციის 10 სამუშაო დღის ვადის დარღვევით მიწოდების მიზეზი. შესაბამისად, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა დანერგონ ისეთი ღონისძიება, რომელიც უზრუნველყოფს მონაცემთა სუბიექტის უფლების რეალიზების ქმედით შესაძლებლობას;

— ასევე, გამოვლინდა მონაცემთა სუბიექტის უფლებების შეზღუდვის ფაქტები. ცალკეულ შემთხვევებში, სამსახურმა კანონიერად მიიჩნია დამუშავებისთვის პასუხისმგებელი პირის მხრიდან მონაცემთა სუბიექტის უფლებების შეზღუდვა მესამე პირების უფლებებისა და თავისუფლებების დაცვის მიზნით, რის შესახებაც დამუშავებისთვის პასუხისმგებელმა პირმა უზრუნველყო მონაცემთა სუბიექტის ინფორმირება. აქვე ხაზგასასმელია, რომ, კანონით გათვალისწინებული მონაცემთა სუბიექტის უფლებების შეზღუდვის რომელიმე საფუძვლის არსებობის შემთხვევაში დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ მონაცემთა სუბიექტის ინფორმირება მისი უფლების შეზღუდვის საფუძვლის შესახებ იმგვარად, რომ თავად შეზღუდვის ინტერესს ზიანი არ მიადგეს;

— ერთ-ერთ შემთხვევაში, როცა საქმე მონაცემთა სუბიექტისათვის აუდიოჩანაწერის გადაცემის მოთხოვნას შეეხებოდა, დამუშავებისთვის პასუხისმგებელმა პირმა (ბანკი) მონაცემთა სუბიექტს შესთავაზა, მიეღო აუდიოჩანაწერის ე. წ. „ტრანსკრიპტი“ ან აუდიოჩანაწერს დამუშავებისთვის

[10] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-13 მუხლის მე-2 პუნქტი ადგენს, განსაკუთრებულ შემთხვევებში და სათანადო დასაბუთებით, კანონით განსაზღვრული ვადის გაგრძელების შესაძლებლობას არა უმეტეს 10 სამუშაო დღისა, რის შესახებაც მონაცემთა სუბიექტს დაუყოვნებლივ უნდა ეცნობოს.

პასუხისმგებელი პირის ოფისში გასცნობოდა, რასთან დაკავშირებითაც მონაცემთა სუბიექტმა უარი განაცხადა. მონაცემთა სუბიექტს სურდა არა მხოლოდ კომუნიკაციის შინაარსის, არამედ – მისი ხმის ჩანაწერის გაცნობაც, რაც მონაცემთა სუბიექტის კანონის მე-14 მუხლის მე-4 პუნქტით განსაზღვრული უფლებაა. შესაბამისად, მონაცემთა სუბიექტმა უარი განაცხადა ბანკის მიერ მონაცემების მიწოდების ალტერნატიულ საშუალებებზე და თავად აირჩია ფორმა (ასლის მიღება), რომლითაც სურდა საკუთარი მონაცემების გაცნობა. ამდენად, სამსახურმა მიიჩნია, რომ დამუშავებისთვის პასუხისმგებელი პირი კანონით დადგენილი წესით იყო ვალდებული, მონაცემთა სუბიექტისთვის გადაეცა მისი მონაცემების შემცველი აუდიოჩანაწერის ასლი, მესამე პირების (გარდა თანამშრომლისა) მონაცემების გადაცემის გარეშე;

— ზოგიერთ შემთხვევაში, მონაცემთა სუბიექტის მიერ მისი მონაცემების შემცველი დოკუმენტაციის გადაცემის მოთხოვნაზე, დამუშავებისთვის პასუხისმგებელი პირები განმარტავდნენ, რომ მოთხოვნილი დოკუმენტაციის ასლები მონაცემთა სუბიექტისათვის უკვე გამჟღავნებული ჰქონდათ. მონაცემთა სუბიექტი ითხოვდა დასაქმების მთელი პერიოდის განმავლობაში მისი მონაცემების შემცველი კონკრეტული დოკუმენტაციის ასლებს. სამსახურის უფროსის მიერ მიღებული გადაწყვეტილების თანახმად, დამუშავებისთვის პასუხისმგებელ პირს ნამდვილად რომ ჰქონოდა მონაცემთა სუბიექტისთვის მოთხოვნილი დოკუმენტაციის ასლის ნაწილი გადაცემული, მას ასლის მიღების უფლების რეალიზებისთვის აქტიური მოქმედებების განხორციელება მაინც მოუწევდა.11 შესაბამისად, სამსახურმა განმარტა, რომ დამუშავებისთვის პასუხისმგებელი პირი კანონით დადგენილი წესით ვალდებული იყო მონაცემთა სუბიექტისთვის გადაეცა მისი მონაცემების შემცველი დოკუმენტაციის ასლები, მესამე პირების მონაცემების გადაცემის გარეშე.

ბ. მონაცემთა დამუშავება გამჭვირვალობის პრინციპის დაცვით

გამჭვირვალობის პრინციპი მჭიდროდაა დაკავშირებული მონაცემთა სუბიექტის უფლებებთან, რომლის მთავარი მოთხოვნაა, ნებისმიერი მონაცემთა სუბიექტისათვის ნათელი იყოს მასთან დაკავშირებული მონაცემების დამუშავების პროცესი (მათ შორის – ვის მიერ, რა გზით, რა მიზნითა და რა მოცულობის მონაცემები მუშავდება) და, ამასთანავე, ამ პროცესთან დაკავშირებული ნებისმიერი ინფორმაცია და კომუნიკაცია უნდა იყოს ადვილად ხელმისაწვდომი და გასაგები, გადმოცემული ნათლად და მარტივი ენით.[12] გამჭვირვალობის პრინციპის

[11] მონაცემთა გამჭვირვალედ დამუშავების პრინციპის მიხედვით, მონაცემთა სუბიექტს მაქსიმალურად მარტივად უნდა მიეწოდოს მოთხოვნილი ინფორმაცია, ყოველგვარი დამატებითი დაბრკოლებების შექმნის გარეშე.

[12] Guidelines on transparency under Regulation 2016/679, 17/EN, WP260 rev.01, Article 29 Working Party, adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018, §6.

სათანადოდ უზრუნველყოფის პირობებში, მონაცემთა სუბიექტები თვითონ ეუფლებიან ინფორმაციას მონაცემების დამუშავებასთან დაკავშირებული რისკებისა და უფლებების განხორციელების საშუალებების შესახებ.

საგულისხმოა, რომ მონაცემთა სუბიექტების უფლებების რეალიზაციის ხელშეწყობის მიზნით მონაცემთა გამჭვირვალედ დამუშავების პრინციპის უზრუნველყოფა სამსახურის ერთ-ერთი მთავარი გამოწვევაა. სამსახურმა შეისწავლა შემთხვევები, რომლებშიც დამუშავებისთვის პასუხისმგებელმა პირებმა მონაცემთა დამუშავების პროცესში ვერ უზრუნველყვეს გამჭვირვალობის პრინციპის მოთხოვნების დაცვა, რის გამოც ჯეროვნად ვერ წარმართეს კანონთან თავსებადი მონაცემთა დამუშავების პროცესი:

— ერთ-ერთ შემთხვევაში მონაცემთა სუბიექტებისთვის მათი მონაცემების შემცველი ინფორმაციის ორგანიზაციიდან გამოთხოვის საშუალებების/გზების თაობაზე ინფორმირება არ შეესაბამებოდა კანონით დადგენილ გამჭვირვალობის პრინციპს. აღნიშნულ შემთხვევაში ორგანიზაციაში მოქმედებდა კონკრეტული ინფორმაციის გამოთხოვის როგორც ფასიანი, ასევე – უფასო საშუალება, თუმცა ორგანიზაცია საჯაროდ არ უზრუნველყოფდა მონაცემთა სუბიექტის ინფორმირებას ფასიანი სერვისის უფასოდ მიღების შესაძლებლობის ალტერნატიული გზების შესახებ. შესაბამისად, სამსახურმა შეაფასა ორგანიზაციის მიერ მონაცემთა სუბიექტისათვის ინფორმაციის საფასურის გადახდის გარეშე მიწოდების მექანიზმის არსებობა (აღნიშნულის შესახებ ამავე სუბიექტის ინფორმირების გარეშე), რაც ზღუდავდა გამჭვირვალობის პრინციპის ეფექტიანობას. სამსახურმა ორგანიზაციას დაავალა ამ პრინციპის მოთხოვნათა დაცვით უზრუნველეყო ვებგვერდისა და პორტალის საშუალებით კონკრეტული ინფორმაციის გამოთხოვის ფასიანი და უფასო მექანიზმების თაობაზე სუბიექტის ინფორმირება;

— კომპანია ტელეფონის მეშვეობით დაუკავშირდა არასრულწლოვან პირს და მასთან კომუნიკაციის პროცესში, მონაცემთა სუბიექტის მოთხოვნის მიუხედავად, არ მომხდარა მონაცემთა სუბიექტისთვის/მისი კანონიერი წარმომადგენლისთვის კომპანიის სახელწოდების და, შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირის შესახებ ინფორმაციის მიწოდება. ამდენად, მონაცემთა სუბიექტისთვის გამჭვირვალე არ იყო, ვინ უკავშირდებოდა მას; შედეგად, მონაცემთა სუბიექტს შეეზღუდა საკუთარი უფლებების რეალიზების შესაძლებლობა (მაგალითად: მიეღო დეტალური ინფორმაცია მის შესახებ დამუშავებული მონაცემების თაობაზე, მოეთხოვა თავისი მონაცემების დამუშავების შეწყვეტა და ა. შ.). საქმეში არსებული ფაქტობრივი გარემოებების გათვალისწინებით, სამსახურმა დაადგინა კომპანიის მიერ მონაცემების დამუშავების შეუსაბამობა გამჭვირვალობის პრინციპთან;

— სამსახურმა ასევე შეაფასა ბანკის მიერ მონაცემთა სუბიექტის მონაცემების დამუშავება, რაც გამოიხატებოდა აღნიშნულ პირთან შეტყობინებების გაგზავნით. მონაცემთა სუბიექტი განმარტავდა, რომ იგი აღარ წარმოადგენდა კონკრეტული ბანკის მომხმარებელს, რამდენადაც დახურული ჰქონდა ყველა არსებული ანგარიში და, შესაბამისად, მას

შეტყობინებები აღნიშნული ბანკის სახელით არ უნდა მიეღო. ბანკმა სამსახურს დაუდასტურა მონაცემთა სუბიექტის მიერ საბანკო ანგარიშების დახურვის ფაქტი, თუმცა განმარტა, რომ ანგარიშების დახურვა საკმარისი არ არის ბანკთან ურთიერთობის სრულად შეწყვეტისთვის და, აღნიშნულის მიუხედავად, მონაცემთა სუბიექტი კვლავ ფიქსირდებოდა ბანკის მომხმარებლად. მიუხედავად იმისა, რომ ბანკმა სამსახურს წარუდგინა მომხმარებელთან დადებული გენერალური ხელშეკრულების ჩანაწერები, რომლებითაც იგი ბანკში არსებული ანგარიშების დახურვის შემთხვევაში ბანკთან ურთიერთობის გაგრძელების თაობაზე მონაცემთა სუბიექტის ინფორმირების უზრუნველყოფას ასაბუთებდა, სამსახურმა მიიჩნია, რომ აღნიშნული ჩანაწერებით აღქმადი არ იყო, რომ ბანკი კლიენტს თავის აქტიურ მომხმარებლად და, შესაბამისად, გენერალური ხელშეკრულების მხარედ მიიჩნევდა იმ შემთხვევაშიც, როცა იგი სრულად აუქმებდა და წყვეტდა ბანკის ყველა მომსახურებას/პროდუქტს/აქტიურ ანგარიშს. ასევე, სამსახურმა მიიჩნია, რომ მონაცემთა სუბიექტს არ ჰქონდა ნათელი წარმოდგენა, რომ ბანკთან ურთიერთობის სრულად შესაწყვეტად საკმარისი არ იყო ბანკის ყველა მომსახურებაზე/პროდუქტზე უარის თქმა და ამისთვის აუცილებელი იყო კონკრეტულად სამართლებრივი ურთიერთობის სრულად შეწყვეტის მოთხოვნა. შესაბამისად, ბანკს დაევალა, გამჭვირვალობის პრინციპის მოთხოვნების დაცვით, შეტყობინების ავტორის ინფორმირება, რომ ბანკთან ურთიერთობის სრულად შესაწყვეტად საკმარისი არ არის ბანკის ყველა მომსახურებაზე/პროდუქტზე უარის თქმა და ამისთვის აუცილებელია კონკრეტულად სამართლებრივი ურთიერთობის სრულად შეწყვეტის თაობაზე მოთხოვნის დაყენება;

— ერთ-ერთი შემთხვევის შესწავლის პროცესში დადგინდა, რომ კომპანიის მიერ მიღებული შიდაორგანიზაციული დოკუმენტები და კომპანიასა და დასაქმებულს შორის დადებული შრომითი ხელშეკრულება არ შეიცავდა ინფორმაციას კომპანიის მხრიდან თანამშრომლის სამსახურებრივი ელექტრონული ფოსტის შესაძლო კონტროლის/წვდომის, თანამშრომლის სამსახურიდან გათავისუფლების შემთხვევაში, სამსახურებრივი ელექტრონული ფოსტის გამოყენების, მასზე არსებული ინფორმაციის შენახვისა და შენახვის ხანგრძლივობის შესახებ. შესაბამისად, კომპანიის მიერ ზემოაღნიშნული დოკუმენტაციის განმცხადებლისათვის გაცნობის შემთხვევაშიც კი, კომპანია ვერ უზრუნველყოფდა კანონის მე-4 მუხლით განსაზღვრული გამჭვირვალობის პრინციპის მოთხოვნების რეალიზებას. აღნიშნულიდან გამომდინარე, სამსახურმა მიიჩნია, რომ კომპანიის მიერ მონაცემთა დამუშავების პროცესში მონაცემთა სუბიექტისათვის არ იყო უზრუნველყოფილი გამჭვირვალობის პრინციპის მოთხოვნები. კომპანიას დაევალა სათანადო წესების შემუშავება, რომლებითაც კომპანიის თანამშრომლები ინფორმირებული იქნებოდნენ სამსახურებრივი ელექტრონული ფოსტის კომპანიის მხრიდან შესაძლო კონტროლის/წვდომის, თანამშრომლის სამსახურიდან გათავისუფლების შემთხვევაში, სამსახურებრივი ელექტრონული ფოსტის გამოყენების, მასზე არსებული ინფორმაციის შენახვისა და შენახვის ხანგრძლივობის შესახებ;

— სამსახურის მიერ შესწავლილ ერთ-ერთ საქმეში, რომელიც ეხებოდა სამედიცინო დაწესებულების მიერ გარდაცვლილი პირის მონაცემების გაცემის გზით დამუშავებას, სამედიცინო დაწესებულების წარმომადგენელმა განმარტა, რომ არ ევალებოდათ მონაცემთა სუბიექტის ან მონაცემთა სუბიექტის მშობლის, შვილის, შვილიშვილის ან მეუღლის ინფორმირება პირის გარდაცვალების შემთხვევაში მონაცემების დამუშავების აკრძალვის უფლების შესახებ. შესაბამისად, ვინაიდან დაწესებულებაში არ მოიპოვებოდა აკრძალვის შესახებ ინფორმაცია, მათ დასაშვებად მიიჩნიეს მესამე პირზე ინფორმაციის გაცემა. საგულისხმოა, რომ მონაცემთა დამუშავების პროცესში კანონით განსაზღვრული პრინციპები და კონკრეტულად, გამჭვირვალობის პრინციპი, არა მხოლოდ ნორმატიულად მბოჭავ ელემენტს წარმოადგენს, რომლითაც იზღუდება დამუშავებისათვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირის მოქმედების ფარგლები, არამედ აღნიშნულ პრინციპს კანონის ნორმების განმარტების ფუნქციაც აქვს. შესაბამისად, სამსახურმა მიიჩნია, რომ, მართალია, კანონის მე-8 მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტში უშუალოდ არ არის მითითებული მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მხრიდან განსახორციელებელი კონკრეტული ინფორმირების ვალდებულების თაობაზე, მაგრამ, დასახელებული ნორმის გამჭვირვალობის პრინციპის საშუალებით განმარტების საფუძველზე, მარტივად დგინდება კანონმდებლის ნება, წინააღმდეგ შემთხვევაში, საფუძველი არ ექნებოდა ნორმის შინაარსობრივ იდეას პირის გარდაცვალების შემდეგ დაეცვა მისი მონაცემები.

გ. მონაცემთა უსაფრთხოების დარღვევა (ინციდენტი) მონაცემთა დამუშავების პროცესში და მონაცემთა უსაფრთხოების მოთხოვნების დაცვის ვალდებულება

კანონის მე-4 მუხლის „ვ“ ქვეპუნქტით კანონმდებელმა მონაცემთა უსაფრთხოება[13] მონაცემთა დამუშავების პრინციპისათვის დამახასიათებელი

[13] მონაცემთა უსაფრთხოების დაცვა მოითხოვს შესაბამის ზომებს, რომელთა მიზანია: მონაცემთა უსაფრთხოების დარღვევის — ინციდენტის თავიდან აცილება და მართვა; მონაცემთა დამუშავების ამოცანების სწორად შესრულება და სხვა პრინციპებთან შესაბამისობის უზრუნველყოფა და პირთა უფლებების ეფექტიანად განხორციელების ხელშეწყობა. უსაფრთხოების ზომები უნდა მოიცავდეს არა მხოლოდ კიბერუსაფრთხოებას, არამედ ფიზიკურ და ორგანიზაციულ უსაფრთხოებას. ორგანიზაციებმა რეგულარულად უნდა შეამოწმონ, არის თუ არა მათი უსაფრთხოების ზომები განახლებული და ეფექტიანი. შესაბამისად, მონაცემთა უსაფრთხოების სათანადო ზომების მიღებისას გათვალისწინებულ უნდა იქნეს მონაცემთა უსაფრთხოების თანამედროვე მეთოდები და ტექნოლოგიები, უახლესი მიღწევები, განხორციელების ხარჯები, ასევე – დამუშავების ხასიათი, ფარგლები, კონტექსტი და მიზნები. ამასთან, გასათვალისწინებელია, ფიზიკური პირების უფლებებსა და თავისუფლებებზე დამუშავების ოპერაციის გავლენა. იხ.: რეკომენდაციები პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ, პერსონალურ მონაცემთა დაცვის სამსახური, თბილისი, 2024, 28. აღნიშნული რეკომენდაცია იხ.: <https://pdps.ge/ka/content/984/rekomendaciebi?page=2> [17.02.2025].

ზოგადი მარეგულირებელი ნორმატიული შინაარსით აღჭურვა, რომლის მიხედვითაც მონაცემების უსაფრთხოების დაცვის მიზნით მონაცემთა დამუშავებისას მიღებულ უნდა იქნეს ის ტექნიკური და ორგანიზაციული ზომები, რომლებიც სათანადოდ უზრუნველყოფენ მონაცემთა დაცვას, მათ შორის – უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვისგან, განადგურებისგან ან/და დაზიანებისგან. საქართველოს საკონსტიტუციო სასამართლომ პირადი ცხოვრების ძირითადი უფლების შემადგენელ კომპონენტად მოიაზრა „მონაცემების ე. ი. პირის შესახებ ინფორმაციის დაცვა გამჟღავნებისაგან“ და აღნიშნა, რომ მის დაცვას „ღირებული ლეგიტიმური მიზანი“[14] აქვს. თავის მხრივ, კანონის მე-4 მუხლის მე-7 პუნქტით, კანონმდებელმა დამუშავებისათვის პასუხისმგებელ პირს დააკისრა მონაცემთა დამუშავებისას მონაცემთა უსაფრთხოების პრინციპის დაცვის ვალდებულება. შესაბამისად, კანონით მონაცემთა უსაფრთხოების დაცვის სტანდარტი კიდევ უფრო გაიზარდა, ვინაიდან იგი განმტკიცდა არა მხოლოდ პრინციპების დონეზე, არამედ მონაცემთა უსაფრთხოების დარღვევის შემთხვევა ცალკე ცნებად განისაზღვრა და დამატებითი რეგულაციის ქვეშ მოექცა. კერძოდ, ინციდენტი არის მონაცემთა უსაფრთხოების დარღვევა, რომელიც იწვევს მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას/მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას. კანონი მონაცემთა სუბიექტების უფლებების დაცვის მიზნით ინციდენტთან დაკავშირებულ შემთხვევებს საკმაოდ ფართო რეგულაციის ქვეშ აქცევს, განსაკუთრებით, თუკი ინციდენტი საშუალო ან მაღალი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს. ასეთ შემთხვევებში მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს ვალდებულება აქვს, ინციდენტის შესახებ აცნობოს როგორც მონაცემთა სუბიექტებს, ასევე – სამსახურს, რომელიც უფლებამოსილია შეამოწმოს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი და საჭიროების შემთხვევაში შესაბამისი დავალებები მისცეს მონაცემთა მიმართ მიღებული უსაფრთხოების განსამტკიცებლად.

იმის გათვალისწინებით, რომ მონაცემთა უსაფრთხოების დარღვევას შეიძლება უარყოფითი გავლენა ჰქონდეს მონაცემთა სუბიექტების პირადი ცხოვრებისა და მონაცემთა დაცვის უფლებაზე, აუცილებელია, დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირის მიერ დაცული იყოს მონაცემების დამუშავებისა და უსაფრთხოების ზომების კანონმდებლობით დადგენილი სტანდარტი.

ინციდენტთან დაკავშირებით, სამსახურს რამდენიმე მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა მომართა, ხოლო ერთ შემთხვევაში მსგავსი შეტყობინება სამსახურმა მესამე პირისგან მიიღო. აღნიშნული შეტყობინებების საფუძველზე, მიმდინარე შემოწმებების დროს, ყველა შემთხვევაში დადგინდა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი

[14] საქართველოს საკონსტიტუციო სასამართლოს 2019 წლის 7 ივნისის №1/4/693,857 გადაწყვეტილება საქმეზე „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ“, II, §25.

პირების მიერ მიღებული ტექნიკური და ორგანიზაციული ზომები არ აღმოჩნდა საკმარისი ინციდენტების თავიდან ასარიდებლად. საქმიანობის შინაარსის გათვალისწინებით, აღნიშნული პირები ვალდებულნი იყვნენ, მონაცემთა დამუშავების პროცესში გაეთვალისწინებინათ იმ მონაცემთა კატეგორიები (მათ შორის – განსაკუთრებული კატეგორიის მონაცემები), რომლებსაც ამუშავებენ, მათი მოცულობა (ერთ შემთხვევაში — ასეულობით ათასი მონაცემი), ფორმა, შენახვის საშუალებები (ყველა შემთხვევაში მონაცემები ინახებოდა ელექტრონულ საშუალებებზე) და მონაცემთა სუბიექტის უფლებების დარღვევის შესაძლო საფრთხეები (განხილულ შემთხვევებში — ელექტრონულ სისტემებზე თავდასხმის საფრთხეები, რომლებსაც მნიშვნელოვნად ზრდიდა იმ მონაცემთა სიმრავლე და კატეგორიები, რომლებსაც კომპანიები ამუშავებენ) და აღნიშნულის საფუძველზე მიეღოთ შესაბამისი უსაფრთხოების ზომები, რაც მონაცემთა უკანონო დამუშავების სათანადო პრევენციას უზრუნველყოფდა.

სამსახურმა დაადგინა, რომ, მართალია, დამუშავებისთვის პასუხისმგებელმა პირებმა სამსახურს აცნობეს ინციდენტთან დაკავშირებით (გარდა ერთი შემთხვევისა), თუმცა სამსახურისთვის ინციდენტის შეტყობინების კანონისმიერი ვალდებულება არასათანადოდ შეასრულეს. კერძოდ, დამუშავებაზე პასუხისმგებელმა არცერთმა პირმა არ უზრუნველყო სამსახურისთვის ინციდენტთან დაკავშირებული ინფორმაციის სრულად მიწოდება ისე, როგორც ამას „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი და შესაბამისი კანონქვემდებარე ნორმატიული აქტი განსაზღვრავს. დამუშავებისთვის პასუხისმგებელი პირების განმარტებით, სამსახურის სათანადო ინფორმირება ინციდენტებთან დაკავშირებით არ განხორციელდა, ვინაიდან ნაკლებსავარაუდო იყო, რომ ინციდენტები მნიშვნელოვან ზიანს გამოიწვევდა ან/და მნიშვნელოვან საფრთხეს შეუქმნიდა ადამიანის ძირითად უფლებებსა და თავისუფლებებს. სამსახურმა არცერთ შემთხვევაში არ გაიზიარა დამუშავებისთვის პასუხისმგებელი პირების მიერ დასახელებული არგუმენტები და განმარტა, რომ საქმეში წარმოდგენილი იყო პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის №19 ბრძანებით დამტკიცებული „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმები და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის“ (შემდგომ — წესი) მე-5 მუხლით გათვალისწინებული რამდენიმე გარემოება, რაც დამუშავებისთვის პასუხისმგებელმა პირმა ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი საფრთხის შექმნის სიმძიმის განსაზღვრის მიზნებისთვის უნდა გაითვალისწინოს. კერძოდ, ერთ შემთხვევაში დადგინდა, რომ ინციდენტის სახეს წარმოადგენდა კონფიდენციალურობის დარღვევა (მონაცემებზე განხორციელდა უკანონო წვდომა), ამასთან, ინციდენტის შედეგად მონაცემთა სუბიექტების მესამე პირის მიერ იდენტიფიცირების შესაძლებლობის ხარისხი იყო მაღალი, ვინაიდან წვდომა განხორციელდა პირადობის დამადასტურებელ დოკუმენტებზე (პირადობის მოწმობა და პასპორტი). ასევე, სახეზე იყო „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით განსაზღვრული დამუშავებისთვის პასუხისმგებელი პირის საქმიანობის განსაკუთრებული ხასიათი, რომლის საქმიანობა განსაკუთრებულ რეგულაციას

ექვემდებარებოდა. ამასთან, ინციდენტს მასშტაბური ხასიათი ჰქონდა როგორც მონაცემთა სუბიექტის, ასევე – მონაცემის რაოდენობისა და მოცულობის თვალსაზრისით (ინციდენტი შეეხებოდა რამდენიმე ათასი ფიზიკური პირის სხვადასხვა მონაცემს).

ერთ-ერთ საქმეში ინციდენტი გამოვლინდა კონფიდენციალურობის დარღვევაში (მონაცემთა უკანონო გამჟღავნება), ხოლო ინციდენტის შედეგად გამჟღავნდა მონაცემთა სუბიექტებთან დაკავშირებული, მათ შორის – განსაკუთრებული კატეგორიის მონაცემები. ამასთან, განსაკუთრებული კატეგორიის მონაცემებთან მიმართებით, სახეზე იყო გამჟღავნებული მონაცემების დიდი მოცულობა[15]. გარდა აღნიშნულისა, ინციდენტის შედეგად მესამე პირის მხრიდან მომხმარებლის იდენტიფიცირების ხარისხი მაღალი იყო, ვინაიდან გამჟღავნდა მონაცემთა სუბიექტის სახელი, გვარი, სქესი, დაბადების თარიღი და პირადი ნომერი. სამსახურმა მიუთითა წესის მე-6 მუხლზე და ვინაიდან დამუშავებისთვის პასუხისმგებელმა პირმა განსაკუთრებული კატეგორიის მონაცემები (ანალიზების პასუხები) უკანონოდ გაამჟღავნა, აღნიშნული ინციდენტი სამსახურმა ადამიანის ძირითადი უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამომწვევად მიიჩნია.

ინციდენტის მომწესრიგებელი ნორმები წარმოადგენს მონაცემთა სუბიექტების უფლებების ეფექტიანად დაცვის, მათი მონაცემების შემდგომი უკანონო დამუშავების პრევენციისა და სამსახურთან, როგორც მონაცემთა დაცვის საზედამხედველო ორგანოსთან, თანამშრომლობის გზით მონაცემთა დაცვის უფლების რეალიზების მნიშვნელოვან სამართლებრივ ინსტრუმენტს, რომლის განხორციელებაში არსებითი მნიშვნელობა აქვს დამუშავებისთვის პასუხისმგებელი პირის მხრიდან მონაცემთა გამჟღავნების ფაქტის, როგორც ინციდენტის, დროულ კვალიფიკაციას. შესაბამისად, დამუშავებისთვის პასუხისმგებელმა პირებმა, კანონითა და აღნიშნული წესით დადგენილი მოთხოვნების დაცვით, სამსახურთან კოორდინაციაში უნდა უზრუნველყონ იმ უარყოფითი ეფექტების მაქსიმალურად განეიტრალება, რომლებიც შეიძლება მოჰყვეს ინციდენტს.

დ. პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავება

მონაცემთა სუბიექტის უფლებების ეფექტიანი რეალიზებისთვის კანონით ახლებურად მოწესრიგდა პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების სპეციალური მუხლი. კერძოდ, მიუხედავად მონაცემთა შეგროვების ან/და მოპოვების საფუძვლისა და მათი ხელმისაწვდომობისა, პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავება შეიძლება მხოლოდ მონაცემთა სუბიექტის თანხმობით.[16] მონაცემთა სუბიექტის სახელის, გვარის, მისამართის,

[15] გამჟღავნდა მომხმარებლის ანალიზის პასუხები, სადაც მითითებული იყო ლაბორატორიული კვლევის შედეგები.

[16] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-12 მუხლის პირველი პუნქტი.

ტელეფონის ნომრისა და ელექტრონული ფოსტის მისამართის გარდა, პირდაპირი მარკეტინგის მიზნით, სხვა მონაცემთა დამუშავებისთვის აუცილებელია მონაცემთა სუბიექტის წერილობითი თანხმობა. მნიშვნელოვანია, რომ, მონაცემთა სუბიექტის თანხმობის მიღებამდე და პირდაპირი მარკეტინგის განხორციელებისას, დამუშავებისთვის პასუხისმგებელმა პირმა/დამუშავებაზე უფლებამოსილმა პირმა მონაცემთა სუბიექტს ნათლად, მარტივ და მისთვის გასაგებ ენაზე უნდა განუმარტოს მის მიერ თანხმობის ნებისმიერ დროს გამოხმობის უფლება და ამ უფლების განხორციელების მექანიზმი და წესი. გარდა ამისა, დამუშავებისთვის პასუხისმგებელი პირი/დამუშავებაზე უფლებამოსილი პირი ვალდებულია, უზრუნველყოს მონაცემთა სუბიექტის შესაძლებლობა, მოითხოვოს პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების შეწყვეტა იმავე ფორმით, რომლითაც პირდაპირი მარკეტინგი ხორციელდება ან განსაზღვროს სხვა ხელმისაწვდომი და ადეკვატური, მარტივი საშუალება მონაცემთა დამუშავების შეწყვეტის მოთხოვნისთვის. ამასთან, მონაცემთა სუბიექტს უნდა მიეცეს მკაფიო და ადვილად აღსაქმელი მითითება ამ საშუალების გამოყენების შესახებ. დაუშვებელია, მონაცემთა სუბიექტის მიერ თანხმობის გამოხმობის უფლების განსახორციელებლად დაწესებულ იქნეს საფასური ან სხვა შეზღუდვა. გარდა ზემოაღნიშნულისა, კანონის მე-3 მუხლის „მ“ და „ნ“ ქვეპუნქტებით განსაზღვრულია მონაცემთა სუბიექტის თანხმობისა და წერილობითი თანხმობის ცნებები. კერძოდ, მონაცემთა სუბიექტის თანხმობა არის მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე აქტიური მოქმედებით, წერილობით (მათ შორის — ელექტრონულად) ან ზეპირად, თავისუფლად და მკაფიოდ გამოხატული ნება, ხოლო მონაცემთა სუბიექტის წერილობითი თანხმობა — თანხმობა, რომელსაც მონაცემთა სუბიექტმა ხელი მოაწერა ან რომელიც მან სხვაგვარად გამოხატა წერილობით (მათ შორის, ელექტრონულად) მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე შესაბამისი ინფორმაციის მიღების შემდეგ.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის თანახმად, მონაცემთა პირდაპირი მარკეტინგის მიზნით დამუშავება შესაძლებელია მხოლოდ მონაცემთა სუბიექტის თანხმობით. იქიდან გამომდინარე, რომ კანონის ამოქმედებამდე ნებადართული იყო საჯაროდ ხელმისაწვდომი წყაროებიდან მოპოვებული მონაცემების პირდაპირი მარკეტინგის მიზნით დამუშავება და, ამასთანავე, დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირებს უფლება ჰქონდათ მონაცემთა შეგროვების მიზნის მიუხედავად, პირდაპირი მარკეტინგის მიზნით დაემუშავებინათ მონაცემები (პირის სახელი, მისამართი, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, ფაქსის ნომერი), აღნიშნული მიმართულებით სამსახურისადმი მომართვიანობა მკვეთრად გაიზარდა. საანგარიშო პერიოდში სამსახურს განცხადებითა და შეტყობინებით მომართა ასობით პირმა, მათ მფლობელობაში არსებულ სატელეფონო ნომრებზე, მათი თანხმობის გარეშე, მარკეტინგული შინაარსის არაერთი მოკლეტექსტური შეტყობინების მიღების შესახებ. წარმოდგენილი მომართვები შეეხებოდა ერთი და იმავე კომპანიებისგან მიღებულ შეტყობინებებსაც. გარდა კონკრეტულ განცხადებებზე რეაგირებისა, სამსახურმა

დააიდენტიფიცირა ელექტრონული კომუნიკაციების სფეროში ავტორიზებული პირები, რომლებიც პირდაპირი მარკეტინგის მიზნით უწევდნენ შესაბამის მომსახურებას დამუშავებისთვის პასუხისმგებელ პირებს. სამსახურში შემოსული განცხადებების/შეტყობინებების რაოდენობისა და შინაარსის, შესაბამისი კომპანიების საქმიანობის სპეციფიკისა და მათ მიერ მონაცემთა დამუშავების შესაძლო მასშტაბის გათვალისწინებით, პირდაპირი მარკეტინგის მიზნით მონაცემების შესაძლო კანონდარღვევით დამუშავების ფაქტების გამოსავლენად, საანგარიშო პერიოდში ჩატარდა არაგეგმური შემოწმებები (ინსპექტირებები).

შემოწმებების (ინსპექტირებების) ფარგლებში, მონაცემთა სუბიექტების მიერ სამსახურში წარმოდგენილი მტკიცებულებების გათვალისწინებით, გამოვლინდა, რომ პირდაპირი მარკეტინგის განსახორციელებლად, ავტორიზებული პირების მომსახურებას იყენებდა ათეულობით კომპანია (კონტრაქტორი კომპანია), რომელთა მიზნებისთვის სატელეფონო ნომრებზე მარკეტინგული შინაარსის შეთავაზებები იგზავნებოდა. ამდენად, სამსახურმა, ასევე შეაფასა კომპანიების მიერ მონაცემთა პირდაპირი მარკეტინგის მიზნით დამუშავების კანონშესაბამისობის საკითხი.

სამსახურმა შეისწავლა შემთხვევები, რომლებშიც დამუშავებისთვის პასუხისმგებელმა პირებმა მონაცემთა სუბიექტების თანხმობის (მათ შორის – წერილობითი თანხმობის) გარეშე დაამუშავეს მათი მონაცემები. ასევე, მონაცემთა სუბიექტის თანხმობის მიღებამდე და პირდაპირი მარკეტინგის განხორციელებისას, მონაცემთა სუბიექტს ნათლად, მარტივ და მათთვის გასაგებ ენაზე არ განუმარტეს თანხმობის ნებისმიერ დროს გამოხმობის უფლება და ამ უფლების განხორციელების მექანიზმი/წესი. აგრეთვე, მონაცემთა სუბიექტის შესაბამისი მოთხოვნის საფუძველზე, კანონით დადგენილ ვადაში არ შეწყვიტეს მონაცემთა სუბიექტის მონაცემების დამუშავება პირდაპირი მარკეტინგის მიზნით, არ განსაზღვრეს მექანიზმი მონაცემთა პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების შეწყვეტისთვის იმავე ფორმით, რომლითაც პირდაპირი მარკეტინგი ხორციელდება. ამასთან, გარკვეულ შემთხვევებში, მონაცემთა სუბიექტის მიერ თანხმობის გამოხმობის უფლების განსახორციელებლად დაწესებული იყო საფასური.

ზემოაღნიშნულ შემთხვევებში სამართალდამრღვევად ცნობილ იქნა არაერთი ფიზიკური და იურიდიული პირი (როგორც დამუშავებისთვის პასუხისმგებელი, ასევე დამუშავებაზე უფლებამოსილი პირი), რომლებსაც სანქციის სახით დაეკისრათ როგორც გაფრთხილება, ასევე – ჯარიმა. სამსახურმა ყველა იმ პირს, რომელიც მონაცემთა სუბიექტების სატელეფონო ნომრებს ამუშავებდა მათი თანხმობის გარეშე, განუსაზღვრა შესასრულებლად სავალდებულო დავალება, როგორც მონაცემთა ბაზებში ასახული სატელეფონო ნომრების პირდაპირი მარკეტინგის მიზნით დამუშავების შეწყვეტის შესახებ, ასევე, უფლებამოსილი პირისთვის კანონით განსაზღვრული მონიტორინგის გაწევის თაობაზე, რაც, თავის მხრივ, უზრუნველყოფს მონაცემების უკანონო დამუშავების პროცესების სამომავლოდ აღკვეთას.

ასევე, შემოწმებებისას გამოიკვეთა შემთხვევები, როდესაც კონტრაქტორ კომპანიებს მონაცემთა სუბიექტების თანხმობები მოპოვებული ჰქონდათ კანონის

მოთხოვნათა დაცვით. ამდენად, მათ მიერ მონაცემების პირდაპირი მარკეტინგის მიზნით დამუშავებისას არ გამოიკვეთა კანონის მოთხოვნათა დარღვევის ფაქტები.

ე. საცხოვრებელ შენობაში ვიდეომონიტორინგის საშუალებით მონაცემთა სუბიექტის მონაცემების დამუშავება

მონაცემთა დამუშავების ერთ-ერთ სახედ კანონი ითვალისწინებს ვიდეომონიტორინგის განხორციელებას, განსაზღვრავს მის ცნებას, მიზნებს და აწესრიგებს, მათ შორის საცხოვრებელი შენობის, ჰიგიენისთვის განკუთვნილი ადგილების ან ისეთი სივრცეების ვიდეომონიტორინგთან დაკავშირებულ საკითხებს, სადაც სუბიექტს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს.[17]

საცხოვრებელ შენობაში ვიდეომონიტორინგის გზით მონაცემების დამუშავებასთან დაკავშირებული მომართვები სამსახურში საკმაოდ ხშირია, ხოლო დამუშავებისთვის პასუხისმგებელი პირების მხრიდან ვიდეომონიტორინგი ძირითად შემთხვევებში კანონით დადგენილი მოთხოვნების შეუსრულებლობით ან ნაკლოვანი შესრულებით მიმდინარეობს:

— არაერთ შემთხვევაში დადგინდა, რომ საცხოვრებელ შენობებში საერთო შესასვლელისა და საერთო სივრცის ვიდეომონიტორინგის განხორციელება მესაკუთრეთა ნახევარზე მეტის წერილობითი თანხმობით (მესაკუთრის დადგენის შეუძლებლობის შემთხვევაში შეიძლება მფლობელის თანხმობის მიღება) არ მიმდინარეობდა. ამასთან, გარკვეულ შემთხვევებში ვიდეომონიტორინგის არეალში ექცეოდა საცხოვრებელ შენობაში არსებული ინდივიდუალური საკუთრების შესასვლელები, რისთვისაც კანონით მესაკუთრის/მფლობელის გადაწყვეტილება ან მისი წერილობითი თანხმობაა აუცილებელი. პირის საკუთრებისა და უსაფრთხოების დაცვა კანონით გათვალისწინებული ლეგიტიმური მიზანია, თუმცა აღნიშნულის არსებობა არ არის ვიდეომონიტორინგის მეშვეობით მონაცემების დამუშავების კანონიერების საკმარისი პირობა. პირის უფლებას წარმოადგენს, სხვა პირთა დაკვირვების გარეშე, თავისუფლად ისარგებლოს საკუთარი საცხოვრებელი სივრცით, მათ შორის – დაუბრკოლებლად შეძლოს საკუთარ საცხოვრებელ სახლში გადაადგილება. აღნიშნული უფლება, ერთი მხრივ, მოიცავს პირის შესაძლებლობას, საკუთარი შეხედულებისამებრ, დამოუკიდებლად შექმნას და განავითაროს თავისი პირადი ცხოვრება და, მეორე მხრივ, დაცული იყოს პირად სივრცეში სხვა პირთა ჩარევისგან. მსგავს შემთხვევებში დამუშავებისთვის პასუხისმგებელ პირებს დაევალათ ვიდეომონიტორინგის შეწყვეტა, ვიდეომონიტორინგის შედეგად მოპოვებული მონაცემების წაშლა, ვიდეოკამერების მოხსნა ან ვიდეომონიტორინგის კანონის მოთხოვნათა დაცვით განხორციელება;

— გარკვეულ შემთხვევებში, დამუშავებისთვის პასუხისმგებელ პირებს განთავსებული არ ჰქონდათ ვიდეომონიტორინგის მიმდინარეობის შესახებ

[17] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლის მე-4 პუნქტი.

გამაფრთხილებელი ნიშანი, რამდენიმე შემთხვევაში კი მათ მიერ განთავსებული ნიშანი არ შეიცავდა ინფორმაციას დამუშავებისთვის პასუხისმგებელი პირის სახელწოდებისა და მისი საკონტაქტო მონაცემების შესახებ. დამუშავებისთვის პასუხისმგებელ პირებს დაევალათ ვიდეომონიტორინგის განხორციელებასთან დაკავშირებული, კანონის მოთხოვნების შესაბამისი გამაფრთხილებელი ნიშნის განთავსება;

— სამსახურის მიერ შესწავლილ რამდენიმე შემთხვევაში დადგინდა, რომ, ვიდეოკამერების საცხოვრებელ შენობაში განთავსების მიუხედავად, ვიდეომონიტორინგისას არ ხდებოდა მონაცემთა სუბიექტების მონაცემების დამუშავება, თუმცა ვიდეოკამერების მეშვეობით იქმნებოდა მცდარი წარმოდგენა ვიდეომონიტორინგის განხორციელებასთან დაკავშირებით. აღნიშნულ შემთხვევებში სამსახურმა შეაფასა, რომ კამერების იმ სივრცეში განთავსებამ, სადაც ვიდეომონიტორინგი რეალურად არ მიმდინარეობს, შესაძლოა შეცდომაში შეიყვანოს მონაცემთა სუბიექტები და შეუქმნას მცდარი წარმოდგენა მათი მონაცემების დამუშავების თაობაზე. ამდენად, მონაცემთა სუბიექტების შეცდომაში შეყვანის თავიდან აცილების მიზნით, დამუშავებისთვის პასუხისმგებელ პირებს დაევალათ კამერების ჩამოხსნა ან ვიდეომონიტორინგის განხორციელების შემთხვევაში კანონით დადგენილი მოთხოვნების დაცვა;

— შესწავლილი საქმეების საფუძველზე დადგინდა, რომ საცხოვრებელ შენობებში ვიდეომონიტორინგის განმახორციელებელ დამუშავებისთვის პასუხისმგებელ პირებს, მონაცემთა კანონის შესაბამისად დამუშავების უზრუნველსაყოფად, მიღებული არ ჰქონდათ სათანადო ტექნიკური და ორგანიზაციული ზომები, კერძოდ: ვიდეომონიტორინგის სისტემაზე წვდომა სხვადასხვა პირს ერთი საერთო მომხმარებლისა და პაროლის მეშვეობით ჰქონდა, ვიდეომონიტორინგის სისტემა განთავსებული იყო საერთო სივრცეში და დაცული არ იყო მესამე პირების წვდომისგან, ვიდეომონიტორინგის სისტემა არ აღრიცხავდა ვიდეოჩანაწერების მიმართ შესრულებულ ყველა მოქმედებას და ა. შ.; რაც ქმნიდა ელექტრონული ფორმით შენახული მონაცემების უკანონო მოპოვების, გამჟღავნების, გამოყენების, განადგურებისა და სხვა უკანონო დამუშავების რისკებს. ამასთან, ასეთი მოქმედების არსებობისას შეუძლებელი იყო პასუხისმგებელი პირის იდენტიფიცირება. ამდენად, თითოეულ შემთხვევაში დამუშავებისთვის პასუხისმგებელ პირებს დაევალათ ვიდეომონიტორინგის შედეგად მოპოვებული მონაცემების მიმართ სათანადო ტექნიკური და ორგანიზაციული ზომების მიღება, მათ შორის – ვიდეომონიტორინგის სისტემაზე წვდომისთვის ინდივიდუალური მომხმარებლისა და პაროლის განსაზღვრა, ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების (მათ შორის: ინციდენტების შესახებ, მონაცემთა შეგროვების, შეცვლის, მათზე წვდომის, მათი გამჟღავნების (გადაცემის), დაკავშირებისა და წაშლის თაობაზე ინფორმაციის) აღრიცხვა და სხვა.

ვ. შრომით ურთიერთობებში მონაცემების დაცვა

შრომითი ურთიერთობის ფარგლებში მუშავდება დიდი მოცულობით მონაცემები, რაც განპირობებულია იმით, რომ იგი მოიცავს როგორც სახელშეკრულებო, ასევე – წინასახელშეკრულებო და ხელშეკრულების შემდგომ ურთიერთობებს. შრომითი ურთიერთობის ნებისმიერ ეტაპზე დამსაქმებელი დასაქმების მსურველი პირების, მოქმედი თუ ყოფილი დასაქმებულების მონაცემებს სხვადასხვა მიზნით ამუშავებს, მაგალითად: კვალიფიციური კადრების შერჩევა, შრომითი ხელშეკრულების დადება, კანონმდებლობით ნაკისრი ვალდებულების შესრულება და სხვა. დამსაქმებლების მიერ მონაცემების დამუშავება ხშირად ხდება სხვადასხვა ელექტრონული სისტემის საშუალებით. როგორც წესი, დამსაქმებლის მიერ დამუშავებული მონაცემების მოცულობის გათვალისწინებით, მონაცემთა დამუშავების პროცესში ჩართულია არაერთი პირი. შესაბამისად, ელექტრონულ სისტემებზე დაშვება შესაძლოა ჰქონდეს არაერთ მათგანს. ამდენად, მონაცემთა კონფიდენციალურობის დასაცავად ადეკვატური ორგანიზაციულ-ტექნიკური ზომების მიუღებლობის შემთხვევაში, შესაძლოა, შეიქმნას მონაცემთა შემთხვევითი ან უკანონო დამუშავების მომეტებული საფრთხე.

დასახელებული ფაქტორების გათვალისწინებით, შრომით ურთიერთობებში მონაცემთა სუბიექტთა უფლებების დაცვისას საანგარიშო პერიოდში დაფიქსირდა კანონმდებლობით ნაკისრი ვალდებულებების შეუსრულებლობის ან ნაკლოვანი შესრულების ფაქტები:

— ერთ-ერთი შესწავლის ფარგლებში გაირკვა, რომ კომპანიის დავალებით, გარე სივრცეში ელექტროენერგიის გამანაწილებელ ქსელზე სამუშაოს შესრულებისას, კომპანიის თანამშრომლები, რომლებიც უშუალოდ იყვნენ ჩართულნი ზემოაღნიშნულ ქსელზე სამუშაოების შესრულების პროცესში, თვითონვე ახორციელებდნენ მოსამზადებელი სამუშაო პროცესის ვიდეომონიტორინგს ე. წ. „სამხრე“ ვიდეოკამერების მეშვეობით და, ვიდეოჩაწერასთან ერთად, დამატებით მიმდინარეობდა აუდიოჩაწერა. განსახილველ შემთხვევაში კომპანიის თანამშრომლები ინფორმირებულები იყვნენ ქსელზე შესრულებული სამუშაოების ვიდეომონიტორინგის განხორციელების სავალდებულო წესსა და მიზნობრიობაზე, თუმცა, კანონით დადგენილი პრინციპებიდან გამომდინარე, კონკრეტულად, გამჭვირვალობის პრინციპის შინაარსის გათვალისწინებით და კანონის მე-10 მუხლის მე-2 პუნქტის შესაბამისად, კომპანიას აუცილებლად უნდა ჰქონოდა შემუშავებული წერილობითი დოკუმენტი, რომლის მეშვეობითაც ცალსახად იქნებოდა განსაზღვრული კომპანიის კუთვნილ ელექტროგამანაწილებელ ქსელზე შესასრულებელი სამუშაოების ვიდეომონიტორინგის განხორციელების სრული პროცესი, ვიდეომონიტორინგის მიზანი და მოცულობა, ვიდეომონიტორინგის ხანგრძლივობა და ვიდეოჩანაწერის შენახვის ვადა, ვიდეოჩანაწერზე წვდომის, მისი შენახვისა და განადგურების წესი და პირობები, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმები. ამასთან, დასაქმებული პირებისთვის აუდიომონიტორინგის

მიმდინარეობის შესახებ ინფორმაციის მიწოდების მიუხედავად, კომპანიას არც ქსელზე შესასრულებელი სამუშაოების აუდიომონიტორინგის განხორციელების წესი ჰქონდა შემუშავებული. ამდენად, ხსენებული დოკუმენტების არარსებობის გათვალისწინებით, სამსახურმა ადმინისტრაციული სამართალდარღვევის ფაქტი გამოავლინა და კომპანიას დაავალა მათი შემუშავების უზრუნველყოფა;

— სამსახურმა შეისწავლა ერთ-ერთი დამსაქმებლის მხრიდან დასაქმებული პირების ბიომეტრიული მონაცემების, კერძოდ, თითის ანაბეჭდის დამუშავების კანონიერების საკითხი. შემოწმების შედეგად გაირკვა, რომ დასაქმებულები, კომპანიის მფლობელობაში არსებულ შენობებში შესვლისთვის და შიდა ტერიტორიაზე გადასაადგილებლად ვალდებულები იყვნენ სპეციალურ მოწყობილობაზე თითის ანაბეჭდი დაეფიქსირებინათ. აღსანიშნავია, რომ, კომპანიის საქმიანობის სპეციფიკიდან გამომდინარე, სამსახურმა გაიზიარა კომპანიის შენობებში არსებულ გარკვეულ სივრცეებში (მაგალითად, სათამაშო სივრცეები, ე. წ. „MCR“-ის („Mission Control Room“), სასერვერო ოთახები, უნიფორმებისა და ოფისის ადმინისტრაციის საცავები და ა. შ.) ბიომეტრიული მონაცემების დამუშავების აუცილებლობასთან დაკავშირებით კომპანიის მიერ დასახელებული არგუმენტები (მათ შორის, სათამაშო ბიზნესში არსებული რისკებიდან გამომდინარე, სათამაშო და მასთან დაკავშირებულ სივრცეებში ბიომეტრიული მონაცემების დამუშავების აუცილებლობა, არაუფლებამოსილ პირთა დაშვების პრევენციის აუცილებლობა, საიდუმლო ინფორმაციის, მაგალითად, თამაშების „კონტენტის“, რომელშიც კომპანიის მიერ შექმნილი „კონტენტიც“ იგულისხმება, სასწავლო და კომპანიის საქმიანობასთან დაკავშირებული სამუშაო მასალების გამჟღავნების რისკი), თუმცა, ზოგიერთ სივრცესთან მიმართებით, ბიომეტრიული მონაცემების დამუშავება სამსახურმა არ მიიჩნია კომპანიის მიერ დასახელებული მიზნებისთვის აუცილებელ ზომად. კერძოდ, სპორტდარბაზში და გამოსაცვლელ ოთახებში წვდომის კონტროლისთვის ბიომეტრიული მონაცემების დამუშავების აუცილებლობასთან მიმართებით კომპანიის მიერ დასახელებული არგუმენტები (არ გადაიტვირთოს სპორტდარბაზი და უფლებამოსილი პირების მიერ არ შეფერხდეს მისით სარგებლობა; დასაქმებულთა პირადი ნივთების/ქონების დაცვის საჭიროება, რათა მოხდეს არაუფლებამოსილ პირთა წვდომის და შესაბამისი დანაშაულებრივი ქმედების პრევენცია). კომპანიაში დასაქმებული პირების რაოდენობის გათვალისწინებით, სამსახურის მიერ აღნიშნული არ იქნა მიჩნეული ბიომეტრიული მონაცემების დამუშავების კანონიერ წინაპირობად, რადგან კომპანიის მიზნების მიღწევა შესაძლებელია ბიომეტრიული მონაცემების დამუშავების გარეშეც. კომპანიის მიერ აღნიშნულ სივრცეებთან მიმართებით დასახელებული რისკები შესაძლოა თან ახლდეს ნებისმიერ სამუშაო პროცესს. რაც შეეხება გამოსაცვლელ ოთახებს, სამსახურმა განმარტა, რომ ჩაკეტვის ფუნქციის მქონე შესანახი კარადების არსებობა, კომპანიის მიერ მიღებულ სხვა ორგანიზაციულ-ტექნიკურ ზომებთან ერთად, ბიომეტრიული მონაცემების დამუშავების გარეშეც ქმნიდა თანამშრომელთა

პირადი ნივთების დაცვის შესაძლებლობას. გარდა ხსენებული სივრცეებისა, სამსახურის მიერ კანონის შეუსაბამოდ შეფასდა სათამაშო სივრცეებში (ე. წ. „სტუდიებში“) მომუშავე თანამშრომლების ცვლაში გამოცხადების აღრიცხვა თითის ანაბეჭდის მეშვეობით. ამგვარი შეთავაზება კომპანიის საქმიანობის განხორციელებისათვის თავისთავად გამორიცხავდა ბიომეტრიული მონაცემების დამუშავების აუცილებლობას, რადგან კომპანია მის მიერ დასახელებულ მიზანს აღწევდა იმ პირობებშიც, როდესაც დასაქმებულები ცვლაში გამოცხადებას სხვა ალტერნატიული მექანიზმით აფიქსირებდნენ. გარდა ამისა, კომპანიის მიერ სხვადასხვა დოკუმენტის მეშვეობით განსაზღვრული იყო ის ზოგადი საკითხები, რომლებიც უკავშირდებოდა კომპანიაში დასაქმებულ პირთა პერსონალური (მათ შორის – განსაკუთრებული კატეგორიის) მონაცემების დამუშავებას და მითითებული იყო ბიომეტრიული მონაცემების შაბლონების დამუშავების მიზნები. აღნიშნულის მიუხედავად, სამსახურმა მითითებული პროცესი არ მიიჩნია სათანადოდ გამჭვირვალედ, ვინაიდან კომპანიის სხვადასხვა დოკუმენტში ფრაგმენტულად მითითებული ზოგადი ჩანაწერები ვერ უზრუნველყოფდა მონაცემთა სუბიექტებისთვის მათი ბიომეტრიული მონაცემების დამუშავების არსთან დაკავშირებული დეტალური ინფორმაციის ნათლად, მარტივ და მათთვის გასაგებ ენაზე მიწოდებას. ამდენად, კომპანიას დაევალა, სპორტდარბაზზე და გამოსაცვლელ ოთახებზე წვდომის კონტროლისა და კომპანიაში დასაქმებულ პირთა ცვლაში გამოცხადების აღრიცხვის მიზნით, დასაქმებულ პირთა ბიომეტრიული მონაცემების დამუშავების შეწყვეტა და, კანონის მე-4 მუხლით გათვალისწინებული პრინციპების შესაბამისად, ბიომეტრიულ მონაცემთა დამუშავების მიზნისა და მოცულობის, ამ მონაცემთა შენახვის ვადის, მათი შენახვისა და განადგურების წესისა და პირობების, აგრეთვე, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმების წერილობით განსაზღვრა.

ზ. საარჩევნო პროცესში მონაცემთა დამუშავების კანონიერება

2024 წლის 26 ოქტომბერს საქართველოს პარლამენტის არჩევნები ჩატარდა. სამსახურში არაერთი განცხადება თუ შეტყობინება იქნა წარმოდგენილი მონაცემთა სუბიექტების მიერ მათი მონაცემების დამუშავების კანონიერების შესწავლის მოთხოვნით. საქართველოს საარჩევნო კოდექსის შესაბამისად, პოლიტიკური პარტია არჩევნებში მონაწილეობისა და გამარჯვების მიზნით, უფლებამოსილია აწარმოოს წინასაარჩევნო კამპანია (აგიტაცია). მოქმედი კანონმდებლობის მიხედვით, მათ შორის მხარდაჭერის მიზნით, მონაცემთა სუბიექტისთვის/ამომრჩევლისთვის ინფორმაციის პირდაპირი და უშუალო მიწოდება, ტელეფონის, ფოსტის, ელექტრონული ფოსტის ან სხვა ელექტრონული საშუალების გამოყენებით, ექცევა პირდაპირი მარკეტინგის განმარტებაში, რომელიც შეიძლება იყოს წინასაარჩევნო კამპანიით (აგიტაციით) განსაზღვრულ ღონისძიებათა შემადგენელი კომპონენტი და აღნიშნული მიზნით მონაცემთა სუბიექტის/ამომრჩევლის მონაცემების დამუშავებისთვის დაცული უნდა იყოს

კანონის მე-12 მუხლით (მონაცემთა დამუშავება პირდაპირი მარკეტინგის მიზნით) დადგენილი მოთხოვნები.

საგულისხმოა, რომ მონაცემთა უკანონო დამუშავების პრევენციის მიზნით, სამსახურმა წინასაარჩევნო პერიოდში გაავრცელა განცხადება, რომლითაც დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირებს შეახსენა საარჩევნო პროცესში ამომრჩეველთა პერსონალური მონაცემების კანონიერად დამუშავების ვალდებულება. საანგარიშო პერიოდში განცხადების განხილვისა თუ შემოწმების (ინსპექტირების) ფარგლებში შესწავლილი საქმეებიდან გამომდინარე, გამოიკვეთა, რომ დამუშავებისთვის პასუხისმგებელი პირები (როგორც წესი, პოლიტიკური პარტიები) მონაცემთა სუბიექტების მონაცემებს ძირითადად ამუშავებდნენ კანონით გათვალისწინებული სამართლებრივი საფუძვლის გარეშე, ზოგიერთ შემთხვევაში კი გამოიკვეთა ამ პროცესში მარკეტინგული მიზნით მონაცემთა დამუშავების წესების დარღვევა. კერძოდ:

— წინასაარჩევნოდ, საარჩევნო კანონმდებლობით დადგენილ ვადებში, პოლიტიკური პარტიები სხვადასხვა საუბნო საარჩევნო კომისიაში საკუთარი კვოტით ნიშნავდნენ კომისიის წევრებს/მონაცემთა სუბიექტებს და ამუშავებდნენ მათ მონაცემებს, თუმცა არ ჰქონდათ მათი მონაცემების დამუშავების კანონით გათვალისწინებული საფუძვლები, ან ვერ უზრუნველყვეს ამ საფუძვლის არსებობის მტკიცების კანონით გათვალისწინებული ვალდებულების რეალიზება. კანონის მე-5 მუხლის მე-2 პუნქტი მონაცემთა სუბიექტის მონაცემების დამუშავების სამართლებრივი საფუძვლის არსებობის მტკიცების ტვირთს დამუშავებისთვის პასუხისმგებელ პირს აკისრებს. სამსახურის მიერ შესწავლილ შემთხვევებში პოლიტიკურმა პარტიებმა ვერ წარმოადგინეს ობიექტური მტკიცებულება, გარდა ზეპირი განმარტებისა, რომლითაც მონაცემთა სუბიექტების მონაცემების დამუშავებას დააფუძნებდნენ კანონის მე-5 მუხლის პირველი პუნქტით განსაზღვრულ მონაცემთა დამუშავების რომელიმე სამართლებრივ საფუძველს;

— ერთ-ერთმა პოლიტიკურმა პარტიამ რამდენიმე ათეულ მონაცემთა სუბიექტს ელექტრონული ფოსტის საშუალებით გაუგზავნა შეტყობინებები არჩევნებში მონაწილეობის თაობაზე. პარტიის წარმომადგენელი განმარტავდა, რომ აღნიშნული წარმოადგენდა საინფორმაციო შინაარსის შეტყობინებებს და მასზე სამსახურს არ უნდა გაევრცელებინა პირდაპირი მარკეტინგის მიზნით მონაცემების დამუშავების წესები. პირდაპირ მარკეტინგად მიიჩნევა როგორც საიმიჯო და სოციალური თემატიკისადმი ინტერესის ფორმირება, ასევე – მხარდაჭერის მიზნით ინფორმაციის მონაცემთა სუბიექტისთვის/ამომრჩევლისთვის მიწოდება. შესაბამისად, პოლიტიკურ პარტიას ჰქონდა ვალდებულება, კანონის მე-12 მუხლის მოთხოვნების დაცვით დაემუშავებინა მონაცემთა სუბიექტების მონაცემები;

— ზემოაღნიშნულ შემთხვევებში სამსახურმა მიიჩნია, რომ პოლიტიკური პარტიების მიერ კანონის მოთხოვნების დარღვევით განხორციელდა მონაცემთა სუბიექტების მონაცემების დამუშავება და გამოიყენა კანონით გათვალისწინებული შესაბამისი სანქციები.

თ. ჯანმრთელობის დაცვის სექტორში მონაცემების დამუშავება

კანონის მე-6 მუხლი განსაზღვრავს განსაკუთრებული კატეგორიის მონაცემების დამუშავების სპეციალურ საფუძვლებს. კანონმდებელმა მონაცემთა სივრციდან ექსპლიციტურად გამოყო მონაცემთა დაცვის უფლებაში მოაზრებული განსაკუთრებული კატეგორიის მონაცემები, რომელთა რეგულირების მიმართ განსხვავებული რეჟიმი დაადგინა.[18] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს 2011 წლის 28 დეკემბრის კანონისგან განსხვავებით, მოქმედი კანონით ახლებურად განისაზღვრა ჯანმრთელობასთან დაკავშირებული მონაცემის ცნება. კანონის მიხედვით, ჯანმრთელობასთან დაკავშირებული მონაცემი არის მონაცემთა სუბიექტის ფიზიკური ან ფსიქიკური ჯანმრთელობის შესახებ, აგრეთვე, ინფორმაცია მისთვის სამედიცინო მომსახურების გაწევის თაობაზე, თუ იგი მონაცემთა სუბიექტის ფიზიკური ან ფსიქიკური ჯანმრთელობის შესახებ ინფორმაციას იძლევა.

მონაცემთა სუბიექტის ჯანმრთელობის შესახებ ინფორმაცია, მისი სენსიტიური ხასიათიდან გამომდინარე, დაცვის მაღალ სტანდარტს ექვემდებარება. ჯანმრთელობის მდგომარეობის შესახებ მონაცემები შეიცავს ინტიმურ დეტალებს ინდივიდის ცხოვრების სტილის, ჩვევების, ფსიქიკური და ფიზიკური მდგომარეობის შესახებ. შესაძლოა, მათი უკანონო გამჟღავნება მნიშვნელოვანი ზიანის მომტანი იყოს პიროვნების პირადი და ოჯახური ცხოვრების, ასევე – დასაქმებისა და საზოგადოებაში ინტეგრირებისთვის. საანგარიშო პერიოდში გამოიკვეთა კანონმდებლობით ნაკისრი ვალდებულებების შეუსრულებლობის ან ნაკლოვანი შესრულების არაერთი ფაქტი, კერძოდ:

— გამოვლინდა შემთხვევები, როდესაც, სამედიცინო დაწესებულებებს არ ჰქონდათ მიღებული შესაბამისი ორგანიზაციულ-ტექნიკური ზომები მონაცემთა უსაფრთხოების დასაცავად. მაგალითად, ერთ-ერთი შემოწმების (ინსპექტირების) ფარგლებში დადგინდა, რომ კლინიკის ელექტრონული ფოსტიდან შეცდომით სხვა ელექტრონული ფოსტის მისამართზე არაუფლებამოსილ პირთან გაიგზავნა შეტყობინება, რომელიც შეიცავდა კლინიკის პაციენტების მონაცემებს, მათ შორის – ჯანმრთელობის მდგომარეობასთან დაკავშირებულ ინფორმაციას, რის მიზეზად კლინიკის წარმომადგენელმა მიუთითა უნებლიე, ადამიანურ შეცდომაზე, რაც განაპირობა ელექტრონული ფოსტის მისამართში ერთი ლათინური ასოს გამორჩენამ. შესაბამისად, ჯანმრთელობის მდგომარეობასთან დაკავშირებული ინფორმაცია, კლინიკის მიერ მონაცემთა უსაფრთხოებისათვის კანონით დადგენილი მოთხოვნების დარღვევით, არაუფლებამოსილი პირისათვის გამჟღავნების გზით დამუშავდა. შესაბამისად, კლინიკას დაეკისრა კანონით გათვალისწინებული სახდელი.

[18] საქართველოს საკონსტიტუციო სასამართლოს 2019 წლის 7 ივნისის №1/4/693,857 გადაწყვეტილება საქმეზე „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ“, II, §57.

მონაცემთა უსაფრთხოების უზრუნველყოფის მიზნებისთვის მნიშვნელოვანია, რომ სამედიცინო დაწესებულებებმა, როგორც დამუშავებისთვის პასუხისმგებელმა პირებმა, მიიღონ შესაბამისი ორგანიზაციულ-ტექნიკური ზომები, რომლებიც მაქსიმალურად შეზღუდავს მონაცემებზე არაუფლებამოსილი პირების წვდომის შესაძლებლობას კლინიკის მიერ მონაცემთა გამჟღავნებისა თუ დამუშავების სხვა სახის გამოყენების პროცესში;

— აქტუალურია ჯანმრთელობის დაცვის სექტორში მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემების სამართლებრივი საფუძვლის გარეშე დამუშავების პრობლემა. აუცილებელია, რომ სამედიცინო დაწესებულებამ (ზოგიერთ შემთხვევაში ექიმმა), როგორც დამუშავებისთვის პასუხისმგებელმა პირმა, მაქსიმალურად უზრუნველყოს მასთან დაცული განსაკუთრებული კატეგორიის მონაცემების უკანონოდ დამუშავების ნებისმიერი ფაქტის პრევენცია, რაც მნიშვნელოვან როლს ასრულებს მონაცემთა დაცვის უფლების პრაქტიკულ რეალიზებაში. სამსახურმა შეისწავლა ექიმის მიერ რამდენიმე მონაცემთა სუბიექტის განსაკუთრებული კატეგორიის მონაცემის (სამედიცინო მომსახურების მიღების შესახებ ინფორმაციის) სოციალურ ქსელ „Facebook“-ზე გამჟღავნების კანონიერება. შემოწმების (ინსპექტირების) ფარგლებში, ექიმის მიერ სამედიცინო მომსახურების გაწევის ფაქტი დადასტურდა მხოლოდ ერთი მონაცემთა სუბიექტის მიმართ, ხოლო დანარჩენ მონაცემთა სუბიექტებთან მიმართებით შესაბამისი მომსახურების გაწევის დამადასტურებელი მტკიცებულება სამსახურში არ ყოფილა წარმოდგენილი. ამასთან, ექიმის მიერ საჯაროდ ხელმისაწვდომი ფორმით ინფორმაციის განთავსება მონაცემთა სუბიექტების მიერ სამედიცინო მომსახურების მიღების შესახებ, აღქმადი იყო მესამე პირებისთვის, რომ მათ ნამდვილად მიიღეს ექიმის მომსახურება; სამედიცინო მომსახურების გაწევის თაობაზე ინფორმაცია წარმოადგენს განსაკუთრებული კატეგორიის მონაცემს. საგულისხმოა, რომ ექიმმა ვერ დაასახელა განსაკუთრებული კატეგორიის მონაცემების დამუშავების სამართლებრივი საფუძველი, შედეგად, მას კანონით გათვალისწინებული სახდელი შეეფარდა.

ი. საფინანსო სექტორში მონაცემების დამუშავება

საფინანსო სექტორი აერთიანებს კომერციულ ბანკებს, მიკროსაფინანსო ორგანიზაციებს, სესხის გამცემ სუბიექტებს, პრობლემური აქტივების მართვის კომპანიებს, რომლებიც ამუშავებენ, მათ შორის, ისეთ ინფორმაციას, როგორიცაა: მონაცემთა სუბიექტების მისამართები, სამუშაო ადგილი, ფინანსური ვალდებულებები და ტრანზაქციები, ნათესაური კავშირები. თანამედროვე ტექნოლოგიების განვითარებასთან ერთად, საფინანსო სექტორში ყოველწლიურად იზრდება მონაცემთა ახალი ელექტრონული ბაზების შექმნისა და მათი სხვადასხვა მიზნისთვის გამოყენების ფაქტები. ავტომატური საშუალებებით მონაცემთა

დამუშავების პროცესში იზრდება ხარვეზებისა და დარღვევების არსებობის რისკები. სამსახურისთვის საფინანსო სექტორში მონაცემების დაცვა საანგარიშო პერიოდში მნიშვნელოვანი გამოწვევა იყო. ამ მიმართულებით დადგინდა კანონმდებლობით ნაკისრი ვალდებულებების შეუსრულებლობის ან ნაკლოვანი შესრულების არაერთი ფაქტი:

— გამოვლინდა საფინანსო სექტორის მიერ მსესხებლის მოძიების მიზნით მესამე პირებთან დაკავშირების და მონაცემების გამჟღავნების ფაქტები – ამ თვალსაზრისით აღსანიშნავია, რომ საფინანსო სექტორმა მხოლოდ აუცილებლობის შემთხვევაში უნდა განახორციელოს მსგავსი ქმედებები, ვინაიდან მესამე პირებთან დაკავშირება და მათთვის იმ ინფორმაციის მიწოდება, თუ რა მიზნით (მაგალითად, მსესხებლის მოძიების მიზნით) უკავშირდებიან, თავისთავად გულისხმობს მსესხებლის მონაცემების შემცველი ინფორმაციის გამჟღავნებას. შესაბამისად, საფინანსო სექტორის წარმომადგენლებმა მსესხებელთან დაკავშირება მათთვის ცნობილი მისი საკონტაქტო მონაცემების გამოყენებით უნდა სცადონ და მხოლოდ ამ მეთოდით, მსესხებლის მოძიების მიზნით, შესაბამისი მიზნის მიუღწევლობის შემთხვევაში დაუკავშირდნენ მესამე პირებს;
— ასევე, გამოვლინდა მსესხებლების მოძიების მიზნით, მესამე პირებთან, მათი წინააღმდეგობის მიუხედავად, კვლავ დაკავშირების ფაქტები – თუ საფინანსო სექტორის წარმომადგენელი, კონკრეტული პირის მოძიების მიზნით, მესამე პირთან ამყარებს კომუნიკაციას, რომელიც უარს აცხადებს თანამშრომლობაზე და ითხოვს საკუთარი მონაცემების დამუშავების შეწყვეტას, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, შეწყვიტოს და აღნიშნული მიზნით აღარ დაამუშაოს მესამე პირის მონაცემი;
— საფინანსო სექტორის წარმომადგენლებმა გარკვეულ შემთხვევებში ვერ უზრუნველყვეს ობიექტური მტკიცებულებების წარმოდგენა მონაცემთა სუბიექტების მონაცემების მოპოვების წყაროსთან დაკავშირებით. ვინაიდან მონაცემთა დამუშავების სამართლებრივი საფუძვლის დასაბუთების ვალდებულება ეკისრება დამუშავებისთვის პასუხისმგებელ პირს, სამსახურმა არ გაითვალისწინა მათი ზეპირი განმარტებები მსესხებლის მოძიების მიზნით მესამე პირთან დაკავშირების კანონშესაბამისობის თაობაზე;
— სამსახურმა შეისწავლა ერთ-ერთი ბანკის მიერ კლიენტებისთვის სადებეტო ბარათების დაულუქავი ფორმით გადაცემის საკითხი და დაადგინა, რომ ზემოაღნიშნულ პროცესში, სერვისცენტრის თანამშრომლებისთვის ბარათებზე დატანილი ინფორმაციის (მაგალითად, პირის სახელი, გვარი, ბარათის ნომერი) სრული და პირდაპირი ხელმისაწვდომობით, ბანკის მიერ სათანადოდ არ იყო უზრუნველყოფილი მონაცემთა უსაფრთხოების დაცვა. რაც უფრო მეტ პირს აქვს მონაცემებზე წვდომის შესაძლებლობა, მით უფრო იზრდება მათი (განსახილველ შემთხვევაში, საბანკო ბარათების მონაცემების) შემთხვევითი ან განზრახი უკანონო დამუშავების (მაგალითად, ბანკის თანამშრომლის მიერ ფოტოგადაღების/დამახსოვრების და შემდგომში მართლსაწინააღმდეგო გამოყენების) რისკები. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მიიღოს ისეთი

ორგანიზაციული და ტექნიკური ზომები, რომლებიც აღმოფხვრის მომხმარებელთა მონაცემებისადმი არამართლზომიერი მოპყრობის რისკებს. ამ თვალსაზრისით, სამსახურმა განმარტა, რომ დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მინიმუმამდე შეამციროს მონაცემებზე წვდომის შესაძლებლობის მქონე პირთა წრე და მონაცემებზე დაშვება უზრუნველყოს მხოლოდ სათანადო აუცილებლობის პირობებში. ამდენად, ბანკი ცნობილ იქნა სამართალდამრღვევად და დაევალა ახალი სადებეტო ბარათების კლიენტებისთვის გადაცემის პროცესის იმგვარად ორგანიზება, რომ ბარათებზე დატანილი მონაცემები ხელმისაწვდომი არ გამხდარიყო ბანკის სერვისცენტრების თანამშრომლებისთვის;

— ერთ-ერთი ბანკის შემოწმების ფარგლებში დადგინდა, რომ ეროვნული ბანკის პრეზიდენტის ბრძანებით დადგენილი მოთხოვნის შესაბამისად, ახორციელებდა უზრუნველყოფის საშუალებად გამოყენებული უძრავი ნივთის მესაკუთრის ინფორმირებას იმ საკრედიტო ხელშეკრულების დეტალების თაობაზე, რომლის უზრუნველყოფის საშუალებადაც იყო გამოყენებული კონკრეტული უძრავი ნივთი. ეროვნული ბანკის პრეზიდენტის ბრძანების თანახმად, აღნიშნული ინფორმაციის მიწოდებისთვის ბანკს განსაზღვრული აქვს 5 სამუშაო დღე, ხოლო, ბანკში დანერგილი პროცედურის შესაბამისად, ბანკი უძრავი ქონების მესაკუთრის ინფორმირებას ახდენს კრედიტის გაცემის მე-2 დღეს. სამსახურში მიმდინარე განხილვის შემთხვევაში, მსესხებელმა ბანკიდან კრედიტის სახით აღებული თანხით, კრედიტის გაცემის დღესვე შეიძინა უძრავი ქონება, ხოლო მესამე პირს, რომელიც საჯარო რეესტრში მიმდინარე სარეგისტრაციო წარმოების ვადების გათვალისწინებით ჯერ კიდევ ფიქსირდებოდა უძრავი ქონების მესაკუთრედ, ბანკმა გაუგზავნა დეტალური ინფორმაცია მსესხებელთან დადებული ხელშეკრულების პირობების შესახებ. სამსახურმა განმარტა, რომ ბანკს, საქმეში არსებული სპეციფიკური ფაქტობრივი გარემოებების გათვალისწინებით, შესაძლებლობა ჰქონდა, შეეფასებინა კონკრეტული სახელშეკრულებო ურთიერთობის ხასიათი, მიზანი და განმცხადებლის მონაცემთა დამუშავების პროცესში არ გამოეყენებინა მსგავსი პროცედურისათვის ბანკის მიერ დადგენილი ზოგადი სტანდარტი. ამასთან, ბანკს გადაწყვეტილება უნდა მიეღო არა მხოლოდ უზრუნველყოფის საგნის მესაკუთრის ან მსესხებლის (მონაცემთა სუბიექტის) ინტერესების რეალიზებისათვის უპირატესობის მინიჭებით, არამედ მათი ინტერესების დაბალანსებით. ბანკს უზრუნველყოფის საგნის მესაკუთრისთვის იმ შემთხვევაში უნდა გაემჟღავნებინა ინფორმაცია, თუ იგი ბანკისთვის ცნობილი სარეგისტრაციო წარმოებისთვის სტანდარტულად გათვალისწინებული ვადის ამოწურვის შემდგომაც იქნებოდა უზრუნველყოფის საგნის მესაკუთრე. ამგვარად, შესაძლებელი იქნებოდა როგორც მსესხებლის მონაცემების დამუშავების მიმართ კანონით დადგენილი პრინციპების დაცვა, ისე – ბანკისთვის დაკისრებული ვალდებულებების შესრულება. ამდენად, სამსახურმა დაადგინა, რომ ბანკს ჰქონდა შესაძლებლობა, საჯარო რეესტრში სარეგისტრაციო წარმოებისთვის

სტანდარტულად გათვალისწინებული ვადის ამოწურვის შემდგომ გადაემოწმებინა რეესტრის ამონაწერში მესაკუთრის ცვლილების ფაქტი და მხოლოდ აღნიშნულის შემდგომ შეეფასებინა და გადაეწყვიტა, რამდენად ჰქონდა მას ვალდებულება უზრუნველყოფის საგნის მესაკუთრესთან მიმართებით.

2.2. პრეცედენტული გადაწყვეტილებები

ა. გამჭვირვალობის პრინციპი

სამსახურს განცხადებით მომართა ფიზიკურმა პირმა და მოითხოვა ერთ-ერთი კომპანიის მიერ მისი მონაცემების დამუშავების კანონიერების შესწავლა და ინფორმირების წესების დარღვევაზე რეაგირება.

განმცხადებლის განმარტებით, მან კომპანიისაგან მოითხოვა საკუთარი მონაცემების (მათ შორის – საკრედიტო „რეპორტისა“ და საკრედიტო ქულის) დამუშავების თაობაზე კანონის მე-13 მუხლით განსაზღვრული ინფორმაცია, რაც კომპანიამ სრულყოფილად არ მიაწოდა.

კომპანიის წარმომადგენელმა საქმისწარმოების ფარგლებში განმარტა, რომ კომპანია მონაცემთა სუბიექტს აწვდიდა ინფორმაციას მის მიერ კომპანიისგან საკრედიტო „რეპორტის“ ან/და საკრედიტო ქულის შესახებ ინფორმაციის გამოთხოვის შესაძლებლობის თაობაზე. აღნიშნული მოთხოვნა კომპანიას შეიძლება წარედგინოს როგორც წერილობით, ისე – ზეპირად, სათანადო იდენტიფიკაციის/ვერიფიკაციის პროცედურის გავლის საფუძველზე, ელექტრონული ფოსტის ან ფოსტის საშუალებით გაგზავნილი განცხადებით, ასევე, ტელეფონით ან კომპანიის პორტალის საშუალებით. კომპანიის წარმომადგენლის განმარტებით, ზემოაღნიშნული ინფორმაციის მიღების გზების თაობაზე მონაცემთა სუბიექტს შეუძლია ნებისმიერი ინფორმაცია მიიღოს კომპანიის ვებგვერდების მეშვეობით ან კომპანიის მიერ პორტალის საშუალებით. საკრედიტო „რეპორტის“ და საკრედიტო ქულის შესახებ ინფორმაციის გაცემისათვის დადგენილია შესაბამისი საფასური (საკრედიტო „რეპორტთან“ დაკავშირებით, საქართველოს ეროვნული ბანკის რეგულაციიდან გამომდინარე, მოქმედებს კომპანიის მიერ მონაცემთა სუბიექტისათვის წელიწადში სამჯერ უფასოდ გაცემის ვალდებულება). თუ მონაცემთა სუბიექტი წერილობით, ზეპირად, სატელეფონო კომუნიკაციის, ელექტრონული ფოსტის ან ფოსტის საშუალებით მიმართავს კომპანიას და მოითხოვს მისი საკრედიტო ისტორიის (საკრედიტო „რეპორტის“) შესახებ ინფორმაციასა და საკრედიტო ქულას, კომპანია იმოქმედებს კანონის მე-13 მუხლის შესაბამისად და დაინტერესებულ პირს ყოველგვარი საფასურის გარეშე მიაწვდის მოთხოვნილ ინფორმაციას.

განცხადების განხილვის ფარგლებში დადგინდა, რომ ერთმანეთთან თანხვედრაში არ იყო კომპანიის წარმომადგენლის განმარტება, კომპანიისაგან ინფორმაციის გამოთხოვის, მონაცემთა სუბიექტისათვის განკუთვნილი

საშუალებების შესახებ და ვებგვერდზე არსებული ინფორმაცია. ერთი მხრივ, კომპანიის წარმომადგენელი განმარტების სახით მიუთითებდა კომპანიისაგან ინფორმაციის (მათ შორის – საკრედიტო „რეპორტის“ და საკრედიტო ქულის შესახებ) გამოთხოვის საშუალებებზე, მაგრამ, მეორე მხრივ, ვებგვერდზე არსებული ინფორმაცია ეხებოდა „პრეტენზიების ეფექტურ და დროულ მართვას“, კომპანიის „საქმიანობაში არსებული ხარვეზების გამოვლენას“ და „მომხმარებლის უფლებას, დააფიქსიროს პრეტენზია“ სხვადასხვა ფორმით. მსგავს შემთხვევებში, ერთია მონაცემთა სუბიექტის მიერ კომპანიისაგან ინფორმაციის მოთხოვნა, ხოლო მეორეა, ამავე სუბიექტის მიერ პრეტენზიის, უკმაყოფილების დაფიქსირება კომპანიის მიერ განხორციელებულ ქმედებაზე. აქედან გამომდინარე, სამსახურმა მიიჩნია, რომ მონაცემთა სუბიექტისათვის პრეტენზიის რეალიზების გზების შესახებ მისთვის ინფორმაციის მიწოდება ვერ ჩაითვლებოდა მის შესახებ მონაცემების გამოთხოვის გზების შესახებ ინფორმაციის მიწოდებად.

ამასთან, კომპანიის პორტალსა და ვებგვერდზე არ იყო განთავსებული ინფორმაცია, რომლითაც დადასტურდებოდა მონაცემთა სუბიექტის კომპანიის მიერ ინფორმირებულობა. აღნიშნულის დამადასტურებელი მტკიცებულებები არც კომპანიის წარმომადგენელს მოუწოდებია, გარდა განმარტებისა. როგორც კომპანიის ვებგვერდზე, ასევე პორტალზე დომინირებდა ინფორმაცია პორტალის საშუალებით უფასო და ფასიანი პაკეტებით სარგებლობის, საკრედიტო „რეპორტის“ და საკრედიტო ქულის შესახებ ინფორმაციის მიღების თაობაზე და ა. შ. კომპანია საჯაროდ არ უზრუნველყოფდა მონაცემთა სუბიექტის ინფორმირებას იმის თაობაზე, რომ არსებობდა პორტალის საშუალებით შეთავაზებული ფასიანი პაკეტით გათვალისწინებული სერვისის უფასოდ მიღების შესაძლებლობის ალტერნატიული გზები; მონაცემთა სუბიექტისათვის კანონით მინიჭებული უფლებების რეალიზებისათვის კი მნიშვნელოვანია კომპანიის მიერ მისი ინფორმირება, რათა სუბიექტმა გააზრებული გადაწყვეტილება მიიღოს საკუთარი მონაცემების შესახებ ინფორმაციის გამოთხოვის თაობაზე.

გარდა მონაცემთა სუბიექტისათვის მისაწოდებელი ინფორმაციის შინაარსისა, მნიშვნელოვანია ინფორმაციის მიწოდების ფორმა. ხშირ შემთხვევაში, ასეთ ინფორმაციას შეიცავს დოკუმენტები, რომლებსაც უწოდებენ მონაცემთა დაცვის შესახებ შეტყობინებას, კონფიდენციალურობის პოლიტიკას და ა. შ. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ არ ითვალისწინებს ამ ინფორმაციის მონაცემთა სუბიექტისათვის მიწოდების კონკრეტულ ფორმატს, თუმცა მასში მკაფიოდ არის მითითებული, რომ დამუშავებისათვის პასუხისმგებელ პირს ევალება „სათანადო ზომების“ მიღება გამჭვირვალობისთვის საჭირო ინფორმაციის უზრუნველყოფის კუთხით. კერძოდ, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს მონაცემთა დამუშავებასთან დაკავშირებული ყველა გარემოება და ისე მიიღოს გადაწყვეტილება მონაცემთა სუბიექტისათვის ინფორმაციის შესაფერისი ფორმატით მიწოდების უზრუნველყოფის თაობაზე. შესაბამისად, სამსახურმა მიიჩნია, რომ კომპანიის მიერ მონაცემთა სუბიექტისათვის ინფორმაციის საფასურის გადახდის გარეშე მიღების მექანიზმის არსებობა, სუბიექტის ინფორმირების გარეშე, ზღუდავდა გამჭვირვალობის პრინციპის პრაქტიკულ ქმედითობას და ხელს უშლიდა მონაცემთა დაცვის უფლების რეალიზებას.

გამჭვირვალობის პრინციპის თანახმად, დამუშავებისათვის პასუხისმგებელი პირი ვალდებულია, რომ მონაცემთა სუბიექტისათვის განკუთვნილი ინფორმაცია შეიმუშაოს „გასაგებად“, რაც ნიშნავს, რომ ინფორმაციის გაგება უნდა შეეძლოს სამიზნე აუდიტორიის „საშუალო“ სტატისტიკურ წევრს, ხოლო აღნიშნული მჭიდროდ უკავშირდება მკაფიო და მარტივი ენის გამოყენების მოთხოვნას.

განცხადების განხილვის ფარგლებში, სამსახურმა დაადგინა, რომ კომპანიის მიერ მონაცემთა დამუშავების პროცესში მონაცემთა სუბიექტებისათვის არ იყო უზრუნველყოფილი გამჭვირვალობის პრინციპის მოთხოვნები, რაც ეწინააღმდეგებოდა კანონის მე-4 მუხლით დადგენილ წესს და წარმოადგენდა 66-ე მუხლით გათვალისწინებულ ადმინისტრაციულ სამართალდარღვევასა და ადმინისტრაციული პასუხისმგებლობის დაკისრების საფუძველს. დამატებით, კომპანიას შესასრულებლად მიეცა სავალდებულო დავალებები.

ერთ-ერთი საქმის განხილვის დროს დადგინდა, რომ კომპანიის მიერ მიღებული შიდაორგანიზაციული დოკუმენტები და კომპანიასა და დასაქმებულს შორის დადებული შრომითი ხელშეკრულება არ შეიცავდა ინფორმაციას კომპანიის მხრიდან თანამშრომლის სამსახურებრივი ელექტრონული ფოსტის შესაძლო კონტროლის/წვდომის, თანამშრომლის სამსახურიდან გათავისუფლების შემთხვევაში, სამსახურებრივი ელექტრონული ფოსტის გამოყენების, მასზე არსებული ინფორმაციის შენახვისა და შენახვის ხანგრძლივობის შესახებ. შესაბამისად, კომპანიის მიერ ზემოაღნიშნული დოკუმენტაციის განმცხადებლისათვის გაცნობის შემთხვევაში, კომპანია ვერ უზრუნველყოფდა კანონის მე-4 მუხლით განსაზღვრული გამჭვირვალობის პრინციპის მოთხოვნების რეალიზებას. კომპანიის წარმომადგენლის განმარტება, განმცხადებლის ზეპირი ინფორმირების თაობაზე, ვერ იქნებოდა მიჩნეული კანონის მე-4 მუხლის მე-7 პუნქტის მიზნებისათვის გათვალისწინებულ ობიექტურ მტკიცებულებად, რაც დაადასტურებდა კომპანიის, როგორც დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დამუშავებისას კანონით განსაზღვრული პრინციპების (მათ შორის, გამჭვირვალობის პრინციპის) დაცვის და მათთან შესაბამისობის დასაბუთების კანონისმიერი ვალდებულების შესრულების ფაქტს. სამსახურმა მიიჩნია, რომ კომპანიის მიერ მონაცემთა დამუშავების პროცესში მონაცემთა სუბიექტისათვის არ იყო უზრუნველყოფილი გამჭვირვალობის პრინციპის მოთხოვნები და დაევალა წესების შემუშავება, რომლებითაც კომპანიის თანამშრომლები ინფორმირებულნი იქნებიან სამსახურებრივი ელექტრონული ფოსტის კომპანიის მხრიდან შესაძლო კონტროლის/წვდომის, თანამშრომლის სამსახურიდან გათავისუფლების შემთხვევაში, სამსახურებრივი ელექტრონული ფოსტის გამოყენების, მასზე არსებული ინფორმაციის შენახვისა და შენახვის ხანგრძლივობის შესახებ.

სამსახურმა შეისწავლა საქმე, რომელიც ეხებოდა სამედიცინო დაწესებულების მიერ გარდაცვლილი პირის მონაცემების გაცემის გზით დამუშავებას. სამედიცინო დაწესებულების წარმომადგენელმა განმარტა, რომ არ ევალებოდათ მონაცემთა სუბიექტის ან მონაცემთა სუბიექტის მშობლის, შვილის, შვილიშვილის ან მეუღლის ინფორმირება პირის გარდაცვალების შემთხვევაში მონაცემების დამუშავების აკრძალვის უფლების შესახებ. შესაბამისად, ვინაიდან დაწესებულებაში არ მოიპოვებოდა აკრძალვის შესახებ ინფორმაცია, მათ

დასაშვებად მიიჩნიეს მესამე პირზე ინფორმაციის გაცემა. მონაცემთა დამუშავების პროცესში კანონის მე-4 მუხლით განსაზღვრული პრინციპები და კონკრეტულად, გამჭვირვალობის პრინციპი, არა მხოლოდ ნორმატიულად მბოჭავ ელემენტს წარმოადგენს, რომლითაც იზღუდება დამუშავებისათვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირის მოქმედების ფარგლები, არამედ კანონის ნორმების განმარტების ფუნქციითაც არის აღჭურვილი. შესაბამისად, სამსახურმა მიიჩნია, რომ კანონის მე-8 მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტში უშუალოდ არ არის რა მითითებული მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მხრიდან განსახორციელებელი ზემოაღნიშნული ინფორმირების ვალდებულების თაობაზე, თუმცა დასახელებული ნორმის გამჭვირვალობის პრინციპის საშუალებით განმარტებისას საფუძველს მოკლებული იქნებოდა ნორმის შინაარსობრივი იდეა - პირის გარდაცვალების შემდეგ მისი მონაცემების დაცვის შესახებ.

ბ. გამჭვირვალობის პრინციპი და მონაცემთა უსაფრთხოების დაცვა

სამსახურს განცხადებით მომართა ფიზიკურმა პირმა და მოითხოვა ტაქსის გამოძახების ერთ-ერთი სერვისის პროვაიდერი კომპანიის მიერ მათი აპლიკაციის მეშვეობით განცხადების ავტორის მონაცემების დამუშავების კანონიერების შესწავლა.

საქმის შესწავლის ფარგლებში დადგინდა, რომ განმცხადებელი დარეგისტრირებული იყო აპლიკაციაში, როგორც „შემკვეთი“. მისი პირადი ანგარიშის გვერდზე მითითებული იყო შემდეგი მონაცემები: სახელი, გვარი, სქესი, ტელეფონის ნომერი, დაბადების თარიღი და ელექტრონული ფოსტის მისამართი. განმცხადებელმა აპლიკაციის ე. წ. შიდა „ჩატის“ მეშვეობით მოითხოვა საკუთარი ანგარიშის და მონაცემების წაშლა. ამ მოთხოვნის პასუხად კომპანიის წარმომადგენელმა განმცხადებელს განუმარტა, რომ მობილური ტელეფონიდან წაეშალა აპლიკაცია, რომლის საშუალებით ანგარიში გაუქმდებოდა.

ზემოაღნიშნულ პასუხთან ერთად, კომპანიამ საკუთარი ბაზიდან წაშლა მონაცემები, თუმცა განმცხადებლის მობილურ აპლიკაციაში კვლავ იყო შენახული სატელეფონო ნომერი და სქესი. ამასთან, მას კვლავ შეეძლო აპლიკაციით და, შესაბამისად, ტაქსის სერვისით სარგებლობა. კომპანიამ სამსახურს განუმარტა, რომ აღნიშნული განპირობებული იყო განმცხადებლის სატელეფონო ნომრის ან/და აპლიკაციის მიერ „cache“ ფაილების შენახვით. კომპანიამ ასევე განმარტა, რომ ასეთ შემთხვევაში მონაცემები მათ მიერ აღარ მუშავდებოდა (წაშლილი იყო მონაცემთა ბაზიდან), თუმცა მობილურ ტელეფონში არსებული „cache“ ფაილების წასაშლელად აუცილებელი იყო მობილური ტელეფონიდან აპლიკაციის წაშლა ან ანგარიშიდან გასვლა ე. წ. „Log out“-ის ფუნქციის გამოყენებით. კომპანიამ, ნაცვლად მოცემული პროცედურის შესახებ ინფორმაციის მიწოდებისა, განმცხადებელს ე.წ. შიდა „ჩატის“ მეშვეობით განუმარტა, რომ ანგარიში აპლიკაციის წაშლის შემთხვევაში გაუქმდებოდა, თუმცა იმის გათვალისწინებით, რომ აპლიკაციაში „cache“ ფაილის სახით დარჩა მონაცემები, განმცხადებლისთვის არ იყო აღქმადი,

ნამდვილად წაშალა თუ არა კომპანიამ მისი მონაცემები. გარდა ამისა, ზემოაღნიშნული პროცედურის შესახებ კომპანიის კონფიდენციალურობის პოლიტიკაში რაიმე სახის ინფორმაცია არ იყო მითითებული.

განხილვის ფარგლებში დადგინდა, რომ კომპანიის ვებგვერდის მეშვეობით რეგისტრაციისას სავალდებულოდ შესავსები იყო ინფორმაცია, რომელიც კომპანიის კონფიდენციალურობის პოლიტიკის თანახმად ასეთად არ მიიჩნეოდა. გარდა ამისა, კომპანიის მონაცემთა ბაზის (რომელშიც გაერთიანებული იყო აპლიკაციაში რეგისტრირებული მომხმარებლების მონაცემები) შემოწმებისას დადგინდა, რომ მას არ გააჩნდა მონაცემთა მიმართ შესრულებული ყველა მოქმედების აღრიცხვის ელექტრონული ჟურნალი (ე. წ. „ლოგირება“), რომლითაც შესაძლებელი იქნებოდა განმცხადებლის მონაცემების/ანგარიშის წაშლის ზუსტი დროის განსაზღვრა.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, კომპანიას დაეკისრა ადმინისტრაციული პასუხისმგებლობა, ერთი მხრივ, მონაცემთა დამუშავების პროცესში გამჭვირვალობის პრინციპის, ხოლო, მეორე მხრივ, უსაფრთხოების მოთხოვნების დარღვევისათვის. ამასთან, კომპანიას დაევალა, მონაცემთა სუბიექტებისათვის, გამჭვირვალობის პრინციპის მოთხოვნების დაცვით, მიეწოდებინა ინფორმაცია რეგისტრაციისას სავალდებულოდ/ნებაყოფლობით მისათითებელი მონაცემების, ხოლო, ანგარიშის გაუქმების/მონაცემთა წაშლის მოთხოვნისას, სრული და ზუსტი ინსტრუქცია შესაბამისი პროცედურის შესახებ. გარდა ამისა, უსაფრთხოების კუთხით კომპანიას დაევალა ისეთი სისტემის დანერგვა, რომლითაც შესაძლებელი იქნებოდა მონაცემთა ბაზაში ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა.

გ. მონაცემთა უსაფრთხოება

სამსახურს შეტყობინებით მომართა ფიზიკურმა პირმა და მოითხოვა ერთ-ერთი ბანკის მიერ შეტყობინების ავტორის სატელეფონო ნომერზე მოკლეტექსტური შეტყობინებების გაგზავნის გზით მესამე პირების მონაცემების გამჟღავნების კანონიერების შესწავლა.

შემოწმების (ინსპექტირების) ფარგლებში დადგინდა, რომ შეტყობინების ავტორმა ბანკის სახელით თავის მფლობელობაში არსებულ სატელეფონო ნომერზე მიიღო მოკლეტექსტური შეტყობინებები, რომლებიც შეიცავდა მესამე პირების/ბანკის მომხმარებლების მონაცემებს (სახელს, გვარს, პირად ნომერს, განვადების განაცხადის ნომერს, განაცხადის ცვლილებების/დამტკიცებისა და განაცხადის გაუქმების შესახებ ინფორმაციას).

ბანკის წარმომადგენელმა აღიარა, რომ ბანკის მოქმედი თანამშრომლის (სესხის ოფიცრის) სატელეფონო ნომერზე გასაგზავნი მესამე პირების/ბანკის მომხმარებლების მონაცემების შემცველი მოკლეტექსტური შეტყობინებები, კონკრეტული პერიოდის განმავლობაში, იგზავნებოდა მონაცემებზე წვდომისთვის არაუფლებამოსილი პირის, ბანკის ყოფილი თანამშრომლის სატელეფონო ნომერზე (ბანკის მოქმედი და ყოფილი თანამშრომლების სახელი და გვარი იყო ერთი და

იგივე), რის მიზეზად დაასახელა ბანკის სისტემური მხარდაჭერის ოფიცრის უნებლიე, ადამიანური შეცდომა. მისი ინფორმაციით, ბანკი საქმიანობის პროცესში, შიდაორგანიზაციული მიზნებისათვის, იყენებდა პროგრამას (შემდგომ - პროგრამა), რომელიც მათ შორის დაკავშირებული იყო ბანკის ე. წ. „HR“ ბაზასთან. პროგრამა იძლეოდა სესხის ოფიცრებისათვის უნიკალური ოთხნიშნა კოდის მინიჭების, მათი დამატების, ცვლილების, წაშლის და სხვა მოქმედებების შესაძლებლობას. პროგრამაში სესხის ოფიცრის დამატების პროცესში ბანკის ე. წ. „HR“ ბაზიდან სესხის ოფიცრის ძიება ხორციელდებოდა მხოლოდ სახელისა და გვარის (ლათინური ასოებით) მითითებით, რის შემდეგაც ძიების განმახორციელებელი პირისათვის ხელმისაწვდომი ხდებოდა საძიებო პირის სხვა მაიდენტიფიცირებელი მონაცემები.

შემოწმების (ინსპექტირების) ფარგლებში სამსახურმა განმარტა, რომ კანონი ადგენს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, მიიღოს ისეთი ორგანიზაციულ-ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო გამჟღავნებისაგან. შესაბამისად, კანონმა იმპერატიულად განსაზღვრა ბანკის, როგორც დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემების დამუშავების უსაფრთხოებისათვის კანონით დადგენილი აუცილებელი მოთხოვნები. ზოგადად, განხორციელებულ ქმედებასა და დამდგარ შედეგს შორის ნებისმიერ შემთხვევაში უნდა არსებობდეს პირდაპირი და არა სავარაუდო მიზეზობრივი კავშირი, რამდენადაც სავარაუდო კავშირი საკმარის ობიექტურ საფუძვლად ვერ გამოდგება სამართლებრივი პასუხისმგებლობისთვის. ბანკს მოცემულ შემთხვევაში რომ მიეღო კანონით განსაზღვრული მონაცემთა უსაფრთხოების ტექნიკური ზომები, არ მოხდებოდა მის მიერ დროის კონკრეტულ პერიოდში არაუფლებამოსილი პირის, შეტყობინების ავტორის მფლობელობაში არსებულ სატელეფონო ნომერზე მოკლეტექსტური შეტყობინებების გაგზავნა, რომელთა საშუალებითაც გამჟღავნდა მესამე პირების/ბანკის მომხმარებლების მონაცემები. დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა დამუშავების პროცესში საქმიანობა იმგვარად უნდა განახორციელოს, რომ დაიცვას მონაცემთა დამუშავების უსაფრთხოების ზომები და მონაცემთა სუბიექტის უფლებები. შეცდომისგან დაცვის ტექნიკური მექანიზმი ბანკს შემუშავებული არ ჰქონდა, კერძოდ, ბანკის მიერ სესხის ოფიცრის პროგრამაში დამატების მიზნით, არსებული მეთოდით ბანკის ე. წ. „HR“ ბაზაში სესხის ოფიცრის მხოლოდ სახელითა და გვარით მოძიება ქმნიდა ადამიანური შეცდომის დაშვებისა და, შესაბამისად, მონაცემთა გამჟღავნების რისკს, რამაც, განსახილველ შემთხვევაში, გამოიწვია ბანკის მომხმარებლების/მესამე პირების მონაცემების არაუფლებამოსილი პირისათვის გამჟღავნება. აღნიშნულის გათვალისწინებით, ბანკს დაევალა, მიეღო ისეთი ორგანიზაციულ-ტექნიკური ზომები, რომელთა განხორციელების შედეგად პროგრამის მეშვეობით ბანკის ე. წ. „HR“ ბაზიდან სესხის ოფიცრის მონაცემების მოძიება მხოლოდ პირის უნიკალური მაიდენტიფიცირებელი მონაცემით იქნებოდა შესაძლებელი.

დ. მონაცემთა სუბიექტის ხელმისაწვდომობა საკუთარ მონაცემებზე

სამსახურს მონაცემთა სუბიექტმა მომართა განცხადებით და მოითხოვა ერთ-ერთი კომპანიისთვის საკუთარი მონაცემების შემცველი დოკუმენტაციის გადაცემის დავალების შესრულება. განცხადების განხილვის ფარგლებში დადგინდა, რომ სამსახურში გადაადგილებისას განმცხადებელს ფეხი აუცურდა და დაეცა, რაც შენობაში განთავსებული ვიდეომონიტორინგის სისტემის ჩანაწერებში დაფიქსირდა. განმცხადებელმა მიმართა დამსაქმებელს და მოითხოვა თავისი მონაცემების შემცველი რამდენიმე დოკუმენტის, მათ შორის – ზემოაღნიშნული ფაქტის ამსახველი კონკრეტული ვიდეოჩანაწერების გადაცემა. დამსაქმებელმა განმცხადებელს მიაწოდა გამოთხოვილი დოკუმენტები, თუმცა არ გადასცა მისი მონაცემების შემცველი ვიდეოჩანაწერების ასლები. კომპანიის წარმომადგენელმა განმარტა, რომ კომპანია მოკლებული იყო შესაძლებლობას, გადაეცა განმცხადებლისთვის მის მიერ გამოთხოვილი ვიდეოჩანაწერები, რადგან ისინი კომპანიაში დასაქმებული სხვა პირების მონაცემებსაც შეიცავდა (აღნიშნული ფაქტი განცხადების განხილვის ფარგლებში დადასტურდა), ხოლო კომპანიას არ ჰქონდა ვიდეოჩანაწერების იმგვარად დამუშავების შესაძლებლობა, რომ მოეხდინა მასში ასახული მესამე პირების მონაცემების დეპერსონალიზაცია (მაგალითად, გამოსახულებების ე. წ. „დაბლარვა“).

განსახილველ შემთხვევაში, სამსახურმა განმარტა, რომ მონაცემების შემცველი დოკუმენტების/ჩანაწერების ასლები უნდა გაიცეს იმგვარად, რომ მონაცემთა სუბიექტის მოთხოვნის დაკმაყოფილების მიუხედავად, არათანაზომიერად არ შეიზღუდოს სხვათა უფლებები. განმცხადებლის მონაცემების შემცველი ვიდეოჩანაწერების მისთვის იმ ფორმით გადაცემა, რომ შესაძლებელი ყოფილიყო ვიდეოჩანაწერებში ასახული მესამე პირების იდენტიფიცირება, სხვა პირთა მონაცემების განუსაზღვრელი ვადით განმცხადებლის მფლობელობაში გადასვლას გამოიწვევდა. დამატებით, შექმნიდა აღნიშნული მონაცემების შემდგომში სხვა პირებისთვის ან/და პირთა განუსაზღვრელი წრისადმი (მაგალითად, სოციალური ქსელის მეშვეობით) გავრცელების რისკს, რასაც შესაძლოა გამოეწვია ჩანაწერებში ასახულ მესამე პირთა უფლებების არათანაზომიერი შეზღუდვა.

დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მიიღოს ყველა საჭირო ტექნიკური და ორგანიზაციული ზომა საკუთარი მონაცემების შემცველი მასალების მომთხოვნი მონაცემთა სუბიექტისა და მესამე პირების ინტერესების დაბალანსებისთვის. მაგალითად, სუბიექტს შეიძლება მიეწოდოს ვიდეოჩანაწერები იმ ფორმით, რომ მათში დაიფაროს კადრში მოხვედრილი მესამე პირების გამოსახულება. თუ ვიდეოჩანაწერი შეიცავს სხვა პირთა მონაცემებს, ხშირ შემთხვევებში თანამედროვე ტექნოლოგიური მიღწევები იძლევა არასაჭირო მონაცემების დაფარვის შესაძლებლობას განსაკუთრებული ძალისხმევის/დანახარჯის გარეშე. კომპანიის წარმომადგენლის განმარტება ვიდეოჩანაწერების იმგვარად დამუშავების შეუძლებლობის შესახებ, რომ მოეხდინა მასში ასახული მესამე პირების მონაცემების დეპერსონალიზაცია (მაგალითად, გამოსახულებების ე. წ. „დაბლარვა“), არ იქნა გაზიარებული.

შესაბამისად, სამსახურის გადაწყვეტილებით, კომპანიას დაევალა, განმცხადებლისთვის გადაეცა მის მიერ გამოთხოვილი, მისი მონაცემების შემცველი ვიდეოჩანაწერების ასლები იმგვარი ფორმით, რომ შეუძლებელი ყოფილიყო ჩანაწერებში ასახული მესამე პირების იდენტიფიცირება.

ე. მონაცემთა საერთაშორისო გადაცემა

სამსახურმა შემოწმების (ინსპექტირების) ფარგლებში შეისწავლა ერთ-ერთი კომპანიის მიერ მონაცემთა სხვა სახელმწიფოში შესაძლო კანონდარღვევით გადაცემის ფაქტი. კომპანია მომხმარებლებს სთავაზობდა ტაქსის სერვისით მომსახურებას აპლიკაციის მეშვეობით.

ინტერნეტკავშირის მონიტორინგის პროცესში აპლიკაცია უკავშირდებოდა რუსეთის ფედერაციაში მდებარე სერვერებს. კომპანიას აპლიკაციის საშუალებით იმგვარად ჰქონდა ორგანიზებული საქართველოს ტერიტორიიდან რეგისტრირებული მომხმარებლების/მონაცემთა სუბიექტების (მგზავრების/მძღოლების) მონაცემების დამუშავების ტექნიკური პროცესი, რომ მისი გამართულად ფუნქციონირებისას რუსეთის ფედერაციაში მდებარე სერვერებთან ქსელური კავშირის დამყარების დროს სერვერებისათვის ცნობილი ხდებოდა აპლიკაციის მოწყობილობის გლობალური ქსელური მისამართი/„IP Address“-ი. შესაბამისად, სახეზე იყო ქსელური მისამართის/„IP Address“-ის სხვა სახელმწიფოსათვის გადაცემის (ხელმისაწვდომობის) ფაქტი.

ამასთან, შემოწმების (ინსპექტირების) დაწყებამდე კომპანიამ განცხადებით მომართა სამსახურს და მოითხოვა საქართველოს ტერიტორიაზე დამუშავებული მონაცემების რუსეთის ფედერაციაში გადაცემის თაობაზე ნებართვის გაცემა. სამსახურმა მითითებული წარმოების ფარგლებში შეისწავლა აღნიშნული კომპანიის მიერ სხვა სახელმწიფოსთვის (რუსეთის ფედერაციისათვის) მონაცემთა გადაცემასთან დაკავშირებული საკითხები, მათ შორის — მონაცემთა საერთაშორისო გადაცემის მთავარ პირობად განსაზღვრული — მონაცემთა სუბიექტის უფლებების დაცვის სათანადო გარანტიების უზრუნველყოფის შესაძლებლობა და მიიჩნია, რომ რუსეთის ფედერაციაში არ არსებობდა მონაცემთა სუბიექტის უფლებების დაცვის სათანადო გარანტიების, კერძოდ, მონაცემთა უსაფრთხოების პრინციპის დაცვის რეალური მოლოდინი. ამ მოცემულობიდან გამომდინარე, სამსახურის უფროსის ბრძანებით უარი ეთქვა კომპანიას, გაეცა სხვა სახელმწიფოსთვის (რუსეთის ფედერაციაში) მონაცემთა გადაცემასთან დაკავშირებული ნებართვა.

სამსახურმა დაადგინა, რომ კომპანიის მიერ აპლიკაციის საშუალებით საქართველოს ტერიტორიიდან რეგისტრირებული მომხმარებლების/მონაცემთა სუბიექტების (მგზავრების/მძღოლების) მონაცემების საერთაშორისო გადაცემისას (დამუშავებისას) დარღვეულ იქნა კანონის მოთხოვნები. შესაბამისად, კომპანია ცნობილ იქნა სამართალდამრღვევად და ადმინისტრაციული სახდელის სახით შეეფარდა ჯარიმა. ამასთან, კომპანიას დაევალა, აპლიკაციის საშუალებით უზრუნველეყო საქართველოს ტერიტორიიდან რეგისტრირებული მომხმარებლების/მონაცემთა სუბიექტების (მგზავრების/მძღოლების) მონაცემების

(გლობალური ქსელური მისამართის/„IP Address“) რუსეთის ფედერაციაში გადაცემის შეწყვეტა.

2.3. დავალებები და რეკომენდაციები

კერძო სექტორზე ზედამხედველობის დეპარტამენტის მიერ მონაცემთა დამუშავების კანონიერების შესწავლის ფარგლებში მიღებული გადაწყვეტილებებით დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირებს მიეცათ შესასრულებლად სავალდებულო დავალებები და რეკომენდაციები.

დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირებს მიეცათ შემდეგი სახის დავალებები და რეკომენდაციები:

- აუდიოჩაწერის გზით მონაცემთა დამუშავების პროცესის იმგვარად ორგანიზება, რომ მონაცემთა სუბიექტების ინფორმირება აუდიოჩაწერისა და მისი განხორციელების მიზნის თაობაზე ავტომატურად მოხდეს, დამატებით, საერთაშორისო ენაზე;
- ისეთი ორგანიზაციულ-ტექნიკური ზომების მიღება, რომელთა შედეგად, ე. წ. „APDB“ პროგრამის მეშვეობით ბანკის ე.წ. „HR“ ბაზიდან სესხის ოფიცრის მონაცემების მოძიება მხოლოდ პირის უნიკალური მაიდენტიფიცირებელი მონაცემით იქნება შესაძლებელი;
- სოციალური ქსელ „Facebook“-ის ანგარიშზე განთავსებული განმცხადებლის მონაცემების შემცველი ტექსტისა და აუდიოვიდეოჩანაწერის წაშლა;
- ელექტრონული ფოსტის მისამართიდან მიღებული მესამე პირების მონაცემების შემცველი შეტყობინებების წაშლა;
- სახელმწიფო ბაჟის გადახდის მიზნით საგადახდო დავალების დოკუმენტების შედგენისას, სასამართლოს განჩინებების შენახვა მხოლოდ იმ მოცულობით, რომელიც აუცილებელი იქნება საგადახდო დავალების დოკუმენტის სათანადოდ შედგენისთვის;
- მომხმარებლების რეგისტრაციის პროცესში მათი სატელეფონო ნომრების ვერიფიკაციის პროცესის დანერგვა;
- მონაცემთა სუბიექტის მიერ თანხმობის გამოხმობის უფლების განხორციელებისთვის საფასურის ან სხვა შეზღუდვის არდაწესება;
- იმ მონაცემთა სუბიექტებს, რომლებიც 2024 წლის 1-ელი მარტიდან გახდნენ კომპანიის აბონენტები, თანხმობის გაცხადების დროს მიეწოდოთ დამატებითი ინფორმაცია თანხმობის გამოხმობის უფლების განხორციელების მექანიზმის/წესის შესახებ;
- მონაცემთა სუბიექტისგან თანხმობის მიღებამდე მისი მარტივ და გასაგებ ენაზე ინფორმირება თანხმობის ნებისმიერ დროს გამოხმობის უფლების განხორციელების მექანიზმის/წესის შესახებ;
- პირდაპირი მარკეტინგის მიზნით, მონაცემთა სუბიექტის სახელის, გვარის, მისამართის, ტელეფონის ნომრისა და ელექტრონული ფოსტის მისამართის გარდა, მონაცემთა სუბიექტის სხვა მონაცემების დამუშავებამდე მონაცემთა

სუბიექტისაგან კანონით განსაზღვრული წერილობითი თანხმობის მოპოვება;

— მონაცემთა სუბიექტის მონაცემების პირდაპირი მარკეტინგის მიზნით დამუშავების შეწყვეტა;
— ვიდეობანკის საშუალებით პირდაპირი მარკეტინგის მიზნით მონაცემთა სუბიექტების თანხმობის მოპოვების შეწყვეტა; ვიდეობანკის საშუალებით მოპოვებული მონაცემთა სუბიექტების თანხმობების საფუძველზე მათი მონაცემების პირდაპირი მარკეტინგის მიზნით დამუშავების შეწყვეტა;
— პირდაპირი მარკეტინგის მიზნით, მონაცემთა სუბიექტის თანხმობის მოპოვების ტექსტში იმ არხების (სატელეფონო ნომერზე მოკლეტექსტური შეტყობინების, ელექტრონული ფოსტის, მობაილ ბანკის და სხვა (ასეთის არსებობის შემთხვევაში)) შესახებ ამომწურავი ინფორმაციის მიწოდება, რომელთა საშუალებითაც ახორციელებს მონაცემთა სუბიექტისათვის მარკეტინგული შინაარსის შეტყობინებების გაგზავნას;
— ვებგვერდზე განთავსებულ „საბანკო პროდუქტებით მომსახურების სტანდარტულ პირობებში“ პირდაპირ მარკეტინგთან დაკავშირებული, კანონის მე-12 მუხლით გათვალისწინებული საკითხების დეტალურად მოწესრიგება (მათ შორის – რა სახის მონაცემები მუშავდება მონაცემთა სუბიექტის შესახებ, რომელი არხების, კერძოდ: ელექტრონული ფოსტის, მობაილ ბანკის თუ სხვა საშუალებით და მისთ.);
— დამუშავებაზე უფლებამოსილი პირის მეშვეობით, პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების შემთხვევაში, მხარეებს შორის დადებული ხელშეკრულების რეგულაციების შესაბამისობა კანონის 36-ე მუხლით დადგენილ მოთხოვნებთან;
— დამუშავებაზე უფლებამოსილი პირის მეშვეობით, პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების შემთხვევაში, დამუშავებაზე უფლებამოსილი პირისთვის მონაცემების კანონის შესაბამისად დამუშავების შესახებ ინფორმაციის წინასწარ მოთხოვნა და დამუშავებაზე უფლებამოსილი პირის მიერ დამუშავების პროცესზე მონიტორინგის განხორციელების უზრუნველყოფა;
— მონაცემთა სუბიექტების შეცდომაში შეყვანის თავიდან აცილების მიზნით, საცხოვრებელი შენობაში ვიდეომონიტორინგის განხორციელების იმიტაციისთვის განთავსებული კამერის დემონტაჟის უზრუნველყოფა;
— საცხოვრებელ სახლში აუდიომონიტორინგის განხორციელების შეწყვეტა და აუდიომონიტორინგის მეშვეობით შეგროვებული პერსონალური მონაცემების წაშლა;
— სტომატოლოგიურ კაბინეტებში განთავსებული ვიდეოკამერების მეშვეობით შეგროვებული მონაცემების წაშლა, ვიდეოკამერების დემონტაჟი ან იმგვარად განთავსება, რომ ხედვის არეალში არ ხვდებოდეს უშუალოდ საპროცედურო სივრცე და მიმართული იყოს მხოლოდ კაბინეტების შესასვლელისკენ;
— ვიდეოჩანაწერების შემნახველ მოწყობილობაში ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა;

— ვიდეომონიტორინგის სისტემაზე წვდომის უფლების მქონე პირებისთვის ინდივიდუალური მომხმარებლისა და პაროლის შექმნა;
— ინციდენტის აღმოჩენის შემთხვევაში, სამსახურის უფროსის 2024 წლის 28 თებერვლის №19 ბრძანებით დამტკიცებული „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმები და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესით“ დადგენილი მოთხოვნების და კრიტერიუმების გათვალისწინებით შეფასებისა და შესაბამისი წინაპირობების არსებობის შემთხვევაში ინციდენტის შესახებ სამსახურისთვის ამავე წესის შესაბამისად შეტყობინების უზრუნველყოფა;
— ახალი სადებეტო ბარათების კლიენტებისთვის გადაცემის პროცესის იმგვარად ორგანიზება, რომ ბარათებზე დატანილი მონაცემები ხელმისაწვდომი არ იყოს ბანკის სერვისცენტრების თანამშრომლებისთვის;
— კანონის მე-4 მუხლით გათვალისწინებული გამჭვირვალობის პრინციპის მოთხოვნების დაცვით მონაცემთა სუბიექტების, მათ შორის – შეტყობინების ავტორის, ინფორმირება, რომ ბანკთან ურთიერთობის სრულად შეწყვეტისთვის საკმარისი არ არის ბანკის ყველა მომსახურებაზე/პროდუქტზე უარის თქმა და ამისთვის აუცილებელია კონკრეტულად სამართლებრივი ურთიერთობის სრულად შეწყვეტის თაობაზე მოთხოვნის დაყენება;
— გამჭვირვალობის პრინციპის მოთხოვნების დაცვით, ვებგვერდისა და პორტალის საშუალებით, მონაცემთა სუბიექტების ინფორმირების სრულყოფილად უზრუნველყოფა კომპანიის მიერ მონაცემთა სუბიექტების მონაცემების დამუშავების შესახებ ინფორმაციის (მათ შორის – საკრედიტო „რეპორტისა“ და საკრედიტო ქულის) გამოთხოვის საშუალებების თაობაზე. ასევე, მონაცემთა სუბიექტების მონაცემების დამუშავების შესახებ ინფორმაციის გამოთხოვის საშუალებებთან მიმართებით, მონაცემთა სუბიექტისათვის მარტივად აღსაქმელი ფორმით საფასურით და საფასურის გარეშე ინფორმაციის მიღების შესაძლებლობის ალტერნატიული გზების შეთავაზების უზრუნველყოფა;
— მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში, მონაცემთა სუბიექტისთვის მისი მონაცემების დამუშავების თაობაზე ინფორმაციის მაქსიმალურად სრულყოფილად მიწოდება, მათ შორის – შესაბამისი ბმულების (ასეთის საჭიროების შემთხვევაში), განმარტებებისა და დამატებითი მითითებების გზით;
— განმცხადებლისთვის მისი მონაცემების შემცველი სატელეფონო კომუნიკაციის აუდიოჩანაწერის მიწოდება იმ პირთა უფლებების დაცვით, რომელთა საუბარი (ხმა) აუდიოჩანაწერში განმცხადებლის მხარეს ისმოდა;
— ვიდეოკამერების მეშვეობით შეგროვებული განმცხადებლის მონაცემების შემცველი ვიდეოჩანაწერების ასლების მონაცემთა სუბიექტისთვის იმგვარი ფორმით გადაცემა, რომ შეუძლებელი იყოს ვიდეოჩანაწერებში ასახული მესამე პირების იდენტიფიცირება;

— კანონის მე-4 მუხლით გათვალისწინებული სამართლიანობისა და გამჭვირვალობის პრინციპების მოთხოვნების დაცვით, საკუთარ ვებგვერდზე რეგისტრირებული მომხმარებლებისათვის/მონაცემთა სუბიექტებისათვის „პერსონალურ მონაცემთა დამუშავების პოლიტიკაში“ განხორციელებული ცვლილებების შესახებ ინფორმაციის მიწოდების გონივრულ ვადაში უზრუნველყოფა; გონივრული ვადით ადრე ვებგვერდზე რეგისტრირებული მომხმარებლების/მონაცემთა სუბიექტების ინფორმირების უზრუნველყოფა „პერსონალურ მონაცემთა დამუშავების პოლიტიკაში“ განსახორციელებელი ცვლილებების თაობაზე;
— „პერსონალურ მონაცემთა დამუშავების პოლიტიკის“ კონკრეტული მუხლით განსაზღვრული რეგულაციის კანონის მე-4 მუხლით გათვალისწინებული სამართლიანობისა და გამჭვირვალობის პრინციპების მოთხოვნებთან შესაბამისობის უზრუნველყოფა;
— აპლიკაციების საშუალებით საქართველოს ტერიტორიიდან რეგისტრირებული მომხმარებლების/მონაცემთა სუბიექტების (მგზავრების/მძღოლების) პერსონალური მონაცემების (გლობალური ქსელური მისამართის/„IP Address“) რუსეთის ფედერაციაში გადაცემის შეწყვეტა;
— ერთ-ერთ პირს მიეცა რეკომენდაცია, როგორც დამუშავებისთვის პასუხისმგებელი პირის ან/და დამუშავებაზე უფლებამოსილი პირის თანამშრომელს დაეცვა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული მონაცემთა უსაფრთხოების მოთხოვნები, მათ შორის, ემოქმედა მისთვის მინიჭებული უფლებამოსილების ფარგლებში, დაეცვა მონაცემთა საიდუმლოება და კონფიდენციალურობა, მათ შორის, სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგ;
— ერთ-ერთ პირს, მიუხედავად მის მიერ მონაცემების აშკარა პირადი მიზნით დამუშავებისა, მიეცა რეკომანდაცია, არასრულწლოვანთა მონაცემები დაემუშავებინა მხოლოდ გამონაკლის შემთხვევაში, მისი პირადი მიზნისა და არასრულწლოვანის საუკეთესო ინტერესების ურთიერთშეჯერების შემდგომ.

3. მონაცემთა დამუშავება სამართალდამცავი ორგანოების მიერ

3.1. მნიშვნელოვანი მიმართულებები და ტენდენციები

სამართალდამცავი ორგანოების საქმიანობის ფარგლებში პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლა, ფარული საგამოძიებო მოქმედების ჩატარებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობის კონტროლი - პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის ერთ-ერთი მნიშვნელოვანი მიმართულებაა.

სამართალდამცავი ორგანოები, საპოლიციო და პრევენციული ღონისძიებების ჩატარების, გამოძიების, სისხლისსამართლებრივი დევნისა და სასჯელის აღსრულების, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის მიზნით განსაზღვრული საქმიანობისა და მათზე დაკისრებული ფუნქციების შესრულებისას ამუშავებენ დიდი მოცულობით პერსონალურ მონაცემებს.

პერსონალური მონაცემების დამუშავება წარმოადგენს საქართველოს კონსტიტუციის მე-15 მუხლითა და ადამიანის უფლებათა დაცვის ევროპული კონვენციის მე-8 მუხლით დაცული პირადი ცხოვრების უფლებაში ჩარევას. მონაცემების არაკანონიერმა დამუშავებამ შესაძლოა გამოიწვიოს მონაცემთა სუბიექტების უფლებების მნიშვნელოვნად შელახვა, ფიზიკურ პირთა დისკრიმინაცია, და ა. შ. ამიტომ პერსონალური მონაცემების შეგროვება სამართალწარმოების მიზნებისათვის უნდა შემოიფარგლოს მხოლოდ იმით, რაც აუცილებელი და პროპორციულია რეალური საფრთხის პრევენციისთვის ან კონკრეტული დანაშაულის პრევენციის, გამოძიების, სისხლისსამართლებრივი დევნისა თუ მათი საქმიანობის კონკრეტული მიზნისათვის.

პერსონალურ მონაცემთა დაცვის უფლებას ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლი განამტკიცებს, რომელიც განსაზღვრავს მასთან დაკავშირებულ ძირითად ღირებულებებს — პერსონალურ მონაცემთა დამუშავება უნდა იყოს სამართლიანი, ხორციელდებოდეს კონკრეტული მიზნებით, შესაბამისი პირის თანხმობითა და ლეგიტიმური საფუძვლით, რომელსაც ადგენს კანონმდებლობა[19].

შესაბამისად, ზღვრული და სამართლიანი ბალანსის დადგენა პირადი ცხოვრების ხელშეუხებლობისა და საზოგადოების უსაფრთხოების ინტერესს შორის სამართალდამცავი ორგანოების საქმიანობაში უცილობლად გასათვალისწინებელია, რათა არ შეფერხდეს სამართალწარმოების პროცესი და მათ შორის უზრუნველყოფილ იქნეს აღნიშნულ სექტორში პერსონალური მონაცემების დაცვა.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ძირითადი მიზანიც სწორედ ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის, პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის

[19] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018 წლის გამოცემა.

ხელშეუხებლობის უფლებების დაცვაა, რომლის უზრუნველსაყოფად, ახალი კანონით შემოღებულ იქნა პერსონალურ მონაცემთა დაცვის ოფიცრის ინსტიტუტი. აღსანიშნავია, რომ სამართალდამცავი სექტორი პასუხისმგებლობით მოეკიდა ახალი კანონის 90-ე მუხლით დათქმულ ვადაში, ამავე კანონის 33-ე მუხლის შესაბამისად, პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნა/განსაზღვრის სავალდებულო მოთხოვნის შესრულებას. 2024 წლის პირველი ივნისისათვის, სამართალდამცავი სისტემის ყველა რგოლში, დაინიშნენ (განისაზღვრნენ) პერსონალურ მონაცემთა დაცვის ოფიცრები. საქმიანობის დიდი მოცულობის ფუნქციებით დატვირთულ უწყებაში შეიქმნა პერსონალურ მონაცემთა დაცვის საკითხებთან დაკავშირებული სტრუქტურული ერთეულები ან ხსენებულ პოზიციაზე დასაქმდა რამდენიმე პირი. აღნიშნული ხელს შეუწყობს სამართალდამცავი ორგანოების კონსტრუქციულ, კანონის 51-ე მუხლით დადგენილ, პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შემოწმების განხორციელებისათვის მინიჭებული უფლება-მოვალეობების შესრულების თვალსაზრისით გათვალისწინებულ თანამშრომლობას, მათ შორის – შემოწმება/ინსპექტირების ფარგლებში, ინფორმაციის დროულად და სრულად მოწოდების საკითხებში.

საანგარიშო პერიოდში 2 უწყების მიმართ, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსისთვის ან სამსახურის უფლებამოსილი პირისთვის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 51-ე მუხლის მე-3 პუნქტით გათვალისწინებული ინფორმაციის ან/და დოკუმენტაციის წარდგენის წესის დარღვევის გამო, სამსახურმა დაადგინა 86-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული სამართალდარღვევა და შესაბამისი პასუხისმგებლობა დააკისრა მათ.

საგულისხმოა, რომ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსისთვის ან სამსახურის უფლებამოსილი პირისთვის კანონით განსაზღვრული უფლების განხორციელებაში ხელის შეშლა 2024 წლის პირველ მარტს ამოქმედებული კანონით განისაზღვრა, როგორც ახალი სამართალდარღვევა, რითაც ხაზი გაესვა სამსახურის მიერ გაცემული სავალდებულო დავალებათა შესრულების მნიშვნელობასაც. ამასთან, პერსონალურ მონაცემთა დაცვის ოფიცრის მიერ კანონით მინიჭებული ფუნქციების განხორციელება კიდევ უფრო გაზრდის ცნობიერებას და გაამარტივებს დამუშავებისთვის პასუხისმგებელი პირისა ან/და უფლებამოსილ პირთა მხრიდან კანონით დადგენილი უფლებების დაცვასა თუ ვალდებულებების შესრულებას.

სამართალდამცავი ორგანოების მხრიდან სამართალწარმოების მიმდინარეობისას განხორციელებული პერსონალური მონაცემების დამუშავების კანონიერების შემოწმებების ანალიზი, ფარული საგამოძიებო მოქმედებების ჩატარებისა და ელექტრონული აქტივობების კონტროლის შედეგად მიღებული დასკვნები, პერსონალურ მონაცემთა დაცვის სამსახურს ამ სფეროში არსებული ტენდენციებისა და გამოწვევების განსაზღვრის საშუალებას აძლევს.

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 18 იანვრის №ბ/0046-2024 ბრძანებით დამტკიცდა „პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმებების 2024 წლის გეგმის ძირითადი მიმართულებები“ და „პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმებების 2024 წლის

გეგმა“. მიზნობრივი ჯგუფებისა თუ სფეროზე გავლენის გათვალისწინებით განისაზღვრა — სამართალდამცავი ორგანოების მიერ პერსონალურ მონაცემთა დამუშავების შესახებ სამსახურში წარმოდგენილი განცხადებებისა თუ შეტყობინებების, საკუთარი ინიციატივითა თუ წინა წლის გეგმური შემოწმებების პრაქტიკისა და განზოგადების შედეგად წარმოშობილი საკითხები.

შესაბამისად, სამართალდამცავ ორგანოებში განსახორციელებელი გეგმური შემოწმებები ორიენტირდა მოწყვლადი ჯგუფების — არასრულწლოვნების, შეზღუდული შესაძლებლობისა თუ სახელმწიფოს ეფექტიანი კონტროლის ქვეშ მყოფი პირების მიზნობრივი ჯგუფების პერსონალური, მათ შორის, განსაკუთრებული კატეგორიის მონაცემების დამუშავების კანონიერების შესწავლაზე.

გარდა ამ სექტორში შრომითსამართლებრივი ურთიერთობების ფარგლებში პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლისა, ყურადღება გამახვილდა ისეთ სფეროებზე, როგორებიცაა: მოქმედი კანონით ახლად განსაზღვრული თემები, მაგალითად, აუდიომონიტორინგი, ასევე: მონაცემთა უსაფრთხოება, ელექტრონული კომუნიკაციები, სპეციალურ (მაგალითად, სუიციდის პრევენციის) პროგრამაში ჩართულ ბრალდებულთა და მსჯავრდებულთა მონაცემების დამუშავება, თანამედროვე ტექნოლოგიები, ფარული საგამოძიებო მოქმედებები.

აღნიშნული ინსპექტირებები თანაბრად შეეხო თითქმის ყველა სამართალდამცავი ორგანოს საქმიანობას. გეგმური შემოწმებები ჩატარდა: საქართველოს პროკურატურაში, საქართველოს შინაგან საქმეთა სამინისტროში, სსიპ — „საქართველოს შინაგან საქმეთა სამინისტროს აკადემიაში“, საქართველოს იუსტიციის სამინისტროს სისტემაში შემავალ სახელმწიფო საქვეუწყებო დაწესებულებაში — სპეციალურ პენიტენციურ სამსახურში (შემდგომში — „სპეციალური პენიტენციური სამსახური“), სსიპ — „საქართველოს ოპერატიულ-ტექნიკურ სააგენტოში“, საქართველოს თავდაცვის სამინისტროში, საქართველოს ფინანსთა სამინისტროს საგამოძიებო სამსახურში, სახელმწიფო უსაფრთხოების სამსახურში, სპეციალურ საგამოძიებო სამსახურში, დანაშაულის პრევენციის არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის ეროვნულ სააგენტოში, საქართველოს იუსტიციის სამინისტროში, საქართველოს სახელმწიფო დაცვის სპეციალურ სამსახურში.

აღსანიშნავია, რომ საანგარიშო პერიოდში შემცირებულია ვიდეოჩანაწერთა გასაჯაროებისა და მონაცემთა სხვა გზით გამჟღავნებისას კანონის მოთხოვნათა დაცვის დარღვევით დამუშავების, აგრეთვე განსაკუთრებული კატეგორიის - ნასამართლობისა და ჯანმრთელობის შესახებ - მონაცემების არამიზნობრივი გამოყენების შემთხვევები, გაუმჯობესდა მონაცემთა ინფორმირების კანონით გათვალისწინებული მოთხოვნების დაცვის მდგომარეობაც, რაზეც, 2023 წელთან შედარებით, საანგარიშო პერიოდში მიღებული საჩივარ-განცხადებების რიცხვის კლებაც მიუთითებს. თუმცა რამდენიმე შემოწმების შედეგმა კვლავ გამოავლინა მონაცემთა სუბიექტისათვის ინფორმაციის არასრულყოფილად გადაცემის ან მოთხოვნილი მასალისა თუ დოკუმენტაციის გადაცემაზე უარის თქმის ფაქტები.

სამართალდამცავი ორგანოების მიერ სამართალწარმოების პროცესში პერსონალურ მონაცემთა დამუშავებისას გამოწვევად რჩება პროპორციულობის

პრინციპის დაცვის ხარისხი. საანგარიშო პერიოდში კვლავ გამოიკვეთა ლეგიტიმურ მიზანსა და საფუძველთან მიმართებით გადაჭარბებული მოცულობით მონაცემთა დამუშავების ფაქტები. ასევე, პრობლემურია უსაფრთხოების სფეროსთან დაკავშირებული საკითხები, დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირების მხრიდან მონაცემთა დამუშავების შესაძლო და თანამდევი საფრთხეების შესაბამისი ორგანიზაციული და ტექნიკური ზომების (მონაცემებზე წვდომის აღრიცხვა, ინფორმაციული უსაფრთხოების მექანიზმები (კონფიდენციალურობა, მთლიანობა, ხელმისაწვდომობა) მიუღებლობის შემთხვევები; მათ შორის, მონაცემებზე კანონიერი წვდომისა და საამისოდ განსაზღვრული სუბიექტის სწორად შერჩევისა თუ მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვის (ე. წ. „ლოგების“) არარსებობა/არასრულყოფილება, წვდომის უფლების მქონე პირებისათვის განპიროვნებული მომხმარებლის არარსებობა და ამასთან დაკავშირებული სხვა საკითხები.

ყურადსაღებია სამართალდამცავი ორგანოების მხრიდან, ვიდეო-აუდიომონიტორინგის გზით პერსონალურ მონაცემთა დამუშავებისას, კანონის მოთხოვნების დარღვევის შემთხვევებიც, მით უმეტეს იმ პირობებში, როცა 2024 წლის პირველი მარტიდან მოქმედი კანონი ითვალისწინებს ვიდეო-აუდიომონიტორინგის განხორციელების წესებს და მე-10, მე-11 მუხლებით განსაზღვრავს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირების დამატებით ვალდებულებებს, რომელთა მიხედვითაც ვიდეო-აუდიომონიტორინგის განმახორციელებელ პირებს (დამუშავებისთვის პასუხისმგებელ პირებს), კანონის მე-4 მუხლით დადგენილი პრინციპების შესაბამისად, დაევალათ, წერილობით განსაზღვრონ ვიდეო-აუდიომონიტორინგის მიზანი და მოცულობა, ვიდეო-აუდიომონიტორინგის ხანგრძლივობა და მათი შენახვის ვადა, ჩანაწერების წვდომის, მისი შენახვისა და განადგურების წესი და პირობები, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმები. საანგარიშო პერიოდში ამ მიმართულებით ჩატარებული შემოწმებების შედეგებმა აჩვენა, რომ ვიდეო-აუდიომონიტორინგის განხორციელებისას მონაცემთა დამუშავების კანონით გათვალისწინებულ მიზანსა და საფუძველთან მიმართებით პრობლემები არ არსებობდა, ნაკლოვანებები და დარღვევები გამოვლინდა ამ გზით მონაცემთა დამუშავებისას უსაფრთხოების ნაწილში. 4 (ოთხ) შემთხვევაში დადგინდა მონაცემთა არასრული აღრიცხვის, ინდივიდუალური მომხმარებლისა და პაროლის არარსებობის, წერილობითი დოკუმენტის შემუშავების ვალდებულების შეუსრულებლობის ან არასრულად შესრულების ფაქტები.

2024 წლის პირველი მარტიდან მოქმედი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით არსებითად შეიცვალა პერსონალურ მონაცემთა დამუშავების მომწესრიგებელი ნორმები, მიდგომები და სტანდარტები. კანონმდებელმა, ერთი მხრივ, დააკონკრეტა საკითხები, რომლებიც კანონის ძველი რედაქციის მოქმედების ფარგლებში წარმოშობდა პრაქტიკულ პრობლემებს, ხოლო, მეორე მხრივ, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს დაუდგინა ახალი მოთხოვნები და გააუქმა კანონის ძველი რედაქციით გათვალისწინებული გარკვეული სახის ვალდებულებები, რომელთა საპირწონედ დამუშავებისთვის პასუხისმგებელ პირებისთვის გაჩნდა სხვა იმპერატიული

ჩანაწერები. ამ უკანასკნელის თვალსაჩინო მაგალითად შეგვიძლია მოვიყვანოთ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლი, რომელიც დამუშავებისთვის პასუხისმგებელ პირს ავალებს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვასა და, მოთხოვნის შემთხვევაში პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინებას.

ახალი კანონით გაუქმდა ფაილური სისტემის კატალოგის რეესტრი და დამუშავებისთვის პასუხისმგებელ პირებს მოეხსნათ ფაილური სისტემის კატალოგში შეტანილი ინფორმაციის რეესტრში აღრიცხვის ვალდებულება; თუმცა კანონის 28-ე მუხლით გათვალისწინებულ იქნა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულება, აღრიცხოს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაცია და მოთხოვნის შემთხვევაში, არა უგვიანეს 3 სამუშაო დღისა, წარუდგინოს პერსონალურ მონაცემთა დაცვის სამსახურს. ახალმა კანონმდებლობამ აღნიშნული დოკუმენტის პროაქტიული წარდგენის აუცილებლობა გააუქმა.

შემოწმების შედეგებმა აჩვენა, რომ 2024 წლის პირველი მარტიდან მოქმედი კანონის სიახლეებიდან, 28-ე მუხლით განსაზღვრული, მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულების შესრულება გამოწვევად იქცა.

2024 წლის პირველი მარტის შემდეგ, სამართალდამცავ ორგანოებზე ზედამხედველობის დეპარტამენტის მიერ დასრულებული 8 (რვა) გეგმური შემოწმების ფარგლებში დადგინდა, რომ არცერთ სამართალდამცავ ორგანოს ჰქონდა შემუშავებული მონაცემების დამუშავების პროცესებთან მიმართებით აღრიცხვის ფორმა. ზოგიერთი მათგანი მიუთითებდა, რომ ხსენებული დოკუმენტი შემუშავების პროცესში იყო, ზოგიერთს მიზანშეწონილად არ მიაჩნდა ერთიანი დოკუმენტის წარმოება. ცხადია, ყველა მსგავს შემთხვევაში, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის გადაწყვეტილებით, უწყებებს დაევალათ კანონის 28-ე მუხლით გათვალისწინებული ინფორმაციის წერილობით ან ელექტრონული ფორმით ასახვა.

საყურადღებოა ერთ-ერთი გეგმური შემოწმება, რომლის ფარგლებშიც დადგინდა, რომ უწყებაში არ იყო შექმნილი ერთიანი დოკუმენტი (წერილობით ან ელექტრონული ფორმით), რომელშიც ასახული იქნებოდა კონკრეტულ მონაცემთა დამუშავების პროცესებთან დაკავშირებული ინფორმაცია. ვინაიდან აღნიშნული პროცესი ისედაც ელექტრონული ფორმით მიმდინარეობდა, (ელექტრონულ სისტემაში აისახებოდა ნებისმიერი ინფორმაცია/დოკუმენტაცია), უწყების მოსაზრებით, ამ ინფორმაციის განცალკევებული აღრიცხვა საჭირო არ იყო. სამართალდამცავი ორგანოს მიერ მითითებული ელექტრონული სისტემის დათვალიერების შედეგად, სისტემა არ შეიცავდა ყველა იმ მონაცემს, რომელთა აღრიცხვის ვალდებულებაც, კანონის 28-ე მუხლის შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს ეკისრებათ.

პერსონალურ მონაცემთა დაცვის სამსახურმა არ გაიზიარა უწყების განმარტება, რომ კანონის 28-ე მუხლით გათვალისწინებული ვალდებულების უზრუნველყოფა ხორციელდებოდა ელექტრონულ სისტემაში მასალებისა და მასთან დაკავშირებული ინფორმაციის ასახვით, ვინაიდან კანონი აღნიშნულ

ვალდებულებას უწესებს მონაცემთა დამუშავებისთვის პასუხისმგებელ ყველა პირს და ამ ვალდებულებას არ უკავშირებს მონაცემთა დამუშავების რომელიმე (ავტომატურ, ნახევრად ავტომატურ და არაავტომატურ) საშუალებას. შესაბამისად, კანონი ხსენებული ვალდებულებისგან არ ათავისუფლებს იმ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს, რომლებიც მონაცემთა დამუშავების პროცესში იყენებენ ავტომატურ საშუალებებს, რომლებშიც გარკვეული სახის ინფორმაცია ელექტრონულად ისედაც აისახება. აღნიშნულის გათვალისწინებით, უწყებას მიეცა შესასრულებლად სავალდებულო დავალება - უზრუნველეყო მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლის შესაბამისად აღრიცხვა.

მნიშვნელოვანია, რომ სამართალდამცავმა ორგანოებმა შემდგომში უნდა გაითვალისწინონ და უზრუნველყონ ამ ვალდებულების შესრულება, ნორმის ამოქმედების მიზანი, დამუშავებისათვის პასუხისმგებელი პირის მიერ მონაცემთა დაცვისათვის ისეთი ღონისძიებების შემუშავებაა, რომლებიც წინასწარ დაგეგმავს ამ პროცესების კანონშესაბამისად წარმართვას და თავიდან აიცილებს მონაცემთა დამუშავების დარღვევებს.

3.2. პრეცედენტული გადაწყვეტილებები

ა. მონაცემების ხელმისაწვდომობა

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მიზნად ისახავს პერსონალური მონაცემების დამუშავებისას ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის, პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცვას.

მონაცემთა სუბიექტი აღჭურვილია კანონით გარანტირებული, სამართლებრივი დაცვის საშუალებებით. ახალი კანონი აწესებს მოთხოვნებს, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის „დაადგინონ უფლების დაცვის უფრო მაღალი სტანდარტი ბავშვის პერსონალური მონაცემების დამუშავებისას, მათ შორის, ბავშვსა და მის კანონიერ წარმომადგენელს შორის მონაცემთა დამუშავებასთან დაკავშირებით არსებული აზრთა სხვადასხვაობის არსებობის დროს ბავშვის საუკეთესო ინტერესისთვის უპირატესობის მინიჭებით“[20].

ახალი კანონმდებლობით მონაცემთა სუბიექტისთვის მინიჭებულია მონაცემთა პორტირების უფლება და უარის საშუალება, დაექვემდებაროს მხოლოდ ავტომატიზებული საშუალებით მიღებულ გადაწყვეტილებას, რაც მიზნად ისახავს საკუთარ პერსონალურ მონაცემებზე მონაცემთა სუბიექტის კონტროლის გაძლიერებას. იგი მჭიდროდ არის დაკავშირებული მონაცემებზე წვდომის უფლებასთან.

[20] პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მიღების თარიღი: 14/06/2023, მე-7 მუხლის მე-5 პუნქტი.

ინფორმაციის მიღების უფლება უშუალოდ მიემართება მონაცემთა სუბიექტის ისეთი მნიშვნელოვანი უფლებების რეალიზაციას, როგორებიცაა: მონაცემთა გასწორება, განახლება, დამატება, დაბლოკვა, წაშლა და განადგურება, თანხმობის უკან გამოთხოვა თუ გასაჩივრება.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, მონაცემთა სუბიექტს უფლება აქვს, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთან გაეცნოს მის შესახებ არსებულ პერსონალურ მონაცემებს და უსასყიდლოდ მიიღოს აღნიშნული მონაცემების ასლები. ინფორმაციის მოთხოვნისა და ასლის მიღების უფლების მიზანია, მიაწოდოს მონაცემთა სუბიექტებს საკმარისი, გამჭვირვალე და ადვილად ხელმისაწვდომი ინფორმაცია მისი პერსონალური მონაცემების დამუშავების შესახებ, რათა იცოდეს და განსაზღვროს დამუშავების კანონიერება და დამუშავებული მონაცემების სიზუსტე.

მონაცემების გაცნობა ან/და მათი ასლების მიღება უზრუნველყოფილი უნდა იქნეს 10 სამუშაო დღის ვადაში, გარდა იმ შემთხვევისა, როდესაც საქართველოს კანონმდებლობით სხვა ვადა არ არის დადგენილი.

პოზიტიურ ტენდენციად უნდა ჩაითვალოს გარემოება, რომ წინა წელთან შედარებით შემცირებულია მოქალაქეთა განცხადება/საჩივრებით მომართვის მაჩვენებელი და რამდენიმე განცხადების შესწავლის ფარგლებში არ დადგინდა ინფორმირების წესების დარღვევის ფაქტები:

— საქართველოს შინაგან საქმეთა სამინისტროს სსიპ — „დაცვის პოლიციის დეპარტამენტი“

საანგარიშო პერიოდში სამსახურმა მოქალაქის განცხადების საფუძველზე შეისწავლა საქართველოს შინაგან საქმეთა სამინისტროს სსიპ — „დაცვის პოლიციის დეპარტამენტის“ მიერ მისი ინფორმირების წესების დარღვევის საკითხი.

განმცხადებელი გამოსაცდელი ვადით იყო დაცვის პოლიციის დეპარტამენტში დასაქმებული. გამოსაცდელი ვადის გასვლის შემდეგ, სპეციალური შემოწმების შედეგების გათვალისწინებით, იგი გათავისუფლდა სამსახურიდან. მან დაცვის პოლიციის დეპარტამენტს ელექტრონული ფოსტის საშუალებით განცხადებით მიმართა და მოითხოვა თავისი პერსონალური მონაცემების დამუშავების შესახებ ინფორმაცია და დოკუმენტაცია, თუმცა არ წარუდგენია საკუთარი პირადობის დამადასტურებელი დოკუმენტი ან თავისი ვინაობის მაიდენტიფიცირებელი სხვა ინფორმაცია.

დაცვის პოლიციის დეპარტამენტმა (ვინაიდან განცხადების მიხედვით, უწყებისთვის სხვა საკონტაქტო ინფორმაცია ხელმისაწვდომი არ იყო), განმცხადებელს ელექტრონული ფოსტის მისამართზე გაუგზავნა საპასუხო კორესპონდენცია, რომლითაც მოსთხოვა მაიდენტიფიცირებელი ინფორმაციის/დოკუმენტაციის წარდგენა. საკითხის გადაწყვეტა მოითხოვდა სხვადასხვა სტრუქტურული ერთეულისგან ინფორმაციის მიღებას, რის გამოც აღნიშნული წერილი უწყებამ გაგზავნა მე-10 სამუშაო დღეს. შემოწმების ფარგლებში დადგინდა, რომ ხსენებული წერილი განმცხადებელმა თავის ელექტრონული ფოსტის მისამართზე მიიღო, თუმცა არ წაუკითხავს, რის გამოც

მოთხოვნილი მაიდენტიფიცირებელი ინფორმაცია/დოკუმენტაცია დამატებით არ წარუდგენია დაცვის პოლიციის დეპარტამენტისთვის.

შესწავლის ფარგლებში მოპოვებული მტკიცებულებებისა და ფაქტობრივი გარემოებების ანალიზის შედეგად, პერსონალურ მონაცემთა დაცვის სამსახურმა დაადგინა, რომ დაცვის პოლიციის დეპარტამენტი ვალდებული იყო განეხილა განმცხადებლის განცხადება, რადგან იგი უკავშირდებოდა მონაცემთა სუბიექტის ინფორმირების საკითხს. ამისათვის აუცილებელი იყო კონკრეტული პირის იდენტიფიცირება. მონაცემთა უსაფრთხოების სტანდარტის გათვალისწინებით, პირის იდენტიფიცირების მიზნით, დაცვის პოლიციის დეპარტამენტი ვერ დაეყრდნობოდა მხოლოდ ელექტრონული ფოსტის მისამართში მითითებულ მონაცემებს და დაცვის პოლიციის მხრიდან მონაცემთა სუბიექტისთვის მაიდენტიფიცირებელი მონაცემების/დოკუმენტაციის მოთხოვნა კანონშესაბამისად შეფასდა. ამ პროცესში გათვალისწინებული იქნა ის გარემოებაც, რომ დაცვის პოლიციის დეპარტამენტის მხრიდან პასუხის აღნიშნულ ვადაში გაგზავნას არსებითი გავლენა არ მოუხდენია მონაცემთა სუბიექტის უფლებებზე, რადგან, როგორც გამოირკვა, განმცხადებელი უწყებისგან მიღებულ სახარვეზო წერილს არ გასცნობია. შესაბამისად, ხარვეზის გასწორებისა და პირის იდენტიფიცირების გარეშე ძირითადი მოთხოვნა ვერ განიხილებოდა.

არსებული ხარვეზის შესახებ კორესპონდენციის მე-10 სამუშაო დღეს გაგზავნასთან დაკავშირებით, უწყებამ განმარტა, რომ აღნიშნული პროცესი - არასამუშაო და უქმე დღეებისა და იმის გათვალისწინებით, რომ კონსულტაციას გადიოდა სამინისტროს ადმინისტრაციის პერსონალურ მონაცემთა დაცვის განყოფილებასთან — ობიექტურად გაჭიანურდა.

პერსონალურ მონაცემთა დაცვის სამსახურმა მიიჩნია: უწყებას განცხადების მიღების შემდეგ, დამატებითი კონსულტაციების გამართვის გარეშე ან აღნიშნულის პარალელურად, დაუყოვნებლივ, პირველივე შესაძლებლობისთანავე ეცნობებინა მონაცემთა სუბიექტის განცხადების განხილვისათვის კანონმდებლობით განსაზღვრული და სავალდებულო მოთხოვნის დაზუსტების შესახებ. დაცვის პოლიციის დეპარტამენტს მიეცა რეკომენდაცია. დამატებით, დაევალა განმცხადებლისთვის მოთხოვნილი ინფორმაცია/დოკუმენტაციის კანონით დადგენილ ვადაში მიწოდება.

— საქართველოს თავდაცვის სამინისტრო

საქართველოს თავდაცვის სამინისტროს გენერალური ინსპექციის (სამხედრო და სამოქალაქო მიმართულებით ინსპექტირებისა და სამსახურებრივი შემოწმების მთავარი სამმართველო) მიერ დისციპლინური წარმოებისას გამოსაკითხი პირების მონაცემების დამუშავების პროპორციულობის კანონიერების გეგმურად შემოწმების ფარგლებში დადგინდა, რომ სამინისტრო მონაცემთა სუბიექტთა ინფორმირებისთვის იყენებდა მხოლოდ ახსნა-განმარტების ოქმში მითითებულ ჩანაწერს — „შემოწმების მიმდინარეობისას კანონით გათვალისწინებული ლეგიტიმური მიზნის მისაღწევად პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მოთხოვნათა დაცვით მუშავდება მისი პერსონალური

მონაცემი“. სამინისტროს წარმომადგენლის განმარტებით, სხვა ფორმით მონაცემების დამუშავების თაობაზე მონაცემთა სუბიექტების ინფორმირება არ ხდებოდა.

გეგმური შემოწმების ფარგლებში, სამინისტროს მიერ წარმოდგენილი ინფორმაციის საფუძველზე გაირკვა, რომ გადაცდომის სავარაუდო ჩამდენის მხრიდან საქმის მასალების გადაცემის მოთხოვნის დაფიქსირების შემთხვევაში, ისინი მოკლებულნი არიან შესაძლებლობას, გადასცენ საქმის მასალის ასლები, „საჯარო სამსახურის შესახებ“ საქართველოს კანონის 92-ე მუხლის „ბ“ ქვეპუნქტის (დისციპლინური გადაცდომის სავარაუდო ჩამდენ პირს უფლება აქვს, მოითხოვოს დისციპლინური წარმოების საქმის მასალების გაცნობა) შესაბამისად. თუმცა მოთხოვნის შემთხვევაში უზრუნველყოფენ საქმის მასალების ადგილზე გაცნობას, ვინაიდან, სამინისტროს განმარტებით, „საჯარო სამსახურის შესახებ“ საქართველოს კანონი ითვალისწინებს დისციპლინური გადაცდომის სავარაუდო ჩამდენი პირის მხრიდან მხოლოდ მასალების გაცნობის უფლებას.

სამსახურმა არ გაიზიარა სამინისტროს მითითება „საჯარო სამსახურის შესახებ“ საქართველოს კანონის 92-ე მუხლის „ბ“ ქვეპუნქტზე, ვინაიდან პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული საკითხები მოწესრიგებულია სპეციალური კანონით — „პერსონალურ მონაცემთა დაცვის შესახებ“ — რომლითაც დეტალურად არის გათვალისწინებული მონაცემთა სუბიექტის ინფორმირების საკითხი, მათ შორის — აღნიშნული უფლების შეზღუდვის სამართლებრივი საფუძვლები. შესაბამისად, მონაცემთა სუბიექტის მიერ ინფორმაციის მოთხოვნის შემთხვევაში, მონაცემთა დამმუშავებელმა უნდა იხელმძღვანელოს ხსენებული სპეციალური კანონით, ყოველ კონკრეტულ შემთხვევაში საქმის ფაქტობრივი გარემოებების გათვალისწინებით, მხოლოდ ამ კანონით დადგენილი რეგულაციის ფარგლებში გადაწყვიტოს მოთხოვნის დაკმაყოფილება/არდაკმაყოფილების საკითხი.

ამდენად, მიზანშეწონილია, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა სუბიექტის უფლებათა შეზღუდვის სამართლებრივი საფუძვლების არსებობა/არარსებობის საკითხი შეფასდეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან შესაბამისობაში და, შესაბამის ნორმაზე მითითებით, საკუთარი უფლების შეზღუდვის შესახებ იმგვარად ეცნობოს განმცხადებელს (ასეთის არსებობის შემთხვევაში), რომ ზიანი არ მიადგეს უფლების შეზღუდვის მიზანს.

თავდაცვის სამინისტროს მიეცა დავალება, მონაცემთა სუბიექტის უფლებების შეზღუდვის საფუძვლის არარსებობის შემთხვევაში, მონაცემების უშუალოდ მონაცემთა სუბიექტისგან შეგროვების პროცესში, მონაცემთა სუბიექტის უფლებების რეალიზების უზრუნველყოფის მიზნით ახსნა-განმარტების ოქმში დატანილი ინფორმირების ნაწილი შესაბამისობაში მოიყვანოს კანონის 24-ე მუხლით გათვალისწინებულ წესთან.

8. შრომითი ურთიერთობები

შრომითი ურთიერთობის ნებისმიერ ეტაპზე, როგორც წინასახელშეკრულებო, ასევე სახელშეკრულებო და ხელშეკრულების შემდგომი ურთიერთობების ფარგლებში, სამართალდამცავი ორგანოები სხვადასხვა მიზნით (კვალიფიციური კადრების შერჩევა, უსაფრთხოება, საქართველოს კანონმდებლობით დადგენილი ვალდებულებების შესრულება და ა. შ.) ამუშავებენ დიდი მოცულობით პერსონალურ მონაცემებს. ამასთან, როგორც წესი, მონაცემთა დამუშავების პროცესში, კომპეტენციის შესაბამისად, ჩართულია არაერთი პირი, რომლებსაც ხელი მიუწვდებათ განმცხადებლების/კანდიდატების, მოქმედი და ყოფილი დასაქმებულების სხვადასხვა, მათ შორის – განსაკუთრებული კატეგორიის მონაცემებზე (მაგალითად, ასეთებია: პირის ჯანმრთელობის მდგომარეობა, ნასამართლობის სტატუსი და ა. შ.).

სამართალდამცავი ორგანოების მიერ შრომით სამართლებრივ ურთიერთობებში მოპოვებული პერსონალური მონაცემების მხოლოდ კანონიერი მიზნით, პროპორციულობის პრინციპისა და კანონის სხვა მოთხოვნათა სრული დაცვით დამუშავება, კვლავ სამსახურის ერთ-ერთ პრიორიტეტულ მიმართულებად ითვლება. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონით დადგენილი აუდიომონიტორინგის განხორციელების სპეციალური წესის შესაბამისად, მონაცემთა დამუშავებისას დამუშავებისთვის პასუხისმგებელი პირებისთვის განსაზღვრულ სხვადასხვა ვალდებულებათა შორის, საინტერესო აღმოჩნდა შრომითსამართლებრივი ურთიერთობებში აუდიომონიტორინგის ფორმით მონაცემთა დამუშავების სპეციფიკა.

— საქართველოს თავდაცვის სამინისტრო

სამსახურმა გეგმური შემოწმების (ინსპექტირების) ფარგლებში შეისწავლა საქართველოს თავდაცვის სამინისტროს მიერ კანდიდატებთან გასაუბრების პროცესში განხორციელებული აუდიომონიტორინგის გზით მონაცემთა დამუშავების კანონიერების საკითხი.

შემოწმების ფარგლებში დადგინდა, რომ საქართველოს თავდაცვის სამინისტრო სამოქალაქო ოფისში კონკურსის მეორე ეტაპზე, ბრიფინგის ოთახებში ათავსებდა პორტატულ ვიდეოკამერას და კანდიდატის შერჩევის პროცესის გამჭვირვალედ წარმართვის, გასაუბრების პროცესში მიუკერძოებლობისა და ობიექტურობის დაცვისა და ანტიდისკრიმინაციული გარემოს შექმნისათვის, მონაცემთა სუბიექტის წერილობითი თანხმობის შემთხვევაში ახორციელებდა კანდიდატებთან გასაუბრების პროცესის ვიდეო-აუდიო ჩაწერას.

შესწავლის შედეგად გამოიკვეთა, რომ კანდიდატების ინფორმირება მონაცემთა დამუშავების შესახებ ხდებოდა როგორც ზეპირსიტყვიერად, ასევე – წერილობითი ფორმით და კანდიდატი თავისი თავისუფალი ნების საფუძველზე იღებდა გადაწყვეტილებას ვიდეო-აუდიომონიტორინგის განხორციელების თაობაზე.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედი რედაქციით ახლებურად ჩამოყალიბდა თანხმობის (მათ შორის, წერილობითი თანხმობის) ცნება და მისი კრიტერიუმები. თანხმობა მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ, მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე აქტიური მოქმედებით, წერილობით (მათ შორის – ელექტრონულად) ან ზეპირად, თავისუფლად და მკაფიოდ გამოხატული ნებაა; წერილობითი თანხმობა კი ისეთი თანხმობა, რომელსაც მონაცემთა სუბიექტმა ხელი მოაწერა ან რომელიც მან სხვაგვარად გამოხატა წერილობით, მათ შორის – ელექტრონულად, მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე ინფორმაციის მიღების შემდეგ.

ამდენად, თანხმობა — როგორც მონაცემთა სუბიექტის სურვილის ნებაყოფლობითი, კონკრეტული, ინფორმირებული და მკაფიო გამოხატულება — შესაბამისი კანონიერი საფუძველია იმ შემთხვევაში, თუ მონაცემთა სუბიექტს სთავაზობენ კონტროლსა და რეალურ არჩევანს შეთავაზებული პირობების მიღებასა და უარყოფას შორის ან მას უარის თქმა შეუძლია საკუთარი თავისათვის ზიანის მიყენების გარეშე; აღნიშნული კი მონაცემთა დამუშავების მიზნების შესახებ ინფორმაციის არარსებობის შემთხვევაში შეუძლებელია. როდესაც დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტისგან ითხოვს თანხმობას, იგი ვალდებულია, შეაფასოს, თუ რამდენად აკმაყოფილებს ნამდვილი თანხმობის მოპოვების ყველა ზემოთჩამოთვლილ მოთხოვნას.[21]

საქართველოს თავდაცვის სამინისტროს გეგმური შემოწმების ფარგლებში გამოიკვეთა, რომ სამინისტროს შემუშავებული ჰქონდა მონაცემთა სუბიექტის წერილობითი თანხმობის ფორმა, რომელზეც ხელმოწერით კანდიდატი ადასტურებდა ან უარს აცხადებდა ვიდეო-აუდიოჩაწერაზე, თუმცა ფორმა, მონაცემთა დამუშავების მიზანთან დაკავშირებით, შეიცავდა ზოგად ინფორმაციას და მასში არ იყო მითითებული, რას გულისხმობდა მონაცემების დამუშავება შრომითსამართლებრივი მიზნებისთვის.

სამსახურმა მიიჩნია, რომ საქართველოს თავდაცვის სამინისტროს მიერ წარმოდგენილი თანხმობის ფორმით არ იყო უზრუნველყოფილი კანდიდატისათვის მონაცემთა დამუშავების კონკრეტული მიზნის თაობაზე ინფორმაციის მიწოდება, რის გამოც დამუშავებისთვის პასუხისმგებელ პირს დაევალა წერილობითი თანხმობის ფორმის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის „ნ“ ქვეპუნქტის შესაბამისად მოდიფიცირება.

— საქართველოს თავდაცვის სამინისტრო

სამსახურმა გეგმურად შეისწავლა საქართველოს თავდაცვის სამინისტროს გენერალური ინსპექციის (სამხედრო და სამოქალაქო მიმართულებით ინსპექტირებისა და სამსახურებრივი შემოწმების მთავარი სამმართველო) მიერ

[21] ევროპის მონაცემთა დაცვის საბჭოს, სახელმძღვანელო რეკომენდაცია 05/2020 თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით, 2020 წლის 4 მაისი, 6.

დისციპლინური წარმოებისას, გამოსაკითხი პირების მონაცემების დამუშავების პროპორციულობის კანონიერების საკითხი.

შესწავლის შედეგად გამოიკვეთა, რომ გამოსაკითხი პირისგან ახსნა-განმარტების მიღების მიზნით დისციპლინური წარმოების დროს სამინისტროს შემუშავებული ჰქონდა შესაბამისი ფორმა, რომლის მეშვეობითაც გროვდებოდა სხვადასხვა სახის პერსონალური, მათ შორის – განსაკუთრებული კატეგორიის მონაცემი. კერძოდ, ოქმში აისახებოდა შემდეგი სახის ინფორმაცია: ოქმის შედგენის თარიღი და ადგილი, მისი შედგენის დაწყებისა და დასრულების დრო, დოკუმენტის შემდგენი პირის სამსახურებრივი თანამდებობა, მისი სახელი და გვარი; ასევე აისახებოდა გამოსაკითხი პირის სახელი, მამის სახელი, გვარი, დაბადების თარიღი — წელი, თვე და რიცხვი, დაბადების ადგილი, განათლება, სპეციალობა, საქმიანობა ან თანამდებობა, წოდება, რეგისტრაციის ადგილი, ფაქტობრივი საცხოვრებელი და საკონტაქტო ტელეფონის ნომერი. უშუალოდ ახსნა-განმარტების შინაარსში მიეთითებოდა კონკრეტულ ფაქტთან დაკავშირებული სხვა გარემოებები, რომლებიც მათ შორის შესაძლოა, რომ დაკავშირებული ყოფილიყო გამოსაკითხი ან მესამე პირების პერსონალურ მონაცემებთან.

შემოწმების შედეგად დადგინდა, რომ გამოკითხვის ოქმში მითითებული ზოგიერთი მონაცემის, მათ შორის ინფორმაცია განათლებისა და სპეციალობის შესახებ, დამუშავების აუცილებლობა პირის გამოკითხვის თავდაპირველ ეტაპზე არ არსებობდა და მათი შეგროვების საჭიროება შესაძლოა მხოლოდ კონკრეტულ საქმეში მნიშვნელოვანი გარემოებების დასაზუსტებლად დამდგარიყო, თუ, მაგალითად, დისციპლინური წარმოება მიემართებოდა სამინისტროს თანამშრომლის კომპეტენციას. შედეგად, საქართველოს თავდაცვის სამინისტროში ოქმის მეშვეობით გროვდებოდა გამოსაკითხი პირის ისეთი მონაცემები, რომელთა დამუშავების მიზნობრიობა ყველა დისციპლინური საქმისწარმოების ფარგლებში არ არსებობდა.

გარდა ამისა, აღნიშნული ოქმი შაბლონური სახის იყო და გამოიყენებოდა როგორც თანამშრომლების, ასევე დისციპლინურ საქმესთან კავშირში მყოფი ყველა პირის გამოკითხვის პროცესში. არათანამშრომელი გამოსაკითხი პირის შემთხვევაშიც გროვდებოდა ის ინფორმაცია (მაგალითად: ნასამართლობის, სახელმწიფო ჯილდოს, ოჯახური მდგომარეობის შესახებ), რომელთა დამუშავება რელევანტური იყო მხოლოდ თანამშრომლებთან მიმართებით. აღნიშნული ზრდიდა მონაცემთა არამიზნობრივად დამუშავების რისკებს.

დამუშავებისთვის პასუხისმგებელ პირს ნაკლოვანების აღმოფხვრის მიზნით დაევალა თანამშრომელთა და სხვა, მესამე პირთა გამოსაკითხად 2 (ორი) დიფერენცირებული ოქმის ფორმის შემუშავება, აგრეთვე – გამოკითხვის პროცესში დასამუშავებელ მონაცემთა მიზნობრიობის შეფასება და გამოსაკითხი ფორმების ველების მეშვეობით მხოლოდ იმ მონაცემების დამუშავება, რომლებიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად, ხოლო კონკრეტული დისციპლინური საქმის განხილვის პროცესში აუცილებელი მონაცემების მოპოვება საჭიროებისამებრ, უშუალოდ ახსნა-განმარტების შინაარსის მეშვეობით.

აგრეთვე, შესწავლის პროცესში სამსახურმა შეაფასა დისციპლინური წარმოების ფარგლებში მოპოვებული მონაცემების შენახვა, რის შედეგადაც

გამოვლინდა, რომ, ინსპექტირების/სამსახურებრივი შემოწმების დასრულების შემდგომ, მასალები სრულად იკინძებოდა და ინახებოდა 10 (ათი) წლის ვადით, თუმცა დამუშავებისთვის პასუხისმგებელმა პირმა ვერ დაასაბუთა მონაცემების ხსენებული ვადით შენახვის აუცილებლობა. აღნიშნულის გათვალისწინებით, დამუშავებისთვის პასუხისმგებელ პირს დაევალა გამოსაკითხ პირთა მონაცემების კონკრეტული მიზნით შენახვის ვადებისა და შენახვის ვადის ამოწურვის შემდგომ მონაცემთა მიმართ განსახორციელებელი ქმედებების წერილობითი ფორმით განსაზღვრა.

— საქართველოს იუსტიციის სამინისტრო

საქართველოს იუსტიციის სამინისტროს გეგმური შემოწმება (ინსპექტირება) მოიცავდა გენერალური ინსპექციის მიერ დისციპლინური წარმოებისას გამოსაკითხი პირების მონაცემების დამუშავების პროპორციულობის საკითხს.

შემოწმების ფარგლებში დადგინდა, რომ საქართველოს იუსტიციის სამინისტროს გენერალური ინსპექციის სამსახურებრივი შემოწმების სამმართველო დისციპლინური წარმოების ფარგლებში გამოსაკითხი პირების პერსონალურ მონაცემებს მოიპოვებს სხვადასხვა ფორმით. ერთ-ერთია უშუალოდ გამოსაკითხი პირის წერილობითი ახსნა-განმარტება, რომელშიც აისახება: პირის სახელი, გვარი, თანამდებობა (თანამშრომლის შემთხვევაში), მისამართი და ტელეფონის ნომერი, ხოლო ახსნა-განმარტების შინაარსში დამატებით გამოსაკითხი პირი საკუთარი ინიციატივით უთითებს სადავო საკითხთან დაკავშირებულ გარემოებებს, რომლებიც შესაძლოა შეიცავდეს როგორც გამოსაკითხი პირის, ასევე – სხვა, მესამე პირების პერსონალურ მონაცემებს.

შემოწმებით დადგინდა, რომ, გარდა ზემოაღნიშნული ფორმით მონაცემების მოპოვებისა, შესაბამისი საჭიროებისას გამოსაკითხი პირების პერსონალური მონაცემები გროვდება სამინისტროსა და მის სისტემაში შემავალი სხვადასხვა სტრუქტურული ერთეულისა და სხვა დაწესებულებებისგან ინფორმაციის გამოთხოვის, ასევე – მის მმართველობაში არსებული საჯარო სამართლის იურიდიული პირების შიდა საქმიანობის ელექტრონულ სისტემებზე პირდაპირი წვდომის გზით. მოპოვებული მტკიცებულებების საფუძველზე დადგინდა, რომ დისციპლინური წარმოების ფარგლებში მონაცემები მუშავდებოდა კანონმდებლობით დაკისრებული მოვალეობის შესრულების მიზნით, დისციპლინური გადაცდომის ფაქტის სწრაფად, სრულად გამოვლენის, ასევე – თანაზომიერი დისციპლინური პასუხისმგებლობის ზომის განსაზღვრისათვის.

სამსახურმა შეაფასა დისციპლინური წარმოების ფარგლებში მოპოვებული მონაცემების შენახვის ვადების კანონიერებაც.

შემოწმების პროცესში გამოვლინდა, რომ დისციპლინური შემოწმების დასრულების შემდგომ მასალები სრულად იკერება და ინახება 5 (ხუთი) წლის ვადით, რომლის საჭიროებაც უწყებამ ახსნა საქართველოს იუსტიციის მინისტრის ბრძანებით დამტკიცებული ნომენკლატურითა და პასუხისმგებლობის დაკისრების ხანდაზმულობის გათვალისწინებით, „საჯარო სამსახურის შესახებ“ საქართველოს კანონით.

შემოწმების ფარგლებში გაანალიზდა „საჯარო სამსახურის შესახებ“ საქართველოს კანონით განსაზღვრული ვადები, რის საფუძველზეც გაირკვა, რომ ეს უკანასკნელი არ ითვალისწინებს დისციპლინური საქმისწარმოების მასალების შენახვის კონკრეტულ დროს, თუმცა განსაზღვრავს სხვადასხვა პროცედურულ ვადას. ხსენებული კანონის 88-ე მუხლის მე-4 პუნქტი მიუთითებს, რომ დისციპლინური წარმოება იწყება დისციპლინური გადაცდომის გამოვლენიდან 1 (ერთი) თვეში, თუკი დისციპლინური გადაცდომის ჩადენიდან 3 (სამი) წელი არ არის გასული. ამასთან, ამავე კანონის 95-ე მუხლის შესაბამისად, დისციპლინური წარმოება არ უნდა აღემატებოდეს 2 (ორი) თვეს. ასევე საგულისხმოა „საჯარო სამსახურის შესახებ“ საქართველოს კანონის 101-ე მუხლის პირველი პუნქტის დათქმა, რომლის მიხედვითაც, პირი დისციპლინური პასუხისმგებლობის მქონედ ითვლება მისთვის დისციპლინური პასუხისმგებლობის ზომის შეფარდებიდან 1 (ერთი) წლის განმავლობაში.

ამდენად, დისციპლინურ წარმოებასთან დაკავშირებული პროცედურული ვადების ჯამური ოდენობა არ შეადგენდა 5 (ხუთი) წელს, რის გამოც სამსახურმა ვერ გაიზიარა მონაცემების ამ დროით შენახვის საჭიროება და დამუშავებისთვის პასუხისმგებელ პირს დაავალა გამოსაკითხ პირთა მონაცემების კონკრეტული მიზნით შენახვის ვადების განსაზღვრა და მისი ამოწურვის შემდგომ მონაცემების წაშლა/განადგურება.

გ. მოწყვლადი ჯგუფები

საკუთარი საქმიანობის ფარგლებში სამართალდამცავი ორგანოები ამუშავებენ მოწყვლადი ჯგუფების მონაცემებს, რომელთა შესწავლა საქართველოს მონაცემთა დაცვის საზედამხედველო ორგანოსთვის პრიორიტეტული საკითხია. აღნიშნულიდან გამომდინარე, სამსახურის უფროსის მიერ განსაზღვრული პერსონალურ მონაცემთა დამუშავების კანონიერების გეგმური შემოწმებების (ინსპექტირება) 2024 წლის გეგმის ერთ-ერთ ძირითად მიმართულებად სწორედ მოწყვლადი ჯგუფის სტატუსის მქონე პირები განისაზღვრა.

პერსონალურ მონაცემთა უკანონო დამუშავება შეიძლება განსაკუთრებით საზიანო იყოს შეზღუდული შესაძლებლობების მქონე პირებისა და არასრულწლოვნის შემთხვევაში მათი მოწყვლადობის გათვალისწინებით. ამავე კატეგორიას ასევე განეკუთვნება პენიტენციურ დაწესებულებაში მოთავსებული ბრალდებული/მსჯავრდებული, რომელსაც ჰქონდა სუიციდის ჩადენის მცდელობა. შესაბამისად, მათი მონაცემების დამუშავება უნდა განხორციელდეს კანონით დადგენილი, კიდევ უფრო მაღალი სტანდარტის შესაბამისად.

არასრულწლოვნის პერსონალური მონაცემების დაცვა ერთ-ერთი აქტუალური და პრობლემური საკითხია, მით უფრო, თუ მონაცემთა სუბიექტი კანონთან კონფლიქტში მყოფი მოზარდია. მისი პირადი ცხოვრების ხელშეუხებლობის დაცვას არსებითი მნიშვნელობა აქვს კანონით განსაზღვრული ლეგიტიმური მიზნების მისაღწევად. სახელმწიფოს აკისრია მთელი რიგი ვალდებულებები, რომელთა საფუძველზე დგინდება არასრულწლოვანთა უფლებების დაცვის ადეკვატური გარანტიები.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ახალი რედაქციის თანახმად, გაიზარდა სუბიექტის უფლებები და გაფართოვდა მათი დაცვის გარანტიები. კანონმა სპეციალური წესებით მოაწესრიგა არასრულწლოვანთა პერსონალური მონაცემების დამუშავებასთან დაკავშირებული საკითხები. კერძოდ, კანონის მე-7 მუხლის მიხედვით, განისაზღვრა არასრულწლოვნის შესახებ მონაცემთა დამუშავებაზე თანხმობის გაცემის წესი და პირობები.

არასრულწლოვნის შესახებ მონაცემთა დამუშავებისას დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაითვალისწინოს და დაიცვას არასრულწლოვნის საუკეთესო ინტერესები. ბავშვთა საუკეთესო ინტერესის დაცვის პრინციპი განმტკიცებულია არაერთი სამართლებრივი აქტით როგორც ეროვნულ,[22] ასევე – საერთაშორისო დონეზე.[23] ბავშვის უფლებების შესახებ საქართველოს კოდექსით გათვალისწინებული ბავშვის საუკეთესო ინტერესის დეფინიცია არ არის ამომწურავი და ტოვებს სუბიექტური შეფასების შესაძლებლობას, რადგან, ბავშვთან დაკავშირებული საკითხების სიმრავლის გათვალისწინებით, მისი ამომწურავი განსაზღვრება შეუძლებელია. ბავშვის საუკეთესო ინტერესების დეფინიცია უნდა იყოს დინამიური და მოქნილი იმისათვის, რომ ადეკვატურად უპასუხოს ბავშვთან დაკავშირებულ ყველა შესაძლო კონკრეტულ შემთხვევას.[24]

საერთაშორისო დონეზე არასრულწლოვნის საუკეთესო ინტერესის დაცვას უზრუნველყოფს „ბავშვის უფლებების შესახებ“ 1989 წლის კონვენცია (“CRC”), რომლის მიხედვითაც, ბავშვთან დაკავშირებით ნებისმიერი მოქმედების განხორციელებისას საჯარო ან კერძო სოციალური კეთილდღეობის დაწესებულებების, სასამართლოების, ადმინისტრაციული თუ საკანონმდებლო ორგანოების მიერ, უპირველეს ყოვლისა, გათვალისწინებული უნდა იყოს ბავშვის საუკეთესო ინტერესები.[25]

სამართალდამცავ ორგანოებს, ასევე, დიდი როლი ეკისრებათ ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების პროცესში. შეზღუდული შესაძლებლობების მქონე პირთა, როგორც მონაცემთა მოწყვლად სუბიექტთა, უფლებების დაცვა პერსონალურ მონაცემთა დაცვის სამსახურის ძირითად მიმართულებად განიხილება. ცალსახაა, რომ შშმ პირები საჭიროებენ გაძლიერებულ დაცვას, რამდენადაც შესაძლებელია, რომ ამ მონაცემების უკანონო დამუშავებამ გამოუსწორებელი ზიანი მიაყენოს მონაცემთა სუბიექტს.

[22] ბავშვის უფლებათა კოდექსი, საქართველოს კანონი, 27/09/2019.

[23] კონვენცია ბავშვის უფლებების შესახებ, საქართველოს საერთაშორისო ხელშეკრულება და შეთანხმება, 1948.

[24] *კილაძე ს., ტურავა პ.,* ბავშვის უფლებათა კოდექსის კომენტარები, 2021, 44.

[25] UN, Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, Article 3.

— სსიპ — „საქართველოს შინაგან საქმეთა სამინისტროს აკადემია“

პერსონალურ მონაცემთა დაცვის სამსახურმა გეგმურად შეისწავლა სსიპ — „საქართველოს შინაგან საქმეთა სამინისტროს აკადემიის“ (შემდგომში — აკადემია) მიერ არასრულწლოვანთა გამოკითხვის სპეციალიზებულ სივრცესა და მიმდებარე ტერიტორიაზე ვიდეო/აუდიომონიტორინგის განხორციელების კანონიერების საკითხი.

შემოწმების ფარგლებში დადგინდა, რომ აკადემიის ტერიტორიაზე 2018 წლიდან მოწყობილია სიმულაციური სწავლების სივრცე (მოიცავს არასრულწლოვანთა გამოკითხვის სპეციალიზებულ სივრცესაც), რომელიც აკადემიის მხრიდან გამოიყენება მხოლოდ მსმენელთა სწავლება/ტესტირების მიზნებისთვის; იგი მოწყობილია თანამედროვე სტანდარტებით, ამიტომ, შესაბამისი საჭიროების არსებობის შემთხვევაში, სამინისტროს გამომძიებლები აღნიშნულ სივრცეს იყენებენ არასრულწლოვანთა გამოკითხვის მიზნებისთვის. მართალია, ამ სივრცეში დამონტაჟებულია ვიდეოკამერები, თუმცა ადგილზე შემოწმების ფარგლებში დადგინდა, რომ ვიდეო-აუდიომონიტორინგი აღნიშნული სისტემის მეშვეობით არ ხორციელდებოდა და გამოცდის/ტესტირების მიზნებისთვის გამომძიებლების მხრიდან არასრულწლოვანთა გამოკითხვის პროცესის ვიდეო-აუდიოჩაწერის უზრუნველყოფისთვის სივრცეში განთავსებული იყო პორტატული კამერა. შემოწმების ფარგლებში მოპოვებული მტკიცებულებების საფუძველზე დადგინდა, რომ არასრულწლოვანთა გამოკითხვის პროცესის ვიდეო-აუდიო ჩაწერა არ განხორციელებულა. არასრულწლოვანთა გამოკითხვის ვიდეო-აუდიოჩაწერის გზით ფიქსაციის პროცესში მონაცემთა დამუშავების ფაქტადგილი არ ჰქონია, შესაბამისად, არ დადგინდა ადმინისტრაციული სამართალდარღვევის ფაქტი.

პროცესის მიმდინარეობისას გამოიკვეთა ნაკლოვანებები, რამაც შესაძლოა სამომავლოდ არასრულწლოვანთა მონაცემთა უკანონო დამუშავების საფრთხეები შექმნას.

კამერების არსებობა, როდესაც არ ხდება ვიდეომონიტორინგი/ვიდეოჩაწერა, და, შესაბამისად, მონაცემების ამ გზით დამუშავება, იწვევს მონაცემთა სუბიექტის ქცევის თავისუფლების შეზღუდვას. უქმნის მას მცდარ წარმოდგენასა და მუდმივ განცდას, რომ იგი ექვემდებარება ვიდეომონიტორინგს. ამის გამო იგი ვალდებულია, სხვაგვარად აკონტროლოს თავისი ქცევა. საგულისხმოა ისიც, რომ დამუშავების ცრუ მოლოდინებით შესაძლოა, ხელი შეეშალოს მონაცემთა სუბიექტის უფლებების, მათ შორის – მონაცემთა გასწორების, განახლების, დაბლოკვისა თუ კანონმდებლობით გარანტირებული სხვა უფლებების რეალიზებას.

აღნიშნული კიდევ უფრო საყურადღებოა, როდესაც საკითხი არასრულწლოვანს მიემართება. მართალია, თითოეულ კამერასთან განთავსებული იყო ვიდეომონიტორინგის მიმდინარეობის გამომრიცხავი შესაბამისი გამაფრთხილებელი ნიშანი, თუმცა ის, გამოკითხვის პროცესში მყოფი პირისთვის, მით უფრო არასრულწლოვნისთვის, შესაძლოა არ წარმოადგენდეს სათანადო ფორმით ინფორმირებას. ამ სივრცეში მოხვედრილმა მოზარდმა, მისი ასაკის, ფიზიკური და გონებრივი განვითარების (მაგალითად, წერა-კითხვის არმცოდნის,

შეზღუდული მხედველობის და ა. შ.) გათვალისწინებით, შესაძლოა, ვერ დააფიქსიროს ან/და ვერ აღიქვას გამაფრთხილებელ ნიშანზე დატანილი ინფორმაცია (მით უმეტეს, როცა დადგენილია, რომ ვიდეო-მონიტორინგი საერთოდ არ მიმდინარეობს და აკადემიაც არ ერევა გამოკითხვის პროცესში, ხსენებულთან დაკავშირებით არც მითითებას იძლევა). შესაბამისად, არასრულწლოვანს სათვალთვალო კამერის დაფიქსირებისთანავე შესაძლოა მცდარი წარმოდგენა შეექმნას საკუთარი მონაცემების დამუშავებასთან დაკავშირებით.

ამდენად, აკადემიას მიეცა რეკომენდაცია — კანონის მოთხოვნათა შესაბამისად, უზრუნველეყო სიმულაციური სწავლების, მათ შორის, არასრულწლოვანთა გამოკითხვის სპეციალიზებულ სივრცეში დამონტაჟებული კამერებით ვიდეომონიტორინგის განხორციელება ან მათი დემონტაჟი, რომლის შესრულებამდეც, ვიდეომონიტორინგის მიმდინარეობის შესახებ არასრულწლოვან მონაცემთა სუბიექტის არასწორი წარმოდგენის თავიდან ასაცილებლად, ვიდეოკამერები უნდა დაფარულიყო.

— საქართველოს პროკურატურა

პერსონალურ მონაცემთა დაცვის სამსახურმა გეგმურად შეისწავლა საქართველოს პროკურატურის მიერ არასრულწლოვანთა გამოკითხვის სპეციალიზებულ სივრცეებში, არასრულწლოვანთა ვიდეო-აუდიო ფიქსაციის პროცესში მონაცემთა დამუშავების კანონიერება.

შემოწმების ფარგლებში დადგინდა, რომ არასრულწლოვანთა გამოკითხვის მიზნით საქართველოს პროკურატურას 8 (რვა) რაიონული პროკურატურის შენობაში მოწყობილი აქვს არასრულწლოვანთა გამოკითხვის სპეციალიზებული ოთახები, რომლებშიც დამონტაჟებულია როგორც ვიდეოკამერები, ასევე – ხმოვანი სიგნალის ჩამწერი (აუდიოჩამწერი) მოწყობილობები, რომელთა მეშვეობითაც აღნიშნულ სივრცეებში გამოკითხვის პროცესის ვიდეო-აუდიომონიტორინგი მხოლოდ საჭიროების შემთხვევაში მიმდინარეობს. გამოკითხვის პროცესის ვიდეო-აუდიო ფიქსაციის თაობაზე გადაწყვეტილების მიღება, ერთი მხრივ, უკავშირდება სავარაუდო დანაშაულის კატეგორიას, მეორე მხრივ კი — არასრულწლოვნის ასაკს, ფიზიკურ და გონებრივ განვითარებას, ასევე – მის მძიმე ემოციურ ფონს, ვინაიდან არსებობს რისკი იმისა, რომ არასრულწლოვანს შესაძლოა დაავიწყდეს გამოძიების მიზნებისთვის მნიშვნელოვანი ინფორმაცია. ამავდროულად, აღნიშნულიემსახურება არასრულწლოვნის მეორეული ვიქტიმიზაციის (რაც შესაძლოა თან ახლდეს არასრულწლოვნის ჩვენების მიცემის მიზნით სასამართლოში მის განმეორებით დაკითხვას) რისკების შემცირებას.

იმის გათვალისწინებით, რომ საკითხის მომწესრიგებელი სამართლებრივი აქტები (საქართველოს სისხლის სამართლის საპროცესო და არასრულწლოვანთა მართლმსაჯულების კოდექსები), შესაბამისი აუცილებლობის არსებობის შემთხვევაში, ითვალისწინებს გამოკითხვის პროცესის ვიდეო-აუდიოჩაწერას, ამდენად, შემოწმების ფარგლებში დადგინდა, რომ პროკურატურას ჰქონდა ვიდეო-

აუდიომონიტორინგის განხორციელების მიზნები და სამართლებრივი საფუძვლები.

შეფასდა მონაცემთა სუბიექტების (გამოსაკითხი არასრულწლოვნების) ინფორმირებისა და ვიდეო-აუდიო ჩაწერის გზით დამუშავებული მონაცემების უსაფრთხოების საკითხებიც.

შემოწმების ფარგლებში დადგინდა, რომ პროკურატურის სისტემაში მოწყობილი 8 (რვა) გამოსაკითხი ოთახიდან 7 (შვიდი) სივრცეში გამაფრთხილებელი ნიშანი საერთოდ არ იყო განთავსებული და გამოკითხვის პროცესში მონაწილე პირების ინფორმირება ვიდეო-აუდიომონიტორინგის მიმდინარეობის თაობაზე ხდებოდა ზეპირსიტყვიერად, რაც აისახებოდა გამოკითხვის ოქმში. ერთ-ერთ რაიონულ პროკურატურაში კი განთავსებული იყო ვიდეო-აუდიომონიტორინგის განხორციელების თაობაზე გამაფრთხილებელი ნიშანი, თუმცა ის არ შეიცავდა მითითებას, რომ ვიდეო-აუდიო ჩაწერა ხორციელდებოდა მხოლოდ გამოკითხვის პროცესში. პერსონალურ მონაცემთა დაცვის სამსახურმა აღნიშნული ფორმით მონაცემთა სუბიექტების ინფორმირება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან შეუსაბამოდ მიიჩნია, ვინაიდან გამაფრთხილებელი ნიშნის გარეშე ვიდეოკამერის არსებობა, როდესაც ხსენებულ სივრცეში მუდმივ რეჟიმში არ მიმდინარეობს ვიდეომონიტორინგი, ოთახში მყოფ პირებს თავისთავად უქმნის მცდარ წარმოდგენას, თითქოს ექვემდებარებიან ვიდეო-აუდიომონიტორინგს.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, სამსახურმა განმარტა, რომ არასრულწლოვანთა მონაცემების დამუშავების პროცესში ჩართულ ნებისმიერ პირს ეკისრება ვალდებულება, მიიღოს ყველა ზომა, რათა მონაცემების დამუშავების პროცესი იყოს გამჭვირვალე, წარიმართოს ისე, რომ საფრთხე არ შეექმნას არასრულწლოვანთა კანონიერ ინტერესს. ამასთან, არასრულწლოვან მონაცემთა სუბიექტს ნათელი წარმოდგენა შეექმნას დამუშავების პროცესის შესახებ. შესაბამისად, კანონის მე-10 მუხლის მე-8 და მე-9 პუნქტებით, ასევე, მე-11 მუხლის მე-3 და მე-4 პუნქტებით გათვალისწინებული ვალდებულებისა და მონაცემთა სუბიექტების სწორი ინფორმირების უზრუნველყოფის მიზნით, პროკურატურას მიეცა დავალება.

— საქართველოს პროკურატურა

პერსონალურ მონაცემთა დაცვის სამსახურმა გეგმურად შეისწავლა საქართველოს პროკურატურის მიერ მის სისტემაში შემავალი, საქართველოს გენერალური პროკურატურის ადამიანის უფლებათა დაცვის დეპარტამენტის მიერ შეზღუდული შესაძლებლობების მქონე პირების მონაცემების დამუშავების კანონიერება.

შემოწმების ფარგლებში დადგინდა, რომ ადამიანის უფლებათა დაცვის დეპარტამენტი შეზღუდული შესაძლებლობის მქონე როგორც სრულწლოვან, ასევე – არასრულწლოვან პირთა პერსონალურ, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებს, რომლებსაც მოიპოვებს პროკურატურის ანალიტიკური

სამმართველოსა და სისხლის სამართლის საქმისწარმოების ელექტრონულ პროგრამიდან, 2021 წლიდან ასახავს და ინახავს ე. წ. ექსელის ფორმატის ფაილში.

საქართველოს პროკურატურამ, შეზღუდული შესაძლებლობის მქონე პირთა პერსონალური მონაცემების დამუშავების მიზნად, ადამიანის უფლებათა დაცვის დეპარტამენტის სხვადასხვა სამართლებრივი აქტით განსაზღვრული უფლებამოსილებების, მათ შორის, საერთაშორისო ვალდებულებების განხორციელება დაასახელა. გამოიკვეთა, რომ, დამუშავებული მონაცემების ანალიზის საფუძველზე, დეპარტამენტი უზრუნველყოფს შეზღუდული შესაძლებლობის მქონე უფლებების დაცვის მონიტორინგსა და საპროკურორო საქმიანობის ხარისხის გაუმჯობესებას. ამასთან, ამ ფორმით დამუშავებული მონაცემის საფუძველზე, პროკურატურა ყოველწლიურად ახდენს ანგარიშგებას შეზღუდული შესაძლებლობის მქონე პირთა უფლებების კონვენციის იმპლემენტაციის უწყებათაშორისი საკოორდინაციო კომიტეტის წინაშე.

საქართველოს პროკურატურის მიერ მითითებული სამართლებრივი აქტების ანალიზის საფუძველზე გაირკვა, რომ პროკურატურას აქვს მონაცემების ამ ფორმით დამუშავების მიზანი და სამართლებრივი საფუძველი. ამდენად, შესაფასებელი გახდა მონაცემთა შენახვის ვადების კანონიერებისა და მონაცემთა უსაფრთხოების საკითხები.

შემოწმების ფარგლებში დადგინდა, რომ საქართველოს პროკურატურას შეფასებული არ ჰქონდა მონაცემთა შენახვის კონკრეტული ვადა. საქართველოს პროკურატურამ მიუთითა, რომ ზემოხსენებული ფორმით მონაცემთა დამუშავება დაწყებულია 2021 წლიდან. შესაბამისად, ამ ინფორმაციის შენახვის საჭიროება კვლავ ჰქონდა.

რაც შეეხება მონაცემთა უსაფრთხოების საკითხს, შემოწმების შედეგად დადგინდა, რომ ე. წ. „ექსელის“ ფორმატში შენახული, შეზღუდული შესაძლებლობის მქონე პირთა პერსონალურ მონაცემებზე წვდომა შეზღუდულია და გამომდინარეობს კონკრეტული საჭიროებიდან. თუმცა ელექტრონული სისტემის (ე. წ. „ექსელის“) ფაილს, რომელშიც ხსენებული მონაცემები ინახებოდა, არ ჰქონდა მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვის ელექტრონული ჟურნალი (ე. წ. „ლოგირება“). ამასთან, აღნიშნული ფუნქციონალი არც უშუალოდ იმ კომპიუტერებში იყო ჩართული, რომელთა მეშვეობითაც ხორციელდებოდა წვდომა ე. წ. „ექსელის“ ფაილზე.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, საქართველოს გენერალურ პროკურატურას დაევალა შეზღუდული შესაძლებლობის მქონე პირთა პერსონალური მონაცემების ე. წ. „ექსელის“ ფაილის სახით შენახვის კონკრეტული ვადების განსაზღვრა და იმგვარი ორგანიზაციული და ტექნიკური ზომების მიღება, რომლებიც უზრუნველყოფდა მონაცემთა მიმართ შესრულებული ყველა მოქმედების აღრიცხვას.

— სპეციალური პენიტენციური სამსახური

საქართველოს იუსტიციის სამინისტროს სისტემაში შემავალ სახელმწიფო საქვეუწყებო დაწესებულებაში — სპეციალურ პენიტენციურ სამსახურში — არსებული სუიციდის პრევენციის პროგრამაში ჩართულ მსჯავრდებულთა შესახებ

მონაცემების სხვა სახელმწიფო დაწესებულებებისთვის გადაცემის პროცესში მონაცემების დამუშავების კანონიერების საკითხი.

შემოწმების ფარგლებში დადგინდა, რომ სპეციალური პენიტენციური სამსახური, „ბრალდებულთა/მსჯავრდებულთა სუიციდის პრევენციის პროგრამის დამტკიცების შესახებ“ საქართველოს იუსტიციის მინისტრის 2020 წლის 26 ოქტომბრის №643 ბრძანებით დადგენილი წესის თანახმად, სავარაუდო სუიციდის რისკის მქონე ბრალდებულთა/მსჯავრდებულთა იდენტიფიცირებისა და მათთვის პროგრამის ფარგლებში შესაბამისი დახმარების გაწევის მიზნით, მოიპოვებს და ინახავს თავისუფლებააღკვეთილი პირების პერსონალურ, მათ შორის განსაკუთრებული კატეგორიის (ფსიქიკური ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციას) მონაცემებს.

ზემოხსენებული ბრძანებით დადგენილი წესის შესაბამისად, თუ დაწესებულებიდან გათავისუფლებული მსჯავრდებულის სასჯელის შემდგომი მოხდის მიზნით ვალდებულია, გამოცხადდეს სააგენტოს შესაბამის ტერიტორიულ ორგანოში ან მსჯავრდებული მთლიანად თავისუფლდება სასჯელის შემდგომი მოხდისგან, მსჯავრდებულის თანხმობის შემთხვევაში, შესაბამისი უფლებამოსილი პირი მსჯავრდებულის სუიციდის პრევენციის პროგრამაში ჩართულობის შესახებ ინფორმაციას აწვდის საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედ საჯარო სამართლის იურიდიულ პირს — დანაშაულის პრევენციის, არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის ეროვნულ სააგენტოს. შემოწმების შედეგად დადგინდა, რომ ასეთ დროს სპეციალური პენიტენციური სამსახური, დოკუმენტბრუნვის ელექტრონული სისტემის გამოყენებით, პრობაციის ეროვნულ სააგენტოს წერილობითი ფორმით აწვდის შემდეგ მონაცემებს: მსჯავრდებულის სახელს, გვარს, მამის სახელს, პირად ნომერს, სუიციდის პრევენციის პროგრამაში ჩართულობის, ბოლო გადამოწმების თარიღისა და სუიციდის რისკის დონის განსაზღვრის თაობაზე ინფორმაციას, ხოლო დანართის სახით უგზავნის მსჯავრდებულის თანხმობას მონაცემების პრობაციის ეროვნული სააგენტოსთვის გამჟღავნებასთან დაკავშირებით.

ვინაიდან მონაცემების სხვა საჯარო დაწესებულებისთვის („პრობაციის ეროვნული სააგენტოსთვის“) გამჟღავნებას შესაბამისი ბრძანება უდევს საფუძვლად, რომელიც, თავის მხრივ, ამ ფორმით მონაცემთა დამუშავებას სწორედ მონაცემთა სუბიექტის თანხმობას უკავშირებს, შეფასდა სპეციალური პენიტენციური სამსახურის მხრიდან სუიციდის პროგრამაში ჩართული მსჯავრდებულის წერილობითი თანხმობის მიღების საკითხი.

პერსონალურ მონაცემთა დაცვის სამსახურმა განმარტა, რომ სპეციალურ პენიტენციურ სამსახურს აქვს ბენეფიციარების განსაკუთრებული კატეგორიის მონაცემების (მსჯავრდების, გარკვეულ შემთხვევებში კი ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის) პრობაციის ეროვნული სააგენტოსთვის გადაცემის ლეგიტიმური მიზანი. კერძოდ, აღნიშნული ემსახურება ბენეფიციარის ინტერესს, მიიღოს უწყვეტი მომსახურება, რომელიც უზრუნველყოფს მის ფიზიკურ უსაფრთხოებასა და სიცოცხლეს (რათა თავიდან იქნეს აცილებული სუიციდი/მისი მცდელობა). საგულისხმოა ისიც, რომ ბენეფიციარი წერილობითი ფორმით ადასტურებს მონაცემების პრობაციის ეროვნული სააგენტოსთვის გადაცემას, თუმცა იმისთვის, რომ სპეციალურმა პენიტენციურმა სამსახურმა

შეძლოს თანხმობის არსებობის დადასტურება, მნიშვნელოვანია, მან თანხმობა მოიპოვოს კანონით დადგენილი წესით, რისთვისაც თანხმობის გაცემამდე მონაცემთა სუბიექტს წინასწარ უნდა მიეწოდოს ინფორმაცია დამუშავების მიზნების შესახებ.

თანხმობას უნდა ჰქონდეს ნებაყოფლობითი ხასიათი და უნდა გამოიხატოს აქტიური მოქმედებით. შემოწმების ფარგლებში გამოიკვეთა, რომ თანხმობის ფორმა არ შეიცავდა ინფორმაციას, კონკრეტულად რომელი მონაცემები (თანხმობის ტექსტით არ იდენტიფიცირდებოდა, რომ პირის სახელი, გვარი, მამის სახელი, პირადი ნომერი, გათავისუფლების თარიღი, ბოლო გადაფასების თარიღისა და რისკის დონის შესახებ ინფორმაციის გადაცემა მოხდება) და რა მიზნით უნდა გადასცემოდა პრობაციის ეროვნულ სააგენტოს. შესაბამისად, სპეციალური პენიტენციური სამსახურის მიერ წარმოდგენილ დოკუმენტზე ხელის მოწერა იმთავითვე არ იქნა მიჩნეული მონაცემების დამუშავებაზე წერილობით თანხმობად, რადგან იგი არ მოიცავდა გადასაცემი მონაცემების ამომწურავ ჩამონათვალსა და მონაცემთა დამუშავების მიზნის თაობაზე ბენეფიციარის ინფორმირების დადასტურებას.

შემოწმების შედეგად არ გამოიკვეთა სამართალდარღვევის ფაქტი, თუმცა სპეციალურ პენიტენციურ სამსახურს მიეცა დავალება - შეემუშავებინა წერილობითი თანხმობის სტანდარტული ტექსტი, რომლითაც ბენეფიციარს მიეწოდება სრული ინფორმაცია პრობაციის ეროვნული სააგენტოსთვის გადასაცემი მონაცემებისა და გადაცემის მიზნის შესახებ, რასაც ბენეფიციარი კანონით დადგენილი წესით დაადასტურებდა. უწყებას ასევე დაევალა, უზრუნველეყო მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლის შესაბამისად აღრიცხვა.

დ. ვიდეო-აუდიომონიტორინგი

ვიდეოკამერების სისტემები სხვადასხვა სახის, დიდი მოცულობით პერსონალური მონაცემების დამუშავების (მოპოვების, ჩაწერის, შენახვის) შესაძლებლობას იძლევა. ამასთან, ტექნოლოგიური ინოვაციების პროგრესირების პარალელურად, სულ უფრო ხელმისაწვდომი ხდება ის ტექნიკური საშუალებები, რომლებიც უზრუნველყოფს პერსონალურ მონაცემთა, კერძოდ, ვერბალური კომუნიკაციის აუდიო ჩანაწერების, დამუშავების შესაძლებლობასაც.

სამართალდამცავი უწყებები, რომელთა ფუნქციებს ფუნდამენტურ უფლებათა და თავისუფლებათა დაცვას, ფიზიკურ და იურიდიულ პირთა ქონებრივი ინტერესების უზრუნველყოფას, დელიქტურ ქმედებათა პრევენციასა და გამოძიებას წარმოადგენს, ახდენენ ვიდეო მონიტორინგის (მათ შორის, აუდიომონიტორინგის განმახორციელებელი) სისტემების ინსტალაციას და მათ გამოყენებას მრავალმხრივი ლეგიტიმური მიზნებისათვის, რაც, თავის მხრივ, მოიცავს პერსონალური მონაცემების მასშტაბურ დამუშავებას.

ტექნოლოგიური განვითარების კვალდაკვალ ნებისმიერი პირისთვის ხელმისაწვდომი გახდა ის ელექტრონული მოწყობილობები, რომელთა

მეშვეობითაც შესაძლებელია ფიზიკური პირების საუბრის ფიქსაციაც (აუდიომონიტორინგი). ბოლო წლების ტენდენციებმა აჩვენა, რომ აუდიომონიტორინგის განხორციელება და, შესაბამისად, ამ ფორმით მონაცემების დამუშავება საკმაოდ გავრცელებულია სამართადამცავი ორგანოების საქმიანობის ფარგლებშიც.

2024 წლის პირველი მარტიდან მოქმედი კანონით განისაზღვრა ვიდეო-აუდიომონიტორინგის განხორციელების სპეციალური წესები.

ამ გზით მონაცემების დამუშავების სპეფიციკურობის გათვალისწინებით, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლი ადგენს ვიდეომონიტორინგის კონკრეტულ მიზნებს და განსაზღვრავს დასაქმებული პირის სამუშაო პროცესის/სივრცის, ასევე – საცხოვრებელი შენობის, გამოსაცვლელი ოთახების, ჰიგიენისთვის განკუთვნილი ადგილების ან ისეთი სივრცეების ვიდეომონიტორინგთან დაკავშირებულ საკითხებს, რომელებიც სუბიექტის პირადი ცხოვრების დაცულობის გონივრულ მოლოდინებს შეეხება. ხოლო ამავე კანონის მე-11 მუხლი ამომწურავად განსაზღვრავს აუდიომონიტორინგის განხორციელების საფუძვლებსა და სუბიექტის ინფორმირების წესებს.

აღსანიშნავია, რომ კანონის მე-10 და მე-11 მუხლებით მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს განესაზღვრათ დამატებითი ვალდებულებები, რომელთა მიხედვითაც ვიდეო-აუდიომონიტორინგის განმახორციელებელმა პირებმა (დამუშავებისთვის პასუხისმგებელმა პირებმა), კანონის მე-4 მუხლით დადგენილი პრინციპების შესაბამისად, წინასწარ წერილობით უნდა განსაზღვრონ ვიდეო-აუდიომონიტორინგის მიზანი და მოცულობა, ვიდეო-აუდიომონიტორინგის ხანგრძლივობა, მათი შენახვის ვადა, ჩანაწერების წვდომის, მისი შენახვისა და განადგურების წესი, ასევე – პირობები, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმები.

მნიშვნელოვანია იმის უზრუნველყოფა, რომ სამართალდამცავი ორგანოების მიერ განხორციელებული მონიტორინგი არ სცდებოდეს კანონით დადგენილ ფარგლებს და არ იწვევდეს მოქალაქეთა პირადი ცხოვრების უფლების გაუმართლებელ შეზღუდვას, რაც განსაკუთრებით აქტუალურია ხელოვნური ინტელექტის, სახის ამოცნობის ტექნოლოგიებისა და სხვა თანამედროვე საშუალებების გამოყენების კონტექსტში.

საანგარიშო პერიოდში, პერსონალურ მონაცემთა დაცვის სამსახურმა როგორც გეგმური, ასევე არაგეგმური შემოწმებების ფარგლებში, შეისწავლა სხვადასხვა სამართალდამცავი უწყების მხრიდან ვიდეო-აუდიომონიტორინგის განხორციელების პროცესში მონაცემთა დამუშავების საკითხები.

— სპეციალური საგამოძიებო სამსახური

საანგარიშო პერიოდში ანონიმური შეტყობინების საფუძველზე სამსახურის მიერ შესწავლილი ერთ-ერთი საქმე უკავშირდებოდა სპეციალური საგამოძიებო სამსახურის ადმინისტრაციულ შენობაში დამონტაჟებული ვიდეო სათვალთვალო კამერებით მონაცემთა დამუშავების კანონიერების საკითხს.

შემოწმების შედეგად დადგინდა, რომ სპეციალური საგამოძიებო სამსახურის ადმინისტრაციულ შენობის (მის.: თბილისი, მ. ასათიანის ქუჩა №9) როგორც შიდა, ასევე გარე პერიმეტრზე განთავსებული იყო ვიდეოკამერები, რომელთა ხედვის არეალში ექცეოდა არა მხოლოდ შენობის მიმდებარე ტერიტორია, საერთო (შესასვლელი, დერეფნები, კიბის უჯრედები) და სასერვერო/სასაწყობე სივრცეები, არამედ საკონფერენციო (ე. წ. „საბრიფინგო“) და გამოსაკითხი ოთახები; ვიდეომონიტორინგის განხორციელების პროცესში გამოყენებული ელექტრონული სისტემის დათვალიერებით კი გაირკვა, რომ ვიდეოკამერების მეშვეობით ხორციელდებოდა მხოლოდ ვიდეომონიტორინგი.

შესწავლის ფარგლებში სპეციალურმა საგამოძიებო სამსახურმა ვიდეომონიტორინგის განხორციელების მიზნად პირის უსაფრთხოების, საკუთრების დაცვის, საიდუმლო ინფორმაციის დაცვის უზრუნველყოფა დაასახელა. იმის გათვალისწინებით, რომ ამ მიზნების მიღწევა სხვა, ნაკლებად ინვაზიური, პირად ცხოვრებაში გაუმართლებელი ჩარევის გამომრიცხავი მეთოდებით იყო შესაძლებელი, ხსენებულ სივრცეებში მუდმივი ვიდეომონიტორინგის განხორციელება ვერ შეფასდა მიზნის ადეკვატურ და პროპორციულ საშუალებად.

შემოწმებით დადგინდა, რომ სპეციალურ საგამოძიებო სამსახურს ვიდეომონიტორინგთან დაკავშირებული საკითხები დარეგულირებული ჰქონდა შესაბამისი ბრძანების საფუძველზე, თუმცა ეს უკანასკნელი სრულად არ შეიცავდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლის მე-2 პუნქტით განსაზღვრულ საკითხებს.

შესწავლის ფარგლებში ასევე გამოიკვეთა ვიდეომონიტორინგის სისტემის მეშვეობით დამუშავებული მონაცემის მიმართ მიღებული უსაფრთხოების ზომების ნაკლოვანებები. კერძოდ, სისტემაში წვდომის უფლების მქონე პირთა ნაწილი (სახელმწიფო დაცვის სამსახურის მხრიდან კანონმდებლობით დაკისრებული მივლენილი დაცვის თანამშრომლები) წვდომას ახორციელებდა საერთო მომხმარებლითა და პაროლით. ამდენად, მართალია, სისტემას ჰქონდა მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვის ელექტრონული ჟურნალი (ე. წ. „ლოგირება“), მაგრამ საერთო მომხმარებლითა და პაროლით სარგებლობის პირობებში ფაქტობრივად წარმოუდგენელია მონაცემთა სავარაუდო უკანონო დამუშავებაზე პასუხისმგებელი პირის იდენტიფიცირება.

ზემოაღნიშნულის გათვალისწინებით, სპეციალური საგამოძიებო სამსახური სამართალდამრღვევად იქნა ცნობილი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 69-ე და 76-ე მუხლების პირველი პუნქტების „ა“ ქვეპუნქტებით გათვალისწინებული ადმინისტრაციული სამართალდარღვევებისთვის. ასევე, ზემოხსენებული ნაკლოვანებების გამოსწორების მიზნით, მიეცა შესასრულებლად სავალდებულო 4 (ოთხი) დავალება.

დადებით ტენდენციად შეფასდა ის, რომ ვიდეო კამერების ხედვის არეალში ექცეოდა უწყებაში დასაქმებული პირების სამუშაო სივრცეებიც და ეს თანამშრომლები წერილობითი ფორმით იყვნენ ინფორმირებულნი მათი სამუშაო სივრცის ვიდეომონიტორინგის თაობაზე. რაც შეეხება სხვა მონაცემთა სუბიექტებს (სხვა დასაქმებული პირები, უწყების შენობაში მყოფი ნებისმიერი სხვა პირი),

კანონის მე-10 მუხლის მე-9 პუნქტის შესაბამისად, ასევე, ინფორმირებულნი იყვნენ ვიდეომონიტორინგის მიმდინარეობის თაობაზე თვალსაჩინო ადგილას განთავსებული შესაბამისი გამაფრთხილებელი ნიშნების მეშვეობით.

— საქართველოს თავდაცვის სამინისტრო

გეგმური შემოწმების (ინსპექტირების) ფარგლებში სამსახურმა შეისწავლა საქართველოს თავდაცვის სამინისტროს (შემდგომში — სამინისტრო) მიერ კანდიდატებთან გასაუბრების პროცესში განხორციელებული აუდიომონიტორინგის ფარგლებში მონაცემთა დამუშავების კანონიერების საკითხი.

შემოწმების ფარგლებში დადგინდა, რომ სამინისტრო, მონაცემთა სუბიექტის (კანდიდატის) წერილობითი თანხმობის შემთხვევაში, ახორციელებდა სამინისტროში დასაქმების მსურველ კანდიდატებთან ჩატარებული გასაუბრების პროცესის ვიდეო-აუდიო ჩაწერას.

დადგინდა, რომ კანდიდატების ინფორმირება ვიდეო-აუდიომონიტორინგის მიმდინარეობის თაობაზე ხდებოდა წერილობითი ფორმით მაშინ, როცა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლის მე-8 პუნქტი ვიდეომონიტორინგის მიმდინარეობის თაობაზე მონაცემთა სუბიექტის შესაბამისი გამაფრთხილებელი ნიშნით ინფორმირების იმპერატიულ ვალდებულებას ითვალისწინებს.

ზემოხსენებული ნაკლოვანების გამოსასწორებლად საქართველოს თავდაცვის სამინისტროს დაევალა ვიდეომონიტორინგის მიმდინარეობის თაობაზე მონაცემთა სუბიექტების „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლის მე-8 პუნქტის შესაბამისად ინფორმირება.

ე. მონაცემთა უსაფრთხოება

მონაცემთა მიმართ მიღებული უსაფრთხოების ზომების მნიშვნელობის გათვალისწინებითა და პერსონალურ მონაცემთა დაცვის სფეროში არსებული კანონმდებლობის ევროპულ სტანდარტებთან დაახლოების მიზნით, კანონის 2024 წლის პირველი მარტიდან მოქმედი რედაციით, მონაცემთა უსაფრთხოება მონაცემთა დამუშავების ერთ-ერთ პრინციპად იქნა აღიარებული, მსგავსად ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციისა“ (“GDPR”).

სამართალდამცავი ორგანოების ხელთ არსებულ მონაცემთა უკანონო დამუშავების შემთხვევაში შესაძლოა რა მონაცემთა სუბიექტს გამოუსწორებელი ზიანი მიადგეს, მათი მხრიდან მონაცემთა უსაფრთხოების ზომების მიღება კიდევ უფრო მეტ მნიშვნელობას იძენს.

მნიშვნელოვანია, უწყებებმა მუდმივად უზრუნველყონ მიღებული უსაფრთხოების ზომების მონიტორინგი და საჭიროების შემთხვევაში შეცვალონ დაცვის უფრო ეფექტიანი მექანიზმებით.

მონაცემთა უსაფრთხოება გულისხმობს ორგანიზაციული და ტექნიკური ზომების კუმულატიურად მიღების აუცილებლობას. ამდენად, თითოეული შემოწმების ფარგლებში მოწმდება მონაცემთა როგორც ფიზიკური, ასევე – ინფორმაციული (ელექტრონული სისტემების) უსაფრთხოება. მონაცემთა დამუშავების პროცესში მისაღები ზომების ნაწილი განსაზღვრულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლით, რომლის ჩამონათვალიც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ახალი რედაქციით გაფართოვდა.

მონაცემთა უსაფრთხოების მნიშვნელობის გათვალისწინებით, საანგარიშო პერიოდში სამსახურმა როგორც მოქალაქეთა მომართვების, ასევე გეგმური შემოწმებების ფარგლებში შეისწავლა არაერთი სამართალდამცავი ორგანოს (მათ შორის: საქართველოს გენერალური პროკურატურის, საქართველოს თავდაცვის სამინისტროს, დანაშაულის პრევენციის, არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის ეროვნული სააგენტოს, სპეციალური პენიტენციური სამსახურის) მიერ მონაცემთა მიმართ მიღებული ზომების „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილ მოთხოვნებთან შესაბამისობის საკითხები, რომელთა საფუძველზეც გამოიკვეთა არაერთი ნაკლოვანი პროცესი.

მონაცემთა უსაფრთხოების თვალსაზრისით, ყველაზე დიდ გამოწვევად რჩება მონაცემთა დამუშავებისთვის გამოყენებული ელექტრონულ სისტემებში მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვის, ელექტრონული ჟურნალისა (ე. წ. „ლოგირება“) და მონაცემებზე წვდომის უფლების მქონე პირებისთვის განპიროვნებული მომხმარებლისა და პაროლის არარსებობა. სამსახურის დადგენილი პრაქტიკითა და კანონმდებლობით იმპერატიულად განსაზღვრული რეგულირებით, ელექტრონული ფორმით დაცული მონაცემების უსაფრთხოების უზრუნველსაყოფად, მათი ადვილად ხელმისაწვდომობისა და მონაცემთა სავარაუდო უკანონო დამუშავებაზე პასუხისმგებელი პირის იდენტიფიცირების მიზნით, მნიშვნელოვანია, ელექტრონული ფორმით არსებული მონაცემების დამუშავების საშუალებას ჰქონდეს მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედების აღრიცხვის, მათ შორის – მონაცემების დამატების, დათვალიერების, რედაქტირების, წაშლის აღრიცხვის შესაძლებლობა. ამასთან, მონაცემებზე წვდომის უფლების მქონე პირები სარგებლობდნენ ინდივიდუალური მომხმარებლითა და პაროლით, რათა არ მოხდეს მონაცემების უკანონო მოპოვება, გამჟღავნება, გამოყენება, განადგურება და ა. შ.

საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის სამსახურს სამართალდამცავმა უწყებამ მომართა სავარაუდო ინციდენტის ფაქტთან დაკავშირებით, თუმცა სამსახურის მიერ ეს ფაქტი ინციდენტად არ იქნა მიჩნეული.[26]

საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის სამსახურმა სხვადასხვა სამართალდამცავ ორგანოში მონაცემთა უსაფრთხოების საკითხები 10

[26] ვრცლად მიმოხილულია საქართველოს თავდაცვის სამინისტროს მიერ კანდიდატებთან გასაუბრების პროცესში განხორციელებული აუდიომონიტორინგის ფარგლებში მონაცემთა დამუშავების კანონიერების საკითხის შესწავლასთან დაკავშირებით პერსონალურ მონაცემთა დაცვის სამსახურის მიერ მიღებული გადაწყვეტილების მოკლე ანალიზში.

(ათი) გეგმური, 1 (ერთი) არაგეგმური და 1 (ერთი) განცხადების განხილვის საფუძველზე დაწყებული წარმოების ფარგლებში შეისწავლა. უმეტეს შემთხვევაში უსაფრთხოების ზომებთან მიმართებით გამოვლინდა ზემოხსენებული ნაკლოვანებები, თუმცა თავისი შინაარსით განსაკუთრებით საყურადღებო იყო 3 (სამი) გეგმური შემოწმებისა და 1 (ერთი) განცხადების განხილვის ფარგლებში გამოვლენილი მონაცემთა უსაფრთხოების ზომების დარღვევებთან დაკავშირებული პერსონალურ მონაცემთა დაცვის სამსახურის შეფასებები. კერძოდ:

— დანაშაულის პრევენციის, არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის ეროვნული სააგენტო

საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის — დანაშაულის პრევენციის, არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის ეროვნული სააგენტოს (შემდგომში — სააგენტო) გეგმური შემოწმების ფარგლები მოიცავდა სააგენტოს მიერ შინაპატიმრობის მონიტორინგის ელექტრონული ზედამხედველობის სისტემის მეშვეობით მონაცემების დამუშავების კანონიერების საკითხის შესწავლას.

დადგინდა, რომ შინაპატიმრობის აღსრულების მიზნით გამოყენებული შინაპატიმრობის მონიტორინგის ელექტრონული ზედამხედველობის სისტემა სააგენტოს შესყიდული ჰქონდა ერთ-ერთი კერძო კომპანიისგან, რომელიც, როგორც დამუშავებაზე უფლებამოსილი პირი, შესაბამისი მომსახურების ხელშეკრულების საფუძველზე ახორციელებდა სისტემის ტექნიკურ მხარდაჭერას (ადმინისტრირებას).

მოპოვებული მტკიცებულებების ანალიზის საფუძველზე გაირკვა, რომ სააგენტოს თანამშრომლები შინაპატიმრობის მონიტორინგის ელექტრონული ზედამხედველობის სისტემაში დაცულ მონაცემებზე წვდომას ახორციელებდნენ განპიროვნებული მომხმარებლითა და პაროლით, თუმცა ისინი, საჭიროების ან/და სურვილის შემთხვევაში, მოკლებულნი იყვნენ პაროლის თავისი მხრიდან შეცვლის შესაძლებლობას. აღნიშნულს ახორციელებდა კონტრაქტორი კერძო კომპანია. ამდენად, მისთვის ცნობილი იყო სააგენტოს თითოეული თანამშრომლის მომხმარებლის პაროლი. გარდა ამისა, შინაპატიმრობის მონიტორინგის ელექტრონული ზედამხედველობის სისტემაში დაცული მონაცემების მიმართ შესრულებული მოქმედებები სრულად არ აღირიცხებოდა, ხოლო მონაცემთა ბაზასა და სერვერზე წვდომის უფლების მქონე პირები არ სარგებლობდნენ ინდივიდუალური მომხმარებლითა და პაროლით. ცხადია, ზემოხსენებული ხარვეზები მონაცემთა უსაფრთხოების ზომების დარღვევას წარმოადგენდა, პასუხისმგებლობის დაკისრების მიზნით, შეფასდა სააგენტოსა და კონტრაქტორ კომპანიას შორის დადებული ხელშეკრულებების პირობებისა და მხარეთა მიერ პასუხისმგებლობების გადანაწილების საკითხი.

შემოწმების ფარგლებში დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებული ხელშეკრულების

ანალიზის საფუძველზე გაირკვა, რომ ის, მართალია, შეიცავდა მონაცემთა უსაფრთხოების საკითხების შესახებ ზოგად დათქმებს, თუმცა დეტალურად არ იყო გაწერილი უსაფრთხოების ყველა ის ზომა, რომლებიც კონტრაქტორ კომპანიას უნდა მიეღო. შემოწმების ფარგლებში გამოიკვეთა, რომ სააგენტოს მხრიდან კონტრაქტორ კომპანიას მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვის ფუნქციონალის შექმნისა და მონაცემთა ბაზასა და სერვერზე ინდივიდუალური მომხმარებლითა და პაროლით წვდომის თაობაზე დავალება არ მისცემია. სააგენტოს არც მოგვიანებით მოუთხოვია გამოვლენილი ნაკლოვანებების გამოსწორება. შესაბამისად, სამსახურმა დაადგინა სააგენტოს მხრიდან „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლით გათვალისწინებული მოთხოვნების დარღვევის ფაქტი. იგი სამართალდამრღვევად იქნა ცნობილი ამავე კანონის 76-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში, რისთვისაც სახდელის სახით შეეფარდა ჯარიმა. ასევე, მიეცა დავალებები შემოწმების ფარგლებში გამოვლენილი დარღვევებისა და ნაკლოვანებების აღმოფხვრის მიზნით.

— საქართველოს პროკურატურა

პერსონალურ მონაცემთა დაცვის სამსახურმა, არასრულწლოვანთა ვიდეო-აუდიო ფიქსაციის პროცესში, საქართველოს პროკურატურის მიერ არასრულწლოვანთა სპეციალურ სივრცეებში გამოკითხვის მონაცემთა დამუშავების კანონიერების გეგმურად შემოწმების ფარგლებში დაადგინა:

საქართველოს პროკურატურას არასრულწლოვანთა გამოკითხვის მიზნით 8 (რვა) რაიონულ პროკურატურაში მოწყობილ არასრუწლოვანთა გამოკითხვის სპეციალიზებული ოთახში დამონტაჟებული იყო როგორც ვიდეოკამერები, ასევე – ხმოვანი სიგნალის ჩამწერი (აუდიოჩამწერი) მოწყობილობები, რომელთა მეშვეობითაც, შესაბამისი საჭიროებისას, ხდებოდა გამოკითხვის პროცესის ვიდეო-აუდიომონიტორინგი. ადგილზე შემოწმების ფარგლებში დადგინდა, რომ რამდენიმე რაიონული პროკურატურის შემთხვევაში ვიდეო-აუდიოჩაწერისთვის გამოყენებული ელექტრონული სისტემები სრულად არ აღრიცხავდა მონაცემთა მიმართ შესრულებულ მოქმედებებს ან აღრიცხავდა, თუმცა ვიდეო-აუდიოჩანაწერის წაშლის შედეგად (ე. წ. „ლოგ“ ჩანაწერებიც იშლებოდა). ამასთან, სისტემაში ავტორიზაციისა და მონიტორინგის განხორციელებისთვის, შექმნილი იყო მხოლოდ 1 (ერთი) მომხმარებელი, რომლითაც სარგებლობდნენ წვდომის უფლების მქონე პირები (თითოეული რაიონული პროკურატურის შემთხვევაში ასეთი რამდენიმე პირი). გარკვეულ შემთხვევებში მომხმარებლისა და პაროლის გაზიარება ხდებოდა დისტანციურ ფორმატში — სატელეფონო კომუნიკაციის გზით.

ასეთ პირობებში იზრდებოდა რა მონაცემთა უკანონო დამუშავების რისკები, პერსონალურ მონაცემთა დაცვის სამსახურმა აღნიშნული გარემოებები შეაფასა მონაცემთა უსაფრთხოებისთვის დადგენილი მოთხოვნების დარღვევად და საქართველოს პროკურატურა სამართალდამრღვევად ცნო „პერსონალურ

მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 76-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში. შემოწმების ფარგლებში გამოვლენილი დარღვევებისა და ნაკლოვანებების აღმოფხვრის მიზნით საქართველოს პროკურატურას მიეცა შესაბამისი დავალებები (სამსახურის უფროსის აღნიშნული გადაწყვეტილება გასაჩივრებულია).

— სპეციალური პენიტენციური სამსახური

პერსონალურ მონაცემთა დაცვის სამსახურმა მოქალაქის განცხადების საფუძველზე შეისწავლა საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი სახელმწიფო საქვეუწყებო დაწესებულების — სპეციალური პენიტენციური სამსახურის მიერ განმცხადებლის პერსონალური მონაცემების შემცველი ინფორმაციის, „Gmail“-ის პლატფორმაზე შექმნილი ელექტრონული ფოსტის მეშვეობით, დამუშავების პროცესში მონაცემთა უსაფრთხოების საკითხი.

განცხადების განხილვის ფარგლებში გამოიკვეთა, რომ თბილისის სააპელაციო სასამართლოში მიმდინარეობდა ადმინისტრაციული დავა, რომელშიც მხარეებად ჩართულნი იყვნენ განმცხადებელი და პენიტენციური სამსახური. პენიტენციური სამსახურის თანამშრომელმა, უშუალო ხელმძღვანელებთან შეთანხმების საფუძველზე, დროის სიმცირისა და რესურსის დაზოგვის მიზნით, სააპელაციო შესაგებელი გააგზავნა „Gmail“-ის პლატფორმაზე სამსახურებრივი მიზნებისთვის შექმნილი ელექტრონული ფოსტის საშუალებით. პენიტენციურმა სამსახურმა განმარტა, რომ მსგავსი ფორმით დოკუმენტაციის სასამართლოში წარდგენა დადგენილ პრაქტიკას წარმოადგენს, თუმცა აქვე მიუთითა, რომ აღნიშნული ელექტრონული ფოსტის მისამართები გამოიყენება მხოლოდ სამსახურებრივი მიზნებისთვის.

პერსონალურ მონაცემთა დაცვის სამსახურმა განმარტა, რომ „Gmail“ პლატფორმაზე შექმნილი ელექტრონული ფოსტის საშუალებით უწყების თანამშრომლების მიერ ერთმანეთსა თუ გარე უწყებებთან პროფესიულ საქმიანობასთან დაკავშირებული ინფორმაციის მიმოცვლა პრობლემური და რისკების შემცველია, ვინაიდან აღნიშნული ელექტრონული სისტემა დასაქმებულებს მონაცემებზე წვდომის შესაძლებლობას სხვა ელექტრონული მოწყობილობებიდანაც აძლევს და უწყება მოკლებულია შესაძლებლობას, აკონტროლოს და დაიცვას მასში დაცული ინფორმაცია. ამასთან, იმის გამო, რომ მონაცემებზე წვდომის შესაძლებლობა დასაქმებულ პირებს უნარჩუნდებათ დამუშავებისთვის პასუხისმგებელ პირთან სამსახურებრივი (შრომითი) კავშირის შეწყვეტის შემდეგაც, არსებობს მონაცემთა მიმართ უსაფრთხოების ზომების დარღვევის საშიშროება.

აღნიშნული გარემოებების საფუძველზე, პენიტენციური სამსახური სამართალდამრღვევად იქნა ცნობილი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 76-ე მუხლის პირველი პუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში და სახდელის სახით შეეფარდა გაფრთხილება. მასვე დაევალა, მიეღო შესაძლო და თანამდევი საფრთხეების შესაბამისი ის ორგანიზაციული და ტექნიკური ზომები, რომლებიც,

ელექტრონული ფორმით მონაცემების დამუშავების პროცესში უზრუნველყოფდა მონაცემთა დაცვას მონაცემთა დაკარგვისგან, უკანონო დამუშავებისგან, მათ შორის – განადგურებისგან, წაშლისგან, შეცვლისგან, გამჟღავნებისგან ან გამოყენებისგან.

— საქართველოს თავდაცვის სამინისტრო

სხვა არაერთი შემოწმების მსგავსად, მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვის ელექტრონული ჟურნალის (ე. წ. „ლოგირება“) არარსებობის პრობლემა გამოიკვეთა საქართველოს თავდაცვის სამინისტროს (შემდგომში — სამინისტრო) გეგმური შემოწმების პროცესშიც, სამინისტროს მიერ კანდიდატებთან გასაუბრების პროცესში განხორციელებული აუდიომონიტორინგის ფარგლებში მონაცემთა დამუშავების კანონიერების საკითხის შესწავლისას.

გადაწყვეტილება ყურადსაღებია კონკრეტული უსაფრთხოების ზომების დარღვევის ინციდენტად კვალიფიცირების თვალსაზრისით. შემოწმების ფარგლებში დადგინდა, რომ კანდიდატის წინასწარი წერილობითი თანხმობის შემთხვევაში სამინისტრო ახდენდა გასაუბრების პროცესის ვიდეო-აუდიოჩაწერას. პროცესი აგებული იყო შემდეგნაირად — კანდიდატი გასაუბრებაზე შესვლამდე წერილობითი ფორმით აცხადებდა თანხმობას/უარს მისი გასაუბრების პროცესის ვიდეო-აუდიოჩაწერასთან დაკავშირებით, რის შემდგომაც სამინისტროს თანამშრომელი (რომელიც უშუალოდ უზრუნველყოფდა კანდიდატისგან თანხმობის მიღებას) საკონკურსო კომისიას აწვდიდა ინფორმაციას სუბიექტის მიერ გაცხადებული თანხმობის/უარის თაობაზე. სამინისტროში არსებულ ვაკანტურ პოზიციაზე გამოცხადებული ერთ-ერთი გასაუბრების ფარგლებში კანდიდატმა წერილობითი ფორმით უარი განაცხადა თავისი გასაუბრების პროცესის ვიდეო-აუდიოჩაწერაზე. სამინისტროს თანამშრომელმა შემთხვევით (ადამიანური შეცდომა), საკონკურსო კომისიის წევრებს მიაწოდა მცდარი ინფორმაცია — თითქოს კანდიდატს თანხმობა ჰქონდა გაცხადებული. ამდენად, განხორციელდა კანდიდატის გასაუბრების ვიდეო-აუდიო ჩაწერა. სამინისტრომ აღნიშნული ფაქტი აღმოაჩინეს მოგვიანებით და ვინაიდან ხსენებული ვიდეო-ჩანაწერი კვლავ ინახებოდა, სამინისტრომ ინციდენტად მიიჩნია ის და გეგმური შემოწმების ფარგლებში წარმოადგინა ინფორმაცია.

პერსონალურ მონაცემთა დაცვის სამსახურმა, სამსახურის უფროსის 2024 წლის 28 თებერვლის №19 ბრძანებით დამტკიცებული „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმები და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესზე“ დაყრდნობით, დაადგინა, რომ სამინისტროს მიერ წარმოდგენილი ფაქტი არ შეიცავდა ინციდენტის განმსაზღვრელ კრიტერიუმებს(მონაცემთა კონფიდენციალურობის, მთლიანობის ან/და ხელმისაწვდომობის დარღვევა). იგი შეფასდა მონაცემთა უსაფრთხოების ორგანიზაციული ზომების (თანხმობის მიღებაზე პასუხისმგებელი პირისა და საკონკურსო კომისიის მდივანს შორის ინფორმაციის გაცვლის წესი) დარღვევად, რადგან საკონკურსო კომისიის წევრებისთვის ინფორმაციის მიწოდების

სამინისტროს მიერ შემუშავებული კომუნიკაციის ორგანიზაციული ფორმა საკმარისი არ აღმოჩნდა ადამიანური შეცდომის გამოსარიცხად.

შემოწმების ფარგლებში სამინისტრო სამართალდამრღვევად იქნა ცნობილი 76-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში, სახდელის სახით განესაზღვრა გაფრთხილება და მიეცა შესაბამისი დავალებები.

3.3. დავალებები და რეკომენდაციები

სამსახურის მიერ შესწავლილი საქმეების, გამოვლენილი ნაკლოვანი პროცესების, სპეციფიკისა და ტენდენციების გათვალისწინებით:

- სამართალდამცავმა ორგანოებმა უნდა გაატარონ ისეთი ღონისძიებები, რომლებიც გამორიცხავს მონაცემთა სუბიექტების მოთხოვნების რეალიზების გაჭიანურების რისკებს;
- ისეთ შემთხვევებში, როდესაც მონაცემთა სუბიექტის უფლებების რეალიზების მოთხოვნით წარდგენილი განცხადებიდან ან სხვა კორესპონდენციიდან ვერ ხერხდება მონაცემთა სუბიექტის იდენტიფიცირება, ხარვეზის შესახებ განმცხადებლის ინფორმირება მოახდინონ დაუყოვნებლივ, პირველივე შესაძლებლობისთანავე, რათა თავიდან იქნეს აცილებული განცხადების განხილვის ძირითადი ვადისა და, შესაბამისად, კანონით დადგენილ ვადაში საბოლოო შედეგის შესახებ ინფორმირება;
- ყურადღებით შეაფასონ სუბიექტის მოთხოვნა, რათა სრულყოფილად გადასცენ მისთვის კანონით უზრუნველყოფილი უფლებით დაცული საქმის მასალა და დოკუმენტაცია; მონაცემთა სუბიექტის უფლების შეზღუდვის შემთხვევაში შეზღუდვის მიზნის დაზიანების გარეშე, პროპორციულობის პრინციპის დაცვით, უზრუნველყონ სუბიექტის ინფორმირების უფლების რეალიზება;
- მონაცემთა დამუშავების ფაქტის არარსებობისა თუ მოთხოვნის დაკმაყოფილებაზე უარის შემთხვევებში უზრუნველყონ უარის ან შეზღუდვის შესაბამისი კანონით გათვალისწინებული საფუძვლის მითითებით დასაბუთებული ინფორმაციის მიწოდება;
- სუბიექტის წერილობითი თანხმობის საფუძველზე მონაცემების დამუშავების შემთხვევაში დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ წერილობითი თანხმობის ფორმის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნებთან შესაბამისობა;
- დამსაქმებლებმა უნდა შეაფასონ სამსახურებრივი შემოწმების დროს გამოკითხვის პროცესში დასამუშავებელი მონაცემების მიზნობრიობა და გამოსაკითხი ფორმების ველების მეშვეობით დაამუშაონ მხოლოდ იმ მოცულობის მონაცემები, რომლებიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად, ხოლო საქმის ინდივიდუალური

თავისებურებების გათვალისწინებით აუცილებელი სხვა მონაცემები მოიპოვონ უშუალოდ ახსნა-განმარტების შინაარსის მეშვეობით, ყოველ კონკრეტულ შემთხვევაში არსებული საჭიროების შესაბამისად;

— დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა განსაზღვრონ სამსახურებრივი შემოწმების ფარგლებში დამუშავებული მონაცემების კონკრეტული მიზნით შენახვის ვადები და შენახვის ვადის ამოწურვის შემდგომ მონაცემთა მიმართ განსახორციელებელი მოქმედებები. ასევე, უზრუნველყონ აღნიშნულ ვადაზე უფრო ხანგრძლივად შენახული მონაცემების წაშალა/განადგურება;
— სამართალდამცავმა ორგანოებმა ვიდეო-აუდიომონიტორინგი უნდა განახორციელონ მხოლოდ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი მიზნების მისაღწევად და მოცულობისა და პროპორციულობის დაცვით განსაზღვრონ ვიდეო-აუდიომონიტორინგის ხანგრძლივობა;
— იმ სივრცეში, რომლის ვიდეო-აუდიომონიტორინგიც ხორციელდება, თვალსაჩინო ადგილზე განათავსონ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში მითითებული აღწერილობითა და სრულყოფილი მონაცემების დატანით გამაფრთხილებელი ნიშნები იქ და იმგვარად, რომ მონაცემთა სუბიექტს არ შეექმნას მცდარი წარმოდგენა ვიდეო-აუდიომონიტორინგის განხორციელებასთან დაკავშირებით (დროისა და საჭიროების გათვალისწინებით);
— ვიდეო-აუდიოჩანაწერების მესამე პირებისთვის გადაცემისას იხელმძღვანელონ შესაბამისი კანონის მოთხოვნების დაცვით კანონითვე მკაცრად განსაზღვრულ შემთხვევაში;
— წინასწარ უზრუნველყონ ვიდეო-აუდიომონიტორინგის მიმდინარეობის თაობაზე წერილობითი დოკუმენტის შემუშავება, რომელშიც ასახული იქნება ვიდეო-აუდიომონიტორინგის მიზანი და მოცულობა, ვიდეო-აუდიომონიტორინგის ხანგრძლივობა და მათი შენახვის ვადა, ჩანაწერების წვდომის, მისი შენახვისა და განადგურების წესი და პირობები, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმები;
— უზრუნველყონ მონაცემთა დამუშავების პროცესებთან დაკავშირებული ინფორმაციის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლის შესაბამისად აღრიცხვა;
— მონაცემთა დამუშავების პროცესში დამუშავებაზე უფლებამოსილი პირის ჩართულობის შემთხვევაში ამ უკანასკნელს მიეწოდოს დეტალური დავალება მონაცემთა უსაფრთხოების ზომების თაობაზე. ამასთან, უზრუნველყოს დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავების პროცესების მუდმივი მონიტორინგი;
— მონაცემებზე წვდომა იყოს შეზღუდული და გამომდინარეობდეს კონკრეტული თანამშრომლების სამსახურებრივი უფლებამოსილების განხორციელების პროცესში არსებული საჭიროებებიდან;
— არაავტომატური საშუალებებით მონაცემთა დამუშავებისას უზრუნველყოფილი იყოს მონაცემთა ფიზიკური უსაფრთხოება (მაგ., შენახულ იქნეს საკეტით დაცულ კარადაში; იმ სივრცეში, სადაც

განთავსებულია დოკუმენტაცია, შეზღუდული იყოს თანამშრომელთა შესვლა, კარი იკეტებოდეს საკეტით და სხვა);

— ავტომატური საშუალებებით მონაცემთა დამუშავებისას, მათ შორის, ვიდეო-აუდიომონიტორინგის განხორციელებისას, გამოყენებულ იქნეს ისეთი ელექტრონული სისტემები, რომელთა მეშვეობითაც შესაძლებელია მონაცემთა მიმართ შესრულებული ყველა მოქმედების აღრიცხვა, რათა შესაძლებელი იყოს კონკრეტულ ქმედებაზე პასუხისმგებელი პირის იდენტიფიცირება;

— ელექტრონულ სისტემაში, მათ შორის, ვიდეო-აუდიომონიტორინგის განხორციელებისას გამოყენებულ ტექნიკურ საშუალებაში, დაცულ მონაცემებზე წვდომის უფლების მქონე პირებს დაშვება ჰქონდეთ მხოლოდ ინდივიდუალური მომხმარებლისა და პაროლის გამოყენებით;

— შეიმუშაონ პაროლების მართვის პოლიტიკა, რომლის გათვალისწინებითაც, სისტემებში არსებული მონაცემები დაცული იქნება მაქსიმალურად რთული და კომპლექსური პაროლებით;

— ელექტრონულ სისტემაში წვდომის უფლების მქონე თითოეულ პირს გააჩნდეს მისთვის მინიჭებული მომხმარებლის პირველადი პაროლის შეცვლის ტექნიკური შესაძლებლობა და ვალდებულება.

4. მონაცემთა დამუშავების კანონიერების გეგმური შემოწმებები

4.1. მნიშვნელოვანი მიმართულებები და ტენდენციები

პერსონალურ მონაცემთა დამუშავების კანონიერების გეგმური შემოწმება (ინსპექტირება) ხორციელდება პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მიერ დამტკიცებული შემოწმებების წლიური გეგმის შესაბამისად. შემოწმებების წლიური გეგმის შემუშავების მიზანია მონაცემთა დამუშავების პროცესების მრავალფეროვნების, დინამიურობისა და კომპლექსურობის გათვალისწინებით, სამსახურის საქმიანობის ეფექტიანობისა და თანმიმდევრულობის უზრუნველყოფა.

აღსანიშნავია, რომ წლიური გეგმა შემუშავდება მონაცემთა დაცვის მომწესრიგებელი კანონმდებლობისა და პერსონალურ მონაცემთა დაცვის სამსახურის პრაქტიკის შესწავლის, აგრეთვე, საქართველოს სხვადასხვა რეგიონებში პრიორიტეტული ან/და მაღალრისკიანი მონაცემთა დამუშავების პროცესების იდენტიფიცირებისა და მათი ანალიზის შედეგების საფუძველზე. მონაცემთა დამუშავების პროცესში ადამიანის უფლებებისა და თავისუფლებების დარღვევის მაღალი ალბათობის შემცველი რისკების განსაზღვრისას, სამსახური ხელმძღვანელობს „პერსონალურ მონაცემთა დამუშავების კანონიერების გეგმური შემოწმებების (ინსპექტირება) გეგმის შემუშავების მეთოდოლოგიით“, რომელიც ადგენს მონაცემთა დამუშავების კანონიერების შესწავლის მიზნით საჯარო და კერძო სექტორის წარმომადგენელი უწყებების თუ ორგანიზაციების შერჩევის პროცედურასა და კრიტერიუმებს. მისი გათვალისწინებით შემუშავდა და პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 18 იანვრის №ბ/0046-2024 ბრძანებით დამტკიცდა პერსონალურ მონაცემთა დამუშავების კანონიერების გეგმური შემოწმებების (ინსპექტირება) 2024 წლის ძირითადი მიმართულებები და გეგმა.

საგულისხმოა, რომ საანგარიშო პერიოდში მონაცემთა დამუშავების გეგმურად შესწავლილი პროცესების საფუძველზე არაერთი მნიშვნელოვანი მიმართულება და ტენდენცია იქნა გამოვლენილი. კერძოდ:

ა. მოწყვლადი ჯგუფებისა და ახალგაზრდების მონაცემების დამუშავება

შეზღუდული შესაძლებლობების მქონე (შშმ) პირების მონაცემთა დამუშავების პროცესები ხშირ შემთხვევებში ითვალისწინებს ჯანმრთელობასთან დაკავშირებული განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავდებას. კერძოდ, შშმ პირების შესახებ ინფორმაცია ხშირად მოიცავს სუბიექტის ფიზიკური და მენტალური ჯანმრთელობის მდგომარეობის შესახებ მონაცემებს, რაც ხასიათდება სენსიტიური ბუნებით და დაცვის მაღალ სტანდარტს საჭიროებს. რაც შეეხება არასრულწლოვნებსა და ახალგაზრდებს, მათთვის შესაძლოა ნაკლებად იყოს ცნობილი ის რისკები, შედეგები, სამართლებრივი დაცვის მექანიზმები და უფლებები, რომლებიც უკავშირდება მათი პერსონალური

მონაცემების დამუშავებას. ამასთან, მონაცემების კანონდარღვევით დამუშავებამ შესაძლოა გამოიწვიოს არასრულწლოვანთა ღირსების შელახვა, სტიგმატიზაცია, ბულინგი, დისკრიმინაცია ან/და სხვა სახის ნეგატიური გავლენა იქონიოს არასრულწლოვნის ემოციურ მდგომარეობასა და მის შემდგომ განვითარებაზე. შესაბამისად, შშმ პირების, არასრულწლოვნებისა და ახალგაზრდების დაცვა საფრთხეებისგან და მათ მხარდაჭერაზე ორიენტირებული სამართლებრივი გარემოს შექმნა უაღრესად მნიშვნელოვანია მათი უფლებების რეალიზაციისთვის. სხვადასხვა საჯარო უწყებებისა და კერძო ორგანიზაციების მიერ ამ კატეგორიის მონაცემთა სუბიექტების პერსონალური მონაცემების დამუშავების პროცესებში 2024 წელს სამსახურის მიერ გეგმურად შესწავლილ საქმეებში გამოვლინდა მნიშვნელოვანი დარღვევები და ნაკლოვანებები.

კერძოდ, სკოლებსა და პროფესიულ საგანმანათლებლო დაწესებულებებში (კოლეჯებში) ვიდეომონიტორინგის განხორციელებისას ხშირია შემთხვევები, როდესაც კონკრეტული შენობა-ნაგებობის შიდა ან გარე პერიმეტრზე ვიდეომონიტორინგის სივრცეებში კანონით გათვალისწინებული გამაფრთხილებელი ნიშნები არასაკმარისი ოდენობით, ან საერთოდ არ არის განთავსებული; ის გამაფრთხილებელი ნიშნები კი, რომლებიც განთავსებულია, არ აკმაყოფილებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლის მე-9 პუნქტით გათვალისწინებულ მოთხოვნებს (კერძოდ, ხშირ შემთხვევაში არ შეიცავს დამუშავებისთვის პასუხისმგებელი პირის სახელწოდებასა და მის საკონტაქტო მონაცემებს). აღსანიშნავია, რომ მონაცემთა სუბიექტების უფლებების რეალიზების მიზნით დამუშავებისთვის პასუხისმგებელი პირი/დამუშავებაზე უფლებამოსილი პირი ვალდებულია იმგვარად განათავსოს ვიდეომონიტორინგის მიმდინარეობის შესახებ გამაფრთხილებელი ნიშნები, რომ მასზე დატანილი წარწერა და გამოსახულება აღქმადი იყოს ვიდეომონიტორინგის სივრცეში მოხვედრილი ნებისმიერი ფიზიკური პირისთვის. ამასთან, მონაცემთა სუბიექტების ინფორმირებულობის თვალსაზრისით, გამაფრთხილებელი ნიშნის თვალსაჩინო ადგილას განთავსების გარდა, მნიშვნელოვანია, აღნიშნული ნიშნები იყოს მარტივად აღქმადი (მაგალითად, გასათვალისწინებელია წარწერის ზომა, ფერი) და აკმაყოფილებდეს კანონის ზემოხსენებული ნორმის მოთხოვნებს.

სკოლებსა და პროფესიულ საგანმანათლებლო დაწესებულებებში (კოლეჯებში) მრავლად არის დამონტაჟებული ისეთი ვიდეოკამერები, რომლებიც არ არის დაკავშირებული ვიდეოჩამწერ მოწყობილობასთან და არ ფუნქციონირებს. ნიშანდობლივია, რომ ვიდეოკამერის განთავსების ფაქტი, თუნდაც ვიდეოჩაწერის განხორციელების გარეშე, ქმნის მონაცემთა სუბიექტის მცდარ წარმოდგენას მისი პერსონალური მონაცემების დამუშავების თაობაზე. აღნიშნულის საფუძველზე მონაცემთა სუბიექტს უყალიბდება მისი პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევის ცრუ მოლოდინი.

საანგარიშო პერიოდში გამოვლინდა შემთხვევა, როცა ვიდეომონიტორინგთან ერთად სკოლაში ასევე ხორციელდებოდა აუდიომონიტორინგიც, რომლის თაობაზეც ინფორმაციას არ ფლობდა არც სკოლა და არც ვიდეოსათვალთვალო სისტემაზე კონტროლის განმახორციელებელი დაწესებულება (სსიპ — „საგანმანათლებლო დაწესებულების მანდატურის სამსახური“). შესაბამისად,

მნიშვნელოვანი მოცულობის პერსონალური მონაცემების შემცველი აუდიოჩანაწერები უკანონოდ მუშავდებოდა.

გარკვეულ შემთხვევებში სკოლებში/კოლეჯებში ვიდეომონიტორინგი მიმდინარეობს სასწავლო სივრცეებში (საკლასო ოთახებში/სასწავლო აუდიტორიებში). აღსანიშნავია, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები შემოწმებების ფარგლებში ამგვარი სივრცეების მონიტორინგის მიზნად მიუთითებდნენ პირთა უსაფრთხოების უზრუნველყოფას, საკუთრების დაცვასა და ზიანის ანაზღაურებაზე პასუხისმგებელი პირის იდენტიფიცირების ინტერესს; თუმცა ნიშანდობლივია, რომ საკლასო ოთახები/აუდიტორიები, საკუთარი ფუნქციური დატვირთვიდან გამომდინარე, წარმოადგენს სტუდენტებისთვის სასწავლო და პედაგოგებისთვის სამუშაო სივრცეს, სადაც მათ შორის კომუნიკაციის საგანს არა მხოლოდ უშუალოდ დარგობრივი სასწავლო, არამედ სხვა, პირადი და ზოგადი ხასიათის საკითხებიცაა (მაგალითად, შესვენების პერიოდში პირადი ხასიათის კომუნიკაცია სტუდენტებთან ან პირადი მიზნით სხვადასხვა აქტივობის განხორციელება). გარდა სწავლებისა, პედაგოგები აღნიშნულ სივრცეში კომუნიკაციას ამყარებენ სტუდენტებთან, რაც უმნიშვნელოვანესია პიროვნების თავისუფალი განვითარების უფლების რეალიზაციისათვის და ექცევა პირადი ცხოვრების უფლებით დაცულ სფეროში; მონაცემთა სუბიექტის პირადი ცხოვრების სფეროში ჩარევა კი უნდა განხორციელდეს თანაზომიერების პრინციპის დაცვით. ასევე, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ დასახელებული მიზნების მიღწევა შესაძლებელია სხვა ისეთი საშუალებებითაც, რომლებიც მონაცემთა სუბიექტების პირადი ცხოვრების სფეროში ნაკლებ ჩარევას გამოიწვევს.

რიგ შემთხვევებში სკოლები და უნივერსიტეტები არასრულწლოვნების/ახალგაზრდების (მათ შორის, შშმ პირის) მონაცემებს ინახავდნენ მუდმივად, ვინაიდან არ ჰქონდათ განსაზღვრული მონაცემთა შენახვის ვადები და ამ ვადების ამოწურვის შემდგომ მონაცემთა მიმართ განსახორციელებელი ღონისძიებები. ასეთი ინფორმაციის განუსაზღვრელი ვადით შენახვა, ერთი მხრივ, არ შეესაბამება კანონის მე-4 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტით გათვალისწინებულ პრინციპს, მეორე მხრივ კი, მონაცემთა ხანგრძლივად და უვადოდ შენახვის შემთხვევაში იზრდება მასზე არასანქცირებული წვდომის, მონაცემთა დამუშავების წესების დარღვევის ან მათი გაჟონვის რისკი. ასევე გამოვლინდა შემთხვევა, როდესაც ელექტრონული ფორმით არსებული მონაცემების შენახვისთვის გათვალისწინებული ვადის გასვლის შემდგომ ეს მონაცემები იშლებოდა მექანიკურად (ხელით). გასათვალისწინებელია, რომ ჩანაწერების არაავტომატურად (ხელით) წაშლის შემთხვევაში (მით უფრო მოცულობითი მონაცემებთან მიმართებით), ადამიანური ჩართულობის მუდმივი საჭიროებიდან გამომდინარე, არსებობს შეცდომების და, შესაბამისად, მონაცემთა არამართლზომიერი დამუშავების მომეტებული რისკები.

ამასთანავე, გამოვლინდა მუნიციპალური ორგანოებისა და საგანმანათლებლო დაწესებულებების მიერ ვებგვერდებზე ან/და სოციალური ქსელის გვერდებზე არასრულწლოვნებისა და ახალგაზრდების მონაცემების უკანონო გამოქვეყნების შემთხვევები (მაგალითად: უნივერსიტეტის მიერ გამოცდაზე დაშვებული სტუდენტების სია და მათ მიერ მიღებული შედეგები;

საბავშვო ბაღებში სარეგისტრაციო პორტალზე რეგისტრირებული ბაღების აღსაზრდელთა პერსონალური მონაცემები; განათლების მუნიციპალური პროგრამების ბენეფიციარების მონაცემები). ნიშანდობლივია, რომ ხშირ შემთხვევაში დამუშავებისთვის პასუხისმგებელი პირები მონაცემთა გამოქვეყნების საფუძვლად მიუთითებდნენ მონაცემთა სუბიექტის თანხმობის არსებობაზე, თუმცა მათ ვერ შეძლეს აღნიშნულის კანონის მოთხოვნათა შესაბამისად მოპოვების ფაქტის დადასტურება. ამასთან, ზემოხსენებულ შემთხვევებში ვერ დასაბუთდა მონაცემთა გამჟღავნების ლეგიტიმური მიზნების არსებობაც.

სამსახურის მიერ ჩატარებულმა შემოწმებებმა ცხადყო, რომ სკოლებს, კოლეჯებს, უნივერსიტეტებსა და მუნიციპალიტეტებს ხშირ შემთხვევაში არ აქვთ მიღებული ახალგაზრდების, არასრულწლოვნებისა და შშმ პირების ელექტრონული და მატერიალური ფორმის მონაცემების უსაფრთხოებისთვის საჭირო ორგანიზაციულ-ტექნიკური ზომები. კერძოდ, გამოიკვეთა შემთხვევები, როდესაც მატერიალური ფორმით დამუშავებული მონაცემები შენახული იყო იმ ფორმით, რომლითაც ის ხელმისაწვდომი ხდებოდა არაუფლებამოსილი პირებისთვის; ელექტრონული ფორმით არსებული მონაცემების მიმართ კი ორგანიზაციები არ აღრიცხავენ ან არასრულად აღრიცხავენ (მათ შორის, მონაცემთა ბაზაზე პირდაპირი წვდომის შემთხვევაში) მონაცემების მიმართ შესრულებულ მოქმედებებს. ხშირ შემთხვევაში, მონაცემებზე წვდომის მიზნით, ელექტრონულ სისტემებში არ არის შექმნილი ინდივიდუალური მომხმარებლის ანგარიშები, ხოლო მის ნაცვლად გამოიყენება საერთო მომხმარებლის ანგარიში და პაროლი.

დაფიქსირდა შემთხვევები, როდესაც ელექტრონულ სისტემას არ ჰქონდა რთული (კომპლექსური) ტიპის პაროლები, რომლებიც არ ინახებოდა დაშიფრული ფორმით. ამასთანავე, ელექტრონულ სისტემაში პაროლის შეცვლა არ შეეძლო თავად მომხმარებელს და ამისათვის მას უნდა მიემართა სისტემის ადმინისტრატორისთვის. ასევე გამოიკვეთა, რომ ზოგიერთი დაწესებულების თანამშრომლები, საკუთარი სამსახურებრივი ფუნქცია-მოვალეობების განხორციელების პროცესში, იყენებენ პირად ელექტრონულ ფოსტებს და მათი მეშვეობით ამუშავებდნენ არასრულწლოვანი ბენეფიციარების შესახებ მოპოვებულ მონაცემებს. ამასთან, გამოიკვეთა მონაცემებზე წვდომის შემთხვევები იმ პირების მხრიდან, რომლებსაც აღნიშნული წვდომა არ ესაჭიროებათ საკუთარი სამსახურებრივი მოვალეობების განსახორციელებლად; აღნიშნული გარემოებები კი, განსაკუთრებით მონაცემთა სენსიტიური ბუნების გათვალისწინებით, ქმნის მონაცემთა კანონდარღვევით დამუშავებისა და მათი არასამსახურებრივი მიზნით გამოყენების რისკებს.

ბ. შრომითი ურთიერთობის ფარგლებში მონაცემების დამუშავება

შრომითი და მისი თანმდევი ურთიერთობის ფარგლებში დამსაქმებლები აგროვებენ სხვადასხვა კატეგორიისა და მოცულობის პერსონალურ მონაცემებს. შრომითი ურთიერთობის შინაარსის გათვალისწინებით, დამსაქმებელს ხელი მიუწვდება დასაქმებულის სენსიტიურ მონაცემებზე და აქვს მათი გამოყენების რეალური მექანიზმები. ამასთანავე, შრომის ორგანიზაციული მოწესრიგების

პირობებში, შრომითსამართლებრივი ურთიერთობის სუბორდინაციის გათვალისწინებითა და ეკონომიკური თვალსაზრისით, დასაქმებული მნიშვნელოვნად დამოკიდებულია დამსაქმებელზე, რის გამოც დასაქმებულთა პერსონალური მონაცემების დამუშავება საჭიროებს განსაკუთრებულ დაცვას, ამის გამო აღნიშნულ პროცესში ორგანიზაციებმა უნდა იმოქმედონ დასაქმებულებისა და დასაქმების მსურველ პირთა ინტერესების გათვალისწინებით. სამსახურის მიერ გეგმურად შესწავლილი საქმეები ადასტურებს, რომ სხვადასხვა საჯარო უწყებისა და კერძო ორგანიზაციის მიერ შრომითი ურთიერთობის ფარგლებში მონაცემების დამუშავების პროცესში ვლინდება გარკვეული დარღვევები და ნაკლოვანებები:

ცალკეულ შემთხვევებში ორგანიზაციებს, შესაბამისი სამართლებრივი საფუძვლის გარეშე, საკუთარ ვებგვერდებზე გამოქვეყნებული ჰქონდათ შრომითი ურთიერთობის ფარგლებში გამოცემული ისეთი სამართლებრივი აქტები, როგორებიცაა: დასაქმებული პირების შვებულების, მივლინების, თანამდებობაზე დანიშვნის, თანამდებობიდან გათავისუფლების, დისციპლინური პასუხისმგებლობის ზომის შეფარდების თაობაზე და სხვა. აღნიშნულ აქტებში მითითებული იყო დასაქმებული პირების სახელი და გვარი, რაც იმთავითვე იძლეოდა მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობას, აღნიშნული შინაარსის აქტებს კი ორგანიზაციების უმრავლესობა პროაქტიულად გამოსაქვეყნებელ საჯარო ინფორმაციად მიიჩნევდა.

გამოვლინდა შემთხვევა, როცა ერთ-ერთი ორგანიზაცია მონაცემთა მინიმიზაციის პრინციპის დარღვევით 2362 (ორი ათას სამას სამოცდაორი) დამსაქმებელს ანიჭებდა წვდომას დასაქმებულების/პოტენციური დასაქმებულების ისეთ მონაცემებზეც, რომლებიც დამსაქმებლებს საქმიანობის განხორციელებისთვის არ ესაჭიროებოდათ.

კანონის მე-10 მუხლის მე-3 პუნქტის მოთხოვნათა დარღვევით, რიგ შემთხვევებში გამოვლინდა დასაქმებული პირების სამუშაო პროცესის/სივრცის ვიდეომონიტორინგის განხორციელების ფაქტები. შემოწმებების ფარგლებში დამუშავებისთვის პასუხისმგებელი პირების მიერ დასახელებული საკუთრებისა და უსაფრთხოების დაცვის მიზანი არ იქნა მიჩნეული ვიდეომონიტორინგის განხორციელების კანონიერების წინაპირობად ისეთ შემთხვევებში, როცა აღნიშნული მიზნების მიღწევა შესაძლებელი იყო სხვა იმგვარი საშუალებებით, რომლებიც არ გამოიწვევდა დასაქმებულთა პირად ცხოვრებაში მაღალი ხარისხით ჩარევას. გამოიკვეთა ისეთი შემთხვევაც, როცა ორგანიზაცია დასაქმებული პირების სამუშაო ადგილის ვიდეომონიტორინგს ახორციელებდა კანონის მოთხოვნების შესაბამისად, თუმცა ვიდეომონიტორინგის კონკრეტული მიზნ(ებ)ის შესახებ დასაქმებული პირები არ იყვნენ გაფრთხილებულნი წერილობითი ფორმით.

გამოიკვეთა შემთხვევები, როცა ორგანიზაციები საჭიროების გარეშე ახორციელებდნენ დასაქმებული პირების სამუშაო სივრცის აუდიომონიტორინგს. ერთ-ერთი ორგანიზაციისთვის შემოწმების მიმდინარეობის ფარგლებში გახდა ცნობილი, რომ ვიდეომონიტორინგის მიზნით განთავსებული მოწყობილობით აუდიომონიტორინგიც მიმდინარეობდა, ერთ-ერთი ორგანიზაცია კი ფლობდა ინფორმაციას აუდიომონიტორინგის მიმდინარეობის შესახებ, თუმცა აღნიშნული ფორმით მონაცემთა დამუშავების შეწყვეტის მიზნით ღონისძიებები არ გაუტარებია. გარდა ამისა, გამოვლინდა მომსახურების ხარისხის კონტროლის,

მისი გაუმჯობესებისა და მომხმარებლის კმაყოფილების უზრუნველყოფის მიზნით დასაქმებული პირების სამუშაო პროცესის/სივრცის მუდმივ რეჟიმში აუდიომონიტორინგის (მაშინაც კი, როცა დასაქმებული პირების მიერ მომხმარებლებთან კომუნიკაცია არ ხორციელდებოდა) შემთხვევაც, რაც მაღალი ხარისხით იწვევდა დასაქმებულთა პირად ცხოვრებაში ჩარევას და არღვევდა სამართლიან ბალანსს მონაცემთა დამუშავების კანონიერ მიზანს, დამუშავებისთვის პასუხისმგებელი პირის ინტერესებსა და სუბიექტის უფლებებს შორის.

ორგანიზაციების უმეტესობას არ აქვს მიღებული ადეკვატური და ეფექტიანი ზომები მონაცემთა უსაფრთხოების დასაცავად. მონაცემების მიმართ განხორციელებულ მოქმედებებს ორგანიზაციების ნაწილი არ აღრიცხავდა, ნაწილი კი — არასრულად. ამასთანავე, გამოვლინდა არაუფლებამოსილი პირებისთვის მონაცემების გაზიარებისა და საერთო მომხმარებლის სახელითა და პაროლით ელექტრონულ სისტემებში დაცულ მონაცემებზე წვდომის შემთხვევები. მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვა ერთ-ერთი ყველაზე მნიშვნელოვანი ორგანიზაციულ-ტექნიკური ზომაა, რომელიც პერსონალური მონაცემების კანონდარღვევით გამჟღავნების ფაქტის დადგომისას უზრუნველყოფს გამჟღავნებაზე პასუხისმგებელი პირის გამოვლენას. გარდა ამისა, უსაფრთხოების დაცვისთვის მიღებული აღნიშნული ზომა ორგანიზაციებს საშუალებას აძლევს, განახორციელონ ეფექტიანი მონიტორინგი, თუ როდის, ვის, რა მიზნითა და რა მოცულობით ჰქონდა წვდომა შრომითი ურთიერთობის ფარგლებში მოპოვებულ მონაცემებზე.

ცალკეულ შემთხვევაში ორგანიზაციებს არ აქვთ განსაზღვრული ელექტრონული ფორმით არსებული მონაცემების შენახვის ვადები ან გეგმავენ, რომ მონაცემების შენახვა მოხდეს უვადოდ (მაგალითად, სტატისტიკური მონაცემების დამუშავების მიზნით). გამოვლინდა ისეთი შემთხვევაც, როცა ორგანიზაცია განსაზღვრულზე მეტი ვადით ინახავდა მონაცემებს. გარკვეული მონაცემები დროის გასვლასთან ერთად ძველდება, კარგავს აქტუალობას და აღარ არსებობს მათი შენახვის საჭიროება, ლეგიტიმური მიზნის მისაღწევად საჭირო ვადით მონაცემების შენახვა კი მონაცემთა დამუშავების ერთ-ერთი უმნიშვნელოვანესი პრინციპია.

გ. ჯანდაცვის სფეროში მონაცემების დამუშავება

ჯანმრთელობის შესახებ ინფორმაცია განსაკუთრებული კატეგორიის მონაცემია და, თავისი სენსიტიური ხასიათიდან გამომდინარე, დაცვის მაღალ სტანდარტს ექვემდებარება. მოქალაქეთა მონაცემები ყოველდღიურად ჯანდაცვის სექტორის მიერ გაწეული არაერთი მომსახურების ფარგლებში მუშავდება. აღნიშნულ ინფორმაციას იყენებენ სამედიცინო დაწესებულებები, სტომატოლოგიური კლინიკები, ლაბორატორიები, ჯანდაცვის სექტორის მართვაზე და ადმინისტრირებაზე პასუხისმგებელი საჯარო სამართლის იურიდიული პირები და სხვა. ვინაიდან ჯანმრთელობასთან დაკავშირებული მონაცემები შეიცავს ინტიმურ დეტალებს ინდივიდის პირადი ცხოვრების, მისთვის

სამედიცინო მომსახურების გაწევის, მისი ფსიქიკური და ფიზიკური მდგომარეობის შესახებ, მათი უკანონო დამუშავება შესაძლოა არა მხოლოდ პირადი ცხოვრების ხელშეუხებლობის დარღვევის, არამედ ღირსების შელახვის, სტიგმატიზაციის ან დისკრიმინაციის მიზეზი გახდეს. სამსახურის მიერ გეგმურად შესწავლილი საქმეები ცხადყოფს, რომ ჯანდაცვის სექტორის მიერ მონაცემების დამუშავების პროცესებში ფიქსირდება გარკვეული დარღვევები და ნაკლოვანებები:

სამედიცინო მომსახურების მიმწოდებელი დაწესებულებები ვიდეომონიტორინგს ახორციელებდნენ სამედიცინო მანიპულაციებისთვის განკუთვნილ ოთახ(ებ)ში, ამავე ოთახებში განთავსებული ვიდეოკამერ(ებ)ის ხედვის არეალში კი ექცევა ის სივრცეც, სადაც პაციენტები იღებენ სამედიცინო მომსახურებას და ამავე მიზნით უტარდებათ პროცედურები. ვინაიდან სამედიცინო დაწესებულებები ვიდეომონიტორინგის შედეგად მოიპოვებენ პაციენტისთვის სამედიცინო პროცედურის გაწევის ამსახველ ჩანაწერებს, ასეთ სივრცეებში კი მონაცემთა სუბიექტს აქვს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი, ვიდეომონიტორინგის განხორციელება ეწინააღმდეგება კანონის მოთხოვნებს.

ასევე, გამოიკვეთა შემთხვევა, როცა სამედიცინო დაწესებულება მომსახურების ხარისხის კონტროლის, მისი გაუმჯობესებისა და მომხმარებლის კმაყოფილების უზრუნველყოფის მიზნით მუდმივად ახორციელებდა დასაქმებულებსა და მომხმარებლებს შორის კომუნიკაციის აუდიომონიტორინგს. მართალია, აღნიშნული მიზნების უზრუნველყოფა წარმოადგენს სამედიცინო დაწესებულების ლეგიტიმურ ინტერესს, თუმცა მის განსახორციელებლად გამოყენებული საშუალება არ არის პროპორციული დამუშავებულ მონაცემებთან მიმართებით და იწვევს არათანაზომიერ ჩარევას, მათ შორის ჩარევას დასაქმებული პირების პირად ცხოვრებაში, ამგვარ შემთხვევაში ირღვევა აუდიომონიტორინგის წესები.

გამოვლინდა, რომ ჯანმრთელობის დაცვის მიზნით ღონისძიებების განმახორციელებელი ერთ-ერთი დაწესებულება იმაზე მეტი მოცულობით მოიპოვებდა მონაცემებს, ვიდრე სჭირდებოდა ლეგიტიმური მიზნის მისაღწევად. საყურადღებოა, რომ არასაჭირო მონაცემების მოპოვება ქმნის მონაცემთა არაპროპორციული მოცულობით დამუშავების საფრთხეს და წარმოადგენს მინიმიზაციის პრინციპის დარღვევას.

ამასთანავე, გამოიკვეთა დაწესებულებებს შორის ხელშეკრულების/შეთანხმების არსებობის გარეშე მონაცემების მიმოცვლის შემთხვევები, რაც ზრდის მონაცემების უკანონო დამუშავების რისკებს.

დაწესებულებების უმეტესობას არ აქვს მიღებული ადეკვატური და ეფექტიანი ზომები მონაცემთა უსაფრთხოების დასაცავად. რიგ შემთხვევებში არასრულად აღირიცხება მონაცემთა მიმართ განხორციელებული მოქმედებები. ამასთან, დაწესებულებების თანამშრომლებს საერთო მომხმარებლის სახელითა და პაროლით წვდომა აქვთ ელექტრონულ სისტემებში არსებულ მონაცემებზე. გამოვლინდა არაუფლებამოსილი პირებისთვის მონაცემების გაზიარების შემთხვევებიც; მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვის გარეშე კი დაწესებულება ვერ განახორციელებს ჯეროვან მონიტორინგს – ვის,

როდის, რა მიზნითა და რა მოცულობით ჰქონდა წვდომა მონაცემებზე. აღნიშნული, კონკრეტული შემთხვევის – მაგალითად, პერსონალური მონაცემების კანონდარღვევით გამჟღავნების ფაქტის დადგომისას, ართულებს ან შეუძლებელს ხდის მონაცემების კანონდარღვევით გამჟღავნებაზე პასუხისმგებელი პირის გამოვლენას.

დ. ფინანსურ სექტორში მონაცემების დამუშავება

ფინანსურ სექტორში მონაცემთა დამუშავების წესების დაცვა უმნიშვნელოვანესია ფინანსური ინფორმაციის სენსიტიური ხასიათისა და დარღვევასთან დაკავშირებული მნიშვნელოვანი რისკების გამო. კანონის მოთხოვნათა დაცვა არა მხოლოდ ფინანსური ინსტიტუტების სამართლებრივი ვალდებულებაა, არამედ ფუნდამენტური პირობაა მათ მიმართ მომხმარებელთა ნდობის შესანარჩუნებლად, უარყოფითი შედეგების თავიდან ასაცილებლად და ეკონომიკური სტაბილურობის უზრუნველსაყოფად. 2024 წელს განხორციელებული შემოწმებების საფუძველზე ფინანსური საქმიანობის ფარგლებში მონაცემების დამუშავების პროცესში გარკვეული დარღვევები და ნაკლოვანებები გამოვლინდა:

გამოიკვეთა მონაცემთა დამუშავებასთან დაკავშირებული საკითხების შესახებ მონაცემთა სუბიექტის არასათანადო ინფორმირების ფაქტები. მაგალითად, ცხელი ხაზის ფუნქციონირების ფარგლებში მონაცემთა დამუშავებასთან დაკავშირებით შესწავლილი ფინანსური ინსტიტუტები (ბანკები) იწერდნენ მომხმარებელთან სატელეფონო საუბარს, თუმცა ზოგიერთ შემთხვევაში არ ხდებოდა მონაცემთა სუბიექტის სრულფასოვნად ინფორმირება მიმდინარე აუდიომონიტორინგის შესახებ. ასევე, გამოიკვეთა შემთხვევა, როდესაც, საუბრის აუდიოჩაწერის განხორციელების შესახებ გაფრთხილების მიუხედავად, არსებობდა შესაძლებლობა, რომ არ მომხდარიყო ხსენებული საუბრის ჩაწერა, რაც ქმნიდა მონაცემთა სუბიექტის შეცდომაში შეყვანის რისკებს მისი მონაცემების დამუშავების შესახებ მცდარი ინფორმაციის მიწოდებით. გამოიკვეთა ისეთი შემთხვევებიც, როდესაც სადაზღვევო კომპანიების ვებგვერდების საშუალებით მომხმარებლებისგან მონაცემების მოპოვებისას არ ხდებოდა ან არასრულყოფილად ხდებოდა მათი ინფორმირება კანონის 24-ე მუხლით გათვალისწინებულ საკითხებთან დაკავშირებით; ცალკეული ორგანიზაციები კი ამავე მუხლით გათვალისწინებულ ინფორმაციას მონაცემთა სუბიექტს არ აწვდიდნენ ერთიანი დოკუმენტით და გაბნეული იყო სხვადასხვა, ხშირ შემთხვევაში მოცულობით დოკუმენტებში, რაც ვერ მიიჩნევა მონაცემთა სუბიექტისთვის მარტივი და აღქმადი ფორმით ინფორმაციის მიწოდებად.

ცალკეულ შემთხვევებში გამოვლინდა მონაცემთა არასათანადო მოცულობით დამუშავების ფაქტები. ერთ-ერთი სადაზღვევო კომპანიის ვებგვერდის გამოყენებით მომხმარებელს, სავალდებულო დოკუმენტაციის გარდა, ასევე შეეძლო დამატებითი დოკუმენტაციის (მაგალითად, განსახილველ სადაზღვევო შემთხვევასთან დაკავშირებული სამედიცინო ანალიზებისა და გამოკვლევის პასუხები) მიწოდებაც, თუმცა, კომპანიის განმარტებით, აღნიშნული

დოკუმენტაციის არსებობა გავლენას არ ახდენდა სადაზღვევო შემთხვევის განხილვაზე. ამასთანავე, გამოვლინდა ბანკის მიერ დასაქმებული პირების პერსონალური მონაცემების საზღვარგარეთ კანონის 37-ე მუხლით დადგენილი წესების დარღვევით გადაცემის შემთხვევაც.

მონაცემთა უსაფრთხოების დასაცავად ადეკვატური და ეფექტიანი ზომების მიუღებლობის შემთხვევები გამოიკვეთა ფინანსური ორგანიზაციების შემოწმებებშიც. მაგალითად, ზოგიერთი ორგანიზაცია არ აღრიცხავდა ან არასრულად აღრიცხავდა მომხმარებელთა მონაცემების მიმართ განხორციელებულ მოქმედებებს. ასევე, გამოიკვეთა შემთხვევები, როდესაც ელექტრონულად დამუშავებულ მონაცემებზე წვდომას ორგანიზაციის თანამშრომლები ახორციელებდნენ საერთო მომხმარებლის გამოყენებით, რაც გამორიცხავდა მონაცემების მიმართ მოქმედებების განმახორციელებელი პირის იდენტიფიკაციას.

ე. მონაცემთა დამუშავების სხვა აქტუალური საკითხები

სხვადასხვა სფეროსთან დაკავშირებით საჯარო უწყებებისა და კერძო ორგანიზაციების მიერ მონაცემების დამუშავების პროცესებში ასევე ფიქსირდება გარკვეული დარღვევები და ნაკლოვანებები:

მონაცემთა დამუშავების სხვადასხვა პროცესის შესწავლის შედეგად გამოიკვეთა მოცულობითი მონაცემების როგორც შესაბამისი სამართლებრივი საფუძვლის გარეშე გასაჯაროების, ასევე – მესამე პირებისთვის გამჟღავნების (მათ შორის, სისტემაზე წვდომის მინიჭების გზით) ფაქტები.

გარკვეულ შემთხვევებში გამოიკვეთა ვიდეომონიტორინგის წესების დარღვევის, აგრეთვე ისეთი სივრცეების ვიდეომონიტორინგის ფაქტები, რომელთა მიზანი და საჭიროებაც დაწესებულებებს არ ჰქონდათ, ცალკეული ორგანიზაციები კი ვიდეომონიტორინგის სისტემის მეშვეობით შესაბამისი ლეგიტიმური მიზნისა და საჭიროების გარეშე ახორციელებდნენ აუდიომონიტორინგს. ამასთან, მიუხედავად შესაბამისი საჭიროების არარსებობისა, არ ჰქონდათ მიღებული ზომები აღნიშნული ფორმით მონაცემთა დამუშავების პროცესის შესაწყვეტად.

გამოიკვეთა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ ვიდეომონიტორინგის, აუდიომონიტორინგისა და ბიომეტრიული მონაცემების დამუშავების პროცესების წერილობითი ფორმით განსაზღვრის ვალდებულების ნაკლოვანი შესრულების შემთხვევები. როგორც წესი, აღნიშნული დოკუმენტები სრულყოფილად არ მოიცავდა კანონით განსაზღვრულ საკითხებს (მაგალითად: ვიდეომონიტორინგის/აუდიომონიტორინგის მიზანს და მოცულობას, ხანგრძლივობას და ჩანაწერის შენახვის ვადას, ჩანაწერზე წვდომის, მისი შენახვისა და განადგურების წესსა და პირობებს, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმებს და სხვა).

გამოიკვეთა მონაცემთა დამუშავების პროცესებში დამუშავებაზე უფლებამოსილი პირების მონაწილეობის არაერთი შემთხვევა. მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებსა და დამუშავებაზე უფლებამოსილ პირებს შორის დადებული ხელშეკრულებები ძირითადად არეგულირებს

მომსახურების გაწევის საკითხს და შინაარსობრივად მოიცავს მონაცემების დამუშავების დავალებასაც, თუმცა არ შეესაბამება კანონის 36-ე მუხლით დადგენილ მოთხოვნებს.

4.2. პრეცედენტული გადაწყვეტილებები

ა. მოწყვლადი ჯგუფებისა და ახალგაზრდების მონაცემების დამუშავება

— ა(ა)იპ — „ბათუმის საბავშვო ბაღების გაერთიანება“

სამსახურმა გეგმურად შეისწავლა ა(ა)იპ — „ბათუმის საბავშვო ბაღების გაერთიანების“ (შემდგომში — ბაღების გაერთიანება) მიერ ვებგვერდის მეშვეობით რეგისტრაციისას საჯარო ბაღების აღსაზრდელთა პერსონალური მონაცემების დამუშავების კანონიერება.

შემოწმების ფარგლებში დადგინდა, რომ ბათუმში არსებულ სკოლამდელი აღზრდის საჯარო დაწესებულებებში მიღების მსურველ აღსაზრდელთა რეგისტრაცია ხორციელდებოდა ბაღების გაერთიანების ვებგვერდზე განთავსებული სარეგისტრაციო ფორმის შევსების გზით. აღნიშნულის შედეგად მუშავდებოდა აღსაზრდელისა და მისი მშობლების პერსონალური მონაცემები (მაგალითად: სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი, მისამართი, შშმ ბავშვის სტატუსი და ა. შ.). ვებგვერდი ფუნქციონირებდა 2015 წლიდან და შემოწმების პერიოდისთვის მისი საშუალებით დამუშავებული იყო 24 947 (ოცდაოთხი ათას ცხრაას ორმოცდაშვიდი) ბავშვის მონაცემები. ნიშანდობლივია, რომ ბაღების გაერთიანების ვებგვერდზე განთავსებულ სარეგისტრაციო განაცხადში ერთ-ერთი მშობლის რეგისტრაციის ადგილის, ბაღის დასახელებისა და ჯგუფის ასარჩევად განკუთვნილი ველების შევსების შედეგად, ბმულის სახით ვებგვერდით მოსარგებლე ნებისმიერი პირისთვის ხელმისაწვდომი ხდებოდა ინფორმაცია შერჩეულ ბაღში/ჯგუფში ჩარიცხული და რიგში მდგომი ბავშვების რაოდენობის შესახებ, მათ შორის – ბავშვების სახელები, გვარები, ბაღის მისამართი და ჩარიცხვის რიგში მდგომი ბავშვებისთვის მინიჭებული რიგის ნომერი.

შემოწმების ფარგლებში ბაღების გაერთიანების განმარტება, რომ არასრულწლოვნების მონაცემების ზემოხსენებული სახით დამუშავება (ხელმისაწვდომობა) აუცილებელი იყო მნიშვნელოვანი საჯარო ინტერესის დასაცავად, კერძოდ, რეგისტრაციის პროცესის გამჭვირვალობისა და დაინტერესებული პირებისთვის სამართლიანობის განცდის ჩამოყალიბებისათვის, სამსახურმა არ გაიზიარა. სამსახურის განმარტებით, უშუალოდ ჩარიცხული და რიგში მდგომი არასრულწლოვნების მონაცემების გასაჯაროების ფაქტი არ წარმოადგენდა გამჭვირვალობის აუცილებელ პირობას და მას არ შეეძლო გავლენა მოეხდინა საზოგადოებაში სამართლიანობის განცდის ჩამოყალიბებაზე. ამასთან, ამ ფორმით მონაცემების ხელმისაწვდომობა განსაკუთრებით საზიანო შეიძლება ყოფილიყო არასრულწლოვნებისთვის, რადგან პირთა ფართო წრეს ეძლეოდა

შესაძლებლობა, მონაცემები გამოეყენებინა პირადი ინტერესებისათვის. შესაბამისად, ბაღების გაერთიანების მიერ დასახელებული მიზნების მიღწევა შესაძლებელი იყო ჩარიცხული და მომლოდინე ბავშვების მონაცემების გამოქვეყნების გარეშეც.

სამსახურმა ასევე არ გაიზიარა საბავშვო ბაღების გაერთიანების განმარტება, რომ მონაცემების ვებგვერდზე გამოქვეყნების გზით, მათ შორის ხდებოდა ბაღში ჩარიცხვის მომლოდინეთა სიაში დაკავებული რიგის ნომრის შესახებ აღსაზრდელების მშობლების/კანონიერი წარმომადგენლების ინფორმირება. სამსახურის განმარტებით, მოცემულ შემთხვევაში, კონკრეტული აღსაზრდელის მშობლის/კანონიერი წარმომადგენლის ინფორმირების მიზნით, მათთან დაკავშირებული ინფორმაციის საჯაროდ, ნებისმიერი პირისთვის ხელმისაწვდომი ფორმით გასაჯაროება დასახელებული მიზნის აუცილებელ და თანაზომიერ საშუალებას არ წარმოადგენდა და გამოყენებული ფორმა ქმნიდა მონაცემთა სუბიექტებისთვის გაუმართლებელი ზიანის მიყენების რისკებს. ასევე გამოიკვეთა, რომ მშობელს/კანონიერ წარმომადგენელს არ ეძლეოდა შესაძლებლობა უარი განეცხადებინა ზემოაღნიშნული ფორმით მონაცემების დამუშავებაზე, რისთვისაც მონაცემთა სუბიექტისთვის განკუთვნილ, სარეგისტრაციო განაცხადზე დატანილ ბმულზე განთავსებული თანხმობის ტექსტი არ იქნა მიჩნეული კანონის მე-3 მუხლის „მ“ ქვეპუნქტით განსაზღვრულ კრიტერიუმებთან შესაბამისად. ამდენად, საბავშვო ბაღების გაერთიანება კანონის მე-5 მუხლით გათვალისწინებული სამართლებრივი საფუძვლის გარეშე გასაჯაროების გზით ამუშავებდა სკოლამდელი აღზრდის საჯარო დაწესებულების აღსაზრდელების პერსონალურ მონაცემებს.

შემოწმების ფარგლებში ასევე დადგინდა, რომ ვებგვერდის მონაცემთა ბაზაზე წვდომისას მონაცემთა მიმართ განხორციელებული მოქმედებები სრულყოფილად არ აღირიცხებოდა, რაც მონაცემთა უსაფრთხოებისთვის დადგენილი მოთხოვნის დარღვევაა. გარდა ამისა, კომპანიის ინფორმაციული ტექნოლოგიების მთავარი სპეციალისტი ვებგვერდის მეშვეობით დამუშავებულ პერსონალურ მონაცემებზე წვდომისთვის არ იყენებდა მასზე განპიროვნებული ანგარიშის მომხმარებელსა და პაროლს; მონაცემთა შენახვისთვის გათვალისწინებული ვადის გასვლის შემდგომ კი მონაცემები იშლებოდა მექანიკურად (ხელით). აღსანიშნავია, რომ მონაცემთა მიმართ განხორციელებული მოქმედებების აღრიცხვა უშედეგო იქნებოდა მონაცემთა მიმართ მოქმედებების განმახორციელებელი თითოეული პირის იდენტიფიცირების გარეშეც.

ზემოხსენებულ დარღვევებთან დაკავშირებით, სამსახურის გადაწყვეტილებით საბავშვო ბაღების გაერთიანება ცნობილ იქნა სამართალდამრღვევად კანონის 67-ე და 76-ე მუხლებით გათვალისწინებული ადმინისტრაციული სამართალდარღვევების ჩადენაში. იმავდროულად, საბავშვო ბაღების გაერთიანებას დაევალა ზემოხსენებული დარღვევების აღმოფხვრა.

— ზუგდიდისა და ფოთის მუნიციპალიტეტების მერიები

სამსახურმა გეგმურად შეამოწმა ზუგდიდის მუნიციპალიტეტის მერიის მიერ ბავშვებისა და ახალგაზრდების შესაძლებლობის განვითარების ხელშეწყობის პროგრამის, ხოლო ფოთის მუნიციპალიტეტის მერიის მიერ — „ნიკო ნიკოლაძის სახელობის სტიპენდია (ჯილდო) წარმატებული სტუდენტებისათვის“ — ქვეპროგრამის განხორციელების ფარგლებში ბენეფიციარების მონაცემების დამუშავების კანონიერება.

შემოწმების შედეგად დადგინდა, რომ ზუგდიდის მუნიციპალიტეტის მერია თავის „Facebook“ გვერდზე, ხოლო ფოთის მუნიციპალიტეტის მერია საკუთარ ოფიციალურ ვებგვერდზე ასაჯაროებდა ბენეფიციარების (ახალგაზრდები ან/და არასრულწლოვნები) პერსონალურ მონაცემებს (პირის სახელს, გვარს, ფოტოსურათს, იმ უნივერსიტეტის დასახელებას, რომელშიც სტუდენტი სწავლობდა და სხვა). აღსანიშნავია, რომ გასაჯაროების სამართლებრივ საფუძვლად ზუგდიდის მუნიციპალიტეტის მერია მიუთითებდა ბენეფიციარების თანხმობას, ხოლო, ფოთის მუნიციპალიტეტის მერიის განმარტებით, სტუდენტების პერსონალური მონაცემების გასაჯაროება ვებგვერდზე ხდებოდა როგორც სტუდენტის თანხმობით, ასევე – მნიშვნელოვანი საჯარო ინტერესის დასაცავად.

განსახილველ შემთხვევაში აღნიშნულმა დაწესებულებებმა ვერ წარმოადგინეს მონაცემების კონკრეტული მიზნით დამუშავების თაობაზე მონაცემთა სუბიექტების წინასწარ ინფორმირებული თანხმობების არსებობის დამადასტურებელი მტკიცებულებები; ფოთის მუნიციპალიტეტის მერიასთან მიმართებით კი სამსახურმა მიიჩნია, რომ საჯარო ინტერესის დასაცავად სტუდენტების მონაცემების ვებგვერდზე გასაჯაროების აუცილებლობის თაობაზე მერიის მიერ შემოწმების ფარგლებში წარმოდგენილი განმარტებები ბუნდოვანი და დაუსაბუთებელი იყო. კერძოდ, მერიამ ვერ წარმოადგინა კონკრეტული და მკაფიო დასაბუთება იმის თაობაზე, თუ რატომ მიეკუთვნებოდა სტუდენტების პერსონალური მონაცემების გასაჯაროება საზოგადოებრივ ინტერესს.

ზემოაღნიშნული გარემოებებიდან გამომდინარე, დადგინდა, რომ როგორც ზუგდიდის მუნიციპალიტეტის მერია, ასევე ფოთის მუნიციპალიტეტის მერია კანონის მე-5 მუხლით გათვალისწინებული სამართლებრივი საფუძვლების გარეშე ასაჯაროებდა ბენეფიციარების მონაცემებს.

ზუგდიდის მუნიციპალიტეტის მერიის შემოწმების ფარგლებში ასევე გამოიკვეთა, რომ საქმისწარმოების ელექტრონულ სისტემაში, რომელშიც რეგისტრირდებოდა დაფინანსების მიღების მიზნით ბენეფიციარების განცხადებები, მათ პერსონალურ მონაცემებზე წინასწარი და უწყვეტი წვდომის შესაძლებლობა ჰქონდათ მერიის შიდა აუდიტისა და ინსპექტირების სამსახურის თანამშრომლებს, რომლებმაც, ფუნქცია-მოვალეობებიდან გამომდინარე, ვერ დაასაბუთეს მათთვის მონაცემებზე მუდმივი წვდომის საჭიროება. შემოწმების შედეგად ასევე დადგინდა, რომ პროგრამის ფარგლებში ბენეფიციართა პერსონალური მონაცემების დასამუშავებლად მერიის თანამშრომლები იყენებდნენ პირად ელექტრონულ ფოსტებს, რომლებზეც მერია ვერ აკონტროლებდა. შესაბამისად, მერია ვერ ახორციელებდა საკუთარი თანამშრომლების მიერ პირადი

ელექტრონულ ფოსტის მეშვეობით მონაცემთა დამუშავების პროცესის მონიტორინგს და მონაცემთა შემდგომი დამუშავების მართლზომიერება, მათ შორის – შრომითი ურთიერთობის შეწყვეტის შემდეგ, მთლიანად დასაქმებული პირის კეთილსინდისიერებაზე იყო დამოკიდებული. ამდენად, დადგინდა ზუგდიდის მუნიციპალიტეტის მერიის მიერ მონაცემთა უსაფრთხოების წესების დარღვევაც.

ზუგდიდის მუნიციპალიტეტის მერიის შემოწმების ფარგლებში გამოიკვეთა, რომ საქმისწარმოების ელექტრონული სისტემის მონაცემთა ბაზაში პირდაპირი წვდომის ფარგლებში მონაცემების დამუშავებისას არ აღირიცხებოდა მონაცემთა დათვალიერება; აღნიშნული სისტემის მონაცემთა ბაზის დასაცავად სათანადო ორგანიზაციულ-ტექნიკური ზომების მიღებაზე კი პასუხისმგებელი იყო დამუშავებაზე უფლებამოსილი პირი — სსიპ — „მუნიციპალური სერვისების განვითარების სააგენტო“ (შემდგომში — სააგენტო). აღნიშნულიდან გამომდინარე, სააგენტოს ასევე დაეკისრა პასუხისმგებლობა მონაცემთა უსაფრთხოების წესების დარღვევისთვის.

მნიშვნელოვანია აღინიშნოს, რომ საქმისწარმოების ელექტრონული სისტემის ფუნქციონირების მიზნებისთვის სსიპ — „სახელმწიფო სერვისების განვითარების სააგენტოს“ მიერ მერიისთვის პერსონალურ მონაცემთა მიწოდების საკითხი არ იყო მოწესრიგებული ხელშეკრულებით. სამსახურმა მიუთითა, რომ ხელშეკრულების არსებობა ემსახურება მონაცემთა კანონიერად, თანმიმდევრულად და ერთგვაროვნად დამუშავების უზრუნველყოფის მიზნებს, ხოლო მისი არსებობის ვალდებულებას ითვალისწინებდა „ზუგდიდის მუნიციპალიტეტის მერიის დებულების დამტკიცების შესახებ“ ქალაქ ზუგდიდის მუნიციპალიტეტის საკრებულოს 2022 წლის 1 ივლისის №21 დადგენილების 26-ე მუხლიც.

ზემოხსენებულ დარღვევებთან დაკავშირებით სამსახურმა ზუგდიდის მუნიციპალიტეტის მერია და სააგენტო ცნო სამართალდამრღვევად კანონის 76-ე მუხლით, ხოლო ფოთის მუნიციპალიტეტის მერია 67-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევების ჩადენაში. იმავდროულად, აღნიშნულ მერიებსა და სააგენტოს დაევალათ ზემოხსენებული დარღვევების აღმოფხვრა.

ბ. მონაცემთა დამუშავების პროცესები კერძო და საჯარო სკოლებში

სამსახურმა გეგმურად შეისწავლა: 3 (სამი) კერძო სკოლის მიერ ელექტრონული ჟურნალების მეშვეობით მოსწავლეთა პერსონალური მონაცემების დამუშავების კანონიერება; 2 (ორი) საჯარო და 2 (ორი) კერძო სკოლის მიერ მოსწავლეთა დისციპლინური გადაცდომების შესახებ მონაცემების დამუშავების კანონიერება; 2 (ორი) საჯარო რესურსსკოლის მიერ ინდივიდუალური სასწავლო გეგმების შექმნისა და შენახვის გზით სპეციალური საგანმანათლებლო საჭიროების მქონე (სსსმ) მოსწავლეთა პერსონალური მონაცემების დამუშავების კანონიერება. შემოწმებების მიმდინარეობის პერიოდში აღნიშნულ სკოლებში დამუშავებული იყო 7000-ზე (შვიდი ათასზე) მეტი მოსწავლის მონაცემები, რომელთა შორის 100 (ასი) შშმ სსსმ მოსწავლე იყო.

— ელექტრონული ჟურნალები

შემოწმების შედეგად გამოიკვეთა სკოლების მიერ მონაცემთა უსაფრთხოებასთან დაკავშირებული დარღვევები. კერძოდ, ერთ-ერთი კერძო სკოლის შემთხვევაში ელექტრონულ ჟურნალში, ასევე – მის მონაცემთა ბაზაში მოსწავლეთა პერსონალური მონაცემების მიმართ განხორციელებულ მოქმედებები არ აღირიცხებოდა, ხოლო მეორე შემთხვევაში ელექტრონულ ჟურნალში განხორციელებული მოქმედებები არასრულად აღირიცხებოდა (კერძოდ, არ აღირიცხებოდა დათვალიერება და ექსპორტი). 2 (ორი) სკოლაში ელექტრონული ჟურნალების მეშვეობით მონაცემებზე წვდომის განმახორციელებელი პირები არ სარგებლობდნენ განპიროვნებული მომხმარებლის ანგარიშებით. გარდა ამისა, გამოიკვეთა შემთხვევა, როდესაც ელექტრონული ჟურნალის მონაცემთა ბაზაზე „ადმინისტრატორის“ როლის მქონე მომხმარებლით წვდომის შესაძლებლობა შენარჩუნებული ჰქონდა სკოლის ყოფილ თანამშრომელს. ამასთან, მოქმედ ელექტრონულ ჟურნალში ერთ-ერთი სკოლა იყენებდა მარტივ პაროლებს. სისტემის მონაცემთა ბაზას არ ჰქონდა პაროლების შიფრაცია, ხოლო სისტემაში დარეგისტრირებულ მომხმარებელს – პაროლის თავად შეცვლის უფლება. აღნიშნული შესაძლებლობა ჰქონდა მხოლოდ „ადმინისტრატორის“ როლის მქონე მომხმარებელს. გარემოებებიდან გამომდინარე, იქმნებოდა მონაცემთა უკანონოდ დამუშავების მნიშვნელოვანი რისკები.

შემოწმების შედეგად ასევე დადგინდა, რომ ერთ-ერთი სკოლა, მოსწავლის რეგისტრაციის მიზნით, ელექტრონულ ჟურნალში მოსწავლის ბარათში აგრეთვე უთითებდა ინფორმაციას ელექტრონული ფოსტისა და მისამართის შესახებ. ამასთან, ხსენებული ელექტრონული ფოსტის მისამართი ხშირ შემთხვევაში რეალური არ იყო, ხოლო მისამართის ველში ყოველთვის მიეთითებოდა არა შესაბამისი მოსწავლის, არამედ – სკოლის მისამართი. სამსახურის განმარტებით, აღნიშნული გარემოება შეიცავდა საფრთხეს, რომ ელექტრონული ჟურნალის რომელიმე მომხმარებელს გაუჩნდებოდა არაზუსტი აღქმა ხსენებული მონაცემების ნამდვილობასთან დაკავშირებით, რაც, თავის მხრივ, ქმნიდა მათი მხრიდან არაზუსტი მონაცემების დამუშავების რისკს.

შემოწმების შედეგად ასევე დადგინდა, რომ რიგ შემთხვევებში სკოლების მიერ არ იყო შეფასებული ელექტრონული ჟურნალის მეშვეობით მოსწავლეთა მონაცემების შენახვის ვადები, ასევე – ამ ვადების ამოწურვის შემდეგ მონაცემთა მიმართ გასატარებელი ღონისძიებები.

— დისციპლინური წარმოება

სკოლების მიერ მოსწავლეთა დისციპლინური გადაცდომების შესახებ მონაცემების დამუშავების კანონიერების შესწავლის პროცესში ასევე გამოიკვეთა ხარვეზები მონაცემთა შენახვის ხანგრძლივობის საკითხთან დაკავშირებით. კერძოდ, ერთ-ერთ შემთხვევაში მოსწავლის დისციპლინური წარმოების

მატერიალური ფორმით არსებული საქმის მასალების შენახვისთვის საჭირო ვადების საკითხი სკოლას არ ჰქონდა შეფასებული; ხოლო, მართალია, სხვა შემთხვევაში აღნიშნული საკითხი სკოლას შეფასებული ჰქონდა, თუმცა იგი პერსონალურ მონაცემებს შენახვისთვის საჭირო ვადაზე უფრო ხანგრძლივად ინახავდა.

ასევე გამოიკვეთა მონაცემთა უსაფრთხოებასთან დაკავშირებული პრობლემაც. კერძოდ, ერთ-ერთი სკოლის შემთხვევაში მატერიალური დოკუმენტაციის ნაწილი ინახებოდა უფლებამოსილი თანამშრომლის — სკოლის საქმისმწარმოებლის სამუშაო ოთახში მდებარე დახურულ კარადაში (რომელიც არ იკეტებოდა საკეტით) დაცულ საქაღალდეში. მათ შორის აღნიშნული ოთახით სარგებლობდა სკოლის ბუღალტერი, რომელსაც პერსონალურ მონაცემებზე წვდომა არ ესაჭიროებოდა, თუმცა მას აღნიშნულის შესაძლებლობა ჰქონდა. სამსახურმა განმარტა, რომ განსახილველ შემთხვევაში მატერიალური ფორმით შენახული მონაცემების ფიზიკურ უსაფრთხოებასთან დაკავშირებით გატარებული ორგანიზაციულ-ტექნიკური ზომა არ წარმოადგენდა მოსწავლეთა მონაცემებზე არაუფლებამოსილ პირთა მხრიდან წვდომის პრევენციის ადეკვატურ საშუალებას.

— **რესურსსკოლები**

რესურსსკოლების მიერ ინდივიდუალური სასწავლო გეგმების შექმნისა და შენახვის გზით, მოსწავლეთა პერსონალური მონაცემების დამუშავების კანონიერების შემოწმების ფარგლებში, გამოიკვეთა მონაცემთა უსაფრთხოების დაცვასთან დაკავშირებული ნაკლოვანებები. ერთ-ერთ შემთხვევაში სამსახურის მიერ მონაცემთა უსაფრთხოებისთვის რისკის შემცველად შეფასდა სკოლის საქმისმწარმოებლის მიერ, კერძოდ, განსაკუთრებული კატეგორიის მონაცემების შემცველი მულტიდისციპლინური გუნდის დასკვნის მოსწავლეთა დამრიგებლებისთვის პირად ელექტრონულ ფოსტაზე გაგზავნის ფაქტები. სამსახურმა განმარტა, რომ პირად ელექტრონულ ფოსტას დამსაქმებელი ორგანიზაცია არ აკონტროლებს და, შესაბამისად, ასეთ შემთხვევაში დამსაქმებელს არ აქვს ეფექტიანი შესაძლებლობა, მიიღოს მონაცემთა რისკების ადეკვატური ორგანიზაციულ-ტექნიკური ზომები აღნიშნული სისტემებით დამუშავებული პერსონალური მონაცემების დაცვის მიზნით; თანამშრომელთან შრომითი ურთიერთობის შეწყვეტის შემთხვევაში კი არსებობს მნიშვნელოვანი რისკი, რომ ამ სისტემებში პერსონალური მონაცემების შენახვა გაგრძელდება და მათზე წვდომის შესაძლებლობა ექნება არაუფლებამოსილ პირს (ყოფილ თანამშრომელს).

სამსახურმა აგრეთვე იმსჯელა სკოლის მასწავლებლების მიერ არქივის ფორმატის, პაროლით დაცული ინდივიდუალური საქაღალდეების სკოლის კომპიუტერებში, საოპერაციო სისტემის საერთო მომხმარებლის ანგარიშის გამოყენებით, შენახვის ფაქტზე. მართალია, საქაღალდეები დაცული იყო შესაბამისი პაროლებით, თუმცა არსებობდა არაუფლებამოსილი პირების მიერ არქივის ფორმატის საქაღალდის შემთხვევითი წაშლის რისკები, ვინაიდან, გარდა მასწავლებლებისა, აღნიშნული კომპიუტერებით საგაკვეთილო სწავლების ფარგლებში სარგებლობდნენ მოსწავლეებიც.

მეორე რესურსსკოლის შემოწმების ფარგლებში ასევე გამოიკვეთა, რომ ინდივიდუალური სასწავლო გეგმების ნაწილი მატერიალური ფორმით ინახებოდა საქმისმწარმოებლის სამუშაო ოთახში არსებული ღია კარადის თაროებზე, ამ ოთახში საქმისმწარმოებელთან ერთად კი თავის სამსახურებრივ ფუნქციებს ახორციელებდა სკოლის ბუღალტერიც, რომელსაც სათანადო საჭიროების გარეშე წვდომის შესაძლებლობა ჰქონდა სსსმ მოსწავლეთა ინდივიდუალურ სასწავლო გეგმებზე. სამსახურმა ყურადღება გაამახვილა მოსწავლეების მონაცემების შემცველი ინდივიდუალური საგნობრივი გეგმის ნიმუშების, „Ms Word“ ფორმატის დოკუმენტების სახით სკოლის მასწავლებელთა პაროლით დაუცველ სამუშაო (პორტატულ) კომპიუტერებში შენახვის საკითხზეც. პერსონალური მონაცემების შემცველი, მათ შორის, განსაკუთრებული კატეგორიის მონაცემების დამუშავება (შენახვა) ქმნიდა მონაცემებზე არაუფლებამოსილი პირების წვდომისა და მონაცემთა უკანონოდ დამუშავების რისკებს.

სამსახურის გადაწყვეტილებით, ზემოხსენებულ დარღვევებთან დაკავშირებით 3 (სამი) სკოლა ცნობილ იქნა სამართალდამრღვევად კანონის 76-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში. იმავდროულად, სკოლებს დაევალათ შემოწმებისას გამოვლენილი დარღვევების აღმოფხვრა.

გ. ვიდეომონიტორინგი სკოლებში და კოლეჯებში

სამსახურმა გეგმურად შეამოწმა 2 (ორი) სახელმწიფო პროფესიული საგანმანათლებლო დაწესებულება/კოლეჯის (შემდგომში — კოლეჯი), ასევე 3 (სამი) საჯარო და 3 (სამი) კერძო სკოლის მიერ ვიდეომონიტორინგის დამუშავების კანონიერება. შემოწმებების მიმდინარეობის პერიოდში ხსენებულ კოლეჯებში სწავლობდა ჯამში 821 (რვაას ოცდაერთი) სტუდენტი, ხოლო სკოლებში — 6,348 (ექვსი ათას სამას ორმოცდარვა) მოსწავლე.

— სკოლები

შემოწმების შედეგად დადგინდა, რომ სკოლების ვიდეოჩამწერ მოწყობილობებში ზოგიერთ შემთხვევაში არ აღირიცხებოდა ვიდეოჩანაწერების მიმართ განხორციელებული ყველა მოქმედება, კერძოდ: ინფორმაცია ჩანაწერების დათვალიერების (გადახვევა და დათვალიერება) და ჩანაწერის გარე მეხსიერების მოწყობილობაზე გადაწერის (ჩანაწერის ამოღება) შესახებ; ვიდეოჩამწერ მოწყობილობებზე წვდომის უფლების მქონე პირები კი არ სარგებლობდნენ განპიროვნებული მომხმარებლების ანგარიშებით და წვდომის მიზნით იყენებდნენ საერთო მომხმარებლის ანგარიშს. ერთ-ერთ სკოლაში ვიდეოჩამწერ მოწყობილობებში მომხმარებლის ანგარიშები შექმნილი იყო პაროლის გარეშე. სხვა სკოლაში გამოიკვეთა შემთხვევა, როდესაც ვიდეოჩამწერი მოწყობილობის პაროლი უცნობი იყო ვიდეოსათვალთვალო მოწყობილობების ადმინისტრირებასა და კონტროლზე პასუხისმგებელი პირისთვის (სსიპ — „საგანმანათლებლო

დაწესებულების მანდატურის სამსახური“; შემდგომში — მანდატურის სამსახური), რის გამოც შეუძლებელი იყო ვიდეოჩანაწერების მიმართ განხორციელებული მოქმედებების მონიტორინგი. ერთ-ერთი სკოლის შემოწმებისას ასევე დადგინდა, რომ ვიდეოჩამწერ მოწყობილობებში მონაცემების მიმართ განხორციელებული მოქმედებების შესახებ ინფორმაცია ვიდეოჩანაწერების შენახვის ვადაზე ნაკლები დროით ინახებოდა. ზემოაღნიშნული უსაფრთხოების მოთხოვნების დაუცველობიდან გამომდინარე, იქმნებოდა ვიდეომონიტორინგის გზით დამუშავებულ მონაცემთა უკანონო გამჟღავნების ან სხვაგვარი დამუშავების რისკები.

გეგმური შემოწმების შედეგად ასევე გამოიკვეთა, რომ ერთ-ერთ სკოლაში ვიდეოსათვალთვალო კამერების მეშვეობით, ვიდეომონიტორინგთან ერთად, ხორციელდებოდა აუდიომონიტორინგიც, რის თაობაზეც ინფორმაციას არ ფლობდა არცერთი თანადამუშავებისთვის პასუხისმგებელი პირი (სკოლა და მანდატურის სამსახური). იმდენად, რამდენადაც ვიდეოსათვალთვალო სისტემის ყოველდღიური გამოყენებისა და ადმინისტრირების უზრუნველყოფა მანდატურის სამსახურს ეკისრებოდა, სამსახურმა მიიჩნია, რომ მანდატურის სამსახურის მიერ აუდიომონიტორინგის მიმდინარეობის ფაქტის იდენტიფიცირებითა და შემდგომი რეაგირების განუხორციელებლობით დაირღვა კანონის მე-11 მუხლის მოთხოვნები.

შემოწმების შედეგად ასევე გამოვლინდა, რომ ერთ-ერთი სკოლა ვიდეომონიტორინგს ახორციელებდა ინფორმატიკის საკლასო ოთახში, რაზეც სკოლამ განმარტა, რომ აღნიშნული საჭირო იყო პირთა უსაფრთხოების უზრუნველყოფისა და საკუთრების დაცვის, ასევე – ზარალის ანაზღაურებაზე პასუხისმგებელი პირის იდენტიფიცირების მიზნით. ეს პოზიცია სამსახურმა არ გაიზიარა, ვინაიდან სკოლის მიერ დასახელებული მიზნების მიღწევა შესაძლებელი იყო ალტერნატიული საშუალებებითაც (მაგალითად, მასწავლებლებთან დადებულ ხელშეკრულებებში მატერიალური ფასეულობების დაცვის მიზნით შესაბამისი ვალდებულებების გათვალისწინება, ნივთებზე პასუხისმგებელი/მეთვალყურე პირის გამოყოფა და სხვა). შესაბამისად, სკოლის მიერ ინფორმატიკის საკლასო ოთახში ვიდეომონიტორინგის განხორციელება სკოლის მიერ დასახელებული მიზნების მიღწევის ადეკვატურ და პროპორციულ საშუალებად არ იქნა მიჩნეული.

2 (ორი) სკოლის გეგმური შემოწმების შედეგად ასევე გამოიკვეთა, რომ ვიდეოჩამწერ მოწყობილობებში ვიდეოჩანაწერები ინახებოდა იმაზე მეტი ვადით, ვიდრე ეს საჭირო იყოს სკოლის მიერ დასახელებული/განსაზღვრული კანონიერი მიზნების მისაღწევად. რიგ შემთხვევებში სკოლების შენობა-ნაგებობების შიდა და გარე პერიმეტრზე არასაკმარისი რაოდენობით ან საერთოდ არ იყო განთავსებული ვიდეომონიტორინგის მიმდინარეობის შესახებ გამაფრთხილებელი ნიშნები. ამასთან, 2024 წლის პირველი მარტის შემდგომ პერიოდში განთავსებული ნიშნები არ შეიცავდა ინფორმაციას დამუშავებისთვის პასუხისმგებელი პირისა და მისი საკონტაქტო ინფორმაციის შესახებ, რაც არ შეესაბამება კანონის მე-10 მუხლის მე-9 პუნქტის მოთხოვნებს. გარდა ამისა, სკოლებში ფიქსირდებოდა ისეთი ვიდეოკამერების არსებობის ფაქტები, რომლებიც ვიდეოჩამწერ მოწყობილობებთან არ იყო დაკავშირებული და არ ფუნქციონირებდა. აღსანიშნავია, რომ

ვიდეოკამერის განთავსების ფაქტი, თუნდაც ვიდეოჩაწერის განხორციელების გარეშე, ქმნის მონაცემთა სუბიექტის მცდარ წარმოდგენას მისი პერსონალური მონაცემების დამუშავების თაობაზე. ხსენებულის საფუძველზე მონაცემთა სუბიექტს უყალიბდება თავისი პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევის ცრუ მოლოდინი, რამაც შესაძლოა მისი მხრიდან საკუთარი ქცევის დამატებითი კონტროლი გამოიწვიოს.

— პროფესიული საგანმანათლებლო დაწესებულებები

კოლეჯებში ვიდეომონიტორინგის განხორციელების კანონიერების შესწავლის შედეგად დადგინდა, რომ მიმდინარეობდა კოლეჯების შენობა-ნაგებობების როგორც შიდა (იგულისხმება სასწავლო აუდიტორიებიც), ისე – გარე პერიმეტრის ვიდეომონიტორინგი, რის საფუძვლადაც კოლეჯების წარმომადგენლები უთითებდნენ კოლეჯის საკუთრების, მათ შორის ხსენებულ აუდიტორიებში განთავსებული ძვირადღირებული მოწყობილობებისა და ინვენტარის, დაცვას. აღსანიშნავია, რომ ხსენებულ სივრცეებში მიმდინარეობდა სასწავლო პროცესი და, შესაბამისად, წარმოადგენდა კოლეჯის სტუდენტებისა და პედაგოგების სასწავლო/სამუშაო სივრცეს.

განსახილველ შემთხვევაში სამსახურმა განმარტა, რომ საკუთრების უფლების დაცვა მართლაც შესაძლებელია კოლეჯის ლეგიტიმური მიზანი იყოს, თუმცა ორივე კოლეჯში ყოველწლიურად ტარდებოდა ინვენტარიზაცია. ამასთან, კოლეჯის პედაგოგებთან დადებული შრომითი ხელშეკრულებები ითვალისწინებდა დასაქმებულების პასუხისმგებლობას კოლეჯის მატერიალურ ქონებაზე და სწორედ მათ ვალდებულებას განეკუთვნებოდა ხსენებულ აუდიტორიებში განთავსებული ინვენტარის, კერძოდ, მოწყობილობებისა და ნივთების დაკარგვის/დაზიანების შემთხვევების შემოწმება. ამასთან, სამსახურმა მიუთითა, რომ აუდიტორია წარმოადგენს პედაგოგების სამუშაო სივრცეს, სადაც, გარდა სწავლებისა, პედაგოგები კომუნიკაციას ამყარებენ სტუდენტებთან და ავითარებენ სოციალურ იდენტობას, რაც უმნიშვნელოვანესია პიროვნების თავისუფალი განვითარების უფლების რეალიზაციისათვის და ექცევა პირადი ცხოვრების უფლებით დაცულ სფეროში. ყოველივე აღნიშნულიდან გამომდინარე, სასწავლო აუდიტორიებში ვიდეომონიტორინგი კანონის მოთხოვნებთან შესაბამისად არ იქნა მიჩნეული.

ასევე, შემოწმების ფარგლებში დადგინდა, რომ ერთ-ერთი კოლეჯის შიდა პერიმეტრის ზოგიერთ სივრცეში, მიუხედავად მიმდინარე ვიდეომონიტორინგისა, გამაფრთხილებელი ნიშნები განთავსებული არ იყო, რაც კანონის მე-10 მუხლის მე-8 პუნქტის მოთხოვნათა დარღვევად შეფასდა. გარდა ამისა, გამოიკვეთა კოლეჯების მხრიდან მონაცემთა უსაფრთხოების დარღვევები. კერძოდ, დადგინდა, რომ კოლეჯების ვიდეოჩამწერ მოწყობილობებში არ აღირიცხებოდა ვიდეოჩანაწერების გადახვევა/დათვალიერება. ამასთან, ვიდეოსათვალთვალო სისტემებში მონაცემთა შენახვის ვადები მნიშვნელოვნად აღემატებოდა ამავე სისტემებში ე. წ. „ლოგ ჩანაწერების“ შენახვის ვადებს. ასევე გამოიკვეთა, რომ

არაუფლებამოსილი პირებს შეეძლოთ ვიდეოსათვალთვალო სისტემაზე რეალურ დროში დაკვირვება.

სამსახურის გადაწყვეტილებით, სკოლები და მანდატურის სამსახური ზემოხსენებულ დარღვევებთან დაკავშირებით ცნობილ იქნენ სამართალდამრღვევებად კანონის 69-ე და 76-ე მუხლებით გათვალისწინებული ადმინისტრაციული სამართალდარღვევების ჩადენაში, ხოლო კოლეჯები ამავე კანონის 76-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევების ჩადენაში. იმავდროულად, გაიცა დავალებები ზემოხსენებული დარღვევების აღმოფხვრის მიზნით.

— უნივერსიტეტები

სამსახურმა გეგმურად შეისწავლა 2 (ორი) კერძო და 2 (ორი) საჯარო უნივერსიტეტის მიერ სასწავლო პროცესის მართვის ელექტრონული პორტალის (შემდგომში — პორტალი) მეშვეობით სტუდენტთა პერსონალური მონაცემების დამუშავების კანონიერება. აღნიშნული პორტალების მეშვეობით უნივერსიტეტები ამუშავებდნენ 34 882-ზე (ოცდათოთხმეტი ათას რვაას ოთხმოცდაორზე) მეტი სტუდენტის მონაცემებს.

ერთ-ერთი უნივერსიტეტის შემოწმების შედეგად დადგინდა, რომ პორტალის მონაცემთა ბაზაზე პირდაპირი წვდომის შემთხვევაში არ აღირიცხებოდა სტუდენტების მონაცემების მიმართ შესრულებულ მოქმედებები; 3 (სამი) უნივერსიტეტის შემოწმების ფარგლებში კი გამოიკვეთა შემთხვევები, როდესაც, ზოგიერთი თანამშრომლის სამსახურებრივი ფუნქცია-მოვალეობებიდან გამომდინარე, ბუნდოვანი იყო სტუდენტების მონაცემებზე წვდომის საჭიროება. 2 (ორი) უნივერსიტეტის შემთხვევაში ამავე უნივერსიტეტების თანამშრომლებს სასწავლო პორტალებზე სტუდენტების პერსონალურ მონაცემებზე წვდომა შეეძლოთ სისტემაში ავტორიზაციის გარეშე, ხოლო ავტორიზაციისას არ სარგებლობდნენ სათანადო სირთულის კომპლექსური პაროლებით და განპიროვნებული მომხმარებლის ანგარიშებით. ერთ-ერთი უნივერსიტეტის პორტალის მეშვეობით სტუდენტების მონაცემების ინტერნეტით გადაცემა არ იყო უზრუნველყოფილი დაშიფრული ფორმით (კერძოდ, არ გამოიყენებოდა „https“ პროტოკოლი). სამსახურის შეფასებით ზემოაღნიშნული გარემოებები, მათ შორის – მონაცემებზე წვდომის უფლებამოსილების მქონე პირების ფართო წრისა და სტუდენტების მონაცემთა დიდი მოცულობის გათვალისწინებით, ქმნიდა მონაცემების უკანონო გამჟღავნების ან სხვაგვარად დამუშავების მნიშვნელოვან საფრთხეებს.

ერთ-ერთი შემოწმების ფარგლებში გამოიკვეთა, რომ უნივერსიტეტი სტუდენტის განსაკუთრებული კატეგორიის მონაცემს, კერძოდ, ინფორმაციას ეთნიკური წარმომავლობის (ეროვნების) შესახებ, ამუშავებდა სათანადო სამართლებრივი საფუძვლის (მათ შორის – სტუდენტის წერილობითი თანხმობის) გარეშე. უნივერსიტეტმა შემოწმების ფარგლებში დაიწყო წერილობითი თანხმობის მოპოვების მიზნით ზომების განხორციელება. აღნიშნულიდან გამომდინარე, უნივერსიტეტის მიმართ დადგინდა კანონის მე-6 მუხლის დარღვევა.

ასევე, ერთ-ერთი უნივერსიტეტი, სათანადო საჭიროების გარეშე, მონაცემთა დამუშავების კანონიერი მიზნის არაპროპორციული მოცულობით ამუშავებდა სტუდენტების ისეთ მონაცემებს, როგორებიცაა, მაგალითად, სტუდენტის ოჯახური მდგომარეობა, მშობლების ელექტრონული ფოსტის მისამართი, ასევე, სტუდენტისთვის სკოლაში ოქროს ან ვერცხლის მედლის მინიჭების თაობაზე ინფორმაცია. იმდენად, რამდენადაც შემოწმების ფარგლებში უნივერსიტეტმა ვერ დაასაბუთა ჩამოთვლილი მონაცემების დამუშავების კონკრეტული საჭიროება, ქმედება სამსახურის მიერ შეფასდა, როგორც მონაცემთა მინიმიზაციის პრინციპის დარღვევა.

შემოწმებების ფარგლებში ასევე გამოიკვეთა, რომ ზოგიერთ უნივერსიტეტს არ ჰქონდა შეფასებული პორტალში სტუდენტების მონაცემთა შენახვის ვადები და ამ ვადების ამოწურვის შემდგომ მონაცემთა მიმართ კანონით გათვალისწინებული ღონისძიებების გატარების საკითხები, რაც მონაცემების არაპროპორციული ვადით შენახვის რისკებს ქმნიდა.

სამსახურის გადაწყვეტილებით, ჩატარებული შემოწმებების შედეგად ერთ-ერთ უნივერსიტეტს ადმინისტრაციული პასუხისმგებლობა დაეკისრა კანონის 68-ე და 76-ე მუხლებით, ხოლო მეორეს — 2011 წლის 28 დეკემბერს მიღებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 44-ე და 46-ე მუხლებით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის. იმავდროულად, უნივერსიტეტებს დაევალათ შემოწმების ფარგლებში გამოვლენილი დარღვევების აღმოფხვრა.

სამსახურმა გეგმურად შეისწავლა სსიპ — „საქართველოს შოთა რუსთაველის თეატრისა და კინოს სახელმწიფო უნივერსიტეტის“ მიერ აბიტურიენტთა და მობილობის მსურველ სტუდენტთა პერსონალური მონაცემების შემცველი ინფორმაციის ვებგვერდზე გასაჯაროების კანონიერება.

შემოწმების შედეგად დადგინდა, რომ უნივერსიტეტი ვებგვერდზე პროაქტიულად აქვეყნებდა აბიტურიენტთა და მობილობის მსურველ სტუდენტთა პერსონალური მონაცემების შემცველ, სხვადასხვა შინაარსის ინფორმაციას. ვებგვერდზე გასაჯაროებული ინფორმაცია მოიცავდა გამოცდაზე დაშვებული აბიტურიენტების/მობილობის მსურველი სტუდენტების სიას (აბიტურიენტთა/სტუდენტთა სახელსა და გვარს, ასევე – გამოცდაზე გამოცხადების კონკრეტულ დღესა და საათს, გამოცდის ჩატარების ადგილმდებარეობას (მისამართი)); გამოცდაზე აპელაციით დაშვებულ აბიტურიენტთა/მობილობის მსურველი სტუდენტების სიას (აბიტურიენტთა/სტუდენტთა სახელს და გვარს, ასევე – მათი გამოცდაზე გამოცხადების კონკრეტულ დღესა და საათს); მობილობის შემოქმედებითი კონკურსის საბოლოო შედეგებს (აბიტურიენტთა სახელს, გვარსა და გამოცდაზე მიღებულ ქულას).

უნივერსიტეტის ვებგვერდზე განთავსებულ აბიტურიენტთა და მობილობის მსურველ სტუდენტთა პერსონალური მონაცემების შემცველი ინფორმაციის იმ ნაწილთან დაკავშირებით, რომელიც თარიღდებოდა 2023 წლით, უნივერსიტეტმა განმარტა, რომ მათი წაშლა უნივერსიტეტს გამორჩა. აღნიშნულიდან გამომდინარე, დადასტურდა, რომ შემოწმების პერიოდამდე 2023 წლის ინფორმაციის გასაჯაროების სამართლებრივი საფუძველი არ არსებობდა. რაც შეეხება აბიტურიენტთა და მობილობის მსურველ სტუდენტთა პერსონალური

მონაცემების შემცველი 2024 წლის ინფორმაციის ვებგვერდზე გასაჯაროებას, აღნიშნულის სამართლებრივ საფუძვლად უნივერსიტეტმა მნიშვნელოვანი საჯარო ინტერესის, კერძოდ, საზოგადოებრივი ინტერესის დაცვის აუცილებლობაზე მიუთითა. უნივერსიტეტის განმარტებით, შემოქმედებითი ტურის გამოცდები ყოველ წელს ხდება საზოგადოების განხილვის საგანი და ვრცელდება ბრალდებები გამოცდების უსამართლოდ/არაობიექტურად ჩატარებასთან დაკავშირებით, რაც, თავის მხრივ, საფრთხეს უქმნის უნივერსიტეტის რეპუტაციას. აღნიშნულიდან გამომდინარე, სწორედ შემოქმედებითი ტურების სამართლიანად და გამჭვირვალედ მიმდინარეობის დასადასტურებლად დანერგა უნივერსიტეტმა ინფორმაციის ვებგვერდზე გამოქვეყნების პრაქტიკა. აღსანიშნავია, რომ შემოწმების ფარგლებში უნივერსიტეტმა ვერ დაასაბუთა, მის მიმართ რაიმე ტიპის საჯარო ბრალდებების და მცდარი ინფორმაციის გავრცელების ფაქტების არსებობა, რაც დაადასტურებდა უნივერსიტეტის რეპუტაციისა და საზოგადოების მხრიდან მის მიმართ ნდობის შელახვის საფრთხის რეალურობას. უნივერსიტეტმა ვერც ის გარემოება განმარტა, თუ რით უკავშირდება და როგორ უზრუნველყოფს აბიტურიენტების/სტუდენტების მაიდენტიფიცირებელი მონაცემების გამოქვეყნება შემოქმედებითი ტურების მიმდინარეობის გამჭვირვალობასა და აღნიშნული პროცესის მიმართ საზოგადოებაში სამართლიანობის განცდის ჩამოყალიბებას.

სამსახურმა ასევე არ გაიზიარა უნივერსიტეტის განმარტება, რომლის მიხედვითაც ინფორმაციის ვებგვერდზე გამოქვეყნება უზრუნველყოფდა აბიტურიენტების/მობილობის მსურველი სტუდენტების ინფორმირებას შემოქმედებითი ტურების მიმდინარეობისა და მიღებული შედეგების შესახებ. კერძოდ, სამსახურმა განმარტა, რომ მოცემულ შემთხვევაში, კონკრეტული სტუდენტების (სტუდენტთა შეზღუდული წრის) ინფორმირების მიზნით, მათთან დაკავშირებული მონაცემების საჯაროდ, ნებისმიერი პირისთვის ხელმისაწვდომი ფორმით ვებგვერდზე განთავსება დასახელებული (ინფორმირების) მიზნის აუცილებელ და თანაზომიერ საშუალებად ვერ ჩაითვლებოდა.

ნიშანდობლივია ისიც, რომ შემოწმების მიმდინარეობის პერიოდში უნივერსიტეტმა შეცვალა ინფორმაციის გამოქვეყნების პროცესი და ნაცვლად მონაცემების იდენტიფიცირებული ფორმით (პირის სახელისა და გვარის მითითებით) გამოქვეყნებისა, შემოქმედებითი ტურების მიმდინარეობისა და შედეგების შესახებ ინფორმაციის გამოქვეყნების გადაწყვეტილება მიიღო აბიტურიენტებისთვის/სტუდენტებისთვის მინიჭებული უნიკალური კოდების გამოყენებით. ამასთან, შემოწმების ფარგლებში უნივერსიტეტის მიერ მოწოდებული ინფორმაციით, 2024-2025 სასწავლო წლის შემოდგომის სემესტრის მობილობის საბოლოო შედეგები, დაწესებულებისადმი აბიტურიენტებისა თუ სტუდენტების ნდობის ჩამოყალიბების მიზნით, სტუდენტთა თანხმობით იდენტიფიცირებული ფორმით გამოაქვეყნა აბიტურიენტთა/სტუდენტთა დახურულ ჯგუფში. საგულისხმოა, რომ თანხმობის არსებობის დამადასტურებელი მტკიცებულებების წარმოდგენა უნივერსიტეტმა ვერ შეძლო. ასევე დადასტურდა, რომ თანხმობის მოპოვებამდე დამუშავების კონკრეტული მიზნის შესახებ მონაცემთა სუბიექტებისთვის ინფორმაციის მიწოდება არ ხდებოდა, რის გამოც თანხმობა ვერ აკმაყოფილებდა კანონის მე-3 მუხლის „მ“

ქვეპუნქტით განსაზღვრულ კრიტერიუმებს. ნიშანდობლივია, რომ ამავე შემოწმების ფარგლებში სამსახურმა იმსჯელა უნივერსიტეტის მიერ სტუდენტების მონაცემთა დამუშავების პროცესში სამართლიანობის პრინციპის დაცვის ვალდებულებაზეც და აღნიშნა, რომ უნივერსიტეტის მიერ არჩეული მონაცემთა დამუშავების ფორმა (დახურულ ჯგუფში მონაცემების სხვა სტუდენტებისთვის ხელმისაწვდომად გახდომა) ასევე არ წარმოადგენდა უნივერსიტეტის მიზნის — აბიტურიენტებსა თუ სტუდენტებში ნდობის ჩამოყალიბების — აუცილებელ და პროპორციულ საშუალებას და თანხმობის არსებობის შემთხვევაშიც ქმნიდა მონაცემთა სუბიექტებისთვის გაუმართლებელი ზიანის მიყენების რისკებს.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, დადგინდა, რომ უნივერსიტეტს აბიტურიენტებისა და მობილობის მსურველი სტუდენტების მონაცემების შემცველი ინფორმაცია ვებგვერდზე გასაჯაროებული ჰქონდა კანონის მე-5 მუხლით გათვალისწინებული შესაბამისი სამართლებრივი საფუძვლების გარეშე.

სამსახურის გადაწყვეტილებით, უნივერსიტეტს დაეკისრა პასუხისმგებლობა კანონის 67-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის და დაევალა ზემოხსენებული დარღვევის აღმოფხვრა.

დ. შრომითი ურთიერთობის ფარგლებში მონაცემების დამუშავება

— მუნიციპალიტეტების მიერ მონაცემთა გასაჯაროება

სამსახურმა გეგმურად შეისწავლა 5 (ხუთი) ადგილობრივი თვითმმართველობის ორგანოს (მერიისა და საკრებულოების) მიერ პერსონალური მონაცემების შემცველი სამართლებრივი აქტების ოფიციალური ვებგვერდების საშუალებით გასაჯაროების კანონიერება. შემოწმებების ფარგლებში გამოიკვეთა, რომ მუნიციპალიტეტების ვებგვერდებზე, საჯარო/საზოგადოებრივი ინტერესის შემცველ სამართლებრივ აქტებთან ერთად, ხშირ შემთხვევაში გამოქვეყნებული იყო დაწესებულებების მიერ შრომითი ურთიერთობის ფარგლებში გამოცემული ისეთი სამართლებრივი აქტები, როგორებიცაა: დასაქმებული პირების შვებულების, მივლინების, თანამდებობაზე დანიშვნის, თანამდებობიდან გათავისუფლების, დისციპლინური პასუხისმგებლობის ზომის შეფარდების თაობაზე და სხვა.

შემოწმების ფარგლებში დადგინდა, რომ მუნიციპალიტეტების ვებგვერდებზე გამოქვეყნებული სამართლებრივი აქტები შეიცავდა მერიაში/საკრებულოში დასაქმებული პირების (მათ შორის – დამლაგებლის, მძღოლის, სპეციალისტების პოზიციებზე დასაქმებული პირების და სხვა) შემდეგ მონაცემებს: პირის სახელს, გვარს, სამსახურებრივ პოზიციას, შვებულების პერიოდსა და მიზეზს (მათ შორის – გართულებული მშობიარობის გამო დეკრეტული შვებულების თაობაზე), მივლინების პერიოდსა და ადგილს, თანამდებობაზე დანიშვნისა და გათავისუფლების თარიღებს, თანამდებობრივი სარგოს შესახებ ინფორმაციას, დისციპლინური წარმოების შესახებ დეტალებს, სატელეფონო ნომრებს და ა. შ.

ვებგვერდზე გამოქვეყნებული, პერსონალური მონაცემების შემცველი დოკუმენტაციის შინაარსი, სიმრავლე და მათი გამოცემის პერიოდები ადასტურებდა, რომ პერსონალური მონაცემების შემცველი სამართლებრივი აქტების გასაჯაროება შემოწმებული ადგილობრივი თვითმმართველობის ორგანოებისთვის დადგენილ პრაქტიკას წარმოადგენდა. აღნიშნული აქტების გამოქვეყნებას მუნიციპალიტეტების ორგანოების უმრავლესობა პროაქტიულად გამოსაქვეყნებელ საჯარო ინფორმაციად მიიჩნევდა.

ადგილობრივი თვითმმართველობის ორგანოების მიერ წარმოდგენილი პოზიციით, მათ შორის შრომითი ურთიერთობის ფარგლებში გამოცემული სამართლებრივი აქტების ვებგვერდზე გამოქვეყნება ემსახურებოდა მუნიციპალიტეტის საქმიანობის გამჭვირვალობის უზრუნველყოფას და მაღალი საჯარო/საზოგადოებრივი ინტერესის დაკმაყოფილებას. 2 (ორი) შემთხვევაში ადგილობრივი თვითმმართველობის ორგანოებმა მონაცემების დამუშავების საფუძვლად ასევე მიუთითეს მონაცემთა სუბიექტების თანხმობა. ერთ-ერთ შემთხვევაში გამოიკვეთა, რომ განსაკუთრებული კატეგორიის მონაცემის დამუშავებაზე მუნიციპალიტეტი ზეპირად იღებდა თანხმობას (რაც არ აკმაყოფილებს კანონის მე-6 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტის მოთხოვნებს); ხოლო მეორე შემთხვევაში, მიუხედავად მონაცემთა სუბიექტების თანხმობის არსებობისა, დარღვეული იყო მონაცემთა დამუშავების პრინციპები, ვინაიდან საკრებულოს მიერ ვერ მიუთითა მონაცემთა დამუშავების კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზანი.

დასაქმებული პირების პერსონალური მონაცემების შემცველი სამართლებრივი აქტების ვებგვერდზე გამოქვეყნებასთან მიმართებით სამსახურის მიერ არ იქნა გაზიარებული ადგილობრივი თვითმმართველობის ორგანოების პოზიცია, რომლის თანახმადაც, მონაცემთა გასაჯაროება ემსახურებოდა მაღალი საჯარო/საზოგადოებრივი ინტერესის დაცვას. სამსახურმა განმარტა, რომ პირადი ინფორმაციის დაცვის სტანდარტი განსხვავებულია თანამდებობის პირთა და მოსამსახურეთა/მოხელეთა შემთხვევებში. აღნიშნულს განაპირობებს საზოგადოების, ასევე, ანგარიშვალდებულებისა და თანამდებობის პირთა და ადმინისტრაციულ ორგანოთა მიმართ მომეტებული საჯარო ინტერესის არსებობა. საჯარო ინტერესის დაცვის მიზნით პერსონალური მონაცემების დამუშავებისას საჯარო ინტერესი უნდა განისაზღვროს კანონის საფუძველზე. ინტერესთა შეპირისპირებისას გათვალისწინებული უნდა იქნეს კანონში მოცემული ფორმულირება, კანონით განსაზღვრული საჯარო ინტერესის შინაარსი, რომლის დაცვის მიზანიც ამართლებს პერსონალური მონაცემების დამუშავებას. საჯარო ინტერესის საფუძვლით პერსონალურ მონაცემთა დაცვის უფლების შეზღუდვა გამართლებულია მხოლოდ იმ შემთხვევაში, თუ ეს არის აუცილებელი და პროპორციული შეზღუდვის მიზანთან. ამასთან, პერსონალური მონაცემების დამუშავება მნიშვნელოვანი საჯარო ინტერესის დასაცავად უნდა ემსახურებოდეს ლეგიტიმური მიზნის მიღწევას და ეს ღონისძიება უნდა იყოს გამოსადეგი, აუცილებელი და თანაზომიერი. ამასთან, სამსახურმა აღნიშნა, რომ მომეტებული საზოგადოებრივი ინტერესი მოიცავს ისეთ საკითხებს, რომლებმაც შესაძლოა საზოგადოებაში აზრთა სხვადასხვაობა გამოიწვიოს მნიშვნელოვან სოციალურ

საკითხებთან ან პრობლემებთან დაკავშირებით და რომლებთან მიმართებითაც საზოგადოებას გააჩნია ინფორმირების ინტერესი.

საჯარო მოხელეების/საჯარო მოსამსახურეების მონაცემების გასაჯაროებასთან დაკავშირებით მსჯელობისას სამსახურმა მიუთითა საქართველოს ზოგადი ადმინისტრაციული კოდექსის 28-ე და 44-ე მუხლებზე, რომელიც განმარტავს, რომ საჯარო ინფორმაცია ღიაა, გარდა კანონით გათვალისწინებული შემთხვევებისა და დადგენილი წესით სახელმწიფო, პროფესიული ან კომერციული საიდუმლოებისთვის ან პერსონალური მონაცემებისთვის მიკუთვნებული ინფორმაციისა. ამასთან, საჯარო დაწესებულება ვალდებულია პირის პერსონალური მონაცემები არ გაახმაუროს ამ პირის თანხმობის გარეშე, გარდა კანონით გათვალისწინებული შემთხვევებისა, როდესაც ეს აუცილებელია სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, საჯარო ინტერესების, ჯანმრთელობის ან სხვათა უფლებების დასაცავად. აღნიშნული ნორმა უშვებს მხოლოდ თანამდებობის პირის და თანამდებობაზე წარდგენილი კანდიდატის მონაცემების საჯაროობას.

სამსახურის გადაწყვეტილებით, ადგილობრივი თვითმმართველობის ორგანოებს ზემოაღნიშნულ დარღვევებთან დაკავშირებით პასუხისმგებლობა დაეკისრათ კანონის 66-ე, 67-ე და 68-ე მუხლებით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის. ამასთან, მათ დაევალათ სამართლებრივი საფუძვლის გარეშე და დამუშავების პრინციპების დარღვევით მუნიციპალიტეტების ოფიციალურ ვებგვერდებზე განთავსებული სამართლებრივი აქტების წაშლა.

— სსიპ — „დასაქმების ხელშეწყობის სახელმწიფო სააგენტო“

სამსახურმა, სააგენტოს მიერ საზოგადოებრივ სამუშაოებზე დასაქმების ხელშეწყობის ქვეპროგრამის განხორციელების ფარგლებში, გეგმურად შეისწავლა დასაქმების საინფორმაციო სისტემის (შემდგომში — პორტალი) მეშვეობით მოსარგებლეების მონაცემთა დამუშავების კანონიერება. აღნიშნული პორტალი განკუთვნილია ქვეპროგრამის ფარგლებში მიმწოდებლის (ადმინისტრაციული ორგანო, რომელიც ქმნის საზოგადოებრივი სამუშაოს ვაკანსიას) მიერ საზოგადოებრივი სამუშაოების ვაკანსიების გამოქვეყნებისთვის და მოსარგებლეების შესახებ ელექტრონული ჩანაწერების შესაქმნელად. შემოწმების დროისთვის პორტალის მეშვეობით ხელმისაწვდომი იყო ქვეპროგრამის 235 789 (ორას ოცდათხუთმეტი ათას შვიდას ოთხმოცდაცხრა) მოსარგებლის შესახებ ინფორმაცია.

შემოწმების ფარგლებში დადგინდა, რომ პორტალში აისახება მოსარგებლის სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი, ასაკი, სქესი, სარეიტინგო ქულა, მოსარგებლის ოჯახის საიდენტიფიკაციო კოდი და სხვა; პორტალის ტექნიკურ მომსახურებას კი უზრუნველყოფს სსიპ — „ინფორმაციული ტექნოლოგიების სააგენტო“, რაც მოიცავს როგორც პორტალის მომხმარებელთა მართვას, ასევე – ქვეპროგრამის მუშაობის პროცესში დაფიქსირებული

პრობლემების აღმოფხვრასა და საჭიროების შემთხვევაში შესაბამისი ტექნიკური ცვლილებების განხორციელებას.

სამსახურის გადაწყვეტილებით, სააგენტოს დაეკისრა პასუხისმგებლობა კანონის 66-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის. ამავე კანონის 76-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის პასუხისმგებლობა დაეკისრა სსიპ — „ინფორმაციული ტექნოლოგიების სააგენტოს“. იმავდროულად, სააგენტოს და სსიპ — „ინფორმაციული ტექნოლოგიების სააგენტოს“ დაევალათ ზემოხსენებული დარღვევების აღმოფხვრა.

— საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო

სამსახურმა გეგმურად შეისწავლა საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს (შემდგომში — სამინისტრო) მიერ ელექტრონული პორტალის მეშვეობით შრომით მიგრანტთა პერსონალური მონაცემების მოპოვებისა და შენახვის გზით დამუშავების კანონიერება. აღსანიშნავია, რომ შემოწმების პერიოდისთვის სამინისტროს ელექტრონულ სისტემაში, რომლის ტექნიკურ მომსახურებას უზრუნველყოფს სსიპ — „ინფორმაციული ტექნოლოგიების სააგენტო“ (შემდგომში — სააგენტო), ასახული იყო 33 411 (ოცდაცამეტი ათას ოთხას თერთმეტი) იმიგრანტის და 469 (ოთხას სამოცდაცხრა) ემიგრანტის მონაცემები.

შემოწმების შედეგად დადგინდა, რომ ელექტრონულ სისტემაში აისახება: ემიგრანტების სახელი და გვარი, დაბადების თარიღი, პირადი ნომერი, სქესი, მოქალაქეობა, პროფესია, სამუშაო გამოცდილება, კვალიფიკაცია, დასაქმების ქვეყანა, საშუალო თვიური ანაზღაურება და სხვა; ხოლო იმიგრანტის შესახებ იმგვარი პერსონალური მონაცემები, როგორებიცაა: სახელი და გვარი, დაბადების თარიღი, სქესი, წარმოშობის ქვეყანა, მოქალაქეობა, პასპორტის ნომერი, ვიზის ნომერი და თარიღი, ბინადრობის ნებართვის გაცემის თარიღი და მოქმედების ვადა, პოზიცია, ანაზღაურების ოდენობა, განათლება, პროფესია და სხვა. აღსანიშნავია, რომ შრომითი მიგრაციის ზედამხედველობა განეკუთვნება სამინისტროს კომპეტენციას; ელექტრონული სისტემის არსებობის მიზანს კი წარმოადგენს შრომით მიგრანტთა შესახებ ინფორმაციის ერთ სივრცეში თავმოყრა, რაც აადვილებს სამინისტროს მიერ საშუამავლო კომპანიებისა და ადგილობრივი დამსაქმებლებისთვის კანონმდებლობით დადგენილი მოთხოვნების შესრულების მონიტორინგს, ასევე – აღნიშნული ინფორმაციის დამუშავებას, ანალიზსა და სტატისტიკის წარმოებას.

შემოწმების ფარგლებში სამინისტროს წარმომადგენლის განმარტებით, მიგრაციის პოლიტიკის ფორმირებისთვის სახელმწიფოს შესაძლოა ნებისმიერ დროს დასჭირდეს სხვადასხვა სახის ინფორმაციის დამუშავება (თუნდაც გასული წლების მიხედვით როგორც ემიგრაციის, ასევე იმიგრაციის მიმართულებით), რის გამოც დაგეგმილი იყო შრომითი მიგრანტების მონაცემების უვადოდ შენახვა. აღნიშნული ასევე ემსახურება შრომითი იმიგრანტების იდენტიფიცირების

მიზანსაც. სამსახურის განმარტებით, დასახელებული მიზნებისთვის შესაძლოა საჭირო იყოს მონაცემების ხანგრძლივად შენახვა, თუმცა ქვეყანაში მიგრაციის პოლიტიკის ფორმირებისთვის შესაძლოა არ იყოს გამოსადეგი რამდენიმე ათწლეულის წინანდელი ინფორმაცია. ანალოგიურად, ბუნდოვანია პირის მუდმივად იდენტიფიცირების საჭიროება, ადამიანის შრომითი უნარებისა და სიცოცხლის საშუალო ხანგრძლივობის გათვალისწინებით.

მოცემულ შემთხვევაში ასევე გამოიკვეთა, რომ მონაცემებზე დაშვების მქონე ერთ-ერთ თანამშრომელს, მასზე დაკისრებული მოვალეობების შესასრულებლად ელექტრონული სისტემის მეშვეობით დამუშავებულ შრომითი იმიგრანტების მონაცემებზე წვდომა არ ესაჭიროებოდა. ამასთანავე დადგინდა, რომ ელექტრონული სისტემის მონაცემთა ბაზიდან განხორციელებული მოქმედებები არ აღირიცხებოდა. აღნიშნული გარემოებები მიუთითებდა მონაცემების დასაცავად საჭირო ორგანიზაციულ-ტექნიკური ზომების მიუღებლობაზე, რაც მონაცემთა შემდგომი არამართლზომიერი დამუშავების თვალსაზრისით მნიშვნელოვანი რისკების შემცველია.

სამსახურის გადაწყვეტილებით, სამინისტროს და სააგენტოს დაეკისრათ პასუხისმგებლობა კანონის 76-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის. იმავდროულად, მათ დაევალათ ზემოხსენებული დარღვევების აღმოფხვრა.

ე. ჯანდაცვის სფეროში მონაცემების დამუშავება

— სსიპ — „ლ. საყვარელიძის სახელობის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნული ცენტრი

პერსონალურ მონაცემთა დაცვის სამსახურმა გეგმურად შეისწავლა სსიპ — „ლ. საყვარელიძის სახელობის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნული ცენტრის“ (შემდგომში – ცენტრი) მიერ დაავადებათა ადრეული გამოვლენისა და სკრინინგის სახელმწიფო პროგრამის განხორციელებისას, ძუძუსა და საშვილოსნოს ყელის კიბოს სკრინინგის ფარგლებში, კიბოს ერთიანი საინფორმაციო სისტემის საშუალებით პერსონალური მონაცემების დამუშავების კანონიერება. აღსანიშნავია, რომ, მითითებული მომსახურების ფარგლებში, ცენტრის საქმიანობა დაკავშირებულია ქალთა მნიშვნელოვანი მოცულობის პერსონალური, მათ შორის – განსაკუთრებული კატეგორიის მონაცემების დამუშავებასთან. სისტემის მეშვეობით შემოწმების პერიოდისთვის დამუშავებული იყო 159 364 (ას ორმოცდაცხრამეტი ათას სამას სამოცდაოთხი) ბენეფიციარის მონაცემები.

შემოწმების ფარგლებში დადგინდა, რომ კიბოს ერთიანი საინფორმაციო სისტემის ადმინისტრირების პროცესში ცენტრს ტექნიკურ მხარდაჭერას უწევს სსიპ — „ინფორმაციული ტექნოლოგიების სააგენტო“ (შემდგომში — სააგენტო), რომელიც სამინისტროსა და მის დაქვემდებარებაში არსებული საჯარო სამართლის იურიდიული პირების ინფორმაციული ტექნოლოგიების მხარდაჭერის მიზნით არის შექმნილი. მოცემულ შემთხვევაში დადგინდა, რომ ქვეპროგრამის

განხორციელების ფარგლებში როგორც ცენტრის, ასევე სააგენტოს მიერ არ იყო მიღებული უსაფრთხოების სათანადო ტექნიკური და ორგანიზაციული ზომები, რაც კანონის 27-ე მუხლის დარღვევას წარმოადგენს.

კერძოდ, კიბოს ერთიანი საინფორმაციო სისტემის მეშვეობით პროგრამის ფარგლებში დამუშავებულ მონაცემებზე წვდომა ჰქონდა ცენტრის 31 (ოცდათერთმეტ) თანამშრომელს, რომელთა უმრავლესობას მათზე დაკისრებული მოვალეობების შესასრულებლად აღნიშნული წვდომის საჭიროება არ ჰქონდა; მონაცემთა უსაფრთხოებისთვის კი აუცილებელია მონაცემთა დამუშავების პროცესები წარიმართოს იმ ფორმით, რომ მასზე წვდომა მხოლოდ შესაბამისი საჭიროების მქონე პირებს ჰქონდეთ. ამავდროულად, შეფასებული, გათვალისწინებული და მაქსიმალურად შემცირებული უნდა იქნეს გარეშე პირების მიერ მონაცემებზე წვდომისა და გამოყენების საფრთხეები; ხსენებული მომხმარებლებისთვის კიბოს ერთიან საინფორმაციო სისტემაზე წვდომის უფლების გაუქმება კი ცენტრმა სააგენტოს მოსთხოვა მხოლოდ შემოწმების მიმდინარეობის ფარგლებში. შესაბამისად, წვდომის უფლების გაუქმების მოთხოვნამდე ცენტრის მიერ არ იყო გათვალისწინებული შესაბამისი უსაფრთხოების ზომები, რაც მონაცემებზე არაუფლებამოსილ პირთა დაშვებას შეზღუდავდა. ამასთანავე, ცენტრის თანამშრომლების მიერ კიბოს ერთიანი საინფორმაციო სისტემის მეშვეობით მონაცემების მიმართ განხორციელებული მოქმედებებიდან არ აღირიცხებოდა მონაცემების დათვალიერება და ექსპორტი; სისტემის მონაცემთა ბაზიდან კიბოს ერთიან საინფორმაციო სისტემაში დაცულ ინფორმაციაზე პირდაპირი წვდომის შემთხვევაში კი არ აღირიცხებოდა მონაცემთა მიმართ განხორციელებული მოქმედებები.

სამსახურის გადაწყვეტილებით სსიპ — „ლ. საყვარელიძის სახელობის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნული ცენტრი“ და სსიპ — „ინფორმაციული ტექნოლოგიების სააგენტო“ ცნობილ იქნენ სამართალდამრღვევებად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 76-ე მუხლის პირველი პუნქტების „ა“ ქვეპუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში და ადმინისტრაციული სახდელის სახით შეეფარდათ გაფრთხილება. ამავდროულად, სსიპ — „ინფორმაციული ტექნოლოგიების სააგენტოს“ დაევალა მონაცემთა უსაფრთხოების დასაცავად სათანადო ორგანიზაციულ-ტექნიკური ზომების მიღება.

— კასპისა და თელავის მუნიციპალიტეტების მერიები

პერსონალურ მონაცემთა დაცვის სამსახურმა სოციალური დაცვის სხვადასხვა ქვეპროგრამის განხორციელების ფარგლებში მონაცემთა დამუშავების საკითხებთან დაკავშირებით გეგმურად შეამოწმა რამდენიმე მუნიციპალიტეტის მერია. მათ შორის შემოწმდა კასპის მუნიციპალიტეტის მერიის მიერ უფასო მედიკამენტებით უზრუნველყოფის ქვეპროგრამის, ასევე – თელავის მუნიციპალიტეტის მერიის მიერ სამედიცინო მომსახურების და მედიკამენტებით

დახმარების ღონისძიებების ქვეპროგრამის განხორციელების პროცესში ბენეფიციართა პერსონალური მონაცემების დამუშავების კანონიერება.

კასპის მუნიციპალიტეტის მერიის შემოწმების ფარგლებში დადგინდა, რომ მერია ბენეფიციართა პერსონალურ მონაცემებს ქვეპროგრამის ფარგლებში რიგ შემთხვევებში კანონის მე-4 მუხლის „გ“ ქვეპუნქტის დარღვევით, კანონიერი მიზნის არაპროპორციული მოცულობით ამუშავებდა. აღსანიშნავია, რომ, ქვეპროგრამის ფარგლებში, სსიპ — „სოციალური მომსახურების სააგენტოს“ სოციალურად დაუცველ პირთა ბაზიდან ბენეფიციართა სოციალური ქულის, ამ ქულის მინიჭების თარიღის, ოჯახის “ID” ნომრის, ოჯახის წარმომადგენლისა და ფაქტობრივი მისამართის შესახებ ინფორმაციის დამუშავების საჭიროება არსებობდა მხოლოდ სოციალურად დაუცველ პენსიონერ ბენეფიციართათვის ერთჯერადი მედიკამენტური დახმარების გაწევის მიზნით. მიუხედავად ამისა, მერია ბენეფიციარების შესახებ სოციალურად დაუცველ პირთა ბაზაში არსებულ ინფორმაციას საჭიროების გარეშე ამუშავებდა ქვეპროგრამით გათვალისწინებული დაავადებების (მაგალითად: ეპილეფსია, ფსორიაზი, ვიტილიგო), ოპერაციების (მაგალითად: კარდიოქირურგიული, მწვავე ინფარქტი, მწვავე ინსულტი) და ონკოლოგიური პაციენტის სიმპტომური მკურნალობის საფუძვლით ქვეპროგრამაში ჩართვის მოთხოვნის შემთხვევაშიც.

კასპის მუნიციპალიტეტის მერიის შემოწმების ფარგლებში ასევე დადგინდა, რომ ქვეპროგრამის ფარგლებში დამუშავებულ მონაცემებზე წვდომის შესაძლებლობა ჰქონდათ იმ პირებსაც, რომელნიც აღნიშნულს არ საჭიროებდნენ. ამასთან, საქმისწარმოების ელექტრონული სისტემის შესაბამის მოდულში და აღნიშნული მოდულის მონაცემთა ბაზაში, კანონის იმპერატიული მოთხოვნის მიუხედავად, სრულყოფილად არ აღირიცხებოდა ქვეპროგრამის ფარგლებში დამუშავებული მონაცემების მიმართ განხორციელებული მოქმედებები. მოცემულ შემთხვევაში ასევე გამოიკვეთა, რომ ბენეფიციარების მონაცემების შემცველი მატერიალური დოკუმენტაცია განთავსებული იყო თანამშრომელთა სამუშაო მაგიდებთან არსებულ სკამებსა და მუყაოს ყუთებზე; დოკუმენტების ამ ფორმით განთავსება კი ქმნის მომეტებულ რისკს, რომ ისინი მარტივად გახდეს ხელმისაწვდომი თუნდაც დღის განმავლობაში ოთახში სხვადასხვა მიზეზით მოხვედრილი მერიის იმ თანამშრომლებისთვის, რომლებსაც არ აქვთ ხსენებულ დოკუმენტაციაზე წვდომის უფლებამოსილება.

თელავის მუნიციპალიტეტის მერიის შემოწმების ფარგლებში დადგინდა, რომ მერია ბენეფიციარების მონაცემების დამუშავების პროცესში სარგებლობდა საერთო საზიარო საქაღალდით, რომელშიც „MS Excel“-ის ფორმატის დოკუმენტების სახით ინახებოდა ბენეფიციარების შესახებ ინფორმაცია. ხსენებულ საქაღალდეზე წვდომა ხორციელდებოდა განპიროვნებული მომხმარებლებითა და პაროლებით, თუმცა არ ხდებოდა საქაღალდეში არსებული მონაცემების მიმართ განხორციელებული მოქმედებების აღრიცხვა, რაც მონაცემთა უსაფრთხოების დარღვევაა.

ორივე შემოწმების ფარგლებში დადგინდა, რომ ქვეპროგრამების განხორციელების პროცესში სსიპ — „სახელმწიფო სერვისების განვითარების სააგენტოს“ მონაცემთა ელექტრონულ ბაზაში არსებული ფიზიკური პირის მონაცემები (სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი, მისამართი და ა.

შ.) მერიებს მიეწოდებოდათ შესაბამისი მარეგულირებელი ხელშეკრულების არსებობის გარეშე. აღსანიშნავია, რომ მონაცემების გადაცემის თაობაზე ხელშეკრულების არსებობა ემსახურება მონაცემთა კანონიერად, თანმიმდევრულად და ერთგვაროვნად დამუშავების უზრუნველყოფის მიზნებს, ვინაიდან აღნიშნული დოკუმენტი მოაწესრიგებს დიდი მოცულობის მონაცემების მრავალჯერადი დამუშავების შემთხვევებს და წინასწარ განსაზღვრავს მონაცემთა დამუშავების საფუძვლებსა და მიზნებს, ხელშეკრულების ფარგლებში მისაწოდებელი ინფორმაციის სახეობასა და მოცულობას, ინფორმაციის მიწოდებისა და ელექტრონული ფორმით არსებულ მონაცემთა მიმართ განხორციელებული ქმედებების აღრიცხვის წესს.

სამსახურის გადაწყვეტილებით, კასპის მუნიციპალიტეტის მერია სამართალდამრღვევად იქნა ცნობილი მონაცემთა დამუშავების პრინციპებისა და უსაფრთხოების წესების დარღვევის გამო, ხოლო თელავის მუნიციპალიტეტის მერიას მონაცემთა უსაფრთხოების წესების დარღვევისთვის პასუხისმგებლობა დაეკისრა. იმავდროულად, დაევალა გამოვლენილი დარღვევების აღმოფხვრა.

— სამედიცინო ლაბორატორიების და სტომატოლოგიური კლინიკა

სამსახურმა გეგმურად შეისწავლა სამედიცინო დაწესებულებების — ორი ლაბორატორიისა და ერთი სტომატოლოგიური კლინიკის — მიერ ვიდეომონიტორინგის განხორციელების კანონიერება.

შემოწმებების ფარგლებში გამოიკვეთა, რომ სტომატოლოგიური კლინიკა ქირურგიული და თერაპიული მანიპულაციებისთვის განკუთვნილ კაბინეტებში, ხოლო ერთ-ერთი ლაბორატორია — ლაბორატორიული ტესტირებისთვის ბიოლოგიური მასალის ნიმუშების აღებისა და დამუშავებისთვის განკუთვნილ ოთახებში ვიდეომონიტორინგს ახორციელებდნენ სამედიცინო პერსონალისთვის დაკისრებული უფლებამოსილებების არაჯეროვანი შესრულების თავიდან აცილებისა და შეცდომების დროული იდენტიფიცირების მიზნით. ლაბორატორია საკუთრების დაცვის მიზნით ვიდეომონიტორინგს ახორციელებდა რადიოლოგიის კაბინეტშიც. სამსახურის შეფასებით, ისეთ სივრცეებში, სადაც პაციენტს უტარდება სამედიცინო მანიპულაციები, პირს აქვს თავისი პირადი ცხოვრების დაცულობისა და პატივისცემის ლეგიტიმური და გონივრული მოლოდინი; სამედიცინო მომსახურების მიღების პროცესში დამუშავებული მონაცემების სენსიტიური ხასიათის გათვალისწინებით კი სამსახურმა განმარტა, რომ განსაკუთრებით მნიშვნელოვანია დაცული იქნეს პაციენტის პირადი ცხოვრების ხელშეუხებლობის უფლება; ხოლო სამედიცინო პროცედურების განხორციელებისთვის განკუთვნილ სივრცეში დამონტაჟებული კამერა პირს უკარგავს კონფიდენციალურობის შეგრძნებას და ზღუდავს მისი ქცევის თავისუფლებას. აღნიშნული შემოწმებების ფარგლებში სამსახურმა ვიდეომონიტორინგის სამედიცინო მანიპულაციების ოთახებში განხორციელება მიიჩნია კანონის მე-10 მუხლის მე-4 პუნქტის დარღვევად და აღნიშნულის აღმოსაფხვრელად გასცა შესაბამისი დავალებები.

მოცემულ შემთხვევაში ასევე დადგინდა, რომ სამედიცინო დაწესებულებები ლაბორატორიის ადგილზე გამოძახების თანამშრომლებისთვის განკუთვნილ

სამუშაო ოთახსა და საკონფერენციო დარბაზში ვიდეომონიტორინგს ახორციელებდნენ საკუთრების დაცვის მიზნებისთვის. სამსახურის შეფასებით, მართალია, დამუშავებისთვის პასუხისმგებელი პირების მიერ ქონების დაცვა შეიძლება მიჩნეულ იქნეს ლეგიტიმურ ინტერესად, თუმცა აღნიშნული მიზნის მიღწევა შესაძლებელია სხვა საშუალებებითაც (კერძო დაწესებულებაში არსებული ნივთების, საკუთრებისა და უსაფრთხოების დაცვის გარანტიებია, მაგალითად, ე. წ. დაცვის სერვისით სარგებლობა, შემოსასვლელში შესაბამისი პასუხისმგებელი პირის დაყენება, ნივთებისთვის სპეციალური სათავსოს განსაზღვრა და სხვა). ამასთან, სამსახურმა დაადგინა, რომ სამედიცინო დაწესებულებების მიერ ლაბორატორიის ადგილზე გამოძახების თანამშრომლებისთვის განკუთვნილ სამუშაო ოთახსა და საკონფერენციო დარბაზში ვიდეომონიტორინგის განხორციელება ვერ აკმაყოფილებს დასაქმებულის სამუშაო ადგილის ვიდეომონიტორინგის კანონიერებისთვის აუცილებელ თანაზომიერების ტესტს და წარმოადგენს დასაქმებულის პირადი ცხოვრების დაცულობის უფლებაში არამართლზომიერ ჩარევას. ამდენად, სამსახურის შეფასებით, აღნიშნული სივრცეების ვიდეომონიტორინგი არ იქნა მიჩნეული კანონის მე-10 მუხლის მე-3 პუნქტის მოთხოვნებთან შესაბამისად.

ერთ-ერთი ლაბორატორიის შემოწმების ფარგლებში დადგინდა, რომ ლაბორატორია ვიდეომონიტორინგს ახორციელებდა პაციენტის მოსაცდელში დაყოვნების დროის კონტროლის, პაციენტთა ნაკადის შემოწმების, კადრის დამატების ან ახალი ფილიალის გახსნის საჭიროების განსაზღვრის მიზნითაც. ხაზგასასმელია, რომ დასახელებული მიზნების მიღწევა ლაბორატორიამ შესაძლოა უზრუნველყოს ვიდეომონიტორინგის განხორციელების გარეშეც (მაგალითად, ე. წ. „მისტიური მომხმარებლის“ მეშვეობით, პაციენტების კმაყოფილების კვლევის კითხვარით, მომხმარებელთა რაოდენობის ანალიზის საშუალებით და ა. შ.). შესაბამისად, აღნიშნული მიზნებით ვიდეომონიტორინგის განხორციელება არ იქნა მიჩნეული მიზნის ადეკვატურ და პროპორციულ საშუალებად.

ერთ-ერთი ლაბორატორიისა და სტომატოლოგიური კლინიკის შემოწმებების ფარგლებში ასევე დადგინდა, რომ სამედიცინო დაწესებულებები ვიდეომონიტორინგის სისტემის მეშვეობით გარკვეულ სივრცეებში ახორციელებდნენ აუდიომონიტორინგსაც.

რეგისტრატურის სივრცესა და მორფოლოგიის ოთახში აუდიომონიტორინგის მიზნად ლაბორატორიამ მიუთითა მნიშვნელოვანი ლეგიტიმური ინტერესის დასაცავად მონაცემების დამუშავების საჭიროება და განმარტა, რომ აუდიომონიტორინგი ხორციელდებოდა სამედიცინო მომსახურების მაღალი ხარისხის უზრუნველსაყოფად. შემოწმების ფარგლებში დადგენილი გარემოებების ერთობლიობით დადასტურდა, რომ აუდიომონიტორინგის მიზანი იყო მომსახურების ხარისხის კონტროლი, მისი გაუმჯობესება და მომხმარებლის კმაყოფილების უზრუნველყოფა. სამსახურის შეფასებით, ამ სივრცეებში აუდიომონიტორინგი არ წარმოადგენდა დასახელებული ინტერესების დაცვის აუცილებელ საშუალებას და იწვევდა არაპროპორციულ ჩარევას მონაცემთა სუბიექტების პირად ცხოვრებაში, რაც ეწინააღმდეგება კანონის მე-11 მუხლის პირველი პუნქტის მოთხოვნებს. შეფასდა ის გარემოებაც, რომ დასახელებულ სივრცეებში მომხმარებლებთან კომუნიკაცია მუდმივად არ ხორციელდებოდა,

თუმცა ლაბორატორია მომხმარებლის არყოფნის შემთხვევაშიც კი ახდენდა თანამშრომლების აუდიომონიტორინგს. შესაბამისად, ლაბორატორიას შესაძლოა დაემუშავებინა ის მონაცემები, რომლებიც არ უკავშირდებოდა თანამშრომლის მიერ მომსახურების განხორციელების ხარისხს (მაგალითად, მის პირად სატელეფონო საუბრებს ან/და კომუნიკაციას სხვა თანამშრომლებთან).

სტომატოლოგიური კლინიკის შემოწმების ფარგლებში დადგინდა, რომ კლინიკისთვის არ იყო ცნობილი ინფორმაცია ვიდეოჩაწერასთან ერთად აუდიოჩაწერის მიმდინარეობის თაობაზე. შესაბამისად, კლინიკას აუდიომონიტორინგის განხორციელების ლეგიტიმური მიზანი და საჭიროება არ ჰქონდა.

სამსახურმა შემოწმების ფარგლებში აგრეთვე იმსჯელა სამედიცინო დაწესებულებების მიერ ვიდეომონიტორინგის გზით დამუშავებული პერსონალური მონაცემების მიმართ მიღებული უსაფრთხოების ორგანიზაციულ-ტექნიკური ზომების მნიშვნელობაზე. კერძოდ, ერთ-ერთი ლაბორატორიის შემოწმების ფარგლებში დადგინდა, რომ ვიდეომონიტორინგის სისტემაზე წვდომისთვის არაერთი პირი გამოიყენებდა ერთსა და იმავე მომხმარებელს, თუმცა შემოწმების ფარგლებში ლაბორატორიამ უზრუნველყო ვიდეომონიტორინგის სისტემაზე წვდომის უფლების მქონე პირების განპიროვნებული, პაროლით დაცული მომხმარებლებით დაშვება.

სამსახურის გადაწყვეტილებით, სამივე სამედიცინო დაწესებულება ვიდეომონიტორინგის წესების დარღვევისათვის ცნობილ იქნა სამართალდამრღვევად, სტომატოლოგიურ კლინიკასა და ერთ-ერთი ლაბორატორიას კი ადმინისტრაციული პასუხისმგებლობა დაეკისრა აუდიომონიტორინგის წესების დარღვევისთვისაც. დამატებით, ერთ-ერთ ლაბორატორიას ადმინისტრაციული სამართალდარღვევისთვის პასუხისმგებლობა დაეკისრა მონაცემთა უსაფრთხოების წესების დარღვევისთვის. შემოწმების ფარგლებში სამივე სამედიცინო დაწესებულებას მიეცა დავალებები გამოვლენილი დარღვევების აღმოფხვრის მიზნით.

ვ. ფინანსურ სექტორში მონაცემების დამუშავება

— ბანკის ცხელი ხაზი

სამსახურმა გეგმურად შეისწავლა სს „ლიბერთი ბანკის“, სს „პროკრედიტ ბანკის“ და სს „თიბისი ბანკის“ მიერ ცხელი ხაზის მეშვეობით აუდიომონიტორინგის განხორციელების კანონიერება.

შემოწმების ფარგლებში დადგინდა, რომ სამივე ბანკი საქმიანობის პროცესში, მათ შორის მომხმარებლებთან კომუნიკაციის მიზნით, იყენებდა სატელეფონო ცხელ ხაზს, რომელზეც ზარის განხორციელების შემთხვევაში ბანკის მომხმარებლებსა და პოტენციურ მომხმარებლებს შეეძლოთ საბანკო მომსახურების (მაგალითად, საკუთარ ანგარიშებს შორის ნაშთის გადატანა/თანხის კონვერტაცია) და ბანკის საქმიანობასთან დაკავშირებული ინფორმაციის (მაგალითად: ფილიალების მისამართების, სამუშაო საათების, საბანკო პროდუქტების შესახებ)

მიღება. ამასთან, სატელეფონო ცხელი ხაზის საშუალებით მომხმარებლები ბანკებს წარუდგენდნენ პრეტენზიებს საქმიანობასთან/მომსახურებასთან დაკავშირებით. აქვე უნდა აღინიშნოს, რომ ცხელ ხაზზე შემავალი სატელეფონო ზარები იწერებოდა და ინახებოდა. ამასთან, ჩაწერის ფუნქცია გააქტიურებული იყო სამივე ბანკის გარკვეულ სტრუქტურულ ერთეულში დასაქმებული თანამშრომლების შიდა სამსახურებრივ ნომრებზეც, მათ შორის იწერებოდა და ინახებოდა ამ თანამშრომლების მომხმარებლებთან/პოტენციურ მომხმარებლებთან საუბარიც.

სს „ლიბერთი ბანკის“ შემოწმების ფარგლებში დადგინდა, რომ ცხელი ხაზის ნომრებზე დარეკვისას ავტომოპასუხე სხვადასხვა ღილაკის გააქტიურების საშუალებით მომხმარებლებს განსხვავებული ინფორმაციის მიწოდებას/მომსახურებას სთავაზობდა. ღილაკებისა და შესაბამისი თემატიკების ჩამოთვლის დასრულების შემდეგ, ისეთ შემთხვევაში, თუ მომხმარებელი არ აირჩევდა არცერთ ღილაკს, ავტომოპასუხე მომხმარებელს აფრთხილებდა მომსახურების სრულყოფის მიზნით საუბრის ჩაწერის განხორციელების შესახებ. ამასთან, ისეთ შემთხვევაში, თუ მომხმარებელი არ დაელოდებოდა ავტომოპასუხის ხსენებულ განმარტებას და მის მოსმენამდე გააქტიურებდა ავტომოპასუხის მიერ მისთვის შეთავაზებულ რომელიმე სასურველ ღილაკს, აუდიოჩაწერის თაობაზე ინფორმაციის მიწოდებას არც ავტომოპასუხე და არც ბანკის ოპერატორი არ უზრუნველყოფდა.

სს „ლიბერთი ბანკის“ შემოწმების ფარგლებში გამოიკვეთა, რომ ბანკის შიდა ნომერთან დაკავშირების შემთხვევაში ავტომოპასუხე ახორციელებდა ზოგად მითითებას მომსახურების სრულყოფის მიზნით საუბრის ჩაწერასთან დაკავშირებით, თუმცა ყველა შიდა ნომერთან საუბარი არ იწერებოდა. შესაბამისად, მომხმარებელს შესაძლოა შექმნოდა არასწორი წარმოდგენა, რომ მისი საუბარი ნებისმიერ შემთხვევაში ჩაიწერებოდა, მათ შორის – ბანკის ყველა შიდა ნომერზე ზარის განხორციელების დროს. ამასთან, შემოწმების ფარგლებში ბანკმა განმარტა, რომ აუდიოჩაწერის გზით მონაცემების დამუშავებაზე ინფორმაცია გათვალისწინებული და ნებისმიერი პირისთვის გასაცნობად ხელმისაწვდომი იყო ბანკის ვებგვერდზე განთავსებული მონაცემთა დამუშავებასთან დაკავშირებული დოკუმენტებით. სამსახურმა განმარტა, რომ აღნიშნული აქტების საჯაროდ გამოქვეყნება მომხმარებელთა ინფორმირებისთვის განხორციელებულ გარკვეულ ზომას წარმოადგენს, თუმცა ვერ იქნება მიჩნეული მონაცემთა სუბიექტის სათანადო ინფორმირების ზომად, ვინაიდან იმ მომხმარებელთა/პოტენციურ მომხმარებელთა მნიშვნელოვან ნაწილს, რომელიც ცხელი ხაზის მომსახურებას იყენებს, შესაძლოა არ ჰქონდეს წაკითხული ხსენებული მოცულობითი დოკუმენტების ჩანაწერები აუდიომონიტორინგთან დაკავშირებით.

სს „თიბისი ბანკის“ შემთხვევაში, ბანკის ზოგიერთი სტრუქტურული ერთეულების თანამშრომლებთან შემავალი და გამავალი სატელეფონო ზარებისას, ავტომოპასუხის გაფრთხილება არ გამოიყენებოდა და აუდიოჩაწერის თაობაზე ინფორმაცია მომხმარებელს მიეწოდებოდა თავად თანამშრომლების მიერ. დადგინდა, რომ აღნიშნული თანამშრომლები მომხმარებლებს აწვდიდნენ ინფორმაციას აუდიოჩაწერის თაობაზე, თუმცა არ განუმარტავდნენ აუდიოჩაწერის მიზანს. ამასთან, მიზნის შესახებ განმარტების სავალდებულო ხასიათზე აღნიშნვას არც ბანკის შიდა ინსტრუქციებისა და მითითებების ერთობლიობა შეიცავდა.

შემოწმების ფარგლებში შესწავლილ იქნა ბანკების მიერ მონაცემთა უსაფრთხოებისთვის კანონით დადგენილი მოთხოვნების შესრულების საკითხიც. სს „თიბისი ბანკის“ შემოწმების ფარგლებში გამოიკვეთა, რომ სერვერებზე, სადაც მუშავდებოდა სატელეფონო ჩანაწერები, არ აღირიცხებოდა მათ მიმართ შესრულებული მოქმედებები; სს „პროკრედიტ ბანკის“ შემთხვევაში კი დადასტურდა, რომ აუდიოჩანაწერების დამუშავებისთვის განკუთვნილ ერთ-ერთ სისტემაში შემოწმების პერიოდამდე არ აღირიცხებოდა მათ მიმართ განხორციელებული მოქმედებები. ზემოხსენებულთან დაკავშირებით დადგინდა კანონის 27-ე მუხლით გათვალისწინებული მონაცემთა უსაფრთხოების დარღვევები.

სამსახურმა სს „პროკრედიტ ბანკის“ და სს „თიბისი ბანკის“ შემოწმების შედეგად დაადგინა სამართალდარღვევები, კანონის 76-ე მუხლის პირველი პუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენის გამო. იმავდროულად, სამივე ბანკს დაევალა ზემოხსენებული დარღვევების აღმოფხვრა.

— **სადაზღვევო კომპანიები**

სამსახურმა გეგმურად შეამოწმა 2 (ორი) სადაზღვევო კომპანიის მიერ მათი ვებგვერდების მეშვეობით ჯანმრთელობის დაზღვევის პოლისის მქონე ფიზიკური პირების მონაცემთა მოპოვებისა და შენახვის კანონიერება.

შემოწმებების ფარგლებში გამოიკვეთა, რომ სადაზღვევო კომპანიები საქმიანობის განხორციელების პროცესში, მომხმარებლისთვის სადაზღვევო მომსახურების მიწოდების დროს, ხელშეკრულებით ნაკისრი ვალდებულებების შესრულების (მაგალითად, მომხმარებლისთვის გაწეული სამედიცინო მომსახურების საფასურის ანაზღაურების) მიზნით, ვებგვერდის მეშვეობით ამუშავებდნენ ჯანმრთელობის დაზღვევის პოლისის მქონე ფიზიკური პირების პერსონალურ მონაცემებს (მაგალითად: პირის სახელს, გვარს, დაბადების თარიღს, პირადი ნომერს, სქესს, მოქალაქეობას, სატელეფონო ნომერს, ჯანმრთელობის შესახებ ინფორმაციას და სხვა).

ერთ-ერთ შემთხვევაში გამოიკვეთა, რომ სადაზღვევო კომპანია გარკვეულ მონაცემებს ვებგვერდის მეშვეობით ამუშავებდა სათანადო საჭიროების გარეშე. კერძოდ, სამედიცინო ანაზღაურების, ასევე საგარანტიო წერილის მიღებასთან დაკავშირებით განაცხადის გაკეთებისას სავალდებულო დოკუმენტაციასთან ერთად მომხმარებელს შესაძლებლობა ჰქონდა ვებგვერდზე განეთავსებინა დამატებითი დოკუმენტაციაც (მაგალითად, განსახილველ სადაზღვევო შემთხვევასთან დაკავშირებული სამედიცინო ანალიზებისა და გამოკვლევის პასუხები), თუმცა, კომპანიის განმარტებით, აღნიშნული დოკუმენტაციის არსებობა გავლენას არ ახდენდა სადაზღვევო შემთხვევის განხილვაზე. აღნიშნული შემთხვევა სამსახურის მიერ მონაცემთა არაპროპორციული მოცულობით დამუშავებად შეფასდა, რაც წარმოადგენს კანონის მე-4 მუხლის პირველი პუნქტის „გ“ ქვეპუნქტის მოთხოვნათა დარღვევას. ასევე აღსანიშნავია, რომ კომპანიას შემოწმების ეტაპზე არ ჰქონდა განსაზღვრული პერსონალური მონაცემების

შენახვის ვადა და ამ ვადის გასვლის შემდგომ მონაცემთა მიმართ გასატარებელი ღონისძიებები.

განხორციელებული შემოწმებების ფარგლებში ასევე დადგინდა, რომ დაზღვეული პირების ინფორმირება ვებგვერდის საშუალების მონაცემთა უშუალოდ მათგან შეგროვების პროცესში ერთ-ერთი კომპანიის მიერ ხდებოდა ვებგვერდზე რეგისტრაციის (ანგარიშის შექმნის) და ვებგვერდის მეშვეობით ჯანმრთელობის დაზღვევის პროდუქტის შეძენის დროს, ხოლო მეორე კომპანიის შემთხვევაში — მხოლოდ ჯანმრთელობის დაზღვევის პროდუქტის შეძენის დროს. აღსანიშნავია, რომ მომხმარებლის მიერ ინფორმირების დოკუმენტებზე თანხმობის ღილაკის მონიშვნა ისე ხდებოდა, რომ ეკრანზე ავტომატურად (სავალდებულო წესით) არ აისახებოდა აღნიშნული დოკუმენტების ტექსტი/შინაარსი და მომხმარებელს მისი გაცნობის გარეშე შეეძლო პროცესის გაგრძელება. ამასთან, ერთ-ერთი კომპანიის შემთხვევაში გამოიკვეთა, რომ, მართალია, ვებგვერდზე რეგისტრაციისას ხდებოდა მომხმარებლებისგან მათი მონაცემების მოპოვება, თუმცა კომპანია არ ახდენდა მათ ინფორმირებას კანონის 24-ე მუხლით გათვალისწინებულ საკითხებთან დაკავშირებით. ამ შემთხვევაში ვებგვერდზე რეგისტრირდებოდნენ მხოლოდ ის მომხმარებლები, რომლებსაც უკვე შეძენილი ჰქონდათ სადაზღვევო პროდუქტი (მაგალითად, კომპანიის გაყიდვების მენეჯერის დახმარებით (შეთავაზებით) ან კომპანიაში ადგილზე ვიზიტის გზით), თუმცა კომპანიასთან ურთიერთობის წინა ეტაპებზე (მაგალითად, პოლისის შეძენის ეტაპი) მათთვის არ იყო უზრუნველყოფილი ინფორმაციის მიწოდება კანონის მოთხოვნათა დაცვით.

ნიშანდობლივია, რომ ზემოხსენებული დოკუმენტები, რომელთა მეშვეობითაც კომპანიები ახდენდნენ მომხმარებლების ინფორმირებას მონაცემთა დამუშავებასთან დაკავშირებულ საკითხებზე, არ შეიცავდა კანონის 24-ე მუხლის პირველი პუნქტით განსაზღვრულ ინფორმაციას (პერსონალურ მონაცემთა დაცვის ოფიცრის, ასევე – დამუშავებაზე უფლებამოსილი პირის (მათი არსებობის შემთხვევაში) ვინაობას/სახელწოდებას და საკონტაქტო ინფორმაციას, მონაცემთა შენახვის კონკრეტული ვადის შესახებ ინფორმაციას, ხოლო, თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, ვადის განსაზღვრის კრიტერიუმების თაობაზე).

აღნიშნული შემოწმებების ფარგლებში სამსახურმა ყურადღება გაამახვილა იმ გარემოებაზეც, რომ კომპანიების მიერ კანონის 24-ე მუხლით გათვალისწინებულ საკითხებზე ინფორმაციის მონაცემები სუბიექტს არ მიეწოდებოდა ერთიანი დოკუმენტით; მონაცემთა სუბიექტის მიერ საკუთარი უფლებების ეფექტური რეალიზებისთვის კი მნიშვნელოვანია, მან ინფორმაცია მიიღოს მისთვის მარტივი და აღქმადი ფორმით (მაგალითად, ერთიანი დოკუმენტით, რომელშიც სრულყოფილად იქნება მითითებული კანონის 24-ე მუხლის პირველი პუნქტით გათვალისწინებული ინფორმაცია), რადგან სწორედ მიწოდებული ინფორმაცია აძლევს მონაცემთა სუბიექტს შესაძლებლობას, შეაფასოს თავისი მონაცემების მიწოდების/გაცემის საჭიროება და მოიპოვოს ინფორმაცია მომავალში საკუთარი უფლებების დაცვის შესახებ.

შემოწმების ფარგლებში ასევე შესწავლილ იქნა სადაზღვევო კომპანიების მიერ მონაცემთა უსაფრთხოებისთვის კანონით დადგენილი მოთხოვნების შესრულების საკითხიც. დადგინდა, რომ მათი ე. წ. „პროვაიდერი სამედიცინო

დაწესებულებების“ თანამშრომლები მონაცემებზე წვდომას არ ახორციელებდნენ მათზე განპიროვნებული ანგარიშების გამოყენებით. ამასთან, არ აღირიცხებოდა პერსონალური მონაცემების შემცველი დოკუმენტის მიმართ განხორციელებული გარკვეული მოქმედებები, აღნიშნული კი კანონის 27-ე მუხლის მოთხოვნების საწინააღმდეგოდ ქმნიდა მონაცემთა უკანონოდ დამუშავების რისკებს.

სამსახურის გადაწყვეტილებით, ორივე სადაზღვევო კომპანიას პერსონალურ მონაცემთა მიმართ უსაფრთხოების დაცვის წესების დარღვევისთვის დაეკისრა კანონის 76-ე მუხლით გათვალისწინებული ადმინისტრაციული პასუხისმგებლობა. ამასთან, სადაზღვევო კომპანია, რომელიც არაპროპორციული მოცულობით ამუშავებდა მონაცემებს, სამსახურის მიერ ცნობილ იქნა სამართალდამრღვევად კანონის 66-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში. იმავდროულად, სადაზღვევო კომპანიებს დაევალა ზემოხსენებული დარღვევების აღმოფხვრა.

— კერძო ბანკები

გეგმურად შემოწმდა 2 (ორი) კერძო ბანკის მიერ დისტანციური იდენტიფიკაციის პროცესში ბიომეტრიული მონაცემების დამუშავების კანონიერება.

შემოწმებების ფარგლებში გამოიკვეთა, რომ ბანკები მათი საქმიანობის განხორციელებისას მომხმარებლისთვის დისტანციური საბანკო მომსახურებ(ებ)ის მიწოდების დროს (მაგალითად: სატელეფონო ნომრის დისტანციურად ცვლილება, ინტერნეტ/მობაილ ბანკის აპლიკაციაზე დისტანციურად რეგისტრაცია და სხვა) ამ მომხმარებლებისთვის უნიკალური იდენტიფიცირების/ვერიფიცირების მიზნით ამუშავებდნენ მათ ბიომეტრიულ მონაცემს (სახის გამოსახულებას). ამისთვის პროგრამა, უპირველეს ყოვლისა, ახდენდა მომხმარებლის პირადობის დამადასტურებელ დოკუმენტზე არსებული ფოტოს და ამავე მომხმარებლისთვის გადაღებული ვიდეოჩანაწერიდან აღებული ფოტოს ბიომეტრიულად დადარებას და მსგავსების პროცენტულობის განსაზღვრას. აღნიშნულის შემდეგ ბანკის მიერ ხორციელდებოდა სსიპ — „სახელმწიფო სერვისების განვითარების სააგენტოს“ ბაზაში არსებული მომხმარებლის ფოტოსურათის ავტომატურად ხორციელდებოდა გამოთხოვა და კომპანიის სერვერზე მიწოდება, რის შემდეგაც პროგრამა აღნიშნული სააგენტოდან გამოთხოვილ ფოტოსურათს ადარებდა მომხმარებლის ზემოხსენებული ვიდეოჩანაწერიდან აღებულ ფოტოს.

შემოწმების ფარგლებში ბანკმა განმარტა, რომ, ვინაიდან საქმე ეხებოდა საბანკო მომსახურების მომხმარებლისთვის დისტანციური ფორმით, როდესაც ცალკეული ოპერაციები სრულდებოდა არა ბანკის რომელიმე ფილიალში მისი ვიზიტის შედეგად, არამედ ელექტრონული საშუალებების გამოყენებით (მაგალითად, კომპიუტერი, მობილური ტელეფონი, პორტატული კომპიუტერი და სხვა), ბიომეტრიული იდენტიფიკაციის გარეშე შეუძლებელი იყო იმ პირის ვინაობის უტყუარი დადასტურება, თუ ვინ იდგა აღნიშნული ელექტრონული მოწყობილობის უკან და ვინ იყენებდა მას ამა თუ იმ საბანკო მომსახურების მისაღებად.

აღნიშნული შემოწმებების ფარგლებში გამოიკვეთა ისიც, რომ, მონაცემთა სუბიექტს ბიომეტრიული იდენტიფიცირების პროცესში, მისგან მონაცემების მოპოვებისას არ მიეწოდებოდა კანონის 24-ე მუხლის პირველი პუნქტით გათვალისწინებული ინფორმაციის ნაწილი (განმარტება/ინფორმაცია ბიომეტრიულ მონაცემთა მიწოდების სავალდებულოობის შესახებ, ხოლო, თუ მონაცემთა მიწოდება სავალდებულოა – მონაცემთა მიწოდებაზე უარის თქმის სამართლებრივი შედეგების თაობაზე; ასევე – უფლებამოსილი პირის საკონტაქტო ინფორმაცია (სატელეფონო ნომერი ან/და ელექტრონული ფოსტის მისამართი). აღსანიშნავია, რომ უფლებამოსილი პირის საკონტაქტო ინფორმაციის მონაცემთა სუბიექტებისთვის მიუწოდებლობა გამორიცხავდა მასთან მონაცემთა სუბიექტის ოპერატიული და სრულფასოვანი კომუნიკაციის შესაძლებლობას. სამსახურმა ასევე იმსჯელა კანონის 24-ე მუხლის პირველი პუნქტით გათვალისწინებული ინფორმაციის მომხმარებლისთვის გაცნობის ფორმაზე. კერძოდ, მომხმარებლისთვის არ იყო უზრუნველყოფილი ხსენებული ინფორმაციის გაცნობა თითოეულ შემთხვევაში, ვინაიდან ინფორმაციის შემცველი დოკუმენტის გაცნობის დადასტურება და პროცესის გაგრძელება მას დოკუმენტის გახსნის/გაცნობის გარეშეც შეეძლო; ერთ-ერთი ბანკის შემთხვევაში კი ამავე მუხლის პირველი პუნქტით გათვალისწინებული გარკვეული ინფორმაცია მითითებული იყო ბანკის სხვადასხვა დოკუმენტში, რაც, სამსახურის განმარტებით, ვერ უზრუნველყოფდა მონაცემთა სუბიექტებისთვის ინფორმაციის მარტივი და აღქმადი ფორმით მიწოდებას.

სამსახურის გადაწყვეტილებით, ორივე ბანკს დაევალა ბიომეტრიული მონაცემების მოპოვების/დამუშავების პროცესში კანონის 24-ე მუხლის პირველი პუნქტით გათვალისწინებული მონაცემთა სუბიექტის ინფორმირების სრულყოფილად, კერძოდ, მარტივი და აღქმადი ფორმით უზრუნველყოფა (მაგალითად, მითითებული პუნქტით გათვალისწინებული ინფორმაციის ერთ დოკუმენტში სრულად ასახვის უზრუნველყოფით). ასევე, დაევალათ შემოწმების ფარგლებში გამოვლენილი სხვა დარღვევების აღმოფხვრა.

— კომერციული ბანკების მიერ მონაცემთა საერთაშორისო გადაცემა

სამსახურმა გეგმურად შეისწავლა 2 (ორი) კომერციული ბანკის მიერ პერსონალურ მონაცემთა საერთაშორისო გადაცემის კანონიერება.

ერთ-ერთი ბანკის შემოწმების ფარგლებში დადგინდა, რომ აღნიშნული ბანკი, დასაქმებული პირებისთვის სამსახურებრივი ელექტრონული ფოსტისა და „Skype for Business“-ის ანგარიშების შექმნის მიზნით, ამ პირების პერსონალურ მონაცემებს გადასცემდა დამფუძნებელ ბანკს თურქეთის რესპუბლიკაში. ნიშანდობლივია, რომ თურქეთი არ არის შეყვანილი სამსახურის უფროსის 2024 წლის 29 თებერვლის №23 ბრძანებით დამტკიცებულ პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხაში. ამასთან, ბანკს მონაცემთა საზღვარგარეთ გადაცემის თაობაზე არ ჰქონდა მოპოვებული სამსახურის ნებართვა. ბანკმა გადაცემის საფუძვლად მიუთითა კანონის 37-ე მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტით გათვალისწინებულ საფუძველზე („შესაბამის სახელმწიფოში

მონაცემთა დაცვის სათანადო გარანტიების არარსებობისა და შესაძლო საფრთხეების შესახებ ინფორმაციის მიღების შემდეგ მონაცემთა სუბიექტი განაცხადებს წერილობით თანხმობას“). სამსახურმა ყურადღება გაამახვილა, რომ დამფუძნებელი ბანკი არ უზრუნველყოფდა ბანკის თანამშრომლების მონაცემთა მიმართ განხორციელებული მოქმედებების სრულყოფილად აღრიცხვას (არ აღირიცხებოდა წვდომის უფლების მქონე პირთა მიერ მათი დათვალიერების ფაქტი), რაც მონაცემთა უსაფრთხოების დაცვის არასათანადო ზომას წარმოადგენს; თუმცა, აღნიშნულის საპირისპიროდ, მონაცემთა თანხმობის ტექსტით ბანკის თანამშრომლებს მიეწოდათ ინფორმაცია, რომ დამფუძნებელი ბანკი ატარებდა შესაბამის ორგანიზაციულ-ტექნიკურ ზომებს თურქეთის რესპუბლიკაში მათი მონაცემების უსაფრთხოების უზრუნველსაყოფად. შესაბამისად, თანხმობა არ აკმაყოფილებდა კანონის მე-3 მუხლის „მ“ და „ნ“ ქვეპუნქტებით გათვალისწინებულ თანხმობის კრიტერიუმებს.

ამასთან, კანონის 37-ე მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტით გათვალისწინებული დანაწესი სამსახურმა განმარტა ხსენებული ნორმის მიზნების ანალიზისა და საერთაშორისო გადაცემისას მონაცემთა სუბიექტის ფუნდამენტური უფლებების დაცვის ინტერესებიდან გამომდინარე. სამსახურმა ასევე განმარტა, რომ მონაცემთა სუბიექტის ფუნდამენტური უფლებების დაცვის უზრუნველყოფის მიზნებისთვის, იმ შემთხვევაში, თუ სახელმწიფო, რომელსაც გადაეცემა მონაცემები, ვერ უზრუნველყოფს მონაცემთა დაცვის სათანადო გარანტიებს, უპირველესად, მნიშვნელოვანია, დამუშავებისთვის პასუხისმგებელმა პირმა აღნიშნული გარანტიები შექმნას მონაცემთა მიმღებთან დადებული ხელშეკრულებით. მხოლოდ აღნიშნული გარანტიების შექმნის შეუძლებლობის შემთხვევაშია დასაშვები მონაცემთა საერთაშორისო გადაცემა მონაცემთა სუბიექტის წერილობითი თანხმობის საფუძველზე. შესაბამისად, განსახილველ შემთხვევაში, ბანკს თანამშრომელთა მონაცემების დამფუძნებელი ბანკისთვის გადაცემამდე, სათანადო ხელშეკრულებისა და სამსახურის წინასწარი ნებართვის საფუძველზე (კანონის 37-ე მუხლის გათვალისწინებით), უნდა უზრუნველეყო მონაცემთა დაცვის სათანადო გარანტიები. ამდენად, ბანკის მიერ დასაქმებული პირების პერსონალური მონაცემების თურქეთის რესპუბლიკაში გადაცემის პროცესში არ გამოიკვეთა კანონის 37-ე მუხლით დადგენილი საფუძვლების არსებობა.

მეორე ბანკის შემოწმების ფარგლებში დადგინდა, რომ ბანკი, მომხმარებლისთვის საბანკო ბარათის დამზადების, აგრეთვე, საბარათე ოპერაციების განხორციელებისა და დამუშავების მიზნით, მომხმარებლების პერსონალურ მონაცემებს გადასცემდა აზერბაიჯანის რესპუბლიკაში დაფუძნებულ კომპანიას; საბარათე ოპერაციების შესრულებისა და დამუშავების მიზნით პერსონალური მონაცემების მონაცემთა მიმღებისთვის გადაცემის თაობაზე კი ბანკს სამსახურისგან მოპოვებული ჰქონდა კანონის 37-ე მუხლის მე-3 პუნქტით გათვალისწინებული ნებართვა. შემოწმების ფარგლებში დადგინდა, რომ ბანკის მიერ მომხმარებლების პერსონალური მონაცემების გადაცემა შეესაბამებოდა საერთაშორისო გადაცემის თაობაზე ხსენებულ ნებართვას და კანონის 37-ე მუხლით გათვალისწინებულ წესებს და პირობებს. აღსანიშნავია, რომ მომხმარებლისთვის საბანკო ანგარიშის გახსნის/ბარათის დამზადების განაცხადით

მონაცემთა გადაცემის მიზნები ამომწურავად არ იყო განსაზღვრული, აღნიშნული კი მონაცემთა დამუშავების პროცესში გამჭვირვალობის პრინციპის რეალიზებასა და მონაცემთა სუბიექტების მონაცემთა დამუშავების კონკრეტული მიზნების შესახებ ინფორმირებას ვერ უზრუნველყოფდა. სამსახურმა განმარტა, რომ გამჭვირვალობის ვალდებულება მჭიდროდ არის დაკავშირებული მონაცემთა სუბიექტის ინფორმირების უფლებასთან და ითვალისწინებს მონაცემთა სუბიექტის მონაცემთა დამუშავების, მათ შორის – დამუშავების მიზნების თაობაზე სრულყოფილ ინფორმირებას. შესაბამისად, მონაცემების დამუშავების პროცესში გამჭვირვალობის პრინციპის დაცვის უზრუნველსაყოფად მნიშვნელოვანია, რომ მონაცემთა სუბიექტს ამომწურავად მიეწოდოს დამუშავების კონკრეტული მიზნის/მიზნების თაობაზე ინფორმაცია.

სამსახურის გადაწყვეტილებით ბანკი, რომელიც კანონის 37-ე მუხლით დადგენილი საფუძვლებით ახორციელებდა მონაცემთა საერთაშორისო გადაცემას თურქეთის რესპუბლიკაში, სამსახურის მიერ ცნობილ იქნა სამართალდამრღვევად კანონის 85-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში. ბანკებს დაევალათ ზემოხსენებული დარღვევების აღმოფხვრა.

ვ. მონაცემთა დამუშავების სხვა აქტუალურ საკითხებთან დაკავშირებული შემთხვევები

— შპს „თბილისის სატრანსპორტო კომპანია“

სამსახურმა გეგმურად შეისწავლა შპს „თბილისის სატრანსპორტო კომპანიის“ მიერ ვიდეომონიროტინგის განხორციელების კანონიერება. აღსანიშნავია, რომ მუნიციპალიტეტისგან დელეგირებული უფლებამოსილების ფარგლებში კომპანიის ძირითად საქმიანობას წარმოადგენს მგზავრთა გადაყვანის უზრუნველყოფა საზოგადოებრივი ტრანსპორტით (მეტრო, „M3“ კატეგორიის ავტობუსი, საბაგირო, მიკროავტობუსი), რომლითაც ყოველდღიურად სარგებლობს ასი ათასობით პირი.

შემოწმების ფარგლებში დადგინდა, რომ პირის უსაფრთხოებისა და საზოგადოებრივი წესრიგისა და საკუთრების უფლების დაცვის მიზნით კომპანია ახორციელებს როგორც საზოგადოებრივი თავშეყრის ადგილების — მეტროს სადგურების, საბაგიროების, ავტობუსების, ისე – ადმინისტრაციული შენობებისა და საქმიანობის განხორციელებისთვის საჭირო სხვა ობიექტების ვიდეომონიტორინგს; თუმცა გამოიკვეთა, რომ კომპანია შესაბამისი საჭიროების/მიზნის გარეშე ახორციელებდა თავისი ერთ-ერთი ობიექტის მომიჯნავედ მდებარე კერძო საკუთრებაში არსებული საცხოვრებელი სახლის ვიდეომონიტორინგს, რაც კანონის მე-10 მუხლის პირველი პუნქტის დარღვევას წარმოადგენს.

ასევე, მოცემულ შემთხვევაში გამოიკვეთა, რომ სტრატეგიული მნიშვნელობის ობიექტებზე დასაქმებული პირების სამუშაო სივრცის ვიდეომონიტორინგი მიმდინარეობდა კანონის მე-10 მუხლის მე-3 პუნქტის მოთხოვნათა დაცვით; თუმცა კომპანიაში დასაქმებული პირები წერილობითი ფორმით არ იყვნენ გაფრთხილებულნი ვიდეომონიტორინგის კონკრეტული მიზნის თაობაზე, რაც არ შეესაბამება კანონის მე-10 მუხლის მე-8 პუნქტის მოთხოვნებს. აგრეთვე დადგინდა, რომ კომპანიას ვიდეომონიტორინგის თაობაზე გამაფრთხილებელი ნიშნები განთავსებული ჰქონდა იმგვარად, რომ გარკვეულ შემთხვევებში არ იყო აღქმადი ვიდეომონიტორინგის არეალი. გარდა ამისა, კომპანია ვიდეომონიტორინგს ახორციელებდა გამოცდის/ტესტირებისთვის განკუთვნილ აუდიტორიაში, რომელიც ამასთანავე გამოიყენებოდა სასწავლო მიზნებისთვისაც, კომპანიის წარმომადგენლის მიერ მოწოდებული ინფორმაციის თანახმად კი კომპანიას არ ჰქონდა სასწავლო პროცესის ვიდეომონიტორინგის საჭიროება და მიზანი.

შემოწმების ფარგლებში დადგინდა, რომ ადამიანის უფლებათა და თავისუფლებათა დაცვის, დანაშაულისა და სხვა სამართალდარღვევებთან ბრძოლის ეფექტურობის გაზრდის, ასევე – პრევენციული ღონისძიებების გაძლიერების, საზოგადოებრივი უსაფრთხოების/წესრიგის უზრუნველყოფისა და არასრულწლოვანთა მავნე ზეგავლენისგან დაცვის მიზნით, კანონის მე-5 მუხლის „გ“, „დ“ და „ზ“ საფუძველზე, კომპანიასა და საქართველოს შინაგან საქმეთა სამინისტროს შორის გაფორმებული მემორანდუმით გათვალისწინებულია სამინისტროს თანამშრომლების წვდომა კომპანიის ვიდეომონიტორინგის სისტემაში არსებულ იმ კამერებზე, რომლებიც განთავსებულია საჯარო სივრცეებში/თავშეყრის ადგილებში, მათ შორის – მეტროს სადგურების გარე და შიდა ტერიტორიებზე. მიუხედავად აღნიშნულისა, კომპანია სამინისტროს მომხმარებლებს შესაბამისი საჭიროების/მიზნის გარეშე ანიჭებდა წვდომას იმ კამერების ჩანაწერებზე, რომლებიც არ იყო განთავსებული საზოგადოებრივი თავშეყრის ადგილებში (მაგალითად: ადმინისტრაციული შენობები, სახელოსნო და ა. შ.). კომპანიამ ვერ წარმოადგინა ასეთი ვიდეოკამერების ჩანაწერების საქართველოს შინაგან საქმეთა სამინისტროსთვის წვდომის გზით გამჟღავნების საფუძველი და სათანადო დასაბუთება, რაც კანონის მე-5 მუხლის დარღვევად შეფასდა.

აგრეთვე, მოცემულ შემთხვევაში დადგინდა, რომ ერთი ტიპის ავტობუსებში განთავსებული ვიდეოკამერების მეშვეობით ვიდეომონიტორინგთან ერთად ხორციელდება აუდიომონიტორინგიც. შემოწმების ფარგლებში წარმოდგენილი ინფორმაციით, კომპანიას არ ჰქონდა ავტობუსებში აუდიომონიტორინგის განხორციელების მიზანი და საჭიროება. ამასთანავე დადგინდა, რომ ვიდეომონიტორინგის სისტემაზე წვდომის უფლების მქონე გარკვეული თანამშრომლები ფლობდნენ ინფორმაციას ერთი ტიპის ავტობუსებში მიმდინარე აუდიომონიტორინგის თაობაზე, თუმცა, აუდიოჩაწერის მიზნის/საჭიროების არარსებობის მიუხედავად, კომპანიას არ მიუღია აუცილებელი ზომები აღნიშნულის შესაწყვეტად. საზოგადოებრივი ტრანსპორტით ყოველდღიურად გადაადგილდება ასი ათასობით პირი, რომლებიც მგზავრობისას შესაძლებელია ამყარებდეს პირადი ხასიათის, მათ შორის – სატელეფონო, კომუნიკაციას. ამდენად,

კომპანიის მიერ აუდიომონიტორინგი მიმდინარეობდა კანონის მე-11 მუხლის პირველი პუნქტით გათვალისწინებული შესაბამისი საფუძვლის გარეშე.

შემოწმების ფარგლებში დადგინდა კომპანიის მიერ კანონის 27-ე მუხლით დადგენილი მოთხოვნების დარღვევის ფაქტებიც. კომპანიის ზოგიერთ თანამშრომელს წვდომა ჰქონდა ვიდეომონიტორინგის სისტემაში არსებულ იმ კამერებზე, რომლებიც არ შედიოდა მათი სამსახურებრივი უფლებამოსილების ფარგლებში. ამასთან, ვიდეოსათვალთვალო სისტემაზე წვდომისთვის კომპანიის არაერთი თანამშრომელი იყენებდა ერთი და იმავე მომხმარებლის ანგარიშს, ხოლო ვიდეომონიტორინგის სისტემაში ჩანაწერების მიმართ განხორციელებული მოქმედებები სრულად არ აღირიცხებოდა. ხსენებული გარემოებები ქმნიდა მონაცემთა უკანონოდ დამუშავების მნიშვნელოვან რისკებს, რის გამოც დაირღვა კანონის 27-ე მუხლის მოთხოვნები.

სამსახურის გადაწყვეტილებით კომპანია ცნობილ იქნა სამართალდამრღვევად კანონის 67-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით, 69-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით (ვიდეომონიტორინგის განხორციელების წესების დარღვევა), 69-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით (აუდიომონიტორინგის წესების დარღვევა) და 76-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევების ჩადენაში. იმავდროულად, კომპანიას მიეცა დავალებები შემოწმების ფარგლებში გამოვლენილი დარღვევებისა და ნაკლოვანებების აღმოფხვრის მიზნით.

— ერთ-ერთი კომპანიის მიერ ე. წ „Gif“-ის ფორმატის გამოსახულებების გასაჯაროების კანონიერება

სამსახურმა გეგმურად შეისწავლა ერთ-ერთი კომპანიის მიერ ფიზიკური პირების ამსახველი ე. წ „Gif“-ის ფორმატის გამოსახულებების გასაჯაროების კანონიერება. აღსანიშნავია, რომ კომპანია დამკვეთთან არსებული გარიგების საფუძველზე, დამკვეთის მიერ განსაზღვრული ადგილითა და პირობებით, უზრუნველყოფს მომსახურების მიწოდებას, რაც მოიცავს დამკვეთის ღონისძიებაზე შესაბამისი მოწყობილობების გამოყენებით ე. წ. „Gif“-ის ფორმატის გამოსახულებების გადაღების დაორგანიზებას და ვებგვერდზე გასაჯაროებას.

შემოწმების ფარგლებში დადგინდა, რომ კომპანიის ვებგვერდზე განთავსებული გამოსახულებების შემცველი საქაღალდეების უდიდესი ნაწილი შესაბამისი პაროლით არ იყო დაცული და ნებისმიერ პირს შეეძლო მათზე წვდომა; ფიზიკური პირების ამსახველი გამოსახულებების ვებგვერდზე გასაჯაროების სამართლებრივ საფუძვლად კი კომპანია მიუთითებდა მონაცემთა სუბიექტის თანხმობასა და გარიგებით ნაკისრი ვალდებულების შესასრულებლად მონაცემების დამუშავების აუცილებლობაზე. კომპანია მონაცემთა სუბიექტის თანხმობად მიიჩნევდა პირის მიერ გამოსახულების გადაღების შემდეგ დადასტურების (მწვანე) ღილაკის მონიშვნას შესაბამის მოწყობილობაზე; თუმცა ამავე მოწყობილობის ეკრანზე არსებული გამოსახულება არ შეიცავდა ინფორმაციას მონაცემების ვებგვერდზე გასაჯაროებისა და აღნიშნულის მიზნის

თაობაზე. ამასთან, კომპანიის განმარტებით, დამკვეთსა და კომპანიას შორის არსებული გარიგებით, კომპანია იღებდა მომსახურების გაწევის ვალდებულებას, რაც გულისხმობდა დამკვეთის ღონისძიებაზე გამოსახულებების გადასაღები ტაბლეტების განთავსებასა და გადაღებული გამოსახულებების ვებგვერდზე გასაჯაროებას. აღსანიშნავია, რომ კანონის მე-5 მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტის საფუძველზე მონაცემთა დამუშავება დასაშვებია იმ შემთხვევაში, თუ გარიგების მხარე თავად მონაცემთა სუბიექტია. დასახელებული სამართლებრივი საფუძვლის არსებობისთვის აუცილებელია გარიგება თავად მონაცემთა სუბიექტთან იყოს დადებული; მოცემულ შემთხვევაში კი კომპანიასთან დადებული გარიგების მხარეს ყოველთვის არ წარმოადგენდა მონაცემთა სუბიექტი. შესაბამისად, სამსახურმა არ გაიზიარა კომპანიის პოზიცია და მიიჩნია, რომ ვებგვერდზე გამოსახულებები განთავსებული იყო შესაბამისი სამართლებრივი საფუძვლის გარეშე.

სამსახურმა შემოწმების ფარგლებში აგრეთვე დაადგინა, რომ მონაცემთა სუბიექტების ინფორმირება არ ხდებოდა კანონის მოთხოვნათა დაცვით (მაგალითად, მას არ მიეწოდებოდა ინფორმაცია მონაცემების დამუშავების კონკრეტული მიზნების, საფუძვლების შესახებ და სხვა). ვებგვერდზე გასაჯაროებული გამოსახულებები იქმნებოდა უშუალოდ მონაცემთა სუბიექტის გადაღების გზით და, შესაბამისად, გროვდებოდა სუბიექტისგან, რა დროსაც მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს ეკისრება კანონის 24-ე მუხლის პირველი პუნქტით გათვალისწინებული ინფორმირების ვალდებულება. მონაცემთა სუბიექტის სათანადო ინფორმირების გარეშე ვერ მიიღწევა მონაცემთა დამუშავების გამჭვირვალობა, რის გარეშეც შეუძლებელია სამართლიანი და მონაცემთა სუბიექტისთვის განჭვრეტადი მონაცემთა დამუშავების პროცესის უზრუნველყოფა.

სამსახურის გადაწყვეტილებით, კომპანია ცნობილ იქნა სამართალდამრღვევად, მათ შორის – კანონის 67-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის, და დაევალა შემოწმების ფარგლებში გამოვლენილი დარღვევების აღმოფხვრა.

— ვიდეომონიტორინგის, აუდიომონიტორინგისა და ბიომეტრიული მონაცემების დამუშავების პროცესების წერილობითი ფორმით განსაზღვრის ვალდებულება

საანგარიშო პერიოდში სამსახურმა შეისწავლა ზემოხსენებული ვალდებულებების შესრულების მრავალი ფაქტი. ორი კომერციული ბანკის მიერ დისტანციური იდენტიფიკაციის პროცესში ბიომეტრიული მონაცემების დამუშავების კანონიერების გეგმური შემოწმებების ფარგლებში დადგინდა, რომ ბანკების მიერ მომხმარებლის ბიომეტრიული მონაცემი (სახის გამოსახულება) მუშავდებოდა მხოლოდ მათი დისტანციური იდენტიფიკაციის პროცესში (მათ შორის: ინტერნეტ ბანკით, ონლაინ განვადების ვებგვერდით სარგებლობის დროს და სხვა შემთხვევებში), რაც, თავის მხრივ, მოიცავდა ხელოვნური ინტელექტის საშუალებით მომხმარებლის გამოსახულების დამუშავებას. შემოწმებების ფარგლებში ერთ-ერთმა ბანკმა წარმოადგინა დოკუმენტი „ბიომეტრიული

მონაცემების დამუშავების თაობაზე“, რომლითაც განსაზღვრული იყო ბიომეტრიულ მონაცემთა დამუშავების მიზანი და მოცულობა, აგრეთვე – მონაცემთა სუბიექტების უფლებების დაცვის მექანიზმები, თუმცა არ იყო დაკონკრეტებული ბიომეტრიულ მონაცემთა შენახვის ვადა, ასევე – შენახვისა და განადგურების წესი/პირობები. ერთ-ერთი ბანკის შემოწმების ფარგლებში წარმოდგენილი განმარტების თანახმად, კანონის მე-9 მუხლის მე-2 პუნქტით გათვალისწინებული საკითხები ბანკს განსაზღვრული ჰქონდა რამდენიმე დოკუმენტით. შემოწმების ფარგლებში ხსენებული დოკუმენტების გაცნობის შედეგად დადგინდა, რომ ისინი ითვალისწინებდა ბიომეტრიული მონაცემების დამუშავების მიზნის შესახებ ინფორმაციას, დოკუმენტებიდან ასევე გამომდინარეობდა ინფორმაცია დამუშავების მოცულობის თაობაზე, პოლიტიკის დოკუმენტში კი მითითებული იყო სუბიექტის უფლებების დაცვის მექანიზმებიც, თუმცა ბანკის მიერ წერილობით არ იყო განსაზღვრული ბიომეტრიული მონაცემების შენახვის ვადა, მათი შენახვისა და განადგურების წესი და პირობები. ზემოაღნიშნულიდან გამომდინარე, კანონის მე-9 მუხლის მე-2 პუნქტით გათვალისწინებული საკანონმდებლო მოთხოვნის სრულად შესრულების მიზნით, ორივე ბანკის მიმართ გაიცა დავალება, წერილობით მომხდარიყო აღნიშნული დანაწესით გათვალისწინებული საკითხების სრულყოფილად გათვალისწინება.

გარდა ამისა, სამსახურმა გეგმურად შეისწავლა ორი კომერციული ბანკის მიერ ცხელი ხაზის მეშვეობით პერსონალურ მონაცემთა დამუშავების კანონიერება. აღნიშნული შემოწმებების ფარგლებში დადგინდა, რომ ერთ-ერთი ბანკის აუდიომონიტორინგის განხორციელებასთან დაკავშირებით წერილობითი დოკუმენტი სრულყოფილად არ განსაზღვრავდა კანონით დადგენილ სავალდებულო საკითხებს (მაგალითად: აუდიომონიტორინგის განხორციელების მოცულობასა და ხანგრძლივობას). ამდენად, ბანკს სამსახურის მიერ დაევალა ხსენებული საკითხების წინასწარ მოწესრიგება. რაც შეეხება მეორე ბანკს, ამ შემთხვევაში დოკუმენტი ითვალისწინებდა მონაცემთა სუბიექტის მიერ საკუთარი მონაცემების შემცველი აუდიოჩანაწერის გაცნობის შეზღუდვას, თუკი შეუძლებელი იყო აუდიოჩანაწერში ასახული სხვა მონაცემთა სუბიექტის პირადი ინფორმაციის ან/და ბანკის კონფიდენციალური ინფორმაციის დაფარვა (კანონმდებლობით პირდაპირ გათვალისწინებული შემთხვევების გარდა). სამსახურმა განმარტა, რომ მონაცემთა სუბიექტის მიერ აუდიოჩანაწერის გაცნობის ან მისი ასლის მიღების მოთხოვნის დაფიქსირების შემთხვევაში მნიშვნელოვანია, ყველა ინდივიდუალურ შემთხვევაში შეფასდეს კანონის 21-ე მუხლით გათვალისწინებული შეზღუდვის საფუძვლების არსებობა. მათ შორის ბანკმა უნდა შეაფასოს აუდიოჩანაწერის გაცემით ნამდვილად ექმნება თუ არა საფრთხე მონაცემთა სხვა სუბიექტის უფლებებსა და თავისუფლებებს. მხოლოდ აღნიშნულის შემდეგ, შესაბამისი შეზღუდვის საფუძვლის დადასტურების შემთხვევაში, უნდა იქნეს მიღებული გადაწყვეტილება ჩანაწერის ასლების გაცნობაზე/გადაცემაზე. ყველა შემთხვევაში წინასწარ უარის თქმა პერსონალური მონაცემების შემცველი აუდიოჩანაწერების გაცნობაზე/გადაცემაზე არ შეესაბამება ზემოხსენებული ნორმით გათვალისწინებულ ვალდებულებას და მონაცემთა სუბიექტის უფლებებთან დაკავშირებით შესაძლოა შეცდომაში შეიყვანოს ის პირები, რომლებიც გაეცნობიან ზემოხსენებულ დოკუმენტს ან/და ევალებათ მისი

აღსრულება. შესაბამისად, აღნიშნულ ბანკს დაევალა მონაცემთა სუბიექტის უფლებების შეზღუდვის შესახებ აუდიომონიტორინგის წესის ზემოაღნიშნული ჩანაწერების კანონის 21-ე მუხლით გათვალისწინებულ რეგულაციასთან შესაბამისობაში მოყვანა.

სამსახურმა ვიდეომონიტორინგის კანონიერებასთან დაკავშირებით ასევე გეგმურად შეისწავლა არაერთი უწყება და ორგანიზაცია (საჯარო სკოლები, პროფესიული სასწავლებლები და სამედიცინო დაწესებულებები). მართალია, დამუშავებისთვის პასუხისმგებელი პირების მიერ უმეტეს შემთხვევაში ვიდეომონიტორინგის განხორციელების შესახებ წერილობითი დოკუმენტები იქნა წარმოდგენილი, თუმცა, როგორც წესი, აღნიშნული დოკუმენტები სრულყოფილად არ მოიცავდა კანონის მე-10 მუხლის მე-2 პუნქტით განსაზღვრულ საკითხებს (მაგალითად: ვიდეომონიტორინგის მიზანსა და მოცულობას, ვიდეომონიტორინგის ხანგრძლივობასა და ვიდეოჩანაწერის შენახვის ვადას, ვიდეოჩანაწერზე წვდომის, მისი შენახვისა და განადგურების წესსა და პირობებს, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმებს). შესაბამისად, დასახელებულ შემთხვევებშიც სამსახურმა გასცა სავალდებულოდ შესასრულებელი დავალებები ზემოაღნიშნული ნორმით განსაზღვრული საკითხების შეფასებისა და წერილობით დოკუმენტებში სრულად ასახვის შესახებ.

— დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებული წერილობითი შეთანხმების/ხელშეკრულების კანონთან შესაბამისობის შემთხვევები

სამსახურის მიერ გეგმურად შესწავლილ მონაცემთა დამუშავებისას არაერთხელ გამოიკვეთა მონაცემთა დამუშავების პროცესში უფლებამოსილი პირის მონაწილეობის შემთხვევა. მათ შორის ერთ-ერთი სკოლის შემოწმების ფარგლებში დადგინდა, რომ სკოლა მოსწავლეთა დასწრებისა და აკადემიური მოსწრების აღრიცხვის მიზნით იყენებდა ელექტრონულ ჟურნალს, რომელიც მას დროებით სარგებლობაში გადაეცა სისტემის ლიცენზიის მფლობელი კომპანიის (შემდგომში — კომპანია) მიერ. საქმიანობის გამართულად წარმართვის უზრუნველსაყოფად კომპანია სკოლას უწევდა ელექტრონული ჟურნალის ტექნიკურ მხარდაჭერას, რაც მათ შორის მოიცავდა ელექტრონულ ჟურნალში დაცული მონაცემების ე. წ. „რეპორტის“ სახით ამოღებას. შემოწმების ფარგლებში დადგინდა, რომ სკოლასა და კომპანიას შორის დადებული ხელშეკრულება არეგულირებდა მომსახურების გაწევის საკითხს და შინაარსობრივად მოიცავდა მონაცემების დამუშავების დავალებასაც. ამასთან, ხელშეკრულება მონაცემთა უსაფრთხოებასთან მიმართებით ითვალისწინებდა მხოლოდ მხარეთა მიერ კონფიდენციალობის დაცვის ვალდებულებას, თუმცა არ შეიცავდა დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონის 36-ე მუხლით გათვალისწინებულ წესებსა და აკრძალვებზე მითითებას. კერძოდ, ხსენებული მუხლის მოთხოვნათა საწინააღმდეგოდ არ ითვალისწინებდა მონაცემთა დამუშავების საფუძვლებსა და მიზნებს, დასამუშავებელ მონაცემთა კატეგორიებს, მონაცემთა დამუშავების ვადას და დამუშავებისთვის პასუხისმგებელი პირისა და

დამუშავებაზე უფლებამოსილი პირის უფლებებსა და ვალდებულებებს. მართალია, ხელშეკრულება დადებული იყო „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს 2011 წლის 28 დეკემბრის კანონის მოქმედების პერიოდში, თუმცა ნიშანდობლივია, რომ იგი არ შეესაბამებოდა ამავე კანონის 2011 წლის 28 დეკემბრის რედაქციის მოთხოვნებსაც (მაგალითად, დასახელებული კანონის მე-16 მუხლის მე-7 პუნქტით გათვალისწინებული მოთხოვნის თანახმად, უფლებამოსილ პირთან დადებულ ხელშეკრულებაში გათვალისწინებული უნდა იყოს მონაცემთა უსაფრთხოებისათვის ზომების მიღების ვალდებულება). აღნიშნულიდან გამომდინარე, სკოლას დაევალა დამუშავებაზე უფლებამოსილ პირთან დადებული ხელშეკრულების „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 36-ე მუხლთან შესაბამისობაში მოყვანა.

გეგმური შემოწმებების ფარგლებში ასევე გამოიკვეთა ისეთი შემთხვევებიც, როდესაც დამუშავებაზე უფლებამოსილი პირები მონაცემთა დამუშავების პროცესში სარგებლობდნენ ქვეკონტრაქტორი პირების[27] მომსახურებით. აღსანიშნავია, რომ კანონის 36-ე მუხლის მე-7 პუნქტი დამუშავებაზე უფლებამოსილი პირის მიერ მესამე პირისთვის თავისი უფლება-მოვალეობების სრულად ან ნაწილობრივ გადაცემას ითვალისწინებს დამუშავებისთვის პასუხისმგებელი პირის წინასწარი წერილობითი თანხმობის შემთხვევაში. უნდა აღინიშნოს, რომ, დამუშავებაზე უფლებამოსილი პირისგან განსხვავებით, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი წარმოადგენს სუბიექტს, რომელიც განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს. ზემოხსენებული ნორმის თანახმად, სწორედ მის კომპეტენციას განეკუთვნება მონაცემთა დამუშავების უფლების სხვა პირისთვის გადაცემის საკითხზე გადაწყვეტილების მიღების უფლება. ხსენებული უფლების მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისთვის მინიჭება იმ გარემოებითაცაა განპირობებული, რომ, კანონის მოთხოვნათა შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს ეკისრება მნიშვნელოვანი პასუხისმგებლობა — მონაცემები მონაცემთა დამუშავების მარეგულირებელი კანონმდებლობის შესაბამისად დაამუშაოს. აღნიშნული პასუხისმგებლობის ჯეროვნად შესრულებისთვის კანონმდებლობა სავალდებულოდ მიიჩნევს მონაცემთა დამუშავების პროცესები ხორციელდებოდეს მისთვის გამჭვირვალედ, მასთან შეთანხმებული ფორმით, მისი დავალებების შესაბამისად და (გარდა კანონმდებლობით პირდაპირ გათვალისწინებული შემთხვევებისა) მის მიერ შერჩეული სუბიექტების მიერ. ნიშანდობლივია, რომ არაერთი შემოწმების ფარგლებში გამოიკვეთა შემთხვევა, როდესაც დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა ქვეკონტრაქტორი პირისთვის გადაცემისას თანხმობის აუცილებლობის საკითხი დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის გაფორმებული ხელშეკრულებით იყო მოწესრიგებული, თუმცა შეთანხმება აქცენტს არ აკეთებდა თანხმობის წერილობითი ფორმით არსებობის საჭიროებაზე. შესაბამისად, დასახელებულ შემთხვევებში სამსახურის მიერ მხარეებს დაევალათ ხელშეკრულებაში

[27] ნებისმიერი პირი, რომელსაც დამუშავებაზე უფლებამოსილი პირი მონაცემთა დამუშავებასთან დაკავშირებულ უფლება-მოვალეობებს სრულად ან ნაწილობრივ გადასცემს.

დამუშავებაზე უფლებამოსილი პირის მიერ უფლებამოსილებების სხვა პირებისთვის გადაცემისას დამუშავებისთვის პასუხისმგებელი პირის წინასწარი წერილობითი თანხმობის აუცილებლობის საკითხის გათვალისწინება.

4.3. დავალებები და რეკომენდაციები

სამსახურის მიერ გეგმურად შესწავლილი საქმეები და განხორციელებული ღონისძიებები ადასტურებს, რომ სხვადასხვა საჯარო უწყებებსა და კერძო ორგანიზაციის მიერ მონაცემების დამუშავების პროცესში დარღვეულია კანონით დადგენილი მოთხოვნები, მონაცემთა დამუშავების პროცესების კანონთან შესაბამისობაში მოყვანის მიზნით კი გაიცა არაერთი სავალდებულოდ შესასრულებელი დავალება. გაცემული დავალებების ანალიზის გათვალისწინებით, იმ პირებმა, რომლებიც ჩართულნი არიან მონაცემების დამუშავების პროცესებში, ყურადღება უნდა მიაქციონ შემდეგ საკითხებს:

— მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა პერსონალური მონაცემები უნდა დაამუშაონ მხოლოდ კანონით გათვალისწინებული სამართლებრივი საფუძვლების არსებობის შემთხვევაში. ამასთან, მათ წინასწარ უნდა განსაზღვრონ მონაცემთა დამუშავების კანონიერი მიზნების მიღწევისთვის საჭირო ვადები, ამ მიზნების მიღწევის შემდეგ კი უნდა განახორციელონ კანონის მე-4 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტით გათვალისწინებული ღონისძიებები. ამასთან, პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად.

— განსაკუთრებით მნიშვნელოვანია მონაცემთა უსაფრთხოდ დამუშავების საკითხი, რომლის დროსაც გასათვალისწინებელია, რომ მონაცემებზე დაშვების უფლების მქონე თითოეულმა პირმა მონაცემებზე წვდომა განახორციელოს მხოლოდ კომპლექსური პაროლით დაცული, მასზე განპიროვნებული მომხმარებლის ანგარიშით. მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ ელექტრონულ მონაცემთა მიმართ განხორციელებული მოქმედებების სრულყოფილად აღრიცხვა და პერიოდული მონიტორინგი, ვინაიდან აღნიშნული მონაცემთა უკანონო დამუშავების პრევენციის ეფექტიანი საშუალებაა. მნიშვნელოვანია, რომ მოქმედებების აღრიცხვის ჟურნალში (ასევე, ვიდეოჩამწერ მოწყობილობებში) დაფიქსირებული ინფორმაცია ინახებოდეს სულ მცირე, პერსონალური მონაცემების (მათ შორის – ვიდეოჩანაწერების) შენახვის ვადით. პერსონალურ მონაცემებზე წვდომა უნდა შეეზღუდოთ იმ თანამშრომლებს, რომლებსაც აღნიშნული არ ესაჭიროებათ თავიანთი სამსახურებრივი მოვალეობების განსახორციელებლად. კრიტიკულად მნიშვნელოვანია, რომ თანამშრომლებს, რომლებსაც მხოლოდ დროის კონკრეტულ მონაკვეთში (დროებით) ესაჭიროებათ პერსონალურ მონაცემებზე დაშვება, შეეზღუდოთ წინასწარი და უწყვეტი წვდომა მონაცემებზე. დამსაქმებელმა ორგანიზაციებმა უნდა გაითვალისწინონ, რომ

თანამშრომელთა მიერ პერსონალური მონაცემების დამუშავების პროცესში პირადი ელექტრონული ფოსტის გამოყენება ეწინააღმდეგება მონაცემთა უსაფრთხოების კანონით გათვალისწინებულ მოთხოვნებს, რადგან ასეთი ელექტრონული ფოსტა არ არის კონტროლირებადი დამსაქმებლის მიერ და ქმნის მონაცემთა უკანონო დამუშავების რისკებს.

— მონაცემთა დამუშავებასთან დაკავშირებული გარემოებებისა და რისკების ანალიზის საფუძველზე უნდა შემუშავდეს სათანადო ზომები მონაცემთა ფიზიკური უსაფრთხოების უზრუნველყოფის მიზნით (მაგალითად, მონაცემების დამუშავებისთვის გათვალისწინებული სივრცე უნდა დაიგეგმოს იმგვარად, რომ გარეშე პირებს არ ჰქონდეთ წვდომა პერსონალურ მონაცემებზე; მონაცემები შენახულ იქნეს შესაბამისი საკეტით დაცულ კარადებში ან/და სხვა დაცულ ადგილას, სადაც არ იარსებებს არაუფლებამოსილი პირების მხრიდან წვდომის შესაძლებლობა და სხვა).

— ზოგადსაგანმანათლებლო და პროფესიულ სასწავლებლებში ვიდეომონიტორინგის განხორციელების პროცესში მნიშვნელოვანია დემონატაჟი იმ კამერებისა, რომლებიც არ ფუნქციონირებს. ვიდეომონიტორინგის მიმდინარეობის შესახებ კანონით გათვალისწინებული გამაფრთხილებელი ნიშნები აღქმადი უნდა იყოს ყველა იმ სივრცეში, სადაც მიმდინარეობს ვიდეომონიტორინგი. იმდენად, რამდენადაც ვიდეომონიტორინგის სისტემებს ხშირად აქვს აუდიოჩაწერის ტექნიკური შესაძლებლობაც, მნიშვნელოვანია, გაკონტროლდეს — ხომ არ ხორციელდება აუდიომონიტორინგიც. გასათვალისწინებელია, რომ აუდიომონიტორინგი მიიჩნევა ინტენსიურ ჩარევად ადამიანის პირადი ცხოვრების სფეროში და იგი უნდა განხორციელდეს მხოლოდ სათანადო საჭიროების შემთხვევაში, კანონით გათვალისწინებული მოთხოვნების სრული დაცვით.

— დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა შეწყვიტონ ვიდეომონიტორინგის სამედიცინო მანიპულაციებისთვის განკუთვნილ სივრცეებში განხორციელება, რადგან ხსენებულ სივრცეებში პირს აქვს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი.

— დამუშავებისთვის პასუხისმგებელმა პირებმა, რომლებიც ამუშავებენ ერთი და იმავე მონაცემებს ან მონაწილეობენ ამ მონაცემთა დამუშავების საერთო პროცესებში, უნდა შეაფასონ — ხომ არ წარმოადგენენ მონაცემთა თანადამუშავების პასუხისმგებელ პირებს; ხოლო ამ უკანასკნელ შემთხვევაში მათ სრულყოფილად უნდა დაიცვან კანონის 35-ე მუხლის მოთხოვნები ხსენებული სტატუსის პირების მიმართ.

— იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელი პირი მონაცემებს რეალურ დროში იღებს სხვა სუბიექტის ელექტრონული სისტემისგან, ამ მონაცემების სათანადო მოცულობით, თანმიმდევრულად და ერთგვაროვნად დამუშავების უზრუნველყოფის მიზნებისთვის მნიშვნელოვანია, ხსენებულ სუბიექტებს შორის წერილობითი შეთანხმებით მოწესრიგდეს მონაცემთა რეალურ დროში მიმოცვლის საკითხი.

— მონაცემების უშუალოდ მონაცემთა სუბიექტისგან შეგროვების შემთხვევაში მნიშვნელოვანია მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა

კანონის 24-ე მუხლის მოთხოვნათა დაცვით უზრუნველყონ მონაცემთა სუბიექტისთვის სრულყოფილი და სწორი ინფორმაციის მიწოდება მონაცემთა დამუშავებასთან დაკავშირებული საკითხების თაობაზე. ამასთან, ინფორმაცია მონაცემთა სუბიექტს უნდა ეცნობოს მისთვის მარტივი და აღქმადი ფორმით.

— კანონის 37-ე მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტით გათვალისწინებული საერთაშორისო გადაცემის საფუძველი (მონაცემთა სუბიექტის წერილობითი თანხმობა) შეიძლება გამოყენებულ იქნეს მხოლოდ გამონაკლის შემთხვევაში. კერძოდ, მონაცემთა სუბიექტის ფუნდამენტური უფლებების დაცვის უზრუნველყოფის მიზნებისთვის უპირველესად უნდა შემოწმდეს, მიმღები სახელმწიფო ექცევა თუ არა სამსახურის უფროსის ბრძანებით დამტკიცებულ პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხაში. იმ შემთხვევაში, თუ სახელმწიფო, რომელსაც მონაცემები გადაეცემა, არ არის აღნიშნულ ნუსხაში და, შესაბამისად, ვერ უზრუნველყოფს მონაცემთა დაცვის სათანადო გარანტიებს, უპირველესად მნიშვნელოვანია, დამუშავებისთვის პასუხისმგებელმა პირმა აღნიშნული გარანტიები შექმნას შესაბამის სახელმწიფოსთან, ასეთი სახელმწიფოს სათანადო საჯარო დაწესებულებასთან, იურიდიულ პირთან, ფიზიკურ პირთან ან საერთაშორისო ორგანიზაციასთან დადებული ხელშეკრულებით. მხოლოდ აღნიშნული გარანტიების შექმნის შეუძლებლობის შემთხვევაშია დასაშვები მონაცემთა საერთაშორისო გადაცემა მონაცემთა სუბიექტის წერილობითი თანხმობის საფუძველზე.
— მონაცემების უშუალოდ მონაცემთა სუბიექტისგან შეგროვების პროცესში დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ მონაცემთა სუბიექტისთვის კანონით გათვალისწინებული ინფორმაციის სრულყოფილად მიწოდება.
— დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის არსებული ხელშეკრულება დეტალურად უნდა ითვალისწინებდეს კანონის 36-ე მუხლის პირველი და მე-2 პუნქტით გათვალისწინებულ პირობებს.
— დამუშავებისთვის პასუხისმგებელი პირები, რომლებიც ახორციელებენ ვიდეომონიტორინგს, აუდიომონიტორინგს ან ამუშავებენ ბიომეტრიულ მონაცემებს, ვალდებულნი არიან დამუშავების პროცესები კანონის მოთხოვნათა დაცვით სრულყოფილად განსაზღვრონ წერილობითი ფორმით.

II თავი. ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობის კონტროლი

1. მნიშვნელოვანი მიმართულებები და ტენდენციები

პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის ერთ-ერთი ძირითადი მიმართულებაა ფარულ საგამოძიებო მოქმედებებზე კონტროლის განხორციელება, რაც ფარული საგამოძიებო მოქმედებების ჩატარებასა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების მონიტორინგს მოიცავს.

2024 წლის პირველ მარტამდე მოქმედი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-40[16] მუხლით განსაზღვრული უფლება-მოვალეობები, კონტროლის ფორმები და შესაბამისი სამართალდამცავი თუ მართლმსაჯულების განმახორციელებელი ორგანოების ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული წესები თითქმის ანალოგიურად მოწესრიგდა ახალი კანონის 54-ე მუხლით, რომლის შესაბამისად, სამსახური მუდმივ რეჟიმში სარგებლობს კონტროლის ელექტრონული და კონტროლის სპეციალური ელექტრონული სისტემებით და აკვირდება ფარული საგამოძიებო მოქმედებების — სატელეფონო კომუნიკაციის ფარული მიყურადების და ჩაწერის და გეოლოკაციის რეალურ დროში განსაზღვრის — მიმდინარეობას.

ფარული საგამოძიებო მოქმედებების ჩატარების სპეციფიკის გათვალისწინებით, ზემოაღნიშნულის გარდა, სხვა ფარული საგამოძიებო მოქმედებები არ ხორციელდება კონტროლის ელექტრონული სისტემის საშუალებით. ამდენად, სამსახურს ფარული საგამოძიებო მოქმედების ჩატარების ნებართვის შესახებ დოკუმენტაცია (სასამართლოს განჩინებები და პროკურორის დადგენილებები) წარედგინება მატერიალური სახით. ზედამხედველობის ფარგლებში სამსახური სასამართლო განჩინებებისა და პროკურორის დადგენილებების მატერიალურ ეგზემპლარებს აღნიშნულ დოკუმენტებში მითითებული მონაცემების სისწორისა და ელექტრონულ სისტემებთან შესაბამისობის დადგენის მიზნით ერთმანეთს ადარებს.

ფარული საგამოძიებო მოქმედებების ჩატარების ნებართვის შესახებ დოკუმენტაციისა და ელექტრონულ სისტემებში ასახული მონაცემების შესაბამისობის მონიტორინგის საფუძველზე, პერსონალურ მონაცემთა დაცვის სამსახური, საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143[6]-ე მუხლის მე-5 ნაწილის შესაბამისად, უფლებამოსილია კონტროლის ელექტრონული სისტემის მეშვეობით შეაჩეროს ფარული საგამოძიებო მოქმედება, თუ:

— ფარული საგამოძიებო მოქმედების – სატელეფონო კომუნიკაციის ფარული მიყურადება და ჩაწერა – ჩატარების შესახებ მოსამართლის განჩინების (რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს)

ელექტრონული ეგზემპლარის პერსონალურ მონაცემთა დაცვის სამსახურისთვის წარმოდგენა არ განხორციელდა;

— არ მოხდა ფარული საგამოძიებო მოქმედების – სატელეფონო კომუნიკაციის ფარული მიყურადება და ჩაწერა – ჩატარების შესახებ მოსამართლის განჩინების (რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს) მატერიალური ეგზემპლარის პერსონალურ მონაცემთა დაცვის სამსახურისთვის წარმოდგენა განჩინების გამოტანისთანავე, დაუყოვნებლივ, მაგრამ არა უგვიანეს 48 (ორმოცდარვა) საათისა;

— პერსონალურ მონაცემთა დაცვის სამსახურში წარმოდგენილი არ არის გადაუდებელი აუცილებლობის შემთხვევაში ფარული საგამოძიებო მოქმედების - სატელეფონო კომუნიკაციის ფარული მიყურადება და ჩაწერა - ჩატარების შესახებ პროკურორის დადგენილების (რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს) ელექტრონული ეგზემპლარი;

— ფარული საგამოძიებო მოქმედების დადგენილებაში მითითებული დაწყების დროიდან არა უგვიანეს 12 საათისა, პერსონალურ მონაცემთა დაცვის სამსახურში წარმოდგენილი არ არის გადაუდებელი აუცილებლობის შემთხვევაში ფარული საგამოძიებო მოქმედების – სატელეფონო კომუნიკაციის ფარული მიყურადება და ჩაწერა – ჩატარების შესახებ პროკურორის დადგენილების (რომელიც მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს შეიცავს) მატერიალური ეგზემპლარი;

— პერსონალურ მონაცემთა დაცვის სამსახურში ელექტრონული სისტემის მეშვეობით ან მატერიალური (დოკუმენტური) სახით წარდგენილი პროკურორის დადგენილების რეკვიზიტები ან/და სარეზოლუციო ნაწილი ბუნდოვანება-უზუსტობას შეიცავს;

— პერსონალურ მონაცემთა დაცვის სამსახურში ელექტრონული სისტემის მეშვეობით წარმოდგენილი პროკურორის დადგენილების ელექტრონული ეგზემპლარის რეკვიზიტებსა და სარეზოლუციო ნაწილში და მატერიალური (დოკუმენტური) სახით წარდგენილი პროკურორის დადგენილების რეკვიზიტებსა და სარეზოლუციო ნაწილში გათვალისწინებული მონაცემები (დადგენილების შედგენის თარიღი და ადგილი; მითითება საქართველოს სისხლის სამართლის კოდექსის იმ მუხლზე, რომლითაც მიმდინარეობს გამოძიება; პროკურორის სახელი და გვარი, ხელმოწერა; საიდუმლოების აღმნიშვნელი გრიფი; ბეჭედი; განსახორციელებელი ფარული საგამოძიებო მოქმედების სახე; მოქმედების განხორციელების პერიოდი (მისი დაწყებისა და დასრულების თარიღებისა და დროის მითითებით)) ერთმანეთს არ ემთხვევა.

საგულისხმოა, რომ პერსონალურ მონაცემთა დაცვის სამსახურის უფლებამოსილება — შეაჩეროს ფარული საგამოძიებო მოქმედება — ვრცელდება იმ შემთხვევაშიც, თუ ბუნდოვანება-უზუსტობა აღმოჩენილია პროკურორის დადგენილებაში. მოსამართლის განჩინებაში მსგავსი ხარვეზის არსებობის შემთხვევაში შეტყობინება კონტროლის ელექტრონული სისტემის საშუალებით

ეგზავნება სსიპ — „საქართველოს ოპერატიულ-ტექნიკური სააგენტოს“, როგორც კონკრეტული ფარული საგამოძიებო მოქმედების ჩატარებაზე ექსკლუზიური უფლებამოსილების მქონე უწყებას.

პერსონალურ მონაცემთა დაცვის სამსახურის მხრიდან ფარული საგამოძიებო მოქმედების შეჩერების შემთხვევაში ფარული საგამოძიებო მოქმედებების ჩატარებაში ჩართული შესაბამისი უწყებები (სსიპ — „საქართველოს ოპერატიულ-ტექნიკური სააგენტო“, სასამართლო და პროკურორი ან შესაბამისი საგამოძიებო უწყების უფლებამოსილი წარმომადგენელი), საკუთარი კომპეტენციის ფარგლებში, ვალდებულნი არიან ფარული საგამოძიებო მოქმედების შეჩერებიდან 3 (სამი) დღის ვადაში სამსახურში წარმოადგინონ შეჩერების აღმოფხვრის დამადასტურებელი მოსამართლის განჩინების ან პროკურორის დადგენილების მატერიალური და ელექტრონული ეგზემპლარები. პერსონალურ მონაცემთა დაცვის სამსახური ხარვეზის აღმოფხვრის დამადასტურებელი მტკიცებულებების მიღებას ადასტურებს ელექტრონულად, რის საფუძველზეც გრძელდება ფარული საგამოძიებო მოქმედება.

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ განჩინებაში ბუნდოვანება-უზუსტობის აღმოჩენის შემთხვევაში, აღნიშნული ინფორმაციის მიღებისთანავე პროკურორი ვალდებულია ხარვეზის აღმოფხვრის მოთხოვნით მიმართოს განჩინების გამომტან სასამართლოს. თავის მხრივ, სასამართლომ აღნიშნული მოთხოვნის მიღებიდან 12 (თორმეტი) საათის ვადაში უნდა უზრუნველყოს განჩინებაში არსებული ბუნდოვანება-უზუსტობის აღმოფხვრა, აღმოფხვრიდან 24 (ოცდაოთხი) საათის განმავლობაში კი უზრუნველყოს ამ განჩინების პერსონალურ მონაცემთა დაცვის სამსახურისთვის წარმოდგენა.

კონტროლის ფუნქცია გულისხმობს ფარული საგამოძიებო მოქმედებების დასრულების შემდგომი ღონისძიებების მონიტორინგსაც. კერძოდ:

— საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143^6 მუხლის მე-14 ნაწილის იმპერატიული მოთხოვნაა, რომ შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანომ, სსიპ — „საქართველოს ოპერატიულ-ტექნიკურმა სააგენტომ“, ფარული საგამოძიებო მოქმედების დასრულებისთანავე შეადგინოს ოქმი, რომელშიც ზუსტად უნდა იყოს აღნიშნული ფარული საგამოძიებო მოქმედების ჩატარების სამართლებრივი საფუძველი, მისი დაწყებისა და დასრულების დრო, ოქმის შედგენის ადგილი, ჩატარებული ფარული საგამოძიებო მოქმედების სახე და მისი ჩატარებისას გამოყენებული ტექნიკური საშუალებები, ფარული საგამოძიებო მოქმედების ჩატარების ადგილი, ფარული საგამოძიებო მოქმედების ობიექტი;

— ფარული საგამოძიებო მოქმედების დასრულების თაობაზე შედგენილი ოქმი დაუყოვნებლივ უნდა წარედგინოს პერსონალურ მონაცემთა დაცვის სამსახურს;

— ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაცია დაუყოვნებლივ უნდა განადგურდეს, თუ მას გამოძიებისთვის ღირებულება არა აქვს, მოპოვებულ იქნა გადაუდებელი აუცილებლობისას მოსამართლის განჩინების გარეშე ჩატარებული ფარული საგამოძიებო მოქმედების შედეგად და, მიუხედავად სასამართლოს მიერ მისი კანონიერად ცნობისა,

ბრალდების მხარემ საქმის არსებითად განმხილველ სასამართლოს იგი მტკიცებულებად არ წარუდგინა ან ფარული საგამოძიებო მოქმედებების შედეგად მოპოვებულია ისეთი მასალა, რომელიც არ ეხება პირის დანაშაულებრივ საქმიანობას, მაგრამ შეიცავს ცნობებს მისი ან სხვა პირის პირადი ცხოვრების შესახებ, პროკურორის გადაწყვეტილებით, ფარული საგამოძიებო მოქმედების შეწყვეტის ან დასრულების შემდეგ. ასეთ შემთხვევაში საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143[8] მუხლის მე-5 ნაწილი საგამოძიებო მოქმედების განმახორციელებელ ორგანოს ავალდებულებს, შეადგინოს ოქმი ფარული საგამოძიებო მოქმედებების შედეგად მოპოვებული მასალის განადგურების თაობაზე, რომელიც ასევე წარმოდგენილ უნდა იქნეს პერსონალურ მონაცემთა დაცვის სამსახურში.

პერსონალურ მონაცემთა დაცვის სამსახური ფარული საგამოძიებო მოქმედებების კონტროლს ახორციელებს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის / დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების შემოწმების(ინსპექტირება) გზითაც.

საქმიანობის ფარგლებში გამოვლენილი ხარვეზებისა და ტენდენციების გათვალისწინებით, პერსონალურ მონაცემთა დაცვის სამსახური ყოველწლიურად ადგენს მომდევნო წლის პრიორიტეტულ მიმართულებებს. ასეთად 2024 წელს გეოლოკაციის დროში განსაზღვრის პროცესში მონაცემთა დამუშავება, ფარული საგამოძიებო მოქმედებების დასრულების თაობაზე ოქმების სამსახურში წარმოდგენის ვალდებულების შესრულების კანონშესაბამისობის შემოწმებაც განისაზღვრა.

ზემოთ დასახელებულ საკითხებთან დაკავშირებით, პერსონალურ მონაცემთა დაცვის სამსახურმა ჩაატარა 4 (ოთხი) გეგმური შემოწმება.[28] ჩატარებული შემოწმებების ფარგლებში სამსახურმა გამოავლინა 2(ორი) სამართალდარღვევის ფაქტი და გასცა 4 (ოთხი) შესასრულებლად სავალდებულო დავალება, რომელთაგან 1 (ერთი) შესრულდა, ხოლო 3 (სამი) მათგანის შესრულების ვადა ჯერ არ ამოწურულა. სამსახურმა ამავე შემოწმებების ფარგლებში გასცა 2 (ორი) რეკომენდაცია.

2. გადაწყვეტილებები

ა. საქართველოს სახელმწიფო უსაფრთხოების სამსახური

საქართველოს სახელმწიფო უსაფრთხოების სამსახურისა და საქართველოს ფინანსთა სამინისტროს საგამოძიებო სამსახურის ერთ-ერთ ამოცანას საკუთარი კომპეტენციის ფარგლებში სისხლის სამართლის საქმეთა გამოძიება წარმოადგენს. ამდენად, საქართველოს სისხლის სამართლის საპროცესო კოდექსის 34-ე მუხლის შესაბამისად, ისინი, სხვა საგამოძიებო ორგანოების მსგავსად, იყენებენ ყველა იმ

[28] 3 (სამი) შემოწმება ჩატარდა საიდუმლო წესით.

ინსტრუმენტს, მათ შორის ფარულ საგამოძიებო მოქმედებებს, რომლებიც საჭიროა გამოძიების სრულად და ობიექტურად ჩასატარებლად.

საქართველოს სისხლის სამართლის საპროცესო კოდექსის XVI[1] თავი არეგულირებს ფარულ საგამოძიებო მოქმედებებთან დაკავშირებულ საკითხებს. ამავე თავშია მოქცეული ფარული საგამოძიებო მოქმედებების შეწყვეტისა და შეჩერების საკითხები. როგორც უკვე აღინიშნა, ხსენებული კოდექსის 143[6] მუხლის მე-14 ნაწილი განსაზღვრავს ფარული საგამოძიებო მოქმედების დასრულების შემდეგ აღნიშნულის თაობაზე უფლებამოსილი სახელმწიფო ორგანოს მიერ ოქმის შედგენის ვალდებულებას. ოქმი გადაეცემა შესაბამის უფლებამოსილ საგამოძიებო ორგანოს, რომელიც აღნიშნულ დოკუმენტს დაუყოვნებლივ წარუდგენს პერსონალურ მონაცემთა დაცვის სამსახურს.

2024 წელს გეგმურად შემოწმდა საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანტიკორუფციული სააგენტოს (დეპარტამენტი), როგორც უფლებამოსილი საგამოძიებო ორგანოს მიერ 2023 წლის პირველი სექტემბრიდან 2024 წლის 14 მარტამდე პერიოდში ჩატარებული ფარული საგამოძიებო მოქმედებების შემთხვევაში, საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143[6] მუხლის მე-14 ნაწილით გათვალისწინებული, ფარული საგამოძიებო მოქმედების დასრულების შესახებ ოქმის პერსონალურ მონაცემთა დაცვის სამსახურში წარმოდგენის ვალდებულების შესრულების საკითხი.

შემოწმებით გაირკვა, რომ სახელმწიფო უსაფრთხოების სამსახური ჯეროვნად უზრუნველყოფს ფარული საგამოძიებო მოქმედებების დასრულების თაობაზე ოქმების პერსონალურ მონაცემთა დაცვის სამსახურში წარმოდგენას. შესაბამისად, შემოწმების ფარგლებში არ გამოვლენილა სამართალდარღვევის ფაქტი.

ბ. სსიპ — „საქართველოს ოპერატიულ-ტექნიკური სააგენტო“

პერსონალურ მონაცემთა დაცვის სამსახურმა გეგმურად[29] შეისწავლა სსიპ — „საქართველოს ოპერატიულ-ტექნიკური სააგენტოს“ მიერ, გეოლოკაციის რეალურ დროში განსაზღვრის კონტროლის სპეციალური ელექტრონული სისტემის საშუალებით, საქართველოს შინაგან საქმეთა სამინისტროს მმართველობის სფეროში მოქმედ სსიპ — „საზოგადოებრივი უსაფრთხოების მართვის ცენტრ „112“-ში განხორციელებული შეტყობინების ინიციატორი მობილური საკომუნიკაციო აღჭურვილობის გეოლოკაციის ავტომატურ რეჟიმში განსაზღვრის ლოგირების მონაცემების პერსონალურ მონაცემთა დაცვის სამსახურისათვის რეალურ დროში მიწოდების ვალდებულების შესრულების საკითხი.

სსიპ — „საზოგადოებრივი უსაფრთხოების მართვის ცენტრ „112“-ის ერთ-ერთ ძირითად ამოცანას წარმოადგენს, გადაუდებელი დახმარების ოპერატიული და ეფექტიანი მართვის მიზნით, საგანგებო სიტუაციებსა და საქართველოს კანონმდებლობით განსაზღვრულ სხვა შემთხვევებში ერთიანი სატელეფონო ნომრის — „112“-ის საშუალებით შეტყობინებების მიღება; ასევე – უფლებამოსილ

[29] შემოწმება დაიწყო 2023 წლის ბოლოს და დასრულდა 2024 წლის დასაწყისში.

სუბიექტებთან ერთად, საგანგებო სიტუაციებისა და გადაუდებელი დახმარების გაწევის აუცილებლობის სხვა შემთხვევების ოპერატიული და ეფექტიანი მართვა და ამ მიზნით აღნიშნულ სუბიექტებთან კოორდინირებული საქმიანობის უზრუნველყოფა. შესაბამისად, სსიპ — „საქართველოს ოპერატიულ-ტექნიკური სააგენტოს“ მიერ შექმნილი, გეოლოკაციის რეალურ დროში განსაზღვრის კონტროლის სპეციალური ელექტრონული საშუალებით ხდება სსიპ — „საზოგადოებრივი უსაფრთხოების მართვის ცენტრ „112“-ში განხორციელებული შეტყობინების ინიციატორი მობილური საკომუნიკაციო აღჭურვილობის მომხმარებლის ადგილმდებარეობის ავტომატურ რეჟიმში დადგენა. „112“-ის ფუნქციებიდან, განხორციელებული შეტყობინებების შინაარსისა და მოცულობიდან გამომდინარე, გეოლოკაციის რეალურ დროში განსაზღვრის ფარგლებში მუშავდება მონაცემთა სუბიექტების დიდი რაოდენობის მონაცემები ადგილმდებარეობის შესახებ. ამ პირობებში მნიშვნელოვანია დაცული იყოს მონაცემთა დამუშავების კანონიერება და კანონმდებლობით გათვალისწინებული ვალდებულებები, რომლებიც მოცემულ შემთხვევაში ხორციელდება გეოლოკაციის ავტომატურ რეჟიმში განსაზღვრის ლოგირების მონაცემების სამსახურისათვის მოწოდების გზით.

შესწავლის ფარგლებში მოპოვებული მტკიცებულებების საფუძველზე არ გამოვლინდა სამართალდარღვევის ფაქტი და არც დავალება/რეკომენდაციის გაცემის საჭიროება დამდგარა.

— კომპიუტერულ მონაცემთან დაკავშირებული საგამოძიებო მოქმედებების განხორციელების პროცესში ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების დამუშავებისას პერსონალურ მონაცემთა დაცვის სამსახურის კონტროლის მექანიზმი

პერსონალურ მონაცემთა დაცვის სამსახურის საზედამხედველო ფუნქციის თვალსაზრისით სამსახურის მანდატი ვრცელდება საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-138-ე მუხლებით გათვალისწინებულ საგამოძიებო მოქმედებებზე. აღნიშნული მუხლებით გათვალისწინებული საგამოძიებო მოქმედებები, რომლებიც არ წარმოადგენს ფარულ საგამოძიებო მოქმედებებს, შეეხება კომპიუტერულ მონაცემთა შესანახ საშუალებაში დაცული სისხლის სამართლის საქმისთვის მნიშვნელოვანი ინფორმაცია/დოკუმენტაციის გამოთხოვას, ინტერნეტტრაფიკის მონაცემთა მიმდინარე შეგროვებასა და შინაარსობრივი მონაცემების მოპოვებას.

ზემოაღნიშნული საგამოძიებო მოქმედებების განხორციელების პროცესში საგამოძიებო ორგანოები უფლებამოსილნი არიან ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემები გამოითხოვონ როგორც ელექტრონული კომუნიკაციების კომპანიებიდან, ასევე სსიპ — „საქართველოს ოპერატიულ-ტექნიკური სააგენტოს“ ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი ბანკიდან, რომელშიც ინახება ელექტრონული კომუნიკაციების კომპანიების მონაცემთა ბაზებში დაცული მონაცემების ასლები.

საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით გათვალისწინებული საგამოძიებო მოქმედების ჩატარებაზე ზედამხედველობის განხორციელების თვალსაზრისით, საგულისხმოა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლის მე-5 ნაწილით გათვალისწინებული იმპერატიული მოთხოვნა, რომლის თანახმადაც, ელექტრონული კომუნიკაციის კომპანიამ სამართალდამცავი ორგანოსთვის ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით დადგენილი წესით გადაცემის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურს უნდა აცნობოს ამ მონაცემების გადაცემიდან 24 საათში.

საგამოძიებო ორგანოების მხრიდან ზემოხსენებული ფორმით მონაცემების მოპოვების კონტროლს პერსონალურ მონაცემთა დაცვის სამსახური უზრუნველყოფს როგორც დამუშავებისთვის პასუხისმგებელი პირის/დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების (ინსპექტირების) შემოწმებით, ასევე – ელექტრონული კომუნიკაციების კომპანიებისა თუ სამართალდამცავი ორგანოების მიერ წარმოდგენილი ინფორმაციის დადარების გზით.

ყურადღება უნდა გამახვილდეს საქართველოს სისხლის სამართლის საპროცესო კოდექსში 2022 წლის 24 მაისის საქართველოს №1575 კანონის საფუძველზე განხორციელებულ ცვლილებებზე, რომელთა მიხედვითაც, 136-ე მუხლით განსაზღვრულ საგამოძიებო მოქმედებაზე აღარ ვრცელდება ამავე კოდექსის XVI[1] თავით დადგენილი ფარული საგამოძიებო მოქმედებების ჩატარებისა და მათზე ზედამხედველობის წესები.

ცვლილების განხორციელებამდე, სსსკ-ის 136-ე მუხლის მე-4 ნაწილის თანახმად, აღნიშნული მუხლით გათვალისწინებულ საგამოძიებო მოქმედებებს, მათი ჩატარების ზოგად წესებსა და პრინციპებს, არეგულირებდა ამავე კოდექსის 143[2]-143[10] მუხლების დებულებები. კერძოდ, 143[3] მუხლის თანახმად, მოსამართლე განჩინებით იღებდა გადაწყვეტილებას ფარული საგამოძიებო მოქმედების ჩატარების ნებართვის გაცემის შესახებ ან მისი ჩატარების ნებართვის გაცემაზე უარის თქმის შესახებ და ერთი ეგზემპლარი, რომელიც შეიცავდა მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, განჩინების გამოტანისთანავე, დაუყოვნებლივ, არა უგვიანეს 48 საათისა, მატერიალური (დოკუმენტური) სახით, სასამართლოს მიერ მიეწოდებოდა პერსონალურ მონაცემთა დაცვის სამსახურს.

2022 წლის 24 მაისის ცვლილებების შედეგად, სსსკ-ის 136-ე მუხლის მე-4 ნაწილი ამოღებულ იქნა და მუხლს დაემატა მე-4[1] ნაწილი, რომლის თანახმად, ამ მუხლით გათვალისწინებულ საგამოძიებო მოქმედებაზე ვრცელდება სსსკ-ის 111-ე, 112-ე და 134-ე მუხლების დებულებები, რომლებიც მიემართება საგამოძიებო მოქმედების ჩატარების ზოგად წესებს.

სსსკ-ის 112-ე მუხლი არ იცნობდა და არც ზემოხსენებული საკანონმდებლო ცვლილებების შედეგად ითვალისწინებს ჩატარებული საგამოძიებო მოქმედების შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისათვის შეტყობინების ვალდებულებას. ამავდროულად, სსსკ-ის 136-ე მუხლის მე-5 ნაწილის როგორც მოქმედი, ასევე ხსენებულ ცვლილებებამდე არსებული რედაქციის თანახმად, ამ მუხლით გათვალისწინებული საგამოძიებო მოქმედების კონტროლსა და

ზედამხედველობას პერსონალურ მონაცემთა დაცვის სამსახური ახორციელებს, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად.

გარდა აღნიშნულისა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს 2024 წლის პირველ მარტამდე მოქმედი კანონის მე-20 მუხლის მე-3 პუნქტი ითვალისწინებდა დათქმას, რომ სამართალდამცავი ორგანოს მიერ მოთხოვნილი ფარული საგამოძიებო მოქმედების ჩატარების ნებართვის გაცემის ან მისი ჩატარების ნებართვის გაცემაზე უარის თქმის შესახებ მოსამართლის განჩინების 1 ეგზემპლარი, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, აგრეთვე – სამართალდამცავი ორგანოს მიერ სასამართლოს ნებართვის გარეშე ჩატარებული ფარული საგამოძიებო მოქმედების კანონიერად/უკანონოდ ცნობის შესახებ მოსამართლის განჩინების 1 ეგზემპლარი, მხოლოდ რეკვიზიტებითა და სარეზოლუციო ნაწილით, წარედგინებოდა პერსონალურ მონაცემთა დაცვის სამსახურს, საქართველოს სისხლის სამართლის საპროცესო კოდექსით დადგენილი წესით.

2024 წლის პირველ მარტამდე მოქმედი კანონის მე-20 მუხლის მე-5 პუნქტის თანახმადაც, გადაუდებელი აუცილებლობის შემთხვევაში ფარული საგამოძიებო მოქმედების ჩატარების შესახებ პროკურორის დადგენილებას, რომელიც შეიცავდა მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, ფარული საგამოძიებო მოქმედების დადგენილებაში მითითებული დაწყების დროიდან არა უგვიანეს 12 საათისა, პროკურორი ან პროკურორის დავალებით გამომძიებელი მატერიალური (დოკუმენტური) სახით წარუდგენდა პერსონალურ მონაცემთა დაცვის სამსახურს; ხოლო ამავე მუხლის მე-4 პუნქტის შესაბამისად, ელექტრონული კომუნიკაციის კომპანიას სამართალდამცავი ორგანოსთვის ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით დადგენილი წესით გადაცემის შესახებ უნდა ეცნობებინა პერსონალურ მონაცემთა დაცვის სამსახურისათვის, ამ მონაცემების გადაცემიდან 24 საათში.

აღნიშნული დათქმები არ შეცვლილა 2024 წლის პირველ მარტს ამოქმედებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით და მოწესრიგდა ამ კანონის 28-ე მუხლის მე-4, მე-5 და მე-6 პუნქტებით.

საკანონმდებლო ცვლილებების შედეგად, საერთო სასამართლოები სამსახურს აღარ უგზავნიან განჩინების სარეზოლუციო ნაწილსა და რეკვიზიტებს, ასევე აღარ იგზავნება პროკურორის დადგენილებები, ვინაიდან სსსკ-ის 136-ე მუხლში აღარ არსებობს აღნიშნული ვალდებულების წარმომშობ ნორმებზე პირდაპირი მითითება.

„პერსონალურ მონაცემთა დაცვის შესახებ’’ საქართველოს კანონის 54-ე მუხლის მე-2 პუნქტის შესაბამისად, საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-138-ე მუხლებით გათვალისწინებული საგამოძიებო მოქმედებების ჩატარების ზედამხედველობას პერსონალურ მონაცემთა დაცვის სამსახური ისევ ახორციელებს სასამართლოს, პროკურატურისა და ელექტრონული კომუნიკაციების კომპანიების მიერ მოწოდებული ინფორმაციის შედარებითა და მონაცემთა დამმუშავებლის/უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების შემოწმებით (ინსპექტირებით).

სისხლის სამართლის საპროცესო კოდექსში განხორციელებულმა ზემოხსენებულმა საკანონმდებლო ცვლილებამ პრაქტიკაში შექმნა სირთულეები, რომლებმაც თავი იჩინა ერთ-ერთი ელექტრონული კომუნიკაციის კომპანიის გეგმური შემოწმების (ინსპექტირების) მიმდინარეობისას. საქმის გარემოებების სრულყოფილად შესწავლისა და ელექტრონული კომუნიკაციის კომპანიის მიერ მასზე დაკისრებული ვალდებულების ჯეროვნად შესრულების კონტროლის მიზნით სასამართლოებს ეთხოვათ სამართალდამცავი ორგანოების მიერ ამ კომპანიიდან ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შესახებ, სსსკ 136-ე მუხლით დადგენილი წესით ინფორმაციის გაზიარება.

მიმართვის საპასუხოდ, საერთო სასამართლოების ნაწილმა სამსახურს მიაწოდა ინფორმაცია/დოკუმენტაცია, ნაწილმა (მათ შორის თბილისისა და ქუთაისის საქალაქო სასამართლოებმა) უარი განაცხადა ინფორმაციის წარმოდგენაზე და მიუთითა, რომ ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების გამოთხოვის შესახებ გაცემული განჩინებების სტატისტიკას არ აღრიცხავენ და, გადატვირთული სამუშაო გრაფიკის გათვალისწინებით, სასამართლოს რესურსის მობილიზებისა და მოთხოვნის დაკმაყოფილების შესაძლებლობას მოკლებულნი იყვნენ, სასამართლოების ნაწილმა კი სამსახურის ზემოხსენებული მოთხოვნა ყოველგვარი რეაგირების გარეშე დატოვა.

შესაბამისად, სამსახურმა სრულყოფილად ვერ შეძლო გადაემოწმებინა, რამდენი განჩინება გასცა სასამართლომ და, მათ საფუძველზე, რამდენ შემთხვევაში და რა სახის ინფორმაცია გადასცა კომპანიამ სამართალდამცავ ორგანოს. სასამართლოთა მხრიდან ინფორმაციის მიუწოდებლობის ფაქტზე შეიქმნა არაგეგმური შემოწმების ჩატარების საჭიროება, რომლის შედეგად დადგინდა სამართალდარღვევა, მაგრამ ეს არ შეიძლება ჩაითვალოს პრობლემის გადაჭრის საშუალებად.

მიზანშეწონილია საკანონმდებლო დონეზე მოწესრიგდეს კონტროლის მექანიზმები, კომპიუტერულ სისტემასა და კომპიუტერულ მონაცემთა შემნახავი საშუალებებიდან ინფორმაციის გამოთხოვის შედეგებზე პერსონალური მონაცემების დაცვის სამსახურისათვის სავალდებულო შეტყობინების შესახებ და ზემოხსენებული წინააღმდეგობების საკანონმდებლო წესით გასწორების მიზნით განახლდეს საკითხის განხილვა.

გ. საქართველოს ფინანსთა სამინისტროს საგამოძიებო სამსახური

პერსონალურ მონაცემთა დაცვის სამსახურმა საქართველოს ფინანსთა სამინისტროს საგამოძიებო სამსახურის გეგმური შემოწმების ფარგლებში შეისწავლა ხსენებული უწყების საგამოძიებო დეპარტამენტის თბილისის მთავარი სამმართველოს მიერ, 2024 წლის პირველი ივნისიდან 2024 წლის პირველ ოქტომბრამდე პერიოდში, ჩატარებული ფარული საგამოძიებო მოქმედებების განხორციელების შემთხვევაში საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143^6 მუხლის მე-14 ნაწილით გათვალისწინებული ფარული საგამოძიებო

მოქმედების დასრულების შესახებ ოქმის პერსონალურ მონაცემთა დაცვის სამსახურში წარმოდგენის ვალდებულების შესრულების საკითხი.

საქართველოს ფინანსთა სამინისტროს საგამოძიებო სამსახურის შემოწმების შედეგად გამოვლინდა სამართალდარღვევის ფაქტი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 66-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული მოქმედებისთვის. ამასთან, საქართველოს ფინანსთა სამინისტროს საგამოძიებო სამსახურს მიეცა რეკომენდაცია იმგვარი ორგანიზაციული ზომების მიღებასთან დაკავშირებით, რომლებიც უზრუნველყოფს ფარული საგამოძიებო მოქმედებების დასრულების შესახებ ოქმების პერსონალურ მონაცემთა დაცვის სამსახურში დაუყოვნებლივ წარმოდგენას.

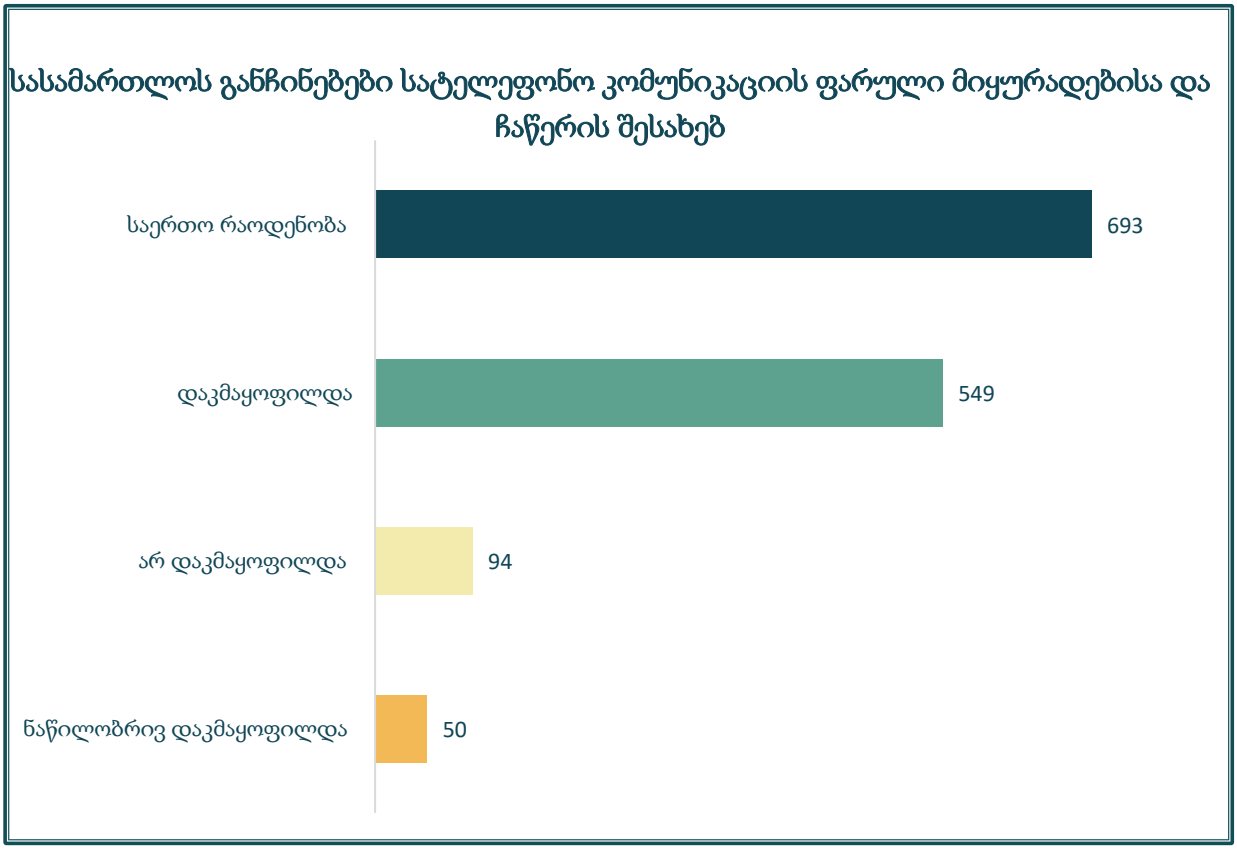
3. დავალებები და რეკომენდაციები

ფარული საგამოძიებო მოქმედებების განხორციელების პროცესში საგამოძიებო ორგანოებმა მაქსიმალურად უნდა გაითვალისწინონ საქართველოს სისხლის სამართლის საპროცესო კოდექსით გათვალისწინებული წესები და პირობები, მათ შორის – ფარული საგამოძიებო მოქმედებების დასრულების თაობაზე ოქმების პერსონალურ მონაცემთა დაცვის სამსახურისთვის დაუყოვნებლივ წარმოდგენის ვალდებულება. გარდა ამისა, მნიშვნელოვანია, დაიცვან „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული მონაცემთა დამუშავების პრინციპი, როგორიცაა მონაცემთა მინიმიზაცია, რომელიც გულისხმობს მხოლოდ იმ მოცულობის მონაცემების დამუშავებას, რაც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად.

სამსახურის პრაქტიკით დადგინდა, რომ კვლავ ფიქსირდება ფარული საგამოძიებო მოქმედებების ჩატარების ნებართვის შესახებ განჩინებების/დადგენილებებისა თუ ფარული საგამოძიებო მოქმედებების დასრულების თაობაზე ოქმების სამსახურში დაგვიანებით წარმოდგენის ფაქტები.

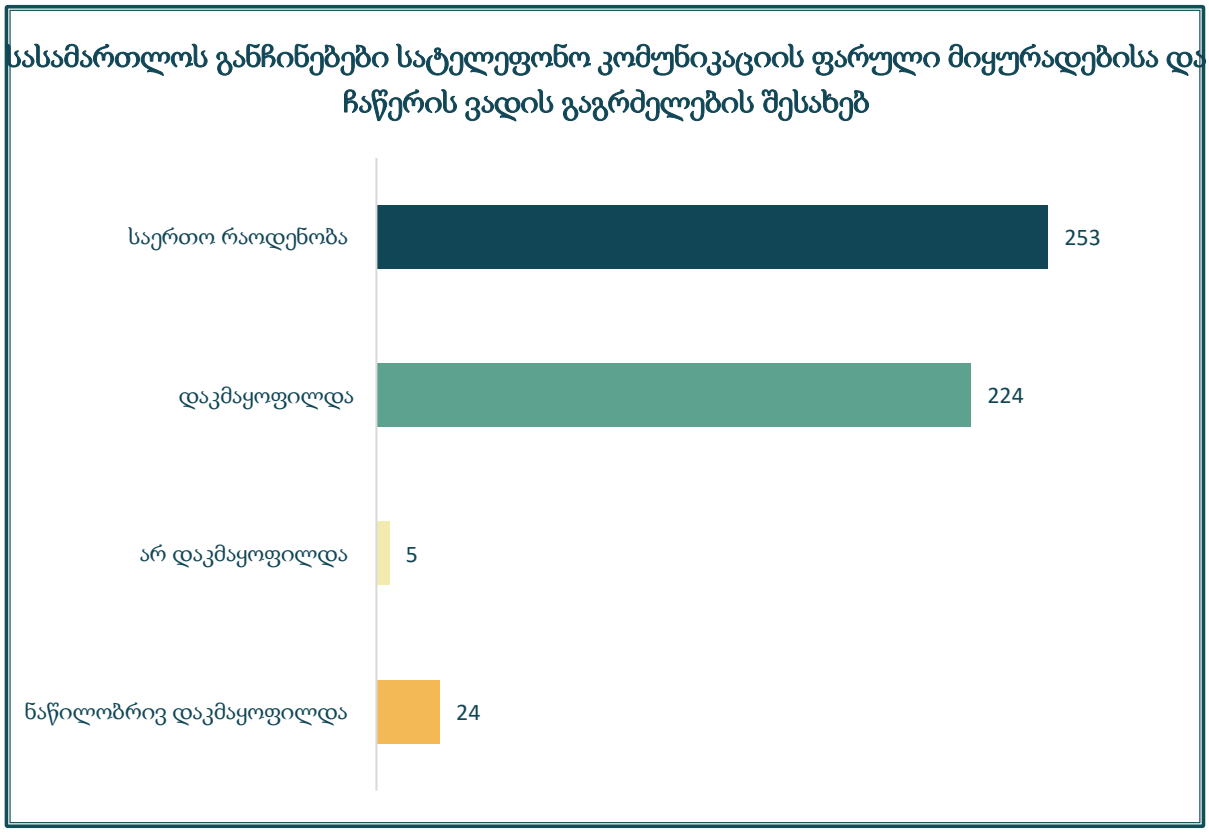
გამოვლენილი ტენდენციების გათვალისწინებით, 2025 წელს პერსონალურ მონაცემთა დაცვის სამსახური განსაკუთრებულ ყურადღებას დაუთმობს იმ პროცესების კანონიერების შესწავლას, რომლებიც კვლავ გამოწვევად რჩება.

4. სტატისტიკური მონაცემი



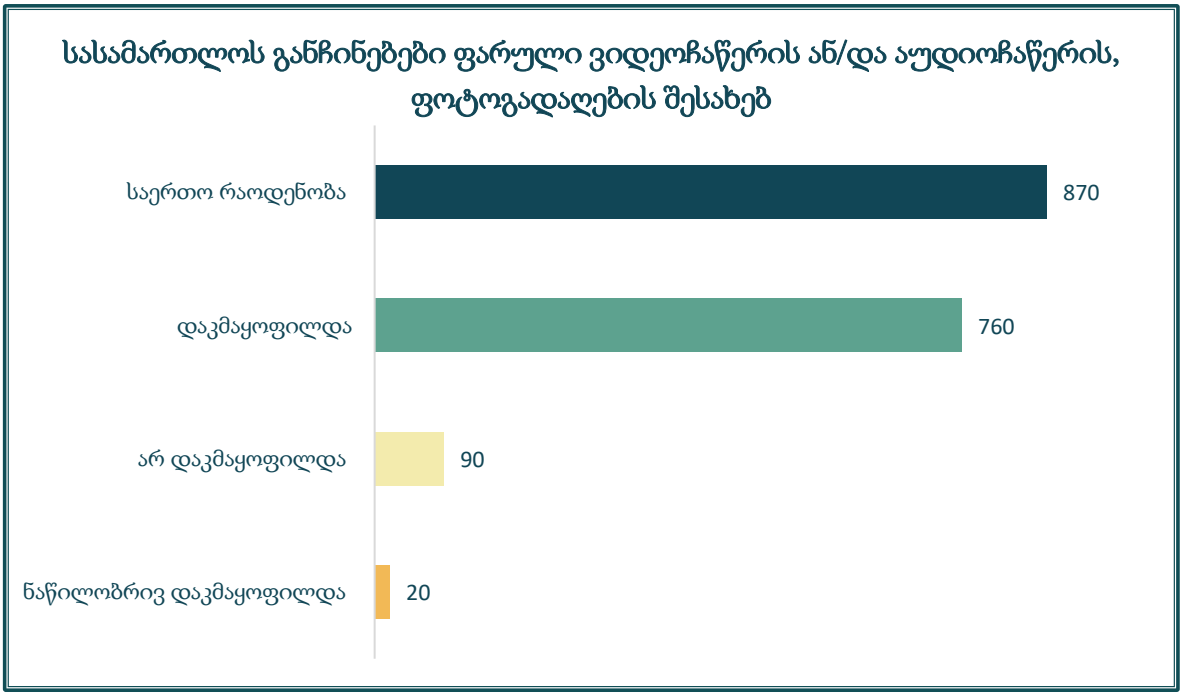
საანგარიშო პერიოდში სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის შესახებ სასამართლომ განიხილა 693 შუამდგომლობა, რომელთა 79% (549) სრულად დაკმაყოფილდა, 14% (94) არ დაკმაყოფილდა, ხოლო 7% (50) ნაწილობრივ დაკმაყოფილდა.

2023 წელს სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის შესახებ სასამართლომ განიხილა 859 შუამდგომლობა, რომელთა 87% (744) სრულად დაკმაყოფილდა, 9% (80) არ დაკმაყოფილდა, ხოლო 4% (35) ნაწილობრივ დაკმაყოფილდა.



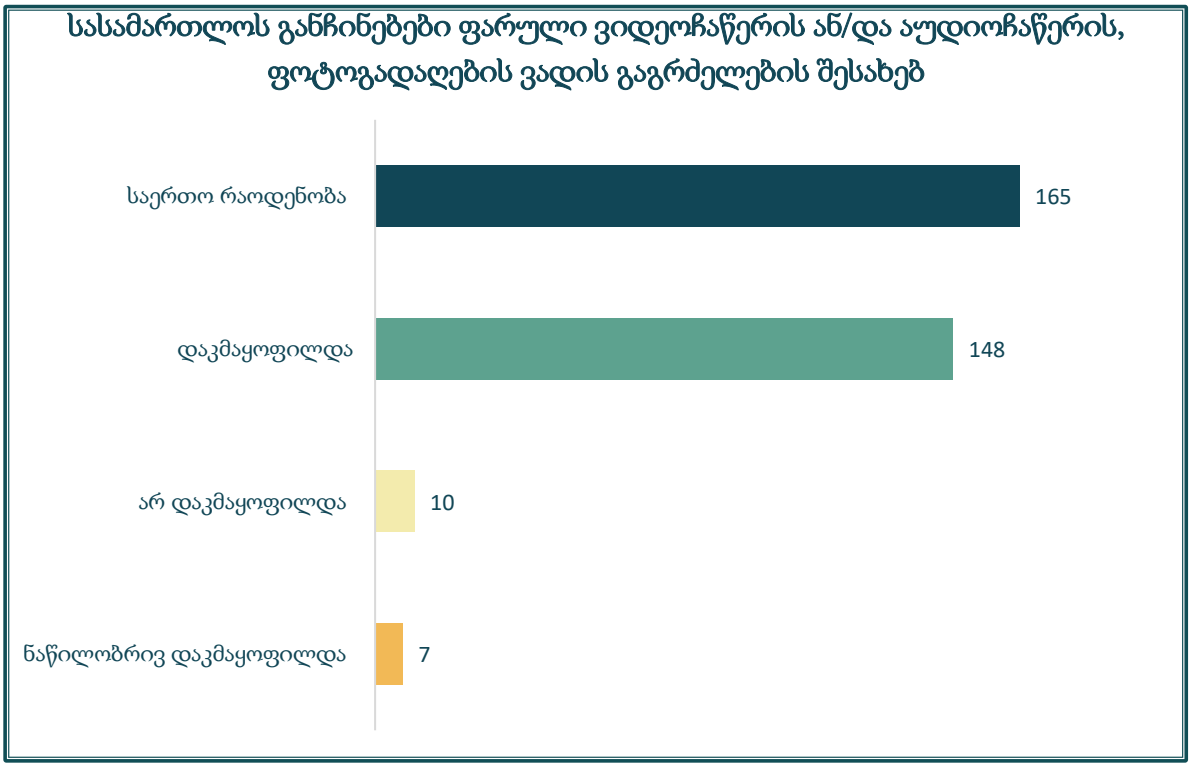
2024 წელს სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ვადის გაგრძელების შესახებ სასამართლომ განიხილა 253 შუამდგომლობა, რომელთაგან დაკმაყოფილდა 89% (224), ნაწილობრივ დაკმაყოფილდა 9% (24), არ დაკმაყოფილდა 2% (5).

2023 წელს სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ვადის გაგრძელების შესახებ სასამართლომ განიხილა 228 შუამდგომლობა, რომელთაგან დაკმაყოფილდა 87% (198), არ დაკმაყოფილდა 4% (8), ნაწილობრივ დაკმაყოფილდა 9% (22).



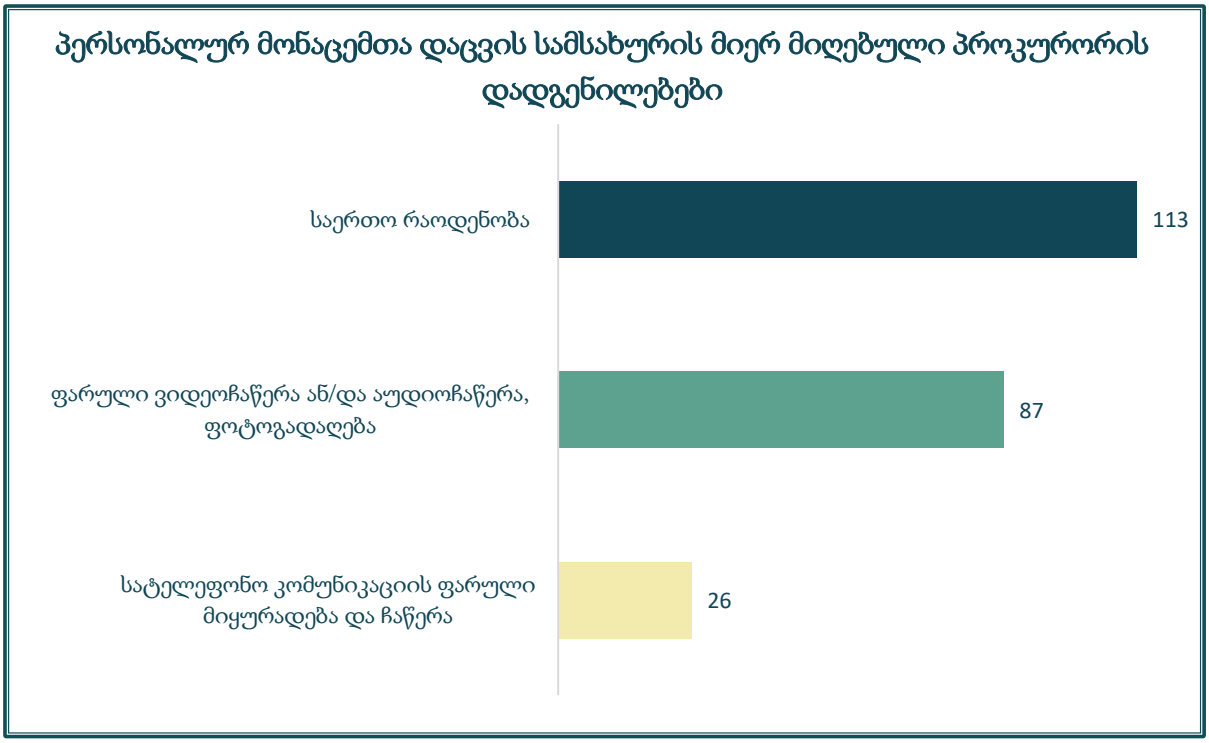
2024 წელს ფარული ვიდეოჩაწერის ან/და აუდიოჩაწერის, ფოტოგადაღების შესახებ სასამართლომ განიხილა 870 შუამდგომლობა, რომელთაგან 88% (760) სრულად დაკმაყოფილდა, 10% (90) არ დაკმაყოფილდა, ხოლო 2% (20) ნაწილობრივ დაკმაყოფილდა.

2023 წელს ფარული ვიდეოჩაწერის ან/და აუდიოჩაწერის, ფოტოგადაღების შესახებ სასამართლომ განიხილა 1022 შუამდგომლობა, რომელთაგან 93% (952) სრულად დაკმაყოფილდა, 6.5% (66) არ დაკმაყოფილდა, ხოლო 0.4% (4) ნაწილობრივ დაკმაყოფილდა.



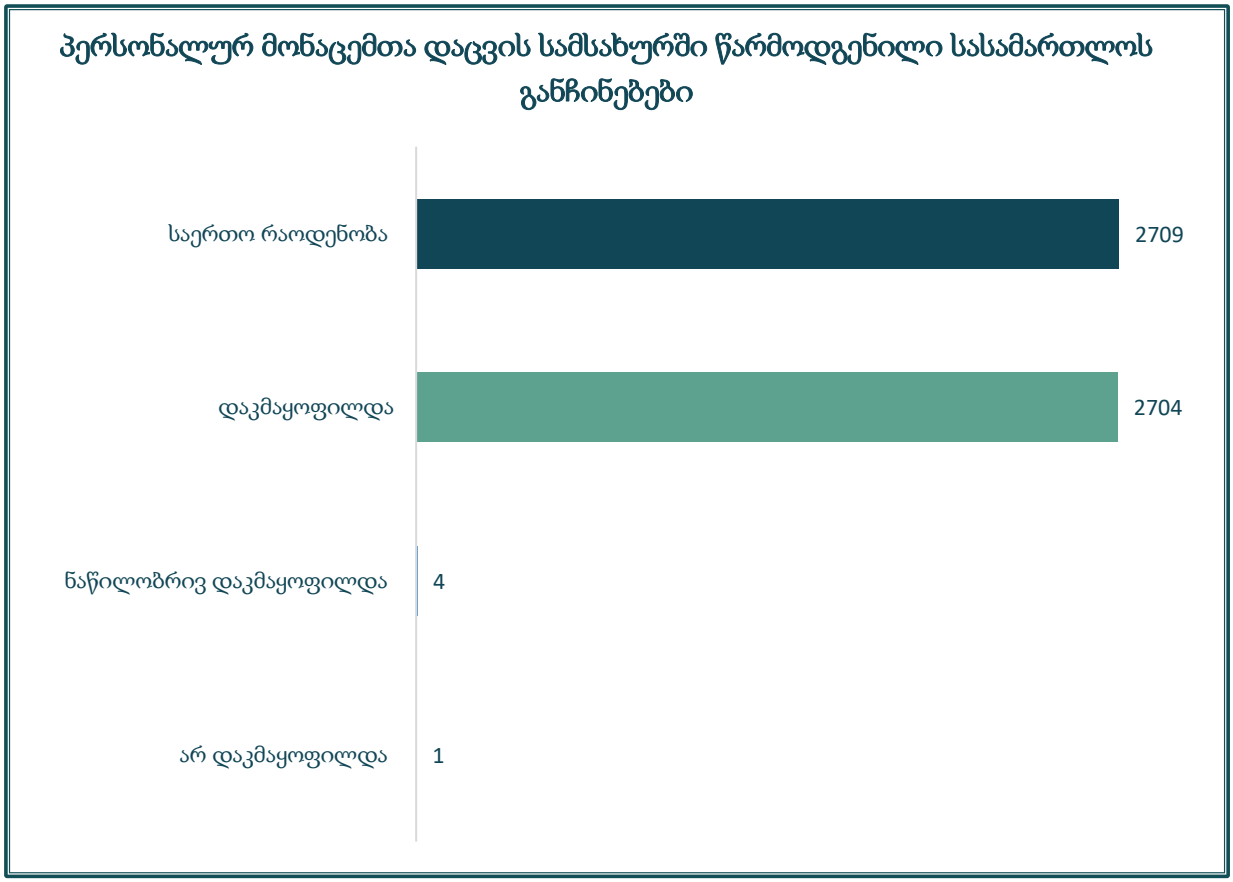
2024 წელს ფარული ვიდეოჩაწერის ან/და აუდიოჩაწერის, ფოტოგადაღების ვადის გაგრძელების შესახებ სასამართლომ განიხილა 165 შუამდგომლობა, რომელთა 90% (148) დაკმაყოფილდა, 6% (10) არ დაკმაყოფილდა, ხოლო 4% (7) ნაწილობრივ დაკმაყოფილდა.

2023 წელს ფარული ვიდეოჩაწერის ან/და აუდიოჩაწერის, ფოტოგადაღების ვადის გაგრძელების შესახებ სასამართლომ განიხილა 122 შუამდგომლობა, რომელთა 86% (105) დაკმაყოფილდა, 12% (15) არ დაკმაყოფილდა, ხოლო 2% (2) ნაწილობრივ დაკმაყოფილდა.



2024 წელს სამსახურს წარედგინა გადაუდებელი აუცილებლობით ფარული საგამოძიებო მოქმედებების ჩატარების შესახებ პროკურორის 113 დადგენილება, რომელთაგან 77% (87) შეეხებოდა ფარულ ვიდეოჩაწერას ან/და აუდიოჩაწერას, ფოტოგადაღებას, 23% (26) შეეხებოდა სატელეფონო კომუნიკაციის ფარულ მიყურადებასა და ჩაწერას.

2023 წელს სამსახურს წარედგინა გადაუდებელი აუცილებლობით ფარული საგამოძიებო მოქმედებების ჩატარების შესახებ პროკურორის 126 დადგენილება.



2024 წელს პერსონალურ მონაცემთა დაცვის სამსახურს წარედგინა სასამართლოს განჩინებები და, გადაუდებელი აუცილებლობიდან გამომდინარე, პროკურორის დადგენილებები სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით გათვალისწინებული საგამოძიებო მოქმედების, დოკუმენტის ან ინფორმაციის გამოთხოვის შესახებ. საანგარიშო პერიოდში კოდექსის 136-ე მუხლთან დაკავშირებით სამსახურს წარედგინა სასამართლოს 2709 განჩინება, რომელთაგან 99.81% (2704) სრულად დაკმაყოფილდა, 0.04% (1) არ დაკმაყოფილდა, ხოლო 0.15% (4) ნაწილობრივ დაკმაყოფილდა.

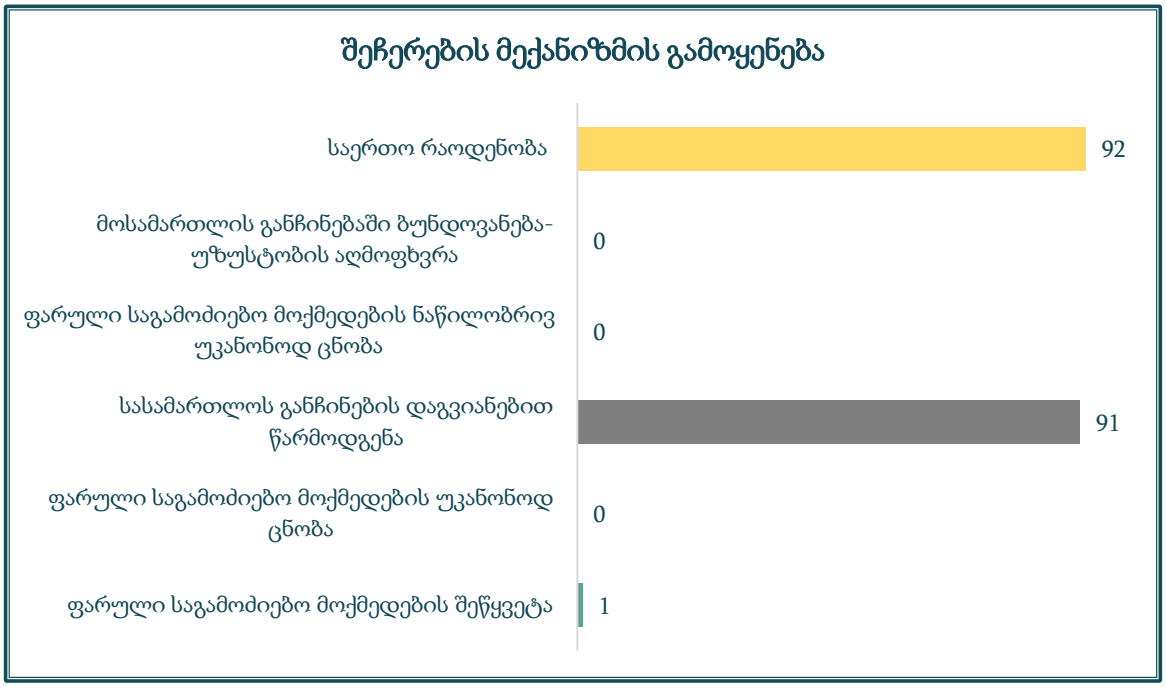
2023 წელს კოდექსის 136-ე მუხლთან დაკავშირებით სამსახურს წარედგინა სასამართლოს 1519 განჩინება, რომელთაგან პროკურორის შუამდგომლობების 99% დაკმაყოფილდა.

დოკუმენტის ან ინფორმაციის წარმოდგენის შესახებ გადაუდებელი აუცილებლობიდან გამომდინარე პროკურორის დადგენილებები

60

2024 წელს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით გათვალისწინებული საგამოძიებო მოქმედების, დოკუმენტის ან ინფორმაციის გამოთხოვის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურს, გადაუდებელი აუცილებლობიდან გამომდინარე, წარედგინა პროკურორის 60 დადგენილება.

2023 წელს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით გათვალისწინებული საგამოძიებო მოქმედების, დოკუმენტის ან ინფორმაციის გამოთხოვის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურს, გადაუდებელი აუცილებლობიდან გამომდინარე, წარედგინა პროკურორის 34 დადგენილება.



2024 წელს სამსახურმა სატელეფონო კომუნიკაციის ფარული მიყურადება-ჩაწერის შეჩერების მექანიზმი (კონტროლის ელექტრონული სისტემის საშუალებით) გამოიყენა 92 შემთხვევაში, რომელთაგან 91 გამოწვეული იყო სასამართლოს განჩინების დაგვიანებით წარმოდგენით, ხოლო 1 - ფარული საგამოძიებო მოქმედების შეწყვეტით.

2023 წელს სამსახურმა სატელეფონო კომუნიკაციის ფარული მიყურადება-ჩაწერის შეჩერების მექანიზმი (კონტროლის ელექტრონული სისტემის საშუალებით) 76 შემთხვევაში გამოიყენა.

სამსახურის მიერ ბუნდოვანება-უზუსტობის შეტყობინების მექანიზმის გამოყენება

9

2024 წელს სასამართლოს მიერ სატელეფონო კომუნიკაციის ფარულ მიყურადება-ჩაწერაზე გაცემულ ნებართვებში არსებულ ბუნდოვანება-უზუსტობაზე (კონტროლის ელექტრონული სისტემის საშუალებით) სსიპ — „საქართველოს ოპერატიულ-ტექნიკურ სააგენტოს“ ეცნობა 9-ჯერ.

2023 წელს სასამართლოს მიერ სატელეფონო კომუნიკაციის ფარულ მიყურადება-ჩაწერაზე გაცემულ ნებართვებში არსებულ ბუნდოვანება-უზუსტობაზე (კონტროლის ელექტრონული სისტემის საშუალებით) სსიპ — „საქართველოს ოპერატიულ-ტექნიკურ სააგენტოს“ ეცნობა 6-ჯერ.

კონტროლის ელექტრონული სისტემის საშუალებით სატელეფონო კომუნიკაციის ფარული მიყურადება-ჩაწერის პროცესში გამოვლენილი ინციდენტების რაოდენობა

1

2024 წელს კონტროლის ელექტრონული სისტემის საშუალებით სატელეფონო კომუნიკაციის ფარული მიყურადება-ჩაწერის პროცესში გამოვლინდა 1 ინციდენტი.

ელექტრონული კომუნიკაციების მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში დაფიქსირებული აქტივობა

89

2024 წელს, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკის კონტროლის ელექტრონული სისტემით სამსახურისთვის მოწოდებული ინფორმაციის საფუძველზე, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკიდან სსიპ — „ოპერატიულ-ტექნიკური სააგენტოს“ მიერ სასამართლოს შესაბამისი გადაწყვეტილებების საფუძველზე მონაცემები გაიცა 89-ჯერ.

2023 წელს, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკის კონტროლის ელექტრონული სისტემით სამსახურისთვის მოწოდებული ინფორმაციის საფუძველზე, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკიდან სსიპ — „ოპერატიულ-ტექნიკური სააგენტოს“ მიერ სასამართლოს შესაბამისი გადაწყვეტილებების საფუძველზე მონაცემები გაიცა 69-ჯერ.

ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობის კონტროლის შედეგად გამოვლენილი ხარვეზი ან ინციდენტი

საანგარიშო პერიოდში ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობის კონტროლის შედეგად რაიმე ხარვეზი ან ინციდენტი არ გამოვლენილა.

ელექტრონული კომუნიკაციების კომპანიების მიერ წარმოდგენილი შეტყობინებები

1965

2024 წელს სამსახურში შეტყობინებები წარმოდგენილ იქნა 13 ელექტრონული კომუნიკაციის კომპანიის მიერ, რომელთაც საანგარიშო პერიოდის განმავლობაში სამართალდამცავი ორგანოების წარმომადგენლებს სასამართლოს 1965 განჩინების საფუძველზე ინფორმაცია გადასცეს.

2023 წელს სამსახურში შეტყობინებები წარმოდგენილ იქნა 11 ელექტრონული კომუნიკაციის კომპანიის მიერ, რომელთაც საანგარიშო პერიოდის განმავლობაში სამართალდამცავი ორგანოების წარმომადგენლებს სასამართლოს 1756 განჩინების საფუძველზე ინფორმაცია გადასცეს.

მოქალაქეების მომართვიანობა მათ მიმართ განხორციელებული ფარული საგამოძიებო მოქმედებების თაობაზე

პერსონალურ მონაცემთა დაცვის სამსახურის მიზანია ადამიანის უფლებათა და თავისუფლებათა, მათ შორის – პირადი ცხოვრების ხელშეუხებლობის დაცვა. შესაბამისად, განსაკუთრებული ყურადღება ეთმობა ისეთი მნიშვნელოვანი სფეროს კონტროლს, როგორიც არის ფარულ საგამოძიებო მოქმედებებზე კონტროლი.

2024 წელს მოქალაქეებს მათ მიმართ განხორციელებული ფარული საგამოძიებო მოქმედებების თაობაზე სამსახურისთვის არ მოუმართავთ.

2023 წლის განმავლობაში პერსონალურ მონაცემთა დაცვის სამსახურს ჯამურად მომართა 4-მა პირმა, რომლებიც სამსახურისგან ითხოვდნენ ინფორმაციას — მიმდინარეობდა თუ არა მათ მიმართ ფარული საგამოძიებო მოქმედებები.

ფარული საგამოძიებო მოქმედების — კავშირგაბმულობის არხებიდან, კომპიუტერული სისტემიდან ინფორმაციის მოხსნისა და ფიქსაციის თაობაზე სასამართლოს განჩინებების რაოდენობა

საანგარიშო პერიოდში სასამართლოს ფარული საგამოძიებო მოქმედების კავშირგაბმულობის არხებიდან, კომპიუტერული სისტემიდან ინფორმაციის მოხსნისა და ფიქსაციის თაობაზე შუამდგომლობა არ განუხილავს.

2023 წელს სასამართლომ განიხილა 3 შუამდგომლობა ფარული საგამოძიებო მოქმედების კავშირგაბმულობის არხებიდან, კომპიუტერული სისტემიდან ინფორმაციის მოხსნისა და ფიქსაციის თაობაზე, რომელთაგან 1 დაკმაყოფილდა, ხოლო 2 არ დაკმაყოფილდა.

სასამართლოს განჩინებები ინტერნეტტრაფიკის მონაცემთა მიმდინარე შეგროვების თაობაზე

საანგარიშო პერიოდში სასამართლოს ინტერნეტტრაფიკის მონაცემთა მიმდინარე შეგროვების თაობაზე შუამდგომლობა არ განუხილავს.

2023 წელს ინტერნეტტრაფიკის მონაცემთა მიმდინარე შეგროვების თაობაზე სასამართლომ განიხილა 1 შუამდგომლობა, რომელიც დაკმაყოფილდა.

ინტერნეტტრაფიკის მონაცემთა მიმდინარე შეგროვების ვადის გაგრძელების თაობაზე სასამართლოს განჩინებების რაოდენობა

2024 წელს ინტერნეტტრაფიკის მონაცემთა მიმდინარე შეგროვების ვადის გაგრძელების თაობაზე სასამართლომ განიხილა 1 შუამდგომლობა, რომელიც დაკმაყოფილდა.

III თავი. საზოგადოების ცნობიერების ამაღლება და საგანმანათლებლო საქმიანობა

1. ცნობიერების ამაღლებაზე ორიენტირებული აქტივობები

თანამედროვე ეპოქაში მონაცემთა დამუშავება ყოველდღიურობის განუყოფელი ნაწილია, ამიტომ პერსონალურ მონაცემთა დაცვამ განსაკუთრებული აქტუალობა შეიძინა. საზოგადოების ინფორმირებულობა და ცნობიერების ამაღლება ამ სფეროში მნიშვნელოვანია, რადგან მონაცემთა ეფექტიანი დაცვა მხოლოდ საკანონმდებლო რეგულაციებით ვერ მიიღწევა – აუცილებელია თითოეული ადამიანის გააზრებული და პასუხისმგებლიანი მიდგომა. შესაბამისად, დიდი მნიშვნელობა აქვს იმ ღონისძიებებსა და აქტივობებს, რომელთაც სამსახური აქტიურად ახორციელებს საზოგადოების ცნობიერების ამაღლების მიმართულებით. ასევე, მნიშვნელოვანია სამსახურის ანგარიშვალდებულება საზოგადოების წინაშე — მიაწოდოს დეტალური ინფორმაცია მონაცემთა დაცვის მდგომარეობისა და განხორციელებული საქმიანობის შესახებ.

პერსონალურ მონაცემთა დაცვის სამსახური საანგარიშო პერიოდში აქტიურად იყენებდა ყველა იმ საკომუნიკაციო არხსა და საშუალებას, რომლებითაც უფრო ეფექტიანად შეძლებდა საზოგადოებისთვის ინფორმაციის მიწოდებას. კერძოდ, 2024 წელსაც აქტიურად გამოიყენებოდა სოციალური ქსელები, ტრადიციული მედია, პირისპირი შეხვედრების ფორმატი, ვიზუალური, ვიდეო- თუ აუდიომასალა. სამსახური მუდმივად მიჰყვება თანამედროვე ტენდენციებსა და საჭიროებებს, შესაბამისად, ცდილობს დანერგოს დაინტერესებულ პირებზე მორგებული სიახლეები. ამ მხრივ, არც გასული წელი იყო გამონაკლისი.

2024 წელი სამსახურისთვის გამორჩეული იყო, რადგან ამოქმედდა საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“. მონაცემთა დამუშავებაზე პასუხისმგებელი პირებისთვის სამსახური აქტიურად მართავდა პირისპირ შეხვედრებს, რომელთა საშუალებითაც სამსახურის თანამშრომლები მონაწილეებს ახალი კანონით გათვალისწინებული სიახლეების შესახებ დეტალურ ინფორმაციას აწვდიდნენ. აქტუალურ საკითხებზე სხვადასხვა საინფორმაციო მასალა მთელი წლის განმავლობაში ონლაინ არხების საშუალებით ვრცელდებოდა. სამსახური შეხვედრების რამდენიმე ფორმატს სთავაზობდა დაინტერესებულ პირებს, მათ შორის – ონლაინ სივრცესაც. აქტიურად ხდებოდა ტრადიციული მედიისა და ონლაინ არხების გამოყენება მონაცემთა სუბიექტებისთვის (მოქალაქეებისთვის) მათ უფლებებთან დაკავშირებით ინფორმაციის მისაწოდებლად.

აქტივობები, რომლებიც სამსახურმა საზოგადოების ცნობიერების ამაღლების მიმართულებით განახორციელა:

- ვიდეომასალა

სამსახურმა 20 პოდკასტი, 9 ვიდეორგოლი, მათგან 1 გრაფიკული ვიდეორგოლი დაამზადა.

— პოდკასტები კანონით გათვალისწინებულ სიახლეებთან დაკავშირებით: სამსახურმა ჯამში 20 პოდკასტი დაამზადა. აღნიშნულ ვიდეოებში სამსახურის თანამშრომლები კანონით გათვალისწინებულ სიახლეებს დეტალურად განმარტავენ. აღსანიშნავია, რომ მათგან 10 პოდკასტი შშმ პირთათვის ხელმისაწვდომი ფორმით (ე. წ. სურდო თარჯიმნით) არის წარმოდგენილი. პოდკასტები სოციალური ქსელების სამ პლატფორმაზე („Facebook“, „YouTube“, „Spotify“) განთავსდა და მნახველთა რაოდენობამ ჯამურად 600 000-ამდე შეადგინა.
— ახალი კანონით გათვალისწინებულ ცვლილებებთან დაკავშირებით სამსახურმა დაამზადა გრაფიკული ვიდეორგოლი, ხოლო მისი მოკლე ვერსია უფასო სოციალური რეკლამის სახით საზოგადოებრივ მაუწყებელსა და აჭარის ტელევიზიის ტელე- და რადიოეთერებში განთავსდა. ვიდეოს ვრცელი ვერსია გამოქვეყნდა სამსახურის ოფიციალურ ვებგვერდსა და სოციალურ ქსელებში. მნახველთა რაოდენობამ 130 000-ამდე შეადგინა.
— კამპანიის — „კონფიდენციალურობა შენი უფლებაა“ — ფარგლებში სამსახურმა 7 ვიდეორგოლი დაამზადა. მათგან 5 ვიდეორგოლის პრეზენტაცია 28 იანვარს, პერსონალურ მონაცემთა დაცვის საერთაშორისო დღეს, შედგა. აღნიშნულ ვიდეორგოლებში ისტორიკოსი - გიორგი კალანდია, ფსიქოლოგი - რამაზ საყვარელიძე, ექიმი - ნუგზარ უბერი, სოციალურ ქსელ „META“-ს პროექტის მენეჯერი - მარიამ შარანგია და ფოტოგრაფი - ანა გოგუაძე პერსონალური მონაცემების დაცვის მნიშვნელობაზე საუბრობდნენ. 2024 წლის მეორე ნახევარში, ეთნიკური უმცირესობებით დასახლებულ რეგიონებში ცნობიერების ამაღლების მიზნით, ამავე კამპანიის ფარგლებში შეიქმნა კიდევ 2 ვიდეორგოლი, რომლებშიც ექიმი - ვარდუჰი მოსოიანი და მწერალი - ქამრან კირიაკოვი სომხურ და აზერბაიჯანულ ენებზე პერსონალურ მონაცემთა დაცვის მნიშვნელობაზე საუბრობენ. ვიდეორგოლები სამსახურის ოფიციალურ ვებგვერდსა და სოციალურ ქსელებში გამოქვეყნდა. აღსანიშნავია, რომ „Facebook“ - ზე მათი ნახვის ჯამურმა რაოდენობამ 1,012,986 შეადგინა.
— საანგარიშო პერიოდში სამსახურისთვის ერთ-ერთ პრიორიტეტს არასრულწლოვნების მონაცემებთან დაკავშირებული საკითხების შესახებ ცნობიერების ამაღლებაც წარმოადგენდა. არასრულწლოვნების უფლებების დაცვის მნიშვნელობის შესახებ წლის განმავლობაში გამოქვეყნდა არაერთი სახელმძღვანელო რეკომენდაცია. ჩატარდა ტრენინგები როგორც მოსწავლეებთან, ასევე – სკოლის წარმომადგენლებსა და პედაგოგებთან. სამსახურის მიერ მომზადდა და სოციალურ ქსელში არასრულწლოვნების მონაწილეობით განთავსდა ვიდეორგოლი, რომელშიც ისინი პერსონალურ მონაცემთა დაცვის საკითხებზე, თავიანთ შეხედულებებსა და ემოციებზე საუბრობენ. აღნიშნული ვიდეო, ერთი მხრივ, ახალგაზრდებს დააფიქრებს საკუთარ უფლებებზე, მეორე მხრივ კი, საზოგადოებას აჩვენებს, თუ

რამდენად სენსიტიური და მნიშვნელოვანია არასრულწლოვნებისთვის პირადი ინფორმაციის დაცვა. ვიდეოს მნახველთა რაოდენობამ სოციალურ ქსელებში 127 000-ამდე შეადგინა.

სკოლის მოსწავლეებისთვის ჩატარდა ესეების კონკურსი, რომელშიც მონაწილეობა საქართველოს სხვადასხვა რეგიონიდან 150-ამდე მოსწავლემ მიიღო. კონკურსის მიზანი სკოლის მოსწავლეებში პერსონალურ მონაცემთა დაცვის მნიშვნელობის შესახებ ცნობიერების ამაღლება იყო.

- **საკომუნიკაციო სტრატეგიის შემუშავება**

სამსახურმა ამერიკის შეერთებული შტატების საერთაშორისო სააგენტოს (USAID) ფინანსური მხარდაჭერით შეიმუშავა გრძელვადიანი საკომუნიკაციო სტრატეგია, რომელიც საკონსულტაციო კომპანია „ჯეპრას“ კონსულტანტების მიერ სამსახურის წარმომადგენლების ჩართულობით მომზადდა.

სტრატეგია გათვლილია სამ წელზე და განსაზღვრავს სამსახურის სტრატეგიული კომუნიკაციის ძირითად საფუძვლებს. მისი მიზანია აამაღლოს პერსონალურ მონაცემთა დაცვის სამსახურის, როგორც პერსონალურ მონაცემთა დამუშავების კანონიერებაზე ზედამხედველი ორგანოს, შესახებ საზოგადოების ცნობადობა, გაზარდოს საზოგადოებაში პერსონალურ მონაცემთა დაცვის საკითხზე ცნობიერება და დაამკვიდროს პერსონალური მონაცემების დაცვისა და პირადი ცხოვრების ხელშეუხებლობის კულტურა.

- **სოციალური მედია**

სოციალურ მედიაარხებსა და სოციალურ ქსელებში სამსახურის მიერ შექმნილ გვერდებზე („Facebook“, „linkedin“, „X“, „YouTube“) მთელი წლის განმავლობაში, შეხვედრებისა და სამსახურის სხვა აქტივობების გარდა, სისტემატურად ქვეყნდებოდა სამსახურის გადაწყვეტილებები, „მსოფლიო პრაქტიკა“, განცხადებები და რელიზები, ხოლო კვარტალურად — სამსახურის მიერ გაწეული საქმიანობის ანგარიშები და სტატისტიკური მონაცემები. ასევე, 2024 წელს ამოქმედდა ორი ახალი რუბრიკა სახელწოდებებით: „DataTech“ ანალიტიკა და „Datanewsroom“. აღნიშნულ რუბრიკებში დაინტერესებულ პირებს შესაძლებლობა აქვთ, გაეცნონ ინფორმაციას მონაცემთა დაცვის სფეროში მსოფლიოში მიმდინარე მნიშვნელოვანი სიახლეების შესახებ, ასევე – აპლიკაციებისა და სხვადასხვა სოციალური ქსელის მიერ მონაცემთა დამუშავების პოლიტიკას.

მზარდია სამსახურის ოფიციალური გვერდის გამომწერების რაოდენობა, რომელიც 2024 წლის დეკემბრის მონაცემებით **23,500** შეადგენს.

სოციალურ ქსელ „Facebook“-ში სამსახურის მიერ ჯამურად **303** პოსტი განთავსდა. აღნიშნულ პოსტებზე მომხმარებლების წვდომის რაოდენობა **1,645,230**-ია, გვერდის ვიზიტორების რაოდენობა კი — **351,085**.

- **„WhatsApp“ არხი**

2024 წლის ივლისიდან პერსონალურ მონაცემთა დაცვის სამსახურმა უწყების საქმიანობის შესახებ მიმდინარე საინტერესო ტენდენციების გაზიარება „WhatsApp“ -ის არხის საშუალებითაც დაიწყო.

- **სამსახურის ახალი ვებგვერდი**

2024 წლის 1-ელი მარტიდან ფუნქციონირება დაიწყო სამსახურის ახალმა ვებგვერდმა (www.pdps.ge). ვებგვერდი სრულად მოერგო ახალი კანონით გათვალისწინებულ საჭიროებებს და მომხმარებლებისთვის მეტად ხელმისაწვდომი გახადა პერსონალურ მონაცემთა დაცვის საკითხებთან დაკავშირებული ინფორმაციის მიღება.

კანონის მოთხოვნებიდან გამომდინარე, ახალ ვებგვერდში ინტეგრირებულია სამსახურისთვის ინციდენტის შესახებ ინფორმაციის შეტყობინებისა და პერსონალურ მონაცემთა დაცვის ოფიცრის განსაზღვრის/დანიშვნის შესახებ სამსახურის ინფორმირების ფუნქციები.

საანგარიშო პერიოდში სამსახურის ძველი და ახალი ვებგვერდების ვიზიტორების რაოდენობამ შეადგინა 167,994.

- **მედიასთან ურთიერთობა**

2024 წელი განსაკუთრებით აქტიური იყო სამსხურის მედიასთან ურთიერთობის თვალსაზრისით. „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის მიღებამ მედიის ინტერესი სამსახურის მიმართ საგრძნობლად გაზარდა.

სამსახური მთელი წლის განმავლობაში აქტიურად თანამშრომლობდა მედიასთან (ტელევიზიებთან, რადიოებთან, პრესასთან, ონლაინ საინფორმაციო სააგენტოებთან) ახალი კანონით გათვალისწინებული სიახლეების გაცნობის, ასევე, ზოგადად, სამსახურის საქმიანობის შესახებ და პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე საზოგადოების ცნობიერების ამაღლების მიზნით.

აღსანიშნავია, რომ საზოგადოების ინფორმირება, გამჭვირვალობა და მათთან ანგარიშვალდებულება სამსახურის ერთ-ერთი უმთავრესი პრიორიტეტია. ამ მიზნით სამსახურის მიერ ორგანიზებულ ყველა მნიშვნელოვან ღონისძიებაზე მოწვეულნი იყვნენ მედიის წარმომადგენლები.

პროაქტიულად ქვეყნდებოდა ინფორმაცია მაღალი საჯარო ინტერესის საქმეების, სამსახურის საქმიანობის, სხვადასხვა აქტივობისა და პრეცედენტული გადაწყვეტილების შესახებ.

2024 წელს მედიასაშუალებებსა და საინფორმაციო სააგენტოებში გაიგზავნა **30** პრესრელიზი. სატელევიზიო საინფორმაციო, დილისა და შუადღის ეთერებში, ასევე – რადიოსა და თემატურ გადაცემებში (ბიზნესი, ეკონომიკა, მედიცინა და ა. შ.) სამსახურის წარმომადგენლებმა მონაწილეობა მიიღეს **25** გადაცემაში.

გამოქვეყნდა ინტერვიუები ონლაინ მედიაში. ჟურნალისტებისთვის საინტერესო საკითხებზე გაკეთდა არაერთი კომენტარი.

- **სახელმძღვანელო რეკომენდაციები**

საანგარიშო პერიოდში სამსახურის მიერ მომზადდა, ასევე, ითარგმნა და გამოქვეყნდა 2024 წლის პირველი მარტიდან მოქმედი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან დაკავშირებული **28** სახელმძღვანელო რეკომენდაცია:

1. რეკომენდაციები ინციდენტთან დაკავშირებული ღონისძიებების განხორციელების თაობაზე;
2. რეკომენდაციები პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ;
3. რეკომენდაცია მონაცემთა გადატანის უფლების შესახებ;
4. სახელმძღვანელო რეკომენდაცია გამჭვირვალობის პრინციპის შესახებ;
5. სახელმძღვანელო რეკომენდაცია 05/2020 თანხმობის შესახებ;
6. სახელმძღვანელო რეკომენდაცია 2/2019 GDPR-ის 6(1)(ხ) მუხლის თანახმად, მონაცემთა სუბიექტებისათვის ონლაინ სერვისების მიწოდების კონტექსტში პერსონალური მონაცემების დამუშავების შესახებ;
7. სახელმძღვანელო რეკომენდაცია მონაცემთა პორტირების უფლების შესახებ;
8. სახელმძღვანელო რეკომენდაცია 4/2019 25-ე მუხლის შესახებ მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას;
9. რეკომენდაციები პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ;
10. სახელმძღვანელო რეკომენდაცია ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებისა და პროფაილინგის შესახებ, 2016/679 რეგულაციის მიზნებისთვის;
11. სახელმძღვანელო რეკომენდაცია 3/2019 პერსონალური მონაცემების ვიდეომოწყობილობებით დამუშავების შესახებ;
12. რეკომენდაციები ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებასთან დაკავშირებული უფლებებისა და პროფაილინგის შესახებ;
13. რეკომენდაციები არასრულწლოვნების პერსონალური მონაცემების დამუშავების შესახებ;
14. სახელმძღვანელო პრინციპები 8/2020 სოციალური მედიის მომხმარებელთა მიზნობრივი შერჩევის (პირთა სასურველი წრისთვის ინფორმაციის შეთავაზების) შესახებ;
15. რეკომენდაციები ვიდეომონიტორინგის და აუდიომონიტორინგის განხორციელების თაობაზე;
16. სახელმძღვანელო პრინციპები 02/2021 ვირტუალური ხმოვანი ასისტენტების შესახებ;

17. სახელმძღვანელო პრინციპები 04/2022 მონაცემთა დაცვის ძირითადი რეგულაციის მიხედვით ადმინისტრაციული ჯარიმის გამოანგარიშების წესის შესახებ;
18. რეკომენდაციები მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) შესახებ;
19. მინიმალური სტანდარტი პერსონალურ მონაცემთა დაცვის ოფიცრებისთვის;
20. მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დაცვის საზედამხედველო ორგანოს მოთხოვნის შეუსრულებლობა (შედარებითსამართლებრივი მიმოხილვა);
21. რეკომენდაციები დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებული ხელშეკრულების არსებითი და სტანდარტული პირობების შესახებ;
22. რა უნდა ვიცოდეთ ბიომეტრიული მონაცემების დამუშავების შესახებ;
23. რეალურ დროში განხორციელებული ვიდეომონიტორინგი საბავშვო ბაღებში;
24. სახელმძღვანელო რეკომენდაციები მცირე და საშუალო ზომის მეწარმე სუბიექტებისათვის;
25. შეზღუდული შესაძლებლობების მქონე (შშმ) პირთა პერსონალური მონაცემების დაცვა (თეორია და პრაქტიკა);
26. საინფორმაციო ბიულეტენი: „ამომრჩევლის უფლებები და საარჩევნო პროცესში პერსონალური მონაცემების დაცვის ცალკეული ასპექტები“;
27. სახელმძღვანელო მითითებები ინსპექტირების ტექნიკისა და მეთოდების შესახებ;
28. სახელმძღვანელო დოკუმენტი ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის მიზნით პერსონალურ მონაცემთა დამუშავების შესახებ.

2. ჩატარებული ტრენინგები და საჯარო ლექციები

2024 წლის პირველი იანვრიდან 31 დეკემბრის ჩათვლით სამსახური აქტიურად მართავდა ცნობიერების ამაღლების მიმართულებით საინფორმაციო კამპანიებს, მათ შორის – ლექცია/ტრენინგების სახით.

სამსახურმა გამართა 108 შეხვედრა, რომელთა ფარგლებშიც 6522 პირი გადამზადდა.

შეხვედრები მოიცავდა როგორც კონკრეტული უწყებებისა და ორგანიზაციებისთვის გამართულ ლექციებს, ასევე – ონლაინ და პირისპირ შეხვედრებს კანონში შესულ ცვლილებებთან დაკავშირებით, პერსონალურ მონაცემთა დაცვის ოფიცერთა გადამზადების კურსებსა და რეგიონულ შეხვედრებს.

ამავდროულად, აქტიურად მიმდინარეობდა შეხვედრები როგორც საჯარო, ისე – კერძო სექტორთან, საგანმანათლებლო დაწესებულებებთან და სხვა.

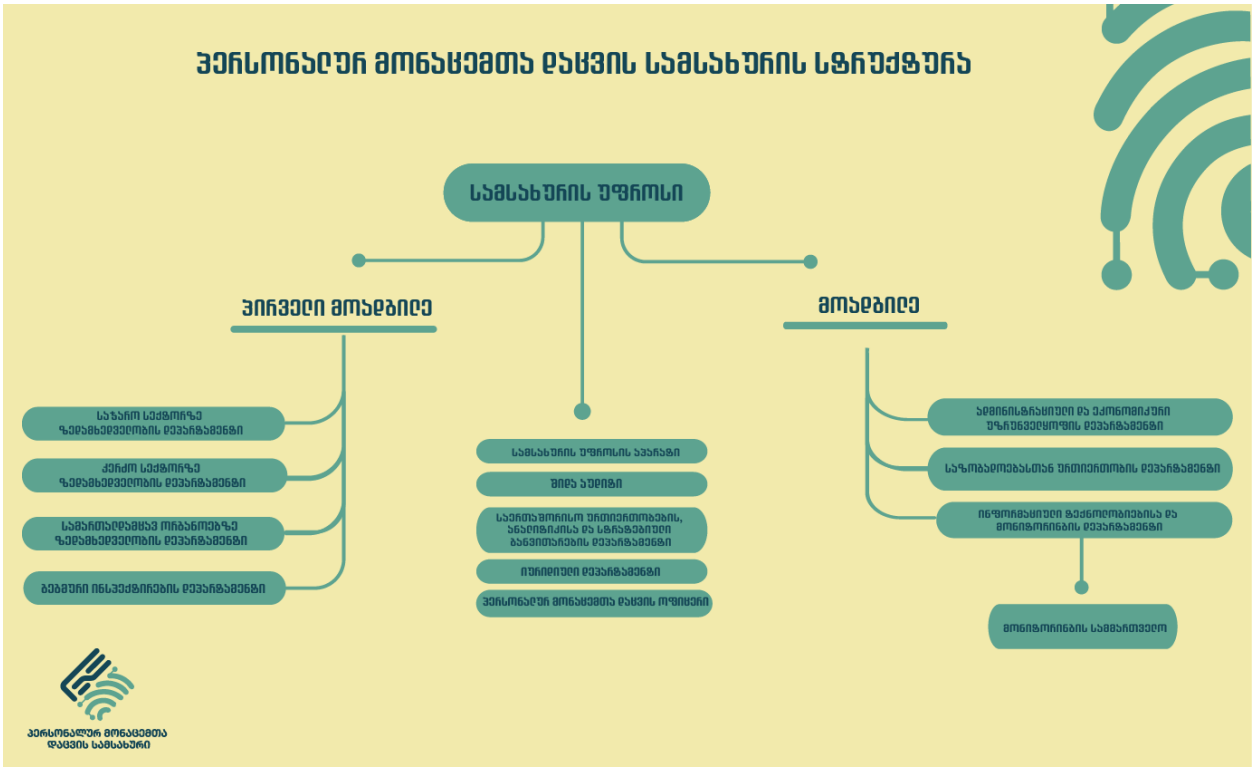
საანგარიშო პერიოდში კანონით გათვალისწინებული სიახლეების შესახებ დაინტერესებულ პირებთან გაიმართა საკონსულტაციო შეხვედრები, რომელთა ჯამური რაოდენობაა 260.

IV თავი. სამსახურის ადმინისტრაციული მართვა

1. სამსახურის ორგანიზაციული მართვის საკითხები

1.1. ინსტიტუციური გაძლიერება და სამსახურის შიდაორგანიზაციული სტრუქტურა

პერსონალურ მონაცემთა დაცვის სამსახურის გაძლიერებისა და მისი სტრატეგიული ამოცანების შესრულებისთვის, მათ შორის სტრუქტურული ერთეულების დაკომპლექტებისა და 2024 წლის პირველი მარტიდან მოქმედი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით მინიჭებული უფლებამოსილების სრულფასოვნად და შეუფერხებლად განხორციელების ხელშეწყობის მიზნით, 2024 წლის პირველი იანვრიდან სამსახურის საშტატო რიცხოვნობა გაიზარდა 17 (ჩვიდმეტი) ერთეულით და ჯამურად შეადგენს 84 (ოთხმოცდაოთხ) საშტატო ერთეულს.



— სტაჟირების პროგრამა

საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის სამსახურში აქტიურად მიმდინარეობდა სტაჟირების პროგრამა, რომლის მიზანია შესაბამისი პროფილის უმაღლესი საგანმანათლებლო დაწესებულებების სტუდენტებისა და კურსდამთავრებულების კვალიფიკაციის ამაღლება და პროფესიული განვითარების ხელშეწყობა. ამასთან, სტაჟირების პროცესში სტუდენტებს პროფესიული გამოცდილების შეძენის შესაძლებლობა მიეცათ, რომლის საშუალებითაც მათ აიმაღლეს კვალიფიკაცია და გამოუმუშავდათ სხვა პრაქტიკული უნარ-ჩვევები. აღსანიშნავია, რომ სამსახურში 5 (ხუთმა) სტუდენტმა გაიარა სტაჟირება.

2024 წლის 29 დეკემბრის მდგომარეობით პერსონალურ მონაცემთა დაცვის სამსახურში დასაქმებულ პირთა ოდენობა კატეგორიების მითითებით, მათ შორის – გენდერული თვალსაზრისით:

N	თანამშრომლების შესახებ ინფორმაცია	რაოდენობა	რაოდენობა - ქალი	რაოდენობა - კაცი	ქალი - %	კაცი - %
1	მოქმედი თანამშრომლების სრული რაოდენობა	95	46	49	48%	52%
2	თანამდებობის პირი	3	1	2	33%	67%
3	ხელმძღვანელ თანამდებობაზე დანიშნული პროფესიული საჯარო მოხელე	20	12	8	60%	40%
4	არახელმძღვანელ თანამდებობაზე დანიშნული პროფესიული საჯარო მოხელე	51	28	23	55%	45%
5	შრომითი ხელშეკრულებით დასაქმებული პირი	21	5	16	24%	76%

1.2. თანამშრომელთა კვალიფიკაციის ამაღლება და ორგანიზაციული ეთიკა

2024 წელი მნიშვნელოვანი იყო თანამშრომელთა პროფესიული განვითარებისა და კვალიფიკაციის ამაღლების მიმართულებით. საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომლებმა მონაწილეობა მიიღეს კვალიფიკაციის ამაღლების ღონისძიებებში და გადამზადნენ სხვადასხვა დისციპლინაში, კერძოდ, 18 შეხვედრის ფარგლებში სამსახურის 95 თანამშრომელი გადამზადდა სხვადასხვა დისციპლინაში, მათ შორის, შემდეგ თემებზე: დროის მართვა, სექსუალური შევიწროების პრევენცია და მასზე რეაგირების მექანიზმი, მოქმედებები და უსაფრთხო ქცევის წესები საგანგებო სიტუაციის დროს, პირველადი სამედიცინო დახმარება, მოხელის პიროვნული და პროფესიული კომპეტენციების განვითარება და სხვა.

ევროკავშირის პროექტის — „უსაფრთხოების სექტორზე ზედამხედველობის მხარდაჭერა საქართველოში“ ფარგლებში, სამსახურის თანაორგანიზებით, თანამშრომლებისთვის გაიმართა ტრენინგი პერსონალურ მონაცემთა დაცვის აქტუალურ საკითხებსა და 2024 წლის მარტიდან მოქმედი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ევროპული სტანდარტების შესაბამისად იმპლემენტაციის თემატიკაზე. ტრენინგი ჩატარდა ევროკავშირის ექსპერტის — ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ხელმძღვანელის — ეკატერინე მაცუკას ხელმძღვანელობით. ასევე, გაიმართა სამუშაო ონლაინ შეხვედრა ხორვატიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს წარმომადგენლებთან, რომელიც დაეთმო „მონაცემთა დაცვის სტანდარტული მოდელის გამოყენებით ინსპექტირების ჩატარებასა“ და „მონაცემთა დაცვის ზეგავლენის შეფასებას“.

განხორციელდა კვალიფიკაციის ამაღლების შიდა კამპანია „თანამშრომლები თანამშრომლებისთვის“, რომლის ფარგლებშიც სამსახურის თანამშრომლები მართავდნენ ლექცია-ტრენინგებს სხვა დაინტერესებული თანამშრომლებისთვის. ამავე კამპანიის ფარგლებში, ორგანიზაციასთან ადაპტაციის პროცესის გამარტივების მიზნით, აქტიურად მიმდინარეობდა საინფორმაციო ხასიათის ტრენინგები ახალი თანამშრომლებისთვის. სამსახურის თანამშრომლებმა ასევე მიიღეს მონაწილეობა შეზღუდული შესაძლებლობების მქონე პირთა უფლებებსა და მათთან კომუნიკაციის სტანდარტების თემატიკაზე გამართულ ტრენინგებში.

საანგარიშო პერიოდში სამსახურში გამოცხადდა 37 (ოცდაჩვიდმეტი) კონკურსი, რომელთა ფარგლებშიც დასაქმდა 28 (ოცდარვა) კანდიდატი. კანონმდებლობის შესაბამისად, 2024 წლის საქმიანობის შეფასების გათვალისწინებით, სამსახურის 12 (თორმეტ) თანამშრომელს მიენიჭა/გაეზარდა მოხელის კლასი. ამასთან, პერსონალურ მონაცემთა დაცვის სამსახურის 35 (ოცდათხუთმეტ) თანამშრომელს პერსონალურ მონაცემთა დაცვის სამსახურის შესაბამისი სახელმწიფო სპეციალური წოდება მიენიჭა.

2. პერსონალურ მონაცემთა დაცვის სამსახურის ბიუჯეტი და მისი შესრულება

2.1. სამსახურის ბიუჯეტი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 46-ე მუხლის მიხედვით, სამსახურის საქმიანობა ფინანსდება საქართველოს სახელმწიფო ბიუჯეტიდან და საჭირო ასიგნებები განისაზღვრება ცალკე კოდით. 2024 წელს დამტკიცებული ბიუჯეტი შეადგენდა 8 000 000 ლარს. 2024 წლის 1 იანვრის მდგომარეობით, სამსახურს განესაზღვრა 84 (ოთხმოცდაოთხი) საშტატო ერთეული და ტოლფას თანამდებობაზე 65 (სამოცდახუთი) საჯარო მოხელე დაინიშნა. სამსახურის სტრუქტურისა და საშტატო ნუსხის შესაბამისად, სამსახურის ორგანიზაციულ სტრუქტურაში შედის 9 (ცხრა) დეპარტამენტი და სამსახურის უფროსის აპარატი.

საანგარიშო პერიოდში ბიუჯეტის საკასო შესრულებამ 7 303 385.95 ლარი შეადგინა. აღსანიშნავია, რომ საკასო შესრულების % წლიურ გეგმასთან მიმართებით შეადგენს 91,29 %-ს.

№	საბიუჯეტო კლასიფიკაციის მუხლი	დაზუსტებული გეგმა	საკასო შესრულება
1	შრომის ანაზღაურება	4 877 000	4 630 467
2	საქონელი და მომსახურება	1 980 000	1 675 452
3	გრანტები	6 000	5 680
4	სოციალური უზრუნველყოფა	100 000	86 007
5	სხვა ხარჯები	135 000	108 372
6	არაფინანსური აქტივები	902 000	797 409
	ჯამი	8 000 000	7 303 386

2.2. გაცემული სარგო, დანამატები და ფულადი ჯილდოები

საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომლებზე (მათ შორის სამსახურის უფროსსა და სამსახურის უფროსის მოადგილეებზე) გაიცა თანამდებობრივი სარგო 3 698 300,18 ლარის ოდენობით, ხოლო წოდებრივი სარგო – 11 616,91 ლარის ოდენობით.

საანგარიშო პერიოდში სამსახურის თანამშრომლებზე დანამატის სახით გაიცა 680 748,87 ლარი, მათ შორის 147 025,75 ლარი – სპეციალური წოდების მქონე თანამშრომელზე „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული სავალდებულო დანამატის ფარგლებში; 33 647,12 ლარი – „საჯარო სამსახურის შესახებ“ საქართველოს კანონის 26-ე მუხლის მე-4 პუნქტით გათვალისწინებული სავალდებულო დანამატის ფარგლებში; ხოლო 500 076,00 ლარი – დამატებითი ფუნქციებისა და ზეგანაკვეთური მუშაობისთვის. 2024 წელს სამსახურის თანამშრომლებზე გაიცა ჯილდო 239 800,80 ლარის ოდენობით.

შრომითი ხელშეკრულებით დასაქმებულ პირთა საშუალო წლიური რაოდენობის (22 (ოცდაორი) თანამშრომლის) შრომის ანაზღაურების ჯამურმა ოდენობამ 592 068,00 ლარი შეადგინა.

2.3. სატრანსპორტო საშუალებები

პერსონალურ მონაცემთა დაცვის სამსახურის ბალანსზე 2024 წლის 1-ელი იანვრის მდგომარეობით ირიცხებოდა 10 (ათი) ერთეული ავტოსატრანსპორტო საშუალება, რომელთა ტექნიკურ მომსახურებაზე გაწეულმა ფაქტობრივმა ხარჯმა შეადგინა 12 197,27 ლარი, ხოლო საწვავის ხარჯმა – 41 670,42 ლარი.

2.4. სამსახურის ბალანსზე რიცხული უძრავი ქონება

№	უძრავი ქონების დასახელება, მისამართი	უფლების სახე	მიზანი
1.	ქ. თბილისი, ნ. ვაჩნაძის ქ. №7	სახელმწიფო საკუთრება, სარგებლობის უფლებით	ადმინისტრაციული შენობა, სადაც განთავსებულია სამსახურის 5 დეპარტამენტი და სამსახურის აპარატი (სტრუქტურული ერთეული)
2.	ქ. ბათუმი, ბაქოს ქ. №48	აჭარის ა/რ საკუთრება. სარგებლობის უფლებით მოთხოვნამდე	ადმინისტრაციული შენობა, სადაც განთავსებულია დასავლეთის წარმომადგენლობა

თანამშრომელთა შესაბამისი სამუშაო სივრცით უზრუნველყოფის მიზნით, სამსახურის 4 (ოთხი) სტრუქტურული ერთეული განთავსდა იჯარით აღებულ კერძო საკუთრებაში, რომლის 2024 წლის იჯარის ხარჯმა შეადგინა 160 992,93 ლარი. 2024 წლის მდგომარეობით სამსახურის ბალანსზე ირიცხებოდა 2 (ორი) უძრავი ქონება, რომლებიც განთავსებულია შემდეგ მისამართებზე: ნ. ვაჩნაძის №7, ქ. თბილისი; ბაქოს ქ. №48, ქ. ბათუმი.

სსიპ — „სახელმწიფო ქონების ეროვნულმა სააგენტომ“ 2022 წლის 20 ივლისის №5/40800 წერილის საფუძველზე პერსონალურ მონაცემთა დაცვის სამსახურს სარგებლობის უფლებით უვადოდ გადასცა ქ. თბილისში, პუშკინის ქ. №10/ნ. ვაჩნაძის ქ. №7/თაბუკაშვილის ქ. №2 მდებარე უძრავი ქონება (მიწის (უძრავი ქონების) საკადასტრო კოდი: 01.15.04.022.003,01.511), რომელიც სსიპ — „საჯარო რეესტრის ეროვნული სააგენტოს“ მიერ 2022 წლის 24 აგვისტოს დარეგისტრირებული იქნა პერსონალურ მონაცემთა დაცვის სამსახურის სახელზე (ფართი შეადგენს 162,39 კვმ.). გაზრდილი ფუნქცია-მოვალეობების განხორციელების მიზნით, საოფისე, სატრენინგო და საკონფერენციო სივრცეების მოსაწყობად, მითითებულ ფართში და შენობის პირველ სართულზე, ქ. თბილისის მერიის თანხმობის საფუძველზე (მითითებული ფართი წარმოადგენს კულტურული მემკვიდრეობის ძეგლის სტატუსის მქონე შენობის ნაწილს) სამსახურმა ჩაატარა სარემონტო სამუშაოები, რომლის ჯამურმა ღირებულებამ შეადგინა 373 170 ლარი, ხოლო ფართის გაფორმებისა და საოფისე ავეჯითა და ინვენტარით მოწყობის ჯამურმა ღირებულებამ შეადგინა 39 914 ლარი.

აღსანიშნავია, რომ მოწყობილ ფართში სამსახური აქტიურად ახორციელებს სატრენინგო და საკონსულტაციო საქმიანობას, რომელიც მნიშვნელოვნად ამცირებს საბიუჯეტო ხარჯებს.

2.5. მივლინებები და სხვა ხარჯები

საანგარიშო პერიოდში მივლინების ხარჯმა ქვეყნის შიგნით შეადგინა 26 965,00 ლარი, ხოლო ქვეყნის გარეთ – 175 861,73 ლარი. საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის სამსახურის სატელეკომუნიკაციო ხარჯებმა შეადგინა 14 937,94 ლარი. ასევე, 2024 წელს სამსახურის მიერ რეკლამის განთავსების ხარჯმა შეადგინა 20 486,08 ლარი. აღსანიშნავია, რომ რეკლამას ექვემდებარებოდა მხოლოდ საზოგადოების ცნობიერების ამაღლებისაკენ მიმართული ღონისძიებები.

დანართი №1. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისობის საკითხი ევროკავშირის პერსონალურ მონაცემთა დაცვის სამართალთან

2023 წელს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის[30] მიღებისა და მისი 2024 წლის 1-ელი მარტიდან ამოქმედების შედეგად, პერსონალურ მონაცემთა დაცვის მომწესრიგებელი ეროვნული კანონმდებლობა მნიშვნელოვნად დაუახლოვდა ევროპულ სტანდარტებს. აღსანიშნავია, რომ ახალი კანონის იმპლემენტაციის შედეგების შესახებ პერსონალურ მონაცემთა დაცვის სამსახურმა გამოაქვეყნა სპეციალური ანგარიში, რომელიც ასახავს კანონით გათვალისწინებული ახალი სამართლებრივი ინსტიტუტების მოქმედებას პრაქტიკაში, კანონის იმპლემენტაციის პროცესში გამოვლენილი სირთულეებსა და სამსახურის მიერ განხორციელებულ აქტივობებს.[31] ახალი კანონი სრულად იზიარებს ევროკავშირის პერსონალურ მონაცემთა დაცვის კანონმდებლობის — „მონაცემთა დაცვის ძირითადი რეგულაციითა“[32] და „კომპეტენტური ორგანოების მიერ დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, ან სასჯელთა აღსრულების მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის, მონაცემთა თავისუფალი მიმოცვლისა და საბჭოს 2008/977/JHA ჩარჩო გადაწყვეტილების გაუქმების შესახებ“,[33] ევროკავშირის დირექტივით გათვალისწინებულ პრინციპებსა და სამართლებრივ ინსტიტუტებს. ამასთან, აღსანიშნავია დარგის საერთაშორისო ექსპერტის დადებითი შეფასება 2024 წლის პირველი მარტიდან მოქმედი კანონის ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციასთან“ შესაბამისობის საკითხზე: *„საქართველოს ახალი კანონი „პერსონალურ მონაცემების დაცვის შესახებ“ ცხადყოფს, რომ კანონმდებელმა ინტენსიურად იფიქრა და ყურადღებით გააანალიზა ევროკავშირის მონაცემთა დაცვის კანონმდებლობა, რისთვისაც იმსახურებს გულწრფელ მილოცვას! საქართველომ*

[30] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 3144-XIმს-Xმპ, 03/07/2023.

[31] პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის სპეციალური ანგარიში „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის იმპლემენტაცია, 2025.

[32] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (შემდგომში — „რეგულაცია“ ან “GDPR”).

[33] 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 (შემდგომში — „საპოლიციო დირექტივა“).

ახალი კანონის მეშვეობით უკვე დიდწილად შეუსაბამა მონაცემთა დაცვის ეროვნული კანონი "GDPR"-ის სტანდარტებს."[34]

საგულისხმოა, რომ პერსონალურ მონაცემთა დაცვის სამართლის საუკეთესო ევროპული პრაქტიკისა და სტანდარტის დანერგვის მიზნით, სამსახურმა არაერთი აქტივობა განახორციელა, მათ შორის ევროპული ღირებულებების მხარდაჭერისა და პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების დამკვიდრების მიმართულებით.[35]

წინამდებარე თავი შედარებითსამართლებრივ ჭრილში მოკლედ მიმოიხილავს კანონის მიმართებას ზემოაღნიშნულ სამართლებრივ ინსტრუმენტებთან.

1. ზოგადი დებულებები

„პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მიზანია პერსონალური მონაცემების დამუშავებისას ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის – პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების, დაცვა. ევროკავშირის რეგულაცია იცავს ფიზიკური პირის ფუნდამენტურ უფლებებსა და თავისუფლებებს, კერძოდ, პერსონალურ მონაცემთა დაცვის უფლებას. "GDPR"-ის მიზანია მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვა და მონაცემთა თავისუფალ მიმოქცევასთან დაკავშირებული წესების განსაზღვრა. მისი პირველი მუხლის მე-3 პუნქტი იმპერატიულად ადგენს ევროკავშირის მასშტაბით პერსონალური მონაცემის მიმოცვლის შეზღუდვის აკრძალვას იმ მიზეზების საფუძველზე, რომლებიც შესაძლოა უკავშირდებოდეს პერსონალური მონაცემების დამუშავებისას ფიზიკური პირის დაცვას. რაც შეეხება საპოლიციო დირექტივას, იგი ადგენს მინიმალურ სტანდარტს კომპეტენტური ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, სასჯელთა აღსრულების, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვის მიზნებისათვის პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის მიზნით. დირექტივა განსაზღვრავს ფიზიკურ პირთა უფლებებისა და თავისუფლებების დაცვის, პერსონალურ მონაცემთა დაცვის ვალდებულებას.

[34] *გერნსდორფი ნ.,* „პერსონალურ მონაცემთა დაცვის შესახებ" ახალი კანონი საქართველოში - მოკლე მიმოხილვა, პერსონალურ მონაცემთა დაცვი სამართლის ჟურნალი, №1, 2024, 128.

[35] პერსონალურ მონაცემთა დაცვის სამსახურის სპეციალური ანგარიში პერსონალურ მონაცემთა დაცვის სამართლის საუკეთესო ევროპული პრაქტიკისა და სტანდარტის დანერგვის მიზნით 2022-2024 წლებში სამსახურის მიერ განხორციელებული საერთაშორისო აქტივობების შესახებ, 2024.

— მოქმედების სფერო

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი მოქმედებს საქართველოს ტერიტორიაზე ავტომატური და ნახევრად ავტომატური საშუალებით მონაცემთა დამუშავებაზე; ასევე – არაავტომატური საშუალებებით დამუშავებისას, თუკი მონაცემები არის ან გახდება ფაილური სისტემის ნაწილი; აგრეთვე, არარეზიდენტი სუბიექტების მიერ მონაცემთა საქართველოში არსებული ტექნიკური საშუალებებით დამუშავებაზე, თუმცა ამგვარი საშუალება არ უნდა გამოიყენებოდეს მონაცემთა ტრანზიტისათვის. კანონის მოქმედება ასევე არ ვრცელდება: პირადი მიზნით ან ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავებაზე; მასობრივი ინფორმაციის საშუალებების მიერ საზოგადოების ინფორმირების მიზნით დამუშავებაზე, თუმცა ამ უკანასკნელ შემთხვევაში ვრცელდება კანონით გათვალისწინებული მოთხოვნები მონაცემთა უსაფრთხოების უზრუნველსაყოფად; აკადემიური, სახელოვნო და ლიტერატურული მიზნით დამუშავების პროცესებზე. აგრეთვე, კანონის მოქმედება არ ვრცელდება სახელმწიფო და ეკონომიკური უსაფრთხოების, თავდაცვის, სადაზვერვო და კონტრდაზვერვითი საქმიანობის ფარგლებში მონაცემთა დამუშავებაზე; ასევე, დანაშაულის თავიდან აცილების, გამოძიების, სისხლის-სამართლებრივი დევნის, ოპერატიულ-სამძებრო ღონისძიებებისა და მართლწესრიგის დაცვის მიზნებისათვის სახელმწიფოს საიდუმლოებისთვის მიკუთვნებულ მონაცემთა ნახევრად ავტომატურ და არაავტომატურ დამუშავებაზე; სასამართლოში სამართალწარმოების მიზნით მონაცემთა დამუშავებაზე. რაც შეეხება „ოფიციალური სტატისტიკის შესახებ“ საქართველოს კანონით გათვალისწინებული მოსახლეობის აღწერას, ამ უკანასკნელზე არ ვრცელდება მხოლოდ განსაკუთრებული კატეგორიის მონაცემების დამუშავების საფუძველთა მომწესრიგებელი ნორმა[36]. საგულისხმოა, რომ კანონი ექსპლიციტურად ადგენს კეთილსინდისიერების ვალდებულებას ისეთ შემთხვევაში, როდესაც პირი უნებლიეთ გახდება მონაცემთა მიმღები. კანონი კრძალავს პერსონალურ მონაცემზე წვდომის ბოროტად გამოყენებას და შემდგომ უკანონო დამუშავებას.

ევროკავშირის რეგულაცია მოქმედებს ავტომატური და ნახევრად ავტომატური საშუალებით მონაცემთა დამუშავებაზე, ასევე – არაავტომატური საშუალებებით დამუშავებისას, თუკი მონაცემები არის ან გახდება ფაილური სისტემის ნაწილი. იგი ვრცელდება კერძო და საჯარო სექტორში მონაცემთა დამუშავების პროცესებზე. მაგრამ არ ვრცელდება ევროკავშირის ინსტიტუტების, ორგანოების მიერ მონაცემთა დამუშავებაზე, ასევე, ისეთ საქმიანობაზე, რომელიც სცილდება ევროკავშირის სამართლის ფარგლებს; არ ვრცელდება ფიზიკური პირის მიერ პირადი ან ოჯახური საქმიანობის ფარგლებში დამუშავების პროცესებზე.

[36] იხ. კანონის მე-6 მუხლი.

“GDPR”-ის მოქმედება ვრცელდება იმ დამუშავებისთვის პასუხისმგებელი ან უფლებამოსილი პირის მიერ მონაცემთა დამუშავებაზე, რომელიც არ არის დაფუძნებული ევროკავშირის ტერიტორიაზე, თუმცა სთავაზობენ საქონელს ან მომსახურებას ევროკავშირის ტერიტორიაზე მყოფ მონაცემთა სუბიექტებს.[37]

საპოლიციო დირექტივა მოქმედებს კომპეტენტური ორგანოების მიერ მონაცემთა დამუშავების პროცესებზე. იგი ვრცელდება მონაცემთა ავტომატური, ნახევრად ავტომატური და ისეთი არაავტომატური საშუალებებით დამუშავებაზე, რომელთა შედეგად დამუშავებული მონაცემი ფაილური სისტემის ნაწილია ან გამიზნულია, რომ იქცეს ფაილური სისტემის ნაწილად. შესაბამისად, მისი მოქმედება არ ვრცელდება ფაილებზე ან მათ წყებაზე/გარეკანზე, თუკი იგი არ არის სტრუქტურირებული კონკრეტული კრიტერიუმის გათვალისწინებით. დირექტივა არ მოქმედებს ევროკავშირის კანონმდებლობის იურისდიქციის ფარგლებში მონაცემთა დამუშავებასა და ევროკავშირის სხვადასხვა ინსტიტუტის/ორგანოს მიერ დამუშავებაზე.[38]

საქართველოსა და ევროკავშირის სამართლით გათვალიწინებული გამონაკლისების შედარებითსამართლებრივი ანალიზის საფუძველზე აღსანიშნავია, რომ “GDPR”-ი განსაზღვრავს პირადი მიზნისა და ოჯახური საქმიანობის გამონაკლისს. სახელმწიფო და ეკონომიკური უსაფრთხოების, თავდაცვის, სადაზვერვო და კონტრდაზვერვითი საქმიანობის გამონაკლისთან მიმართებით აღსანიშნავია, რომ საპოლიციო დირექტივის იურისდიქციაში არ ექცევა ეროვნულ უსაფრთხოებასთან დაკავშირებული საქმიანობა, ეროვნულ უსაფრთხოებასთან დაკავშირებული უწყებების ან ქვედანაყოფების საქმიანობა,[39] თუმცა იგი ვრცელდება საზოგადოების უსაფრთხოების ფარგლებში მონაცემთა დამუშავებაზე. რაც შეეხება დანაშაულის თავიდან აცილების, გამოძიების, სისხლისსამართლებრივი დევნის, ოპერატიულ-სამძებრო ღონისძიებებისა და მართლწესრიგის დაცვის მიზნებისათვის სახელმწიფოს საიდუმლოებისთვის მიკუთვნებულ მონაცემთა ნახევრად ავტომატურ და არაავტომატურ დამუშავებაზე არსებულ გამონაკლისს, აღსანიშნავია, რომ დირექტივა არ ვრცელდება ისეთი საქმიანობის პროცესში მონაცემთა დამუშავებაზე, რომელიც სცილდება ევროკავშირის საკანონმდებლო მოწესრიგების ფარგლებს.

მნიშვნელოვანია, რომ, ევროკავშირის რეგულაციის პრეამბულის თანახმად, სასამართლო ამოცანების განხორციელებისას და გადაწყვეტილებების მიღების პროცესში სასამართლოს დამოუკიდებლობის უზრუნველსაყოფად პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს უფლებამოსილება არ უნდა ვრცელდებოდეს სასამართლოების მიერ სამოსამართლო ფუნქციების შესრულებისას მონაცემთა დამუშავებაზე. ამდენად, ეროვნული კანონით გათვალისწინებული გამონაკლისი სასამართლოში სამართალწარმოების მიზნით

[37] იხ. რეგულაციის მე-3 მუხლი.

[38] იხ. საპოლიციო დირექტივის მე-2 მუხლი.

[39] საპოლიციო დირექტივის პრეამბულა, § 11.

მონაცემთა დამუშავების შესახებ, ასევე, შეესაბამება ევროკავშირის მონაცემთა დაცვის სამართალს.

პერსონალური დაცვის უფლების გამოხატვისა და ინფორმაციის თავისუფლებასთან ურთიერთბალანსის მიღწევის მიზნით, მასობრივი ინფორმაციის საშუალებების მიერ საზოგადოების ინფორმირების, აგრეთვე აკადემიური, სახელოვნო და ლიტერატურული მიზნით მონაცემთა დამუშავების გამონაკლისი გათვალისწინებულია ევროკავშირის რეგულაციითაც, მისი 85-ე მუხლის პირველი და მე-2 პუნქტებიდან გამომდინარე. აღნიშნულ საქმიანობასთან მიმართებით წევრმა სახელმწიფოებმა შეიძლება დაუშვან გამონაკლისები და დათქმები რეგულაციის მე-8 (უფლების აღდგენის/დაცვის საშუალებები, პასუხისმგებლობა და სანქციები), მე-10 (დელეგირებული აქტები და საიმპლემენტაციო აქტები) და მე-11 (გარდამავალი დებულებები) თავებთან მიმართებით, თუ არსებობს პერსონალურ მონაცემთა დაცვის უფლების გამოხატვის თავისუფლებასთან შესაბამისობის უზრუნველყოფის აუცილებლობა.

რეგულაციის 89-ე მუხლი ასევე ითვალისწინებს სტატისტიკური მიზნებისთვის მონაცემთა დამუშავებას, რომელიც უნდა განხორციელდეს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის სათანადო გარანტიებით. თუმცა აღნიშნული მიზნით შესაძლოა, შეიზღუდოს რეგულაციის მე-15, მე-16, მე-18 და 21-ე მუხლებით განსაზღვრული მონაცემთა სუბიექტის უფლებები, მათი დაცვის სათანადო გარანტიების ფარგლებში, იმ შემთხვევაში თუ მათი უფლებების გახორციელება შეუძლებელს ხდის ან ხელს უშლის ხსენებული მიზნების მიღწევას და ამგვარი გამონაკლისების არსებობა აუცილებელია. გასათვალისწინებელია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ასევე ადგენს კანონის შესაბამისად საჯარო ინტერესებისთვის არქივირების, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის მონაცემთა დამუშავების სათანადო გარანტიების უზრუნველყოფის ვალდებულებას.

გამონაკლისების შესახებ ეროვნული კანონის ფარგლებში აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მე-2 მუხლის მე-5 პუნქტის სახით ითვალისწინებს კეთილსინდისიერების ვალდებულებას ნებისმიერი ისეთი პირის მიმართ, რომელიც უნებლიეთ მიიღებს სხვის მონაცემებს, რომელიც მისთვის არ იყო განკუთვნილი. კერძოდ, მან პატივი უნდა სცეს მონაცემთა სუბიექტის უფლებებს და არ უნდა შეეცადოს მონაცემთა უკანონო დამუშავებას. აღნიშნული ვალდებულების განსაზღვრით, კანონი გაცილებით მაღალ სტანდარტს ადგენს, ვიდრე – რეგულაცია და საპოლიციო დირექტივა, რადგან ევროკავშირის სამართალში მსგავსი შინაარსის ექსპლიციტური ნორმა არ მოიძებნება.

— ტერმინთა განმარტება

საგულისხმოა, რომ სამივე აქტი დარგობრივ ტერმინს იდენტურად განმარტავს.[40] მიუხედავად ამისა, ზოგიერთ შემთხვევაში საქართველოს კანონი იმგვარი ცნებებისა და ტერმინების დეფინიციასაც ითვალისწინებს, რომლებიც არ არის განმარტებული "GDPR"-ისა და საპოლიციო დირექტივის შესაბამისი მუხლით (მაგალითად: მონაცემთა ავტომატური, ნახევრად ავტომატური და არაავტომატური საშუალებებით დამუშავება; მონაცემთა მიმღების კატეგორია; პერსონალურ მონაცემთა დაცვის ოფიცერი; ვიდეომონიტორინგი; აუდიომონიტორინგი; პირდაპირი მარკეტინგი; მონაცემთა დეპერსონალიზაცია და სხვა). განსხვავებით ევროკავშირის რეგულაციისა და საპოლიციო დირექტივისგან, თავის მხრივ, ეროვნული კანონმდებლობა არ განმარტავს ისეთ სამართლებრივ ინსტიტუტებთან დაკავშირებულ ტერმინებს, რომლებიც „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონით არ არის მოწესრიგებული (მაგალითად: ძირითადი დაწესებულების, საწარმოს, საერთაშორისო დამუშავების, საერთაშორისო ორგანიზაციის, ორგანიზაციათა ჯგუფის, დაინტერესებული საზედამხედველო ორგანოს ცნებებს, სავალდებულო კორპორაციული წესების განმარტებას და სხვა).

2. მონაცემთა დამუშავების კანონიერება

— მონაცემთა დამუშავების პრინციპები

მსგავსად ევროკავშირის მეორეული კანონმდებლობისა, „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონით განსაზღვრულია პერსონალურ მონაცემთა დამუშავების ექვსი პრინციპი: კანონიერად, სამართლიანად და გამჭვირვალედ მონაცემთა დამუშავება (აღსანიშნავია, რომ საპოლიციო დირექტივა არ ითვალისწინებს გამჭვირვალედ მონაცემთა დამუშავების პრინციპს[41]); მიზნის შეზღუდვის პრინციპი; მინიმიზაციის პრინციპი; სიზუსტის პრინციპი; ვადით შეზღუდვის პრინციპი; მონაცემთა უსაფრთხოების პრინციპი.[42] სამივე აქტი ითვალისწინებს, რომ პერსონალურ მონაცემთა დამუშავების პრინციპებთან შესაბამისობის მტკიცების ტვირთი აკისრია დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირს (ანგარიშვალდებულება).

საგულისხმოა, რომ საქართველოს კანონი, ევროკავშირის სამართლისაგან განსხვავებით, მონაცემთა კანონიერად, სამართლიანად, გამჭვირვალედ დამუშავების პრინციპთან მიმართებით ადგენს დამატებით ვალდებულებას, რომლის თანახმად, მონაცემები აგრეთვე უნდა დამუშავდეს მონაცემთა სუბიექტის

[40] იხ. კანონის მე-3, ევროკავშირს რეგულაციის მე-4 და საპოლიციო დირექტივის მე-3 მუხლები.
[41] იხ. საპოლიციო დირექტივის მე-4 მუხლის პირველი პუნქტი.
[42] იხ. კანონის მე-4, ევროკავშირს რეგულაციის მე-5 და საპოლიციო დირექტივის მე-4, მე-5 და მე-7 მუხლები.

ღირსების შეულახავად.[43] გასათვალისწინებელია, რომ ევროკავშირის კანონმდებლობა ექსპლიციტურად არ ითვალისწინებს მონაცემთა სუბიექტის ღირსების შეულახავად მონაცემთა დამუშავების სტანდარტს. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის თანახმად, მონაცემთა დამუშავების გამჭვირვალობის ვალდებულება არ ვრცელდება კანონით დადგენილ გამონაკლის შემთხვევებზე. ამ კონტექსტში აღსანიშნავია, რომ, სამართალდამცავ ორგანოთა კომპეტენციებიდან გამომდინარე, მონაცემთა გამჭვირვალედ დამუშავების პრინციპს საპოლიციო დირექტივა არ ითვალისწინებს.

— მონაცემთა დამუშავების საფუძვლები

აღსანიშნავია, რომ ევროკავშირის კანონმდებლობით გათვალისწინებული ყველა სამართლებრივი საფუძველი ასევე წარმოდგენილია ეროვნულ კანონმდებლობაში.[44] დამატებით საქართველოს კანონი ითვალისწინებს შემდეგ სამართლებრივ საფუძვლებს: მონაცემთა დამუშავება გათვალისწინებულია კანონით; კანონის თანახმად, მონაცემი საჯაროდ ხელმისაწვდომია ან მონაცემთა სუბიექტმა იგი საჯაროდ ხელმისაწვდომი გახადა; მონაცემთა დამუშავება აუცილებელია მნიშვნელოვანი საჯარო ინტერესის დასაცავად. აღნიშნულ საფუძველთან მიმართებით შეიძლება ითქვას, რომ “GDPR”-ი ითვალისწინებს მონაცემთა დამუშავებას „საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად“ ან „მონაცემთა დამმუშავებლისათვის მინიჭებული ოფიციალური უფლებამოსილების განსახორციელებლად“. თუმცა, საქართველოს კანონით განსაზღვრულ სამართლებრივ საფუძველს, კერძოდ, როდესაც „მონაცემთა დამუშავება აუცილებელია მნიშვნელოვანი საჯარო ინტერესის დასაცავად“[45] — იგი ცალკე არ ადგენს. რაც შეეხება საპოლიციო დირექტივას, მისი მოქმედების სფეროდან გამომდინარე, მონაცემთა დამუშავება უკავშირდება კომპეტენტური ორგანოების მიერ უფლებამოსილების განხორციელებას. ამასთანავე, საქართველოს კანონი ადგენს დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დამუშავების სამართლებრივი საფუძვლის დასაბუთების ვალდებულებას.

ევროკავშირის რეგულაციის თანახმად, მსგავსად საქართველოს კანონისა, მონაცემთა დამუშავების ერთ-ერთი საფუძველია მონაცემთა სუბიექტის თანხმობა, რომლის მოპოვებისა და გამოხმობის პირობები[46] მოწესრიგებულია სპეციალური ნორმით, კერძოდ, “GDPR”-ის მე-7 მუხლით. აღსანიშნავია, რომ თანხმობის მოპოვების პირობები საქართველოს კანონით მონაცემთა ცალკეული დამუშავების

[43] კანონის მე-4 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტი.

[44] იხ. კანონის მე-5, ევროკავშირს რეგულაციის მე-6 და საპოლიციო დირექტივის მე-8 და მე-9 მუხლები.

[45] კანონის მე-5 მუხლის პირველი პუნქტის „ზ“ ქვეპუნქტი.

[46] აღნიშნულზე უფრო ვრცლად იხ. მე-3 ქვეთავში მონაცემთა სუბიექტის უფლებების შესახებ.

მიხედვით, ასევე, მონაცემთა სუბიექტისგან მის მოპოვებასთან ან გამოხმობასთან დაკავშირებული დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებების მომწესრიგებელი სპეციალური ნორმებით განისაზღვრება[47] (მაგალითად: პირდაპირი მარკეტინგისთვის, აუდიომონიტორინგისთვის და სხვა). შესაბამისად, ევროკავშირის რეგულაციის მე-7 მუხლით დადგენილი სტანდარტი უზრუნველყოფილია კანონის ცალკეული მუხლებით[48]. სწორედ აღნიშნული მუხლებით განისაზღვრება, ერთი მხრივ, თანხმობის ცნება, გაცემის წესი, დამუშავებისთვის პასუხისმგებელი ან დამუშავებაზე უფლებამოსილი პირების ვალდებულებები თანხმობის მოპოვებისა და მონაცემთა სუბიექტის მიერ გამოხმობის დროს. "GDPR"-ისა და „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის შედარებითსამართლებრივ ანალიზზე დაყრდნობით, აღსანიშნავია, რომ ორივე აქტი განსაზღვრავს დამუშავებისთვის პასუხისმგებელი პირის მტკიცების ტვირთს თანხმობის არსებობის შესახებ. საგულისხმოა, რომ პირობები თანხმობის გამოხმობის შესახებ ორივე აქტის მიხედვით ერთგვაროვანია. ამასთანავე, როგორც კანონი, ისევე ევროკავშირის რეგულაცია თანხმობის ნებაყოფლობითობის განსაზღვრისას დამუშავებისთვის პასუხისმგებელ პირს ავალდებულებს, შეაფასოს თანხმობის მოპოვების აუცილებლობა.[49]

— განსაკუთრებული კატეგორიის მონაცემთა დამუშავების საფუძვლები

„პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი და ევროკავშირის სამართალი სპეციალური ნორმით ადგენს განსაკუთრებული კატეგორიის მონაცემთა დამუშავების სტანდარტს. რეგულაციის მე-9 მუხლი („განსაკუთრებული კატეგორიის მონაცემთა დამუშავება") თავისი სამართლებრივი ბუნებით ამკრძალველი ხასიათისაა და მისი პირველი პუნქტით, ერთი მხრივ, განისაზღვრება განსაკუთრებული კატეგორიის მონაცემის ცნება, ხოლო, მეორე მხრივ, კრძალავს მის დამუშავებას. ხსენებული მუხლის მე-2 პუნქტი აყალიბებს ერთგვარ გამონაკლის შემთხვევებს, როდესაც ამ კატეგორიის მონაცემთა დამუშავება დასაშვებია.

განსაკუთრებული კატეგორიის მონაცემის ანალოგიურ განმარტებას აყალიბებს საპოლიციო დირექტივა და ამავდროულად ითვალისწინებს მათი დამუშავების შესაძლებლობას იმ შემთხვევაში, თუკი „უზრუნველყოფილია მონაცემთა სუბიექტის უფლებებისა და ინტერესების დაცვის ამ კანონით გათვალისწინებული გარანტიები".[50] მსგავსად საპოლიციო დირექტივისა, საქართველოს კანონი განსაკუთრებული მონაცემების დამუშავებისთვის ადგენს მონაცემთა სუბიექტის დაცვის სათანადო გარანტიების უზრუნველყოფის ვალდებულებასა და მისი დამუშავების შემთხვევაში, კანონის სპეციალური

[47] კანონი, 32-ე მუხლი.
[48] იხ. კანონის მე-3 მუხლის „მ" და „ნ" ქვეპუნქტები, აგრეთვე, მე-20 და 32-ე მუხლები.
[49] იხ. რეგულაციის მე-7 მუხლის მე-4 პუნქტი და კანონის 32-ე მუხლის მე-2 პუნქტი.
[50] იხ. საპოლიციო დირექტივის მე-10 მუხლი.

ნორმით განსაზღვრული ერთ-ერთი სამართლებრივი საფუძვლის არსებობას. სამივე აქტით გათვალისწინებულ სამართლებრივ საფუძველთა შედარებითსამართლებრივ ანალიზზე დაყრდნობით, აღსანიშნავია, რომ საქართველოს კანონი ადგენს ყველა იმ საფუძველს, რომლებსაც აწესრიგებს "GDPR"-ი გარდა ერთისა, კერძოდ, შემთხვევისა, როდესაც „დამუშავება აუცილებელია სამართლებრივი მოთხოვნის დასამტკიცებლად, განსახორციელებლად ან დასაცავად ან როდესაც სასამართლოები ახორციელებენ მართლმსაჯულებას"[51]. რაც შეეხება საქართველოს კანონით გათვალისწინებულ სხვა სამართლებრივ საფუძვლებს,[52] მათ ევროკავშირის კანონმდებლობა არ ითვალისწინებს. ამასთანავე, ევროკავშირის რეგულაცია ითვალისწინებს სპეციალურ ნორმას ნასამართლობასთან და დანაშაულის ჩადენასთან დაკავშირებული მონაცემების დამუშავების შესახებ.[53] მართალია, საქართველოს კანონი არ ითვალისწინებს ამგვარი შინაარსის სპეციალურ ნორმას, თუმცა აღნიშნულ დამუშავებაზე ვრცელდება მე-6 მუხლით დადგენილი სტანდარტი.

საგულისხმოა, რომ საქართველოს კანონი, განსაკუთრებული კატეგორიის მონაცემთა სუბიექტის თანხმობის საფუძველზე დამუშავების შემთხვევაში, ითვალისწინებს წერილობითი თანხმობის ფორმას, როგორც სუბიექტის უფლებების დაცვის უზრუნველყოფის მაღალ სტანდარტს. "GDPR"-ი არ განსაზღვრავს მონაცემთა სუბიექტის თანხმობის წერილობით ფორმას.

— **არასრულწლოვანის პერსონალური მონაცემების დამუშავება**

„პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი და ევროკავშირის რეგულაცია ითვალისწინებს არასრულწლოვანის პერსონალური მონაცემების დამუშავების სპეციალურ ნორმებს. მართალია, საპოლიციო დირექტივა მე-6 მუხლით განასხვავებს მონაცემთა სუბიექტების სხვადასხვა კატეგორიას, თუმცა იგი არ შეიცავს არასრულწლოვანის პერსონალურ მონაცემთა დამუშავების მომწესრიგებელ სპეციალურ მუხლს. შედარებითსამართლებრივი ანალიზიდან გამომდინარე, აღსანიშნავია, რომ რეგულაციის მე-8 მუხლის მოქმედების სფერო შემოიფარგლება არასრულწლოვანისთვის ელექტრონული მომსახურების შეთავაზების მიზნით მისი პერსონალური მონაცემების დამუშავების სტანდარტის განსაზღვრით; საქართველოს კანონი კი ელექტრონული მომსახურების გარდა სხვა სფეროებსა და სექტორში არასრულწლოვანი პირის პერსონალური მონაცემების დამუშავებასაც მიემართება.[54] ამასთანავე, კანონი უფრო ფართოდ განსაზღვრავს არასრულწლოვანის მონაცემთა დამუშავების სტანდარტს; კერძოდ – მისი საუკეთესო ინტერესების გათვალისწინების

[51] რეგულაციის მე-9 მუხლის მე-2 პუნქტის „ვ" ქვეპუნქტი.
[52] იხ. კანონის მე-6 მუხლის პირველი პუნქტის „ზ", „კ", „ნ", „ო", „პ", „ჟ", „რ", „ს", „ტ" ქვეპუნქტები.
[53] იხ. რეგულაციის მე-10 მუხლი.
[54] იხ. კანონის მე-7 მუხლი.

ვალდებულებას; აგრეთვე, განსაკუთრებული კატეგორიის პერსონალური მონაცემის დამუშავების შემთხვევაში: თანხმობის წერილობით ფორმას, მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობის ნამდვილობის სპეციალურ კრიტერიუმს. რაც შეეხება თანხმობის ასაკობრივ ცენზს, საქართველოს კანონი იზიარებს რეგულაციით გათვალისწინებულ სტანდარტს. საგულისხმოა, რომ საქართველოს კანონი, მსგავსად "GDPR"-ისა, ითვალისწინებს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, რომ არსებული ტექნოლოგიების გათვალისწინებით მიღებულ იქნეს გონივრული ღონისძიებები, რათა დადგინდეს, არის თუ არა გაცემული თანხმობა ან ნებადართული მშობლის უფლების მქონე პირის მიერ.

— მონაცემთა დამუშავების სხვა ცალკეული შემთხვევები

საქართველოს კანონი ასევე აწესრიგებს გარდაცვლილი პირის, როგორც მონაცემთა სუბიექტის, პერსონალური მონაცემების დამუშავების პროცესს. საგულისხმოა, რომ "GDPR"-ი არ ითვალისწინებს სპეციალურ ნორმას გარდაცვლილი პირის მონაცემთა დაცვის შესახებ. მისი პრეამბულის 37-ე პუნქტის თანახმად, „რეგულაცია არ ვრცელდება გარდაცვლილი პირების პერსონალურ მონაცემებზე. წევრმა სახელმწიფოებმა შესაძლოა დაადგინონ წესები გარდაცვლილი პირების პერსონალური მონაცემების დამუშავებისათვის." აგრეთვე, ეროვნული კანონმდებლობისაგან განსხვავებით, "GDPR"-ი არ ითვალისწინებს სპეციალურ ნორმას ბიომეტრიულ მონაცემთა დამუშავების შესახებ, თუმცა, რეგულაციის მე-9 მუხლის მე-4 პუნქტის თანახმად, „წევრმა სახელმწიფოებმა შეიძლება შეინარჩუნონ ან დააწესონ დამატებითი პირობები, მათ შორის – შეზღუდვები, რომლებიც ეხება გენეტიკური, ბიომეტრიული ან ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავებას."

რაც შეეხება საპოლიციო დირექტივას, მართალია, იგი არ ითვალისწინებს სპეციალურ ნორმას, თუმცა, თანახმად მე-10 მუხლისა, ამგვარი მონაცემის დამუშავება ნებადართული იქნება, თუკი მიღებულია მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის სათანადო ზომები და არსებობს დამუშავების ერთ-ერთი სამართლებრივი საფუძველი მაინც, მათ შორისაა ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით ამგვარი მონაცემის დამუშავების გათვალისწინება.

აღსანიშნავია, რომ, განსხვავებით „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონისა[55], ევროკავშირის კანონმდებლობა არ ითვალისწინებს ვიდეო- და აუდიომონიტორინგის მომწესრიგებელ სპეციალურ ნორმებს, თუმცა მონაცემთა ამ გზით დამუშავებაზე ვრცელდება კანონიერი დამუშავების

[55] იხ. კანონის მე-10 და მე-11 მუხლები.

სტანდარტი, მათ შორის — მონაცემთა სუბიექტის სათანადო ინფორმირების თაობაზე.[56]

საქართველოს კანონის მე-12 მუხლი აწესრიგებს პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების პროცესს. "GDPR"-ის პრეამბულის 70-ე პუნქტის მიხედვით, „როდესაც მონაცემთა დამუშავება ხორციელდება პირდაპირი მარკეტინგის მიზნებისათვის, მონაცემთა სუბიექტს აქვს უფლება ნებისმიერ დროს მოითხოვოს დამუშავების, მათ შორის, პროფილირების შეწყვეტა, რამდენადაც იგი დაკავშირებულია პირდაპირ მარკეტინგთან. ეს უფლება მოიცავს მონაცემთა პირველად და მეორად დამუშავებას, არ არის შეზღუდული დროით და არ მოითხოვს გადასახადის გადახდას. სუბიექტს პირდაპირ უნდა განემარტოს დამუშავების შეწყვეტის მოთხოვნის უფლება. ამ ინფორმაციის მიწოდება უნდა მოხდეს გასაგებად და ნებისმიერი სხვა ინფორმაციისაგან განცალკევებულად". გასათვალისწინებელია რეგულაციის 21-ე მუხლის („მონაცემთა დამუშავების შეწყვეტის მოთხოვნის უფლება") მე-2 პუნქტი, რომლის თანახმად, თუკი მონაცემების მუშავდება პირდაპირი მარკეტინგის მიზნით, მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს მოითხოვოს ამ მიზნით მონაცემთა დამუშავების შეწყვეტა; ხოლო რეგულაციის 21-ე მუხლის მე-3 პუნქტი განსაზღვრავს ვალდებულებას, კერძოდ, სუბიექტის მიერ მონაცემთა პირდაპირი მარკეტინგის მიზნებისათვის დამუშავების შეწყვეტის მოთხოვნის შემთხვევაში, პირდაპირი მარკეტინგის მიზნით, მონაცემთა შემდგომი დამუშავების დაუშვებლობის შესახებ. საქართველოს კანონის მე-12 მუხლის მე-4 პუნქტის თანახმად, მონაცემთა სუბიექტის შესაბამისი მოთხოვნის შემთხვევაში, არა უგვიანეს 7 სამუშაო დღისა, პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავება უნდა შეწყდეს, რაც თავისთავად გულისხმობს რეგულაციის 21-ე მუხლის მე-3 პუნქტით დადგენილი სტანდარტის ეროვნულ კანონმდებლობაში არსებობას.

[56] იხ. რეგულაციის მე-13 და მე-14 მუხლები.

3. მონაცემთა სუბიექტის უფლებები

საქართველოს და ევროკავშირის კანონმდებლობა ადგენს დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირების ვალდებულებას, დაიცვან მონაცემთა სუბიექტის უფლებები:

მონაცემთა სუბიექტის უფლების კატეგორია	საქართველოს კანონი	ევროკავშირის რეგულაცია	საპოლიციო დირექტივა
მონაცემთა დამუშავების შესახებ ინფორმაციის მიღების უფლება	მე-13 მუხლი	მე-15 მუხლი	მე-14 და მე-15 მუხლები
მონაცემთა გაცნობისა და ასლის მიღების უფლება	მე-14 მუხლი	მე-12 მუხლი	მე-12 მუხლი
მონაცემთა გასწორების, განახლებისა და შევსების უფლება	მე-15 მუხლი	მე-16 მუხლი	მე-16 მუხლის პირველი პუნქტი
მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლება	მე-16 მუხლი	მე-17 და 21-ე მუხლები	მე-16 მუხლის მე-2 პუნქტი
მონაცემთა დაბლოკვის უფლება	მე-17 მუხლი	მე-18 მუხლი	მე-16 მუხლის მე-3 პუნქტი
მონაცემთა გადატანის (პორტირების) უფლება	მე-18 მუხლი	მე-20 მუხლი	[არ ითვალისწინებს]
ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებასთან დაკავშირებული უფლებები	მე-19 მუხლი	22-ე მუხლი	მე-11 მუხლი
თანხმობის გამოხმობის უფლება	მე-20 მუხლი	მე-7 მუხლის მე-3 პუნქტი	[არ ითვალისწინებს]
გასაჩივრების უფლება	22-ე მუხლი	77-ე, 78-ე და 79-ე მუხლები	52-ე, 53-ე და 54-ე მუხლები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონისა და ევროკავშირის კანონმდებლობის თანახმად, მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს იმის დადასტურება, მუშავდება თუ არა მის შესახებ მონაცემები, დასაბუთებულია თუ არა მონაცემთა დამუშავება და მოთხოვნის შესაბამისად უსასყიდლოდ მიიღოს შესაბამისი ინფორმაცია. აღსანიშნავია, რომ საქართველოს კანონი, მსგავსად ევროკავშირის რეგულაციისა და საპოლიციო დირექტივისა, უზრუნველყოფს მონაცემთა სუბიექტისათვის გამჭვირვალედ, მარტივად გასაგები, ნათელი და ხელმისაწვდომი ფორმით ინფორმაციის გაზიარებას. აღსანიშნავია, რომ საქართველოს კანონი ფიზიკური პირისათვის მონაცემების დამუშავების პროცესის თაობაზე ინფორმაციის მიღების უფრო შემჭიდროვებულ ვადას ადგენს, ვიდრე – “GDPR”-ი. კერძოდ, კანონის მე-13 მუხლის თანახმად, ინფორმაცია მონაცემთა სუბიექტს უნდა მიწოდოს მოთხოვნიდან არა უგვიანეს 10 სამუშაო დღისა, ხოლო, განსაკუთრებულ შემთხვევებში და სათანადო დასაბუთების საფუძველზე, აღნიშნული ვადა შეიძლება გახანგრძლივდეს არა უმეტეს 10 სამუშაო დღისა, რის შესახებაც მონაცემთა სუბიექტს დაუყოვნებლივ უნდა ეცნობოს. საგულისხმოა, რომ, “GDPR”-ი მე-12 მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს შესაბამისი ინფორმაცია უნდა გაუზიაროს დაუყოვნებლივ ან მოთხოვნის მიღებიდან ერთი თვის ვადაში, ხოლო, მოთხოვნათა სირთულიდან და რაოდენობიდან გამომდინარე, აღნიშნული ვადა შესაძლოა გაგრძელდეს ორი თვით. საქართველოს კანონითა და ევროკავშირის რეგულაციით გათვალისწინებული მისაღები ინფორმაციის კატეგორია ურთიერთთანმხვედრია. ამასთანავე, კანონი ითვალისწინებს მონაცემთა სუბიექტს უფლებას, გაეცნოს მის შესახებ არსებულ პერსონალურ მონაცემებს და უსასყიდლოდ მიიღოს ამ მონაცემების ასლები. გამონაკლისს წარმოადგენს იმგვარი შემთხვევა, როდესაც: ა) საქართველოს კანონმდებლობით გათვალისწინებულია საფასური; ბ) დამუშავებისთვის პასუხისმგებელი პირის მიერ დადგენილია გონივრული საფასური მონაცემთა შენახვის ფორმისგან განსხვავებული ფორმით მათი გაცემისთვის დახარჯული რესურსის ან/და მოთხოვნის სიხშირის გამო.[57] ევროკავშირის რეგულაციაც ანალოგიურად ადგენს შესაბამისი საფასურის განსაზღვრის შესაძლებლობას, თუკი მონაცემთა სუბიექტის მოთხოვნები ცალსახად დაუსაბუთებელი ან გადაჭარბებულად მოცულობითია, განსაკუთრებით კი მათი განმეორებითი ხასიათის გამო.[58] ასეთ შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია, დააწესოს გონივრული საფასური ინფორმაციის მიწოდების, კომუნიკაციის ან მოთხოვნილი ქმედებების განხორციელების ადმინისტრაციული ხარჯების გათვალისწინებით; ან

[57] იხ. კანონის მე-14 მუხლის პირველი პუნქტის „ა“ და „ბ“ ქვეპუნქტები.
[58] იხ. რეგულაციის მე-12 მუხლის მე-5 პუნქტი.

უარი თქვას მოთხოვნის შესრულებაზე. ანალოგიურ მოწესრიგებას ითვალისწინებს საპოლიციო დირექტივა.[59]

საგულისხმოა, რომ ეროვნული კანონმდებლობა, განსხვავებით ევროკავშირის სამართლისა, შემჭიდროვებულ ვადას ადგენს მცდარი, არაზუსტი ან/და არასრული მონაცემების გასწორების, განახლების ან/და შევსების უფლების განხორციელებასთან დაკავშირებით. კერძოდ, საქართველოს კანონის მე-15 მუხლის მე-2 პუნქტის თანახმად, მოთხოვნის წარდგენიდან არა უგვიანეს 10 სამუშაო დღისა (თუ საქართველოს კანონმდებლობით სხვა ვადა არ არის დადგენილი) მონაცემები უნდა გასწორდეს, განახლდეს ან/და შეივსოს ან მონაცემთა სუბიექტს ეცნობოს მოთხოვნაზე უარის თქმის საფუძველი და განემარტოს უარის გასაჩივრების წესი. გარდა აღნიშნულისა, ეროვნული კანონმდებლობა ითვალისწინებს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, უზრუნველყოს მონაცემთა სუბიექტის ინფორმირება იმ ობიექტური გარემოებების შესახებ, რომლებიც შეუძლებელს ხდის აღნიშნული უფლების რეალიზაციას; აგრეთვე – აღნიშნულ მონაცემთა ყველა მიმღების, სხვა დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის, რომლებსაც თავად გადასცა მონაცემები, მონაცემთა განახლებისა და შევსების შესახებ ინფორმირების ვალდებულებას.[60]

რაც შეეხება მონაცემთა წაშლის უფლების განხორციელებას, ნორმათა შედარებითი ანალიზიდან გამომდინარე, შესაძლებელია ითქვას, რომ აღნიშნულ უფლებებთან დაკავშირებით საქართველოს კანონი მოთხოვნათა განხორციელებაზე უარის თქმის უფრო ფართო საფუძვლებს ადგენს. კერძოდ, “GDPR”-ის თანახმად, დამუშავებისთვის პასუხისმგებელი პირის აღნიშნული ვალდებულება არ ვრცელდება, თუ მონაცემთა დამუშავება აუცილებელია: გამოხატვის თავისუფლებისა და ინფორმაციის მიღების უფლების განხორციელებისათვის; ევროკავშირის ან წევრი სახელმწიფოს კანონის შესაბამისად დამუშავებისთვის პასუხისმგებელი პირის კანონისმიერი ვალდებულების შესასრულებლად, ან საჯარო ინტერესის სფეროში შემავალი ფუნქციების შესასრულებლად ან დამუშავებისთვის პასუხისმგებელი პირისთვის კანონით მინიჭებული უფლებამოსილების განსახორციელებლად; საჯარო ინტერესის მიზნებისათვის საყოველთაო ჯანმრთელობის დაცვის სფეროში მე-9 მუხლის მე-2 პუნქტის „თ“ და „ი“ ქვეპუნქტების და მე-9 მუხლის მე-3 პუნქტის შესაბამისად; საჯარო ინტერესებისათვის არქივირების მიზნით, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებისათვის 89-ე მუხლის პირველი პუნქტის შესაბამისად იმ შემთხვევაში, თუ ამ მუხლის პირველი პუნქტით განსაზღვრული უფლების განხორციელება შეუძლებელს გახდის ან

[59] იხ. საპოლიციო დირექტივის მე-12 მუხლის მე-4 პუნქტი.
[60] იხ. კანონის მე-15 მუხლის მე-5 და მე-6 პუნქტები.

მნიშვნელოვნად დააზიანებს დამუშავების მიზნების მიღწევას; ან სამართლებრივი მოთხოვნის დადგენის, განხორციელების ან დაცვის მიზნებისთვის.[61]

საგულისხმოა, რომ საქართველოს კანონი, მსგავსად ევროკავშირის რეგულაციისა, ასევე ადგენს მონაცემთა სუბიექტის აღნიშნული უფლების შეზღუდვისა და მისგან გამომდინარე მოთხოვნაზე უარის თქმის ისეთ სამართლებრივ საფუძვლებს, როგორებიცაა: მონაცემთა დამუშავება სამართლებრივი მოთხოვნის ან შესაგებლის დასაბუთების მიზნით; აგრეთვე, გამოხატვის ან ინფორმაციის თავისუფლების უფლების განხორციელების მიზნით; ამასთან, კანონით გათვალისწინებული საჯარო ინტერესებისთვის არქივირების, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის და თუკი მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლების განხორციელება შეუძლებელს გახდის ან მნიშვნელოვნად დააზიანებს დამუშავების მიზნების მიღწევას.[62] თუმცა, გარდა აღნიშნული საფუძვლებისა, კანონის მე-16 მუხლის მე-3 პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს უფლება აქვს, უარი თქვას მონაცემთა სუბიექტის შესახებ მონაცემთა დამუშავების (მათ შორის, პროფაილინგის) შეწყვეტა, წაშლა ან განადგურების შესახებ იმ შემთხვევაშიც, თუკი არსებობს მონაცემთა დამუშავების კანონის მე-5 და მე-6 მუხლებით გათვალისწინებული მონაცემთა დამუშავების რომელიმე სამართლებრივი საფუძველი.[63] თუმცა გასათვალისწინებელია, რომ ეროვნული კანონმდებლობა, განსხვავებით "GDPR"-ისგან, მონაცემთა სუბიექტის აღნიშნული უფლების განხორციელების უფრო შემჭიდროვებულ ვადას ადგენს და „მოთხოვნიდან არა უგვიანეს 10 სამუშაო დღისა (თუ საქართველოს კანონმდებლობით სხვა რამ არ არის დადგენილი) უნდა შეწყდეს მონაცემთა დამუშავება ან/და მონაცემები უნდა წაიშალოს ან განადგურდეს ან მონაცემთა სუბიექტს უნდა ეცნობოს მოთხოვნაზე უარის თქმის საფუძველი და განემარტოს უარის გასაჩივრების წესი".[64]

მონაცემთა სუბიექტის მიერ მონაცემთა დაბლოკვის მოთხოვნის უფლებას ითვალისწინებს როგორც ეროვნული, ისევე – ევროკავშირის კანონმდებლობა. საგულისხმოა, რომ საქართველოს კანონი ადგენს "GDPR"-ით გათვალისწინებულ მონაცემთა დაბლოკვის ანალოგიურ გარემოებებს იმ განსხვავებით, რომ ეროვნული კანონმდებლობა ითვალისწინებს მონაცემთა სუბიექტის მიერ აღნიშნული მოთხოვნის წარდგენის დამატებით შემთხვევებს (მე-17 მუხლის პირველი პუნქტის „დ" და „ე" ქვეპუნქტების სახით); თუმცა კანონი ასევე ადგენს მონაცემთა სუბიექტის მოთხოვნის შეზღუდვის საფუძვლებს.[65] ევროკავშირის რეგულაციისა და საპოლიციო დირექტივისგან განსხვავებით, ეროვნული კანონმდებლობა ითვალისწინებს დაბლოკვის ხანგრძლივობის დადგენის, ასევე – დაბლოკვის

[61] იხ. რეგულაციის მე-17 მუხლის მე-3 პუნქტი.
[62] იხ. კანონის მე-16 მუხლის მე-3 პუნქტი.
[63] იხ. კანონის მე-16 მუხლის მე-3 პუნქტის „ა" ქვეპუნქტი.
[64] იხ. კანონის მე-16 მუხლის მე-2 პუნქტი.
[65] იხ. კანონის მე-17 მუხლის მე-2 პუნქტი.

შესახებ გადაწყვეტილების შესაბამის მონაცემებთან დართვის სტანდარტებს და მონაცემთა დაბლოკვის თაობაზე მიღებული გადაწყვეტილების ან მონაცემთა დაბლოკვაზე უარის თქმის საფუძვლის შესახებ გადაწყვეტილების მიღებისთანავე, დაუყოვნებლივ, მაგრამ არა უგვიანეს მოთხოვნიდან 3 სამუშაო დღისა, მონაცემთა სუბიექტის ინფორმირების ვალდებულებებს.[66]

მონაცემთა პორტირების, იგივე გადატანის უფლება, ეროვნულ კანონმდებლობაში ახალ ინსტიტუტს წარმოადგენს. აღსანიშნავია, რომ საქართველოს კანონით გათვალისწინებული მოწესრიგება შეესაბამება ევროკავშირის მონაცემთა დაცვის ძირითად რეგულაციას. ასევე, "GDPR"-ი ადგენს აღნიშნული უფლების შეზღუდვის შესაძლებლობას, თუკი მონაცემთა დამუშავება აუცილებელია საჯარო ინტერესის სფეროში შემავალი ფუნქციების/ამოცანების შესასრულებლად ან დამუშავებისთვის პასუხისმგებელი პირისთვის კანონით მინიჭებული უფლებამოსილების განსახორციელებლად; ამავდროულად, პორტირების უფლების განხორციელებით არ უნდა შეილახოს სხვათა უფლებები და თავისუფლებები.[67]

ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებისა და მასთან დაკავშირებული უფლებების მომწესრიგებელი ნორმა (კანონის მე-19 მუხლი) შეესაბამება ევროკავშირის კანონმდებლობას. აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, "GDPR"-ი და საპოლიციო დირექტივა უზრუნველყოფენ მონაცემთა სუბიექტის უფლებას, არ დაექვემდებაროს მხოლოდ ავტომატიზებულად, მათ შორის – პროფაილინგის საფუძველზე მიღებულ გადაწყვეტილებას, რომელიც მისთვის წარმოშობს სამართლებრივ ან სხვა სახის არსებითი მნიშვნელობის მქონე შედეგს. ასევე, გათვალისწინებულია აღნიშნული უფლების შეზღუდვის სამართლებრივი საფუძვლები, რომლებიც, შედარებითსამართლებრივ ანალიზზე დაყრდნობით, ურთიერთშესაბამისია. აღსანიშნავია, რომ საქართველოს კანონი, ძირითადი რეგულაცია და საპოლიციო დირექტივა მხოლოდ ავტომატიზებულად, მათ შორის – პროფაილინგის საფუძველზე გადაწყვეტილების მიღებისას, განსაკუთრებული კატეგორიის მონაცემების გამოყენებას შესაძლებელს ხდის მხოლოდ იმპერატიულად განსაზღვრულ შემთხვევებში. კერძოდ, "GDPR"-ის თანახმად, აღნიშნული დასაშვებია, თუკი არსებობს მე-9 მუხლის მე-2 პუნქტის „ა"[68] ან „ზ"[69]

---

[66] იხ. კანონის მე-17 მუხლის მე-4 და მე-5 პუნქტები.

[67] იხ. რეგულაციის მე-20 მუხლის მე-3 და მე-4 პუნქტები.

[68] „არსებობს მონაცემთა სუბიექტის ნათლად გამოხატული თანხმობა ერთი ან რამდენიმე კონკრეტული მიზნით ამგვარი პერსონალური მონაცემების დამუშავებაზე, გარდა იმ შემთხვევისა, როდესაც წევრი სახელმწიფოს კანონის თანახმად, მონაცემთა სუბიექტი ვერ ეწინააღმდეგება პირველ პუნქტში მითითებულ აკრძალვას".

[69] „დამუშავება აუცილებელია არსებითი საჯარო ინტერესიდან გამომდინარე, ევროკავშირის ან წევრი სახელმწიფოს კანონის საფუძველზე, რომელიც დასახული მიზნის პროპორციული უნდა იყოს, პატივს სცემდეს მონაცემთა დაცვის უფლების არსს და ითვალისწინებდეს სათანადო და კონკრეტულ ღონისძიებებს მონაცემთა სუბიექტის ფუნდამენტური უფლებებისა და ინტერესების დასაცავად".

ქვეპუნქტებით განსაზღვრული გარემოებები და არსებობს მონაცემთა სუბიექტის უფლებების, თავისუფლებებისა და კანონიერი ინტერესების დაცვის სათანადო გარანტიები. საქართველოს კანონის თანახმად, გადაწყვეტილების მიღებისას განსაკუთრებული კატეგორიის მონაცემების გამოყენება დასაშვებია, ერთი მხრივ, თუკი არსებობს მონაცემთა სუბიექტის უფლებების, თავისუფლებებისა და ლეგიტიმური ინტერესების დაცვის სათანადო გარანტიები, ხოლო, მეორე მხრივ, კანონის მე-6 მუხლის პირველი პუნქტის „ა“, „ვ“ და „კ“ ქვეპუნქტებით გათვალისწინებულ შემთხვევებში, რაც უკავშირდება: მონაცემთა სუბიექტის წერილობით თანხმობას; დანაშაულის თავიდან აცილების (მათ შორის, სათანადო ანალიტიკური კვლევის), გამოძიების, სისხლისსამართლებრივი დევნის, მართლმსაჯულების განხორციელების, პატიმრობისა და თავისუფლების აღკვეთის აღსრულებისა და ზემოაღნიშნული მუხლის „ვ“ ქვეპუნქტით გათვალისწინებული სხვა საჯაროსამართლებრივი ინტერესებიდან გამომდინარე; ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების უზრუნველსაყოფად მონაცემთა დამუშავებას.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი სპეციალური ნორმით აწესრიგებს მონაცემთა სუბიექტის მიერ გაცემული თანხმობის გამოხმობის საკითხს. აღსანიშნავია, რომ, მსგავსად “GDPR”-ისა, კანონი ადგენს სუბიექტის უფლებას, ნებისმიერ დროს გამოიხმოს თანხმობა. უფრო მეტიც, კანონი აკონკრეტებს უფლების განხორციელების სტანდარტს, კერძოდ, ყოველგვარი განმარტების ან დასაბუთების გარეშე აღნიშნული მოთხოვნის განხორციელების შესაძლებლობას; ასევე – მოთხოვნიდან არა უგვიანეს 10 სამუშაო დღის ვადაში მონაცემთა დამუშავების შეწყვეტის ან/და დამუშავებული მონაცემების წაშლის ან განადგურების ვალდებულებას. კანონი უზრუნველყოფს მონაცემთა სუბიექტის მიერ თანხმობის გამოხმობის იმავე ფორმის შესაძლებლობას, რომელიც მის გასაცემად იქნა გამოყენებული; აგრეთვე – სუბიექტის მიერ თანხმობის გამოხმობის სამართლებრივი შედეგების თაობაზე ინფორმაციის მიღების უფლებას.[70]

მონაცემთა სუბიექტის უფლებებს განეკუთვნება გასაჩივრების უფლება, რომელიც ერთ-ერთი ეფექტიანი სამართლებრივი საშუალებაა მისთვის უზრუნველყოფილი უფლებების დასაცავად. აღსანიშნავია, რომ ეროვნული კანონმდებლობა, მსგავსად ევროკავშირის სამართლისა, ადგენს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსათვის, ასევე – სასამართლოსთვის ან/და ზემდგომი ადმინისტრაციული ორგანოსათვის მიმართვის შესაძლებლობას.[71]

მონაცემთა სუბიექტის უფლებების შეზღუდვა დასაშვებია იმ შემთხვევაში, თუკი აღნიშნული გათვალისწინებულია კანონმდებლობით, ემსახურება ფუნდამენტური უფლებებისა და თავისუფლებების არსს და წარმოადგენს

[70] იხ. კანონის მე-20 მუხლი.

[71] იხ. კანონის 22-ე მუხლი.

აუცილებელ და პროპორციულ ზომას დემოკრატიულ საზოგადოებაში.[72] ამასთანავე, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 21-ე მუხლის თანახმად, მონაცემთა სუბიექტის უფლებების შეზღუდვა დასაშვებია იმ ინტერესების დასაცავად, რომლებიც, თავის მხრივ, აგრეთვე გათვალისწინებულია ევროკავშირის რეგულაციით, თუმცა იმ განსხვავებით, რომ ეროვნული კანონმდებლობით მონაცემთა სუბიექტის უფლების შეზღუდვის საფუძველს ასევე წარმოადგენს სახელმწიფო, კომერციული, პროფესიული და კანონით გათვალისწინებული სხვა სახის საიდუმლოებების დაცვა[73]. ამასთანავე, კანონი ადგენს მონაცემთა სუბიექტის უფლებათა შეზღუდვის პროპორციულობის სტანდარტს მისაღწევ ლეგიტიმურ მიზანთან მიმართებით, ასევე – უფლების შეზღუდვასთან დაკავშირებით დამუშავებისთვის პასუხისმგებელი პირის მტკიცების ტვირთსა და მონაცემთა სუბიექტის ინფორმირების ვალდებულებას, თუკი აღნიშნული საფრთხეს არ შეუქმნის ლეგიტიმური მიზნის მიღწევის ინტერესს. განსხვავებით ევროკავშირის რეგულაციისა, საქართველოს კანონი არ ითვალისწინებს ვალდებულებას, რომლის თანახმად, უფლების შესაზღუდად მიღებული სამართლებრივი ზომები უნდა შეიცავდეს სულ მცირე იმგვარ ინფორმაციას, როგორიცაა, მაგალითად: მონაცემთა დამუშავების მიზანი ან დამუშავების კატეგორიები; წარმოდგენილი შეზღუდვების ფარგლები; მონაცემთა უკანონოდ გამოყენების, წვდომის ან გადაცემისაგან დაცვის გარანტიები და სხვა.[74]

4. დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის ვალდებულებები

საქართველოს კანონმდებლობა, მსგავსად ევროკავშირის ძირითადი რეგულაციისა და საპოლიციო დირექტივისა, ითვალისწინებს მონაცემთა დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირის ზოგად ვალდებულებას — მიიღოს ყველა ზომა კანონის მოთხოვნებთან შესაბამისობის და საჭიროების შემთხვევაში მათი დემონსტრირების მიზნით.[75] ანალოგიურად, “GDPR”-ის 24-ე მუხლის მიხედვით, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაატაროს შესაბამისი ტექნიკურ-ორგანიზაციული ზომები, რათა უზრუნველყოს და შეძლოს დაადასტუროს, რომ მონაცემთა დამუშავება ხორციელდება რეგულაციის შესაბამისად, ხოლო საჭიროების შემთხვევაში აღნიშნული ზომები უნდა გადაიხედოს და განახლდეს. საპოლიციო დირექტივის მე-12 მუხლი აგრეთვე ითვალისწინებს მონაცემთა

[72] იხ. კანონის 21-ე მუხლის პირველი პუნქტი.
[73] იხ. კანონის 21-ე მუხლის პირველი პუნქტის „თ“ ქვეპუნქტი.
[74] იხ. რეგულაციის 23-ე მუხლის მე-2 პუნქტი.
[75] იხ. კანონის 23-ე მუხლის პირველი პუნქტი.

სუბიექტის უფლებების უზრუნველსაყოფად სათანადო ღონისძიებების განხორციელების ვალდებულებას.

მონაცემთა სუბიექტის უფლებების განხორციელებასთან დაკავშირებული ვალდებულებების გარდა, ეროვნული და ევროკავშირის მონაცემთა დაცვის კანონმდებლობა ითვალისწინებს დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა სუბიექტის ინფორმირების სტანდარტს ორ შემთხვევაში: ა) თუ მონაცემები უშუალოდ მისგან — მონაცემთა სუბიექტისგან გროვდება; ბ) თუ მონაცემები არა უშუალოდ მონაცემთა სუბიექტისგან, არამედ მესამე პირისგან გროვდება. საგულისხმოა, რომ ეროვნული კანონმდებლობა მონაცემების უშუალოდ სუბიექტისგან შეგროვების შემთხვევაში აკონკრეტებს შესაბამისი ინფორმაციის გაზიარების ეტაპს, კერძოდ, მონაცემთა შეგროვებამდე ან შეგროვების დაწყებისთანავე. "GDPR"-ის მე-13 მუხლის პირველი და მე-2 პუნქტებისა და საქართველოს კანონის 24-ე მუხლის პირველი პუნქტების შედარებისამართლებრივ ანალიზზე დაყრდნობით შესაძლებელია ითქვას, რომ ორივე აქტი ადგენს ერთსა და იმავე სტანდარტს მონაცემთა სუბიექტისათვის გასაზიარებელ მინიმალურ ინფორმაციასთან დაკავშირებით. გარდა ამისა, აღსანიშნავია, რომ ეროვნული კანონმდებლობა განსაკუთრებულ ყურადღებას ანიჭებს არასრულწლოვანი მონაცემთა სუბიექტისათვის ინფორმაციის ხელმისაწვდომობის საკითხს და, განსხვავებით "GDPR"-ის აღნიშნული ნორმისა, ადგენს პასუხისმგებელი პირის ექსპლიციტურ ვალდებულებას, მარტივ და მისთვის გასაგებ ენაზე გაზიარების სახით. აღსანიშნავია, რომ ეროვნული კანონმდებლობა ასევე ითვალისწინებს მონაცემთა სუბიექტის ინფორმირებისგან გამონაკლის შემთხვევას, როდესაც სპეციალური კანონმდებლობა მონაცემების შეგროვებისას ადგენს მონაცემთა სუბიექტისგან მისი ინფორმირების განსხვავებულ წესს და აღნიშნული არ იწვევს მისივე ძირითადი უფლებებისა და თავისუფლებების დარღვევას. ასევე საგულისხმოა, რომ ასეთ შემთხვევაში სუბიექტის წერილობითი მოთხოვნის არსებობისას დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტს მიაწოდოს შესაბამისი ინფორმაცია მოთხოვნიდან 10 სამუშაო დღის ვადაში, როცა არ არსებობს უფლების შეზღუდვის კანონით დადგენილი სამართლებრივი საფუძველი. თუკი მონაცემები არ გროვდება უშუალოდ მონაცემთა სუბიექტისაგან, გარდა ზემოაღნიშნული ინფორმაციისა, როგორც საქართველოს, ისე ევროკავშირს კანონმდებლობის შესაბამისად, მონაცემთა სუბიექტს ასევე უნდა ეცნობოს, თუ რომელი მონაცემები მუშავდება და ასევე მათი მოპოვების წყაროს შესახებ; მათ შორის, მოპოვებულ იქნა თუ არა მონაცემები საჯაროდ ხელმისაწვდომი წყაროდან.

საგულისხმოა მონაცემთა სუბიექტის ინფორმირების ვადის საკითხი. კერძოდ, „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის 25-ე მუხლის თანახმად, „პასუხისმგებელმა პირმა მონაცემთა სუბიექტს ინფორმაცია უნდა მიაწოდოს გონივრულ ვადაში ან, თუ მონაცემები გამოიყენება მონაცემთა სუბიექტთან დასაკავშირებლად, მასთან პირველი კომუნიკაციისთანავე, ხოლო თუ

დაგეგმილია მონაცემთა გამჟღავნება, — მონაცემთა გამჟღავნებამდე, მაგრამ მონაცემთა მოპოვებიდან არაუგვიანეს 10 სამუშაო დღისა," თუკი არ არსებობს სუბიექტის უფლების შეზღუდვის სამართლებრივი გარემოება. საგულისხმოა, რომ "GDPR"-ის მე-14 მუხლი ადგენს ინფორმირების შემდეგ სტანდარტს — ინფორმაცია, მონაცემების დამუშავების სპეციფიური გარემოებების გათვალისწინებით, სუბიექტს უნდა მიეწოდოს მონაცემების შეგროვების შემდგომ გონივრულ ვადაში, თუმცა არა უგვიანეს ერთი თვისა; ხოლო, თუ მონაცემები გამოიყენება მონაცემთა სუბიექტთან კომუნიკაციის მიზნით — არა უგვიანეს მონაცემთა სუბიექტთან კავშირის პირველად დამყარებისას ან, თუ მონაცემები გამიზნულია სხვა მიმღებისთვის გადასაცემად, არა უგვიანეს მონაცემების პირველად გადაცემის მომენტისა. ორივე აქტი ადგენს მონაცემთა სუბიექტის ინფორმირებისგან გამონაკლის ერთგვაროვან შემთხვევებს იმ განსხვავებით, რომ, რეგულაციის თანახმად, დამუშავებისთვის პასუხისმგებელ პირზე აღნიშნული ვალდებულება არ ვრცელდება, თუკი მონაცემთა შეგროვება ან გაცემა გათვალისწინებულია ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით, რომელიც ვრცელდება დამუშავებისთვის პასუხისმგებელ პირზე და განსაზღვრავს მონაცემთა სუბიექტის კანონიერი ინტერესების დაცვის სათანადო ზომებს; ან ევროკავშირის ან წევრი სახელმწიფოს პროფესიული საიდუმლოების მარეგულირებელი სამართლებრივი ნორმების შესაბამისად, რაც ასევე მოიცავს კანონით გათვალისწინებულ ვალდებულებას საიდუმლოების დაცვის შესახებ. მონაცემთა კონფიდენციალობა უნდა იყოს დაცული.[76] ხოლო საქართველოს კანონის თანახმად, ინფორმაციის მიწოდების ვალდებულება არ ვრცელდება დამუშავებისთვის პასუხისმგებელ ან/და დამუშავებაზე უფლებამოსილ პირებზეც, თუ მონაცემთა შეგროვება ან გამჟღავნება დადგენილია კანონით ან საჭიროა საქართველოს კანონმდებლობით დაკისრებული მოვალეობის შესასრულებლად.[77] აღნიშნულ შემთხვევათა მიზნისა და სპეციფიკის გათვალისწინებით, შესაძლებელია ითქვას, რომ განხილული გამონაკლისები ურთიერთთანმხვედრია.

დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირების ვალდებულებათა სახით საქართველოს კანონი, მსგავსად ევროკავშირის რეგულაციისა და საპოლიციო დირექტივისა, ითვალისწინებს იმგვარ სამართლებრივ ინტიტუტებს, როგორებიცაა:

— **მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას**

[76] რეგულაციის მე-14 მუხლის მე-5 პუნქტის „გ" და „დ" ქვეპუნქტები.
[77] კანონის 25-ე მუხლის მე-3 პუნქტი.

ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა მეტად დაფარვის პრიორიტეტი წარმოადგენს პრევენციულ ღონისძიებას, რომლის გათვალისწინება ხორციელდება მონაცემთა დამუშავების საშუალების განსაზღვრის ეტაპზე. აღნიშნული სტანდარტის მიზანია, რომ დამუშავების პროცესის ყველა ეტაპი განხორციელდეს კანონის მოთხოვნათა და მონაცემთა დამუშავების პრინციპების სრული დაცვით, სისტემების შექმნის ეტაპზე და მონაცემთა დამუშავების პროცესში კონფიდენციალურობისა და მონაცემთა დაცვის პრინციპების ინტეგრირების გზით.[78] საგულისხმოა, რომ კანონი სრულად იზიარებს ევროკავშირის რეგულაციისა და საპოლიციო დირექტივის მოწესრიგებას ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინებისა ("Privacy by Design") და პირველად პარამეტრად მონაცემთა დაცვის ("Privacy by Default") ვალდებულების შესახებ[79]. განსხვავებით ეროვნული მოწესრიგებისაგან, "GDPR"-ი ასევე ადგენს აღნიშნულ სტანდარტთან შესაბამისობის დემონსტრირების შესაძლებლობას მონაცემთა დაცვის სერტიფიცირების მექანიზმის[80] გამოყენებით. ეროვნული კანონმდებლობა არ იცნობს ამგვარ ინსტრუმენტს.

— **მონაცემთა უსაფრთხოება**

საგულისხმოა, რომ 2024 წლის მარტიდან ამოქმედებული „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის თანახმად, მონაცემთა უსაფრთხოება წარმოადგენს მონაცემთა დამუშავების ერთ-ერთ ძირითად პრინციპს, რომელიც აგრეთვე მოწესრიგებულია კანონის 27-ე მუხლით. იგი ადგენს მონაცემთა დამუშავების პროცესის კანონთან შესაბამისობის უზრუნველსაყოფად, დამუშავებისთვის პასუხისმგებელი პირების მიერ სათანადო ტექნიკური და ორგანიზაციული ზომების მიღების ვალდებულებას.

ევროკავშირის რეგულაცია ისევე, როგორც საპოლიციო დირექტივა, აწესრიგებს ზემოაღნიშნული ზომების განხორციელების ვალდებულებას, რა დროსაც, მსგავსად ეროვნული საკანონმდებლო მოთხოვნისა, მხედველობაში მიიღება მონაცემთა დამუშავების შესაძლო და თანამდევი საფრთხეთა სპეციფიკა, მონაცემთა კატეგორიები, მოცულობა, მონაცემთა დამუშავების მიზანი, ფორმა, საშუალებები, მათ შორის – უახლესი ტექნოლოგიებისა და განხორციელების ხარჯების კონტექსტი, აგრეთვე მონაცემთა სუბიექტის უფლებების დარღვევის შესაძლო საფრთხეები.[81] ამავდროულად, "GDPR"-ი და საპოლიციო დირექტივა

[78] პერსონალურ მონაცემთა დაცვის სამსახური, სახელმძღვანელო რეკომენდაცია მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას, 2024.

[79] იხ. რეგულაციის 25-ე მუხლი და საპოლიციო დირექტივის მე-20 მუხლი.

[80] იხ. რეგულაციის 42-ე მუხლი.

[81] იხ. რეგულაციის 32-ე მუხლის პირველი პუნქტი და საპოლიციო დირექტივის 29-ე მუხლის პირველი პუნქტი.

განსაზღვრავს შესაბამისი ტექნიკურ-ორგანიზაციული ღონისძიებების სხვადასხვა კატეგორიას, რომელთანაც თანმხვედრია ეროვნული კანონმდებლობით შემოთავაზებული ზომები, რაც, თავის მხრივ, არ არის ამომწურავი ჩამონათვალი.[82] ამავდროულად, საქართველოს კანონი ადგენს დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირების ვალდებულებას, უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა (ე. წ. „ლოგირება“), ხოლო არაელექტრონული ფორმით არსებული დამუშავების შემთხვევაში — მონაცემთა გამჟღავნებასთან ან/და ცვლილებასთან დაკავშირებული ყველა მოქმედების აღრიცხვა.[83] აღნიშნული სტანდარტი ეხმიანება საპოლიციო დირექტივით დადგენილი რისკების შეფასების მიზნით სათანადო ღონისძიებების ვალდებულებასაც, რაც მათ შორის გულისხმობს მოწყობილობაზე დაშვების კონტროლს, მონაცემთა მატარებლის კონტროლს, შენახვის კონტროლს და სხვა.[84]

ამასთანავე, კანონი ითვალისწინებს დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირების ვალდებულებას თანამშრომელთა მონაცემებზე წვდომის ფარგლების განსაზღვრის, ცნობიერების ამაღლების, მათ შორის სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგაც, კონფიდენციალურობის დაცვის თვალსაზრისით.

— მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლის, ევროკავშირის რეგულაციის 30-ე მუხლისა და საპოლიციო დირექტივის 24-ე მუხლის შედარებითსამართლებრივ ანალიზზე დაყრდნობით, შესაძლებელია ითქვას, რომ ეროვნული კანონმდებლობა საკმაოდ მაღალ სტანდარტს აწესებს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვისა და პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსათვის მისი ინფორმირების თვალსაზრისით. კერძოდ, გარდა რეგულაციისა და საპოლიციო დირექტივით გათვალისწინებული აღსარიცხი ინფორმაციისა, კანონის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი და მისი სპეციალური წარმომადგენელი (ასეთის არსებობის შემთხვევაში), ხოლო დამუშავების პროცესში დამუშავებაზე უფლებამოსილი პირის მონაწილეობის შემთხვევაში ეს უკანასკნელიც, ვალდებულნი არიან ასევე აღრიცხონ ინფორმაცია მონაცემთა უსაფრთხოების

[82] იხ. კანონის 27-ე მუხლის მე-2 პუნქტი.
[83] კანონის 27-ე მუხლის მე-4 პუნქტი.
[84] იხ. საპოლიციო დირექტივის 29-ე მუხლის მე-2 პუნქტი.

დარღვევის შესახებ.[85] ასევე, კანონის თანახმად, აღრიცხული ინფორმაცია პერსონალურ მონაცემთა დაცვის სამსახურს უნდა მიეწოდოს მოთხოვნისთანავე, დაუყოვნებლივ, მაგრამ არა უგვიანეს 3 სამუშაო დღისა მაშინ, როდესაც ევროკავშირის რეგულაცია არ განსაზღვრავს კონკრეტულ ვადას ინფორმაციის მონაცემთა დაცვის საზედამხედველო ორგანოსათვის გასაზიარებლად.[86] ამგვარი ვადა არც საპოლიციო დირექტივით არის დადგენილი.[87] ამასთან, ეროვნული კანონი სპეციალური მოწესრიგების სახით ასევე ითვალისწინებს ვალდებულებას სამართალდამცავ ორგანოებთან მიმართებით.[88]

საგულისხმოა, რომ "GDPR"-ი ითვალისწინებს აღნიშნული ვალდებულების განხორციელებისგან გამონაკლისს, რაც უკავშირდება იმგვარი მეწარმე სუბიექტის საქმიანობას, რომელშიც დასაქმებულ პირთა რაოდენობა 250-ზე ნაკლებია.[89] ხაზგასასმელია, რომ მონაცემთა დამუშავების ეროვნული სტანდარტი არ ადგენს აღნიშნული ვალდებულებისაგან მსგავსი სახის გამონაკლისს.

— ინციდენტის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულება

როგორც ეროვნული, ასევე ევროკავშირის კანონმდებლობა ადგენს მონაცემთა უსაფრთხოების დარღვევის — ინციდენტის მართვისა და მისი აღმოჩენიდან არა უგვიანეს 72 საათისა — პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსათვის ინფორმირების ვალდებულებას. ევროკავშირის რეგულაციის 33-ე მუხლისა და საპოლიციო დირექტივის 30-ე მუხლის თანახმად, ინფორმირება უნდა განხორციელდეს დაუყოვნებლივ და შესაძლებლობის შემთხვევაში დარღვევის შესახებ შეტყობიდან არა უგვიანეს 72 საათისა, ხოლო აღნიშნულ ვადაში ვალდებულების შეუსრულებლობის შემთხვევაში საზედამხედველო ორგანოს უნდა წარედგინოს განმარტება დაყოვნების მიზეზების თაობაზე. ეროვნული კანონმდებლობა არ ითვალისწინებს „დაუყოვნებლივ" შეტყობინების სტანდარტს, რამდენადაც პერსონალურ მონაცემთა დაცვის სამსახურისადმი მიმართვის მაქსიმალურ ვადად 72 საათია დასახელებული, ამასთან კანონი არ ადგენს დაყოვნების მიზეზების განმარტების შესაძლებლობას.

სამივე აქტის მიხედვით, დარღვევასთან დაკავშირებული ვალდებულება არ ვრცელდება, თუკი ნაკლებსავარაუდოა, რომ ინციდენტი გამოიწვევს ფიზიკურ

[85] ევროკავშირის რეგულაცია პერსონალურ მონაცემებთან დაკავშირებული ნებისმიერი დარღვევის, შესაბამისი ფაქტების, გამოწვეული შედეგებისა და მიღებული ზომების ჩათვლით აღრიცხვის ვალდებულებას ითვალისწინებს 33-ე მუხლის მე-5 პუნქტის თანახმად.

[86] იხ. რეგულაციის 30-ე მუხლის მე-4 პუნქტი.

[87] იხ. საპოლიციო დირექტივის 24-ე მუხლის მე-3 პუნქტი.

[88] კანონი, 28-ე მუხლის მე-4 — მე-7 პუნქტები. დამატებით იხ. პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის სპეციალური ანგარიში „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის იმპლემენტაცია, 2025, გვ. 55-59.

[89] რეგულაცია, 30-ე მუხლის მე-5 პუნქტი.

პირთა უფლებებისა და თავისუფლებების შელახვის რისკს. მნიშვნელოვანია, რომ გარდა "GDPR"-ითა და საპოლიციო დირექტივით გათვალისწინებული ინფორმაციის წარდგენის ვალდებულებისა, დამუშავებისთვის პასუხისმგებელი პირი, საქართველოს კანონის 29-ე მუხლის თანახმად, ვალდებულია საზედამხედველო ორგანოს წარუდგინოს ინფორმაცია ინციდენტის გარემოებების, სახისა და დროის შესახებ; აგრეთვე – გეგმავს თუ არა დამუშავებისთვის პასუხისმგებელი პირი, ინციდენტის შესახებ შეატყობინოს მონაცემთა სუბიექტ(ებ)ს კანონის 30-ე მუხლით დადგენილი წესით და რა ვადაში. განსხვავებით "GDPR"-ისა და საპოლიციო დირექტივისა, საქართველოს კანონის მიხედვით, ინციდენტის გარემოებების, სავარაუდო ზიანის ან/და მონაცემთა სუბიექტების რაოდენობის გათვალისწინებისა, პერსონალურ მონაცემთა დაცვის სამსახური უფლებამოსილია, ინციდენტის შესახებ მის ხელთ არსებული ინფორმაცია გაასაჯაროოს, თუკი, წარდგენილი შეტყობინების თანახმად, დამუშავებისთვის პასუხისმგებელი პირი არ უზრუნველყოფს ან ვერ უზრუნველყოფს ინციდენტის თაობაზე მონაცემთა სუბიექტის ინფორმირებას. აღნიშნულთან დაკავშირებით კანონის 29-ე მუხლის მე-6 პუნქტი და 30-ე მუხლის მე-3 პუნქტი ასევე ითვალისწინებს გამონაკლის შემთხვევებს. ევროკავშირის რეგულაციის თანახმად, თუკი მონაცემთა სუბიექტს არ მიეწოდა ინფორმაცია მონაცემთა უსაფრთხოების დარღვევის შესახებ, საზედამხედველო ორგანო უფლებამოსილია, რომ მოითხოვოს სუბიექტის სათანადო ინფორმირების განხორციელება ან შეაფასოს, არსებობს თუ არა სუბიექტისათვის შეტყობინების ვალდებულებისაგან "GDPR"-ით გათვალისწინებული გამონაკლისი შემთხვევა.

საგულისხმოა, რომ ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმები და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ამ ინციდენტის შეტყობინების წესი განსაზღვრულია პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის №19 ბრძანებით — „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ".

— ინციდენტის შესახებ მონაცემთა სუბიექტის ინფორმირების ვალდებულება

ევროკავშირს რეგულაციის 34-ე მუხლის თანახმად, „თუ პერსონალური მონაცემების უსაფრთხოების დარღვევა გამოიწვევს ფიზიკურ პირთა უფლებებისა და თავისუფლებების შელახვის მაღალ რისკს, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაუმართლებელი შეფერხების გარეშე შეატყობინოს მონაცემთა სუბიექტს მონაცემთა უსაფრთხოების დარღვევის შესახებ". საგულისხმოა, რომ საპოლიციო დირექტივა, მსგავსად საქართველოს კანონისა,

აღნიშნულ ვალდებულებას ფიზიკური პირების უფლებებისა და თავისუფლებების დარღვევის მაღალი რისკის „დიდი ალბათობით“ გამოწვევას უკავშირებს მაშინ, როდესაც რეგულაციის მიხედვით პირთა უფლებებისა და თავისუფლებების შელახვის მაღალი რისკი დადგენილი გარემოებაა. აღნიშნული მიუთითებს ეროვნული კანონმდებლობის მკაცრ სტანდარტზე მონაცემთა სუბიექტის სათანადო ინფორმირების უზრუნველყოფის თვალსაზრისით.

გარდა აღნიშნულისა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ითვალისწინებს მონაცემთა სუბიექტის ინციდენტის შესახებ მარტივ და მისთვის გასაგებ ენაზე ინფორმირების ვალდებულებას.[90] საგულისხმოა, რომ კანონი აღნიშნულისგან გამონაკლისს მხოლოდ ორ გარემოებას უქვემდებარებს, კერძოდ, საჯაროსამართლებრივი ინტერესის დაცვასა და დამუშავებისთვის პასუხისმგებელი პირის მიერ სათანადო უსაფრთხოების ღონისძიებების მიღებას, რომლის შედეგად თავიდან იქნა აცილებული ადამიანის ძირითადი უფლებებისა და თავისუფლებების დარღვევის მნიშვნელოვანი საფრთხე. საპოლიციო დირექტივა მონაცემთა სუბიექტისათვის შეტყობინების გადადების, შეზღუდვის ან გაუქმების შესაძლებლობას განსაზღვრავს მე-13 მუხლის მე-3 პუნქტით გათვალისწინებული საფუძვლით; კერძოდ, მხოლოდ იმ შემთხვევაში და იმ პირობით, როდესაც ამგვარი ღონისძიება წარმოადგენს აუცილებელ და პროპორციულ ზომას დემოკრატიულ საზოგადოებაში და დირექტივის ზემოაღნიშნული პუნქტით განსაზღვრული მიზნებისათვის სათანადოდ იქნება გათვალისწინებული დაინტერესებული ფიზიკური პირის ფუნდამენტური უფლებები და ლეგიტიმური ინტერესები.

— მონაცემთა დაცვაზე ზეგავლენის შეფასება

ზეგავლენის შეფასება პროცესია, რომელიც ადამიანის უფლებების დარღვევის მომეტებული საფრთხეების შემცირებას ემსახურება და აღწერს დამუშავების პროცესის მიმდინარეობას მისი აუცილებლობისა და პროპორციულობის გათვალისწინებით. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 31-ე მუხლის პირველი პუნქტის თანახმად, „თუ მონაცემთა დამუშავებისას ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია წინასწარ განახორციელოს მონაცემთა დაცვაზე ზეგავლენის შეფასება“. ევროკავშირის რეგულაციის 35-ე მუხლის თანახმად, „როდესაც სავარაუდოა, რომ მონაცემთა კონკრეტული ტიპის დამუშავება უახლესი ტექნოლოგიების გამოყენებით და დამუშავების ხასიათის, მოცულობის, კონტექსტისა და მიზნების

[90] იხ. საქართველოს კანონის 30-ე მუხლის პირველი პუნქტი.

გათვალისწინებით, შესაძლოა იწვევდეს ფიზიკურ პირთა უფლებებისა და თავისუფლებების დარღვევის მაღალ რისკებს, მონაცემთა დამმუშავებელმა დამუშავების დაწყებამდე უნდა ჩაატაროს დაგეგმილი დამუშავების ოპერაციების რისკების შეფასება. ერთი შეფასებით შეიძლება შემოწმდეს დამუშავების მსგავსი მოქმედებები, რომლებიც სავარაუდოდ იწვევენ ერთნაირ მაღალ რისკებს.“ “GDPR”-ის სტანდარტი ეყრდნობა „ვარაუდს“, რომლის თანახმად, მონაცემთა კონკრეტული დამუშავების პროცესი, უახლესი ტექნოლოგიების გამოყენებითა და დამუშავების ხასიათის, მოცულობის, კონტექსტისა და მიზნების გათვალისწინებით, შესაძლოა იწვევდეს ფიზიკურ პირთა უფლებებისა და თავისუფლებების დარღვევის მაღალ რისკებს. ასეთ შემთხვევაში რეგულაციის თანახმად, სავალდებულოა მონაცემთა დაცვაზე ზეგავლენის ჩატარება. საქართველოს კანონი ითვალისწინებს „მაღალი ალბათობის“ სტანდარტს, კერძოდ, როდესაც მონაცემთა დამუშავებისას ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, „მაღალი ალბათობით“ შელახვის საფრთხე იქმნება. ზეგავლენის შეფასებისთვის კანონით დადგენილი მავალდებულებელი გარემოებების ანალიზით ვიღებთ ერთგვარ კრიტერიუმს იმის განსასაზღვრად, თუ რა შემთხვევაშია საჭირო და აუცილებელი ზეგავლენის შეფასების განხორციელება.[91] აღსანიშნავია, რომ საპოლიციო დირექტივაც ტერმინოლოგიური თვალსაზრისით იყენებს „დიდი ალბათობის“ სტანდარტს, რომელიც შელახვის მაღალი რისკის მაიდენტიფიცირებელი ერთ-ერთი კრიტერიუმია.

ევროკავშირის კანონმდებლობის თანახმად, მონაცემთა დაცვაზე ზეგავლენის ერთი (ერთიანი) შეფასებით შეიძლება შემოწმდეს დამუშავების მსგავსი მოქმედებები, რომლებიც სავარაუდოდ იწვევს ერთგვაროვან მაღალ რისკებს. აღნიშნულზე რაიმე სახის პირდაპირ მითითებას არ ითვალისწინებს საქართველოს კანონი. გასათვალისწინებელია, რომ ეროვნული რეგულაცია შეესაბამება “GDPR”-ის 35-ე მუხლის მე-3 პუნქტით დადგენილ გარემოებებს, რომელთა გათვალისწინებით განსაკუთრებით მნიშვნელოვანია ზეგავლენის შეფასების ჩატარება; მაგალითად, როდესაც დამუშავებისთვის პასუხისმგებელი პირი ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემებს, ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში, მონაცემთა სუბიექტისთვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებს სრულად ავტომატიზებულად.[92]

აღსანიშნავია, რომ როგორც საქართველოს, ისევე ევროკავშირის კანონმდებლობა განსაზღვრავს, თუ რა ინფორმაციას უნდა შეიცავდეს ზეგავლენის

[91] დამატებით იხ. პერსონალურ მონაცემთა დაცვის სამსახური, რეკომენდაციები მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) შესახებ, 2024.

[92] იხ. კანონის 31-ე მუხლის მე-2 პუნქტი.

შეფასების დოკუმენტი. ნორმათა შედარების საფუძველზე შესაძლებელია ითქვას, რომ ეროვნული მოწესრიგება ითვალისწინებს ევროკავშირის ძირითადი რეგულაციისა და საპოლიციო დირექტივის სტანდარტს იმ განსხვავებით, რომ ევროპული კანონმდებლობა განსაზღვრავს მინიმალური ინფორმაციის ჩამონათვალს და, ასევე, უფრო ფართოდ ადგენს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას — შეფასების შედეგად შექმნილ დოკუმენტში გაითვალისწინოს გამოვლენილი რისკების დაძლევისაკენ მიმართული ზომები, მათ შორის – პერსონალური მონაცემების დაცვის გარანტიები და მექანიზმები, რომლებიც ახდენს რეგულაციასთან შესაბამისობის დემონსტრირებას და რომლებიც ითვალისწინებს მონაცემთა სუბიექტის და სხვა დაინტერესებული პირების კანონიერ ინტერესებსა და უფლებებს;[93] საქართველოს კანონის თანახმად კი, მონაცემთა კატეგორიის, მათი დამუშავების მიზნების, პროპორციულობის, პროცესისა და საფუძვლების აღწერის გარდა, წერილობითი დოკუმენტი ასევე უნდა შეიცავდეს ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეების შეფასებასა და მონაცემთა უსაფრთხოების დაცვის მიზნით გათვალისწინებული ორგანიზაციულ-ტექნიკური ზომების აღწერას.[94]

გასათვალისწინებელია, რომ, კანონის თანახმად, შეფასების შედეგად იდენტიფიცირებული დამუშავებისთვის პასუხისმგებელი პირი მაღალი საფრთხის შემთხვევაში ვალდებულია, მიიღოს ყველა აუცილებელი ზომა საფრთხეების არსებითად შესამცირებლად და საჭიროებისამებრ, კონსულტაციის მიზნით, მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს; ხოლო, თუკი დამატებითი ორგანიზაციულ-ტექნიკური ზომებით შეუძლებელია ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის არსებითად შემცირება, მონაცემთა დამუშავება არ უნდა განხორციელდეს. განსხვავებით ევროკავშირის სამართლისა, საქართველოს კანონი განსაზღვრავს შემუშავებული შეფასების შენახვის ხანგრძლივობას, მონაცემთა სუბიექტის დიდი რაოდენობის მნიშვნელობას და ასევე – ზეგავლენის შეფასების დოკუმენტის გასაჯაროების ვალდებულებისაგან გამონაკლისს შემთხვევებს.[95]

საგულისხმოა, რომ ევროკავშირის რეგულაცია ითვალისწინებს საზედამხედველო ორგანოს შესაძლებლობას, დაადგინოს დამუშავების ის მოქმედებები, რომლებიც საჭიროა “GDPR”-ის 35-ე მუხლის პირველი პუნქტით დადგენილი მონაცემების დაცვის რისკების შეფასებისთვის. შესაბამისად, მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესი განსაზღვრულია

[93] იხ. რეგულაციის 35-ე მუხლის მე-7 პუნქტი.
[94] კანონი, 31-ე მუხლის მე-2 პუნქტი.
[95] იხ. კანონის 31-ე მუხლის მე-4, მე-7 და მე-8 პუნქტები.

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის 21-ე ბრძანებით.[96]

“GDPR”-ისა და საპოლიციო დირექტივის მსგავსად, ეროვნული კანონმდებლობაც ადგენს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსთან კონსულტაციის გავლის შესაძლებლობას; თუმცა მნიშვნელოვანია, რომ ევროკავშირის სამართალი უფრო ფართოდ აწესრიგებს საზედამხედველო ორგანოსთან კონსულტაციის გავლის საკითხს. დამუშავებისთვის პასუხისმგებელ პირს აღნიშნული ვალდებულება წარმოეშობა იმ შემთხვევაში, როდესაც დაგეგმილმა დამუშავებამ შესაძლოა გამოიწვიოს ფიზიკურ პირთა უფლებებისა და თავისუფლებების დარღვევის მაღალი რისკი, თუკი დამუშავებისთვის პასუხისმგებელი რისკების აღმოსაფხვრელად სათანადო ზომებს არ გაატარებს. დამუშავების დაწყებამდე სავალდებულოა პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსთან კონსულტაციის გავლა.[97] რაც შეეხება ეროვნულ მოწესრიგებას კონსულტაციის გავლის შესაძლებლობის შესახებ, იგი მხოლოდ „საჭიროების შემთხვევაში“ ითვალისწინებს.[98] კანონი, მსგავსად ევროკავშირის სამართლისა, ადგენს საზედამხედველო ორგანოსათვის გასაზიარებელი მინიმალური ინფორმაციის ფარგლებს, რომელიც შინაარსობრივად ურთიერთთანმხვედრია.

— პერსონალურ მონაცემთა დაცვის ოფიცერი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებულ კიდევ ერთ საკანონმდებლო სიახლეს პერსონალურ მონაცემთა დაცვის ოფიცრის ინსტიტუტი წარმოადგენს. აღსანიშნავია, რომ ეროვნული კანონმდებლობა სრულად ითვალისწინებს მონაცემთა დაცვის ოფიცრის მიმართ ევროკავშირის სამართლით განსაზღვრულ სტანდარტს. მათ შორის: დანიშვნის ან განსაზღვრის ვალდებულების წარმომშობ გარემოებებს, რომლებიც დამატებით წესრიგდება პერსონალურ მონაცემთა დაცვის სამსახურის ნორმატიული აქტით[99], საერთო ოფიცრის ინსტიტუტს, დამუშავებისთვის პასუხისმგებელი პირის თანამშრომლის ოფიცრის დანიშვნის/განსაზღვრის შესაძლებლობას იმის გათვალისწინებით, რომ აღნიშნული არ წარმოშობს ინტერესთა კონფლიქტს. საგულისხმოა, რომ ევროკავშირის სამართლით დამუშავებისთვის

[96] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ.

[97] იხ. რეგულაციის 36-ე მუხლის პირველი პუნქტი.

[98] კანონი, 31-ე მუხლის მე-5 პუნქტი.

[99] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის №22 ბრძანება „დამუშავებისთვის პასუხისმგებელ პირთა და დამუშავებაზე უფლებამოსილ პირთა წრის განსაზღვრის შესახებ, რომლებსაც არ აქვთ ვალდებულება დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი“.

პასუხისმგებელი პირი ვალდებულია, საჯაროდ გამოაქვეყნოს მონაცემთა დაცვის ოფიცრის საკონტაქტო ინფორმაცია და ასევე აცნობონ პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს. აღნიშნულ ვალდებულებას აგრეთვე ითვალისწინებს ეროვნული კანონმდებლობა იმ განსხვავებით, რომ პერსონალურ მონაცემთა დაცვის სამსახურის ინფორმირების ვადა ოფიცრის დანიშვნიდან ან განსაზღვრიდან, აგრეთვე – მისი შეცვლიდან 10 სამუშაო დღით განისაზღვრება.[100]

საქართველოს კანონი ევროკავშირის სამართლის მსგავსად აყალიბებს ოფიცრის ფუნქცია-მოვალეობებს, მათ მიმართ დაკისრებული ვალდებულებების შესრულების სტანდარტს.[101] "GDPR"-ი არ ადგენს პირდაპირ მოთხოვნას მონაცემთა დაცვის ოფიცრის საკვალიფიკაციო მოთხოვნებზე, მათ შორის – ლიცენზირების საკითხზე, თუმცა სავალდებულოა, ოფიცერს ჰქონდეს შესაბამისი კომპეტენცია, რომელსაც შესაძლებელია ადასტურებდეს პროფესიული სერტიფიცირების შესაბამისი პროგრამა.[102] მნიშვნელოვანია, რომ არც ეროვნული კანონმდებლობით და არც ევროპული სამართლით არ არის განსაზღვრული ოფიცრის გაწვევის ან მასთან დადებული ხელშეკრულების შეწყვეტის სამართლებრივი პირობები.

— სპეციალური წარმომადგენელი

აღნიშნულ ინსტიტუტს ითვალისწინებს როგორც „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, ისევე — ევროკავშირის ძირითადი რეგულაცია.[103] საგულისხმოა, რომ საპოლიციო დირექტივა არ შეიცავს დებულებებს სპეციალური წარმომადგენლის დანიშვნის თაობაზე.

რეგულაციის თანახმად, სპეციალური წარმომადგენლის დანიშვნის ვალდებულების განმსაზღვრელი სივრცითი არეალი დგინდება ევროკავშირის ტერიტორიის გარეთ რეგისტრირებული დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირ(ებ)ის წარმომადგენლებზე მითითებით; ხოლო საქართველოს კანონი ითვალისწინებს საქართველოს ფარგლებს გარეთ რეგისტრირებული დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირ(ებ)ის ვალდებულებას სპეციალური წარმომადგენლის დანიშვნის ან განსაზღვრის თაობაზე. აღნიშნული ვალდებულების მოწესრიგების სპეციფიკის გათვალისწინებით, განსხვავებულია ეროვნული და ევროპული კანონმდებლობით დადგენილი გამონაკლისებიც. კერძოდ, საქართველოს კანონის თანახმად, სპეციალური წარმომადგენლის დანიშვნის ან განსაზღვრის

[100] იხ. რეგულაციის 37-ე მუხლის მე-7 პუნქტი, საპოლიციო დირექტივის 32-ე მუხლის მე-4 პუნქტი და საქართველოს კანონის 33-ე მუხლის მე-8 პუნქტი.

[101] იხ. რეგულაციის 38-ე და 29-ე მუხლები, საპოლიციო დირექტივის 33-ე და 34-ე მუხლები, საქართველოს კანონის 33-ე მუხლის პირველი, მე-3, მე-4 — მე-7 პუნქტები.

[102] დამატებით იხ.: პერსონალურ მონაცემთა დაცვის სამსახური, რეკომენდაცია პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ, 2024.

[103] იხ. საქართველოს კანონის 34-ე მუხლის და რეგულაციის 27-ე მუხლი.

ვალდებულება არ წარმოიშობა, თუკი პასუხისმგებელი ან/და უფლებამოსილი პირი დაფუძნებულია ევროკავშირის წევრ სახელმწიფოებში და მასზე ვრცელდება ევროკავშირში მოქმედი პერსონალურ მონაცემთა დაცვის წესები ან თუკი დაფუძნებულია ევროკავშირის მიერ აღიარებულ მონაცემთა ადეკვატური დაცვის მქონე სახელმწიფოში;[104] "GDPR"-ი კი გამონაკლისის სახით ითვალისწინებს იმგვარ შემთხვევებს, როდესაც: მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი სახელმწიფო ორგანოა; მონაცემთა დამუშავება ხორციელდება პერიოდულად, არ ხორციელდება ფართო მასშტაბით; არ მოიცავს განსაკუთრებული კატეგორიის მონაცემთა დიდი მოცულობით დამუშავებას, როგორც აღნიშნული მითითებულია რეგულაციის მე-9 მუხლის პირველ პუნქტში ან ნასამართლობასთან და დანაშაულის ჩადენასთან დაკავშირებული მონაცემების დამუშავებას, რეგულაციის მე-10 მუხლის შესაბამისად, და ნაკლებად წარმოშობს დამუშავების ხასიათის, კონტექსტის, მასშტაბისა და მიზნების გათვალისწინებით ფიზიკური პირების უფლებებისა და თავისუფლებების დარღვევის რისკსაც. აღსანიშნავია, რომ, საქართველოს კანონის თანახმად, სპეციალური წარმომადგენლის რეგისტრაციის წესი დადგენილია პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტით.[105]

— დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის სხვა ვალდებულებები

„პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი ასევე განსაზღვრავს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებებს, მონაცემთა სუბიექტისგან თანხმობის მიღების და მის მიერ თანხმობის გამოხმობის შემთხვევებში, თანადამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის როლს. ეროვნული კანონმდებლობა ევროკავშირის რეგულაციის ანალოგიურ სტანდარტს ადგენს დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა სუბიექტისგან თანხმობის მიღებასა და მის მიერ თანხმობის გამოხმობასთან დაკავშირებული ვალდებულებების მიმართ. კერძოდ, კანონის 32-ე მუხლი, "GDPR"-ის მე-7 მუხლის მსგავსად, თანხმობის მოსაპოვებლად წერილობითი დოკუმენტის შედგენის შემთხვევაში ითვალისწინებს თანხმობის შესახებ ტექსტის მკაფიო, მარტივი და გასაგები ენით ჩამოყალიბების ვალდებულებას. როგორც საქართველოს, ისევე ევროკავშირის კანონმდებლობის თანახმად, თანხმობის ნებაყოფლობითობის შეფასებისას, სხვა გარემოებებთან ერთად, უნდა შეფასდეს, არის თუ არა ეს თანხმობა ხელშეკრულების ან მომსახურების აუცილებელი პირობა და თუ შეიძლება ამ თანხმობის გარეშე

[104] იხ. საქართველოს კანონის 34-ე მუხლის მე-6 და მე-7 პუნქტები.

[105] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის №20 ბრძანება „პერსონალურ მონაცემთა დაცვის სამსახურის მიერ სპეციალური წარმომადგენლის რეგისტრაციის წესის დამტკიცების შესახებ".

შესაბამისი მომსახურების მიღება/ხელშეკრულების დადება. კანონი ასევე ითვალისწინებს თანხმობის მიღებამდე მონაცემთა სუბიექტის ინფორმირების ვალდებულებას მის მიერ თანხმობის გამოხმობის უფლების, თანხმობის გამოხმობის შედეგების შესახებ.[106] მსგავსად ევროკავშირის რეგულაციისა, კანონი ადგენს თანხმობის გამოხმობის უსასყიდლო, მარტივი და ხელმისაწვდომი მექანიზმის დანერგვის ვალდებულებას, მათ შორის – თანხმობის გამოხმობის იმავე ფორმის გამოყენების შესაძლებლობას, რომლითაც იგი იქნა გაცემული მონაცემთა სუბიექტის მიერ.[107]

საქართველოს კანონის მოთხოვნები თანადამუშავებისთვის პასუხისმგებელი პირების მიმართ, მათ შორის წერილობითი შეთანხმებით კანონის მოთხოვნების შესრულებასთან დაკავშირებით თითოეულის ვალდებულებებისა და პასუხისმგებლობის განსაზღვრის თაობაზე, სრულად შეესაბამება ევროკავშირის რეგულაციითა და საპოლიციო დირექტივით დადგენილ სტანდარტს.[108] მსგავსად ევროკავშირის კანონმდებლობისა, საქართველოს კანონი აწესრიგებს დამუშავებისთვის პასუხისმგებელ და დამუშავებაზე უფლებამოსილ პირებს შორის სამართლებრივი ურთიერთობის სხვადასხვა ასპექტს, აგრეთვე – დადებული წერილობითი ხელშეკრულების არსებით პირობებს, ვალდებულებებისა და პასუხისმგებლობის საკითხებს.[109] განსხვავებას ქმნის ის გარემოება, რომ, GDRP-ის თანახმად, დამუშავებაზე უფლებამოსილი პირის მიერ ვალდებულებათა შესრულების სადემონსტრაციო ელემენტად შესაძლებელია გამოყენებულ იქნეს უფლებამოსილი პირის მიერ დამტკიცებულ ქცევის კოდექსთან მიერთება, რეგულაციის 40-ე მუხლის ან დამტკიცებული სერტიფიცირების მექანიზმების გამოყენება 42-ე მუხლის შესაბამისად, რასაც, თავის მხრივ, არ აწესრიგებს ეროვნული კანონმდებლობა.[110] საგულისხმოა, რომ, საპოლიციო დირექტივის თანახმად, პასუხისმგებელ და უფლებამოსილ პირებს შორის დადებული ხელშეკრულება ან სხვა სამართლებრივი აქტი უნდა გაფორმდეს წერილობით, მათ შორის – ელექტრონულად.[111]

5. მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა

[106] იხ. საქართველოს კანონის 32-ე მუხლის მე-3 და მე-7 პუნქტები, ასევე, რეგულაციის მე-7 მუხლის მე-3 და მე-4 პუნქტები.

[107] იხ. საქართველოს კანონის 32-ე მუხლის მე-8 პუნქტი და რეგულაციის მე-7 მუხლის მე-3 პუნქტი.

[108] იხ. საქართველოს კანონის 35-ე მუხლი, ევროკავშირის რეგულაციის 26-ე მუხლის და საპოლიციო დირექტივის 21-ე მუხლი.

[109] იხ.: პერსონალურ მონაცემთა დაცვის სამსახური, რეკომენდაციები დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებული ხელშეკრულების არსებითი და სტანდარტული პირობების შესახებ, 2024.

[110] იხ. რეგულაციის 28-ე მუხლის მე-5 პუნქტი.

[111] იხ. საპოლიციო დირექტივის 22-ე მუხლის მე-4 პუნქტი.

მონაცემთა საერთაშორისო გადაცემა მოწესრიგებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 37-ე – 38-ე მუხლებით, ევროკავშირის რეგულაციის 44-ე – 50-ე მუხლებითა და საპოლიციო დირექტივის 35-ე – 40-ე მუხლებით. რეგულაციის 44-ე მუხლის თანახმად, პერსონალური მონაცემების მესამე ქვეყნიდან ან საერთაშორისო ორგანიზაციიდან სხვა მესამე ქვეყანაში ან საერთაშორისო ორგანიზაციაში გადაცემა დასაშვებია მხოლოდ იმ შემთხვევაში, თუ მონაცემთა დამუშავებაში ჩართული მხარეები დაიცავენ “GDPR”-ის მოთხოვნებს იმ მიზნით, რომ რეგულაციით დადგენილი ფიზიკური პირის დაცვის გარანტიები სრულად იყოს უზრუნველყოფილი. აღნიშნულ საკითხზე საპოლიციო დირექტივის მიდგომა იდენტურია: შესაბამისი მუხლები მონაცემთა საერთაშორისო გადაცემის დასაშვებობის წინაპირობად მიიჩნევს, ერთი მხრივ, მონაცემთა დაცვის კანონმდებლობის მოთხოვნათა შესრულებას, ხოლო, მეორე მხრივ, მონაცემთა სუბიექტების უფლებათა დაცვის სათანადო გარანტიების არსებობის დადასტურებას.

აღსანიშნავია, რომ საქართველოს კანონი სრულად იზიარებს ზემოაღნიშნული საერთაშორისო აქტების მიდგომას მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემის საკითხის რეგულირებისას. კერძოდ, კანონის 37-ე მუხლის თანახმად, 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.

მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნებისა და საერთაშორისო ორგანიზაციებისთვის მონაცემთა გადაცემისათვის დამატებითი ნებართვის თვალსაზრისით, მოწესრიგება იდენტურია სამივე აქტის მიხედვით. შესაბამისი ნებართვის არსებობა საჭირო არ არის და ამგვარი ქვეყნებისა და ორგანიზაციების ნუსხა მტკიცდება შესაბამისი სამართლებრივი აქტით. საქართველოს მაგალითზე აღნიშნულ ნუსხას ამტკიცებს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი, ხოლო ევროკავშირის რეგულაციისა და საპოლიციო დირექტივის მიხედვით — ევროკომისია.

რაც შეეხება მონაცემთა დაცვის სათანადო გარანტიების დადგენისთვის აუცილებელ კრიტერიუმებს, აღნიშნულიც მაქსიმალურად იდენტურად განისაზღვრება. მსგავსად საერთაშორისო აქტებისა, საქართველოს კანონიც ყურადღებას ამახვილებს მონაცემთა დაცვის კანონმდებლობისა და საერთაშორისო ვალდებულებების შესრულების საკითხებსა და მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის გარანტიების, მათ შორის – ეფექტიანი სამართლებრივი დაცვის მექანიზმების არსებობაზე. ამ კუთხით ეროვნული კანონმდებლობის განმარტება ბევრად ფართოა და, თუკი ევროკავშირის რეგულაცია და საპოლიციო დირექტივა სამართლებრივი დაცვის მექანიზმების გამოსახატად იყენებს ტერმინს „სასამართლო პრაქტიკა“, კანონში ეს ცნება განზოგადებულია და არა მხოლოდ სამართალწარმოების შედეგად დადგენილ

პრაქტიკას მოიაზრებს, არამედ მათ შორის – საზედამხედველო ორგანოს როლს, რაც ასევე ხაზგასმულია ნორმის ტექსტში.

ეროვნულ კანონმდებლობაში ევროპული რეგულირების იდენტურად არის მოწესრიგებული მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ან/და საერთაშორისო ორგანიზაციების ნუსხის გადასინჯვის პერიოდულობა და შემოწმების შედეგად ცვლილების შეტანის წესი. მათ შორის სამივე აქტი ადგენს, რომ აღნიშნული სიის შესწორებისა და შეცვლის გადაწყვეტილებებს არ აქვთ უკუქცევითი ძალა. თავის მხრივ, საქართველოს კანონი განსაზღვრავს პერიოდულობას ნუსხის გადასინჯვის მიზნებისთვის და ადგენს შესაბამის ვადას („სულ მცირე 3 წელიწადში ერთხელ“).

როგორც რეგულაციის, ასევე დირექტივის შესაბამისობის გადაწყვეტილების საფუძველზე მონაცემთა გადაცემის მომწესრიგებელი ნორმები განსაზღვრავს ევროკომისიის ვალდებულებას[112], ევროკავშირის ოფიციალურ ბეჭდურ ორგანოსა და საკუთარ ვებგვერდზე გამოაქვეყნოს იმ მესამე ქვეყნების, მისი ნაწილის, კონკრეტული სექტორებისა და საერთაშორისო ორგანიზაციების ნუსხა, რომლებიც უზრუნველყოფენ პერსონალური მონაცემების დაცვის სათანადო გარანტიებს. ნუსხის საჯაროდ გამოქვეყნების თვალსაზრისით, საქართველოს კანონი სრულ თანხვედრაშია “GDPR”-ის მოთხოვნებთან, რადგან პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტი საჯაროდ ქვეყნდება როგორც ოფიციალურ ბეჭდვით ორგანოში, ასევე – სამსახურის ოფიციალურ ვებგვერდზე.[113]

აღსანიშნავია, რომ მონაცემთა საერთაშორისო გადაცემის დასაშვებობის კრიტერიუმად სამივე აქტი განსაზღვრავს მონაცემთა დაცვის სათანადო გარანტიებისა და მონაცემთა სუბიექტის უფლებათა დაცვის სამართლებრივი საშუალებების არსებობას, თუმცა საქართველოს კანონი აღნიშნულ ნაწილში განსხვავებული რედაქცია გვხვდება. მართალია, სამივე აქტში ჩამოთვლილია ის შემთხვევები, როდესაც მონაცემთა საერთაშორისო გადაცემისთვის სამართლებრივი საფუძველი არსებობს, თუმცა განსხვავება არის როგორც ჩამონათვალში, ასევე – პროცედურაში. ეროვნული კანონის შესაბამისი ნორმის თანახმად, მათ შორის, დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დაცვის სათანადო გარანტიების უზრუნველყოფა ხდება მონაცემთა მიმღებთან გაფორმებული ხელშეკრულებით, რა დროსაც საჭიროა ნებართვის მიღების პროცედურის გავლა. ევროკავშირის სამართალში პერსონალური მონაცემების გადაცემა მესამე ქვეყნებისა თუ საერთაშორისო ორგანიზაციებისთვის ნებადართულია ორი გზით: 1) ევროკომისიის შესაბამისობის გადაწყვეტილების საფუძველზე ან 2) თუ დამმუშავებელი ან უფლებამოსილი პირი მონაცემთა სუბიექტისათვის უზრუნველყოფს უსაფრთხოების სათანადო ზომებს, მათ შორის – აღსრულებად უფლებებსა და სამართლებრივი დაცვის საშუალებებს. კანონის 37-

[112] იხ. რეგულაციის 45-ე მუხლის მე-8 პუნქტი და საპოლიციო დირექტივის 36-ე მუხლის მე-8 პუნქტი.

[113] კანონის 38-ე მუხლის მე-2 პუნქტი; აღნიშნული ნორმის თანახმად, სამსახურის უფროსი ნორმატიულ აქტს გამოსცემს სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე. შესაბამისად, ნორმატიული აქტი თავისთავად გულისხმობს ოფიციალურ ბეჭდვით ორგანოში, საკანონმდებლო მაცნეს ვებგვერდზე გამოქვეყნებას. იხ. ელექტრონული ბმული: <https://matsne.gov.ge/ka/document/view/6119485>.

ე მუხლის მე-2 პუნქტი საკმაოდ მრავალ სამართლებრივ საფუძველს მოიცავს, რომელთა შემთხვევაშიც მონაცემთა საერთაშორისო გადაცემა დასაშვებია. მათ შორისაა: საქართველოს საერთაშორისო ხელშეკრულებითა და შეთანხმებით გათვალისწინებული მონაცემთა გადაცემის შემთხვევა; ასევე, როდესაც მონაცემთა გადაცემა გათვალისწინებულია საქართველოს სისხლის სამართლის საპროცესო კოდექსით (საგამოძიებო მოქმედების განხორციელების მიზნით), „უცხოელთა და მოქალაქეობის არმქონე პირთა სამართლებრივი მდგომარეობის შესახებ“ საქართველოს კანონით, „სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის შესახებ“ საქართველოს კანონით, „სამართალდაცვით სფეროში საერთაშორისო თანამშრომლობის შესახებ“ საქართველოს კანონით, „საქართველოს ეროვნული ბანკის შესახებ“ საქართველოს ორგანული კანონის ან „ფულის გათეთრებისა და ტერორიზმის დაფინანსების აღკვეთის ხელშეწყობის შესახებ“ საქართველოს კანონის საფუძველზე მიღებული ნორმატიული აქტით. რაც შეეხება მონაცემთა სუბიექტის თანხმობას, მნიშვნელოვან საჯარო ინტერესისა და სუბიექტის სასიცოცხლო ინტერესის საფუძველზე მონაცემთა საერთაშორისო გადაცემას, აღნიშნულს სამივე განსახილველი აქტი იცნობს და იზიარებს.

საგულისხმოა, რომ ევროკავშირის ძირითადი რეგულაციასა და საპოლიციო დირექტივაში არ არის წარმოდგენილი „პერსონალური მონაცემების მესამე ქვეყანაში ან საერთაშორისო ორგანიზაციაში საერთაშორისო გადაცემის“ სამართლებრივი დეფინიცია. “GDPR”-ის მე-4 მუხლის 23-ე პუნქტის შესაბამისად, მონაცემთა დამმუშავებელს ან უფლებამოსილ პირს აქვთ წარმომადგენლობა ერთზე მეტ წევრ სახელმწიფოში ან როდესაც მონაცემთა დამუშავება არსებით გავლენას ახდენს, ან არსებობს ალბათობა, რომ გავლენას იქონიებს მონაცემთა სუბიექტებზე ერთზე მეტ წევრ სახელმწიფოში.[114] საქართველოს კანონიც არ განმარტავს აღნიშნულ ცნებას.

გამომდინარე იქიდან, რომ “GDPR”-ში მონაცემთა საერთაშორისო გადაცემის ზუსტი დეფინიცია არ არის მოცემული, „მონაცემთა დაცვის ევროპულმა საბჭომ“ (“EDPB”) შეიმუშავა სახელმძღვანელო მონაცემთა საერთაშორისო გადაცემასთან დაკავშირებით და განსაზღვრა 3 კუმულაციური კრიტერიუმი, რომელთა შესაბამისადაც დამუშავების ოპერაცია ჩაითვლება „მონაცემთა გადაცემად“:[115]

— ***მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი („ექსპორტიორი“) ექვემდებარება ევროკავშირის ძირითად რეგულაციას მონაცემთა დამუშავების კონკრეტული მოქმედებისთვის:***

დაკმაყოფილებული უნდა იყოს რეგულაციის მე-3 მუხლის მოთხოვნები, ანუ მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი ექვემდებარებოდეს “GDPR”-ს მონაცემთა დამუშავების კონკრეტული მოქმედების მიზნებს.

[114] The EU General Data Protection Regulation (GDPR), A Commentary, Christopher Kuner, Lee A. ByGrave, Christopher Docksey, Oxford University Press, 2020, 762.

[115] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, 7-12 https://shorturl.at/kY7Ea.

— *მონაცემთა „ექსპორტიორი“ მონაცემთა გადაცემის გზით გასცემს (ამჟღავნებს) ან სხვაგვარად ხდის ხელმისაწვდომს პერსონალურ მონაცემებს მონაცემთა სხვა დამმუშავებლის, თანადამმუშავებლის ან უფლებამოსილი პირისთვის („იმპორტიორი“):*

მონაცემთა „ექსპორტიორი“ მონაცემთა გადაცემით ამჟღავნებს, ან სხვაგვარად ხელმისაწვდომს ხდის მონაცემებს სხვა მონაცემთა დამმუშავებლის ან უფლებამოსილი პირისთვის.

— *მონაცემთა „იმპორტიორი“ არის საერთაშორისო ორგანიზაცია ან იმყოფება მესამე ქვეყანაში, მიუხედავად იმისა, ექვემდებარება თუ არა აღნიშნული „იმპორტიორი“ კონკრეტული მონაცემთა დამუშავების მიზნებისთვის ევროკავშირის ძირითადი რეგულაციის მე-3 მუხლს:*

აღნიშნული კრიტერიუმის მიხედვით, მონაცემთა „იმპორტიორი“ გეოგრაფიულად იმყოფება მესამე ქვეყანაში, მიუხედავად იმისა, ვრცელდება თუ არა მასზე “GDPR”-ით განსაზღვრული წესები. „მონაცემთა დაცვის ევროპული საბჭოს“ განმარტებით, წარმოდგენილი კრიტერიუმის მიზანია პირთა შესაბამისი დაცვა, რაც გარანტირებულია რეგულაციით.

ჩამოთვლილი სამი კრიტერიუმის დაკმაყოფილებისას, სახეზე იქნება მონაცემთა გადაცემა და, შესაბამისად, გავრცელდება ძირითადი რეგულაციის V თავი. აღნიშნულის მსგავსად, საქართველოში მოქმედი საერთაშორისო გადაცემის მომწესრიგებელი წესები და დადგენილი პრაქტიკა გვაძლევს იმის თქმის საშუალებას, რომ სამივე კრიტერიუმი გაზიარებულია და კანონის აღნიშნული თავით განსაზღვრული ნორმები შეეხება კანონის მოქმედების სფეროში შემავალ დამუშავების პროცესებს, როდესაც დამუშავებაში ჩართული ერთ-ერთი მხარე, ანუ მონაცემთა მიმღები, არის სხვა სახელმწიფო ან საერთაშორისო ორგანიზაცია.

6. საზედამხედველო ორგანოს მანდატი და უფლებამოსილებათა განხორციელების ფარგლები

ევროკავშირის ძირითადი რეგულაცია იმპერატიულად ადგენს, რომ თითოეულმა წევრმა სახელმწიფომ უნდა განსაზღვროს ერთი ან მეტი დამოუკიდებელი საჯარო უწყება, რომლებიც პასუხისმგებელნი იქნებიან, ზედამხედველობა გაუწიონ ამ რეგულაციის დანერგვას პერსონალურ მონაცემთა დამუშავებისას ფიზიკური პირების ფუნდამენტური უფლებებისა და თავისუფლებების დასაცავად და ევროკავშირის მასშტაბით პერსონალურ მონაცემთა თავისუფალი მიმოცვლის ხელშესაწყობად („საზედამხედველო ორგანო“).

საქართველოს კანონი, მსგავსად ევროკავშირის სამართლისა, ითვალისწინებს საზედამხედველო ორგანოს — პერსონალურ მონაცემთა დაცვის სამსახურის,

შექმნის მნიშვნელობას და იზიარებს მისი საქმიანობის ძირითადი მიმართულებების შესახებ “GDPR”-ის მიდგომებს მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე საკონსულტაციო, კონტროლისა და მონიტორინგის, მონაცემთა დამუშავების კანონიერების შემოწმების, საჩივრების განხილვის, საზოგადოების ინფორმირებულობის გაზრდის თვალსაზრისით და სხვა.

განსხვავებით ევროკავშირის კანონმდებლობისა, საქართველოს კანონი არ შეიცავს რეგულაციებს სერტიფიცირების, აკრედიტაციისა და ავტორიზაციის კუთხით. ასევე არ შეიცავს უფლებამოსილებას „მონაცემთა დაცვის ევროპული საბჭოს“ საქმიანობის მხარდაჭერის მიმართულებით.

საგულისხმოა, რომ საზედამხედველო ორგანოს ფუნქციების მომწესრიგებელ მუხლში ძირითადი რეგულაცია ადგენს დანაწესს, რომ საზედამხედველო ორგანოს მიერ ფუნქციების შესრულება უფასო უნდა იყოს მონაცემთა სუბიექტისათვის და საჭიროების შემთხვევაში მონაცემთა დაცვის ოფიცრისათვის; თუმცა იმავდროულად აწესებს საზედამხედველო ორგანოს შესაძლებლობას, ცალსახად დაუსაბუთებელი ან გადაჭარბებულად მოცულობითი (განსაკუთრებით მათი განმეორებითი ხასიათის გამო) მოთხოვნების შესრულებაზე დააწესოს საფასური ან სათანადო დასაბუთების პირობებში თქვას უარი. ამ კუთხით საქართველოს კანონმდებლობა ნაწილობრივ შეესაბამება ევროკავშირის კანონმდებლობას — სამსახურის საქმიანობა და მონაცემთა სუბიექტის უფლებების რეალიზაციის აღნიშნული მექანიზმი, ასევე, პერსონალურ მონაცემთა დაცვის ოფიცრების ინსტიტუციურად მხარდამჭერი მექანიზმის განხორციელება, მათ შორის, საკონსულტაციო-საგანმანათლებლო მიმართულებითაც, არის უსასყიდლო. რაც შეეხება საზედამხედველო ორგანოს მხრიდან ფუნქციის შესრულებაზე უარის თქმის ან საფასურის დაწესების ნორმას, აღნიშნულს არ ითვალისწინებს საქართველოს კანონი.

6.1. საზედამხედველო ორგანოს საქმიანობის პრინციპები

ევროკავშირის ძირითადი რეგულაცია, საპოლიციო დირექტივა და საქართველოს კანონი იმპერატიულად ადგენს საზედამხედველო ორგანოს დამოუკიდებლობისა და რომელიმე ორგანოსთვის ან თანამდებობის პირისთვის დაქვემდებარების აკრძალვის პრინციპებს მასზე დაკისრებული ამოცანების შესრულებისა და უფლებამოსილების განხორციელების პროცესში. ამასთან, აღსანიშნავია, რომ საქართველოს კანონი ხსენებული პრინციპების რეალიზებისა და განმტკიცების მიზნებისთვის დეკლარირებს საზედამხედველო ორგანოზე/მის თანამშრომელზე ნებისმიერი ფორმით ზემოქმედებისა და მათ საქმიანობაში უკანონო ჩარევის დასჯადობას.

საზედამხედველო ორგანოთა შექმნის წესების მომწესრიგებელ მუხლებში “GDPR”-ი ადგენს თითოეული საზედამხედველო ორგანოს წევრის მხრიდან მის საქმიანობასთან/ვალდებულებებთან შეუსაბამო ქმედების განხორციელებისგან თავის შეკავების პრინციპს, რომელიც გათვალისწინებულია საპოლიციო

დირექტივის მიხედვითაც. საქართველოს კანონში აღნიშნული პრინციპი სამსახურის უფროსის თანამდებობრივი შეუთავსებლობის მომწესრიგებელი ნორმის სახით გვხვდება, ხოლო საზედამხედველო ორგანოს სხვა თანამშრომელთა მიმართ ინტერესთა კონფლიქტისა და თანამდებობრივი შეუთავსებლობის საკითხები ცალკე საკანონმდებლო აქტით რეგულირდება.

“GDPR”-ის არსებული დანაწესი განამტკიცებს საზედამხედველო ორგანოთა დამოუკიდებლობის პრინციპს იმ თვალსაზრისით, რომ თითოეული წევრი სახელმწიფოს ვალდებულებას წარმოადგენს, უზრუნველყოს საზედამხედველო ორგანოს შემადგენლობისა და ანგარიშვალდებულების საკითხების საკუთრივ საზედამხედველო ორგანოს მიერ მოწესრიგება. თანამშრომელთა დასაქმებისა და უფლებამოსილებათა დაკისრების წესებთან დაკავშირებით საქართველოს კანონი სწორედ ზემოაღნიშნული პრინციპისა და დანაწესის რეალიზებას ახდენს და ადგენს, რომ პერსონალურ მონაცემთა დაცვის სამსახურის სტრუქტურა, საქმიანობისა და თანამშრომელთა შორის უფლებამოსილებების განაწილების წესები დგინდება პერსონალურ მონაცემთა დაცვის სამსახურის დებულებით, რომელსაც ამტკიცებს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი. აღნიშნული პრინციპი რეალიზდება საზედამხედველო ორგანოს დაფინანსების წესებშიც. სამივე აქტი შეიცავს ნორმებს დამოუკიდებელი ბიუჯეტის არსებობის შესახებ. ევროკავშირის კანონმდებლობა მოიცავს ფინანსური კონტროლის იმგვარად განხორციელებას, რომ ხელი არ შეეშალოს ორგანოს დამოუკიდებელ საქმიანობას. საქართველოს კანონი ფინანსური ინსტრუმენტების გამოყენებით საქმიანობის დამოუკიდებლობაში ჩარევის პრევენციის კონკრეტულ მექანიზმს ადგენს — ნორმა ხარჯების შემცირებას მხოლოდ სამსახურის უფროსის წინასწარ თანხმობას უკავშირებს.

6.2. საზედამხედველო ორგანოს შექმნის წესები

ევროკავშირის ძირითადი რეგულაციის თანახმად, „წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ საზედამხედველო ორგანოს თითოეული წევრი დაინიშნოს გამჭვირვალე პროცედურით და არჩეულ იქნეს პარლამენტის, მთავრობის, სახელმწიფოს მეთაურის ან დამოუკიდებელი ორგანოს მიერ, რომელსაც არჩევის უფლებამოსილება ენიჭება წევრი სახელმწიფოს კანონმდებლობით“.[116]

ქართულმა კანონმდებლობამ “GDPR”-ით განსაზღვრული ალტერნატივებიდან საპარლამენტო გზა აირჩა. აღსანიშნავია, რომ საერთაშორისო აქტები (როგორც რეგულაცია, ასევე საპოლიციო დირექტივა) აწესრიგებს საზედამხედველო ორგანოს ხელმძღვანელის არჩევის წესს, ხოლო ეროვნული კანონმდებლობით პარლამენტის მიერ ირჩევა მხოლოდ სამსახურის უფროსი, სამსახურში დასაქმებული სხვა პირების მიმართ კი საკადრო გადაწყვეტილება მიიღება სამსახურის უფროსის მიერ.

[116] იხ. რეგულაციის 53-ე მუხლის პირველი პუნქტი.

ეროვნული ნორმა ადგენს სამსახურის უფროსის კანდიდატურისათვის წაყენებულ მოთხოვნებს მაშინ, როდესაც ძირითადი რეგულაცია და საპოლიციო დირექტივა საზედამხედველო ორგანოს წევრთა მიმართ მხოლოდ საგნობრივი ცოდნისა და გამოცდილების ქონის ვალდებულებას განსაზღვრავს. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 41-ე მუხლის პირველი პუნქტის თანახმად: „პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის თანამდებობაზე შეიძლება არჩეულ იქნეს საქართველოს მოქალაქე, რომელიც არ არის ნასამართლევი და რომელსაც აქვს უმაღლესი იურიდიული განათლება და მართლმსაჯულების ან სამართალდამცავი ორგანოების სისტემაში ან ადამიანის უფლებათა დაცვის სფეროში მუშაობის არანაკლებ 5 წლის გამოცდილება და მაღალი პროფესიული და მორალური რეპუტაცია.“ კანონით მოწესრიგებულია საზედამხედველო ორგანოს თანამშრომელთა უფლებამოსილების შეწყვეტის საფუძვლებიც: უფლებამოსილების ვადის ამოწურვა, გადადგომა, სავალდებულო საპენსიო ასაკის მიღწევა; ასევე — პერსონალურ მონაცემთა დაცვის სამსახურის უფროსს უფლებამოსილების ვადამდე შეწყვეტის განსხვავებული წინაპირობები: საქართველოს მოქალაქეობის დაკარგვა, ჯანმრთელობის მდგომარეობა, კანონიერ ძალაში შესული სასამართლოს გამამტყუნებელი განაჩენის არსებობა, სტატუსთან შეუთავსებელი თანამდებობის დაკავება და სხვა. რაც შეეხება ვადამდე გათავისუფლების საკითხს, ერთ-ერთ საფუძვლად, მსგავსად საერთაშორისო აქტებისა,[117] საქართველოს კანონი ითვალისწინებს უფლებამოსილებების შეუსრულებლობისა და სასამართლოს გამამტყუნებელი განაჩენის კანონიერ ძალაში შესვლის შემთხვევებს.

“GDPR”-ის მოწესრიგება საზედამხედველო ორგანოს შექმნის წესების, მის წევრთა თანამდებობაზე არჩევისა და დანიშვნისთვის აუცილებელი საკვალიფიკაციო მოთხოვნების, საქმიანობა უფლებამოსილების განხორციელების პროცესში და ვადის ამოწურვის შემდეგ, მოქმედებებისა და შეღავათების აკრძალვებისა და საქმიანობის შეწყვეტის თაობაზე ქართულ კანონმდებლობაში შემდეგნაირად აისახა: განისაზღვრა პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის უფლებამოსილების ვადა, დადგინდა არჩევის ჯერადობა. როგორც რეგულაცია, ასევე საპოლიციო დირექტივა კანონმდებელს ანიჭებს პრეროგატივას, კანონით განსაზღვროს საზედამხედველო ორგანოს ხელმძღვანელი პირის ხელახლა არჩევის საკითხი. საქართველოს კანონის თანახმად, პირი პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის თანამდებობაზე არ შეიძლება არჩეულ იქნეს ზედიზედ ორჯერ.

ევროკავშირის კანონმდებლობა ასევე ადგენენ საზედამხედველო ორგანოს წევრების ვალდებულებას, დაიცვან კონფიდენციალურობის პრინციპი როგორც სამსახურებრივი საქმიანობის დროს, ასევე – უფლებამოსილების შეწყვეტის შემდგომაც. საქართველოს კანონის თანახმად, პერსონალურ მონაცემთა დაცვის სამსახურის თანამშრომელი ვალდებულია, დაიცვას ნებისმიერი სახის საიდუმლოების შემცველი ინფორმაციის უსაფრთხოება და არ გაამჟღავნოს მისთვის სამსახურებრივი მოვალეობის შესრულების დროს მიღებული მონაცემები. აღნიშნული ვალდებულება, მსგავსად საერთაშორისო რეგულაციისა, პერსონალურ

[117] იხ. რეგულაციის 53-ე მუხლის მე-4 პუნქტი; საპოლიციო დირექტივის 43-ე მუხლის მე-4 პუნქტი.

მონაცემთა დაცვის სამსახურის თანამშრომელს უფლებამოსილების შეწყვეტის შემდეგაც უნარჩუნდება.

6.3. საზედამხედველო ორგანოს უფლებამოსილება მონაცემთა დამუშავების კანონიერების შესწავლის მიმართულებით

მონაცემთა დამუშავების ფაქტების/გარემოებების შესწავლის/ინსპექტირების მიმართულებით საზედამხედველო ორგანოს უფლებამოსილებათაგან ევროკავშირის ძირითადი რეგულაცია, საპოლიციო დირექტივა და საქართველოს კანონი მსგავს ღონისძიებებს ითვალისწინებს, რომლებიც უშუალოდ დარღვევის დადგენის შემთხვევაში გამოიყენება. ამ თვალსაზრისით განსხვავება ვლინებდა აკრედიტაცია-ავტორიზაციის, სერტიფიცირებისა და სავალდებულო კორპორაციული წესების დადგენის უფლებამოსილებებში, რასაც ქართული კანონმდებლობა არ არის ითვალისწინებს. ამასთან, საქართველოს კანონის თანახმად, საზედამხედველო ორგანოს ფუნქციაში შედის ფარული საგამოძიებო მოქმედებების ჩატარებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობის კონტროლი.

"GDPR"-ს საზედამხედველო ორგანოებს ანიჭებს როგორც გამოსასწორებელი ღონისძიებების,[118] ასევე რეგულაციის 83-ე მუხლით გათვალისწინებული ადმინისტრაციული ჯარიმების დაწესების შესაძლებლობას.[119] აღსანიშნავია, რომ ზოგიერთი სახელმწიფო აღნიშნულ საკითხს "GDPR"-თან ერთად დამატებითი, ეროვნული კანონმდებლობის საშუალებით არეგულირებს. ძირითადი რეგულაციის 83-ე მუხლის პირველი პუნქტის თანახმად, ჯარიმები უნდა იყოს „ეფექტიანი, პროპორციული და პრევენციული" ფუნქციის, განსაზღვრული იმ რაოდენობით, რომელიც არ წაახალისებს მონაცემთა დამუშავების კანონის მოთხოვნებთან შეუსაბამო პრაქტიკის შემდგომში განხორციელებას.[120] თუმცა, რეგულაციის ამავე მუხლის მე-7 პუნქტი წევრ სახელმწიფოებს უტოვებს თავისუფალ ნებას, რომ თავად გადაწყვიტონ საჯარო დაწესებულებათა დაჯარიმების საკითხი და ადმინისტრაციული ჯარიმის ოდენობა. აღნიშნული წარმოშობს სამართლებრივ რეგულირებასთან დაკავშირებულ განსხვავებებს. კერძოდ, ზოგიერთი წევრი სახელმწიფოს საჯარო უწყება მონაცემთა დაცვასთან დაკავშირებული დარღვევისთვის ადმინისტრაციული წესით არ ჯარიმდება, ხოლო ზოგიერთ წევრ სახელმწიფოში აღნიშნული დარღვევისთვის დაწესებულებები ისევე ჯარიმდებიან, როგორც კერძო კომპანიები. საგულისხმოა, რომ „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი

[118] იხ. რეგულაციის 58-ე მუხლი.

[119] *Bovens M.,* Analysing and Assessing Accountability: A Conceptual Framework, in: *European Law Journal, 13*(4), 2007, 447-468.

[120] *Ayres I., Braithwaite J., Responsive Regulation: Transcending the Deregulation Debate,* Oxford University Press,1992.

პერსონალურ მონაცემთა დაცვის სამსახურს ანიჭებს უფლებამოსილებას, რომ სამართალდარღვევათა გამოვლენის შემთხვევაში, საქართველოს კანონმდებლობით გათვალისწინებული ღონისძიებები განახორციელოს როგორც საჯარო, ისევე კერძო სექტორის წარმომადგენელი უწყების თუ ორგანიზაციის მიმართ.[121]

საგულისხმოა, საზედამხედველო ორგანოს საქმიანობის წლიური ანგარიში, საქმიანობის გამჭვირვალობის პრინციპის უზრუნველსაყოფად, საჯაროა და მისი ხელმისაწვდომობა გარანტირებულია როგორც რეგულაციის, ასევე – დირექტივის თანახმად. ევროპული რეგულაციების მსგავსად, ანგარიშის საჯაროობა დადგენილია საქართველოს კანონითაც; თუმცა, საერთაშორისო აქტებისგან განსხვავებით, კანონი დამატებით შეიცავს სპეციალური ანგარიშის წარდგენის მომწესრიგებელ ნორმასაც — პერსონალურ მონაცემთა დაცვის სამსახური უფლებამოსილია საკუთარი ინიციატივით ნებისმიერ დროს გამოაქვეყნოს სპეციალური ანგარიში იმ საკითხების თაობაზე, რომლებიც მის საქმიანობას უკავშირდება და მას მნიშვნელოვნად მიაჩნია.

6.4. საზედამხედველო ორგანოში საჩივრის წარდგენის წესი

პირის უფლებას, საკუთარი უფლების დასაცავად წარადგინოს საჩივარი საზედამხედველო ორგანოში, მიღებული გადაწყვეტილება გაასაჩივროს სასამართლოში და დავა აწარმოოს დამუშავებისთვის პასუხისმგებელი ან უფლებამოსილი პირის წინააღმდეგ, განსაზღვრავენ “GDPR”-ის 77-ე, 78-ე და 79-ე მუხლები და დირექტივის 52-ე მუხლი. შესაბამისად, საზედამხედველო ორგანოს აქვს დისკრეციული უფლებამოსილება, შეისწავლოს უფლების დარღვევასთან დაკავშირებული საჩივარი. ამ თვალსაზრისით ასევე გასათვალისწინებელია “GDPR”-ის 57-ე მუხლის პირველი პუნქტის „ვ“ ქვეპუნქტი, რომელიც ადგენს საზედამხედველო ორგანოს ფუნქციებს საჩივრის განხილვასთან დაკავშირებით: საჩივრის განხილვა უნდა მიმდინარეობდეს სათანადო ზრუნვითა და კანონმდებლობის სრული დაცვით. ამავე დროს, საზედამხედველო ორგანოს მიერ მიღებული გადაწყვეტილება უნდა იყოს სამართლებრივად დასაბუთებული როგორც დაკმაყოფილების, ასევე – დაკმაყოფილებაზე უარის თქმის შემთხვევაში.[122]

ანალოგიური დათქმა გვხვდება საქართველოს კანონშიც, კერძოდ, კანონის 22-ე მუხლის პირველ პუნქტსა და 50-ე მუხლის მე-2 და მე-7 პუნქტებში. გასათვალისწინებელია, რომ განცხადების/საჩივრის/შეტყობინების განხილვის დროს სამსახური კანონთან ერთად ხელმძღვანელობს სამსახურის უფროსის 2024 წლის 1 მარტის №34 ბრძანებით დამტკიცებული „პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის წესით“.

[121] იხ. კანონის 52-ე მუხლი.

[122] Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements, version 1.0, adopted on 2 feb., 2021.

7. სასამართლოსთვის მიმართვის უფლება

ევროკავშირის ძირითადი რეგულაციის 78-ე მუხლის პირველი პუნქტში ასახულია ზოგადი პრინციპი სასამართლოში საჯარო დაწესებულების მიერ მიღებული გადაწყვეტილების გასაჩივრების თაობაზე. შესაბამისად, აღნიშნული ნორმის დისპოზიციიდან გამომდინარე, მონაცემთა სუბიექტს აქვს უფლება თავისი ინტერესების დასაცავად მიმართოს სასამართლოს და გაასაჩივროს საზედამხედველო ორგანოს მიერ მის მიმართ მიღებული გადაწყვეტილება. საზედამხედველო ორგანოს მიერ მიღებული გადაწყვეტილების გასაჩივრების უფლება გათვალისწინებულია ასევე საპოლიციო დირექტივის 53-ე მუხლში. საქართველოს კანონის 22-ე მუხლის პირველი პუნქტითა და 63-ე მუხლის პირველი პუნქტებით განსაზღვრულია ზოგადი წესი, რომლის მიხედვითაც, პირს აქვს შესაძლებლობა კანონით დადგენილ ვადაში სასამართლოში გაასაჩივროს სამსახურის უფროსის მიერ მიღებული გადაწყვეტილება. ამავდროულად, "GDPR"-ის 78-ე მუხლის მე-2 პუნქტი ადგენს მონაცემთა სუბიექტის მხრიდან სასამართლოსადმი მიმართვის კონკრეტულ ვადას („იმ შემთხვევაში თუკი პირის განაცხადი არ იქნება განხილული 3 თვის ვადაში ან მას არ ეცნობება 77-ე მუხლში გათვალისწინებული ინფორმაცია, სუბიექტს წარმოეშობა უფლება, საკუთარი ინტერესების დასაცავად მიმართოს სასამართლოს").

რეგულაციის 79-ე მუხლის პირველი პუნქტი ადგენს მონაცემთა სუბიექტის ეფექტიანი სასამართლო დაცვის უფლებას, როდესაც სუბიექტი მიიჩნევს, რომ მისი მონაცემები მუშავდება "GDPR"-ით გათვალისწინებული წესების დარღვევით; ხოლო 79-ე მუხლის მეორე პუნქტი შეეხება იურისდიქციას. როგორც უკვე აღინიშნა, კანონის 22-ე მუხლის პირველი პუნქტი განამტკიცებს პირის შესაძლებლობას კანონით გათვალისწინებული უფლებებისა და კანონით დადგენილი წესების დარღვევის შემთხვევაში მიმართოს სამსახურს, სასამართლოს ან/და ზემდგომ ადმინისტრაციულ ორგანოს, რაც ანალოგიური/იდენტური სახით არის მოწესრიგებული საპოლიციო დირექტივის 53-ე მუხლში.

8. კომპენსაცია პერსონალური მონაცემების დამუშავების დარღვევისთვის

საგულისხმოა, რომ, პერსონალურ მონაცემთა დამუშავების ცალკეული გადაცდომების პირობებში, ევროკავშირის ძირითადი რეგულაციის 82-ე მუხლით და საპოლიციო დირექტივის 56-ე მუხლით განსაზღვრულია მონაცემთა სუბიექტის მხრიდან კომპენსაციის/ანაზღაურების მიღების უფლება. აღნიშნული მოწესრიგების მიზანია იმ პირის უფლებრივი მდგომარეობის აღდგენა, რომელსაც მონაცემთა უკანონო დამუშავებით მიადგა მატერიალური ან მორალური ზიანი. მიუხედავად იმისა, რომ საკითხს სპეციალური ნორმით აწესრიგებს ევროპული კანონმდებლობა, აღნიშნულ ნორმათა მსგავსი დისპოზიცია არ არის

გათვალისწინებული საქართველოს კანონში, თუმცა ზიანის ანაზღაურების მოთხოვნის უფლება დარეგულირებულია სამოქალაქო კოდექსით.

9. ადმინისტრაციული სახდელის დადების ზოგადი წესები და პირობები

ადმინისტრაციული ჯარიმების დაკისრების წინაპირობებისა და პროცედურების თვალსაზრისით, საქართველოს კანონი იზიარებს ევროკავშირის ძირითადი რეგულაციის 83-ე მუხლის სულისკვეთებას, თუმცა მას ნაწილობრივ შეესაბამება. კერძოდ, განსხვავებული წესია დადგენილი ჯარიმის გამოთვლის ნაწილში: "GDPR"-ის მიხედვით, ჯარიმის ოდენობა დაკავშირებულია იურიდიული პირის წლიური ბრუნვასთან, კერძოდ, ადმინისტრაციული ჯარიმა შეადგენს 10 000 000 ევრომდე ან საწარმოს შემთხვევაში – გასული ფინანსური წლის მთლიანი წლიური ბრუნვის 2%-მდე ოდენობას (გამოიყენება ის სანქცია, რომელიც უფრო მაღალია).

საგულისხმოა, რომ კანონი, ევროკავშირის ძირითადი რეგულაციისა და საპოლიციო დირექტივისგან განსხვავებით, ფიქსირებული ჯარიმის ოდენობებს განსაზღვრავს, თუმცა, 2024 წლის 1-ელ მარტამდე მოქმედი კანონით გათვალისწინებულ სანქციებთან მიმართებით, საგრძნობლად გაზრდილია მათი მოცულობა. კერძოდ, კანონმდებელმა ჯარიმის ოდენობა დაუკავშირდა სამართალდამრღვევის ორგანიზაციულ ფორმასა და მის წლიურ ბრუნვას. ამასთან, ჯარიმის ოდენობა იურიდიული პირისთვის გამოიანგარიშება არა მისი წლიური ბრუნვის პროცენტის მიხედვით, არამედ კონკრეტული თანხით — 10 000 ლარით, თუკი წლიური ბრუნვა 500 000 ლარს არ აღემატება, და 20 000 ლარით, თუკი წლიური ბრუნვა 500 000 ლარს სცდება. მაგალითად: კანონით გათვალისწინებული მონაცემთა დამუშავების რომელიმე პრინციპის დარღვევა იწვევს ფიზიკური პირის, საჯარო დაწესებულების, არასამეწარმეო (არაკომერციული) იურიდიული პირის, აგრეთვე იურიდიული პირის, უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის, რომელთა წლიური ბრუნვა 500 000 ლარს არ აღემატება, გაფრთხილებას ან დაჯარიმებას 1 000 ლარის ოდენობით; ხოლო იგივე ქმედების ჩადენა იურიდიული პირის (გარდა არასამეწარმეო (არაკომერციული)იურიდიული პირისა), უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის, რომელთა წლიური ბრუნვა 500 000 ლარს აღემატება, გამოიწვევს მათ გაფრთხილებას ან დაჯარიმებას 2 000 ლარის ოდენობით. შესაბამისად, კანონით გათვალისწინებულია სანქციათა გაზრდილი ზღვრული ოდენობა, რომელიც შეიძლება შეეფარდოს სამართალდამრღვევ პირს მისი სამართლებრივი სტატუსისა და შემოსავლების გათვალისწინებით.

აღსანიშნავია, რომ საქართველოს კანონში ერთმანეთისგან გამიჯნულია დამამძიმებელი და შემამსუბუქებელი გარემოებები, ხოლო ევროკავშირის ძირითადი რეგულაციის 83-ე მუხლის მე-2 პუნქტი ითვალისწინებს დათქმას იმის თაობაზე, თუ რომელ გარემოებებს უნდა მიექცეს ყურადღება ადმინისტრაციული ჯარიმის დაკისრების ან მისი ოდენობის განსაზღვრისას. ამავდროულად,

საქართველოს კანონსა და მონაცემთა დაცვის ძირითად რეგულაციაში ჩამოთვლილი პასუხისმგებლობის დამამძიმებელი და შემამსუბუქებელი გარემოებები ერთმანეთის იდენტური არ არის. მაგალითად, საქართველოს კანონში შემამსუბუქებელ გარემოებას წარმოადგენს შემთხვევა, როდესაც სამართალდარღვევა ჩადენილია არასრულწლოვნის მიერ, "GDPR"-ი კი არ ითვალისწინებს შეაბამის მოწესრიგებას. ევროკავშირის რეგულაციის თანახმად, სახდელის დადებისა და ოდენობის განსაზღვრის დროს გასათვალისწინებელია, ჩადენილია თუ არა მონაცემთა დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირის მიერ მსგავსი დარღვევები. რაც შეეხება საქართველოს კანონს, მასში გადაცდომის განმეორებით ჩადენილად მისაჩნევად და დამამძიმებელი გარემოების არსებობის შესაფასებლად დაკონკრეტებულია დროის პერიოდი, კერძოდ, დამამძიმებელ გარემოებას წარმოადგენს ერთი წლის განმავლობაში იმავე ადმინისტრაციული სამართალდარღვევის განმეორებით ჩადენა. საქართველოს კანონი შემამსუბუქებელი გარემოების შემთხვევაში გარკვეული პროცენტით იძლევა ჯარიმის ოდენობის შემცირების შესაძლებლობას, რაც ევროკავშირის რეგულაციის 83-ე მუხლით არ არის განსაზღვრული.

ჯარიმის ოდენობის გამოთვლის პროცესში უნდა შეფასდეს საქმისთვის მნიშვნელობის მქონე თითოეული გარემოება და შემდგომ უნდა იქნეს მიღებული გადაწყვეტილება ჯარიმის საბოლოო ოდენობის დაკისრების შესახებ.[123] ამ დათქმას სრულად შეესაბამება საქართველოს კანონის 61-ე — 64-ე მუხლები, რომლებიც ჯარიმის ოდენობის გამოთვლის პროცესში, შემამსუბუქებელი და დამამძიმებელი გარემოების შეფასებისა და ურთიერთშეჯერების შესაძლებლობას იძლევა.

სანქციათა განსაზღვრის თვალსაზრისით, ევროკავშირის ძირითადი რეგულაციის 84-ე მუხლი ასახავს წევრი სახელმწიფოების როლს და ადგენს, რომ წევრმა სახელმწიფოებმა მიიღონ ეროვნული კანონმდებლობა, რომელიც განსაზღვრავს სანქციებს "GDPR"-ის დარღვევისთვის, რაც თავის მხრივ არ არის გათვალისწინებული 83-ე მუხლით. მართალია, აღნიშნული ნორმის დისპოზიცია მიემართება ევროკავშირის წევრ სახელმწიფოებს, თუმცა საქართველოს კანონის 52-ე მუხლით განსაზღვრულია სამსახურის უფლებამოსილება, კანონის ან მონაცემთა დამუშავების მომწესრიგებელი სხვა ნორმატიული აქტის დარღვევის შემთხვევაში პირს მოსთხოვოს შემდეგი ღონისძიებებიდან ერთ-ერთის ან რამდენიმეს შესრულება: ა) მოითხოვოს დარღვევისა და მონაცემთა დამუშავებასთან დაკავშირებული ნაკლოვანებების გამოსწორება მის მიერ მითითებული ფორმით და მითითებულ ვადაში; ბ) მოითხოვოს მონაცემთა დამუშავების დროებით ან სამუდამოდ შეწყვეტა, თუ დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა უსაფრთხოების დაცვისთვის განხორციელებული ღონისძიებები და პროცედურები არ შეესაბამება საქართველოს კანონმდებლობით დადგენილ მოთხოვნებს; გ) მოითხოვოს მონაცემთა დამუშავების შეწყვეტა, მონაცემთა დაბლოკვა, წაშლა, განადგურება ან დეპერსონალიზაცია, თუ მიიჩნევს, რომ მონაცემთა დამუშავება საქართველოს კანონმდებლობის დარღვევით ხორციელდება; დ) მოითხოვოს მონაცემთა სხვა

[123] EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR Version 2.1, Adopted on 24 May 2023

სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემის შეწყვეტა, თუ მონაცემთა გადაცემა საქართველოს კანონმდებლობის დარღვევით ხორციელდება; ე) წერილობით მისცეს რჩევები და გაუწიოს რეკომენდაცია დამუშავებისთვის პასუხისმგებელ პირს ან/და დამუშავებაზე უფლებამოსილ პირს მის მიერ მონაცემთა დამუშავებასთან დაკავშირებული წესების უმნიშვნელოდ დარღვევის შემთხვევაში; ვ) სამართალდამრღვევს დააკისროს ადმინისტრაციული პასუხისმგებლობა.

10. საგამონაკლისო შემთხვევები

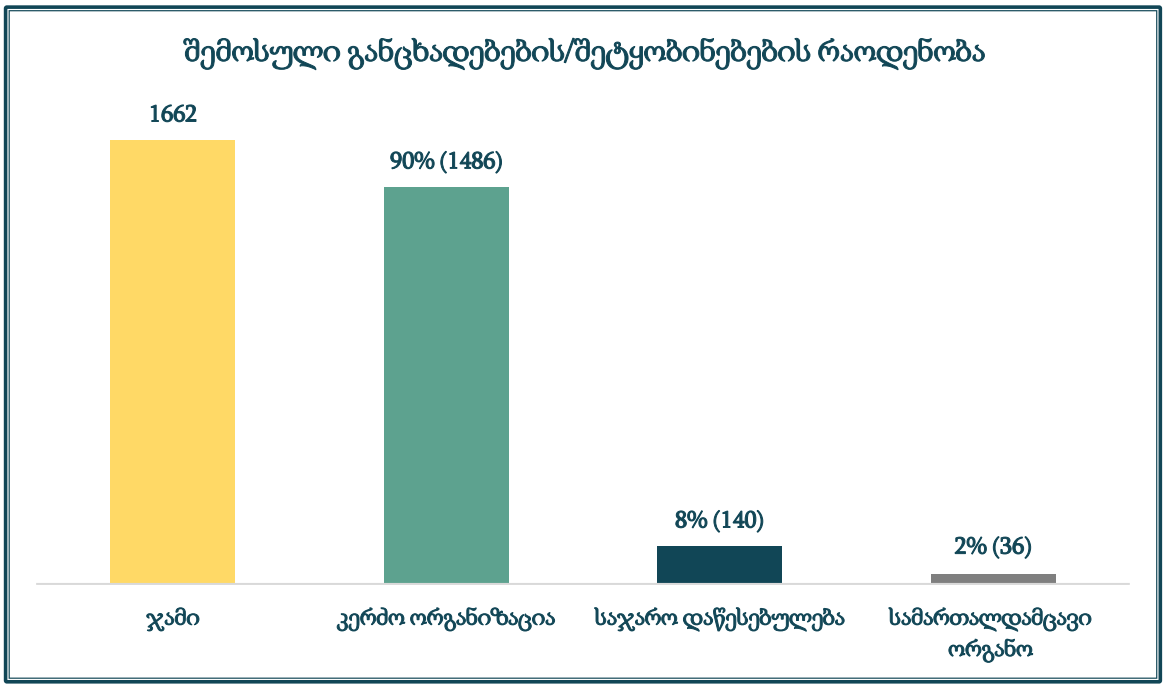
ევროკავშირის ძირითადი რეგულაციის 85-ე მუხლი უზრუნველყოფს ბალანსს პერსონალური მონაცემების დაცვასა და გამოხატვის თავისუფლებას შორის და ადგენს, რომ გარკვეულ შემთხვევაში პერსონალური მონაცემების დამუშავება აუცილებელია გამოხატვისა და ინფორმაციის თავისუფლების განსახორციელებლად, რაც მოიცავს გამოხატვის თავისუფლებას, ჟურნალისტურ საქმიანობასა და ინფორმაციის ხელმისაწვდომობას. ამავე ნორმით გათვალისწინებულია გამონაკლისები აკადემიური, სახელოვნო და ლიტერატურული მიზნით მონაცემთა დამუშავებასთან დაკავშირებით. საგულისხმოა, რომ ხსენებული რეგულაციები სრულად არის ასახული საქართველოს კანონშიც, კერძოდ, კანონის მე-2 მუხლის მე-2 პუნქტის „ე“ და „ვ“ ქვეპუნქტებში.

გარდა ამისა, “GDPR”-ის 89-ე მუხლი ადგენს, რომ პერსონალური მონაცემების დამუშავება, რომელიც განხორციელებულია საზოგადოებრივი ინტერესებიდან გამომდინარე და მოიცავს სამეცნიერო, ისტორიული კვლევების ან სტატისტიკურ მიზნებს, უნდა დაექვემდებაროს შესაბამისი დაცვის ღონისძიებებს, რათა მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების უზრუნველყოფის ინტერესიდან გამომდინარე. აღნიშნულის მიზანია მონაცემთა დამუშავების მინიმიზაციის პრინციპის დაცვა იმგვარი ტექნიკური და ორგანიზაციული ზომების მიღებით, როგორებიცაა ანონიმიზაცია და ფსევდონიმიზაცია. ამასთან, ნორმის პირველი პუნქტი ხაზს უსვამს არა მარტო მინიმიზაციის პრინციპის მნიშვნელობას, არამედ – კონფიდენციალურობისა და მონაცემთა დაცვის მნიშვნელობას.[124] მსგავს რეგულაციას ითვალისწინებს საპოლიციო დირექტივის მე-4 და მე-9 მუხლებიც. საგულისხმოა, რომ საქართველოს კანონის არაერთი ნორმა (მაგალითად, მე-4 მუხლის მე-6 პუნქტი, მე-6 მუხლის „მ“ ქვეპუნქტი, მე-16 მუხლის მე-3 პუნქტის „დ“ ქვეპუნქტი) ადგენს საჯარო ინტერესებისთვის არქივირების, სამეცნიერო ან ისტორიული კვლევის, ან სტატისტიკური მიზნებისთვის მონაცემთა დამუშავების სათანადო გარანტიებს.

[124] EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, adopted on 21 Apr. 2020, 11

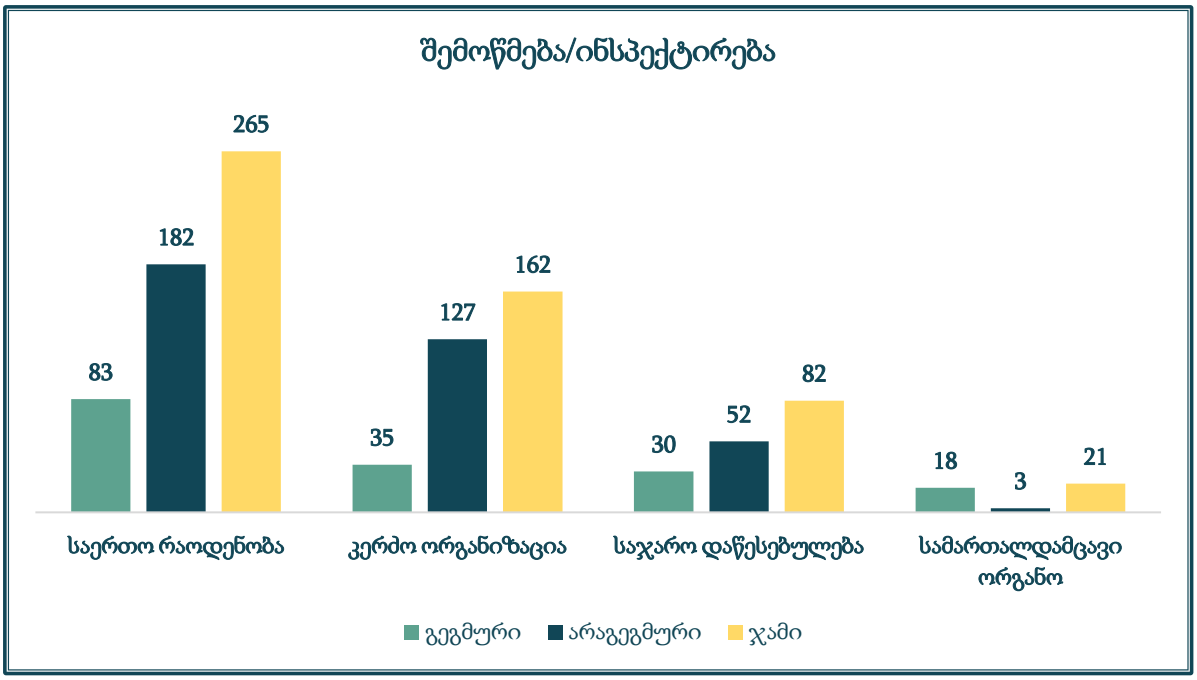
დანართი №2: სტატისტიკური მონაცემი

1. მონაცემთა დამუშავების კანონიერების კონტროლის სტატისტიკა



საანგარიშო პერიოდში სამსახურმა ჯამურად მიიღო 1662 განცხადება/შეტყობინება, მათგან 52% (863) — განცხადება, ხოლო 48% (799) – შეტყობინება. შემოსულ განცხადებათა/შეტყობინებათა 90% (1486) შეეხებოდა მონაცემთა დამუშავებას კერძო ორგანიზაციებში, 8% (140) – საჯარო უწყებებში, ხოლო 2% (36) – სამართალდამცავ ორგანოებში.

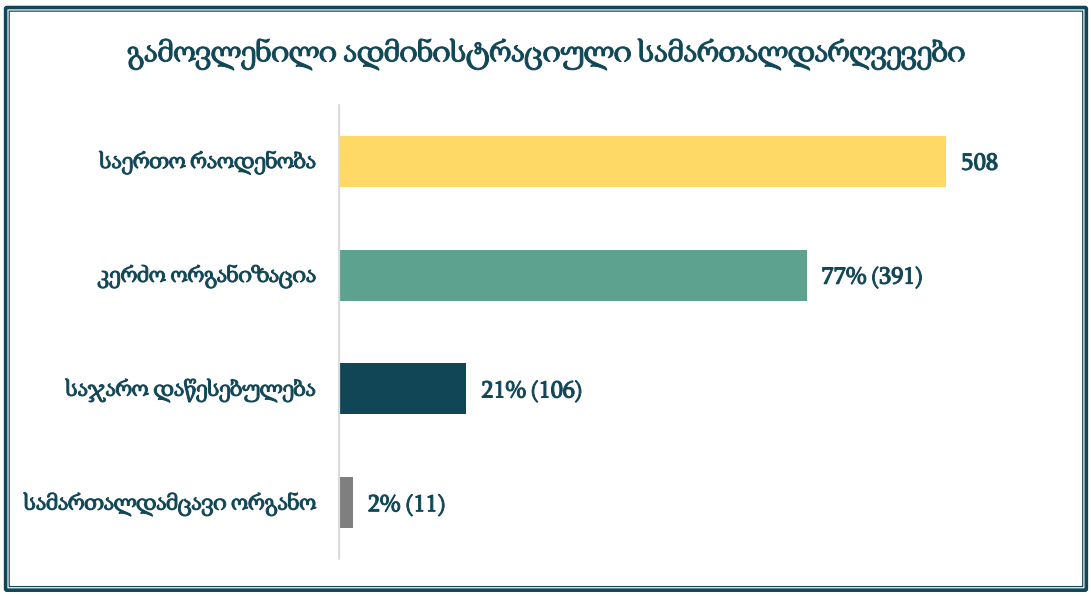
აღსანიშნავია, რომ 2023 წელთან შედარებით მკვეთრად გაზრდილია შემოსული განცხადებების/შეტყობინებების რაოდენობა. კერძოდ, 2023 წელს სამსახურმა ჯამურად მიიღო 526 განცხადება/შეტყობინება, მათგან 83% (436) იყო განცხადება, ხოლო 17% (90) – შეტყობინება. შემოსულ განცხადებათა/ შეტყობინებათა 66% (350) შეეხებოდა კერძო დაწესებულებების/ფიზიკური პირების მიერ მონაცემთა დამუშავებას, 23% (120) შეეხებოდა საჯარო დაწესებულების მიერ მონაცემთა დამუშავებას, ხოლო 11% (56) – სამართალდამცავ ორგანოებს.



2024 წელს სამსახურმა ჩაატარა მონაცემთა დამუშავების კანონიერების შემოწმება (ინსპექტირება) 265 ფაქტზე. მათგან 31% (83) ჩატარდა გეგმურად, ხოლო 69% (182) – არაგეგმურად. ჩატარებული 265 შემოწმებიდან (ინსპექტირებიდან) 61% (162) შეეხებოდა კერძო სექტორის, 31% (82) საჯარო დაწესებულებების, ხოლო 8% (21) სამართალდამცავი ორგანოების მიერ მონაცემთა დამუშავების კანონიერების შემოწმებას.

2023 წელს სამსახურმა ჩაატარა პერსონალურ მონაცემთა დამუშავების კანონიერების 192 შემოწმება (ინსპექტირება), რომელთაგან 59% (114 შემოწმება) იყო არაგეგმური, ხოლო 41% (78 შემოწმება) – გეგმური. ჩატარებული 192 შემოწმებიდან (ინსპექტირებიდან) 54% (103) შეეხებოდა კერძო სექტორის, 32% (62) საჯარო დაწესებულებების, ხოლო 14% (27) სამართალდამცავი ორგანოების მიერ მონაცემთა დამუშავების კანონიერების შემოწმებას.

ადმინისტრაციული სამართალდარღვევები



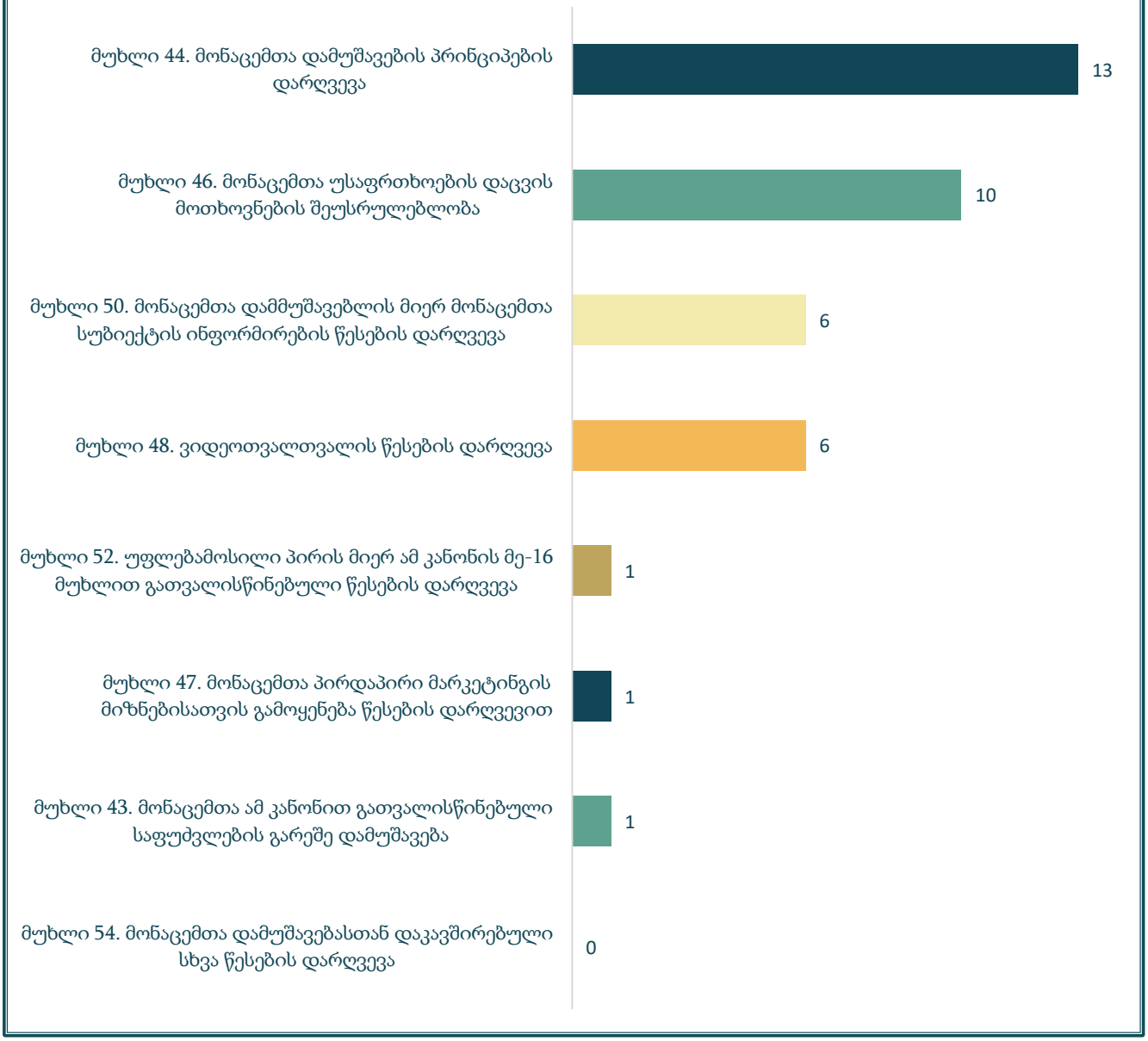
2024 წელს სამსახურმა დაადგინა პერსონალურ მონაცემთა არაკანონიერი დამუშავების 508 ფაქტი, მათგან 29 ფაქტი გამოვლინდა 2023 წელს დაწყებული და საანგარიშო პერიოდში დასრულებული, ხოლო 479 ფაქტი – საანგარიშო პერიოდში დაწყებული და დასრულებული შემოწმების (ინსპექტირების) საფუძველზე. 77% (391) შემთხვევა შეეხებოდა კერძო სექტორში, 21% (106) – საჯარო სექტორში, ხოლო 2% (11) – სამართალდამცავ ორგანოებში მონაცემთა არაკანონიერ დამუშავებას.

აღსანიშნავია, რომ 2023 წელთან შედარებით გაიზარდა გამოვლენილი სამართალდარღვევების რაოდენობა. 2023 წელს სამსახურმა დაადგინა პერსონალურ მონაცემთა არაკანონიერი დამუშავების 267 ფაქტი, მათგან 39 ფაქტი გამოვლინდა 2022 წელს დაწყებული და საანგარიშო პერიოდში დასრულებული, ხოლო 228 ფაქტი – საანგარიშო პერიოდში დაწყებული და დასრულებული შემოწმების (ინსპექტირების) საფუძველზე. 63% (168) შემთხვევა შეეხებოდა კერძო სექტორში, 26% (70) საჯარო სექტორში, ხოლო 11% (29) სამართალდამცავ ორგანოებში მონაცემთა არაკანონიერ დამუშავებას.

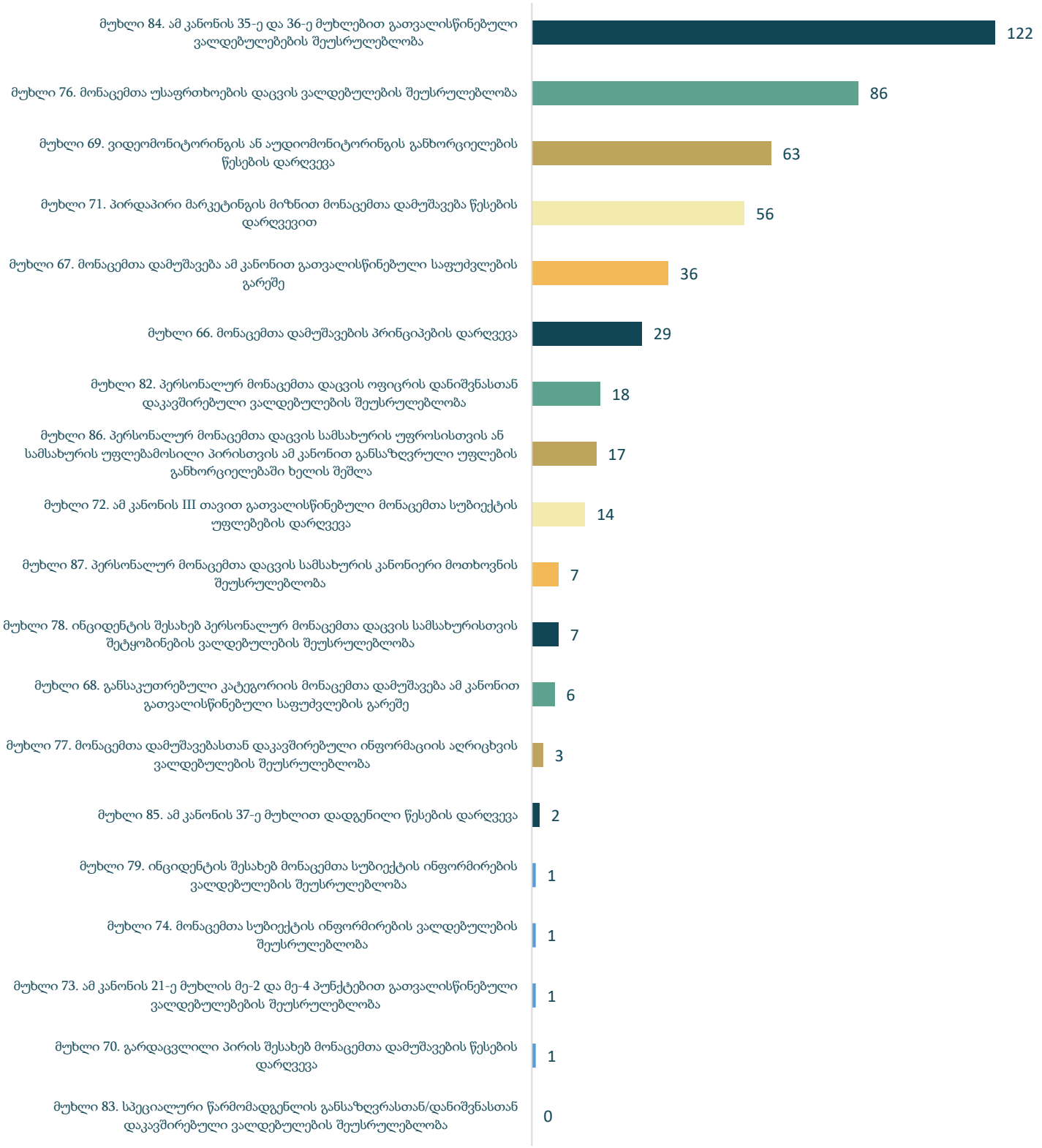
გამოვლენილი ადმინისტრაციული სამართალდარღვევები

2024 წლის პირველი მარტიდან ამოქმედდა „პერსონალურ მონაცემთა დაცვის შესახებ“. აღნიშნულიდან გამომდინარე, 2024 წლის იანვარი-თებერვლის სტატისტიკური ინფორმაცია წარმოდგენილია ძველი კანონის მოქმედების ფარგლებში, ხოლო პირველი მარტიდან 31 დეკემბრის ჩათვლით სტატისტიკური ინფორმაცია კანონის 2024 წლის მარტიდან მოქმედების ფარგლებში.

2024 წლის პირველ მარტამდე მოქმედი კანონის ფარგლებში გამოვლენილი სამართალდარღვევები



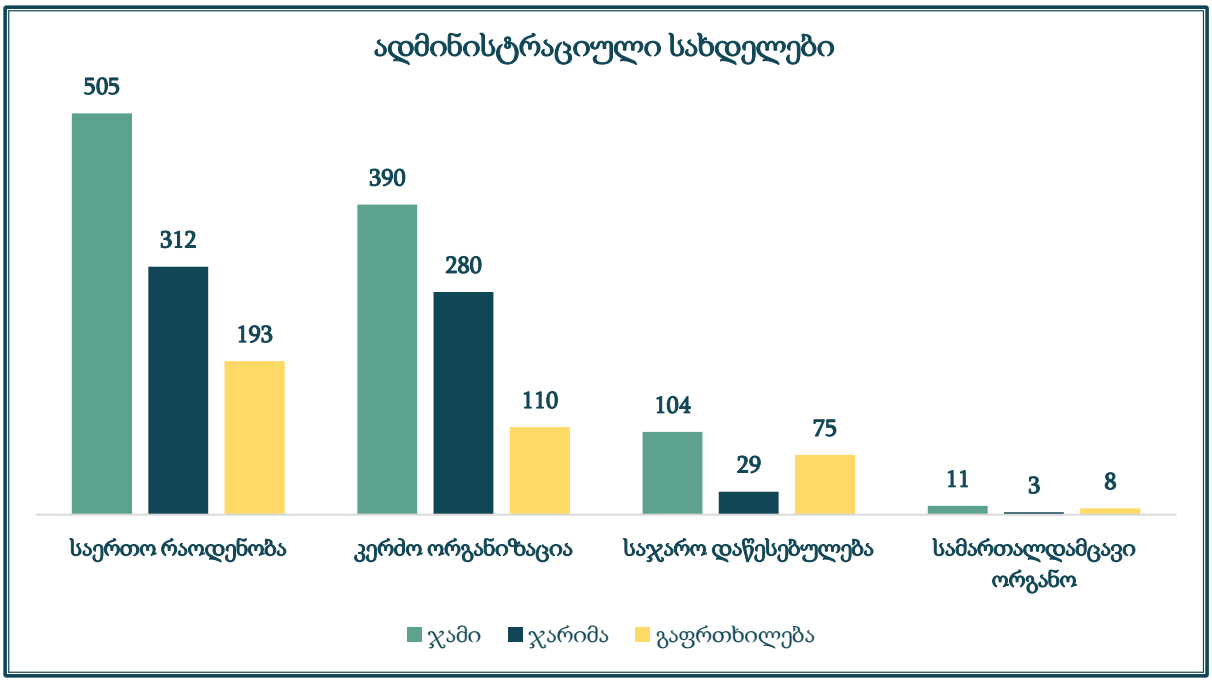
2024 წლის პირველი მარტის შემდგომ კანონის მოქმედების ფარგლებში გამოვლენილი სამართალდარღვევები



საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის სამსახურის მიერ გამოვლენილი 508 სამართალდარღვევიდან 24% (122) შეეხებოდა „პერსონალურ

მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 35-ე და 36-ე მუხლებით გათვალისწინებული ვალდებულებების შეუსრულებლობას, 17% (86) – მონაცემთა უსაფრთხოების დაცვის ვალდებულების შეუსრულებლობას, 12% (63) – ვიდეომონიტორინგის ან აუდიომონიტორინგის განხორციელების წესების დარღვევას.

რაც შეეხება 2023 წელს, პერსონალურ მონაცემთა დაცვის სამსახურის მიერ გამოვლენილი 267 სამართალდარღვევიდან 33% (89) შეეხებოდა მონაცემთა უსაფრთხოების დაცვის მოთხოვნების შეუსრულებლობას, 18% (49) – მონაცემთა დამუშავების პრინციპების დარღვევას, 15% (39) – ვიდეომონიტორინგის წესების დარღვევას.



საანგარიშო პერიოდში გამოვლენილ სამართალდარღვევათაგან სამსახურმა ადმინისტრაციული სახდელის სახით ჯარიმა და გაფრთხილება გამოიყენა 505 შემთხვევაში. სახდელის სახით დაკისრებული 9 ჯარიმა მიემართებოდა 2023 წელს დაწყებულ და საანგარიშო პერიოდში დასრულებულ შემოწმებებს (ინსპექტირებებს), ხოლო 303 – საანგარიშო პერიოდში დაწყებულ და დასრულებულ შემოწმებებს (ინსპექტირებებს). დაკისრებული 193 გაფრთხილებიდან 17 მიემართებოდა 2023 წელს დაწყებულ და საანგარიშო პერიოდში დასრულებულ, ხოლო 176 – საანგარიშო პერიოდში დაწყებულ და დასრულებულ შემოწმებებს (ინსპექტირებებს). დაკისრებული ადმინისტრაციული სახდელებიდან 77% (390) მიემართებოდა კერძო დაწესებულებებს, 21% (104) – საჯარო დაწესებულებებს, ხოლო 2% (11) – სამართალდამცავ ორგანოებს.

2023 წელთან შედარებით გაიზარდა გამოყენებული ადმინისტრაციული სახდელების რაოდენობა. კერძოდ, საანგარიშო პერიოდში ჩატარებული

შემოწმების (ინსპექტირების) შედეგად 225 პირს დაეკისრა ადმინისტრაციული სახდელი. გამოვლენილ ადმინისტრაციულ სამართალდამრღვევთაგან 123 პირს (55%) ადმინისტრაციული სახდელის სახით დაეკისრა ჯარიმა, ხოლო 102 პირს (45%) – გაფრთხილება.

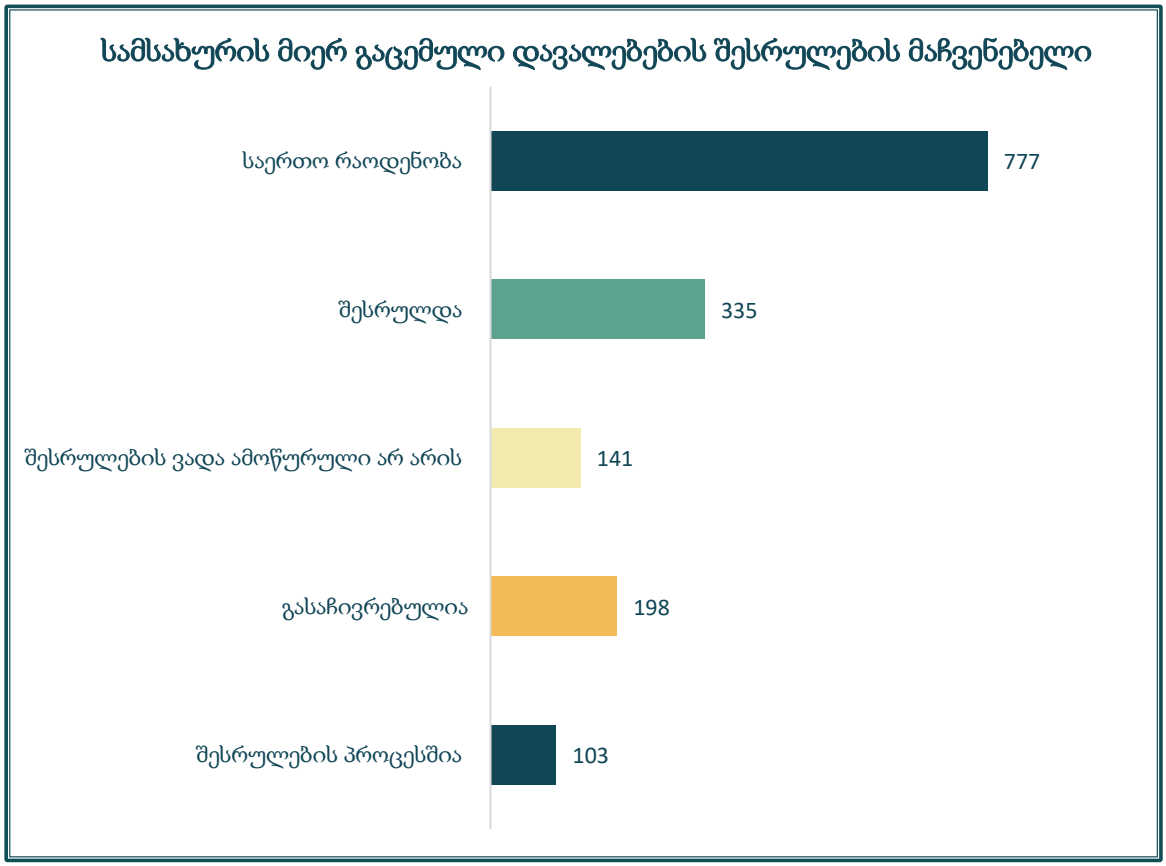
გარდა ადმინისტრაციული სახდელის დაკისრებისა, აღმოჩენილ ნაკლოვანებათა აღმოფხვრის მიზნით, სამსახურმა საჯარო დაწესებულებებისთვის და კერძო ორგანიზაციებისთვის, სამართალდამცავი ორგანოებისათვის გასცა 794 დავალება[125] და რეკომენდაცია.[126] გაცემული 777 დავალებიდან 60 მიემართებოდა 2023 წელს დაწყებულ და საანგარიშო პერიოდში დასრულებულ, ხოლო 717 – საანგარიშო პერიოდში დაწყებულ და დასრულებულ შემოწმებებს (ინსპექტირებებს). გაცემული 17 რეკომენდაციიდან 1 მიემართებოდა 2023 წელს დაწყებულ და საანგარიშო პერიოდში დასრულებულ შემოწმებას (ინსპექტირება), ხოლო 16 რეკომენდაცია – საანგარიშო პერიოდში დაწყებულ და დასრულებულ შემოწმებას (ინსპექტირებას). გაცემული 794 დავალებიდან და რეკომენდაციიდან

[125] **დავალება** არის სამსახურის მიერ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისთვის ან/და დამუშავებაზე უფლებამოსილი პირისთვის წერილობითი ფორმით მიცემული შესასრულებლად სავალდებულო მითითება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 52-ე მუხლის პირველი პუნქტის „ა“-„დ“ ქვეპუნქტებით გათვალისწინებული ღონისძიებების განხორციელების შესახებ.

[126] **რეკომენდაცია** არის სამსახურის მიერ დამუშავებისთვის პასუხისმგებელი პირისთვის ან/და დამუშავებაზე უფლებამოსილი პირისთვის წერილობითი ფორმით მიცემული რჩევა მონაცემთა დამუშავების პროცესში დარღვევების რისკების შემცირების მიზნით.

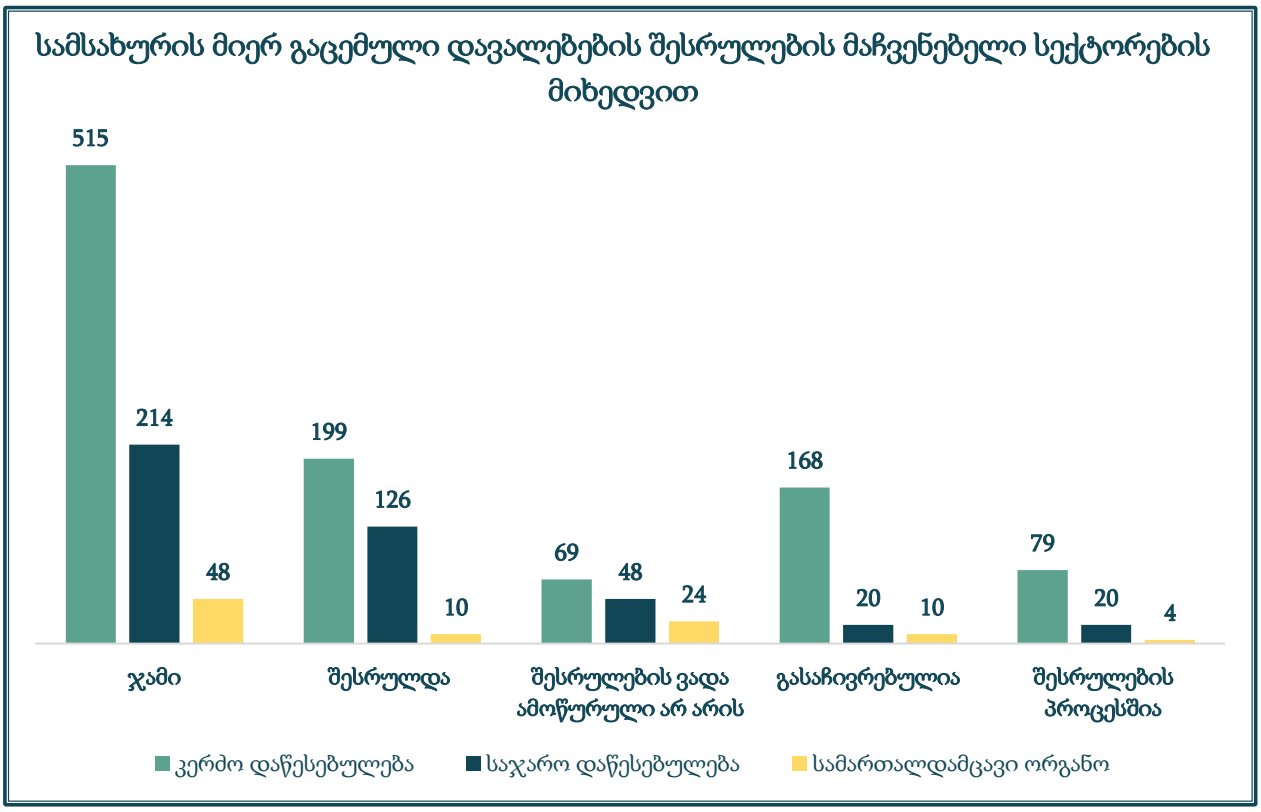
65% (519) მიემართებოდა კერძო დაწესებულებას, 28% (220) – საჯარო დაწესებულებას, ხოლო 7% (55) – სამართალდამცავ ორგანოს.

აღსანიშნავია, რომ 2023 წელთან შედარებით გაიზარდა გაცემული დავალებებისა და რეკომენდაციების მაჩვენებელი. კერძოდ, 2023 წელს სამსახურმა საჯარო დაწესებულებებისა და კერძო ორგანიზაციებისთვის, სამართალდამცავი ორგანოებისათვის გასცა 472 დავალება და რეკომენდაცია.



აღსანიშნავია, რომ გაცემული 777 დავალებიდან დავალებათა 43% (335) სრულად შესრულდა, შესრულების ვადა ამოწურული არ არის გაცემული დავალებების 18%-ისთვის (141), 26% (198) გასაჩივრებულია, ხოლო 13% (103) შესრულების პროცესშია.

საგულისხმოა, რომ 2023 წელთან შედარებით გაიზარდა სამსახურის მიერ გაცემული დავალებების შესრულების მაჩვენებელი. კერძოდ, 2023 წელს შესრულდა გაცემულ დავალებათა 52% (239).



საანგარიშო პერიოდში კერძო დაწესებულებების მიმართ გაცემული 515 დავალებიდან შესრულდა 39% (199), შესრულების ვადა ამოწურული არ არის გაცემული დავალებების 13%-ისთვის (69), გასაჩივრებულია გაცემულ დავალებათა 33% (168), ხოლო შესრულების პროცესშია 15% (79).

საჯარო დაწესებულებების მიმართ გაცემული 214 დავალებიდან შესრულდა 60% (126), შესრულების ვადა ამოწურული არ არის გაცემული დავალებების 22%-ისთვის (48), გასაჩივრებულია გაცემულ დავალებათა 9% (20), ხოლო შესრულების პროცესშია 9% (20).

სამართალდამცავი ორგანოების მიმართ გაცემული 48 დავალებიდან შესრულდა 21% (10), შესრულების ვადა ამოწურული არ არის გაცემული დავალებების 50%-ისთვის (24), გასაჩივრებულია გაცემულ დავალებათა 21% (10), ხოლო შესრულების პროცესშია 8% (4).

მონაცემთა უსაფრთხოების დარღვევის (ინციდენტი) შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულება

11

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის „წ“ ქვეპუნქტის თანახმად, ინციდენტი წარმოადგენს მონაცემთა უსაფრთხოების დარღვევას, რომელიც იწვევს მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას/მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას“.

კანონის 29-ე მუხლის შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირს ეკისრება ვალდებულება აღრიცხოს ინციდენტი, დამდგარი შედეგი, მიღებული ზომები და ინციდენტის აღმოჩენიდან არა უგვიანეს 72 საათისა მის შესახებ წერილობით ან ელექტრონულად შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს, გარდა იმ შემთხვევისა, როდესაც ნაკლებსავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.[127]

საანგარიშო პერიოდში სამსახურმა მონაცემთა უსაფრთხოების დარღვევის (ინციდენტი) თაობაზე მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისგან მიიღო 11 შეტყობინება.

- ### ფიზიკური პირის ხელმისაწვდომობა საკუთარ მონაცემებზე

2024 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის III და IV თავების ფარგლებში შეისწავლა სხვადასხვა უწყების მიერ ფიზიკური პირის ინფორმირების კანონიერების 56 შემთხვევა, რომელთაგან 10 განხორციელდა პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით, 4 – არაგეგმურად, ხოლო 42 – განცხადების საფუძველზე.

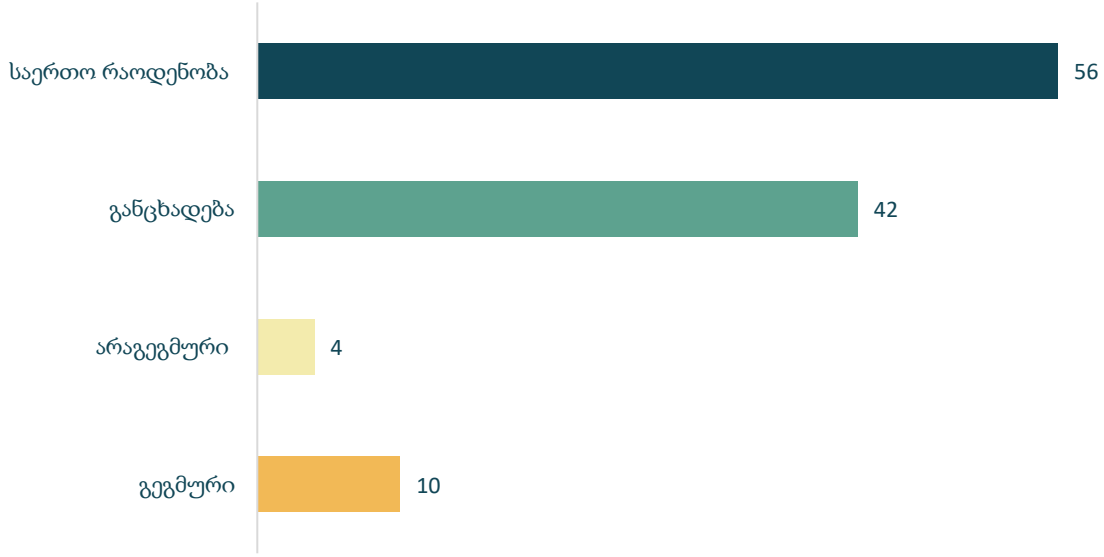
პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე, ადმინისტრაციული პასუხისმგებლობა დაეკისრა 22 პირს. სანქციის სახით 9 პირის მიმართ გამოყენებულ იქნა გაფრთხილება, ხოლო 13 პირის მიმართ – ჯარიმა. ადმინისტრაციული სახდელების პარალელურად, საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების გაუმჯობესებისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან მათი შესაბამისობის უზრუნველყოფის მიზნით, სამსახურმა გასცა შესასრულებლად სავალდებულო 49 დავალება და 4 რეკომენდაცია.

2023 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა სხვადასხვა უწყების მიერ ფიზიკური პირის ინფორმირების კანონიერების 91

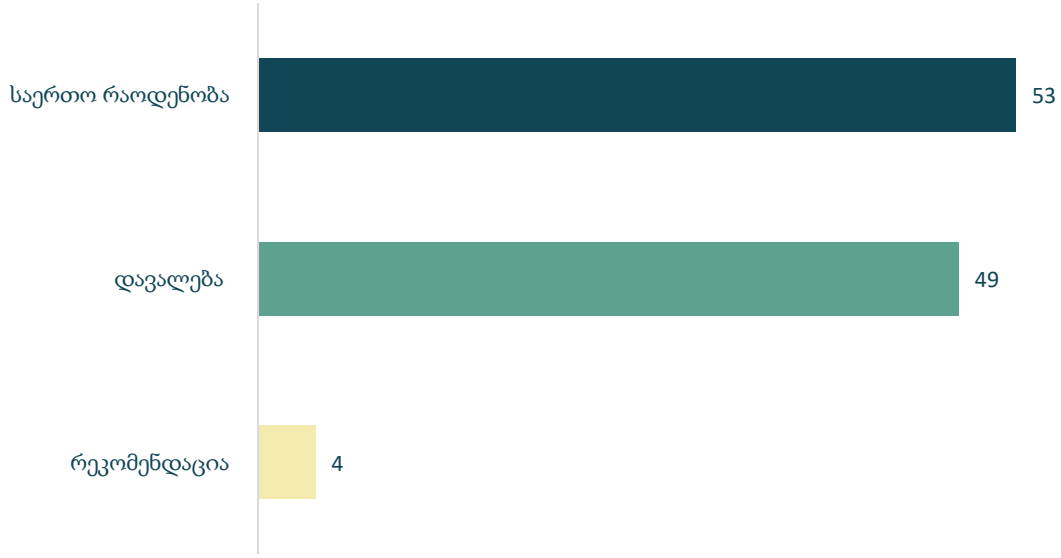
[127] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 29-ე მუხლის პირველი პუნქტი.

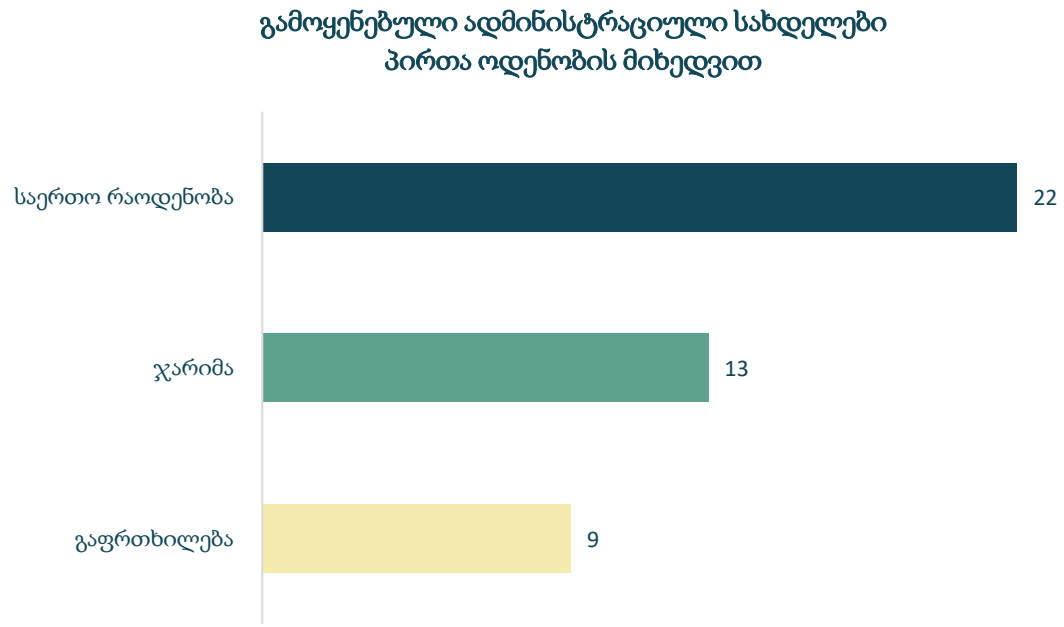
შემთხვევა. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 36 პირს. სამსახურმა გასცა შესასრულებლად სავალდებულო 73 დავალება და 1 რეკომენდაცია.

შემოწმება/ინსპექტირება



გაცემული დავალებები და რეკომენდაციები





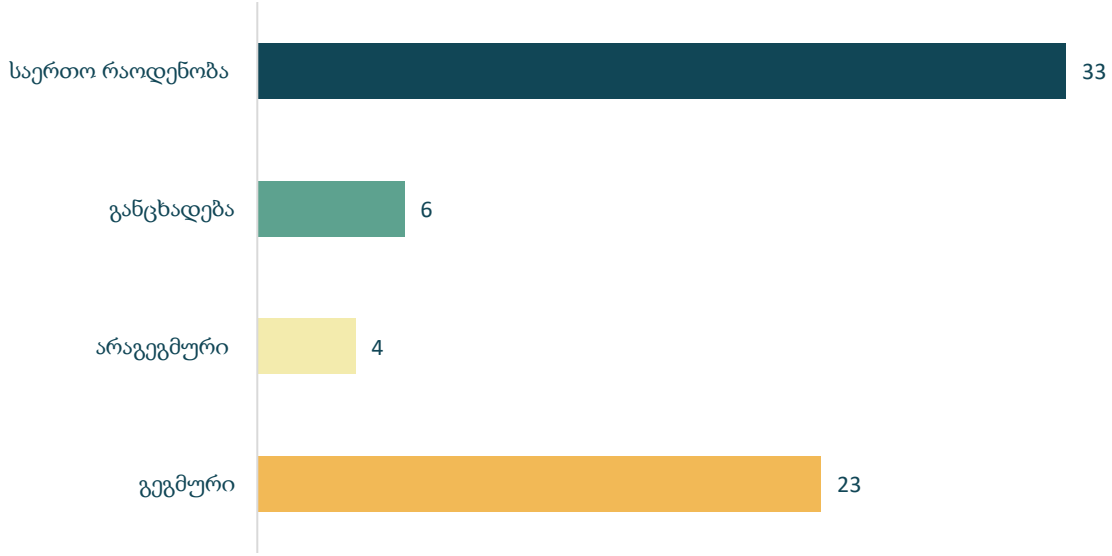
- **არასრულწლოვნების პერსონალური მონაცემების დაცვა**

2024 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა არასრულწლოვნების პერსონალური მონაცემების დამუშავების 33 შემთხვევა, რომელთაგან 23 განხორციელდა პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით, 4 – არაგეგმურად, ხოლო 6 – შემოსული განცხადების საფუძველზე.

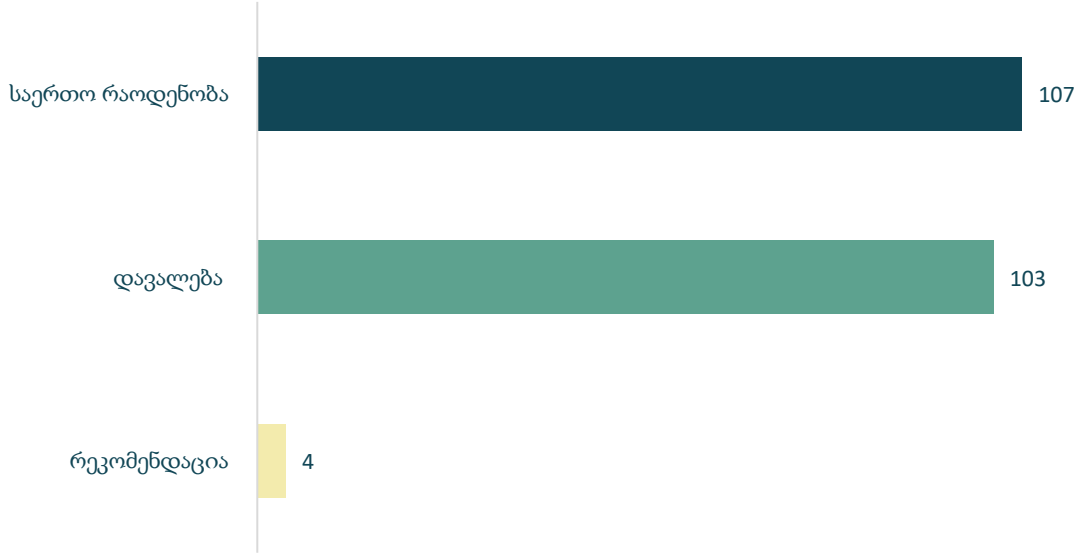
პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 33 პირს. სანქციის სახით 9 პირის მიმართ გამოყენებულ იქნა გაფრთხილება, ხოლო 24 პირის მიმართ – ჯარიმა. ადმინისტრაციული სახდელების პარალელურად, საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების გაუმჯობესებისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან მათი შესაბამისობის უზრუნველყოფის მიზნით, სამსახურმა გასცა 4 რეკომენდაცია და შესასრულებლად სავალდებულო 103 დავალება.

2023 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა არასრულწლოვნების პერსონალური მონაცემების დამუშავების 34 შემთხვევა. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 24 პირს. სამსახურმა გასცა 3 რეკომენდაცია და შესასრულებლად სავალდებულო 77 დავალება.

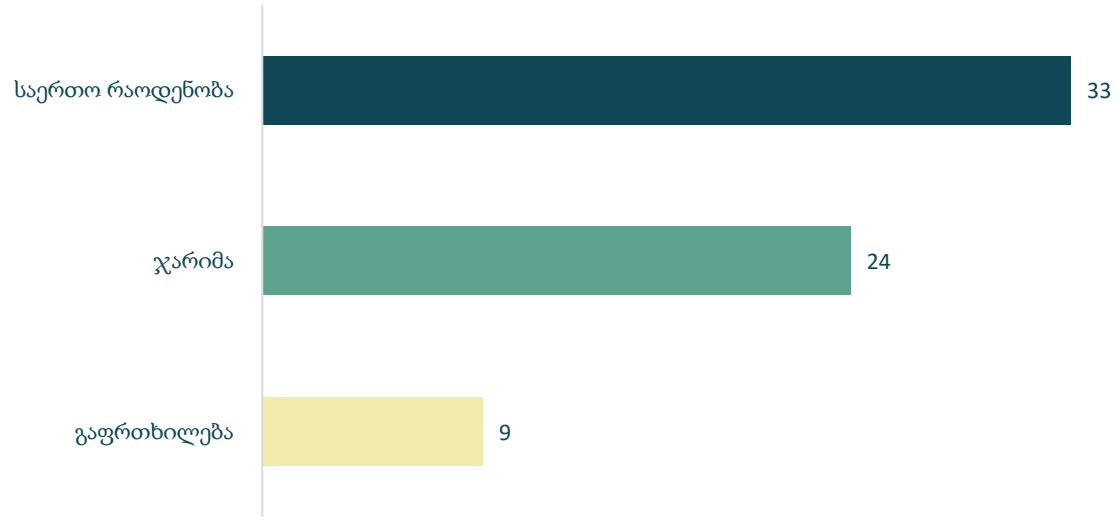
შემოწმება/ინსპექტირება



გაცემული დავალებები და რეკომენდაციები



გამოყენებული ადმინისტრაციული სახდელები
პირთა ოდენობის მიხედვით



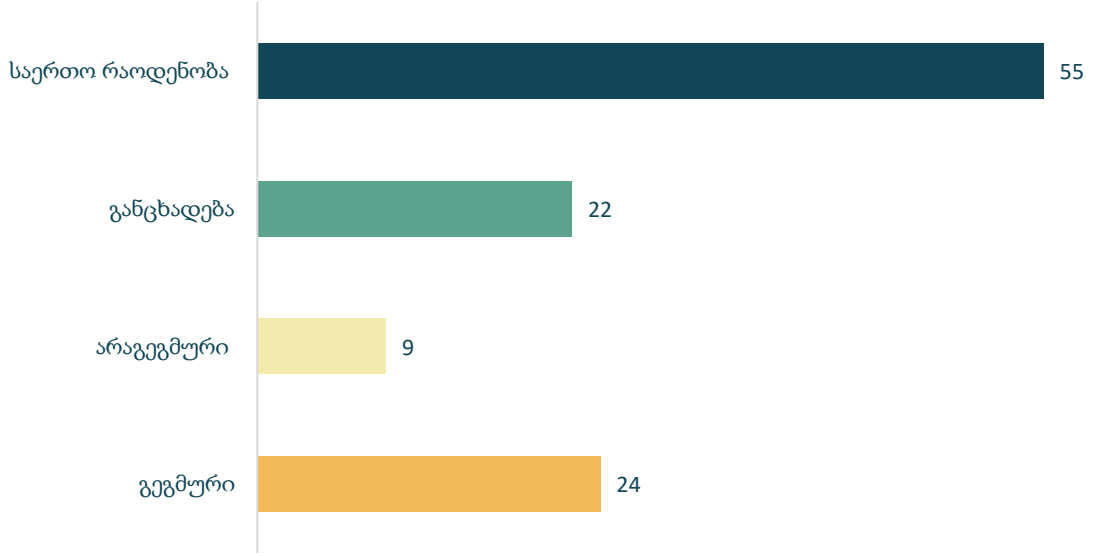
- **პერსონალური მონაცემების დაცვა შრომით ურთიერთობებში**

2024 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა შრომითი ურთიერთობის ფარგლებში პერსონალური მონაცემების დამუშავების 55 შემთხვევა, რომელთაგან 24 განხორციელდა სამსახურის ინიციატივით, 9 – არაგეგმურად, ხოლო 22 – მოქალაქეთა განცხადების საფუძველზე.

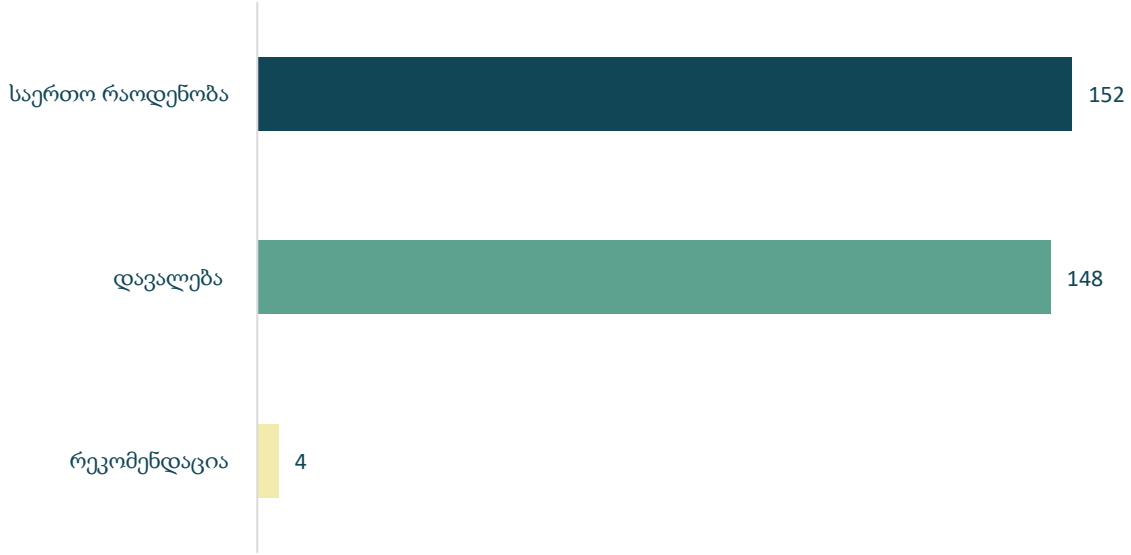
პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 72 პირს. სანქციის სახით 37 პირის მიმართ გამოყენებულ იქნა გაფრთხილება, ხოლო 35 პირის მიმართ – ჯარიმა. ადმინისტრაციული სახდელების პარალელურად, საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების გაუმჯობესებისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან მათი შესაბამისობის უზრუნველყოფის მიზნით, სამსახურმა გასცა 4 რეკომენდაცია და შესასრულებლად სავალდებულო 148 დავალება.

2023 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა შრომითი ურთიერთობის ფარგლებში პერსონალური მონაცემების დამუშავების 57 შემთხვევა. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 26 პირს. სამსახურმა გასცა 7 რეკომენდაცია და შესასრულებლად სავალდებულო 74 დავალება.

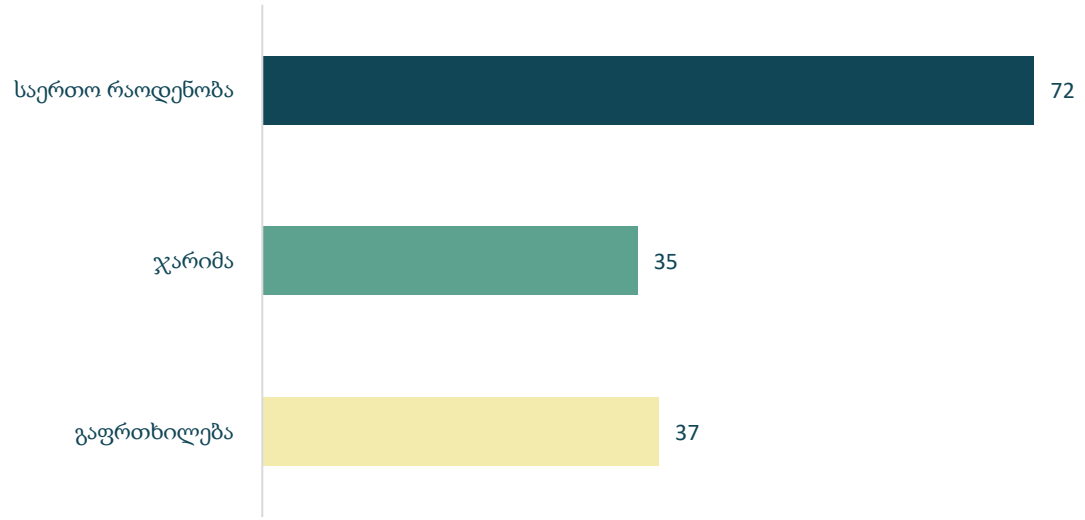
შემოწმება/ინსპექტირება



გაცემული დავალებები და რეკომენდაციები



გამოყენებული ადმინისტრაციული სახდელები
პირთა ოდენობის მიხედვით

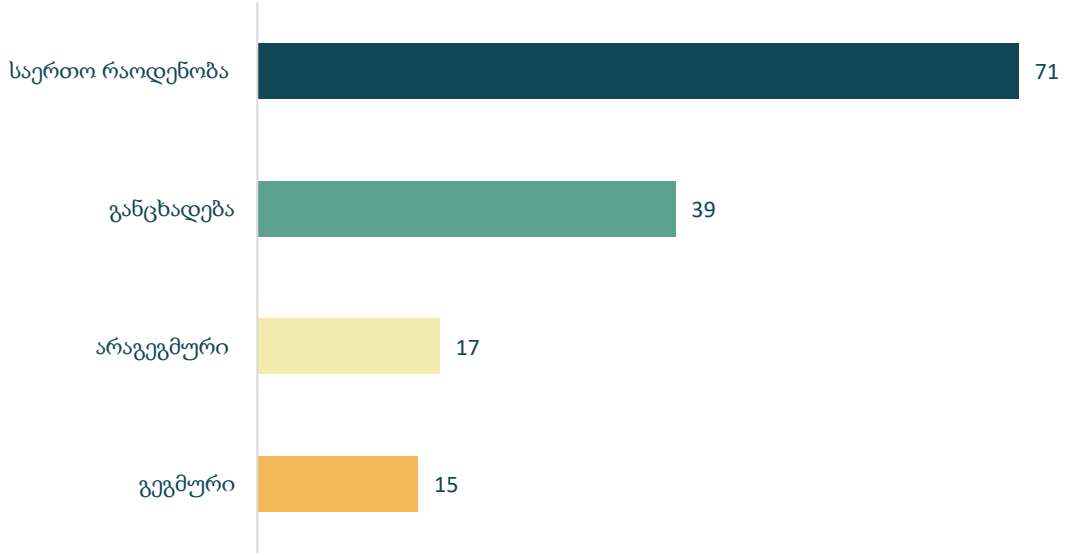


• ვიდეომონიტორინგი

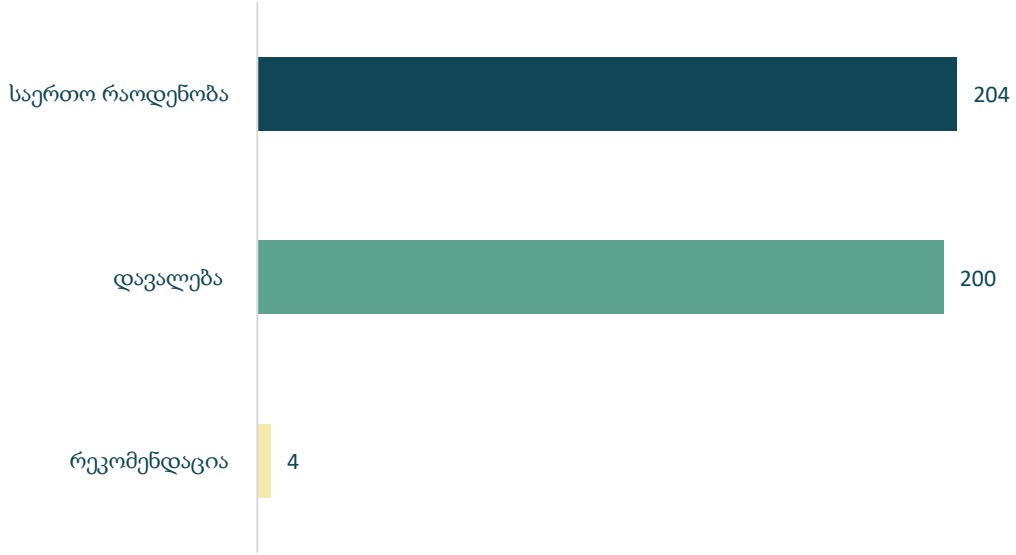
2024 წელს სამსახურმა სახელმწიფო სტრუქტურებსა და კერძო დაწესებულებებში მიმდინარე ვიდეომონიტორინგის 71 შემთხვევა შეისწავლა. მათგან 15 განხორციელდა პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით, 17 – არაგეგმურად, ხოლო 39 – განცხადებების საფუძველზე.

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 81 პირს. სანქციის სახით 39 პირის მიმართ გამოყენებულ იქნა გაფრთხილება, ხოლო 42 პირის მიმართ – ჯარიმა. ადმინისტრაციული სახდელების პარალელურად, საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების გაუმჯობესებისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან მათი შესაბამისობის უზრუნველყოფის მიზნით, სამსახურმა გასცა 4 რეკომენდაცია და შესასრულებლად სავალდებულო 200 დავალება.

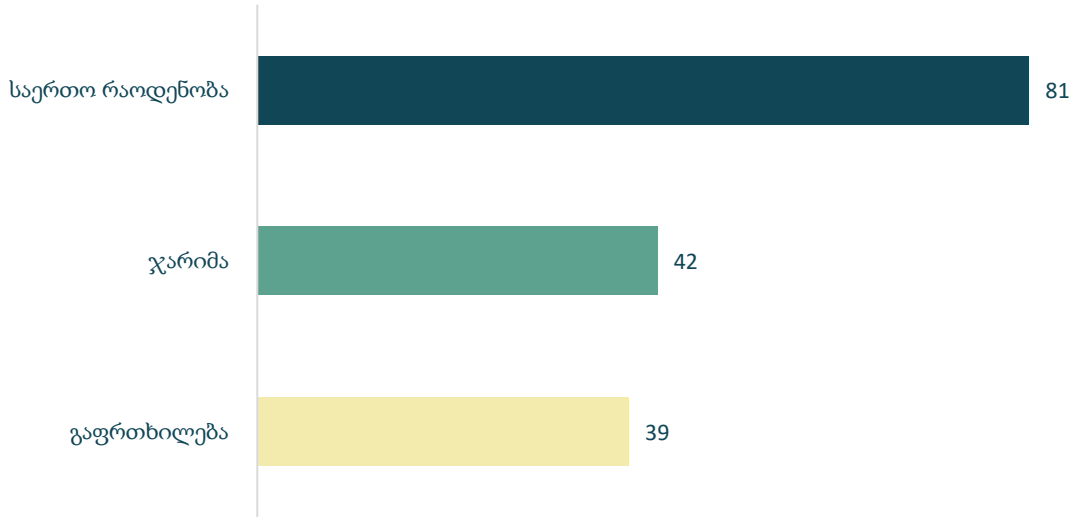
შემოწმება/ინსპექტირება



გაცემული დავალებები და რეკომენდაციები



გამოყენებული ადმინისტრაციული სახდელები
პირთა ოდენობის მიხედვით



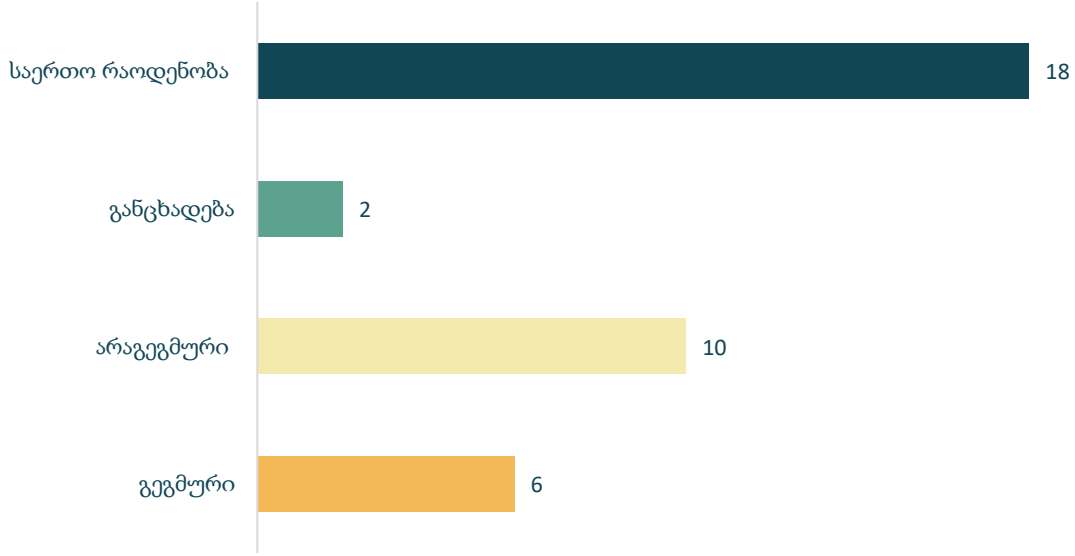
- ჯანდაცვის სექტორში პერსონალური მონაცემების დამუშავება

საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა ჯანდაცვის სექტორში მონაცემთა დამუშავების 18 შემთხვევა, რომელთაგან 6 განხორციელდა პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით, 10 – არაგეგმურად, ხოლო 2 – მოქალაქეთა განცხადების საფუძველზე.

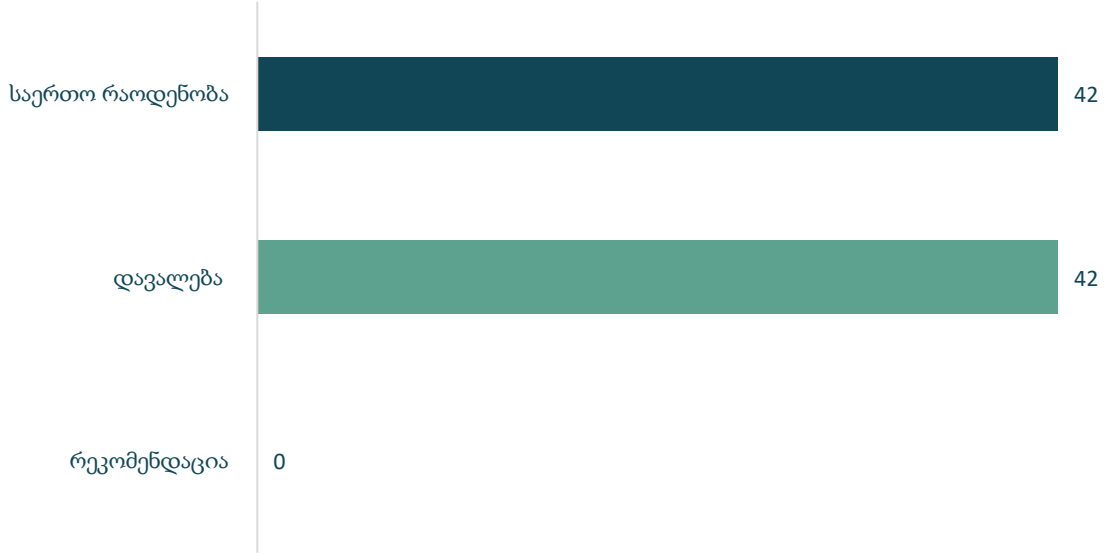
პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 30 პირს. სანქციის სახით 18 პირის მიმართ გამოყენებულ იქნა გაფრთხილება, ხოლო 12 პირის მიმართ – ჯარიმა. ადმინისტრაციული სახდელების პარალელურად, საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების გაუმჯობესებისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან მათი შესაბამისობის უზრუნველყოფის მიზნით, სამსახურმა გასცა შესასრულებლად სავალდებულო 42 დავალება.

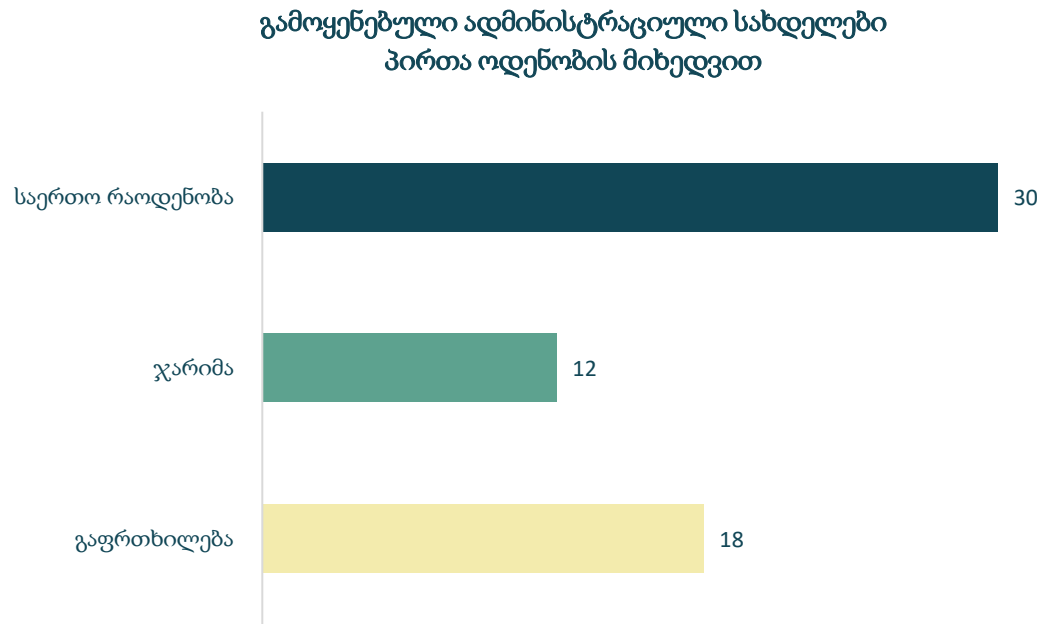
2023 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა ჯანდაცვის სექტორში მონაცემთა დამუშავების 15 შემთხვევა. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 18 პირს. სამსახურმა გასცა შესასრულებლად სავალდებულო 35 დავალება და 1 რეკომენდაცია.

შემოწმება/ინსპექტირება



გაცემული დავალებები და რეკომენდაციები





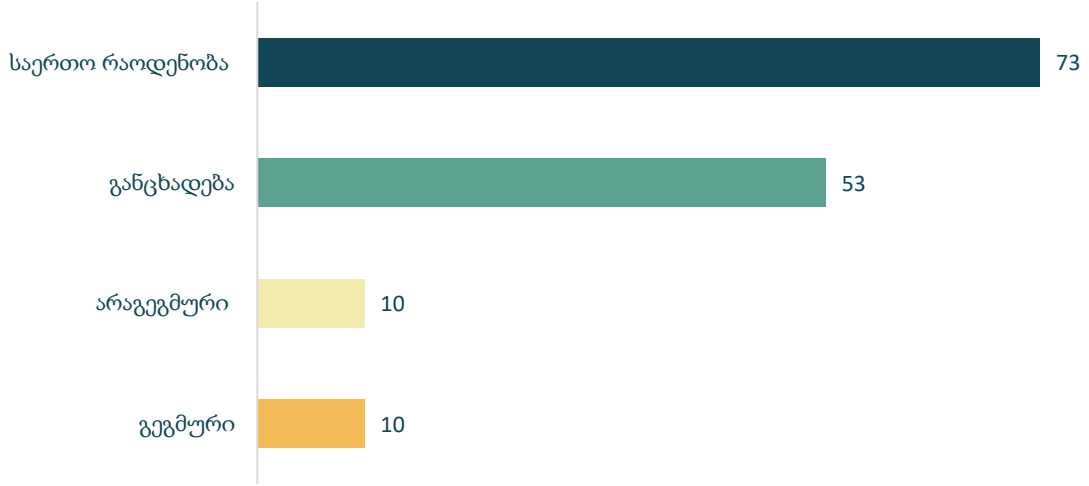
- **ფინანსურ სექტორში პერსონალური მონაცემების დამუშავება**

2024 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა საფინანსო სექტორში პერსონალური მონაცემების დამუშავების 73 შემთხვევა, რომელთაგან 10 განხორციელდა სამსახურის ინიციატივით, 10 – არაგეგმურად, ხოლო 53 – მოქალაქეთა განცხადებების საფუძველზე.

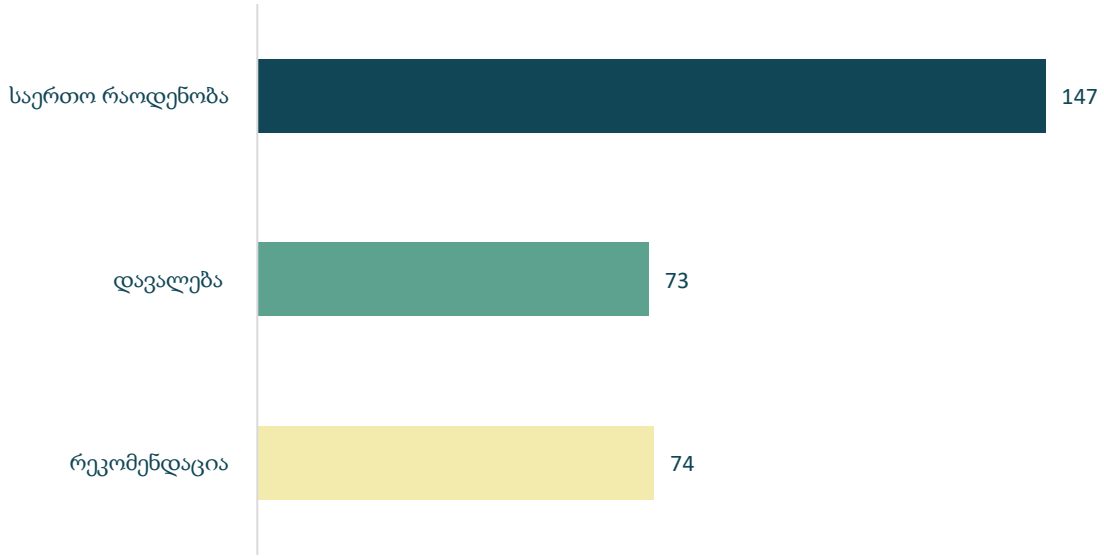
პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 62 პირს. სანქციის სახით 7 პირის მიმართ გამოყენებულ იქნა გაფრთხილება, ხოლო 55 პირის მიმართ – ჯარიმა. ადმინისტრაციული სახდელებთან ერთად, კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების გაუმჯობესებისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან მათი შესაბამისობის უზრუნველყოფის მიზნით, სამსახურმა გასცა შესასრულებლად სავალდებულო 73 დავალება და 74 რეკომენდაცია.

2023 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა საფინანსო სექტორში პერსონალური მონაცემების დამუშავების 41 შემთხვევა. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 18 პირს. სამსახურმა გასცა შესასრულებლად სავალდებულო 24 დავალება.

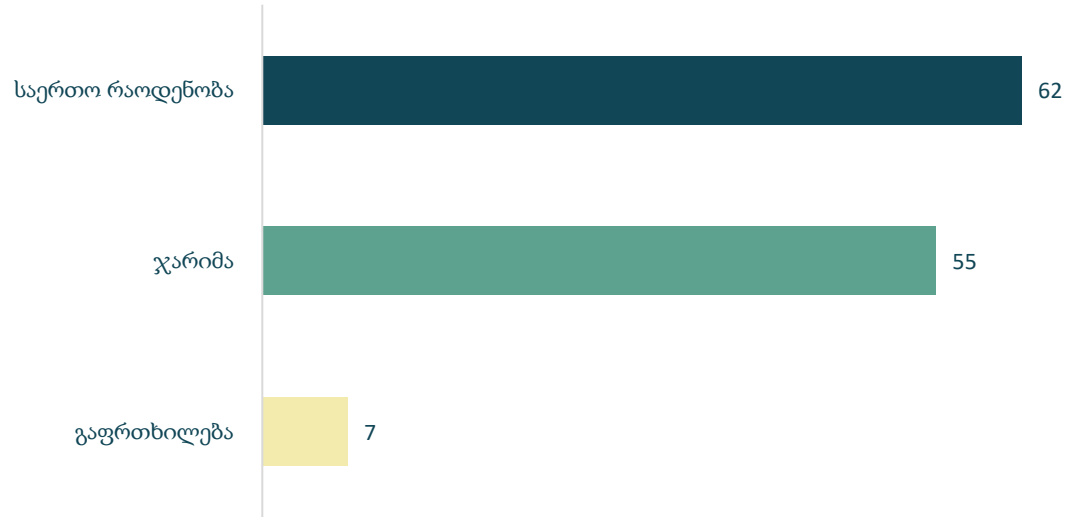
შემოწმება/ინსპექტირება



გაცემული დავალებები და რეკომენდაციები



გამოყენებული ადმინისტრაციული სახდელები
პირთა ოდენობის მიხედვით



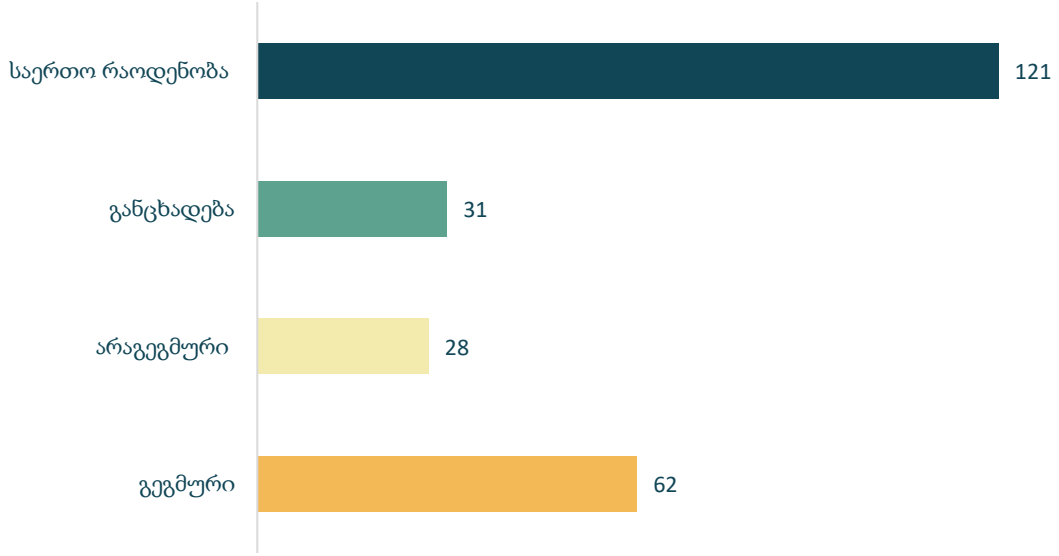
- **მონაცემთა უსაფრთხოება**

2024 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა მონაცემთა უსაფრთხოებასთან დაკავშირებული 121 შემთხვევა, რომელთაგან 62 განხორციელდა პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით, 28 – არაგეგმურად, ხოლო 31 – მოქალაქეთა განცხადებების საფუძველზე.

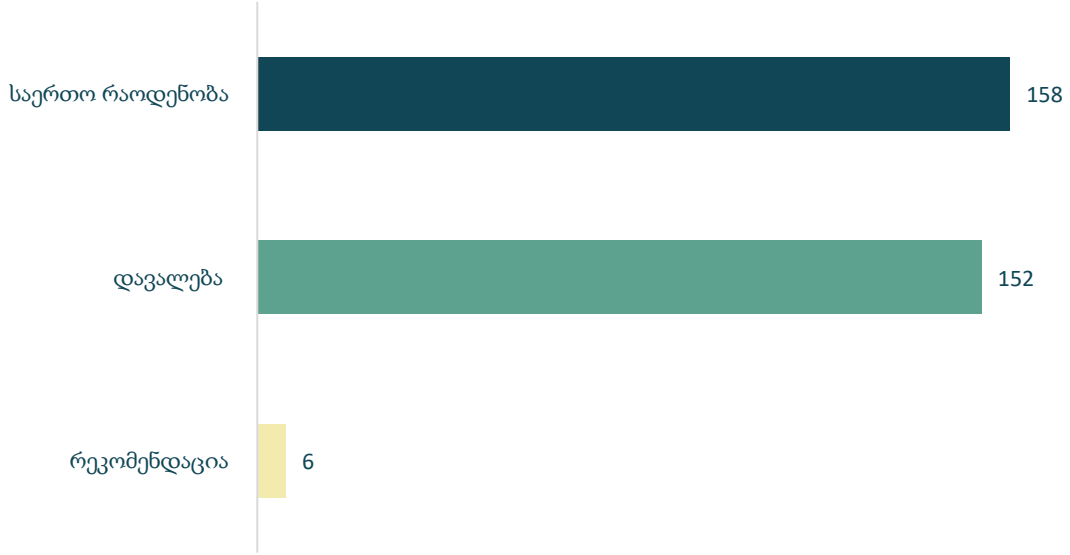
პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 100 პირს. სანქციის სახით 57 პირის მიმართ გამოყენებულ იქნა გაფრთხილება, ხოლო 43 პირის მიმართ – ჯარიმა. ადმინისტრაციული სახდელების პარალელურად, საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების გაუმჯობესებისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან მათი შესაბამისობის უზრუნველყოფის მიზნით, სამსახურმა გასცა 6 რეკომენდაცია და შესასრულებლად სავალდებულო 152 დავალება.

2023 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა მონაცემთა უსაფრთხოებასთან დაკავშირებული 90 შემთხვევა. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 84 პირს. სამსახურმა გასცა 4 რეკომენდაცია და შესასრულებლად სავალდებულო 155 დავალება.

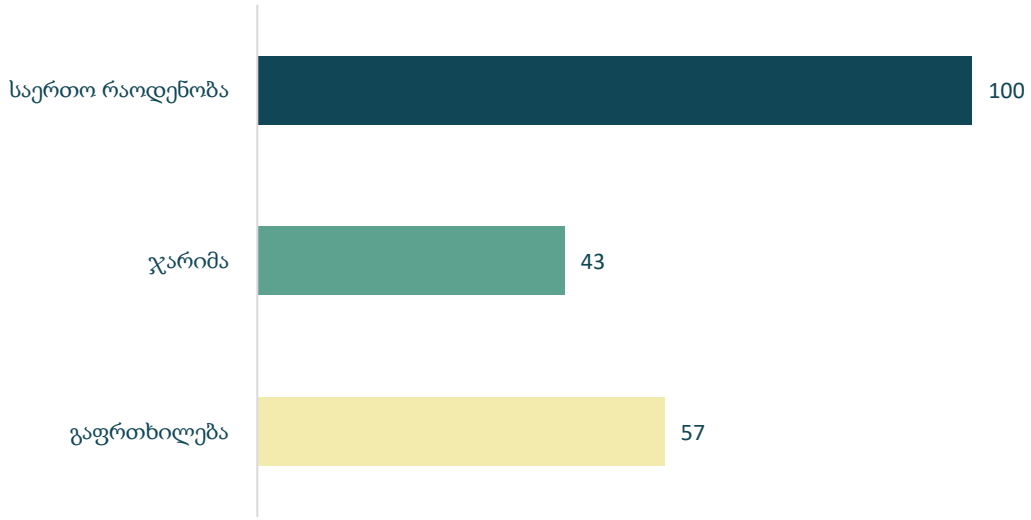
შემოწმება/ინსპექტირება



გაცემული დავალებები და რეკომენდაციები



გამოყენებული ადმინისტრაციული სახდელები
პირთა ოდენობის მიხედვით

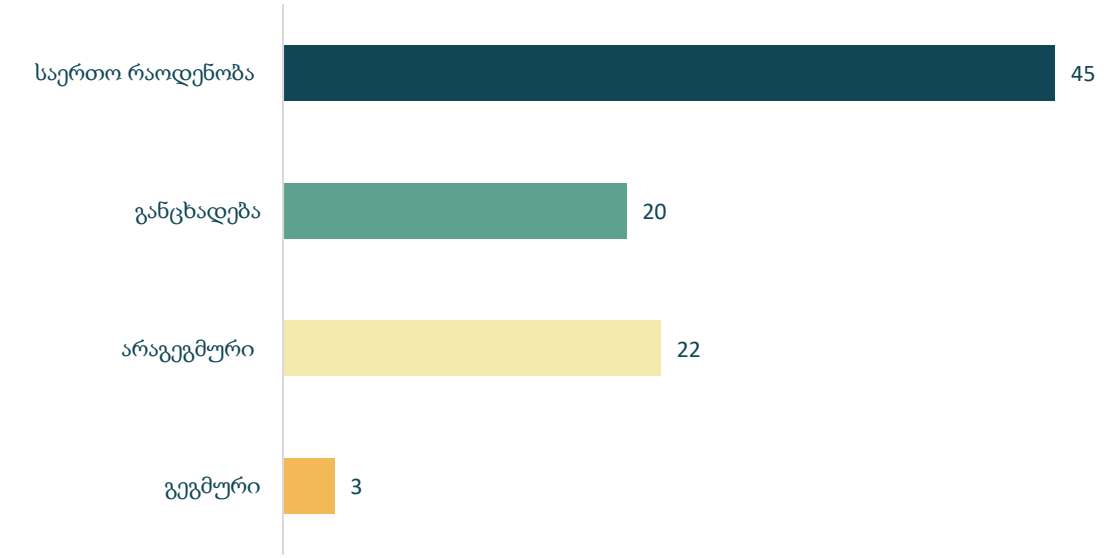


- **პირდაპირი მარკეტინგის მიზნით პერსონალური მონაცემების დამუშავება**

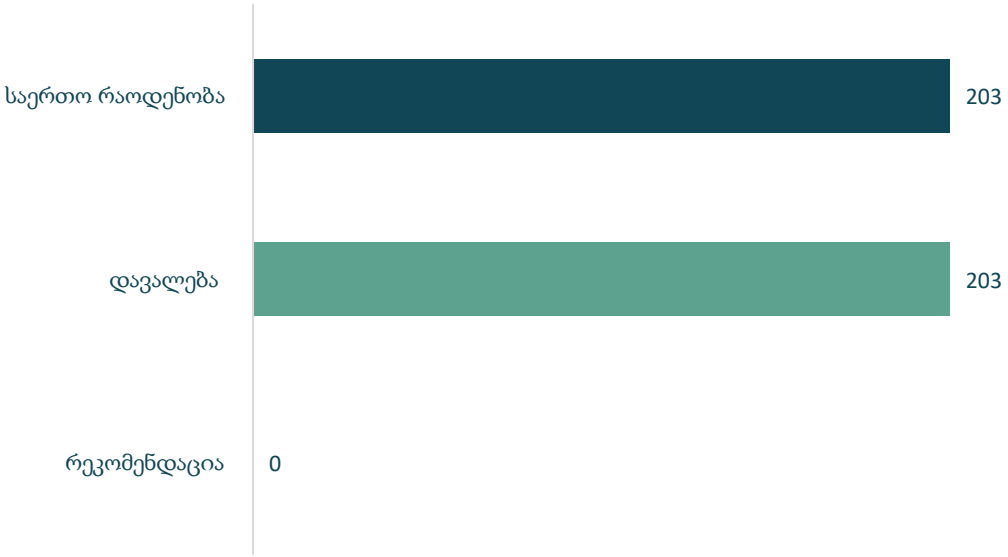
საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის სამსახურმა შეისწავლა პირდაპირი მარკეტინგის მიზნით პერსონალური მონაცემების დამუშავების 45 შემთხვევა, რომელთაგან 3 განხორციელდა პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით, 22 – არაგეგმურად, ხოლო 20 – მოქალაქეთა განცხადებების საფუძველზე.

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 165 პირს. სანქციის სახით 11 პირის მიმართ გამოყენებულ იქნა გაფრთხილება, ხოლო 154 პირის მიმართ – ჯარიმა. ადმინისტრაციული სახდელების პარალელურად, საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების გაუმჯობესებისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან მათი შესაბამისობის უზრუნველყოფის მიზნით, სამსახურმა გასცა შესასრულებლად სავალდებულო 203 დავალება.

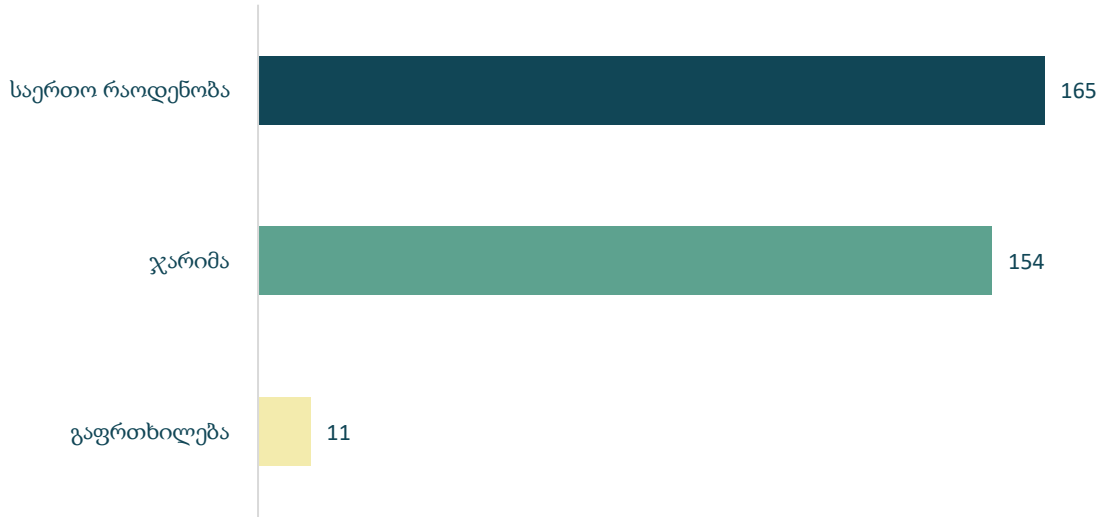
შემოწმება/ინსპექტირება



გაცემული დავალებები და რეკომენდაციები



გამოყენებული ადმინისტრაციული სახდელები
პირთა ოდენობის მიხედვით

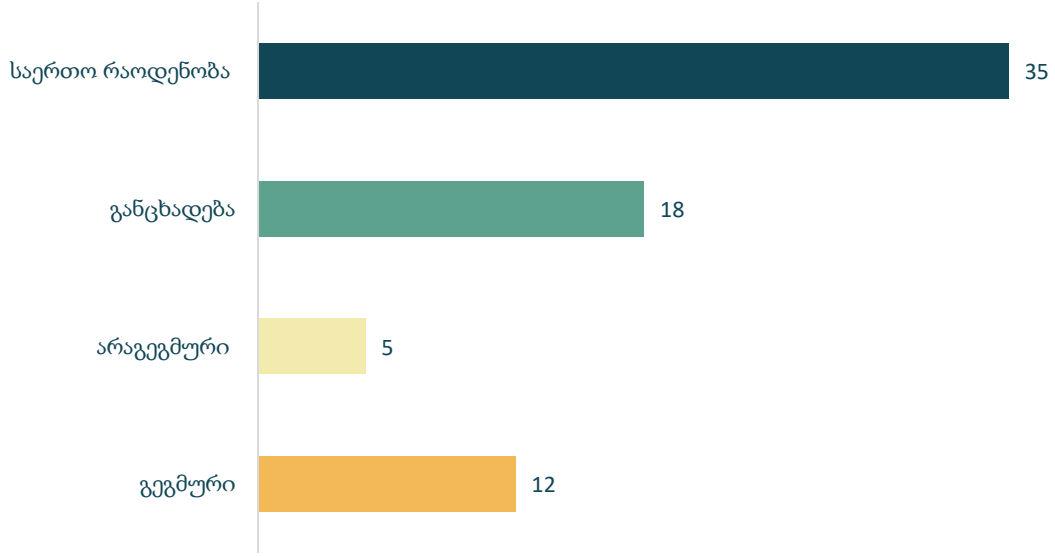


- აუდიომონიტორინგის განხორციელება

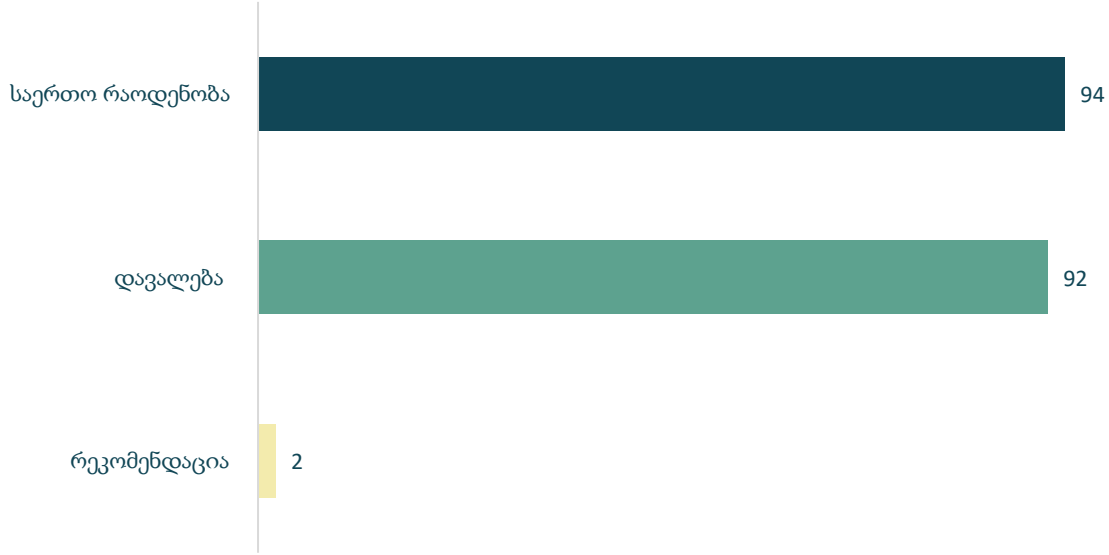
2024 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა აუდიომონიტორინგის განხორციელებასთან დაკავშირებით შეისწავლა პერსონალური მონაცემების დამუშავების 35 შემთხვევა, რომელთაგან 12 განხორციელდა პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით, 5 – არაგეგმურად, ხოლო 18 – მოქალაქეთა განცხადებების საფუძველზე.

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 38 პირს. სანქციის სახით 19 პირის მიმართ გამოყენებულ იქნა გაფრთხილება და 19 პირის მიმართ – ჯარიმა. ადმინისტრაციული სახდელების პარალელურად, საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების გაუმჯობესებისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან მათი შესაბამისობის უზრუნველყოფის მიზნით, სამსახურმა გასცა შესასრულებლად სავალდებულო 92 დავალება და 2 რეკომენდაცია.

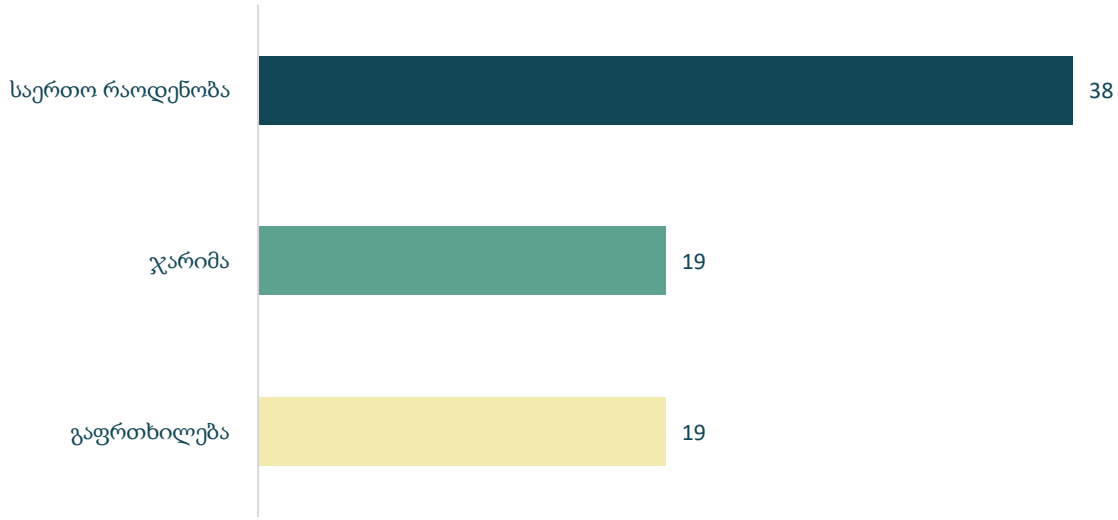
შემოწმება/ინსპექტირება



გაცემული დავალებები და რეკომენდაციები



გამოყენებული ადმინისტრაციული სახდელები
პირთა ოდენობის მიხედვით

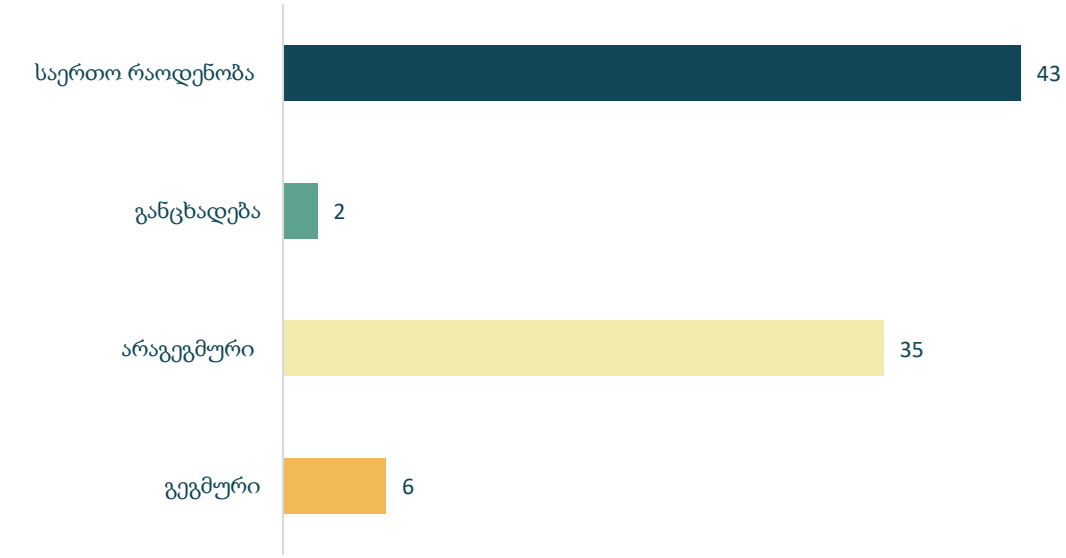


- **პერსონალურ მონაცემთა დაცვის ოფიცერი**

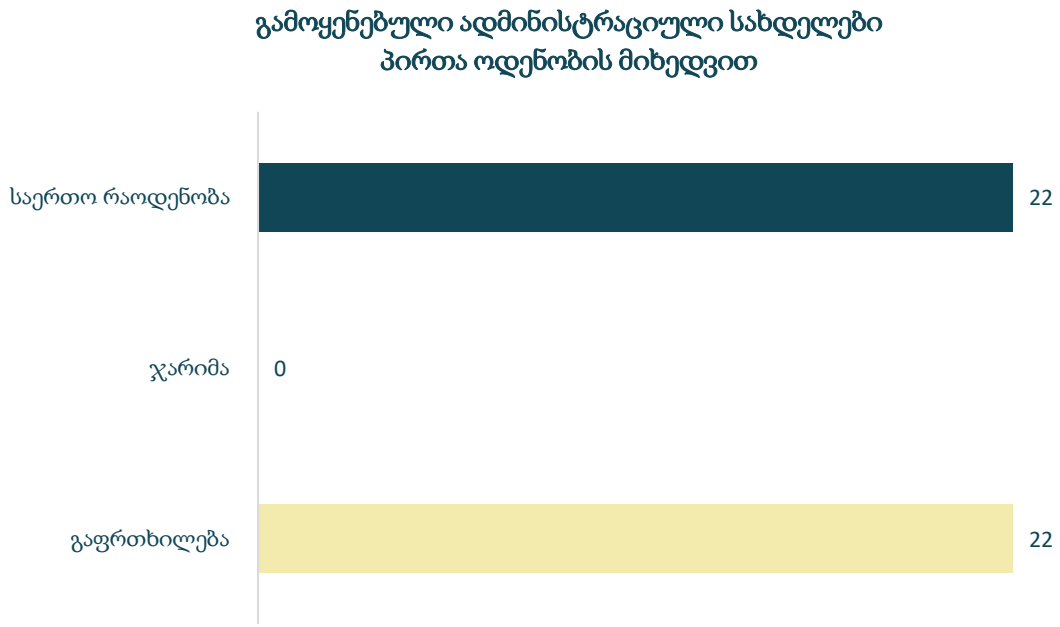
პერსონალურ მონაცემთა დაცვის სამსახურმა პერსონალურ მონაცემთა დაცვის ოფიცერთან დაკავშირებული ვალდებულებების ფარგლებში შეისწავლა პერსონალური მონაცემების დამუშავების 43 შემთხვევა, რომელთაგან 6 განხორციელდა პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით, 35 – არაგეგმურად, ხოლო 2 – მოქალაქეთა განცხადებების საფუძველზე.

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესწავლილი საქმეების საფუძველზე ადმინისტრაციული პასუხისმგებლობა დაეკისრა 22 პირს. სანქციის სახით 22 პირის მიმართ გამოყენებულ იქნა გაფრთხილება. ადმინისტრაციული სახდელების პარალელურად, საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების გაუმჯობესებისა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან მათი შესაბამისობის უზრუნველყოფის მიზნით, სამსახურმა გასცა შესასრულებლად სავალდებულო 42 დავალება და 2 რეკომენდაცია.

შემოწმება/ინსპექტირება



გაცემული დავალებები და რეკომენდაციები

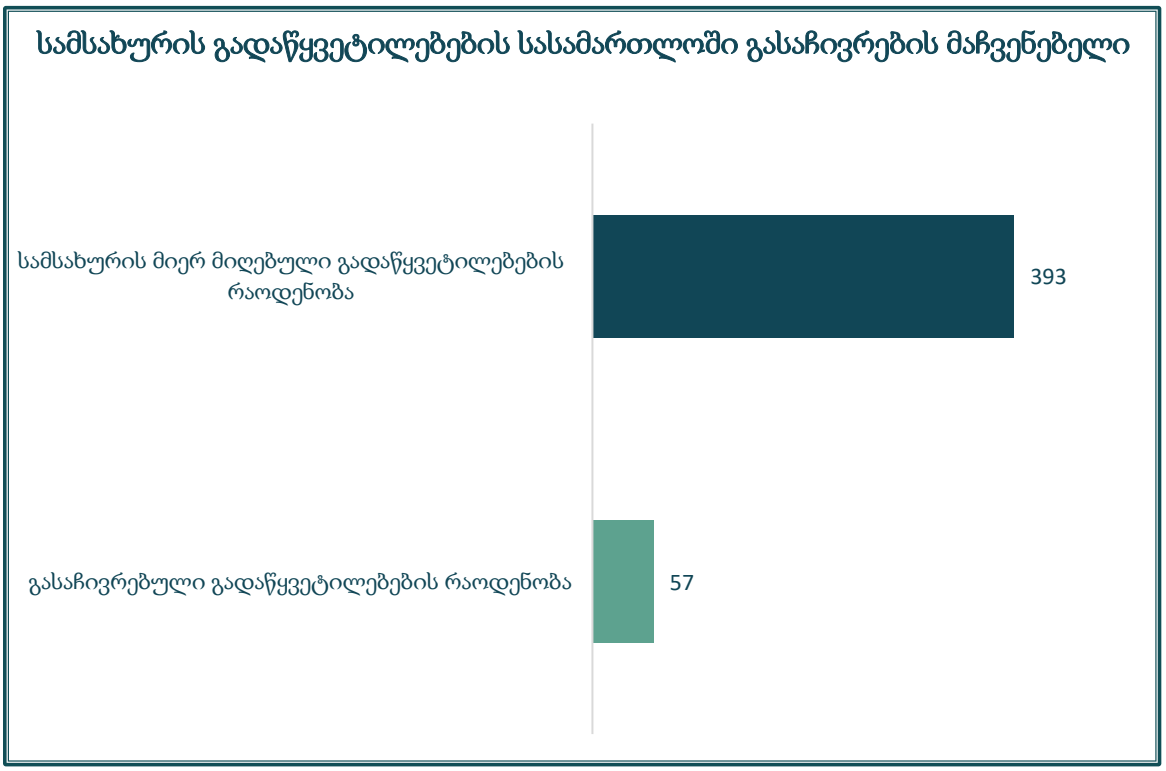


2. სხვა სტატისტიკური ინფორმაცია

გაცემული კონსულტაციების ჯამური რაოდენობა

16 462

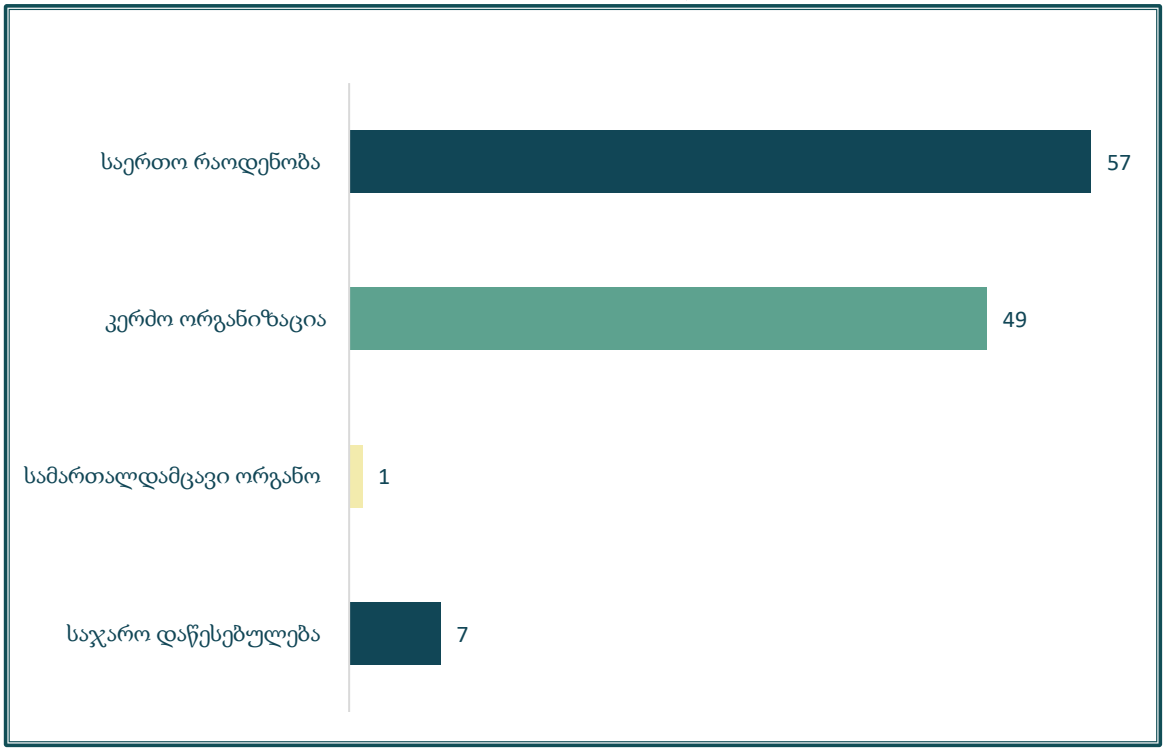
საანგარიშო პერიოდში სამსახურმა პერსონალურ მონაცემთა დაცვის კანონიერების კონტროლსა და სხვა სამართლებრივ საკითხებთან დაკავშირებით გასცა ჯამურად 16 462 კონსულტაცია. აღსანიშნავია, რომ 2023 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა გასცა ჯამურად 5106 კონსულტაცია.



საანგარიშო პერიოდში მიღებული 393 შემაჯამებელი გადაწყვეტილებიდან გასაჩივრებულია 15% (57).

2023 წელს მიღებული 338 შემაჯამებელი გადაწყვეტილებიდან გასაჩივრებულია 17% (59).

სამსახურის მიერ მიღებული გადაწყვეტილებების გასაჩივრების მაჩვენებელი სექტორების მიხედვით



საანგარიშო პერიოდში გასაჩივრებული 57 გადაწყვეტილებიდან 86% (49) შეეხებოდა კერძო ორგანიზაციების, 2% (1) – სამართალდამცავი ორგანოების, ხოლო 12% (7) – საჯარო დაწესებულების მიმართ მიღებულ გადაწყვეტილებას.

2023 წელს გასაჩივრებული 59 გადაწყვეტილებიდან 59% (35) შეეხებოდა კერძო დაწესებულებების, 4% (2) – სამართალდამცავი ორგანოების, ხოლო 37% (22) – საჯარო დაწესებულების მიმართ მიღებულ გადაწყვეტილებას.

საზოგადოების ცნობიერების ამაღლება, საინფორმაციო შეხვედრები და ტრენინგები

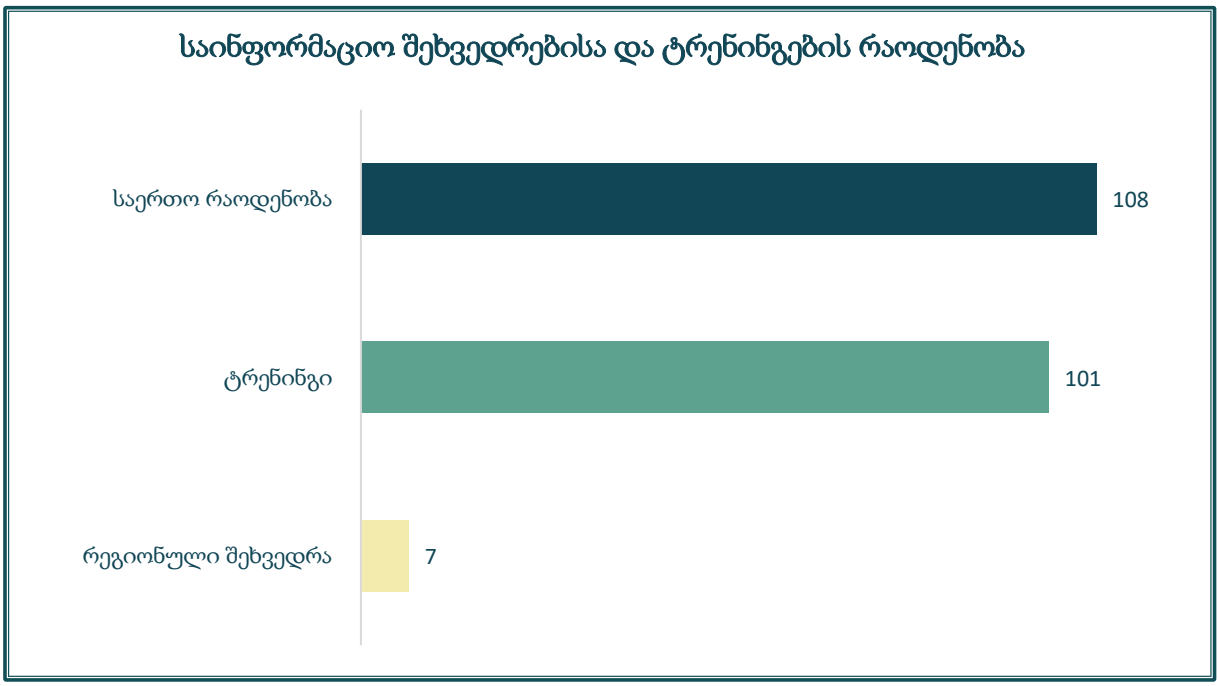
დამსწრე პირთა რაოდენობა

6522

სამსახური აქტიურად ახორციელებს საგანმანათლებლო საქმიანობას მონაცემთა დამუშავებასა და დაცვასთან დაკავშირებულ საკითხებზე. პერსონალურ მონაცემთა დაცვის შესახებ ცნობიერების ამაღლების მიზნით სამსახური სისტემატურად მართავს საჯარო ლექციებს, საინფორმაციო შეხვედრებსა და

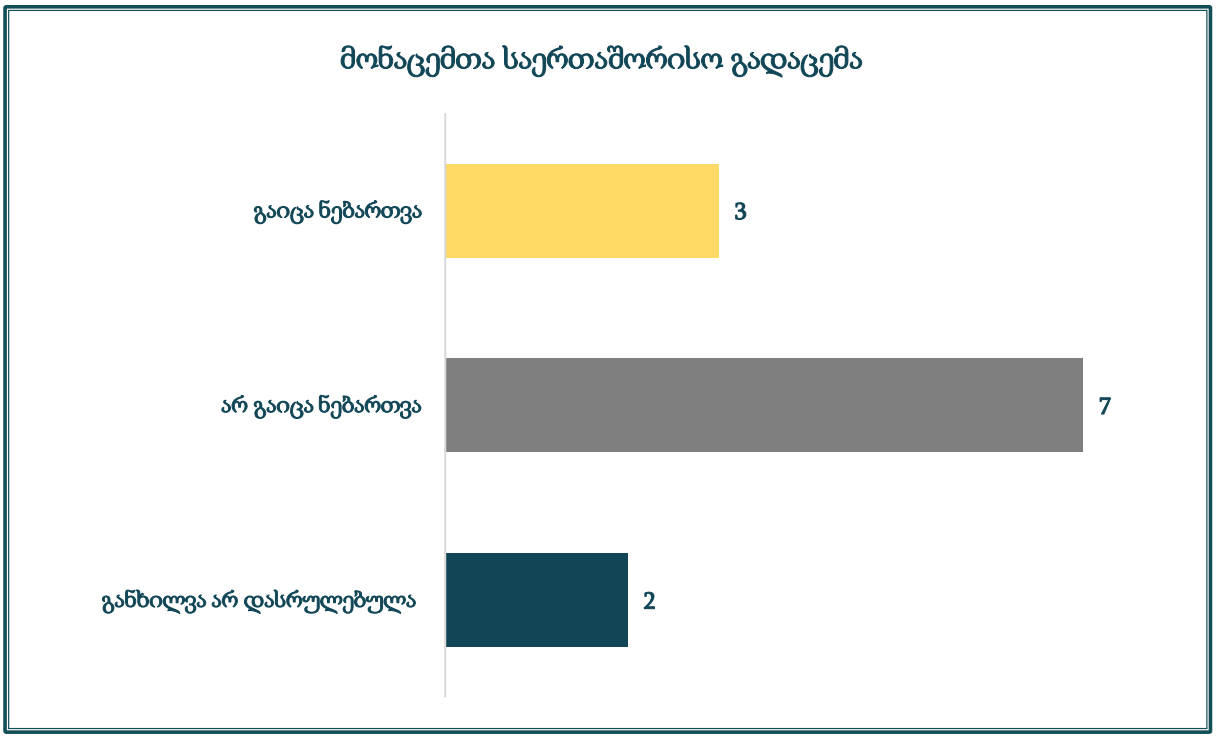
ტრენინგებს კერძო და საჯარო სექტორის, სამართალდამცავი ორგანოების წარმომადგენლებისთვის.

2024 წელს სამსახურმა გამართა 108 შეხვედრა 6522 დამსწრე პირთან, რომელთა ნაწილი წარმოადგენდა როგორც მონაცემთა სუბიექტს, ისე – დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირებს.
2023 წელს სამსახურმა გამართა 62 შეხვედრა 3158 დამსწრე პირთან.



აღსანიშნავია, რომ საანგარიშო პერიოდში გამართული 108 შეხვედრიდან 94% (101) წარმოადგენდა ტრენინგს, ხოლო 6% (7) – რეგიონულ შეხვედრას.

2023 წელს გამართული 62 შეხვედრიდან 90% (56) წარმოადგენდა ტრენინგს, ხოლო 10% (6) – რეგიონულ შეხვედრას.



2024 წლის 31 დეკემბრის მდგომარეობით წარმოება დასრულდა 10 განაცხადთან დაკავშირებით, რომელთაგან მონაცემთა გადაცემის შესახებ 3 შემთხვევაში გაიცა ნებართვა, 7 შემთხვევაში არ გაიცა ნებართვა, ხოლო 2 განაცხადთან დაკავშირებით სამსახურს განხილვა არ დაუსრულებია.

2023 წელს წარმოება დასრულდა 20 განაცხადთან დაკავშირებით და ყველა მათგანზე გაიცა მონაცემთა გადაცემის შესახებ ნებართვა, ხოლო 2 განაცხადთან დაკავშირებით სამსახურს განხილვა არ დაუსრულებია.

საერთაშორისო ხელშეკრულებისა და შეთანხმების პროექტების სამართლებრივი ექსპერტიზა

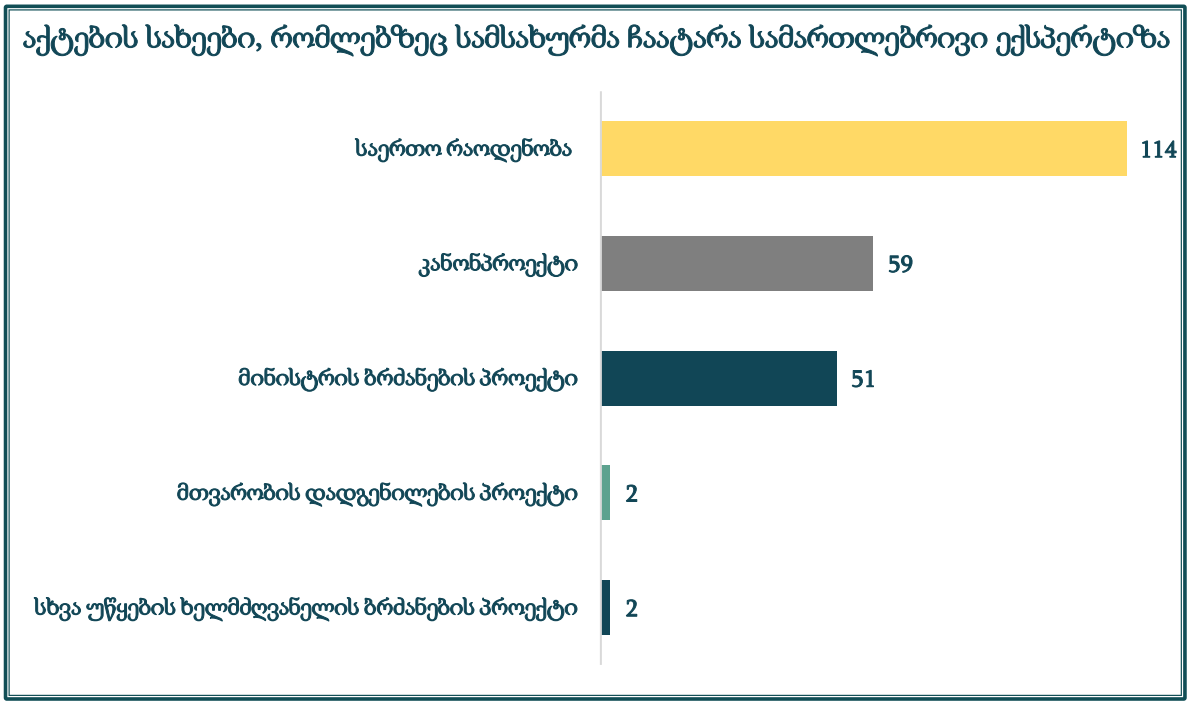
საერთაშორისო ხელშეკრულებისა და შეთანხმების პროექტების სამართლებრივი ექსპერტიზა
13

ექსპერტიზის ფარგლებში სამსახური შეისწავლის წარმოდგენილი საერთაშორისო შეთანხმების პროექტს, შეთანხმების მხარე სახელმწიფოში პერსონალურ მონაცემთა დაცვის საკანონმდებლო და ინსტიტუციურ მექანიზმებს,

რომელთა საფუძველზეც გაიცემა შეთანხმების პროექტში ცვლილებების განხორციელების რეკომენდაცია.

საანგარიშო პერიოდში სამსახურმა ჩაატარა 13 საერთაშორისო შეთანხმების პროექტის ექსპერტიზა, რომელთაგან რეკომენდაცია 4 შემთხვევაში გაიცა.

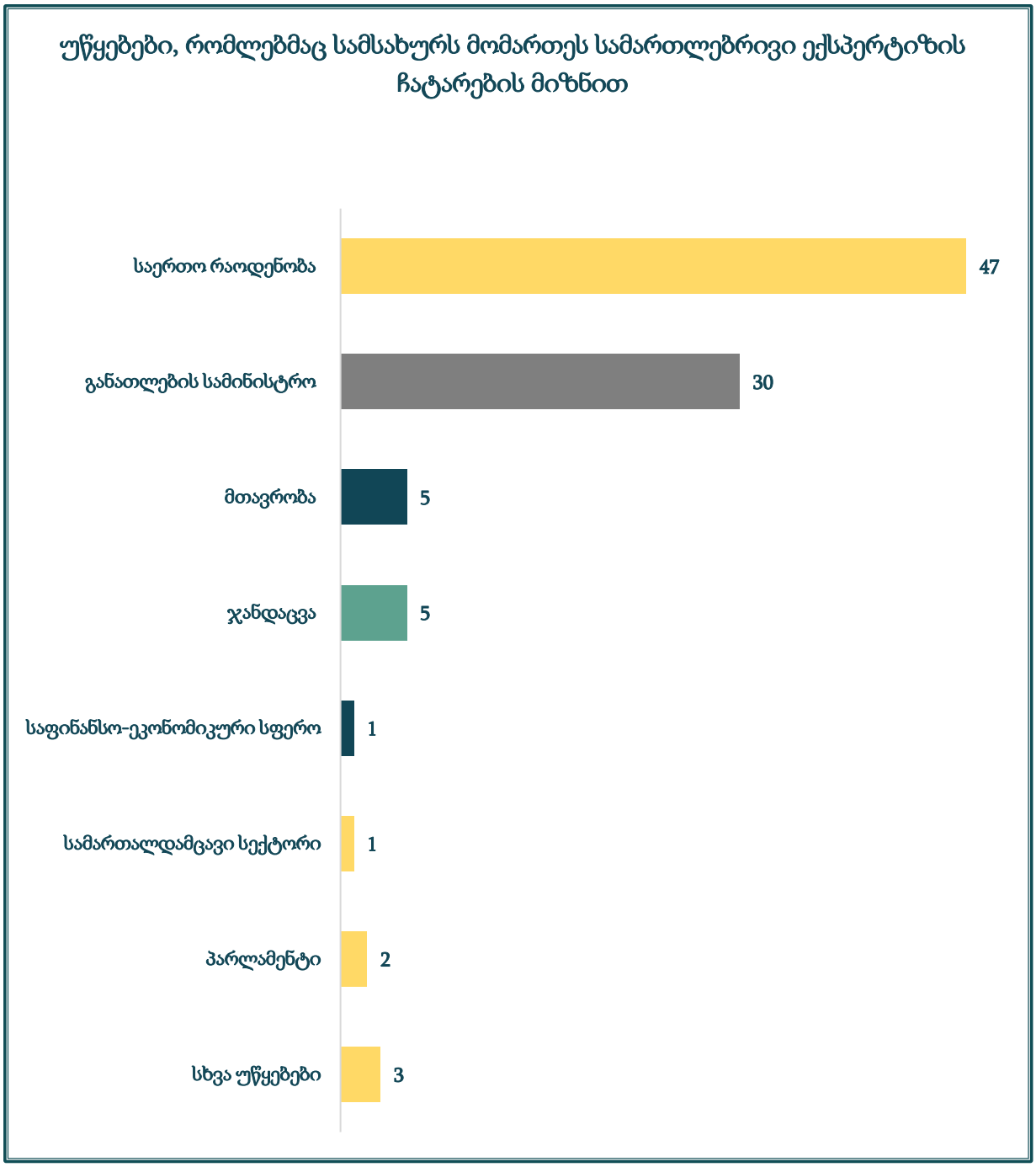
2023 წელს სამსახურმა ჩაატარა საქართველოს სახელით დასადები 12 საერთაშორისო ხელშეკრულებისა და შეთანხმების პროექტების სამართლებრივი ექსპერტიზა, რომელთა ფარგლებში სამსახურის მიერ რეკომენდაცია არ გაცემულა.



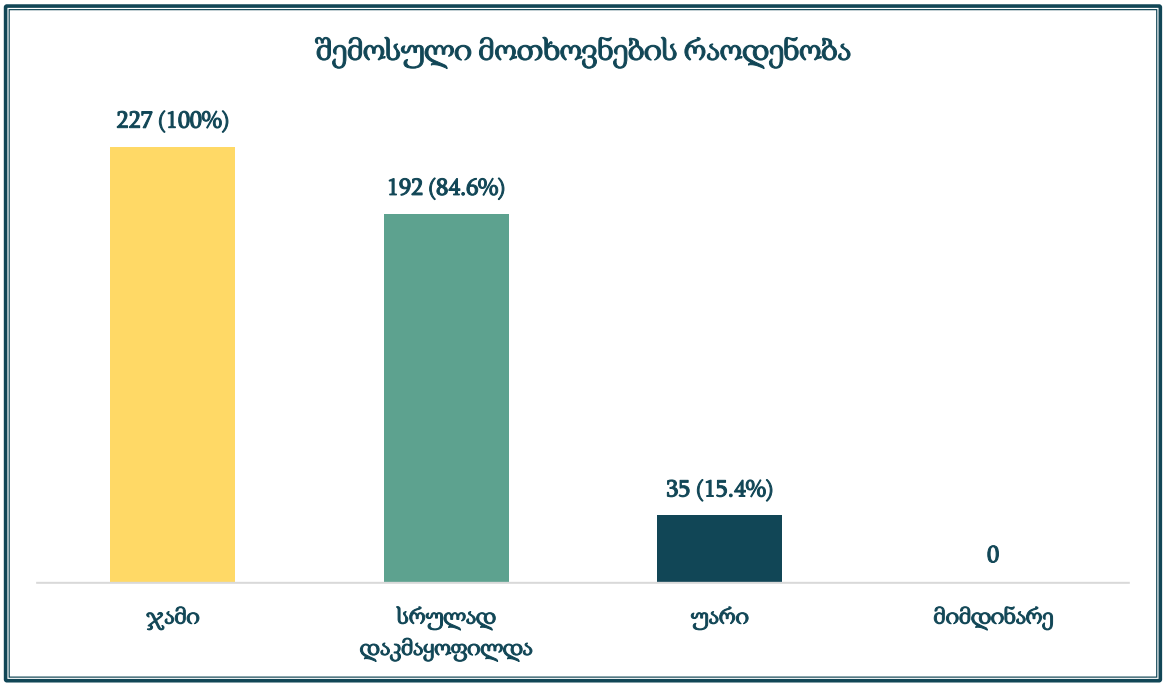
პერსონალურ მონაცემთა დაცვის მაღალი სტანდარტის უზრუნველყოფის მიზნით, სხვა უწყებების მომართვის საფუძველზე, პერსონალურ მონაცემთა დაცვის სამსახური ატარებს საკანონმდებლო და კანონქვემდებარე აქტების პროექტების სამართლებრივ ექსპერტიზას.

2024 წელს სამსახურმა შეაფასა 59 კანონპროექტის, მინისტრის ბრძანების 51 პროექტის, მთავრობის დადგენილების 2 პროექტისა და სხვა უწყების ხელმძღვანელი პირის ბრძანების 2 პროექტის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან შესაბამისობა.

2023 წელს სამსახურმა შეაფასა 141 კანონპროექტის, მინისტრის ბრძანების 21 პროექტის, მთავრობის დადგენილების 5 პროექტისა და სხვა უწყების ხელმძღვანელი პირის ბრძანების 3 პროექტის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან შესაბამისობა.


უწყებები, რომლებმაც სამსახურს მომართეს სამართლებრივი ექსპერტიზის ჩატარების მიზნით
საერთო რაოდენობა
47
განათლების სამინისტრო
30
მთავრობა
5
ჯანდაცვა
5
საფინანსო-ეკონომიკური სფერო
1
სამართალდამცავი სექტორი
1
პარლამენტი
2
სხვა უწყებები
3

საჯარო ინფორმაციის გაცემასთან დაკავშირებით შემოსული მოთხოვნების რაოდენობა



2023 წლის 11 დეკემბრიდან 2024 წლის 10 დეკემბრის ჩათვლით პერსონალურ მონაცემთა დაცვის სამსახურში საჯარო ინფორმაციის გაცემაზე შემოვიდა 227 მოთხოვნა. მათ შორის 192 შემთხვევაში მოთხოვნა დაკმაყოფილდა სრულად, ხოლო 35 შემთხვევაში მოთხოვნა არ დაკმაყოფილდა, რადგან:

- 15 შემთხვევაში ინფორმაცია არ იყო მოთხოვნილი დადგენილი ფორმით, რის გამოც გამოვლინდა ხარვეზი, რომელიც განმცხადებლების მიერ არ შეივსო. შესაბამისად, მოთხოვნები დარჩა განუხილველი, განმცხადებლებს გაეცათ დასაბუთებული პასუხები და განემარტათ გასაჩივრების წესი.
- 20 შემთხვევაში მოთხოვნილი ინფორმაცია პერსონალურ მონაცემთა დაცვის სამსახურში არ იყო დაცული.

საანგარიშო პერიოდში შემოსული ყველა მოთხოვნის განხილვა დასრულებულია.

სამსახურის მიერ განხილული საჩივრები განცხადების/შეტყობინების განუხილველად დატოვების/დაწყებული წარმოების შეწყვეტის შესახებ მიღებულ გადაწყვეტილებებთან დაკავშირებით

15

„პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის წესის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის პირველი მარტის №34 ბრძანების თანახმად, სამსახურის სტრუქტურული ერთეულის ინდივიდუალური სამართლებრივი აქტები შეიძლება გასაჩივრდეს სამსახურში ან სასამართლოში. საანგარიშო პერიოდში სამსახურში გასაჩივრდა განცხადების/შეტყობინების განუხილველად დატოვების/დაწყებული წარმოების შეწყვეტის შესახებ სტრუქტურული ერთეულის ხელმძღვანელის მიერ მიღებული 15 გადაწყვეტილება.

2023 წელს სამსახურში გასაჩივრდა სტრუქტურული ერთეულის ხელმძღვანელის 20 გადაწყვეტილება.

სამართალშემოქმედებითი საქმიანობა

16

2024 წელს პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის უზრუნველყოფის მიზნით სამსახურმა შეიმუშავა 16 კანონქვემდებარე აქტი.

2023 წელს სამსახურმა შეიმუშავა 11 კანონქვემდებარე აქტი.

დანართი №3: საჯარო ინფორმაცია პერსონალურ მონაცემთა დაცვის სამსახურის დაფინანსებისა და ხარჯთაღრიცხვის შესახებ

სამსახურის ბალანსზე რიცხული ავტოსატრანსპორტო საშუალებების ჩამონათვალი მოდელისა და გამოშვების წლების მითითებით:

№	სატრანსპორტო საშუალების დასახელება	გამოშვების წელი
1	KIAOPTIMA; LG917GL	2014
2	HONDACRV;OO781GG	2013
3	TOYOTACAMRY; PP643FF	2019
4	HYUNDAIACCENT WW825UW	2021
5	HYUNDAIACCENT WW816UW	2021
6	HYUNDAIACCENT WW817UW	2021
7	FIAT TIPO BB846YY	2022
8	HYUNDAI ELANTRA GG293GR	2023
9	HYUNDAI ELANTRA; GG291GR;	2023
10	MITSUBISHI L200; MI554MM	2023

2024 წელს განხორციელდა 1 508 437 ლარის სახელმწიფო შესყიდვა, მათ შორის – სამსახურის სრულფასოვანი ფუნქციონირებისათვის 1 448 952 ლარის სახელმწიფო შესყიდვა, წარმომადგენლობითი ხარჯი კი შეადგენდა 59 485 ლარს.

აღსანიშნავია, რომ 2023 წელს განხორციელებული სახელმწიფო შესყიდვების ოდენობა შეადგენდა 1 102 500 ლარს. სამსახურის სრულფასოვანი ფუნქციონირებისათვის განხორციელდა 1 042 182 ლარის სახელმწიფო შესყიდვა, წარმომადგენლობითი ხარჯი კი შეადგენდა 60 318 ლარს.

მის.: საქართველო, თბილისი, ნ. ვაჩნაძის N7, 0105
ბათუმი, ბაქოს N 48, 6010

ტელ.: (+995 32) 242 1000
E-mail: office@pdps.ge
www.pdps.ge