პერსონალურ მონაცემთა
დაცვის სამსახური

პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობის

სპეციალური ანგარიში

„პერსონალურ მონაცემთა დაცვის შესახებ“
საქართველოს კანონის იმპლემენტაცია

© პერსონალურ მონაცემთა დაცვის სამსახური, 2025

სპეციალური ანგარიში მომზადებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 48-ე მუხლის მე-5 პუნქტის შესაბამისად, რომლის თანახმად, პერსონალურ მონაცემთა დაცვის სამსახური უფლებამოსილია, საკუთარი ინიციატივით, ნებისმიერ დროს გამოაქვეყნოს სპეციალური ანგარიში იმ საკითხთა შესახებ, რომლებიც მის საქმიანობას უკავშირდება და მას მნიშვნელოვნად მიაჩნია.

სარჩევი

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მიმართვა..... 4

I თავი. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის მიღება და იმპლემენტაციის სტრატეგია 6

1. ახალი კანონით გათვალისწინებული ინსტიტუტები..... 6

2. ახალი კანონის ამოქმედებამდე განხორციელებული აქტივობები..... 10

II თავი. მონაცემთა უსაფრთხოების დარღვევის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისათვის შეტყობინებისა და მონაცემთა სუბიექტის ინფორმირების ვალდებულება..... 13

1. მონაცემთა უსაფრთხოების დარღვევა 13

1.1. მონაცემთა უსაფრთხოების დარღვევა საჯარო სექტორში 13

1.2. მონაცემთა უსაფრთხოების დარღვევა კერძო სექტორში..... 19

2. პირველად პარამეტრად მონაცემთა დაცვის მნიშვნელობა სუბიექტების ინფორმირების უფლების ჯეროვანი განხორციელებისთვის..... 20

3. მონაცემთა სუბიექტისათვის მონაცემების გამჭვირვალედ დამუშავება 23

3.1. გამჭვირვალობის პრინციპის უზრუნველყოფის შესწავლა საჯარო სექტორში 23

3.2. გამჭვირვალობის პრინციპის უზრუნველყოფის შესწავლა კერძო სექტორში..... 25

4. პერსონალური მონაცემების პირდაპირი მარკეტინგის მიზნით დამუშავება 28

5. აუდიომონიტორინგის განხორციელება 30

6. ვიდეომონიტორინგის გზით პერსონალური მონაცემების დამუშავების კანონიერება..... 37

7. ვიდეომონიტორინგის, აუდიომონიტორინგისა და ბიომეტრიული მონაცემების დამუშავების პროცესების წერილობითი ფორმით განსაზღვრის ვალდებულება..... 42

8. პერსონალურ მონაცემთა დაცვის სამსახურის კანონიერი მოთხოვნის შეუსრულებლობა..... 45

9. დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებული წერილობითი შეთანხმების სავალდებულო პირობები..... 47

10. საქართველოს პროკურატურის მიერ პერსონალურ მონაცემთა დამუშავების კანონიერების გეგმური შემოწმების (ინსპექტირების) შესახებ 52

11. ახალი კანონის 28-ე მუხლით გათვალისწინებული ვალდებულების შესრულება .. 55

III თავი. კონსულტაციები და საგანმანათლებლო აქტივობები 61

1. საკონსულტაციო პლატფორმა 61

1.1. წერილობითი კონსულტაციები 61

1.2. ზეპირი კონსულტაციები..... 62

1.3. საინფორმაციო ლექცია-შეხვედრები 63
2. პერსონალურ მონაცემთა დაცვის ოფიცრებთან განხორციელებული შეხვედრები . 77
2.1. პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული ვალდებულება 77
2.2. ცნობიერების ამაღლება 79
3. ადგილობრივი და რეგიონული შეხვედრები 79
3.1. გარე საინფორმაციო შეხვედრები 79
3.2. შიდა საკონსულტაციო შეხვედრები 80
4. საგანმანათლებლო აქტივობები 80
4.1. ზოგადი სასწავლო კურსები 80
4.2. პერსონალურ მონაცემთა დაცვის ოფიცრებთან განხორციელებული შეხვედრები . 81
4.3. სასწავლო პუბლიკაციები 81

IV თავი. კანონის იმპლემენტაციის პროცესში გამოვლენილი სირთულეები 82

1. სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლთან დაკავშირებით 82
2. იურიდიული პირის, უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის წლიური ბრუნვის საკითხი 87
3. სპეციალური წარმომადგენლები 91
4. პერსონალურ მონაცემთა დაცვის ოფიცრებთან დაკავშირებით 95
4.1. ძირითადი სირთულეები 95
4.2. პრეცედენტული გადაწყვეტილებები 97

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მიმართვა

მაქვს პატივი, წარმოგიდგინოთ პერსონალურ მონაცემთა დაცვის სამსახურის მეორე სპეციალური ანგარიში „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის იმპლემენტაციის თაობაზე.

პერსონალურ მონაცემთა დაცვის კანონმდებლობის ჰარმონიზაცია და კონსოლიდაცია საქართველოს მიერ ევროპის კავშირთან ასოცირების შეთანხმებითა და ასოცირების დღის წესრიგით ნაკისრ ვალდებულებას წარმოადგენს. ასოცირების შეთანხმების თანახმად, საქართველო ვალდებულია, უზრუნველყოს პერსონალურ მონაცემთა დაცვის ეროვნული კანონმდებლობის ჰარმონიზება ევროკავშირის შესაბამის კანონმდებლობასთან. ამ თვალსაზრისით აღსანიშნავია, „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”), რომელიც 2016 წელს ევროპის პარლამენტისა და საბჭოს მიერ იქნა მიღებული და ძალაში შევიდა 2018 წელს. თანამედროვე ტექნოლოგიური პროგრესის გათვალისწინებით, ევროკავშირის რეგულაციით განისაზღვრა პერსონალურ მონაცემთა დაცვის ახალი სტანდარტები, პერსონალურ მონაცემთა დაცვის სფეროს მნიშვნელოვანი ცნებები და ინსტიტუტები.

საქართველოს, როგორც ევროპული სამართლებრივი კულტურისა და ევროპული ინტეგრაციის პროცესში მყოფი ქვეყნისათვის, უაღრესად მნიშვნელოვანია პერსონალურ მონაცემთა დაცვის ეროვნული კანონმდებლობის ჰარმონიზაცია ევროკავშირის კანონმდებლობასთან და შესაბამისად, ახალი დემოკრატიული სტანდარტების იმპლემენტაცია ეროვნულ დონეზე. ახალი კანონის იმპლემენტაციის შედეგად, პერსონალურ მონაცემთა დაცვის მომწესრიგებელი კანონმდებლობა შეესაბამება ევროკავშირის საკანონმდებლო სტანდარტს, რაც უზრუნველყოფს პერსონალური მონაცემის დამუშავებისას ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის ეფექტიან დაცვას, ასევე, პერსონალურ მონაცემთა დაცვის დამოუკიდებელი საზედამხედველო ორგანოს საქმიანობისთვის აუცილებელი, სათანადო მექანიზმებითა და უფლებამოსილებებით აღჭურვას.

2023 წლის 14 ივნისს განხორციელებული საკანონმდებლო ცვლილებები აღსანიშნავია პერსონალურ მონაცემთა დაცვის სამსახურის ინსტიტუციური გაძლიერების, საქართველოს პერსონალურ მონაცემთა დაცვის სამართლის განვითარების, ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვისა და პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლის თვალსაზრისით.
პირადი ცხოვრების ხელშეუხებლობა და პერსონალურ მონაცემთა დაცვა წარმოადგენს ფუნდამენტურ უფლებებს, რომლებიც უზრუნველყოფილია

როგორც საერთაშორისო, ასევე ეროვნული კანონმდებლობით. აღნიშნულ უფლებათა დაცვა ყველასთვის თანაბრად მნიშვნელოვანია და სწორედ ამ მიზნით, ახალი კანონით დიდი მნიშვნელობა მიენიჭა პერსონალურ მონაცემთა დაცვის დამოუკიდებელი საზედამხედველო ორგანოს სათანადო მექანიზმებითა და უფლებამოსილებებით აღჭურვას, როგორც საჯარო და კერძო სექტორთან, აგრეთვე, სამართალდამცავ ორგანოებთან მიმართებით. ამ თვალსაზრისით აღსანიშნავია, რომ გაიზარდა პერსონალური მონაცემების საზედამხედველო ორგანოს გამჭვირვალობა და ანგარიშვალდებულება, პერსონალურ მონაცემთა დაცვის სფეროს მომწესრიგებელი კანონმდებლობა მეტად განჭვრეტადი გახდა და შემუშავდა ადამიანის უფლებათა დაცვაზე ორიენტირებული პერსონალურ მონაცემთა დაცვის მდგრადი და ეფექტიანი მექანიზმები. კანონმდებლობა მნიშვნელოვნად დაუახლოვდა ევროპულ სტანდარტებს და საქართველოს მიერ ნაკისრი საერთაშორისო ვალდებულებების შესრულებას შეუწყო ხელი, რაც, თავის მხრივ, განაპირობებს ჩვენს ქვეყანაში საერთაშორისოდ აღიარებული პრინციპებისა და საუკეთესო პრაქტიკის დამკვიდრებას.

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 შესახებ“ საქართველოს ახალი კანონის მიღება და იმპლემენტაციის სტრატეგია

1. ახალი კანონით გათვალისწინებული ინსტიტუტები

2023 წლის 14 ივნისს საქართველოს პარლამენტმა მიიღო „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი[1], რომელმაც შეცვალა პერსონალურ მონაცემთა დაცვის სფეროში დამკვიდრებული ტერმინები (მაგალითად: ტერმინი „დამმუშავებელი“ შეიცვალა „დამუშავებისთვის/თანადამუშავებისთვის პასუხისმგებელი პირით“, „უფლებამოსილი პირი“ – „დამუშავებაზე უფლებამოსილი პირით“). ასევე კანონით განიმარტა და დამკვიდრდა სრულიად ახალი ცნებები (მაგალითად: ტერმინი „თანადამმუშავებელი“, რაც გულისხმობს მონაცემთა ორი ან მეტი პირის მიერ, ერთობლივად განსაზღვრული მიზნითა და საშუალებებით დამუშავებას). ამასთანავე, განისაზღვრა ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემისა და გენეტიკური მონაცემის ცნებები, აუდიომონიტორინგის განხორციელების საფუძვლები, აუდიო ჩაწერის პირობებში მონაცემთა დამუშავების კანონიერების წესები და პირობები. აგრეთვე, გარკვეული ცვლილებები განიცადა ვიდეომონიტორინგის განხორციელებისთვის არსებულმა მოწესრიგებამ.

საკანონმდემბლო სიახლეებიდან აღსანიშნავია არასრულწლოვნისა და გარდაცვლილი პირის პერსონალურ მონაცემთა დაცვა, მათი დამუშავებისას თანხმობის მოპოვების წესი და პირობები. ახალი კანონით განსაზღვრულ ინსტიტუტებს შორის ასევე საგულისხმოა: პროფაილინგი, მონაცემთა უსაფრთხოების დარღვევა (ინციდენტი), მონაცემთა უსაფრთხოების მიზნებისთვის მათი დეპერსონალიზაცია/ფსევდონიმიზაცია. ამავდროულად, გაფართოვდა, ხოლო ცალკეულ შემთხვევებში, დაკონკრეტდა მონაცემთა დამუშავების საფუძვლები, დამკვიდრდა მონაცემთა დამუშავების პრინციპები, როგორიცაა: გამჭვირვალობის, გაუმართლებელი დაყოვნების გარეშე მონაცემების წაშლა/განადგურებისა და მონაცემთა უსაფრთხოების პრინციპები.

საკანონმდებლო ცვლილებათაგან განსაკუთრებით აღსანიშნავია მონაცემთა სუბიექტის უფლებათა გაფართოებული წრე და მათი დაცვის გარანტიები. განისაზღვრა პერსონალურ მონაცემთა დაცვის ოფიცრისა და სპეციალური წარმომადგენლის ინსტიტუტები, პერსონალურ მონაცემთა დამუშავებასთან

[1] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 3144-XIმს-Xმპ, 03/07/2023.

დაკავშირებული მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინებისა და მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულებები.

საგულისხმოა, რომ ახალი საკანონმდებლო მოწესრიგებით შეიცვალა ადმინისტრაციული სამართალდარღვევებისთვის გათვალისწინებული ადმინისტრაციული პასუხისმგებლობის მასშტაბიც. მართალია, კანონი ფიქსირებული ჯარიმის ოდენობებს განსაზღვრავს, თუმცა საგრძნობლად გაზრდილია მათი მოცულობა. კერძოდ, ჯარიმის ოდენობა დაუკავშირდა სამართალდამრღვევის ორგანიზაციულსამართლებრივ ფორმასა და მის წლიურ ბრუნვას. ამავდროულად, განისაზღვრა ადმინისტრაციული სამართალდარღვევისთვის დადგენილი პასუხისმგებლობის ზომის შემამსუბუქებელი და დამამძიმებელი გარემოებები, ხოლო სამართალდარღვევათა თვალსაზრისით, მნიშვნელოვან სიახლეს წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის კანონიერი მოთხოვნის შეუსრულებლობის ადმინისტრაციულ სამართალდარღვევად მიჩნევა, რაც, არსებული პრაქტიკის გათვალისწინებით, ხელს უწყობს პერსონალურ მონაცემთა დაცვის სამსახურის მიერ მიღებული გადაწყვეტილებების ეფექტიან აღსრულებასა და ქვეყანაში პერსონალურ მონაცემთა დაცვის საერთო მდგომარეობის გაუმჯობესებას.

საკანონმდებლო სიახლეთაგან განსაკუთრებით მნიშვნელოვანია საჯარო და გარკვეულ კერძო დაწესებულებებში პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ან განსაზღვრის ვალდებულება. კანონის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი ან დამუშავებაზე უფლებამოსილი პირი განსაზღვრავს ან ნიშნავს ოფიცერს, რომელიც უზრუნველყოფს:

- მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე, დამუშავებისთვის პასუხისმგებელი პირის, დამუშავებაზე უფლებამოსილი პირისა და მათი თანამშრომლების ინფორმირებას, მათთვის კონსულტაციისა და მეთოდური დახმარების გაწევას;
- მონაცემთა დამუშავებასთან დაკავშირებული შიდა რეგულაციებისა და მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის შემუშავებაში მონაწილეობას, აგრეთვე დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ საქართველოს კანონმდებლობისა და შიდა ორგანიზაციული დოკუმენტების შესრულების მონიტორინგს;
- მონაცემთა დამუშავებასთან დაკავშირებით შემოსული განცხადებებისა და საჩივრების ანალიზსა და შესაბამისი რეკომენდაციების გაცემას;

- პერსონალურ მონაცემთა დაცვის სამსახურისგან კონსულტაციების მიღებას, დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის წარმომადგენლობას სამსახურთან ურთიერთობაში;
- მონაცემთა სუბიექტის მიმართვის შემთხვევაში მისთვის მონაცემთა დამუშავების პროცესებისა და მისი უფლებების შესახებ ინფორმაციის მიწოდებას;
- ასევე, პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავების სტანდარტების ამაღლების მიზნით სხვა ფუნქციების შესრულებას.

კანონის 33-ე მუხლის თანახმად, ოფიცრის დანიშვნის ან განსაზღვრის ვალდებულება ეკისრებათ საჯარო დაწესებულებებს, სადაზღვევო ორგანიზაციებს, კომერციულ ბანკებს, მიკროსაფინანსო ორგანიზაციებს, საკრედიტო ბიუროებს, ელექტრონული კომუნიკაციის კომპანიებს, ავიაკომპანიებს, აეროპორტებს, სამედიცინო დაწესებულებებს, აგრეთვე დამუშავებისთვის პასუხისმგებელ და დამუშავებაზე უფლებამოსილ იმ პირებს, რომლებიც ამუშავებენ დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან ახორციელებენ მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს. ამასთან, პირთა წრე, რომელსაც არ აქვს ვალდებულება, დანიშნოს ან განსაზღვროს პერსონალურ მონაცემთა დაცვის ოფიცერი, მოწესრიგებულია პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის კანონქვემდებარე ნორმატიული აქტით.

კერძო სექტორში პერსონალურ მონაცემთა დამუშავების თვალსაზრისით, საკანონმდებლო ცვლილება შეეხო სარეკლამო ხასიათის შეტყობინებების მომხმარებლებისთვის გაგზავნის წესებსა და პირობებს. კანონით ახლებურად განსაზღვრა პირდაპირ მარკეტინგთან დაკავშირებული საკითხები, კერძოდ, იგი განიმარტება, როგორც ტელეფონის, ფოსტის, ელექტრონული ფოსტის ან სხვა ელექტრონული საშუალებით მონაცემთა სუბიექტისთვის ინფორმაციის პირდაპირ და უშუალო მიწოდება ფიზიკური პირის ან/და იურიდიული პირის, საქონლის, იდეის, მომსახურების, სამუშაოს ან/და წამოწყების, აგრეთვე საიმიჯო და სოციალური თემატიკისადმი ინტერესის ფორმირების, შენარჩუნების, რეალიზაციის ან/და მხარდაჭერის მიზნით. ამასთან, პირდაპირ მარკეტინგად არ მიიჩნევა სახელმწიფო დაწესებულების მიერ ფიზიკური პირისთვის ინფორმაციის მიწოდება, თუ ამ ინფორმაციის მიწოდება თავსებადია ამ კანონით გათვალისწინებულ მონაცემთა დამუშავების რომელიმე საფუძველთან. საყურადღებოა, რომ მიუხედავად მონაცემთა შეგროვების ან/და მოპოვების საფუძვლისა და მათი ხელმისაწვდომობისა, პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავება შესაძლებელია მხოლოდ მონაცემთა სუბიექტის

თანხმობით. მონაცემთა სუბიექტის სახელის, გვარის, მისამართის, ტელეფონის ნომრისა და ელექტრონული ფოსტის მისამართის გარდა, პირდაპირი მარკეტინგის მიზნით სხვა მონაცემთა დამუშავებისთვის აუცილებელია მონაცემთა სუბიექტის წერილობითი თანხმობა. აღსანიშნავია ისიც, რომ მონაცემთა სუბიექტის თანხმობის მიღებამდე და პირდაპირი მარკეტინგის განხორციელებისას დამუშავებისთვის პასუხისმგებელმა პირმა ან/და 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.

კანონით განისაზღვრა მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულება, რაც პერსონალურ მონაცემთა დაცვის ქართული კანონმდებლობისთვის სიახლეს წარმოადგენს და ადამიანის უფლებების დარღვევის მომეტებული საფრთხეების შემცირებას ისახავს მიზნად. კანონის 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. გარდა ამისა, კანონით დადგენილია ზეგავლენის შეფასების სავალდებულო განხორციელების კონკრეტული შემთხვევები. ამგვარი ვალდებულება არსებობს, თუ დამუშავებისთვის პასუხისმგებელი პირი:

- მონაცემთა სუბიექტისთვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებს სრულად ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე;
- ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემებს (მონაცემთა სუბიექტების დიდ რაოდენობად მიიჩნევა საქართველოს მოსახლეობის არანაკლებ 3 პროცენტისა);
- ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში.

კანონის თანახმად, მონაცემთა დაცვაზე ზეგავლენის შეფასებისას, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, შექმნას წერილობითი დოკუმენტი, რომელიც შეიცავს მონაცემთა კატეგორიის, მათი დამუშავების მიზნების, პროპორციულობის, პროცესისა და საფუძვლების აღწერას; ასევე, ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეების შეფასებას და მონაცემთა უსაფრთხოების დაცვის მიზნით

გათვალისწინებული ორგანიზაციულ-ტექნიკური ზომების აღწერას. პასუხისმგებელი პირი ვალდებულია, მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი შეინახოს მონაცემთა დამუშავების მთელი პერიოდის განმავლობაში, ხოლო მონაცემთა დამუშავების შეწყვეტის შემთხვევაში – არანაკლებ ერთი წლის ვადით. ისეთ შემთხვევებში კი, როცა ზეგავლენის შეფასების შედეგად გამოვლინდება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის მაღალი საფრთხე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მიიღოს ყველა აუცილებელი ზომა იდენტიფიცირებული საფრთხეების არსებითად შესამცირებლად. ასევე, საჭიროების შემთხვევაში, იგი უფლებამოსილია, კონსულტაციის მიზნით მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს. აღსანიშნავია, რომ თუ დამატებითი ორგანიზაციულ-ტექნიკური ზომებით შეუძლებელია ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის არსებითად შემცირება, მონაცემთა დამუშავება არ უნდა განხორციელდეს.

2. ახალი კანონის ამოქმედებამდე განხორციელებული აქტივობები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ეტაპობრივ ამოქმედებასთან ერთად, გამოიკვეთა ის ძირითადი ტენდენციები, რაც, ერთი მხრივ, საკანონმდებლო ცვლილებების მიზნობრიობასა და დროულობაზე მეტყველებს, ხოლო, მეორე მხრივ, ცხადჰყოფს პერსონალურ მონაცემთა დაცვის სამსახურის გაძლიერებული მანდატის ფარგლებში განხორციელებული და სამომავლოდ დაგეგმილი ღონისძიებების გატარების აუცილებლობას.

საქართველოში პირადი ცხოვრების ხელშეუხებლობის, მათ შორის, პერსონალურ მონაცემთა დაცვის უზრუნველყოფაზე ინსტიტუციური ზედამხედველობის ფარგლებში, მონაცემთა დამუშავების კანონიერებაზე კონტროლის მიზნით, პერსონალურ მონაცემთა დაცვის სამსახური მუდმივ რეჟიმში შეისწავლის საჯარო და კერძო სექტორის წარმომადგენლების, სამართალდამცავ ორგანოთა მიერ პერსონალურ მონაცემთა დამუშავების კანონიერებას, როგორც საკუთარი ინიციატივით — გეგმური ინსპექტირების, ასევე არაგეგმური ინსპექტირების, მათ შორის, დაინტერესებული პირების შეტყობინებისა და მოქალაქეთა განცხადების საფუძველზე. სამსახური მონაცემთა არაკანონიერი დამუშავების ფაქტებზე რეაგირებისას ორიენტირებულია არა მხოლოდ ადმინისტრაციული სახდელის დაკისრებაზე, არამედ მონაცემთა დამუშავებისას აღმოჩენილ ნაკლოვანებათა აღმოფხვრაზეც. გამოვლენილი ხარვეზების აღმოფხვრის მიზნით, სამსახური გამოსცემს რეკომენდაციებს და შესასრულებლად სავალდებულო დავალებებს,

ასევე, ახორციელებს პრევენციულ ღონისძიებებს, მათ შორის, კონსულტაციას უწევს დაინტერესებულ პირებს, ზრუნავს საზოგადოების ცნობიერების ამაღლებაზე, მართავს საინფორმაციო შეხვედრებსა და ტრენინგებს, გამოსცემს სარეკომენდაციო ხასიათის სახელმძღვანელო მითითებებს და ამზადებს ყოველწლიურ ანგარიშს მონაცემთა დაცვის მდგომარეობის, ფარული საგამოძიებო მოქმედებების ჩატარებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლის შესახებ.

ზემოხსენებული მანდატის ფარგლებში, 2023 წლის 14 ივნისის კანონის იმპლემენტაციის პროცესების ეფექტიანად წარმართვის მიზნით, სამსახურმა შეიმუშავა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის იმპლემენტაციის სტრატეგია და სამოქმედო გეგმა, რომელმაც გააერთიანა სამსახურის ამოცანები, აქტივობები, მათი შესრულების ინდიკატორები, აქტივობებზე პასუხისმგებელი თუ დამხმარე სტრუქტურული ერთეულები და ამოცანებისა თუ ცალკეული აქტივობების შესრულების ვადები.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 88-ე მუხლის მე-4 პუნქტის შესაბამისად, გამოიცა პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის კანონქვემდებარე ნორმატიული აქტები. ამასთანავე, ახალი კანონის ამოქმედებამ რიგი ცვლილებები გამოიწვია პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის კანონქვემდებარე ნორმატიულ აქტებშიც, მათ შორის, გადამუშავდა ბრძანება „პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის წესის დამტკიცების შესახებ“ და დამკვიდრდა მონაცემთა დამუშავების კანონიერების შესწავლის ახალი, სპეციფიკური მიდგომები და რეგულაციები.

კანონით გათვალისწინებული სიახლეების კომპლექსურობიდან გამომდინარე, პერსონალურ მონაცემთა დაცვის სამსახური აქტიურად ცდილობს მონაცემთა დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირების დახმარებას, დანერგონ პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული საუკეთესო პრაქტიკა საკუთარ პროცესებში. ამ მიზნით სამსახურმა იხელმძღვანელა მსოფლიოში ერთ-ერთი აპრობირებული და ეფექტიანი საშუალებით, ე. წ. „რბილი სამართლის“ ინსტრუმენტების შემუშავებით და ყველა იმ საკითხთან დაკავშირებით, რომლებიც დამატებით განმარტებებს საჭიროებდა, გამოიცა შესაბამისი სახელმძღვანელოები და რეკომენდაციები.

სექტორული სამართლებრივი აქტების „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალ კანონთან უზრუნველყოფის მხარდაჭერის მიზნით, სამსახურმა შეიმუშავა სპეციალური კითხვარი, რომლის მეშვეობითაც დადგინდა და შეფასდა საჯარო და კერძო დაწესებულებების მზადყოფნა ახალი კანონით გათვალისწინებულ მოთხოვნებთან მიმართებით.

კანონის იმპლემენტაციის პროცესში პერსონალურ მონაცემთა დაცვის სამსახურმა დაგეგმა და განახორციელა არაერთი მნიშვნელოვანი გასვლითი თუ ადგილობრივი ღონისძიება პერსონალურ მონაცემთა დაცვის საკითხებზე საზოგადოების ცნობიერების ასამაღლებლად, მათ შორის, სექტორული შეხვედრები სხვადასხვა მსხვილ მონაცემთა დამმუშავებელთან, როგორც საჯარო, ისე კერძო სექტორში. ძირითადი აქცენტი კი გაკეთდა ისეთ სფეროებზე, რომლებიც უკავშირდება საფინანსო სექტორს, ჯანდაცვას, სადაზღვევო საქმიანობას, ელექტრონულ მმართველობას, საგანმანათლებლო საქმიანობას და სხვა. შეხვედრების საერთო რაოდენობამ 2024 წლის პირველი იანვრიდან - 2024 წლის 31 დეკემბრამდე პერიოდში შეადგინა 108(ას რვა), რომელსაც ესწრებოდა ჯამში 6522 (ექვსი ათას ხუთას ოცდაორი) პირი.

2024 წლის თებერვალში, გაიმართა მნიშვნელოვანი, ფართომასშტაბიანი შეხვედრა ყველა მსხვილი, საჯარო დაწესებულების უმაღლეს მმართველ რგოლთან, რომლის ფარგლებშიც დამსწრე აუდიტორიას წარედგინა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონისა და სამსახურის მიერ კანონის იმპლემენტაციის მიზნით მომზადებული სამართლებრივი აქტები და სახელმძღვანელო რეკომენდაციები. ამასთან, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის სივრცეში მოწყობილ პერსონალურ მონაცემთა დაცვის სტენდთან ჩაიწერა და სოციალურ ქსელში გავრცელდა ე. წ. „პოდკასტები“, რომლის ფარგლებშიც სამსახურის თანამშრომლებმა მიმოიხილეს ახალი კანონით განსაზღვრული ყველა მნიშვნელოვანი სიახლე და მათი პრაქტიკაში განხორციელების, იმპლემენტაციის საკითხი.

2023 წლის პირველი დეკემბრიდან, პერსონალურ მონაცემთა დაცვის სამსახური ახალი კანონით გათვალისწინებულ ცვლილებებთან დაკავშირებით, სამსახურმა დანერგა ინდივიდუალური საკონსულტაციო ხასიათის შეხვედრები ნებისმიერ დაინტერესებულ პირთან, მათ შორის, კერძო და საჯარო უწყების წარმომადგენლებთან, რაც უწყვეტ რეჟიმში მიმდინარეობს ყოველი კვირის პარასკევ დღეს, სამსახურის ოფისში. საანგარიშო პერიოდში ჯამში 292 (ორას ოთხმოცდათორმეტ) პირს გაეწია კონსულტაცია.

II თავი. მონაცემთა უსაფრთხოების დარღვევის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისათვის შეტყობინებისა და მონაცემთა სუბიექტის ინფორმირების ვალდებულება

1. მონაცემთა უსაფრთხოების დარღვევა

1.1. მონაცემთა უსაფრთხოების დარღვევა საჯარო სექტორში

საანგარიშო პერიოდში სამსახურმა შეისწავლა მონაცემთა უსაფრთხოებასთან დაკავშირებული რამდენიმე ფაქტი. ერთ-ერთი შემთხვევის ფარგლებში გამოვლინდა, რომ საჯარო დაწესებულება (დამუშავებაზე უფლებამოსილი პირი) ახორციელებდა იმ ელექტრონული სისტემის მართვასა და ადმინისტრირებას, რომელშიც სხვადასხვა მუნიციპალური სერვისის მიღების მიზნით, დაინტერესებული ფიზიკური პირები და ორგანიზაციები რეგისტრირდებოდნენ. ამასთან, მითითებული სისტემის მეშვეობით, საჯარო უწყებას ჰქონდა სსიპ — სერვისების განვითარების სააგენტოს მონაცემთა ელექტრონულ ბაზაზე რეალურ დროში დაშვებისა და ფიზიკურ პირებზე ინფორმაციის მიღების შესაძლებლობა, ხოლო ელექტრონულ სისტემაში მომხმარებლის რეგისტრაციის მეთოდი იძლეოდა სხვა პირის საიდენტიფიკაციო მონაცემებით რეგისტრაციის შესაძლებლობას, ვინაიდან ანგარიშის შესაქმნელად საჭირო იყო ორი ზუსტი მონაცემი — გვარი და პირადი ნომერი, თუმცა ელექტრონული ფოსტის მისამართად და სატელეფონო ნომრად შეიძლებოდა გამოყენებულიყო ის მონაცემი, რომელსაც რეგისტრაციის განმახორციელებელი პირი ფლობდა. შესწავლის შედეგად დადგინდა, რომ ინციდენტის განმახორციელებელმა სუბიექტმა ზემოაღნიშნულ ელექტრონულ სისტემაში რამდენიმე მომხმარებლის ანგარიშის რეგისტრაციის მიზნით მიითვისა ამ პირების საჯაროდ ხელმისაწვდომი გვარი და პირადი ნომერი. ფიზიკური პირები, რომელთა მონაცემებიც მითვისებულ იქნა, წარმოადგენდნენ სამეწარმეო სუბიექტების დირექტორებს/ხელმძღვანელებს. ინციდენტის განმახორციელებელმა ელექტრონულ სისტემაში შექმნა სამეწარმეო სუბიექტების დირექტორების/ხელმძღვანელების მომხმარებლები, ხოლო რეგისტრაციის პროცესში გამოიყენა ერთჯერადი “Email” სერვისის პროვაიდერების დომეინზე რეგისტრირებული ელექტრონული ფოსტის მისამართები, რომლის მეშვეობითაც მიიღო სხვა პირების მომხმარებლების რეგისტრაციის პროცესის წარმატებით დასრულებისათვის საჭირო ინფორმაცია. აღნიშნულის შემდეგ, მითითებული ელექტრონული სისტემის ერთ-ერთი ფუნქციონალის (ხელმძღვანელის მიერ სამეწარმეო სუბიექტის წარმომადგენლებად სხვა პირების დამატების

ფუნქციონალი) მეშვეობით, სხვადასხვა გვარებისა და პირადი ნომრების ასახვით, რამდენიმე დღის განმავლობაში, მოთხოვნები გააგზავნა სსიპ — 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 (მაგალითად, ტელეფონის ნომერი, მისამართი, ელექტრონული ფოსტის მისამართი და სხვა) მოპოვების შესაძლებლობა ჰქონდა მხოლოდ მაშინ, თუ კონკრეტული პირის გვარი და პირადი ნომერი რეგისტრირებული იქნებოდა, როგორც დამუშავებაზე უფლებამოსილi პირის მართვისა და ადმინისტრირების ქვეშ არსებულ ელექტრონულ სისტემაში, ისე სსიპ — სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ელექტრონულ ბაზაში. ინციდენტის განმახორციელებელი პირის მიერ გაგზავნილი ასი ათასობით მოთხოვნიდან ათეულობით ათას შემთხვევაში ფიზიკური პირების გვარები და პირადი ნომრები ერთმანეთს ორივე ბაზაში დაემთხვა. შესაბამისად, ინციდენტის განმახორციელებელმა პირმა მოიპოვა რამდენიმე ათეულობით ათასი პირის სხვადასხვა პერსონალური მონაცემი (მაგალითად, ტელეფონის ნომერი, მისამართი, ელექტრონული ფოსტის მისამართი და სხვა).

საქმის შესწავლის ფარგლებში დადგინდა, რომ 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, ხოლო პირის გვარი და პირადი ნომერი საჯარო რეესტრისა და სხვა საჯაროდ ხელმისაწვდომი მონაცემთა ბაზების გათვალისწინებით მარტივად მოპოვებადი ინფორმაციაა. 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, რომელიც გათვალისწინებული იყო სააგენტოსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებულ ხელშეკრულებაში, თუმცა ამ მონაცემებიდან სხვადასხვა სერვისს განსხვავებული მოცულობის ინფორმაცია სჭირდებოდა. გარდა ამისა,

უწყებას შემუშავებული არ ჰქონდა ელექტრონულ სისტემაში მონაცემების მიმართ განხორციელებული მოქმედებების აღრიცხვის (ე. წ. „ლოგირების“) სრულყოფილი მექანიზმი. ასევე, გათვალისწინებული არ იყო ინციდენტის დროული გამოვლენისთვის მნიშვნელოვანი ორგანიზაციულ-ტექნიკური ზომები, რაც არსებითია ინციდენტის მიმდინარეობის პროცესის შეწყვეტისა და გამოწვეული შედეგების შემსუბუქებისათვის.

ინციდენტის განხორციელების პერიოდში, განსაკუთრებულად მაღალი აქტივობის შესახებ, სსიპ — სახელმწიფო სერვისების განვითარების სააგენტომ აცნობა დამუშავებაზე უფლებამოსილ პირს, რომელმაც ელექტრონულ სისტემაში გაატარა გარკვეული სახის უსაფრთხოების ზომები, ასევე, ინფორმაცია მიაწოდა საგამოძიებო ორგანოსა და დამუშავებისათვის პასუხისმგებელ პირს. გარდა ამისა, შემოწმების ფარგლებში დადგინდა, რომ ერთ-ერთ ვებგვერდზე, გასაყიდად და პოტენციური მყიდველებისთვის საილუსტრაციოდ, ღიად მითითებული და განთავსებული იყო ათასობით ფიზიკური პირის პერსონალური მონაცემი. აღნიშნულზე ინფორმაციას ფლობდა მოცემული ელექტრონული სისტემის მართვაზე და ადმინისტრირებაზე პასუხისმგებელი საჯარო დაწესებულება, ხოლო ღიად განთავსებული პირების მონაცემები ასახული იყო იმ ელექტრონულ სისტემაში, რომლის საშუალებითაც ინციდენტის განმახორციელებელმა არასანქცირებულად იმოქმედა.

მიუხედავად იმისა, რომ სახეზე იყო ინციდენტი, დამუშავებაზე უფლებამოსილმა პირმა და დამუშავებისათვის პასუხისმგებელმა პირმა არ აღრიცხეს იგი. ამასთან, დამუშავებისათვის პასუხისმგებელმა პირმა არ შეაფასა, თუ რა სახის ზიანს გამოიწვევდა ინციდენტი ან/და რა სახის საფრთხეს შეუქმნიდა ადამიანის ძირითად უფლებებსა და თავისუფლებებს. შესაბამისად, მან ინციდენტის თაობაზე არ შეატყობინა სამსახურს და არც მონაცემთა სუბიექტების ინფორმირება მოახდინა.

საქმის შესწავლის ფარგლებში მოპოვებულ მტკიცებულებებზე 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. შესწავლის ფარგლებში გამოვლინდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე, 29-ე და 30-ე მუხლების დარღვევა. შესაბამისად, დამუშავებაზე უფლებამოსილ პირსა და დამუშავებისათვის პასუხისმგებელ პირს დაევალათ ინციდენტის აღრიცხვა,

ხოლო დამუშავებისათვის პასუხისმგებელ პირს ინციდენტის თაობაზე სამსახურისათვის შეტყობინება და მონაცემთა სუბიექტების ინფორმირება.

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

შესწავლის დაწყებისთანავე ცხადი იყო, რომ გასაჯაროებული დოკუმენტი შეიცავდა ორასამდე ფიზიკური პირის სახელს, გვარს, პირად ნომერს, ჩატარებული სამედიცინო კვლევების დასახელებასა და თარიღს. სახელმწიფო შესყიდვის ობიექტს წარმოადგენდა სამედიცინო-მოლეკულური კვლევების თაობაზე მომსახურების შესყიდვა. დოკუმენტში მითითებული კვლევები ტარდებოდა სხვადასხვა დიაგნოზის მქონე ონკოლოგიურ პაციენტებში, სათანადო მკურნალობის შერჩევის მიზნით. პლატფორმა, სადაც დოკუმენტი გასაჯაროვდა — სახელმწიფო შესყიდვების პორტალი, უზრუნველყოფს საჯარო დაწესებულებების მიერ შესყიდვების განხორციელებას ღია და გამჭვირვალე ელექტრონული ტენდერების მეშვეობით. პორტალის ადმინისტრირებას ახორციელებს სსიპ — სახელმწიფო შესყიდვების სააგენტო. ამასთან, შემსყიდველი ორგანიზაცია განსაზღვრავს ტენდერში წარსადგენი დოკუმენტების ნუსხას, ხოლო მონაწილე ორგანიზაცია — პრეტენდენტი შესაბამის დოკუმენტებს სისტემაში ტვირთავს დამოუკიდებლად. საყურადღებოა, რომ ელექტრონულ ტენდერთან დაკავშირებით სისტემაში განთავსებული ინფორმაცია საჯაროა, ხოლო პრეტენდენტს მათი წაშლის შესაძლებლობა არ აქვს. შესაბამისად იმისათვის, რომ არსებითად შემცირებულიყო დოკუმენტში მითითებული ფიზიკური პირების ზიანი, შესწავლის დასრულებამდე, სამსახურმა დაბლოკა მათი მონაცემები. აღნიშნულის შედეგად, საჯარო ვებგვერდის ვიზიტორებს დოკუმენტში ასახულ ჯანმრთელობასთან დაკავშირებულ მონაცემებზე წვდომა შეეზღუდათ.

საქმის არსებითი მოკვლევის შედეგად დადგინდა, რომ პაციენტების პერსონალური მონაცემების შემცველი დოკუმენტი არ წარმოადგენდა სატენდერო დოკუმენტაციის ნაწილს და იგი სისტემაში შეცდომით ატვირთა პრეტენდენტი კომპანიის ერთ-ერთმა თანამშრომელმა. რაც შეეხება შეცდომის გამომწვევ მიზეზებს, კომპანიამ ელექტრონულ ტენდერებთან დაკავშირებული დოკუმენტების სისტემაში ატვირთვა დაავალა იმ პირს, რომელსაც სახელმწიფო შესყიდვების მიმართულებით გამოცდილება არ ჰქონდა და არც რაიმე სახის

კვალიფიკაციის ასამაღლებელი ტრენინგ-კურსი ჰქონდა გავლილი. იგი ასევე არ იყო ინფორმირებული სისტემაში განთავსებული მონაცემების საჯარო ბუნებაზე და მისი ფუნქციონირების ზოგად და საბაზისო პრინციპებზე.

სამსახურმა ყურადღება გაამახვილა იმ გარემოებაზე, რომ აუცილებელია ტენდერში მონაწილე ორგანიზაცია ისევე, როგორც ელექტრონულ ტენდერებზე პასუხისმგებელი პირი, სრულად აცნობიერებდეს შესყიდვების პროცესში მონაცემების დამუშავების სპეციფიკასა და შესაძლო რისკებს. აღნიშნული საკითხი მით უფრო აქტუალურია, როდესაც პრეტენდენტი სამედიცინო დაწესებულებაა, სადაც თავს იყრის დიდი რაოდენობის ფიზიკურ პირთა შესახებ ჯანმრთელობასთან დაკავშირებული სხვადასხვა შინაარსის მონაცემები. სწორედ დამუშავებისთვის პასუხისმგებელი პირია ვალდებული, მათ შორის საკადრო ცვლილებების შემთხვევაში, გაითვალისწინოს თანამშრომლების გამოცდილებიდან მომდინარე საფრთხეები და მიიღოს ადეკვატური ზომები მონაცემთა უსაფრთხოების უზრუნველსაყოფად. ამასთან, ელექტრონული ტენდერის ფარგლებში, სისტემაში მონაცემების ატვირთვისას მნიშვნელოვანია სათანადო სიფრთხილის გამოჩენა, ვინაიდან ინფორმაცია ან/და დოკუმენტაცია პირთა განუსაზღვრელი წრისთვის ხდება ხელმისაწვდომი, ხოლო ტენდერში მონაწილე პირს აღარ აქვს შესაძლებლობა შეცვალოს, დაამატოს ან წაშალოს ტექნიკური დოკუმენტაცია.

ამდენად სამსახურის შეფასებით, კომპანიის მიერ, მონაცემთა უსაფრთხოების დასაცავად არ იქნა მიღებული სათანადო ორგანიზაციულ-ტექნიკური ზომები, რაც გამოიხატა არაკომპეტენტური კადრისთვის მნიშვნელოვანი ფუნქციების სათანადო მომზადების გარეშე დაკისრებაში, რამაც თავის მხრივ, პაციენტების მონაცემების საჯაროდ გამოქვეყნება გამოიწვია. შესაბამისად, კომპანიის მიერ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის მოთხოვნების დარღვევის ფაქტზე შედგენილი იქნა ადმინისტრაციული სამართალდარღვევის ოქმი.

განხილვის ფარგლებში გამოვლინდა, რომ კომპანიამ პაციენტების პერსონალური მონაცემების შემცველი დოკუმენტის საჯაროდ გამოქვეყნება მართებულად მიიჩნია ინციდენტად და შექმნა ინციდენტის შესახებ ოქმი. თუმცა მის გამოვლენასთან ერთად პრეტენდენტს არ შეუფასებია ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა და სიმძიმე. ამასთან, კომპანიას არც სამსახურისთვის შეუტყობინებია ინციდენტის თაობაზე. ამის სანაცვლოდ, ის საკუთარი ძალებით ეცადა პრობლემის მოგვარებას, თუმცა უშედეგოდ. შემდგომ

კი სსიპ — სახელმწიფო შესყიდვების სააგენტოს აცნობა დოკუმენტის არასწორად ატვირთვის ფაქტი და მასზე წვდომის შეზღუდვა/წაშლა მოსთხოვა.

სამსახურის უფროსის ნორმატიული აქტით[2] დამტკიცებული კრიტერიუმების შესაბამისად, პერსონალურ მონაცემთა დაცვის სამსახურმა შეაფასა ინციდენტის სახე და სიმძიმე. მიჩნეულ იქნა, რომ ვინაიდან საჯაროდ ხელმისაწვდომ ვებგვერდზე მონაცემები იდენტიფიცირებადი ფორმით გამოქვეყნდა, დაირღვა მონაცემთა კონფიდენციალურობა. ამასთან, ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა შეფასებული იქნა როგორც საშუალო. შეფასებისას მხედველობაში იქნა მიღებული მონაცემთა სუბიექტების ოდენობა — ორასამდე ფიზიკური პირი. მონაცემების ხასიათი — გასაჯაროებული ანალიზების შინაარსი მიუთითებდა იმაზე, რომ საკვლევ პირებს ჰქონდათ სიმსივნე და იყვნენ მკურნალობის მეთოდის შერჩევის რეჟიმში. ამასთან დადგინდა, რომ დოკუმენტი ნანახი იყო დაახლოებით სამოცდაათჯერ. გათვალისწინებული იქნა ისიც, რომ ინციდენტი აღმოჩენილი იქნა სისტემაში დოკუმენტის გასაჯაროებიდან მოკლე ვადაში, ხოლო დოკუმენტის სახელწოდება იმგვარი იყო, რომ ნაკლებად მიანიშნებდა მასში პერსონალური მონაცემების არსებობაზე.

ამასთან, გამოვლინდა, რომ ვინაიდან სსიპ — სახელმწიფო შესყიდვების სააგენტომ ფაქტის შესახებ სამსახურს აცნობა, კომპანია ინციდენტის შესახებ სამსახურისთვის შეტყობინების ვალდებულებას შესრულებულად მიიჩნევდა, თუმცა აღნიშნული პოზიცია სამსახურმა არ გაიზიარა. მიღებულ გადაწყვეტილებაში ხაზი გაესვა, რომ სააგენტოს მიერ სამსახურში ინფორმაციის წარმოდგენა არ და ვერ ჩაანაცვლებდა დამუშავებისთვის პასუხისმგებელი პირის მიერ კანონითა და ნორმატიული წესით განსაზღვრული ფორმისა და შინაარსის მქონე ინფორმაციის საზედამხედველო ორგანოსთვის მოწოდების საჭიროებას. სააგენტოს სამსახურისთვის არ უცნობებია და ობიექტურადაც ვერ შეძლებდა, რომ განემარტა ინციდენტთან დაკავშირებული მნიშვნელოვანი საკითხები, მაგალითად, რა გარემოებებმა გამოიწვია ინციდენტი, როდის იქნა აღმოჩენილი, შეეხებოდა თუ არა არასრულწლოვანებს და სხვა. სამსახურისთვის ინციდენტის შეტყობინების პროცესი არ არის ფორმალური. მონაცემთა დაცვის საზედამხედველო ორგანოს, საკუთარი მანდატის ფარგლებში, აქვს ისეთი ეფექტიანი მექანიზმების (მაგალითად, დაბლოკვის) გამოყენების

[2]პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის №19 ბრძანება „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ“.

უფლებამოსილება, რომლითაც შესაძლოა არსებითად შემსუბუქდეს ინციდენტის შედეგები.

შესაბამისად, საკითხის შესწავლის შედეგად გამოიკვეთა მეორე სამართალდარღვევაც — კომპანიამ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 29-ე მუხლის შესაბამისად ვერ უზრუნველყო ადამიანის უფლებებისთვის საშუალო საფრთხის შემცველი ინციდენტის შესახებ სამსახურისთვის შეტყობინების ვალდებულების შესრულება, რის გამოც მას დაეკისრა ჯარიმა. ამასთან სააგენტოს, როგორც შესყიდვების ელექტრონული სისტემის ფუნქციონირებაზე პასუხისმგებელ დაწესებულებას, დაევალა დოკუმენტის სისტემიდან წაშლა.

1.2. მონაცემთა უსაფრთხოების დარღვევა კერძო სექტორში

კერძო სექტორში დაფიქსირებული მონაცემთა უსაფრთხოების დარღვასთან დაკავშირებით, სამსახურს მონაცემთა დამუშავებისთვის პასუხისმგებელმა რამდენიმე პირმა თავად მიმართა, ხოლო ერთ შემთხვევაში შეტყობინება სამსახურმა მესამე პირისგან მიიღო. დასახელებული შეტყობინებების საფუძველზე მიმდინარე შემოწმებების დროს, ყველა შემთხვევაში დადგინდა, რომ კომპანიების საქმიანობის შინაარსის გათვალისწინებით, მათ მიერ მიღებული ტექნიკური და ორგანიზაციული ზომები არ აღმოჩნდა საკმარისი ინციდენტების თავიდან ასარიდებლად. მაგალითად, ერთ შემთხვევაში დადგინდა, რომ კომპანია ამუშავებდა დიდი რაოდენობით მონაცემთა სუბიექტის (ასეულობით ათასი), მათ შორის, განსაკუთრებული კატეგორიის არაერთი სახის მონაცემს (სახელი, გვარი, პირადი ნომერი, ჯანმრთელობასთან დაკავშირებული ინფორმაცია, ფიზიკურ პირებთან დადებული ხელშეკრულებები და სხვა), რომელიც ინახებოდა ელექტრონულ სისტემებში და რომლებზეც კიბერ თავდასხმა განხორციელდა. დასახელებული თავდასხმის შედეგად, კომპანიას შეეზღუდა პერსონალურ მონაცემებზე წვდომა, შესაბამისად, სახეზე იყო ინციდენტის ერთ-ერთი სახე — ხელმისაწვდომობის დარღვევა. აღნიშნულ შემთხვევაში ელექტრონულ სისტემებზე თავდასხმის საფრთხეებს მნიშვნელოვნად ზრდიდა იმ მონაცემთა სიმრავლე და კატეგორიები, რასაც კომპანია ამუშავებდა და რაც კომპანიამ, მონაცემთა უსაფრთხოების ზომების განსაზღვრისას არ გაითვალისწინა. შესაბამისად, სამსახურმა დაადგინა დარღვევა და განმარტა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს უნდა მიეღოთ ზემოაღნიშნული გაზრდილი საფრთხის თავიდან ასაცილებლად შესაბამისი უსაფრთხოების ზომები, რაც მონაცემთა უკანონო დამუშავების სათანადო პრევენციას უზრუნველყოფდა.

გარდა ზემოაღნიშნულისა, სამსახურმა ასევე დაადგინა, რომ მართალია დამუშავებისთვის პასუხისმგებელმა პირებმა სამსახურს აცნობეს ინციდენტთან დაკავშირებით (გარდა ერთი შემთხვევისა), თუმცა მათ დასახელებული ცნობების ვალდებულება არასათანადოდ შეასრულეს. კერძოდ, არც ერთმა დამუშავებისთვის პასუხისმგებელმა პირმა უზრუნველყო სამსახურისთვის ინციდენტთან დაკავშირებული ინფორმაცია იმ ფორმით და მოცულობით გაზიარება, რასაც კანონი და საკითხის მომწესრიგებელი კანონქვემდებარე ნორმატიული აქტი განსაზღვრავს. კომპანიების განმარტებით, სამსახურის სათანადო ინფორმირება ინციდენტებთან დაკავშირებით არ განხორციელდა, ვინაიდან ნაკლებსავარაუდო იყო, რომ მონაცემთა უსაფრთხოების დარღვევა მნიშვნელოვან ზიანს გამოიწვევდა ან/და მნიშვნელოვან საფრთხეს შეუქმნიდა ადამიანის ძირითად უფლებებსა და თავისუფლებებს. სამსახურმა არ გაიზიარა კომპანიების დასახელებული არგუმენტები და განმარტა, რომ სახეზე იყო არაერთი გარემოება, რომელიც დამუშავებისთვის პასუხისმგებელმა პირებმა ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი საფრთხის შექმნის სიმძიმის განსაზღვრის მიზნებისთვის უნდა გაითვალისწინოს. მაგალითად, ერთ-ერთ შემთხვევაში დადგინდა, რომ ინციდენტის ცალკეულ 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 საქმიანობაც განსაკუთრებულ რეგულაციას ექვემდებარებოდა და ინციდენტის მასშტაბურობა, როგორც მონაცემთა სუბიექტების, ასევე მონაცემის რაოდენობის და მოცულობის თვალსაზრისით (ინციდენტი შეეხებოდა რამდენიმე ათასი ფიზიკური პირის არაერთი სახის მონაცემს).

2. პირველად პარამეტრად მონაცემთა დაცვის მნიშვნელობა სუბიექტების ინფორმირების უფლების ჯეროვანი განხორციელებისთვის

მონაცემთა სუბიექტის უფლებების ეფექტიანი უზრუნველყოფის მიზნით, დამუშავებისთვის პასუხისმგებელ პირებს ახალი კანონით დამატებითი ვალდებულებები განესაზღვრათ, მათ შორის, მონაცემთა დამუშავების

გამჭვირვალობის პრინციპის დაცვა ისევე, როგორც მონაცემთა დაცვის სტანდარტების გათვალისწინების აუცილებლობა ახალი პროდუქტის ან მომსახურების შექმნის პროცესში და მონაცემთა დაცვა პირველად პარამეტრად (“Data Protection by Design/by Default”). შესაბამისად, სავალდებულო გახდა პერსონალური მონაცემების დასაცავად, რიგი ღონისძიებების მონაცემთა დამუშავების დაწყებამდე გათვალისწინება, აუცილებელი ზომების პროაქტიულად მიღება, შემდგომში კი მათი ეფექტიანობის პერიოდული გადახედვა დამუშავების სრული ციკლის განმავლობაში. ამასთან, საჭირო გახდა ტექნიკური და ორგანიზაციული ზომების იმგვარად შერჩევა, რომ მონაცემთა დამუშავების პროცესებში ჯეროვნად დაინერგოს მონაცემთა დამუშავების პრინციპები (მათ შორის, გამჭვირვალობის პრინციპი), ასევე, სუბიექტის უფლებების დაცვის მექანიზმები. კანონით თითოეულ შემთხვევაში მნიშვნელობა მიენიჭა ტექნოლოგიების, განხორციელების ხარჯების თუ დამუშავების ხასიათს, მასშტაბს, კონტექსტსა და მიზნებს, აგრეთვე მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისთვის მოსალოდნელ რისკებს.

ელექტრონული ტექნოლოგიების დახმარებით მონაცემთა დამუშავების პროცესებთან მიმართებით ერთ-ერთი აქტუალური საკითხია, სუბიექტის უფლებების რეალიზების მიზნით მათი გამოყენების ეფექტიანობა. მონაცემთა სუბიექტები მათთვის მინიჭებული უფლებებიდან შედარებით უფრო ხშირად სარგებლობენ საკუთარი პერსონალური მონაცემების და მათი შემცველი მასალების გამოთხოვის უფლებებით. ამ თვალსაზრისით დიდია სამსახურის წინაშე მომართვიანობაც.

საანგარიშო პერიოდში სამსახურმა შეისწავლა ისეთი შემთხვევები, რომლებშიც დამუშავებისთვის პასუხისმგებელმა პირებმა საქმისწარმოების ელექტრონულ პროგრამაში არსებული ძიების პარამეტრებისა და გარკვეული მონაცემების მითითების მიუხედავად, ვერ უზრუნველყვეს განმცხადებლებთან დაკავშირებული დოკუმენტაციის სრულად მოძიება. შედეგად კი, უწყებებმა სუბიექტებს არასრულად უპასუხეს და მიუხედავად სურვილისა, მათი მოთხოვნების დაკმაყოფილება ჯეროვნად ვერ შეძლეს. კერძოდ, ერთ-ერთ შემთხვევაში, საჯარო დაწესებულებამ სრულყოფილად ვერ მოიძია მოთხოვნილი დოკუმენტები მხოლოდ იმიტომ, რომ კანცელარიის თანამშრომლები საქმისწარმოების ელექტრონულ პროგრამაში კორესპონდენციების „ანოტაციების“, „შინაარსის“ ველებს სხვადასხვაგვარად ავსებდნენ — ისინი ფიზიკური პირების საიდენტიფიკაციო ინფორმაციას ინიციალებით ან საერთოდ არ უთითებდნენ. ხოლო სხვა ველები მსგავსი ინფორმაციის ყველა ჯერზე დაფიქსირების საშუალებას არ იძლეოდა. შესაბამისად, ელექტრონული სისტემის საძიებო

პარამეტრებით ვერ ხერხდებოდა იმ მასალების სრულად მიკვლევა, რომლებიც მოთხოვნის ავტორის მონაცემებს შეიცავდა. რაც შეეხება მეორე შემთხვევას, საქმისწარმოების სისტემის მეშვეობით დოკუმენტების მოძებნა შესაძლებელი იყო მხოლოდ მასალის ფორმალური რეკვიზიტების (მაგალითად, დასკვნის ნომერი, თარიღი) მითითების პირობებში. ამდენად, მასალის მოსაძიებლად აუცილებელი იყო კონკრეტული დოკუმენტის არსებობის და მის შესახებ დეტალური ინფორმაციის ცოდნა, აღნიშნულის უწყებისთვის მიწოდება კი სუბიექტმა შეიძლება ვერ მოახერხოს. ისინი უმეტესად მხოლოდ ვარაუდობენ მათი მონაცემების შემცველი მასალების არსებობას და სწორედ ამის გამოსარკვევად, მათ გასაცნობად სარგებლობენ ინფორმირების უფლებებით. აქედან გამომდინარე, მოთხოვნილი მასალის კონკრეტული რეკვიზიტები ფიზიკურმა პირმა შესაძლოა ვერ დაასახელოს, რამაც ხელი არ უნდა შეუშალოს მის ჯეროვან ინფორმირებას, თუკი დაწესებულება მოთხოვნილ დოკუმენტებს ფლობს. მოცემულ შემთხვევაში, ვინაიდან საძიებო მასალის რეკვიზიტები უცნობი იყო, მონაცემთა სუბიექტის სახელის, გვარის და პირადი ნომრის ფლობის მიუხედავად, დაწესებულებამ ვერ მოძებნა ის, იმის გათვალისწინებითაც კი, რომ მასთან ინახებოდა. ამან კი სუბიექტის ნაკლოვანი ინფორმირება განაპირობა.

აღნიშნულ შემთხვევებში გამოვლინდა, რომ მონაცემთა დამუშავებისთვის გამოყენებული ელექტრონული სისტემების დიზაინი და საძიებო ფუნქციები არ იყო გამოსადეგი სუბიექტების უფლებების ჯეროვანი რეალიზებისთვის. შესაბამისად, სამსახურმა დაავალა დამუშავებისთვის პასუხისმგებელ/უფლებამოსილ პირებს ელექტრონული დოკუმენტბრუნვის პროგრამაში მონაცემთა სუბიექტის შესახებ ინფორმაციის/დოკუმენტაციის ძიების პარამეტრების/ველების ან/და რეკვიზიტების იმგვარად მოწესრიგება, რომ შესაძლებელი გამხდარიყო ფიზიკურ პირთან დაკავშირებული დოკუმენტის მოძიება, მისი საიდენტიფიკაციო მონაცემების საფუძველზე. აგრეთვე, საერთო სახელმძღვანელო წესის ანდა ინსტრუქციის შემუშავება და დანერგვა, რომლითაც განისაზღვრებოდა კორესპონდენციის რეგისტრაციისას საქმისწარმოების ელექტრონული სისტემის თითოეულ ველში მისათითებელი მონაცემის შინაარსი, ფორმა და დასახელება, მათ შორის რომელ ველში და რა ფორმით უნდა აესახათ ფიზიკური პირის მაიდენტიფიცირებელი მონაცემები.

3. მონაცემთა სუბიექტისათვის მონაცემების გამჭვირვალედ დამუშავება

3.1. გამჭვირვალობის პრინციპის უზრუნველყოფის შესწავლა საჯარო სექტორში

საკანონმდებლო სიახლეთაგან ერთ-ერთს მონაცემთა გამჭვირვალედ დამუშავების პრინციპი წარმოადგენს, რომლის თანახმად, ნებისმიერი ინფორმაცია, რომლის ადრესატი საზოგადოება ან მონაცემთა სუბიექტია, უნდა იყოს ადვილად ხელმისაწვდომი, მარტივი ენით გადმოცემული და გასაგები. აღნიშნული პრინციპი ემსახურება ფიზიკური პირებისათვის მათთან დაკავშირებული მონაცემთა დამუშავების პროცესების სიცხადის უზრუნველყოფას, მათ შორის: ვის მიერ, რა გზით, რა მიზნითა და რა მოცულობის მონაცემები მუშავდება. ამასთან, გამჭვირვალობის სათანადოდ უზრუნველყოფის პირობებში, ფიზიკური პირები თავად ეუფლებიან ინფორმაციას მონაცემების დამუშავებასთან დაკავშირებული რისკებისა და უფლებების განხორციელების საშუალებების შესახებ. ხსენებული პრინციპი, განსაკუთრებით აქტუალურია ისეთ შემთხვევებში, როდესაც სხვადასხვა გარემოების გამო გართულებულია იმის დადგენა, თუ ვინ და რომელ ინფორმაციას ამუშავებს.

საანგარიშო პერიოდში სამსახურმა შეისწავლა ისეთი შემთხვევა, სადაც ერთ-ერთი ადმინისტრაციული სამართალდარღვევის გამოვლენის პროცესში უზრუნველყოფილი არ იყო გამჭვირვალობის პრინციპი. შესწავლის ფარგლებში დადგინდა, რომ განმცხადებელმა ტაქსის სერვისის აპლიკაციის დახმარებით განახორციელა მგზავრების გადაყვანის მომსახურება. მოგვიანებით კი, მისთვის ცნობილი გახდა, რომ ქუჩაში განთავსებული ვიდეოკამერით მოპოვებული ფოტო-ვიდეო მასალის გამოყენებით ავტომობილის მესაკუთრის მიმართ შედგა საჯარიმო ქვითარი. ამასთან, გამოვლენილი ადმინისტრაციული დარღვევა გულისხმობდა საქართველოს დედაქალაქში მსუბუქი ავტომობილით — ტაქსით მგზავრთა გადაყვანას შესაბამისი ნებართვის გარეშე. ხოლო მითითებული ფოტო-ვიდეო მასალა ხელმისაწვდომი იყო საჯარიმო ქვითრის შემდგენელი დაწესებულების ვებგვერდზეც.

განხილვის შედეგად დადგინდა, რომ შემთხვევის ადგილზე განთავსებული იყო ერთ-ერთი უწყების მიერ ვიდეომონიტორინგის განხორციელების თაობაზე გამაფრთხილებელი ნიშნები, თუმცა არ იყო დამონტაჟებული იმ საჯარო დაწესებულების გამაფრთხილებელი ნიშანი, რომელმაც სამართალდარღვევის გამოსავლენად თავის მფლობელობაში არსებული ვიდეოკამერა გამოიყენა. გარდა ამისა, განმცხადებელმა მოგვიანებით შეიტყო, რომ ადმინისტრაციული წარმოების

მასალაში მოიპოვებოდა მგზავრების გადაყვანის გაწეული მომსახურების თაობაზე მტკიცებულებები (ტაქსის გამოძახების აპლიკაციის ველების ეკრანის ანაბეჭდები (ე.წ. „სქრინშოთები“)). მათში კი ჩანდა მძღოლის სახელი, გვარი, მგზავრების დაწყების და დასრულების ადგილი, მგზავრობის ღირებულება, სატრანსპორტო საშუალების მარკა, სახელმწიფო ნომერი, ფერი და სხვა.

საქართველოს მოქმედი კანონმდებლობის თანახმად, ზემოხსენებული სამართალდარღვევის გამოვლენის მიზნით, კონტროლის განმახორციელებელ ორგანოს შეუძლია, შეამოწმოს ნებისმიერ დროს, ნებისმიერი სახით და ფორმით, თუმცა დაკონკრეტებული არ არის შემოწმების სახე და ფორმა. თავის მხრივ, ნორმატიული აქტების მიხედვით, უწყების თანამშრომლები სამსახურებრივ უფლებამოსილებას, როგორც წესი, სპეციალური ფორმის ტანსაცმლით ახორციელებენ. შესწავლის შედეგად, მონაცემთა დამუშავებაზე პასუხისმგებელი ადმინისტრაციული ორგანოს განმარტებებით, დადგინდა, რომ მოცემული სამართალდარღვევის გამოვლენის მიზნით, პრაქტიკაში მხოლოდ ერთი მეთოდი გამოიყენება: საჯარო უწყების თანამშრომელი აპლიკაციის მეშვეობით იძახებს ტაქსს; იმ შემთხვევაში, თუ ავტომობილის მესაკუთრეს არ აქვს ტაქსით გადაყვანის ნებართვა, ჯდება გამოძახებულ ტრანსპორტში და გარკვეული მიმართულებით გადაადგილდება. ამ პროცესში უწყების თანამშრომელი არ ატარებს სპეციალური ფორმის ტანსაცმელს. ამასთან იგი, მგზავრობის დასრულების შემდეგ, მომსახურების ფაქტის დაფიქსირების მიზნით, მობილური მოწყობილობის საშუალებით იღებს ტაქსის სერვისის აპლიკაციის ე.წ. „სქრინშოთს“. ხოლო დაწესებულების სხვა თანამშრომელი, შუქნიშნის ბოძებზე განთავსებული ვიდეოკამერის საშუალებით ქმნის მომსახურების დაწყების/მომსახურების დასრულების პროცესის ამსახველ მტკიცებულებებს და შესაბამის ელექტრონულ საჯარიმო ქვითარს ადგენს.

სამსახურის გადაწყვეტილებით აღინიშნა, რომ საგზაო მოძრაობის რეგულირების, სამართალდარღვევების პრევენციისა და სხვა ლეგიტიმური მიზნებისთვის, ვიდეომონიტორინგს სხვადასხვა დაწესებულებები (მაგალითად, საქართველოს შინაგან საქმეთა სამინისტრო, თბილისის მუნიციპალიტეტის მერია) ახორციელებენ. გამჭვირვალობის პრინციპის უზრუნველყოფის მიზნით კი, თითოეულ დაწესებულებას ერთმანეთისგან დამოუკიდებლად აკისრია ვიდეომონიტორინგის განხორციელების თაობაზე შესაბამისი გამაფრთხილებელი ნიშნების განთავსების ვალდებულება, რათა საზოგადოებისათვის წინასწარ იყოს ცნობილი თუ რომელმა დაწესებულებამ შეიძლება გამოიყენოს ვიდეოჩანაწერი. აღსანიშნავია, რომ შესაბამისი ნორმატიული აქტით დადგენილია თბილისის მუნიციპალიტეტის მერიის ვიდეოკამერით მონიტორინგის მიმდინარეობის

თაობაზე გამაფრთხილებელი ნიშნის ფორმა, ხოლო თავად გამაფრთხილებელი ნიშანი ქალაქის მასშტაბით არაერთ ადგილზეა განთავსებული. შესაბამისად, საზოგადოებისათვის მოცემული ნიშანი ამოცნობადია. თავის მხრივ, ტაქსის მომსახურების საკონტროლო შესყიდვის მეთოდი სამართლებრივად არ არის რეგლამენტირებული და მონაცემთა დამუშავების ამ პროცესის შესახებ საზოგადოებისთვის არც სხვა ფორმით არის ცნობილი (მაგალითად, უწყების ვებგვერდზე გამოქვეყნებული ინსტრუქციებით, ადვილად ხელმისაწვდომი საინფორმაციო დოკუმენტებით). შესაბამისად, პოტენციური სამართალდამრღვევი არ არის ინფორმირებული, მონაცემთა დამუშავების რა პროცესსა და რა მოცულობის მონაცემების შეგროვებას გულისხმობს ზემოხსენებული სამართალდარღვევის გამოვლენა.

აღიშნული გარემოებების გათვალისწინებით, სამსახურის გადაწყვეტილებით დადგინდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლის მე-8 პუნქტის დარღვევა და მე-4 მუხლით განსაზღვრული გამჭვირვალობის პრინციპის ნაკლოვანი დაცვის შემთხვევა. შესაბამისად, სამსახურმა საჯარო უწყებას დაავალა ვიდეომონიტორინგის მიმდინარეობის შესახებ სათანადო გამაფრთხილებელი ნიშნების განთავსება. ამასთან, ამავე დაწესებულებას დაევალა მითითებული სამართალდარღვევის გამოვლენის მიზნით, მონაცემთა დამუშავების კონკრეტული პროცესების, მონაცემების მოცულობის, დამუშავების გზებისა და ფორმების განსაზღვრა. ასევე, აღნიშნულის თაობაზე გონივრული და ხელმისაწვდომი საშუალებებით საზოგადოებისათვის ინფორმაციის მიწოდება.

3.2. გამჭვირვალობის პრინციპის უზრუნველყოფის შესწავლა კერძო სექტორში

განსახილველ პერიოდში, სამსახურმა შეისწავლა კერძო ორგანიზაციების მიერ მონაცემების გამჭვირვალობის პრინციპის დაცვით დამუშავების საკითხი. ერთ-ერთ საქმეში, კომპანიის წარმომადგენელი მიუთითებდა, რომ კომპანია მონაცემთა სუბიექტს ვებგვერდისა და პორტალის საშუალებით აწვდიდა ინფორმაციას კომპანიისგან საკრედიტო „რეპორტის“ ან/და საკრედიტო ქულის შესახებ გამოთხოვის ფასიანი და უფასო მექანიზმების თაობაზე, მაგრამ განხილვის ფარგლებში დადგინდა, რომ ერთმანეთთან თანხვედრაში არ იყო კომპანიის წარმომადგენლის განმარტება ინფორმაციის გამოთხოვის მექანიზმების შესახებ და კომპანიის ვებგვერდზე/პორტალზე განთავსებული ინფორმაცია. აღნიშნულის საპირისპიროდ, როგორც კომპანიის ვებგვერდის, ასევე პორტალის საშუალებით,

კომპანია საჯაროდ არ უზრუნველყოფდა მონაცემთა სუბიექტების ინფორმირებას იმის თაობაზე, რომ არსებობდა კომპანიის მიერ პორტალის საშუალებით შეთავაზებული ფასიანი პაკეტით გათვალისწინებული სერვისის უფასოდ მიღების შესაძლებლობის ალტერნატიული გზები. სამსახურმა მიიჩნია, რომ მონაცემთა სუბიექტისათვის კანონით მინიჭებული უფლებების რეალიზებისათვის მნიშვნელოვანი იყო კომპანიის მიერ მონაცემთა სუბიექტების ინფორმირება, რათა შემდეგ სუბიექტს გააზრებული გადაწყვეტილება მიეღო მისი მონაცემების შესახებ ინფორმაციის გამოთხოვის თაობაზე. ამასთან, სამსახურმა განმარტა, რომ კომპანიის მიერ მონაცემთა სუბიექტისათვის ინფორმაციის საფასურის გადახდის გარეშე მიღების მექანიზმის არსებობა, აღნიშნულის თაობაზე ამავე სუბიექტის ინფორმირების გარეშე, ზღუდავდა გამჭვირვალობის პრინციპის პრაქტიკულ ქმედითობას და ხელს უშლიდა მონაცემთა დაცვის უფლების რეალიზებას. შესაბამისად, განხილვის ფარგლებში, სამსახურმა დაადგინა, რომ კომპანიის მიერ მონაცემთა დამუშავების პროცესში მონაცემთა სუბიექტებისათვის არ იყო უზრუნველყოფილი გამჭვირვალობის პრინციპის მოთხოვნები და კომპანიას დაევალა ამ პრინციპის მოთხოვნათა დაცვით უზრუნველეყო ვებგვერდისა და პორტალის საშუალებით საკრედიტო „რეპორტის“ ან/და საკრედიტო ქულის შესახებ გამოთხოვის ფასიანი და უფასო მექანიზმების თაობაზე სუბიექტის ინფორმირება.

ერთ-ერთი საქმის განხილვის ფარგლებში 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 ან 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. ამასთან, მხოლოდ კომპანიის წარმომადგენლის განმარტება, განმცხადებლის ზეპირი ინფორმირების თაობაზე, ვერ იქნებოდა მიჩნეული კანონის მე-4 მუხლის მე-7 პუნქტის მიზნებისათვის გათვალისწინებულ ობიექტურ მტკიცებულებად, რომელიც 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. აღნიშნულიდან

გამომდინარე, სამსახურმა მიიჩნია, რომ კომპანიის მიერ მონაცემთა დამუშავების პროცესში მონაცემთა სუბიექტისათვის არ იყო უზრუნველყოფილი გამჭვირვალობის პრინციპის მოთხოვნები და დაევალა წესების შემუშავება, რომლითაც კომპანიის თანამშრომლები ინფორმირებული იქნებიან სამსახურებრივი ელექტრონული ფოსტის კომპანიის მხრიდან შესაძლო კონტროლსა და წვდომაზე, ხოლო თანამშრომლის სამსახურიდან გათავისუფლების შემთხვევაში, სამსახურებრივი ელექტრონული ფოსტის გამოყენების, მასზე არსებული ინფორმაციის შენახვისა და შენახვის ხანგრძლივობის შესახებ.

ერთ-ერთ საქმეში, რომელიც ეხებოდა სამედიცინო დაწესებულების მიერ გარდაცვლილი პირის მონაცემების გაცემის გზით დამუშავებას, 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. სამსახურმა აღნიშნული საქმის ფაქტორბივი გარეოებების შესწავლის შედეგად დაადგინა, რომ მონაცემთა დამუშავების პროცესში კანონის მე-4 მუხლით განსაზღვრული პრინციპები და კონკრეტულად, გამჭვირვალობის პრინციპი, არა მხოლოდ ნორმატიულად მბოჭავ ელემენტს წარმოადგენს, რომლითაც იზღუდება დამუშავებისათვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირის მოქმედების ფარგლები, არამედ კანონის ნორმების განმარტების ფუნქციითაც არის აღჭურვილი. შესაბამისად, სამსახურმა მიიჩნია, რომ მართალია, კანონის მე-8 მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტში უშუალოდ არ არის მითითებული მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მხრიდან განსახორციელებელი ზემოაღნიშნული ინფორმირების ვალდებულება, მაგრამ ხსენებული ნორმის გამჭვირვალობის პრინციპის საშუალებით, განმარტების საფუძველზე, მარტივად დგინდება კანონმდებლის ნება — წინააღმდეგ შემთხვევაში, საფუძველი გამოეცლება ნორმის შინაარსს პირის გარდაცვალების შემდეგ მისი მონაცემების დაცვის თაობაზე.

ამასთანავე, ხაზგასასმელია, რომ ახალი კანონის მოქმედების ფარგლებში დამკვიდრებული პრაქტიკის თანახმად, სამსახური მონაცემთა დამუშავების გამჭვირვალობის პრინციპს იყენებს ნორმატიული შინაარსით, როგორც უშუალოდ დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირის ვალდებულების დამდგენ ნორმას, ასევე, სუბსიდიური შინაარსით კანონის სხვა ნორმების განმარტების ფუნქციით.

4. პერსონალური მონაცემების პირდაპირი მარკეტინგის მიზნით დამუშავება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალმა კანონმა, მონაცემთა სუბიექტის უფლებების ეფექტიანი რეალიზებისთვის, ახლებურად ჩამოაყალიბა პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების მომწესრიგებელი სპეციალური მუხლი. კერძოდ, კანონის თანახმად, მიუხედავად მონაცემთა შეგროვების ანდა მოპოვების საფუძვლისა და მათი ხელმისაწვდომობისა, პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავება შეიძლება მხოლოდ მონაცემთა სუბიექტის თანხმობით. მონაცემთა სუბიექტის სახელის, გვარის, მისამართის, ტელეფონის ნომრისა და ელექტრონული ფოსტის მისამართის გარდა, პირდაპირი მარკეტინგის მიზნით სხვა მონაცემთა დამუშავებისთვის აუცილებელია მონაცემთა სუბიექტის წერილობითი თანხმობა. მნიშვნელოვანია ისიც, 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 საშუალება მონაცემთა დამუშავების შეწყვეტის მოთხოვნისთვის, რომელიც მარტივი უნდა იყოს. ამასთანავე, 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“ პუნქტები განმარტავს მონაცემთა სუბიექტის თანხმობისა და წერილობითი თანხმობის ცნებებს, 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.

იქიდან გამომდინარე, რომ ახალი 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 გარკვეული მონაცემები (სახელი, მისამართი, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, ფაქსის ნომერი), აღნიშნული მიმართულებით სამსახურის წინაშე 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, მათ შორის, შეეხებოდა ერთი და იმავე კომპანიებისგან მიღებულ შეტყობინებებს. გარდა კონკრეტულ განცხადებებზე რეაგირებისა, სამსახურმა დააიდენტიფიცირა პირდაპირი მარკეტინგის განმახორციელებელი, ელექტრონული კომუნიკაციების სფეროში ავტორიზებული პირები, წარმოდგენილი განცხადებების/შეტყობინებების რაოდენობისა და შინაარსის, მოცემული კომპანიების საქმიანობის სპეციფიკისა და მათ მიერ პერსონალურ მონაცემთა დამუშავების შესაძლო მასშტაბის გათვალისწინებით, პირდაპირი მარკეტინგის მიზნით მონაცემების შესაძლო კანონდარღვევით დამუშავების ფაქტების გამოსავლენად, დაიწყო 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 მიზნებისთვისაც სატელეფონო ნომრებზე იგზავნებოდა მარკეტინგული შეთავაზებები. ამდენად, სამსახურმა ასევე შეაფასა კომპანიების მიერ მონაცემთა პირდაპირი მარკეტინგის მიზნით დამუშავების კანონშესაბამისობის საკითხიც.

სამსახურმა შეისწავლა ისეთი შემთხვევები, რომლებშიც დამუშავებისთვის პასუხისმგებელმა პირებმა მონაცემთა სუბიექტის თანხმობის (მათ შორის, წერილობითი თანხმობის) გარეშე დაამუშავეს მათი პერსონალური 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, 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 სამომავლო აღკვეთას.

შემოწმებების მიმდინარეობისას, ასევე, გამოიკვეთა შემთხვევებიც, 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.

5. აუდიომონიტორინგის განხორციელება

აუდიომონიტორინგის გზით მონაცემთა დამუშავება შესაძლოა მონაცემთა სუბიექტისთვის საკმაოდ სენსიტიურ ხასიათს ატარებდეს — იწვევდეს მონაცემთა სუბიექტისთვის მისი პირადი ცხოვრების ხელშეუხებლობით დაცულ სფეროში ინტენსიურ და უკანონო ჩარევას. შესაბამისად, მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა/დამუშავებაზე უფლებამოსილმა პირმა მკაცრად დაიცვას აუდიომონიტორინგის განხორციელების წესები. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განისაზღვრა აუდიომონიტორინგის დეფინიცია. კერძოდ, აუდიომონიტორინგი არის საჯარო ან

კერძო სივრცეში განთავსებული/დამონტაჟებული ტექნიკური საშუალებების გამოყენებით ხმოვანი სიგნალის მონაცემთა დამუშავება, კერძოდ, აუდიოკონტროლი ან/და აუდიოჩაწერა (გარდა ფარული საგამოძიებო მოქმედებისა). აუდიომონიტორინგის ახალი კანონით გათვალისწინებული ფორმულირება საკმაოდ ფართოა და მოიცავს ნებისმიერ ტექნიკურ საშუალებას, რომლითაც აუდიომონიტორინგი ხორციელდება.

საანგარიშო პერიოდში სამსახურმა შეისწავლა აუდიომონიტორინგის რამდენიმე ფაქტი. კანონის მე-11 მუხლი ამომწურავად განსაზღვრავს მონაცემთა აუდიომონიტორინგის გზით დამუშავების კონკრეტულ საფუძვლებს. ერთ-ერთი შემოწმების ფარგლებში, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა აუდიომონიტორინგის გზით მონაცემთა დამუშავების საფუძვლად მიუთითა მონაცემთა სუბიექტის წერილობითი თანხმობა. დამუშავებისთვის პასუხისმგებელი პირის განმარტებით, მონაცემთა სუბიექტმა შრომით ხელშეკრულებაზე ხელმოწერით თანხმობა განაცხადა კომპანიის მიერ აუდიომონიტორინგის გზით მისი მონაცემების დამუშავებაზე. აუდიომონიტორინგის შესახებ ინფორმაცია მოცემული იყო შინაგანაწესში, რომელიც, თავის მხრივ, წარმოადგენდა შრომითი ხელშეკრულების განუყოფელ ნაწილს, თუმცა სამსახურმა მიიჩნია, რომ შინაგანაწესის ჩანაწერი არ მიემართებოდა უშუალოდ აუდიომონიტორინგის განხორციელების საკითხს. შესაბამისად, დასაქმებულისთვის მხოლოდ დასახელებული დოკუმენტით არ იყო აღქმადი, კომპანიის მიერ მიმდინარეობდა თუ არა სამუშაო სივრცის აუდიომონიტორინგი. ამასთან, გასათვალისწინებელია, რომ 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. ყოველივე ზემოაღნიშნულიდან გამომდინარე, ხსენებულ შემთხვევაში, სამსახურმა განმარტა, რომ სახეზე არ იყო მონაცემთა სუბიექტის თანხმობა მისი მონაცემების აუდიომონიტორინგის საშუალებით დამუშავების თაობაზე და დაადგინა დარღვევა. ამასთან, დამუშავებისთვის პასუხისმგებელ პირს მიეცა შესაბამისი დავალებები აუდიომონიტორინგის შეწყვეტისა და ხსენებული გზით დამუშავებული მონაცემების წაშლის თაობაზე.

კანონის მე-11 მუხლი აუდიომონიტორინგის გზით მონაცემთა დამუშავების ერთ-ერთ საფუძვლად მიუთითებს დამუშავებისთვის პასუხისმგებელი პირის მნიშვნელოვანი ლეგიტიმური ინტერესის დაცვას, თუ განსაზღვრულია სათანადო და კონკრეტული ღონისძიებები მონაცემთა სუბიექტის უფლებებისა და

ინტერესების დასაცავად. ამ თვალსაზრისით აღსანიშნავია, რომ სამსახურმა შეისწავლა შემთხვევა, რომლის ფარგლებშიც ერთ-ერთი კომპანიის, როგორც დამუშავებისთვის პასუხისმგებელი პირის, ლეგიტიმურ ინტერესს წარმოადგენდა მისი თანამშრომლების მიერ სამუშაოს შესრულების პროცესში აუდიომონიტორინგის გზით მონაცემთა დამუშავება. გასათვალისწინებელია, რომ ლეგიტიმური ინტერესის არსებობა დგინდება კანონით გათვალისწინებული კონკრეტული დათქმის არსებობის პირობებში, კერძოდ, აუდიომონიტორინგის განხორციელება დასაშვებია დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური ინტერესის დასაცავად, თუ განსაზღვრულია სათანადო და კონკრეტული ღონისძიებები მონაცემთა სუბიექტის უფლებებისა და ინტერესების დასაცავად. ხსენებულ შემთხვევაში, სამსახურმა განმარტა, რომ მართალია, კომპანიის თანამშრომლები წერილობით ინფორმირებულები იყვნენ მათ მიერ სამუშაოს შესრულების მიმდინარეობისას აუდიომონიტორინგის განხორციელების თაობაზე, თუმცა დამუშავებისთვის პასუხისმგებელი პირის მიერ სუბიექტის უფლებებისა და ინტერესების დასაცავი კონკრეტული ღონისძიებების სრულყოფილად განსაზღვრის მიზნით, შემუშავებული უნდა ყოფილიყო კანონით განსაზღვრული წერილობითი დოკუმენტი. კერძოდ, ახალი კანონით დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, შეიმუშაოს დოკუმენტი, რომელიც განსაზღვრავს აუდიომონიტორინგთან დაკავშირებულ მთელ რიგ პროცესებს და შესაძლებელი იქნება ხსენებული პროცესის პროაქტიულად დაგეგმვა და ორგანიზება. სამსახურის მიერ გამოვლენილი სამართალდარღვევის შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირებს მიეცათ შესაბამისი დავალებები აუდიომონიტორინგის განხორციელების მიზნით წერილობითი დოკუმენტის შემუშავების თაობაზე.

სამსახურმა გეგმურად შეისწავლა ორი კომერციული ბანკის მიერ ცხელი ხაზის მეშვეობით აუდიომონიტორინგის განხორციელების კანონიერება. შემოწმების ფარგლებში დადგინდა, რომ ბანკები საქმიანობის პროცესში, მომხმარებლებთან კომუნიკაციის მიზნით იყენებენ სატელეფონო ცხელ ხაზს, რომელზე შემავალი სატელეფონო ზარები უმეტეს შემთხვევებში იწერება და ინახება. თითოეულ შემთხვევაში, ცხელ ხაზზე ზარის განხორციელებით ბანკის მომხმარებლებსა და პოტენციურ მომხმარებლებს შეუძლიათ მიიღონ ინფორმაცია ბანკის საქმიანობასთან დაკავშირებულ საკითხებზე (მაგალითად: ფილიალების მისამართები, სამუშაო საათები და სხვა). ამასთან, ცხელ ხაზზე დარეკვის გზით მომხმარებლებს ასევე შესაძლებლობა აქვთ მიიღონ სხვადასხვა სახის მომსახურება (მაგალითად: საკუთარ ანგარიშებს შორის ნაშთის გადატანა/თანხის კონვერტაცია; ინტერნეტ ბანკინგის ხელშეკრულების დაბლოკვა; ინტერნეტ ბანკის მომხმარებლის სახელის მიწოდება (შეხსენება); ერთჯერადი პაროლის განახლება

და სხვა). გარდა ამისა, სატელეფონო ცხელი ხაზის გზით მომხმარებლები წარადგენენ ბანკის საქმიანობასთან და მომსახურებასთან დაკავშირებით პრეტენზიებს (მაგალითად, მათი მხრიდან პროტესტის საგანი შესაძლოა გახდეს ბანკისგან არასწორი ინფორმაციის მიღება და სხვა).

შემოწმების შედეგად გამოიკვეთა, რომ ბანკებს, როგორც მეწარმე სუბიექტებს, საკუთარი ლეგიტიმური ინტერესების დასაცავად, ცხელი ხაზის მეშვეობით განხორციელებული კომუნიკაციის აუდიომონიტორინგის და აღნიშნულის შედეგად მოპოვებული ჩანაწერების შენახვის საჭიროება გააჩნიათ როგორც მომხმარებლის მხრიდან დავის წარმოშობის შემთხვევაში, საკუთარი პოზიციის დადასტურებისთვის, ისე მომხმარებლისთვის სწრაფი, მოქნილი და ხარისხიანი მომსახურების გაწევის უზრუნველსაყოფად. ამდენად, შემოწმების შედეგად, აღნიშნული საფუძვლის არსებობის პირობებში აუდიომონიტორინგის განხორციელება კანონის მე-11 მუხლის პირველ პუნქტთან შესაბამისად იქნა მიჩნეული.

აღსანიშნავია, რომ ახალი კანონის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, წინასწარ ან აუდიომონიტორინგის დაწყებისთანავე გააფრთხილოს მონაცემთა სუბიექტი აუდიომონიტორინგის განხორციელების შესახებ და განუმარტოს უარის თქმის თაობაზე მისი უფლება (ასეთის არსებობის შემთხვევაში). შემოწმებების შედეგად სამსახურმა დაადგინა, რომ აუდიომონიტორინგის განხორციელებისა და აღნიშნულის თაობაზე ინფორმაცია, უმეტეს შემთხვევაში, მომხმარებელს მიეწოდება ავტომოპასუხის მეშვეობით. გამოვლინდა ისეთი შემთხვევაც, როცა ერთ-ერთი ბანკის თანამშრომელი ცხელი ხაზით კომუნიკაციის ფარგლებში თავად ახდენდა მომხმარებლის გაფრთხილებას ზარის ჩაწერის თაობაზე და არ განუმარტავდა აუდიოჩაწერის მიზანს. ხსენებულ გარემოებასთან დაკავშირებით სამსახურმა აღნიშნა, რომ სუბიექტის უფლებების რეალიზებისა და მონაცემთა დამუშავების პროცესის გამჭვირვალობის უზრუნველსაყოფად, მნიშვნელოვანია მომხმარებლის ინფორმირება მოხდეს არა მხოლოდ აუდიომონიტორინგის მიმდინარეობის, არამედ აღნიშნულის მიზნის თაობაზეც. ამდენად, სამსახურის გადაწყვეტილებით, ბანკს დაევალა შესაბამისი ღონისძიებების მიღება.

ამასთან, სამსახურის მიერ განხორციელებული ორივე შემოწმების ფარგლებში გამოვლინდა ბანკების მიერ უსაფრთხოების წესების დარღვევა. კერძოდ, ერთ შემთხვევაში აუდიოჩანაწერებზე წვდომის მქონე პირები ერთ-ერთ სისტემაში არ სარგებლობდნენ განპიროვნებული მომხმარებლით და პაროლით, ხოლო მეორე შემთხვევაში სერვერებზე პირდაპირი წვდომის გზით აუდიოჩანაწერთა მიმართ

განხორციელებული მოქმედებები არ აღირიცხებოდა. აღსანიშნავია, რომ ელექტრონული ფორმით დაცული მონაცემების, მათ შორის, აუდიოჩანაწერების, უსაფრთხოების უზრუნველსაყოფად განსაკუთრებით მნიშვნელოვანია, რომ ელექტრონული ფორმით არსებული მონაცემების დამუშავების საშუალებას გააჩნდეს მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედების აღრიცხვის (მათ შორის, მონაცემების დათვალიერების, მოსმენის, გადმოწერის, წაშლის) შესაძლებლობა, რათა არ მოხდეს მონაცემების უკანონო მოპოვება, გამჟღავნება, გამოყენება, განადგურება და ა.შ. თუმცა ხსენებული ღონისძიებების მიღება უშედეგო იქნებოდა მონაცემთა მიმართ მოქმედებების განმახორციელებელი თითოეული პირის იდენტიფიცირების გარეშე. ელექტრონული ფორმით დაცულ მონაცემებზე განხორციელებული მოქმედებების აღრიცხვა და აღნიშნული მოქმედებების კანონიერების პერიოდული მონიტორინგი კი მნიშვნელოვნად ამცირებს მონაცემებზე უკანონო წვდომის შესაძლებლობას და ახდენს მონაცემთა უკანონო დამუშავების პრევენციას. შესაბამისად, სამსახურის მიერ ორივე შემთხვევაში დადგინდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის დარღვევა და ბანკებს დაეკისრათ პასუხისმგებლობა კანონის 76-ე მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის. ამასთან, სამსახურის მიერ გაიცა შესასრულებლად სავალდებულო დავალებები მონაცემებზე წვდომის უფლების მქონე პირებისთვის განპიროვნებული მომხმარებლების შექმნისა და მონაცემების მიმართ განხორციელებული ყველა ქმედების აღრიცხვის მიზნით.

აუდიომონიტორინგის განხორციელებასთან დაკავშირებული დარღვევა, ასევე, გამოვლინდა სამსახურის მიერ მომხმარებლებისთვის სამედიცინო დიაგნოსტიკური მომსახურების მიმწოდებელი ერთ-ერთი დაწესებულების (შემდგომში — ლაბორატორია) შენობაში ვიდეომონიტორინგის განხორციელების კანონიერების გეგმური შემოწმების ფარგლებში. აღნიშნული შემოწმების შედეგად დადგინდა, რომ ლაბორატორია შენობაში განთავსებული ვიდეოკამერების მეშვეობით, რეგისტრატურის სივრცეში და მორფოლოგიის ოთახში ვიდეომონიტორინგთან ერთად ახორციელებდა აუდიომონიტორინგსაც. შემოწმების ფარგლებში ლაბორატორიის მიერ წარმოდგენილი ინფორმაციით, რეგისტრატურაში ხორციელდებოდა პაციენტების მიერ მოთხოვნილი კვლევის გაფორმება და შესაბამისი საფასურის გადახდა, რეგისტრატორების მიერ პაციენტებისთვის კვლევის წინ მოსამზადებელი წესების ამსახველი წერილობითი დოკუმენტის გადაცემა და ამავე წესების ზეპირსიტყვიერად განმარტება, საკვლევი მასალების მოსათავსებლად განკუთვნილი სინჯარების მარკირება, პაციენტისთვის გადაცემა და საკვლევი მასალების ჩაბარება. მორფოლოგიის განყოფილების კაბინეტში კი — ონკოლოგიური პაციენტების მიღება, მათთვის

კონსულტაციის გაწევა, მათთან კვლევის შესახებ ხელშეკრულების გაფორმება, საკვლევი მასალების ჩაბარება/შენახვა, პაციენტებისთვის საკვლევი მასალის აღების წესების წერილობით გადაცემა და იმავე წესების ზეპირსიტყვიერად განმარტება.

აღნიშნულ სივრცეებში აუდიომონიტორინგის მიზნად ლაბორატორიამ კანონის მე-11 მუხლის პირველი პუნქტის „გ“ ქვეპუნქტი (დამუშავებისთვის პასუხისმგებელი პირის მნიშვნელოვანი ლეგიტიმური ინტერესის დასაცავად მონაცემების დამუშავება) დაასახელა და ასევე განმარტა, რომ აუდიომონიტორინგი ხორციელდებოდა სამედიცინო მომსახურების მაღალი ხარისხის უზრუნველსაყოფად. ლაბორატორიის პოზიციის თანახმად, მიუხედავად იმისა, რომ მომხმარებლის მიერ სამართლებრივი დავის წამოწყების შემთხვევაში, არსებობს საკმარისი წერილობითი მტკიცებულებები მომხმარებლისთვის სწორი ინფორმაციის მიწოდების ფაქტის დასადასტურებლად, ლაბორატორიის მიზანი არ არის პაციენტს საკუთარი მომსახურების მართებულობა დაუდასტუროს სამართლებრივი დავის ფარგლებში. პრეტენზიის წარმოდგენის შემთხვევაში, საკითხის მოგვარების გაცილებით მარტივ და ეფექტიან გზად ლაბორატორიას მიაჩნია მომხმარებლისთვის მომსახურების გაწევის ამსახველი ვიდეო-აუდიო ჩანაწერის გაცნობა და ამ საშუალებით დარწმუნება, რომ პრეტენზია უსაფუძვლოა. ამასთან, ლაბორატორიის განმარტებით, რეგისტრატურის აუდიო-ვიდეო მონიტორინგის მიზანს ასევე წარმოადგენდა დასაქმებულების მიერ დაკისრებული ფუნქციების, კერძოდ, პაციენტებისთვის რეგისტრაციის პროცესში გაწეული მომსახურების ხარისხის შეფასება, რასაც შესაძლოა მოჰყვეს შემდგომი რეაგირება (მაგალითად, განისაზღვროს აღნიშნული დასაქმებულისთვის კვალიფიკაციის ასამაღლებელი კურსების გავლის საჭიროება). შემოწმების ფარგლებში ასევე დადგინდა, რომ პაციენტი ხელმოწერით ადასტურებდა მის მიერ მოთხოვნილი კვლევის შეკვეთის ფაქტს, ასევე მას წერილობით გადაეცემოდა პრეანალიტიკის წესები. მორფოლოგიური კვლევის საწყის ეტაპზე კი პაციენტთან იდებოდა წერილობითი ხელშეკრულება, ხოლო დამატებითი კვლევის წარმოშობის შემთხვევაში ასევე ხდებოდა პაციენტის წერილობითი ინფორმირება. ამდენად, სადავო საკითხის წარმოშობის შემთხვევაში, ლაბორატორიას გააჩნდა წერილობითი მტკიცებულებები საკუთარი ინტერესების დასაცავად და სწორედ ხსენებული გზით უზრუნველყოფდა პაციენტის მხრიდან პრეტენზიის დაფიქსირების შემთხვევების განსახილველად საჭირო მტკიცებულებების არსებობას.

აღნიშნული გარემოებების ერთობლიობით დადასტურდა, რომ ლაბორატორიის მიერ აუდიომონიტორინგის განხორციელების მიზანს, პრეტენზიის

დაფიქსირების შემთხვევებში საკუთარი ლეგიტიმური ინტერესების დასაცავად შესაბამისი მტკიცებულებების შექმნა არ წარმოადგენდა. არამედ, აღნიშნულის მიზანი იყო მომსახურების ხარისხის კონტროლი, მისი გაუმჯობესება და მომხმარებლის კმაყოფილების უზრუნველყოფა.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-11 მუხლის პირველი პუნქტის „გ“ ქვეპუნქტის თანახმად, აუდიომონიტორინგის განხორციელება დასაშვებია დამუშავებისთვის პასუხისმგებელი პირის მნიშვნელოვანი ლეგიტიმური ინტერესის დასაცავად, მხოლოდ იმ შემთხვევაში თუ განსაზღვრულია სათანადო და კონკრეტული ღონისძიებები მონაცემთა სუბიექტის უფლებებისა და ინტერესების დასაცავად. გადაწყვეტილებაში სამსახურმა იმსჯელა ლეგიტიმური მიზნის მიღწევისთვის გამოყენებული საშუალების პროპორციულობაზე და აღნიშნა, რომ მართალია, მომსახურების ხარისხის კონტროლი, მისი გაუმჯობესება და მომხმარებლის კმაყოფილების უზრუნველყოფა წარმოადგენს ლაბორატორიის ლეგიტიმურ ინტერესს, თუმცა ხსენებული ლეგიტიმური ინტერესის შესრულების საშუალება არ არის პროპორციული დამუშავებულ მონაცემებთან მიმართებაში და იწვევს არათანაზომიერ ჩარევას, მათ შორის, დასაქმებული პირების პირად ცხოვრებაში. სამსახურმა ასევე მიუთითა, რომ მნიშვნელოვანია, განისაზღვროს სათანადო და კონკრეტული ღონისძიებები მონაცემთა სუბიექტის უფლებებისა და ინტერესების დასაცავად, რაც სწორედ თანაზომიერების, აუცილებლობისა და პროპორციულობის დაცვის გზით მიიღწევა.

სამსახურის გადაწყვეტილებით შეფასდა ის გარემოებაც, რომ დასახელებულ სივრცეებში მომხმარებლებთან კომუნიკაცია არ ხორციელდებოდა მუდმივ რეჟიმში, თუმცა ლაბორატორია მომხმარებლის არყოფნის შემთხვევაშიც კი ახდენდა თანამშრომლების აუდიომონიტორინგს. შესაბამისად, ლაბორატორიას შესაძლოა, დაემუშავებინა ისეთი მონაცემები, რაც კავშირში არ იყო თანამშრომლის მიერ მომსახურების განხორციელების ხარისხთან (მაგალითად, მისი პირადი სატელეფონო საუბრები ან/და კომუნიკაცია სხვა თანამშრომლებთან). სამსახურის შეფასებით, აღნიშნული განსაკუთრებით მაღალი ხარისხით იწვევდა მათ პირად ცხოვრებაში ჩარევას და არღვევდა სამართლიან ბალანსს მონაცემთა დამუშავების კანონიერ მიზანს, დამუშავებისთვის პასუხისმგებელი პირის ინტერესებსა და სუბიექტის უფლებებს შორის.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, სამსახურმა დაადგინა, რომ რეგისტრატურის და მორფოლოგიის კაბინეტის ვიდეო-აუდიო მონიტორინგი

მომსახურების ხარისხის კონტროლის, მისი გაუმჯობესებისა და მომხმარებლის კმაყოფილების უზრუნველყოფის მიზნით არ წარმოადგენდა ლაბორატორიის მიერ დასახელებული ინტერესების დაცვის აუცილებელ საშუალებას. იგი შეფასდა როგორც არაპროპორციულ ჩარევა მონაცემთა სუბიექტების პირად ცხოვრებაში და ეწინააღმდეგებოდა კანონის მე-11 მუხლის პირველი პუნქტის მოთხოვნებს. შესაბამისად, სამსახურის გადაწყვეტილებით, ლაბორატორიას დაეკისრა პასუხისმგებლობა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 69-ე მუხლის პირველი პუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევისთვის და დაევალა აუდიომონიტორინგის განხორციელების დაუყოვნებლივ შეწყვეტა.

სამსახურმა, აგრეთვე, შეისწავლა აუდიომონიტორინგის განხორციელების თაობაზე მონაცემთა სუბიექტების წინასწარი ინფორმირების ვალდებულების საკითხთან დაკავშირებული შემთხვევები, რომლის ფარგლებშიც გამოვლინდა არაერთი დარღვევა. კერძოდ, ერთ-ერთ შემთხვევაში მესამე პირმა თანადამუშავებისთვის პასუხისმგებელი პირების თანდასწრებით განახორციელა სატელეფონო ზარი მონაცემთა სუბიექტთან და შენობაში განთავსებული აუდიომონიტორინგის სისტემის მეშვეობით განხორციელდა ხსენებული სატელეფონო კომუნიკაციის აუდიოჩაწერა მონაცემთა სუბიექტის წინასწარი ინფორმირების გარეშე. თანადამუშავებისთვის პასუხისმგებელმა პირებმა განმარტეს, რომ სატელეფონო ზარის წამოწყება განხორციელდა სპონტანურად და მათ ინტერესს არ წარმოადგენდა კომუნიკაციის აუდიოჩაწერა. აქედან გამომდინარე, მათ არ ჰქონდათ ვალდებულება, განემარტათ მონაცემთა სუბიექტისთვის სატელეფონო საუბრის აუდიომონიტორინგის თაობაზე. არსებული მტკიცებულებების ანალიზის შედეგად, სამსახურმა დაადგინა დარღვევა მონაცემთა სუბიექტის წინასწარი ინფორმირების გარეშე აუდიომონიტორინგის გზით მისი მონაცემების დამუშავებასთან დაკავშირებით.

6. ვიდეომონიტორინგის გზით პერსონალური მონაცემების დამუშავების კანონიერება

თანამედროვე ეპოქაში, მზარდი ტექნოლოგიური განვითარების პირობებში, ვიდეომონიტორინგი მონაცემთა დამუშავების ერთ-ერთი ყველაზე აქტუალური სახეა, რომელიც აქტიურად გამოიყენება როგორც საჯარო და კერძო დაწესებულებების, ისე ფიზიკური პირების მიერ. ახალი კანონის მე-10 მუხლით განსხვავებულად მოწესრიგდა ვიდეომონიტორინგის განხორციელებასთან დაკავშირებული წესები. ტერმინთა განმარტებით ასევე განისაზღვრა

„ვიდეომონიტორინგის“ ცნება, რომლის თანახმად: ვიდეომონიტორინგი არის „საჯარო ან კერძო სივრცეში განთავსებული/დამონტაჟებული ტექნიკური საშუალებების გამოყენებით ვიზუალური გამოსახულების მონაცემთა დამუშავება, კერძოდ, ვიდეოკონტროლი ან/და ვიდეოჩაწერა (გარდა ფარული საგამოძიებო მოქმედებისა).

საანგარიშო პერიოდში სამსახურმა შეისწავლა სამედიცინო დაწესებულებების, საჯარო და კერძო სკოლების, აგრეთვე, პროფესიული სასწავლებლების მიერ ვიდეომონიტორინგის განხორციელების რამდენიმე ფაქტი. სამსახურმა გეგმურად შეისწავლა სამედიცინო დაწესებულებების (ორი სამედიცინო ლაბორატორია და ერთი სტომატოლოგიური კლინიკა) მიერ ვიდეომონიტორინგის განხორციელების კანონიერება. აღნიშნული შემოწმებების ფარგლებში დადგინდა, რომ შენობის გარე და შიდა პერიმეტრზე — დერეფნებში, კიბის უჯრედებში, პაციენტების მოსაცდელში და დასაქმებულთა გარკვეულ სამუშაო სივრცეებში (მაგალითად, რეგისტრატურაში, ელიმინაციის ოთახში, სადაც ხდება მეტადონით ჩანაცვლების პროგრამით მოსარგებლეებისთვის მედიკამენტების გაცემა და სტერილიზაციის ოთახში) დაწესებულებები ვიდეომონიტორინგს საკუთრების, უსაფრთხოებისა და პაციენტების ჯანმრთელობის დაცვის მიზნებისთვის ახორციელებდნენ. სამსახურის შეფასებით, ხსენებულ სივრცეებში ვიდეომონიტორინგის განხორციელება მათი დანიშნულების გათვალისწინებით, წარმოადგენს ლეგიტიმური მიზნის მიღწევის ადეკვატურ და პროპორციულ საშუალებას და კანონის მე-10 მუხლის პირველი და მე-3 პუნქტებით განსაზღვრულ მიზნებთან შესაბამისია.

შემოწმებების ფარგლებში ასევე დადგინდა, რომ სამედიცინო დაწესებულებები ლაბორატორიის ადგილზე გამოძახების თანამშრომლებისთვის განკუთვნილ სამუშაო ოთახში და საკონფერენციო დარბაზში, ხოლო პროფესიული კოლეჯები — სასწავლო სივრცეებში, ვიდეომონიტორინგს ახორციელებდნენ საკუთრების დაცვის მიზნით. სამსახურის შეფასებით, დამუშავებისთვის პასუხისმგებელი პირების მიერ ქონების დაცვა, მართალია შეიძლება მიჩნეულ იქნეს ლეგიტიმურ ინტერესად, თუმცა აღნიშნული მიზნის მიღწევა შესაძლებელია სხვა, ნაკლებად მზღუდავი საშუალებებითაც. მაგალითად, კერძო დაწესებულებაში არსებული ნივთების, საკუთრების და უსაფრთხოების დაცვის ერთ-ერთი გარანტიაა ე. წ. დაცვის სერვისით სარგებლობა, შემოსასვლელში შესაბამისი პასუხისმგებელი პირის დაყენება, ნივთებისთვის სპეციალური სათავსოს განსაზღვრა და სხვა. ამასთან, სამსახურმა დაადგინა, რომ სამედიცინო დაწესებულებებისა და პროფესიული კოლეჯების მიერ ლაბორატორიის ადგილზე გამოძახების ოთახში, საკონფერენციო დარბაზში და სასწავლო სივრცეებში 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 შეესაბამებოდა კანონის მე-10 მუხლის მე-3 პუნქტის მოთხოვნებს.

გარდა ზემოაღნიშნულისა, სამსახურმა ერთი-ერთი ლაბორატორიის შემოწმების ფარგლებში, კანონის მოთხოვნებთან შეუსაბამოდ მიიჩნია ვიდეომონიტორინგი პაციენტის მოსაცდელში დაყოვნების დროის კონტროლის, პაციენტთა ნაკადის შემოწმების, კადრის დამატების ან ახალი ფილიალის გახსნის საჭიროების განსაზღვრის მიზნით. სამსახურის შეფასებით, მომსახურების მონიტორინგის და ხარისხის გაუმჯობესების (მათ შორის, კადრის დამატების ან ახალი ფილიალის გახსნის შესახებ გადაწყვეტილების მიღების), ასევე, მაღალი ხარისხის სამედიცინო მომსახურების მიწოდების მიზნის 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, სამსახურის შეფასებით, ლაბორატორიის მიერ დასახელებული მიზნებით ვიდეომონიტორინგის განხორციელება ვერ ჩაითვლება მიზნის ადეკვატურ და პროპორციულ საშუალებად. სამსახურის გადაწყვეტილებით, ლაბორატორიას დაევალა ხსენებული მიზნებით სისტემაზე დაშვების მქონე პირებისათვის ვიდეოსათვალთვალო სისტემის ჩანაწერებზე წვდომის შეზღუდვა.

სამსახურის მიერ ჩატარებული სამედიცინო დაწესებულებების შემოწმებების ფარგლებში გამოიკვეთა, რომ ვიდეომონიტორინგი ასევე მიმდინარეობდა ისეთ სივრცეებში, სადაც მონაცემთა სუბიექტს აქვს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი.[3] აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს 2011 წლის 28 დეკემბრის კანონის თანახმად, ვიდეომონიტორინგის განხორციელება დაუშვებელი იყო მხოლოდ გამოსაცვლელ ოთახებსა და ჰიგიენისთვის განკუთვნილ ადგილებში. ახალი კანონით გაფართოვდა ხსენებული შეზღუდვის არეალი და სუბიექტის ღირსების უფლების მაღალი სტანდარტის დაცვის მიზნით, დააწესა ვიდეომონიტორინგის ისეთ სივრცეებში შეზღუდვა, სადაც პირს აქვს მისი პირადი ცხოვრების დაცულობის გონივრული მოლოდინი. კერძოდ, კანონის მე-10 მუხლის მე-4 პუნქტის თანახმად, დაუშვებელია ვიდეომონიტორინგის განხორციელება გამოსაცვლელ ოთახებში,

[3] მაგალითად: სამანიპულაციო ოთახები, რადიოლოგიის ოთახი.

ჰიგიენისთვის განკუთვნილ ადგილებში ან ისეთ სივრცეში, სადაც მონაცემთა სუბიექტს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს ან/და ვიდეომონიტორინგის განხორციელება საყოველთაოდ აღიარებულ ზნეობრივ ნორმებს ეწინააღმდეგება. ნიშანდობლივია, რომ ასეთ სივრცეებს შესაძლოა, მიეკუთვნებოდეს ისეთი არეალები, სადაც თავად სივრცის შინაარსისა და დანიშნულებიდან გამომდინარე, პრივატულობის დაცვა განსაკუთრებით მნიშვნელოვანია. აღნიშნული დაკავშირებულია პირადი ცხოვრების დაცულობის უფლებასთან, რომელიც თავის მხრივ, ღირსების უფლებით დაცულ სფეროში ექცევა.

ნიშანდობლივია, რომ სამსახურმა სამედიცინო დაწესებულებების შემოწმების ფარგლებში, ვიდეომონიტორინგი სამედიცინო მანიპულაციების ოთახებში მიიჩნია დაუშვებლად. ხსენებული შემოწმებების ფარგლებში დადგინდა, რომ სამედიცინო დაწესებულებები კლინიკის სამედიცინო პერსონალისთვის დაკისრებული უფლებამოსილებების არაჯეროვანი შესრულების თავიდან აცილების, აგრეთვე, სამედიცინო პერსონალის შეცდომების დროული იდენტიფიცირების მიზნით, ვიდეომონიტორინგს ახორციელებდნენ სამანიპულაციო (თერაპიულ და ქირურგიულ) კაბინეტებში და სამედიცინო მანიპულაციებისთვის (ლაბორატორიული ტესტირებისთვის ბიოლოგიური მასალის ნიმუშების აღება და დამუშავება) განკუთვნილ ოთახებში. საკუთრების დაცვის მიზნით კი — რადიოლოგიის კაბინეტში. სამსახურის შეფასებით, ისეთ სივრცეებში, სადაც პაციენტს უტარდება სამედიცინო მანიპულაციები, პირს აქვს მისი პირადი ცხოვრების დაცულობის და პატივისცემის ლეგიტიმური და გონივრული მოლოდინი.[4] სამედიცინო მომსახურების მიღების პროცესში დამუშავებული მონაცემების სენსიტიური ხასიათის გათვალისწინებით, განსაკუთრებით მნიშვნელოვანია დაცული იქნეს პაციენტის პირადი ცხოვრების ხელშეუხებლობის უფლება. სამედიცინო პროცედურების განხორციელებისთვის განკუთვნილ სივრცეში დამონტაჟებული ვიდეოსათვალთვალო კამერა კი, პირს უკარგავს კონფიდენციალურობის შეგრძნებას და იმის აღქმა, რომ შესაძლოა მის მონაცემებზე, გარდა სამედიცინო პერსონალისა, კიდევ სხვა პირ(ებ)ს აქვთ წვდომა, ზღუდავს მისი ქცევის თავისუფლებას. ამასთან, „პაციენტის უფლებების შესახებ“ საქართველოს კანონის 30-ე მუხლის თანახმად, სამედიცინო მომსახურების გაწევისას, დასაშვებია მხოლოდ მასში უშუალოდ მონაწილე პირთა დასწრება, გარდა იმ შემთხვევებისა, როცა პაციენტი თანახმაა ან მოითხოვს სხვა პირთა დასწრებას. აღნიშნულიდან გამომდინარე, სამსახურმა ხსენებული სამედიცინო დაწესებულების მიერ ვიდეომონიტორინგის იმ სივრცეებში

[4] ECtHR, Case Of Von Hannover v. Germany Application No. 59320/00, Judgement, 24/09/2004, §51.

განხორციელება, სადაც მონაცემთა სუბიექტებს (პაციენტებს) უტარდებათ სამედიცინო მანიპულაციები, მიიჩნია კანონის მე-10 მუხლის მე-4 პუნქტის დარღვევად და აღნიშნულის აღმოსაფხვრელად გასცა შესაბამისი დავალებები.

სამედიცინო დაწესებულებების, აგრეთვე, საჯარო და კერძო სკოლების მიერ ვიდეომონიტორინგის განხორციელების გზით, პერსონალური მონაცემების დამუშავების კანონიერების გეგმური შემოწმებების ფარგლებში გამოიკვეთა ვიდეომონიტორინგის განხორციელების თაობაზე გამაფრთხილებელი ნიშნების კანონის შესაბამისად განთავსების ვალდებულების ნაკლოვანი შესრულების ფაქტები. კერძოდ, ზოგიერთ შემთხვევაში, ვიდეომონიტორინგის შიდა და გარე სივრცეებში განხორციელების მიუხედავად, ნიშნები განთავსებული იყო მხოლოდ შენობის შიდა სივრცეში. ამასთან, რამდენიმე დაწესებულების შემოწმების ფარგლებში გამოიკვეთა, რომ ვიდეომონიტორინგის თაობაზე გამაფრთხილებელი ნიშნები არც შიდა და არც გარე სივრცეში იყო განთავსებული იმგვარად, რომ მონაცემთა სუბიექტისთვის სრულად ყოფილიყო აღქმადი ვიდეომონიტორინგის არეალი. გარდა ამისა, განთავსებული ნიშნები, მიუხედავად იმისა, რომ ზოგიერთ შემთხვევაში ხდებოდა მათი მუდმივი განახლება, მათ შორის, 2024 წლის პირველი მარტის შემდგომ პერიოდში, არ შეიცავდა ინფორმაციას დამუშავებისთვის პასუხისმგებელი პირის და მისი საკონტაქტო ინფორმაციის შესახებ. აღნიშნული კი კანონის მე-10 მუხლის მე-8 და მე-9 პუნქტებით განსაზღვრულ ვალდებულებას წარმოადგენს.

ვიდეომონიტორინგის განხორციელების პროცესში მონაცემთა სუბიექტის უფლებების დაცვის თვალსაზრისით და გამჭვირვალობის პრინციპის უზრუნველსაყოფად, მნიშვნელოვანია, ვიდეომონიტორინგის მიმდინარეობის შესახებ გამაფრთხილებელი ნიშნები განთავსებული იყოს იმგვარად, რომ მონაცემთა სუბიექტისთვის აღქმადი იყოს ვიდეომონიტორინგის არეალი სრულად. ამასთანავე, მართალია, ხსენებული ნიშნების განთავსების ვალდებულება არ გულისხმობს მათ თითოეულ ვიდეოსათვალთვალო კამერასთან განთავსების აუცილებლობას, თუმცა აღნიშნული პირობების დაკმაყოფილებისთვის, ნიშნები უნდა განთავსდეს გონივრულ დისტანციაზე.[5] ამდენად, აღნიშნული ნაკლოვანებების გამოსწორების მიზნით, სამსახურის მიერ დამუშავებისთვის პასუხისმგებელ პირებს დაევალათ ვიდეომონიტორინგის განხორციელების თაობაზე გამაფრთხილებელი ნიშნების „პერსონალურ

[5] EDPB, Guidelines 3/2019 on processing of personal data through video devices Version 2.0 Adopted on 29 January 2020, 26, par., 112-113, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf> [11/08/2024].

მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლის მე-8 და მე-9 პუნქტების მოთხოვნათა დაცვით განთავსება.

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

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონით გარკვეულ მონაცემთა დამუშავების პროცესებთან, კერძოდ, ვიდეომონიტორინგთან, აუდიომონიტორინგთან და ბიომეტრიულ მონაცემთა დამუშავებასთან დაკავშირებით დამუშავებისთვის პასუხისმგებელ პირს დაეკისრება მონაცემთა დამუშავების პრინციპების შესაბამისად, წინასწარ წერილობით განსაზღვროს მონაცემთა დამუშავების პროცესთან დაკავშირებული რიგი გარემოებები. კერძოდ, კანონის მე-9 მუხლის მე-2 პუნქტის მიხედვით, ბიომეტრიული მონაცემების დამუშავებისას მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა წინასწარ წერილობით უნდა განსაზღვროს ბიომეტრიულ მონაცემთა დამუშავების მიზანი და მოცულობა, ამ მონაცემთა შენახვის ვადა, მათი შენახვისა და განადგურების წესი, პირობები და მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმები. აგრეთვე, კანონის მე-10 მუხლის მე-2 პუნქტის და მე-11 მუხლის მე-2 პუნქტის მიხედვით, ვიდეომონიტორინგისა და აუდიომონიტორინგის შემთხვევაში, გარდა ზემოხსენებული საკითხებისა, დამუშავებისთვის პასუხისმგებელმა პირმა დამატებით წერილობით უნდა გაითვალისწინოს ვიდეო/აუდიო მონიტორინგის ხანგრძლივობა, ჩანაწერზე წვდომის წესი და პირობები.

ზემოაღნიშნული ვალდებულებების მიზანია, უზრუნველყოს მონაცემთა დამუშავების პროცესის კანონთან შესაბამისი ფორმით დაგეგმვა და განხორციელება, რაც დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა დამუშავების პროცესის წინასწარი ორგანიზებისა და მონაცემთა სუბიექტების უფლებების ხელყოფის თავიდან არიდების შესაძლებლობას მისცემს. ამასთან, ზემოხსენებული ინფორმაციის წინასწარ, წერილობით განსაზღვრის პირობებში, მონაცემთა დამმუშავებელი ორგანიზაციის თანამშრომლებისთვის ბევრად უფრო მარტივად აღქმადი გახდება მონაცემთა დამუშავების კონკრეტული პროცესის მიზანი და მოცულობა.

საანგარიშო პერიოდში სამსახურმა შეისწავლა ვიდეომონიტორინგის, აუდიომონიტორინგის და ბიომეტრიულ მონაცემთა დამუშავების პროცესში ზემოხსენებული ვალდებულებების შესრულების არაერთი ფაქტი. სამსახურმა გეგმურად შეისწავლა ორი კომერციული ბანკის მიერ დისტანციური იდენტიფიკაციის პროცესში ბიომეტრიული მონაცემების დამუშავების კანონიერება. შემოწმებების ფარგლებში დადგინდა, რომ ბანკების მიერ მომხმარებლის ბიომეტრიული მონაცემი (სახის გამოსახულება) მუშავდებოდა მხოლოდ მათი დისტანციური იდენტიფიკაციის პროცესში (მათ შორის ინტერნეტ ბანკინგით, ონლაინ განვადების ვებგვერდით სარგებლობის დროს და სხვა შემთხვევებში), რაც, თავის მხრივ, მოიცავდა ხელოვნური ინტელექტის საშუალებით მომხმარებლის გამოსახულების დამუშავებას. ერთ-ერთი კომერციული ბანკის შემოწმების ფარგლებში, წარმოდგენილ იქნა 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. ხოლო მეორე კომერციული ბანკის შემოწმების ფარგლებში წარმოდგენილი განმარტების თანახმად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-9 მუხლის მე-2 პუნქტით გათვალისწინებული საკითხები ბანკს განსაზღვრული ჰქონდა რამდენიმე დოკუმენტით, კერძოდ: პერსონალური მონაცემების დაცვის პოლიტიკით, საბანკო მომსახურების სტანდარტული პირობებით და „ფიზიკური პირების ელექტრონული იდენტიფიკაცია/ვერიფიკაცია და პრევენციული ღონისძიებების“ 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 წერილობით გათვალისწინება.

სამსახურმა ასევე გეგმურად შეისწავლა ორი კომერციული ბანკის მიერ ცხელი ხაზის მეშვეობით პერსონალურ მონაცემთა დამუშავების კანონიერება.

შემოწმებების ფარგლებში დადგინდა, რომ ერთ-ერთი ბანკის აუდიომონიტორინგის განხორციელებასთან დაკავშირებით წერილობითი დოკუმენტი სრულყოფილად არ განსაზღვრავდა კანონით დადგენილ სავალდებულო საკითხებს (მაგალითად, აუდიომონიტორინგის განხორციელების მოცულობას და ხანგრძლივობას). ამდენად, ბანკს სამსახურის მიერ დაევალა ხსენებული საკითხების წინასწარ მოწესრიგება. რაც შეეხება, მეორე კომერციულ ბანკს, ამ შემთხვევაში, დოკუმენტი ითვალისწინებდა მონაცემთა სუბიექტის მიერ საკუთარი მონაცემების შემცველი აუდიოჩანაწერის გაცნობის შეზღუდვას, იმ შემთხვევაში, როდესაც 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 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 21-ე მუხლით გათვალისწინებული შეზღუდვის საფუძვლების არსებობა: 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. აღნიშნულთან დაკავშირებით, ყველა შემთხვევაში, წინასწარ უარის თქმა არ არის შესაბამისობაში ზემოხსენებული ნორმით გათვალისწინებულ ვალდებულებასთან და მონაცემთა სუბიექტის უფლებებთან დაკავშირებით შესაძლოა შეცდომაში შემყვანი აღმოჩნდეს იმ პირებისთვის, რომლებიც გაეცნობიან ზემოხსენებულ დოკუმენტს ან/და ევალებათ მისი აღსრულება. შესაბამისად, კომერციულ 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 ორგანიზაცია (საჯარო სკოლები, პროფესიული სასწავლებლები და სამედიცინო დაწესებულებები). მართალია, დამუშავებისთვის პასუხისმგებელი პირების მიერ უმეტეს შემთხვევაში წარმოდგენილი იქნა ვიდეომონიტორინგის განხორციელების შესახებ წერილობითი დოკუმენტები, თუმცა როგორც წესი აღნიშნული დოკუმენტები სრულყოფილად არ მოიცავდა კანონის მე-10 მუხლის მე-2 პუნქტით განსაზღვრულ საკითხებს (მაგალითად: ვიდეომონიტორინგის მიზანს და მოცულობას, ვიდეომონიტორინგის ხანგრძლივობას და ვიდეოჩანაწერის შენახვის ვადას, ვიდეოჩანაწერზე წვდომის,

მისი შენახვისა და განადგურების წესსა და პირობებს, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმებს). შესაბამისად, დასახელებულ შემთხვევებშიც სამსახურის მიერ გაცემული იქნა დავალებები აღნიშნული ნორმით განსაზღვრული საკითხების შეფასებისა და წერილობით დოკუმენტებში სრულად ასახვის შესახებ.

8. პერსონალურ მონაცემთა დაცვის სამსახურის კანონიერი მოთხოვნის შეუსრულებლობა

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის ერთ-ერთ მნიშვნელოვან სიახლეს წარმოადგენს, პერსონალურ მონაცემთა დაცვის სამსახურის კანონიერი მოთხოვნის (დავალების) შეუსრულებლობის სამართალდარღვევად განსაზღვრა. კერძოდ, აღნიშნული კანონის 87-ე მუხლის თანახმად, ადმინისტრაციული პასუხისმგებლობის დაკისრების საფუძველს წარმოადგენს კანონის 52-ე მუხლის პირველი პუნქტის „ა“–„დ“ ქვეპუნქტების შესაბამისად გაცემული დავალებების შეუსრულებლობა. თავის მხრივ, კანონის 52-ე მუხლის პირველი პუნქტის „ა“–„დ“ ქვეპუნქტების, მე-2 და მე-6 პუნქტების მიხედვით, თუ პერსონალურ მონაცემთა დაცვის სამსახური გამოავლენს ამ კანონის ან მონაცემთა დამუშავების მომწესრიგებელი სხვა ნორმატიული აქტის დარღვევას, იგი უფლებამოსილია მოითხოვოს დარღვევისა და მონაცემთა დამუშავებასთან დაკავშირებული ნაკლოვანებების მის მიერ მითითებული ფორმით და მითითებულ ვადაში გამოსწორება, მონაცემთა დამუშავების შეწყვეტა, მონაცემთა დაბლოკვა, წაშლა, განადგურება, დეპერსონალიზაცია და სხვა.

ნიშანდობლივია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს 2011 წლის 28 დეკემბრის კანონი არ შეიცავდა მსგავს დანაწესს, რის გამოც მისი მოქმედების პერიოდში სამსახურს, ფაქტობრივად, არ გააჩნდა პერსონალურ მონაცემთა დაცვის საკითხებთან დაკავშირებით მის მიერ გამოცემული დავალებების აღსრულების ხელშემწყობი ეფექტური მექანიზმი. აღნიშნული საკანონმდებლო ცვლილების შედეგად, სამსახურს მიეცა მნიშვნელოვანი სამართლებრივი ბერკეტი, გააკონტროლოს მონაცემთა დამუშავების პროცესების კანონმდებლობასთან შესაბამისობის უზრუნველყოფის მიზნით გაცემული დავალებების შესრულება, მათი შეუსრულებლობის შემთხვევაში კი დაიწყოს შემოწმება, გამოიყენოს კანონის 87-ე მუხლით გათვალისწინებული სახდელი და კვლავ გასცეს სავალდებულო დავალება, კანონის 52-ე მუხლის პირველი პუნქტით გათვალისწინებული წესით.

საანგარიშო პერიოდში სამსახურმა შეისწავლა პერსონალურ მონაცემთა დაცვის სამსახურის კანონიერი მოთხოვნის შეუსრულებლობის რამდენიმე ფაქტი. მათ შორის, სამსახურმა არაგეგმურად განახორციელა სამი საჯარო სკოლის (სსიპ - ქალაქ ჭიათურის №12 საჯარო სკოლა, სსიპ - ქრისტეფორე III-ის სახელობის ხაშურის მუნიციპალიტეტის დაბა სურამის №4 საჯარო სკოლა და სსიპ - ქალაქ თბილისის №200 საჯარო სკოლა) შემოწმება (ინსპექტირება), რა დროსაც შეისწავლა პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან/განსაზღვრასთან დაკავშირებით გაცემული დავალებების შეუსრულებლობის ფაქტები. კერძოდ, სამსახურის უფროსის ბრძანების საფუძველზე განხორციელებული, სკოლების მიერ ინდივიდუალური სასწავლო გეგმების შექმნისა და შენახვის გზით მოსწავლეთა პერსონალური მონაცემების დამუშავების კანონიერების გეგმური შემოწმების ფარგლებში გამოიკვეთა, რომ სკოლებს კანონის 33-ე მუხლის პირველი პუნქტის მოთხოვნათა საწინააღმდეგოდ, 2024 წლის პირველი ივნისის შემდგომ პერიოდში, არ ჰყავდათ დანიშნული/განსაზღვრული ოფიცრები. აღნიშნულის საფუძველზე, სამსახურის უფროსის გადაწყვეტილებებით სკოლებს დაევალათ კანონით დადგენილი წესით, ოფიცრის დაუყოვნებლივ დანიშვნა/განსაზღვრა.

გადაწყვეტილებების კანონიერ ძალაში შესვლის შემდგომ, გაცემული დავალებების შესრულებასთან დაკავშირებით, სამსახურის მიერ მოპოვებული ინფორმაციით გამოიკვეთა, რომ სკოლებს კვლავ არ ჰყავდათ დანიშნული/განსაზღვრული ოფიცერი. აღნიშნულის საფუძველზე სკოლების მიერ, კანონის 33-ე მუხლით გათვალისწინებული, ოფიცრის დანიშვნასთან/განსაზღვრასთან დაკავშირებული ვალდებულების სავარაუდო შეუსრულებლობის ფაქტის შესწავლის მიზნით, სამსახურის მიერ კვლავ დაიწყო შემოწმებები. დასახელებული შემოწმებების ფარგლებში დადასტურდა სკოლების მიერ სამსახურის უფროსის დავალებების შეუსრულებლობის ფაქტი. საკითხის შეფასებისას, სამსახურმა ყურადღება გაამახვილა იმ გარემოებაზე, რომ კანონის 33-ე მუხლის პირველი პუნქტი იმპერატიული ხასიათისაა და არ ტოვებს სივრცეს საგამონაკლისო შემთხვევებისთვის. ამასთან, ყურადღება გამახვილდა იმაზეც, რომ კანონის 90-ე მუხლის მე-3 პუნქტის საფუძველზე, ოფიცრის დანიშვნის/განსაზღვრის ვალდებულება კანონის მიღებიდან (მიღების თარიღი: 2023 წლის 14 ივნისი) თითქმის ერთი წლის შემდეგ (2024 წლის პირველი ივნისიდან) ამოქმედდა. შესაბამისად, დაწესებული მოთხოვნის შესრულების მომზადებისთვის კანონმდებელმა გაითვალისწინა ხანგრძლივი გარდამავალი პერიოდი. მიუხედავად, ამისა შემოწმების პერიოდისთვის სკოლებს კვლავ არ ჰყავდათ დანიშნული/განსაზღვრული ოფიცერი.

ყოველივე აღნიშნულიდან გამომდინარე, შემოწმების ფარგლებში სამსახურმა დაადგინა, რომ სკოლებმა კანონის 52-ე მუხლის მე-2 პუნქტის მოთხოვნათა საწინააღმდეგოდ არ შეასრულეს, ამავე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტის და 33-ე მუხლის პირველი პუნქტის მოთხოვნათა შესაბამისად, სამსახურის უფროსის გადაწყვეტილებებით მიცემული დავალებები. ამდენად, სამსახურის კანონიერი მოთხოვნის შეუსრულებლობისთვის სკოლებს დაეკისრათ ადმინისტრაციული პასუხისმგებლობა. ამასთან, სამსახურის მიერ გაიცა დავალება სამსახურის გადაწყვეტილებით განსაზღვრულ ვადაში ოფიცრის დანიშვნა/განსაზღვრასთან დაკავშირებით.

9. დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებული წერილობითი შეთანხმების სავალდებულო პირობები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 36-ე მუხლის თანახმად, დამუშავებაზე უფლებამოსილმა პირმა მონაცემები შეიძლება დაამუშაოს მხოლოდ შესაბამისი სამართლებრივი აქტის ან დამუშავებისთვის პასუხისმგებელ პირთან დადებული წერილობითი შეთანხმების საფუძველზე, რომლითაც უნდა განისაზღვროს მონაცემთა დამუშავების საფუძვლები, მიზნები, დასამუშავებელ მონაცემთა კატეგორიები, მონაცემთა დამუშავების ვადა და დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის უფლებები და ვალდებულებები. აღსანიშნავია, რომ მხარეთა შორის არსებული სამართლებრივი ურთიერთობის გათვალისწინებით, სწორედ დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას განეკუთვნება მონაცემთა დამუშავების მიზნებისა და საშუალებების განსაზღვრა. დამუშავებაზე უფლებამოსილი პირი კი, მონაცემებს დამუშავებისთვის პასუხისმგებელი პირის სახელით, მის მიერ განსაზღვრული დავალებებისა და მითითებების საფუძველზე ამუშავებს.

საანგარიშო პერიოდში სამსახურმა შეისწავლა დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებული წერილობითი შეთანხმების/ხელშეკრულების კანონთან შესაბამისობის შემთხვევები. არაერთი შემოწმების ფარგლებში გამოიკვეთა დამუშავებაზე უფლებამოსილი პირების მიერ დამუშავებისთვის პასუხისმგებელ პირებთან დადებული ხელშეკრულების ფარგლების გაცდენის ფაქტებიც, რის საფუძველზეც გამოვლინდა კანონის 36-ე

მუხლის მოთხოვნების დარღვევები. სამსახურმა შეისწავლა შემთხვევა, რომლის ფარგლებში დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებული ხელშეკრულებით განსაზღვრული იყო დამუშავებაზე უფლებამოსილი პირის ვალდებულება, მოეხდინა კანონით განსაზღვრული უსაფრთხოების ზომების დაცვა, რაც ასევე გათვალისწინებულია კანონის 36-ე მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტით, რომლის მიხედვით, მხარეთა შორის დადებული წერილობითი შეთანხმების საფუძველზე, დამუშავებაზე უფლებამოსილი პირი ვალდებულია უზრუნველყოს მონაცემთა უსაფრთხოება ამ კანონის შესაბამისად. შემოწმების ფარგლებში დადგინდა, რომ დამუშავებაზე უფლებამოსილი პირის ელექტრონულ სისტემაში არ აღირიცხებოდა ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედება. ელექტრონული ფორმით დაცული მონაცემების უსაფრთხოების უზრუნველსაყოფად, მათზე წვდომის ადვილად ხელმისაწვდომობის გათვალისწინებით, კანონის 27-ე მუხლის მე-4 პუნქტი განსაზღვრავს დამუშავებაზე უფლებამოსილი პირის ვალდებულებას უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების (ინციდენტების, მონაცემთა შეგროვების, შეცვლის, მათზე წვდომის, მათი გამჟღავნების (გადაცემის), დაკავშირებისა და წაშლის თაობაზე ინფორმაციის) აღრიცხვა. ყოველივე ზემოაღნიშნულის გათვალისწინებით დადგინდა, რომ დამუშავებაზე უფლებამოსილ პირის მიერ არ იყო მიღებული მონაცემთა უსაფრთხოებისთვის კანონით დადგენილი ზომები, რის შედეგადაც გასცდა დამუშავებისთვის პასუხისმგებელ პირთან დადებული ხელშეკრულების ფარგლებს, და დაარღვია კანონის 36-ე მუხლის მოთხოვნები. აღნიშნულის გათვალისწინებით, სამსახურმა დამუშავებაზე უფლებამოსილ პირს დაავალა ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვის უზრუნველყოფა.

ერთ-ერთი შემოწმების ფარგლებში გამოიკვეთა, რომ კომპანია, როგორც დამუშავებაზე უფლებამოსილი პირი, მარკეტინგული შინაარსის მოკლეტექსტურ შეტყობინებებს აგზავნიდა სხვადასხვა პირებთან დადებული ხელშეკრულებების საფუძველზე. კომპანიასა და დამუშავებისათვის პასუხისმგებელ პირებს შორის დადებული ხელშეკრულებების თანახმად, მხარეთათვის ხელშეკრულებით განსაზღვრული მოვალეობები არ უნდა გადასცემოდა ნებისმიერ მესამე პირს მეორე მხარის წერილობითი თანხმობის გარეშე. ამასთან, კანონის 36-ე მუხლის მე-7 პუნქტის თანახმად, თუ საქართველოს კანონმდებლობით სხვა რამ არ არის დადგენილი, დაუშვებელია, დამუშავებაზე უფლებამოსილმა პირმა თავისი უფლება-მოვალეობები სრულად ან ნაწილობრივ გადასცეს სხვა პირს დამუშავებისთვის პასუხისმგებელი პირის წინასწარი წერილობითი თანხმობის

გარეშე. აგრეთვე, დამუშავებისთვის პასუხისმგებელი პირის თანხმობა დამუშავებაზე უფლებამოსილ პირს არ ათავისუფლებს შესაბამისი ვალდებულებებისა და პასუხისმგებლობისგან. შემოწმების ფარგლებში დადგინდა, რომ დამუშავებისთვის პასუხისმგებელი პირები, კომპანიას აძლევდნენ კონკრეტულ დავალებას — კერძოდ, აწვდიდნენ მარკეტინგული შინაარსის შეტყობინების ტექსტს და სახელწოდებას, რომელიც უნდა გაგზავნილიყო ადრესატებთან. აღნიშნული ვალდებულების შესრულების მიზნით დამუშავებაზე უფლებამოსილმა პირმა ხელშეკრულება დადო სხვა კომპანიასთან, რომლის ფარგლებშიც დამუშავებისთვის პასუხისმგებელი პირების სახელით, მარკეტინგული შინაარსის შეტყობინებები გააგზავნა სხვა კომპანიის პლატფორმის მეშვეობით. დამუშავებაზე უფლებამოსილი პირის წარმომადგენელმა მიუთითა, რომ დამუშავებისათვის პასუხისმგებელი პირები არ იყვნენ ინფორმირებულები სხვა კომპანიის მომსახურებისა და სატელეფონო ნომრების ბაზის გამოყენების თაობაზე. აღნიშნულის გათვალისწინებით, შემოწმების ფარგლებში დადგინდა, რომ დამუშავებაზე უფლებამოსილმა პირმა დამუშავებისთვის პასუხისმგებელი პირის წინასწარი წერილობითი თანხმობის გარეშე თავისი უფლება-მოვალეობები გადასცა სხვა პირს, შესაბამისად დაარღვია კანონის 36-ე მუხლით განსაზღვრული მოთხოვნები.

გასათვალისწინებელია, რომ დამუშავებისთვის პასუხისმგებელი პირის თანხმობა დამუშავებაზე უფლებამოსილ პირს არ ათავისუფლებს შესაბამისი ვალდებულებებისა და პასუხისმგებლობისგან. განსახილველ შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირების წინასწარი წერილობითი თანხმობების არსებობის პირობებშიც კი, ხსენებულ კომპანიას, რამდენიმე დამუშავებისთვის პასუხისმგებელი პირის წინაშე ნაკისრი ჰქონდა ვალდებულება, რომ მარკეტინგული შინაარსის შეტყობინებების გაგზავნის პროცესი და მათ შორის, სატელეფონო ნომრების ბაზა, რომლებზეც მოხდებოდა შეტყობინებების გაგზავნა, შესაბამისობაში იყო კანონთან. ამდენად, დამუშავებაზე უფლებამოსილ პირს ჰქონდა ვალდებულება დარწმუნებულიყო, რომ მის მიერ გამოყენებული, სხვა კომპანიის სატელეფონო ნომრების ბაზა მოპოვებული იყო კანონით დადგენილი მოთხოვნების შესაბამისად, რაც ვერ უზრუნველყო, ვინაიდან ხსენებულ სხვა კომპანიას მის სატელეფონო ბაზაში არსებული ნომრების პირდაპირი მარკეტინგის მიზნით დამუშავებასთან დაკავშირებით, მონაცემთა სუბიექტებისგან არ ჰქონდა მოპოვებული თანხმობა კანონით დადგენილი წესით.

აღნიშნულის გათვალისწინებით, შემოწმების ფარგლებში დადგინდა, რომ დამუშავებაზე უფლებამოსილმა პირმა დამუშავებისთვის პასუხისმგებელ

პირებთან დადებული წერილობითი შეთანხმების გარეშე მონაცემების დამუშავების პროცესში და თავისი უფლება-მოვალეობების დამუშავებისთვის პასუხისმგებელი პირების წინასწარი წერილობითი თანხმობის გარეშე, სხვა კომპანიისთვის გადაცემის პროცესში დაარღვია კანონის 36-ე მუხლით განსაზღვრული მოთხოვნები. შესაბამისად, დამუშავებაზე უფლებამოსილ პირს დაევალა თავისი უფლება-მოვალეობები სრულად ან ნაწილობრივ სხვა პირს გადასცეს მხოლოდ დამუშავებისთვის პასუხისმგებელი პირის წინასწარი წერილობითი თანხმობის საფუძველზე და დარწმუნდეს აღნიშნული პირის მიერ მონაცემების პირდაპირი მარკეტინგის მიზნით დამუშავების კანონთან შესაბამისობაში.

გარდა ზემოაღნიშნული დარღვევებისა ორივე შემოწმების ფარგლებში გამოვლინდა დამუშავებაზე უფლებამოსილი პირების მიერ დამუშავებისთვის პასუხისმგებელი პირების სახელით პერსონალურ მონაცემთა დამუშავება კანონის 36-ე მუხლის პირველი პუნქტით დადგენილი წერილობითი ფორმის დაუცველად.

სამსახურის მიერ გეგმურად შესწავლილი მონაცემთა დამუშავების პროცესებში 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 გენერირებას. 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, მათ შორის, ხსენებული მუხლის მოთხოვნათა საწინააღმდეგოდ არ განსაზღვრავდა 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 ხელშეკრულება არ იყო შესაბამისი არც ხსენებული კანონის მოთხოვნებთან (მაგალითად, დასახელებული კანონი 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 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 ნორმა სწორედ მის კომპეტენციას აკუთვნებს მონაცემთა დამუშავების უფლების სხვა პირისთვის გადაცემის გადაწყვეტილების მიღების უფლებას. ხსენებული უფლების მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისთვის მინიჭება განპირობებულია, მათ შორის, იმ გარემოებით, რომ კანონის მოთხოვნათა შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს ეკისრება მნიშვნელოვანი პასუხისმგებლობა მონაცემთა დამუშავების მარეგულირებელი კანონმდებლობის შესაბამისად მონაცემთა დამუშავებაზე (მათ შორის, მონაცემთა უსაფრთხოების უზრუნველყოფაზე), 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. აღნიშნულთან დაკავშირებით ნიშანდობლივია, რომ არაერთი შემოწმების ფარგლებში გამოიკვეთა შემთხვევა, როდესაც დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა ქვეკონტრაქტორი პირისთვის გადაცემისას თანხმობის

აუცილებლობის საკითხი მოწესრიგებული იყო დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის გაფორმებული ხელშეკრულებით, თუმცა აღნიშნული ხელშეკრულება აქცენტს არ აკეთებდა ხელშეკრულების წერილობითი ფორმით დადების საჭიროებაზე. შესაბამისად, დასახელებულ შემთხვევებში სამსახურის მიერ მხარეებს დაევალათ უფლებამოსილი პირის მიერ უფლებამოსილებების სხვა პირებისთვის გადაცემისას დამუშავებისთვის პასუხისმგებელი პირის წინასწარი წერილობითი თანხმობის აუცილებლობის საკითხის გათვალისწინება ხელშეკრულებაში.

10. საქართველოს პროკურატურის მიერ პერსონალურ მონაცემთა დამუშავების კანონიერების გეგმური შემოწმების (ინსპექტირების) შესახებ

როგორც აღინიშნა, ახალი საკანონმდებლო მოწესრიგებით განისაზღვრა აუდიომონიტორინგის განხორციელების სპეციალური წესი. კერძოდ, კანონის მე-11 მუხლით ამომწურავად მოწესრიგდა აუდიომონიტორინგის გზით მონაცემთა დამუშავების კონკრეტული სამართლებრივი საფუძვლები. რაც შეეხება ვიდეომონიტორინგის განხორციელებას, მართალია, სპეციალურ მოწესრიგებას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს 2011 წლის 28 დეკემბრის კანონიც ითვალისწინებდა, თუმცა ახალი კანონით გააფართოვა იმ მიზნების ჩამონათვალი, რომელთა არსებობის შემთხვევაშიც ვიდეომონიტორინგის განხორციელება დასაშვებია. კანონის მე-10 და მე-11 მუხლებით განისაზღვრა დამატებითი ვალდებულებები, რომლის მიხედვითაც, ვიდეო/აუდიომონიტორინგის განმახორციელებელმა პირებმა (დამუშავებისთვის პასუხისმგებელმა პირებმა) კანონის მე-4 მუხლით დადგენილი პრინციპების შესაბამისად, წერილობით უნდა განსაზღვრონ ვიდეო/აუდიო მონიტორინგის მიზანი და მოცულობა, აუდიო/ვიდეო მონიტორინგის ხანგრძლივობა და მათი შენახვის ვადა, ჩანაწერების წვდომის, შენახვისა და განადგურების წესი და პირობები ისევე, როგორც მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმები.

ზემოაღნიშნული სიახლისა და საქართველოს კანონმდებლობით განსაზღვრული საქართველოს პროკურატურის უფლებამოსილებების (მათ შორის, არასრულწლოვანთა გამოკითხვასა და ამ პროცესის აუდიო-ვიდეოჩაწერის გზით ფიქსაციის განხორციელების უფლებამოსილები) გათვალისწინებით, მიზანშეწონილად იქნა მიჩნეული საქართველოს პროკურატურის მიერ არასრულწლოვანთა გამოკითხვის სპეციალიზებულ სივრცეებში,

არასრულწლოვანთა ვიდეო-აუდიო ფიქსაციის პროცესში მონაცემთა დამუშავების კანონიერების საკითხის შესწავლის მიზნით გეგმური შემოწმების ჩატარება.

შემოწმების ფარგლებში დადგინდა, რომ არასრულწლოვანთა გამოკითხვის მიზნით, 8 (რვა) რაიონულ პროკურატურაში მოწყობილ არასრუწლოვანთა გამოკითხვის სპეციალიზებულ ოთახებში (ჯამში 8 (რვა) ოთახი), დამონტაჟებულია გამოსახულებისა და ხმოვანი სიგნალის ჩამწერი მოწყობილობები (ვიდეოკამერები და ე.წ. „მიკროფონები“), რომელთა მეშვეობითაც შესაბამისი საჭიროების არსებობისას, ხდება მხოლოდ გამოკითხვის პროცესის ვიდეო-აუდიო ჩაწერა.

შემოწმების ფარგლებში პროკურატურის მიერ წარმოდგენილი განმარტებებისა და საქართველოს სისხლის სამართლის საპროცესო კოდექსისა და არასრულწლოვანთა მართლმსაჯულების კოდექსის ანალიზის საფუძველზე დადგინდა, რომ პროკურატურის მიერ არასრულწლოვანთა გამოკითხვის პროცესში ვიდეომონიტორინგის განხორციელება (ვიდეოჩანაწერის შექმნა), ერთი მხრივ უკავშირდება არასრულწლოვნის დაცვის (არასრულწლოვნის მეორეული ვიქტიმიზაციის თავიდან აცილებას) მიზანს, მეორე მხრივ კი იგი გამომდინარეობს სხვა ლეგიტიმური ინტერესის სფეროს მიკუთვნებული ამოცანების შესრულების საჭიროებიდან (არასრულწლოვნის ასაკის, ფიზიკური და გონებრივი განვითარების, მისი მძიმე ემოციურ ფონის გათვალისწინებით, არსებობს რისკი იმისა, რომ არასრულწლოვანს შესაძლოა დაავიწყდეს გამოძიების მიზნებისთვის მნიშვნელოვანი ინფორმაცია, რითაც ხელი შეეშლება მტკიცებულების მოპოვებას, შესაბამისად, დაზიანდება გამოძიების ინტერესი), ვინაიდან სრული და ობიექტური გამოძიების წარმოება პირდაპირ კავშირშია სამართლიან სასამართლო უფლებასა და მართლმსაჯულების განხორციელებასთან, რაც სახელმწიფოს ლეგიტიმური ინტერესის სფეროს წარმოადგენს.

რაც შეეხება აუდიომონიტორინგის განხორციელებას, პროკურატურის მხრიდან აუდიომონიტორინგის განხორციელება, უპირველეს ყოვლისა, მიემართება საოქმო ჩანაწერის წარმოებას (თავისი შინაარსით, აღნიშნული ჩანაწერი წარმოადგენს აუდიო ოქმს). გარდა ამისა, გამოკითხვის პროცესში შექმნილი ვიდეო-აუდიო ჩანაწერი წარმოადგენს სისხლის სამართლის საქმის მასალას. ამდენად, იმის გათვალისწინებით, რომ პროკურატურა სისხლისსამართლებრივი დევნის ორგანოა და მხარს უჭერს სახელმწიფო ბრალდებას სასამართლოში, ცხადია, მას აღნიშნული ფუნქციის შესრულების პროცესში გააჩნია მნიშვნელოვანი ლეგიტიმური ინტერესი შექმნას გამოკითხვის პროცესის ამსახველი ჩანაწერი, მით

უფრო იმ პირობებში, რომ არასრულწლოვანმა ზემოთ ჩამოთვლილი ფაქტორების გათვალისწინებით, მოგვიანებით, სასამართლო პროცესზე შესაძლოა ვეღარ გაიხსენოს სავარაუდო დანაშაულთან დაკავშირებული მისთვის ცნობილი ფაქტები.

ზემოხსენებულის მიუხედავად, შემოწმების ფარგლებში დადგინდა, რომ პროკურატურას, მართალია, შემუშავებული ჰქონდა ვიდეო-აუდიომონიტორინგის განხორციელების პროცესში „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 და მე-11 მუხლების მე-2 პუნქტებით გათვალისწინებული წერილობითი დოკუმენტი, თუმცა იგი არ იყო სრული. გამოკითხვის პროცესში ვიდეო-აუდიო მონიტორინგის განხორციელების თაობაზე მონაცემთა სუბიექტ(ებ)ის ინფორმირებასთან დაკავშირებით, შემოწმების ფარგლებში დადგინდა, რომ პროკურატურის სისტემაში მოწყობილი 8 (რვა) გამოსაკითხი ოთახიდან 7 (შვიდ) სივრცეში გამაფრთხილებელი ნიშანი არ იყო განთავსებული და გამოკითხვის პროცესში მონაწილე პირების ინფორმირება ვიდეო-აუდიომონიტორინგის მიმდინარეობის თაობაზე ხდებოდა მხოლოდ ზეპირსიტყვიერად, რაც აისახებოდა გამოკითხვის ოქმში. 1 (ერთი) რაიონული პროკურატურის შემთხვევაში კი განთავსებული იყო გამაფრთხილებელი ნიშანი, რომელიც ხსენებულ ოთახში მყოფ პირს უჩენდა განცდას, რომ ექვემდებარებოდნენ მუდმივ ვიდეო-აუდიო მონიტორინგს. აღსანიშნავია, რომ ორივე შემთხვევაში მონაცემთა სუბიექტების ინფორმირება წინააღმდეგობაშია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან, ვინაიდან გამაფრთხილებელი ნიშნის არარსებობის პირობებში, ვიდეოსათვალთვალო კამერის არსებობა ან ისეთი გამაფრთხილებელი ნიშნის არსებობა, რომლითაც მონაცემთა სუბიექტისთვის არ არის ცხადი ვიდეო-აუდიო მონიტორინგის განხორციელების პერიოდსა და ხანგრძლივობაზე, ოთახში მყოფ პირებს თავისთავად უქმნიდა არასწორ განცდას, თითქოს ისინი ექვემდებარებოდნენ ვიდეო-აუდიომონიტორინგს, რაც, შემოწმების ფარგლებში დადგინდა, რომ არ შეესაბამებოდა რეალობას.

აგრეთვე, ვინაიდან ვიდეო-აუდიომონიტორინგის განხორციელებისთვის პროკურატურა გამოიყენებდა ელექტრონულ სისტემებს, შემოწმდა ხსენებულ სისტემებში დაცული მონაცემების მიმართ მიღებული უსაფრთხოების ზომები. აღნიშნულის შედეგად დადგინდა, რომ სისტემაში ავტორიზაციის, ვიდეო-აუდიო ჩაწერის, ჩანაწერების დათვალიერების, გადმოწერისა და წაშლისთვის, თითოეულ რაიონულ პროკურატურაში შექმნილი იყო თითო-თითო მომხმარებელი. ამ უკანასკნელით კი სარგებლობდა რაიონულ პროკურატურაში წვდომის უფლების მქონე ყველა პირი. გარკვეულ შემთხვევებში მომხმარებლის პაროლის თაობაზე

ინფორმაციის წვდომის უფლების მქონე პირისთვის გაზიარება ხდებოდა დისტანციურ ფორმატში — სატელეფონო კომუნიკაციის გზით. ამასთან, სისტემებს გააჩნდათ მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვის ელექტრონული ჟურნალები (ე.წ. „ლოგირება“), თუმცა ერთ-ერთი რაიონული პროკურატურის შემთხვევაში, არასრულად აღირიცხებოდა მონაცემთა მიმართ შესრულებული მოქმედებები (ე.წ. „ლოგები“), ხოლო 3 (სამი) რაიონული პროკურატურის შემთხვევაში, მართალია სრულად აღირიცხებოდა, თუმცა, ჩანაწერის წაშლის შემდეგ სრულად იშლებოდა ე.წ. „ლოგ“ ჩანაწერებიც. გარდა ამისა, ყველა სისტემას ჰქონდა რეალურ დროსთან ცდომილება.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, ზემოჩამოთვლილი ტექნიკური ხარვეზები წარმოადგენს უსაფრთხოების კომპონენტის დარღვევას, საქართველოს პროკურატურა ცნობილ იქნა სამართალდამრღვევად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 76-ე მუხლის (მონაცემთა უსაფრთხოების დაცვის ვალდებულების შეუსრულებლობა) მეორე პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენაში და მიეცა შესასრულებლად სავალდებულო 6 (ექვსი) დავალება. კერძოდ, პროკურატურას დაევალა არასრულწლოვანთა გამოკითხვის ოთახებში აუდიო-ვიდეომონიტორინგის მიმდინარეობის თაობაზე იმგვარი გამაფრთხილებელი ნიშნის განთავსება, რომლითაც მოხდებოდა მონაცემთა სუბიექტების სრული ინფორმირება; დაევალა კანონის მე-10 და მე-11 მუხლების მე-2 პუნქტებით გათვალისწინებული ერთიანი სრულყოფილი წერილობითი დოკუმენტის შექმნა; არასრულწლოვანთა გამოკითხვის სპეციალიზებულ სივრცეში, ვიდეო-აუდიოჩაწერის გზით, მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლის შესაბამისად აღრიცხვა; ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს არასრულწლოვანთა გამოკითხვის პროცესის ვიდეო-აუდიოჩაწერის განხორციელებისთვის გამოყენებულ ელექტრონულ სისტემებზე ინდივიდუალური მომხმარებლითა და პაროლით შესვლას, ელექტრონულ სისტემებში არსებული თარიღისა და დროის ცდომილების გამოსწორებასა და მონაცემთა მიმართ შესრულებული ყველა მოქმედების აღრიცხვას.

11. ახალი კანონის 28-ე მუხლით გათვალისწინებული ვალდებულების შესრულება

სამსახურმა გეგმური თუ არაგეგმური შემოწმებების ფარგლებში შეისწავლა სხვადასხვა სამართალდამცავი ორგანოს მიერ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლით გათვალისწინებული ვალდებულების შესრულების საკითხი. ახალი საკანონმდებლო მოწესრიგებით არსებითად შეიცვალა პერსონალურ მონაცემთა დამუშავების მომწესრიგებელი ნორმები, მიდგომები და სტანდარტები. კანონმდებელმა, ერთი მხრივ, დააკონკრეტა გარკვეული საკითხები, რომლებიც კანონის ძველი რედაქციის მოქმედების ფარგლებში წარმოშობდა პრაქტიკულ პრობლემებს, ხოლო მეორე მხრივ, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს განესაზღვრათ ახალი მოთხოვნები ან/და გაუქმდა კანონის ძველი რედაქციით გათვალისწინებული გარკვეული სახის ვალდებულებები, რომელთა საპირწონედ დამუშავებისთვის პასუხისმგებელი პირებისთვის გაჩნდა სხვა იმპერატიული ჩანაწერები. ამ უკანასკნელის თვალსაჩინო მაგალითია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლი, რომელიც დამუშავებისთვის პასუხისმგებელ პირს ავალებს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვასა და პერსონალურ მონაცემთა დაცვის სამსახურის შეტყობინებას.

აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს 2011 წლის 28 დეკემბრის კანონის მე-19 მუხლის მიხედვით, მონაცემთა დამმუშავებელს (დამუშავებისთვის პასუხისმგებელი პირი) ეკისრებოდა თითოეულ ფაილურ სისტემასთან დაკავშირებით ფაილური სისტემის კატალოგის წარმოების ვალდებულება, რომელშიც უნდა აღრიცხულიყო შემდეგი შინაარსის ინფორმაცია: ფაილური სისტემის სახელწოდება; მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის დასახელებები და მისამართები, მონაცემთა შენახვის ან/და დამუშავების ადგილი; მონაცემთა დამუშავების სამართლებრივი საფუძველი; მონაცემთა სუბიექტის კატეგორია; მონაცემთა კატეგორია ფაილურ სისტემაში; მონაცემთა დამუშავების მიზანი; მონაცემთა შენახვის ვადა; მონაცემთა სუბიექტის უფლების შეზღუდვის ფაქტი და საფუძვლები; ფაილურ სისტემაში განთავსებულ მონაცემთა მიმღები და მათი კატეგორიები; ინფორმაცია მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის შესახებ და ასეთი გადაცემის სამართლებრივი საფუძველი და მონაცემთა უსაფრთხოების დაცვისათვის დადგენილი პროცედურის ზოგადი აღწერილობა. ხსენებული ინფორმაცია, თავის მხრივ, პროაქტიულად უნდა ასახულიყო პერსონალურ მონაცემთა დაცვის სამსახურის მიერ წარმოებულ ფაილურ სისტემათა კატალოგების რეესტრში, ასევე, პროაქტიულად უნდა წარდგენილიყო პერსონალური მონაცემთა დაცვის საზედამხედველო ორგანოსთვის და უზრუნველყოფილიყო აღნიშნული ინფორმაციის სისტემატური განახლება.

ახალი საკანონმდებლო მოწესრიგებით გაუქმდა ფაილური სისტემის კატალოგის რეესტრი და დამუშავებისთვის პასუხისმგებელ პირებს მოუხსნა ფაილური სისტემის კატალოგში შეტანილი ინფორმაციის რეესტრში აღრიცხვის ვალდებულება, თუმცა კანონის 28-ე მუხლით გათვალისწინებულია მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულება, აღრიცხოს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაცია და სამსახურის მოთხოვნის შემთხვევაში წარუდგინოს მას.

დასახელებული მუხლის პირველი პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი და მისი სპეციალური წარმომადგენელი (ასეთის არსებობის შემთხვევაში) ვალდებულნი არიან წერილობით ან ელექტრონულად უზრუნველყონ მონაცემთა დამუშავებასთან დაკავშირებული შემდეგი ინფორმაციის აღრიცხვა: დამუშავებისთვის პასუხისმგებელი პირის, სპეციალური წარმომადგენლის, პერსონალურ მონაცემთა დაცვის ოფიცრის, თანადამუშავებისთვის პასუხისმგებელი პირების, დამუშავებაზე უფლებამოსილი პირის ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია; მონაცემთა დამუშავების მიზნების შესახებ; მონაცემთა სუბიექტებისა და მონაცემთა კატეგორიების შესახებ; მონაცემთა მიმღების (მათ შორის, სხვა სახელმწიფოში არსებული მონაცემთა მიმღების ან საერთაშორისო ორგანიზაციის) კატეგორიების შესახებ; სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის მონაცემთა გადაცემის, აგრეთვე მონაცემთა დაცვის სათანადო გარანტიების თაობაზე, მათ შორის, პერსონალურ მონაცემთა დაცვის სამსახურის ნებართვის შესახებ (ასეთის არსებობის შემთხვევაში); მონაცემთა შენახვის ვადების შესახებ, ხოლო თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, მათი შენახვის ვადის განსაზღვრის კრიტერიუმების თაობაზე; მონაცემთა უსაფრთხოებისთვის მიღებული ორგანიზაციულ-ტექნიკური ზომების ზოგადი აღწერა; ინციდენტების შესახებ ინფორმაცია (ასეთის არსებობის შემთხვევაში). ამავე მუხლის მე-2 პუნქტის მიხედვით კი, თითოეული დამუშავებაზე უფლებამოსილი პირი და მის მიერ მონაცემთა დამუშავებაში ამ კანონის 36-ე მუხლის მე-7 პუნქტით[6] დადგენილი წესით ჩართული პირი, ვალდებულნი არიან წერილობით ან ელექტრონულად უზრუნველყონ მონაცემთა დამუშავებასთან დაკავშირებული

[6] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 36-ე მუხლის მე-7 პუნქტის თანახმად, თუ საქართველოს კანონმდებლობით სხვა რამ არ არის დადგენილი, დაუშვებელია, დამუშავებაზე უფლებამოსილმა პირმა თავისი უფლება-მოვალეობები სრულად ან ნაწილობრივ გადასცეს სხვა პირს დამუშავებისთვის პასუხისმგებელი პირის წინასწარი წერილობითი თანხმობის გარეშე. დამუშავებისთვის პასუხისმგებელი პირის თანხმობა დამუშავებაზე უფლებამოსილ პირს არ ათავისუფლებს შესაბამისი ვალდებულებებისა და პასუხისმგებლობისგან.

შემდეგი ინფორმაციის აღრიცხვა: დამუშავებაზე უფლებამოსილი პირის, პერსონალურ მონაცემთა დაცვის ოფიცრის, დამუშავებისთვის პასუხისმგებელი პირის, თანადამუშავებისთვის პასუხისმგებელი პირების, სპეციალური წარმომადგენლის ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია; დამუშავებისთვის პასუხისმგებელი პირისთვის ან მისი სახელით განხორციელებული მონაცემთა დამუშავების სახეების შესახებ; ამ მუხლის პირველი პუნქტის „ე“ ქვეპუნქტით გათვალისწინებული ინფორმაცია, თუ იგი მონაწილეობს სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის მონაცემთა გადაცემის პროცესში; მონაცემთა უსაფრთხოების უზრუნველსაყოფად მიღებული ორგანიზაციულ-ტექნიკური ზომების ზოგადი აღწერა; ინციდენტების შესახებ ინფორმაცია (ასეთის არსებობის შემთხვევაში).

2024 წლის 1 მარტამდე მოქმედი კანონის დათქმებთან ძირითადი განსხვავება ის არის, რომ აღრიცხული ინფორმაციის პერსონალურ მონაცემთა დაცვის სამსახურისთვის პროაქტიულად წარდგენა საჭირო არ არის და კანონის 28-ე მუხლის მე-3 პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა, თანადამუშავებისთვის პასუხისმგებელმა პირებმა, დამუშავებაზე უფლებამოსილმა პირმა და სპეციალურმა წარმომადგენელმა ამ მუხლის პირველი და მე-2 პუნქტებით გათვალისწინებული ინფორმაცია შესაბამისი მოთხოვნისთანავე, დაუყოვნებლივ, მაგრამ არაუგვიანეს 3 (სამი) სამუშაო დღისა უნდა მიაწოდონ პერსონალურ მონაცემთა დაცვის სამსახურს. ამდენად, ხსენებული მუხლი მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს ავალდებულებს, რომ შექმნას მასთან არსებული მონაცემთა დამუშავების პროცესების ზოგადი აღწერა, რომელიც უნდა შეიცავდეს თითოეულ მსგავს პროცესთან დაკავშირებულ ინფორმაციას.

მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა მნიშვნელოვანია, როგორც პერსონალურ მონაცემთა დაცვის სამსახურისთვის, რათა საჭიროების შემთხვევაში გამოითხოვოს იგი, ასევე დამუშავებისთვის პასუხისმგებელ პირისთვის, ვინაიდან აღნიშნული დოკუმენტის შემუშავების პროცესში თავად დაფიქრდეს მონაცემთა დამუშავების მიზნებზე, საფუძვლებზე, მიღებული უსაფრთხოების ზომების ადეკვატურობაზე, გამოავლინოს ხარვეზები და თავადვე გამოასწოროს იგი.

ამდენად, აღნიშნული ვალდებულების მნიშვნელობის გათვალისწინებით, 2024 წლის პირველი მარტის შემდეგ, განხორციელებული გეგმური შემოწმებების ფარგლებში, შესწავლილ იქნა სამართალდამცავი ორგანოების მიერ კანონის 28-ე მუხლით გათვალისწინებული აღრიცხვის ფორმის წარმოების საკითხი. კერძოდ,

საანგარიშო პერიოდში დასრულებული 7 (შვიდი) გეგმური შემოწმების შედეგად დადგინდა, რომ არცერთ სამართალდამცავ ორგანოს ჰქონდა შემუშავებული კონკრეტული მონაცემების დამუშავების პროცესებთან მიმართებით აღრიცხვის ფორმა. ზოგიერთი მათგანი მიუთითებდა, რომ უწყებას მიზანშეწონილად არ მიაჩნდა აღნიშნული დოკუმენტის წარმოება, ხოლო ნაწილი აღნიშნავდა, რომ ხსენებული დოკუმენტი იყო შემუშავების პროცესში. ცხადია, ყველა მსგავს შემთხვევაში, ხსენებულ უწყებებს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანებით დაევალათ კანონის 28-ე მუხლით გათვალისწინებული ინფორმაციის წერილობით ან ელექტრონული ფორმით ასახვა და წარმოება.

საყურადღებოა ერთ-ერთი გეგმური შემოწმება, რომლის ფარგლებშიც დადგინდა, რომ უწყებაში არ იყო შექმნილი რაიმე სახის ერთიანი დოკუმენტი (წერილობითი ან ელექტრონული ფორმით), რომელშიც ასახული იქნებოდა უწყების მიერ კონკრეტულ მონაცემთა დამუშავების პროცესებთან დაკავშირებული ინფორმაცია, რაც განიმარტა, რომ ვინაიდან აღნიშნული პროცესი ისედაც ელექტრონული ფორმით მიმდინარეობს (ელექტრონულ სისტემაში აისახებოდა ნებისმიერი ინფორმაცია/დოკუმენტაცია), ამიტომ უწყებას ცალკე ამ ინფორმაციის აღრიცხვის საჭიროება არ ჰქონდა. აქვე, აღსანიშნავია, რომ უწყების მიერ მითითებული ელექტრონული სისტემის დათვალიერების შედეგად მოპოვებული მტკიცებულებების მიხედვით, ხსენებული სისტემა არ შეიცავდა ყველა იმ მონაცემს, რომლის აღრიცხვის ვალდებულებაც კანონის 28-ე მუხლის შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს ეკისრებათ.

პერსონალურ მონაცემთა დაცვის სამსახურმა არ გაიზიარა უწყების მითითება, 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 (ავტომატური, ნახევრად ავტომატური და არაავტომატური საშუალებებით) რომელიმე სახეს. 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.

III თავი. კონსულტაციები და საგანმანათლებლო აქტივობები

1. საკონსულტაციო პლატფორმა

1.1. წერილობითი კონსულტაციები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 53-ე მუხლის პირველი პუნქტის თანახმად, პერსონალურ მონაცემთა დაცვის სამსახური ვალდებულია, შესაბამისი თხოვნის არსებობის შემთხვევაში, კონსულტაცია გაუწიოს სახელმწიფო ხელისუფლების ორგანოებს, მუნიციპალიტეტის ორგანოებს, სხვა საჯარო დაწესებულებებს, კერძო სამართლის იურიდიულ პირებსა და ფიზიკურ პირებს მონაცემთა დამუშავებასა და დაცვასთან დაკავშირებულ ნებისმიერ საკითხზე. აღნიშნული მუხლის საფუძველზე, პერსონალურ მონაცემთა დაცვის სამსახურმა, 2024 წლის საანგარიშო პერიოდში, გასცა ჯამში 16 462 (თექვსმეტი ათას ოთხას სამოცდაორი) კონსულტაცია, მათ შორის, ხუთასამდე წერილობითი ფორმით, რომელთა უმეტესობა პერსონალურ მონაცემთა დაცვის ოფიცერს, პირდაპირ მარკეტინგსა და პერსონალურ მონაცემთა დაცვის სხვადასხვა ტიპის პოლიტიკის დოკუმენტებს ეხებოდა.

საკონსულტაციო შეკითხვების ტენდენცია იხრება პერსონალურ მონაცემთა დაცვის ოფიცრის თანამდებობის არსებული კადრისთვის შეთავსებისა თუ სრულიად ახალი პირის ამ პოზიციაზე განსაზღვრის საკითხების გარშემო. ასევე, საკონსულტაციო მომართვაში დაფიქსირებული შეკითხვათა უმრავლესობა მიემართება ოფიცრის კომპეტენციის დადგენისა და ინტერესთა კონფლიქტის აღმოფხვრის საკითხებს. რაც შეეხება პირდაპირი მარკეტინგის შესახებ დასმულ შეკითხვებს, მათი უმეტესობა შეეხება სამსახურის მხრიდან კონკრეტული შემთხვევების შეფასებას, კერძოდ, ექცევა თუ არა ესა თუ ის ქმედება კანონით განსაზღვრული პირდაპირი მარკეტინგის ცნებაში და წარმოეშობათ თუ არა მონაცემთა დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირებს აღნიშნული ნორმით გათვალისწინებული ვალდებულებები.

მიმართვიანობის მაღალი მაჩვენებელია პერსონალურ მონაცემთა დაცვის ისეთი ტიპის პოლიტიკის დოკუმენტების სამსახურისთვის გამოგზავნასა და მათი შეფასების მოთხოვნის მიმართ, როგორიცაა, მაგალითად, ვიდეო/აუდიომონიტორინგის განხორციელების წესი, ბიომეტრიულ მონაცემთა დამუშავების წესები, ორგანიზაციათა შიდა უწყებრივი პოლიტიკის დოკუმენტები, მონაცემთა დაცვაზე ზეგავლენის შეფასების, ინფორმაციის

აღრიცხვისა თუ მონაცემთა სუბიექტისგან თანხმობის მოპოვების ფორმები, აგრეთვე, სხვა, ზოგადი ხასიათის შიდაორგანიზაციული პოლიტიკის დოკუმენტები.

აღსანიშნავია, რომ წერილობითი საკონსულტაციო ხასიათის მომართვიანობის მაჩვენებელი „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის ამოქმედებამდე, 2024 წლის პირველ მარტამდე გაიზარდა. კერძოდ, 2024 წლის იანვრიდან სამსახური აქტიურად იღებდა ახალი საკანონმდებლო მოწესრიგებით გათვალისწინებული ამა თუ იმ დებულებების განმარტებასთან დაკავშირებულ შეკითხვებს. თუმცა კანონის ნაწილობრივ ძალაში შესვლის შემდგომ — 2024 წლის პირველი ივნისის მდგომარეობით, ამგვარი საკონსულტაციო წერილების რაოდენობა მნიშვნელოვნად გაიზარდა. აღნიშნული ტენდენცია გრძელდება დღემდე, მიუხედავად კანონის სრული ძალით ამოქმედების ფაქტისა.

მოცემული მდგომარეობით, საკონსულტაციო რეჟიმში დასმული შეკითხვების შინაარსი ცხადყოფს, რომ პერსონალურ მონაცემთა დამუშავების პროცესში გამოწვევად რჩება პერსონალურ მონაცემთა დაცვის ოფიცრად დასანიშნი პირის კომპეტენციის შეფასების საკითხები, ასეთი პოზიციის ორგანიზაციაში განსაზღვრის ვალდებულების დადგენა და პერსონალურ მონაცემთა დაცვის ოფიცრის საქმიანობის ჭრილში ინტერესთა კონფლიქტის არსებობის შეფასება. ხსენებულ საკითხებთან მიმართებით, არსებულ სირთულეთა დაძლევისა და მონაცემთა დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირებისა თუ თავად მონაცემთა დაცვის ოფიცრების დახმარების მიზნით, სამსახურმა გამოსცა და საჯაროდ ხელმისაწვდომი ფორმით განათავსა არაერთი გზამკვლევი და სახელმძღვანელო რეკომენდაცია, გამართა საინფორმაციო ხასიათის შეხვედრები და ჩაატარა საგანმანათლებლო შინაარსის ტრენინგები. საგულისხმოა, რომ მონაცემთა დამუშავების საკითხებთან დაკავშირებულ პრობლემურ საკითხებზე სამსახურის მხრიდან მსგავსი ღონისძიებების გამართვის ტენდენცია განგრძობად ხასიათს ატარებს.

1.2. ზეპირი კონსულტაციები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს მოქმედი კანონის 49-ე მუხლის თანახმად, სამსახურის ერთ-ერთ ძირითად მიმართულებას წარმოადგენს მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე კონსულტაციების გაწევა და საზოგადოების ცნობიერების ამაღლება მათი ინფორმირებით.

აღნიშნული ფუნქციების ეფექტიანად წარმართვის მიზნით, 2024 წლის პირველი იანვრიდან, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის აპარატს განესაზღვრა კომპეტენციის ფარგლებში პერსონალური მონაცემების დამუშავებასთან დაკავშირებული ზეპირი კონსულტაციების გაწევის ფუნქცია, როგორც სატელეფონო, ასევე ადგილზე ვიზიტის ფარგლებში, საჯარო თუ კერძო სექტორის წარმომადგენლებისთვისა და ფიზიკური პირებისთვის.

საგულისხმოა, რომ საანგარიშო პერიოდში სამსახურმა ზეპირი კომუნიკაციის ფორმატში გასცა 14 381 (თოთხმეტი ათას სამას ოთხმოცდაერთი) კანონით გათვალისწინებულ ისეთ სიახლეებზე, როგორიცაა: პერსონალურ მონაცემთა დაცვის ოფიცერი (1 421 (ათას ოთხას ოცდაერთი)), პირდაპირი მარკეტინგი (874 (რვაას სამოცდათოთხმეტი)), ვიდეომონიტორინგი (711 (შვიდას თერთმეტი)), სამსახურის უფროსის ნორმატიული აქტები (579 (ხუთას სამოცდაცხრამეტი)). საგულისხმოა, რომ სამსახურისთვის მომართვის წესი (1 010 (ათას ათი)) განემარტა ათასამდე ფიზიკური პირს, რაც სუბიექტების უფლებებისა და სამსახურის კომპეტენციის თაობაზე ინფორმირებულობის გაზრდაზე მიგვანიშნებს. აღსანიშნავია, რომ კონსულტაციების აღნიშნული ფორმატი სამსახურს ეხმარება მნიშვნელოვანი საკითხებისა და ზოგიერთ შემთხვევაში არსებული სირთულეების იდენტიფიცირებაში, ასევე, შესაბამისი სახელმძღვანელო რეკომენდაციების მომზადებაში.

მიმდინარე წლის განმავლობაში, დაიდენტიფიცირდა ხშირად დასმული კითხვები და გამოქვეყნდა, როგორც სამსახურის ვებგვერდის, ასევე სოციალური ქსელი მეშვეობით. აგრეთვე, მომზადდა ისეთი დოკუმენტები, როგორიცაა: „რეალურ დროში განხორციელებული ვიდეომონიტორინგი საბავშვო ბაღებში“, „პერსონალური მონაცემების თვითნებური გასაჯაროების მოსალოდნელი რისკები და რეკომენდაციები“, „ფოტოგრაფია და პერსონალურ მონაცემთა დაცვა“, საგანმანათლებლო დაწესებულებებისთვის ბროშურები და საინფორმაციო კამპანია - „სასწავლო წლის დაწყებასთან დაკავშირებული ფოტოების გაზიარებისას გასათვალისწინებელი რჩევები“. სამსახურის ვებ-გვერდს დაემატა “#DataTech” - ანალიტიკის რუბრიკა, რაც საზოგადოებაში ტექნოლოგიურ სფეროში მონაცემთა დაცვაზე ინფორმირებულობის გაზრდას ემსახურება.

1.3. საინფორმაციო ლექცია-შეხვედრები

პერსონალურ მონაცემთა დაცვის ახალი კანონის მიღების შემდგომ, საზოგადოების ცნობიერების ამაღლებისთვის, შესაბამისი სარეკომენდაციო

სახელმძღვანელოების გაცნობის მიზნით, სამსახური აქტიურად მართავს საინფორმაციო ხასიათის ლექცია-ტრენინგებს. აღსანიშნავია, რომ ამგვარი საინფორმაციო ხასიათის ლექცია-ტრენინგების გამართვა სამსახურმა 2023 წლის შემოდგომიდან დაიწყო, რომელსაც თავდაპირველ ეტაპზე სექტორული ხასიათი ჰქონდა. პირველი მასშტაბური შეხვედრა ახალ კანონთან დაკავშირებულ თემებზე 2023 წლის 24 ოქტომბერს გაიმართა და მას საქართველოს პარლამენტის, საქართველოს მთავრობის, ცალკეული საჯარო დაწესებულებებისა და სამეცნიერო სფეროს წარმომადგენლები დაესწრნენ. ამის შემდეგ აქტიურად გაგრძელდა ახალი კანონის ირგვლილ საინფორმაციო-სადისკუსიო შეხვედრები სახელწოდებით „საუბრები კანონზე“, რომლებშიც აქტიურად მონაწილეობდნენ საჯარო და კერძო სექტორის წარმომადგენლები. აღსანიშნავია, რომ 2023 წელს, თბილისსა და საქართველოს სხვა რეგიონებში (მათ შორის, აჭარის ავტონომიურ რესპუბლიკაში) სამსახურის ინიციატივით გაიმართა 20 (ოცი) შეხვედრა ჩატარდა და 1565 (ათას ხუთას სამოცდახუთი) დაინტერესებული პირი დაესწრო. მათ შორის. სამართალდამცავი ორგანოების წარმომადგენლები, საქართველოს მთავრობის ადმინისტრაცია, სხვადასხვა სამინისტროს და სამინისტროთა სისტემაში/დაქვემდებარებაში არსებული საჯარო სამართლის პირებისა და საქვეუწყებო დაწესებულებების წარმომადგენლები, თბილისის მერიის, თბილისის რაიონული გამგეობებისა და მერიის სისტემაში/დაქვემდებარებაში არსებული საჯარო სამართლის იურიდიული პირების/არასამეწარმეო იურიდიული პირებისა და სხვა საჯარო უფლებამოსილების განმახორციელებელი ორგანიზაციების წარმომადგენლები. განსაკუთრებული ყურადღება დაეთმო ასევე საფინანსო, საგანმანათლებლო, ჯანდაცვის სექტორის, მედიისა და დამსაქმებელთა და ბიზნეს ასოციაციების წარმომადგენლებთან შეხვედრებს.

2023-2024 წლებში, ახალი კანონის შესახებ საინფორმაციო შეხვედრები აქტიურად ტარდებოდა რეგიონებშიც და მოიცვა: აჭარის ავტონომიური რესპუბლიკა, კახეთის რეგიონის თვითმმართველობების წარმომადგენლები, იმერეთის რეგიონის თვითმმართველობების წარმომადგენლები, სამეგრელო-ზემო სვანეთის თვითმმართველობების წარმომადგენლები, სამცხე-ჯავახეთის რეგიონი, შიდა ქართლის და ქვემო ქართლის რეგიონები, მცხეთა-მთიანეთის რეგიონი, რაჭა-ლეჩხუმისა და ქვემო სვანეთის რეგიონი. რეგიონულ შეხვედრებს ჯამში 990 (ცხრაას ოთხმოცდაათი) პირი დაესწრო.

აღსანიშნავია, რომ შეხვედრები აქტიურად მიმდინარეობდა საგანმანათლებლო სექტორის წარმომადგენლებისთვის. სექტორული შეხვედრის გარდა, რომელშიც საქართველოს განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტრო და მის დაქვემდებარებაში არსებული საჯარო სამართლის იურიდიული პირები და

არასამეწარმეო იურიდიული პირები მონაწილეობდნენ, სხვადასხვა დროს აქტიურად ჩატარდა შეხვედრები რეგიონებისა და თბილისის საგანმანათლებლო რესურს ცენტრების წარმომადგენლებთან და ასევე სხვადასხვა საგანმანათლებლო დაწესებულების წარმომადგენლებთან. შეხვედრებს სულ 1460 (ათას ოთხას სამოცი) პირი დაესწრო.

საანგარიშო პერიოდში აქტიურად მიმდინარეობდა ლექციები-ტრენინგები როგორც ონლაინ, ასევე ფიზიკურ ფორმატში, პერსონალურ მონაცემთა დაცვის ოფიცრებთან და აღნიშნული საკითხით დაინტერესებულ პირებთან. შეხვედრებში მონაწილეობა მიიღო 690 (ექვსას ოთხმოცდაათმა) დაინტერესებულმა პირმა.

ზემოაღნიშნული შეხვედრების პარალელურად, პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივით, 2023 წლის 24 ნოემბრიდან ყოველ პარასკევს საკონსულტაციო შეხვედრები ტარდება დაინტერესებულ პირებთან. საგულისხმოა, რომ სპეციალური პროგრამის საშუალებით რეგისტრირებულ მოქალაქეებს შეუძლიათ ახალ კანონთან დაკავშირებულ საკითხებზე კონსულტაცია უშუალოდ პერსონალურ მონაცემთა დაცვის სამსახურის წარმომადგენლებთან გაიარონ. „პარასკევის კონსულტაციები“ მიმდინარეობს სატელეფონო და წერილობითი კონსულტაციის პარალელურად. აღნიშნული სერვისით 260 (ორას სამოცმა) პირმა ისარგებლა.

საერთო ჯამში, 2023 წლის პირველი სექტემბრიდან 2024 წლის 20 ნოემბრამდე, სამსახურმა 145 (ას ორმოცდახუთი) საინფორმაციო ლექცია-ტრენინგი როგორც პირისპირ, ასევე ონლაინ და ჰიბრიდულ ფორმატში, ჩაატარა, რომელშიც 8304 (რვა ათას სამასოთხმა) პირმა მიიღო მონაწილეობა. ხოლო 2024 წლის პირველი იანვრიდან 31 დეკემბრის ჩათვლით, სამსახურმა გამართა 108 (ას რვა) შეხვედრა 6522 (ექვსი ათას ხუთას ოცდაორ) დამსწრე პირთან, რომელთა ნაწილი წარმოადგენდა როგორც მონაცემთა სუბიექტს, მონაცემთა დამუშავებისთვის პასუხისმგებელ და დამუშავებაზე უფლებამოსილ პირებს.

აღსანიშნავია, სამსახურის მიერ საზოგადოების ცნობიერების ამაღლების მიზნით განხორციელებული აქტივობები. 2023 წლის 9 სექტემბერს, პერსონალურ მონაცემთა დაცვის სამსახურმა უმაღლესი საკანონმდებლო ორგანოს წარმომადგენლებთან, მთავრობის წევრებთან, საჯარო და კერძო ორგანიზაციების, ასევე დიპლომატიური, აკადემიური და არასამთავრობო სექტორის წარმომადგენლებთან ახალი კანონის იმპლემენტაციის საკითხებზე შეხვედრა გამართა. შეხვედრაზე წარმოდგენილი იყო სამოქმედო გეგმა, რომლის განხორციელებასაც სამსახური აქტიურად შეუდგა.

საანგარიშო პერიოდში საზოგადოების ცნობიერების ამაღლების მიზნით, სამსახურის მიერ გამოქვეყნდა 20 (ოცი) პოდკასტი, რომლის ფარგლებშიც სამსახურის წარმომადგენლები დეტალურად განიხილავენ ყველა იმ მნიშვნელოვან ცვლილებას, რომელსაც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ითვალისწინებს. აღსანიშნავია, რომ მათგან 10 (ათი) პოდკასტი შშმ პირთათვის ხელმისაწვდომი ფორმით (ე.წ. სურდო თარჯიმანი) არის წარმოდგენილი. საგულსიხმოა, რომ აღნიშნული პოდკასტები სოციალური ქსელების სამ პლატფორმაზე (“Facebook”, “YouTube”, “Spotify”) განთავსდა და ჯამში ოცივე მათგანის მნახველთა რაოდენობამ 600 000-მდე (ექვსას ათასამდე) პირი შეადგინა (იხ. დანართი 1).

ახალი კანონით გათვალისწინებულ ცვლილებებთან დაკავშირებით სამსახურმა გამოაქვეყნდა გრაფიკული ვიდეორგოლი, ხოლო მისი მოკლე ვერსია უფასო სოციალური რეკლამის სახით საზოგადოებრივ მაუწყებელსა და აჭარის ტელევიზიის და რადიო ეთერებში განთავსდა. ვიდეოს ვრცელი ვერსია გამოქვეყნდა სამსახურის ოფიციალურ ვებ გვერდსა და სოციალურ ქსელებში. მნახველთა რაოდენობამ 130 000 (ას ოცდაათი ათასი) შეადგინა (იხ. დანართი 2).

საანგარიშო პერიოდში სამსახურის წარმომადგენლების მონაწილეობით დაიგეგმა 30 (ოცდაათი) ტელე და რადიო ეთერი, რომლის ფარგლებშიც განხილულ იქნა კანონით გათვალისწინებული მნიშვნელოვანი ცვლილებები. აღსანიშნავია, რომ პირდაპირ ეთერებში მონაწილეობდა პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი (2023 წლის 11 სექტემბერს, ტელეკომპანია „იმედი“; 2023 წლის 31 ოქტომბერს, ტელეკომპანია „ევრონიუსი“), გარდა ამისა, გამოქვეყნდა სამსახურის უფროსის ინტერვიუ საინფორმაციო სააგენტოში (2024 წლის პირველ მარტს, „ინტერპრესნიუსი“).

საგულისხმოა, რომ სამსახურის მიერ გამოქვეყნდა თემატური ქარდები ახალი კანონით გათვალისწინებულ ცვლილებებთან დაკავშირებით სოციალური ქსელებისთვის. აღსანიშნავია, რომ მნახველთა წვდომამ გამოქვეყნებულ მასალაზე 90 000-მდე (ოთხმოცდაათი ათასამდე) შეადგინა (იხ. დანართი 3). ასევე, მომზადდა ხშირად დასმული კითხვების დოკუმენტი ქართულ, სომხურ და აზერბაიჯანულ ენებზე.

საანგარიშო პერიოდში სამსახურის მიერ მომზადდა და გამოქვეყნდა ახალ კანონთან დაკავშირებული 25 (ოცდახუთი) რეკომენდაცია და გაიდლაინი, მათ შორისაა:

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 052020 თანხმობის შესახებ;
6. სახელმძღვანელო რეკომენდაცია 2/2019 GDPR-ის 6(1)(b) 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).

აგრეთვე, აღსანიშნავია, რომ სამსახურმა საჯარო და კერძო სექტორის წარმომადგენელ პერსონალურ მონაცემთა დაცვის ოფიცრებს ყოველ ხუთშაბათს სამსახურის ოფისში კონსულტაციების ახალი ფორმატი შესთავაზა, რომლის ფარგლებშიც მათ პერსონალურ მონაცემთა დაცვის სამსახურის ოფიცერთან კონსულტაციის გავლის შესაძლებლობა ეძლევათ.

ახალი კანონით გათვალისწინებულ ცვლილებებთან დაკავშირებით, ნებისმიერ დაინტერესებულ პირს, მათ შორის, საჯარო და კერძო უწყების წარმომადგენლებს, ყოველ პარასკევს სამსახურის ოფისში, ინდივიდუალური კონსულტაციების ფორმატში, სამსახურის სხვადასხვა დეპარტამენტის წარმომადგენლებთან კონსულტაციის გავლის შესაძლებლობა აქვთ.

დანართი №1

პოდკასტი / ნახვების რაოდენობა
(Facebook, Youtube, Spotify)

20 - 44k +

19 – 55k +

18 – 58k +

17 - 59k +

16 -47 k +

15-46 k +

14-49 k +

13- 49 k +

12- 31 k +

11 -58 k +

10 -11 k +

9- 7,2 k +

8- 8,1 k +

7- 4,4 k +

6-10 k +

5 - 10 k +

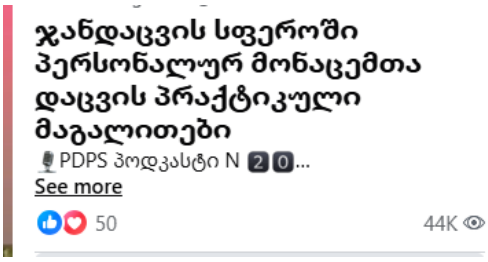
4- 1,2 k +

3 -13 k +

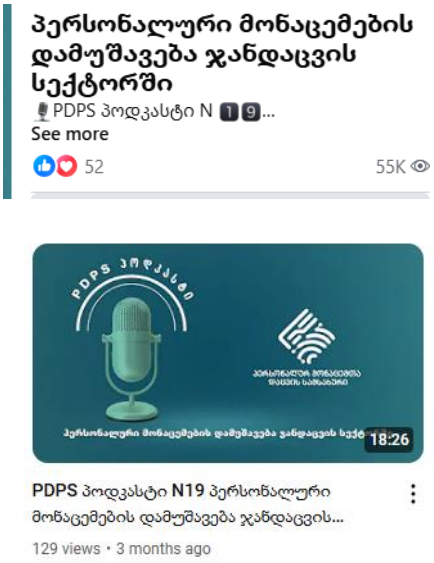
2 - 15 k +

1 -15 k +

- პოდკასტი 20

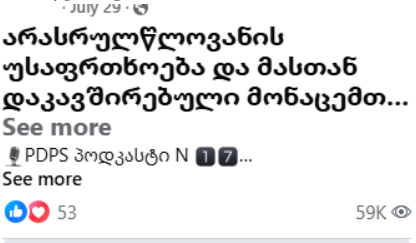


- პოდკასტი 19

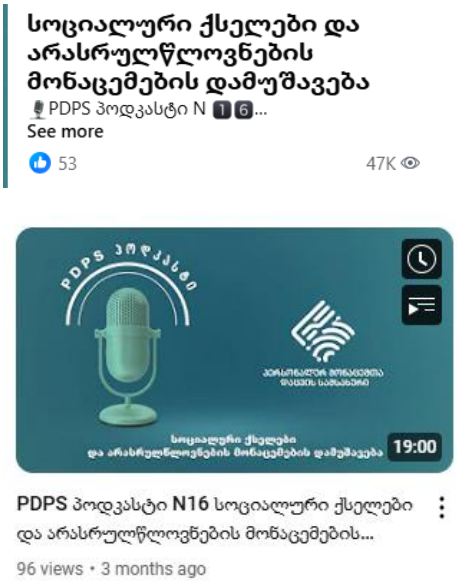


- პოდკასტი 18

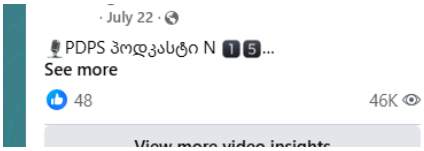
- პოდკასტი 17



- პოდკასტი 16



- პოდკასტი 15



PDPS პოდკასტი N15 Privacy by design and by default

142 views • 4 months ago

- პოდკასტი 14

· July 19 ·

მონაცემთა დაცვაზე ზეგავლენის შეფასება

PDPS პოდკასტი N 14...

See more

52 1 49K

PDPS პოდკასტი N14 მონაცემთა დაცვაზე ზეგავლენის შეფასება

195 views • 4 months ago

- პოდკასტი 13

· July 17 ·

პერსონალურ მონაცემთა დაცვის ოფიცრის უფლებები და პასუხისმგებლობა,

PDPS პოდკასტი N 13...

See more

71 49K

PDPS პოდკასტი N13 პერსონალურ მონაცემთა დაცვის ოფიცრის უფლებები ...

257 views • 4 months ago

- პოდკასტი 12

· July 15 ·

პერსონალურ მონაცემთა დაცვის ოფიცრის საქმიანობის ძირითადი პრინციპები

PDPS პოდკასტი N 12...

See more

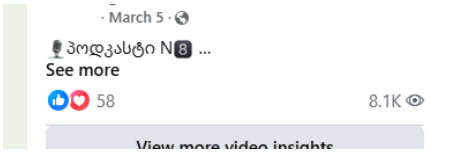
103 1 31K

PDPS პოდკასტი N12 პერსონალურ მონაცემთა დაცვის ოფიცრის საქმიანობის...

236 views • 4 months ago

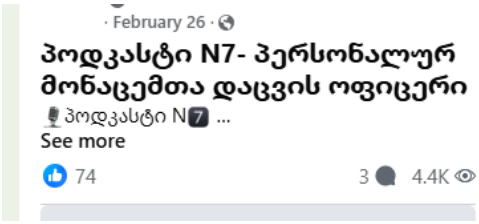
- პოდკასტი 11

- პოდკასტი 8



- პოდკასტი 10

- პოდკასტი 7



- პოდკასტი 9

PDPS პოდკასტი N7 - პერსონალურ მონაცემთა დაცვის ოფიცერი

977 views • 8 months ago

- პოდკასტი 6

· February 23 ·

პოდკასტი N6 - მონაცმთა უსაფრთხოება

🎙 ახალი კანონით გათვალისწინებულ სიახლეებთან დაკავშირებით გიზიარებთ მომდევნო პოდკასტს ...

See more

61 1 10K

PDPS პოდკასტი N 6 - მონაცემთა დამუშავება

532 views • 8 months ago

- პოდკასტი 5

· February 20 ·

პოდკასტი N5 -ვიდეომონიტორინგის და აუდიომონიტორინგის განხორციელების წესები

🎙📹ვიდეომონიტორინგის და აუდიომონიტორინგის განხორციელების წესებთან დაკავშირებით გიზიარებთ პოდკასტების...

See more

83 1 10K

PDPS პოდკასტი N5 - ვიდეომონიტორინგის და აუდიომონიტორინგის განხორციელებ...

619 views • 9 months ago

- პოდკასტი 4

· February 16 ·

პოდკასტი 4

🎙 პოდკასტების სერიის ფარგლებში 🔸 თემაზე: დამუშავებისთვის პასუხისმგებელი პირი, თანადამუშავებისთვის პას...

See more

46 1.2K

PDPS პოდკასტი N4 - დამუშავებისთვის პასუხისმგებელი პირი,...

606 views • 9 months ago

- პოდკასტი 3

· February 14 ·

🎙ახალი კანონით გათვალისწინებულ სიახლეებთან დაკავშირებით გიზიარებთ მომდევნო პოდკასტს ...

See more

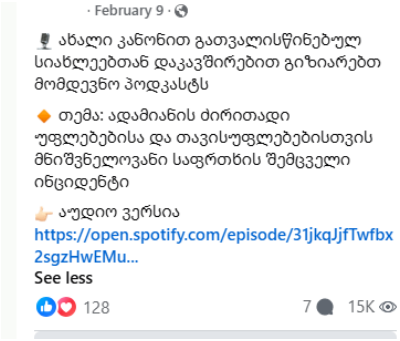
84 13K

View more video insights

PDPA პოდკასტი N3- მონაცემთა სუბიექტის უფლებები

629 views • 9 months ago

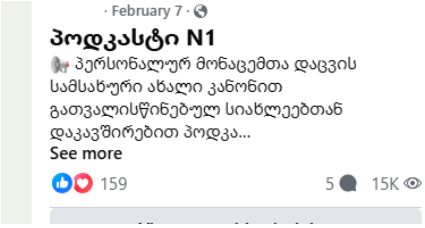
- პოდკასტი 2



PDPS პოდკასტი N2 - ინციდენტის შეტყობინება

658 views • 9 months ago

- პოდკასტი 1



PDPS პოდკასტი N1 - კანონის მოქმედების სფერო, მონაცემთა დამუშავების ახალი...

1.4K views • 9 months ago

დანართი №2

გრაფიკული ვიდეორგოლის ნახვების რაოდენობა facebook/ youtube

Facebook

youtube

დანართი №3

ახალ კანონთან დაკავშირებულ საინფორმაციო ბარათებზე წვდომა ფეისბუქში

2. პერსონალურ მონაცემთა დაცვის ოფიცრებთან განხორციელებული შეხვედრები

2.1. პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული ვალდებულება

პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული ვალდებულება ერთ-ერთია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს 2023 წლის 14 ივნისის კანონით გათვალისწინებულ იმ მთავარ სიახლეთაგან, რომელიც ქართული კანონმდებლობის ევროკავშირში მოქმედ სტანდარტთან მნიშვნელოვნად დაახლოებას განაპირობებს. აღსანიშნავია, რომ დაწესებულებების ორგანიზაციულ სტრუქტურაში პერსონალურ მონაცემთა დაცვის ოფიცრის გათვალისწინება მონაცემთა დამუშავების პროცესის კანონიერების ხელშემწყობ, საკვანძო ღონისძიებად განიხილება, როგორც ევროკავშირში, ისე მონაცემთა დაცვის მაღალი სტანდარტის მქონე სხვა არაერთ სახელმწიფოში მოქმედი სამართლებრივი რეგულირებით, რამდენადაც პერსონალურ მონაცემთა დაცვის ოფიცრის ეფექტიანი საქმიანობა მნიშვნელოვნად ამცირებს დაწესებულებაში მონაცემების კანონშეუსაბამოდ დამუშავების რისკებს.

საქმიანობის ფარგლებში წარმართული მონაცემთა დამუშავების პროცესის მასშტაბის, სპეციფიკის და მის შედეგად ადამიანის უფლებებისადმი მომდინარე შესაძლო საფრთხეების გათვალისწინებით, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულება დაეკისრათ საჯარო დაწესებულებებს, სადაზღვევო ორგანიზაციებს, კომერციულ ბანკებს, მიკროსაფინანსო ორგანიზაციებს, საკრედიტო ბიუროებს, ელექტრონული კომუნიკაციის კომპანიებს, ავიაკომპანიებს, აეროპორტებს, სამედიცინო დაწესებულებებს, აგრეთვე იმ პირებს, რომლებიც ამუშავებენ დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან/და ახორციელებენ მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს.

ამასთან, აღნიშნული კანონით გათვალისწინებული უფლებამოსილების შესაბამისად, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსმა გამოსცა 2024 წლის 28 თებერვლის №22 ბრძანება იმ პირთა წრის განსაზღვრის შესახებ, რომლებსაც არ აქვთ ვალდებულება, დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი.

კანონის თანახმად, პერსონალურ მონაცემთა დაცვის ოფიცრის ძირითადი მოვალეობაა, სიღრმისეულად შეისწავლოს დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი ორგანიზაციის მიერ წარმართული მონაცემთა დამუშავების პროცესი, დაეხმაროს დაწესებულებას პერსონალურ მონაცემთა დაცვასთან დაკავშირებით კანონმდებლობით გათვალისწინებული ვალდებულებების ჯეროვნად აღქმაში და გაუწიოს ქმედითი კონსულტაცია აღნიშნულ ვალდებულებებთან თავსებადობის უზრუნველსაყოფად. ამასთან, პერსონალურ მონაცემთა დაცვის ოფიცრის საქმიანობის დამოუკიდებლობის, მიუკერძოებლობის და ეფექტიანობის უზრუნველსაყოფად, კანონმა განსაზღვრა პირისთვის პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციების დაკისრებისას სავალდებულოდ გასათვალისწინებელი შემდეგი წესები:

- პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციების ისეთი პირისთვის დაკისრება, რომელიც დაწესებულებაში იმავდროულად სხვა ფუნქციებს ასრულებს მხოლოდ იმ შემთხვევაშია დასაშვები, თუ არ წარმოიქმნება ინტერესთა კონფლიქტი;
- პირი, რომელსაც პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციები დაეკისრება, ანგარიშვალდებული უნდა იყოს დაწესებულების მაქსიმალურად მაღალი დონის მმართველობითი სტრუქტურის წინაშე;
- პირს, რომელსაც პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციები დაეკისრება, უნდა ჰქონდეს სათანადო ცოდნა მონაცემთა დაცვის სფეროში;
- დაწესებულებებს იმ შემთხვევაში შეუძლიათ დანიშნონ საერთო პერსონალურ მონაცემთა დაცვის ოფიცერი, თუ თითოეულ დაწესებულებასთან მიმართებით უზრუნველყოფილი იქნება პერსონალურ მონაცემთა დაცვის ოფიცრის მიერ მისი ფუნქციების სრულფასოვანი შესრულება.

კანონის თანახმად, დაწესებულებები ვალდებულნი არიან, პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნიდან ან მისი შეცვლიდან 10 (ათო) სამუშაო დღის ვადაში ოფიცრის ვინაობა და საკონტაქტო ინფორმაცია აცნობონ პერსონალურ მონაცემთა დაცვის სამსახურს და პროაქტიულად გამოაქვეყნონ ვებგვერდზე ან სხვა ხელმისაწვდომი საშუალებით. პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული აღნიშნული ვალდებულება ძალაში მიმდინარე წლის პირველი ივნისიდან შევიდა.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 82-ე მუხლის თანახმად, აღნიშნული ვალდებულების შეუსრულებლობა ადმინისტრაციულ სამართალდარღვევას წარმოადგენს და გამოიწვევს სამართალდამრღვევის გაფრთხილებას. ხსენებული ვალდებულების შეუსრულებლობა პერსონალურ

მონაცემთა დაცვის სამსახურის უფროსის მიერ ადმინისტრაციული სახდელის დადებიდან ერთი წლის განმავლობაში კი გამოიწვევს სამართალდამრღვევის დაჯარიმებას 3000 (სამი ათასი) ლარის ოდენობით.

აღსანიშნავია, რომ კანონის თანახმად, სამართალდამრღვევად ცნობის საფუძველია დაწესებულების მიერ პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულების სრული შეუსრულებლობა. ოფიცრის დანიშვნისას ზემოთ მითითებული წესების დარღვევა კი წარმოადგენს პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შესასრულებლად სავალდებულო დავალებების გაცემის საფუძველს ნაკლოვანი შესრულების აღმოფხვრის მიზნით.

2.2. ცნობიერების ამაღლება

კანონით გათვალისწინებული ახალი ვალდებულებების ეფექტიანი იმპლემენტაციისთვის არსებითია, რომ პასუხისმგებელ სუბიექტებს სრულყოფილად ესმოდეთ ხსენებული ვალდებულებების არსი. აღნიშნულიდან გამომდინარე, პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული ვალდებულების ჯეროვნად აღსრულების ხელშეწყობის მიზნით, პერსონალურ მონაცემთა დაცვის სამსახურმა განსაკუთრებული ყურადღება დაუთმო ხსენებული ვალდებულების შესახებ დაინტერესებული პირების სრულფასოვან ინფორმირებას.

აღნიშნული ვალდებულების ფარგლების და მისი შესრულების წესების შესახებ ცნობიერების ამაღლების მიზნით, შესაბამისი ღონისძიებების გატარება, მათ შორის, საინფორმაციო შეხვედრების წარმოება პერსონალურ მონაცემთა დაცვის სამსახურმა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს 2023 წლის 14 ივნისის კანონის მიღების პერიოდიდანვე დაიწყო და პროცესი მოცემული დროისთვისაც აქტიურად გრძელდება.

3. ადგილობრივი და რეგიონული შეხვედრები

3.1. გარე საინფორმაციო შეხვედრები

საანგარიშო პერიოდის განმავლობაში, პერსონალურ მონაცემთა დაცვის სამსახურმა კერძო და საჯარო სექტორის წარმომადგენლებთან თბილისსა და საქართველოს რეგიონებში 67 (სამოცდაშვიდი) სხვადასხვა ფორმატის გასვლითი

საინფორმაციო შეხვედრა გამართა, რომელთა ფარგლებშიც 3896 (სამი ათას რვაას ოთხმოცდათექვსემეტ) დაინტერესებულ პირს მიეწოდა დეტალური ინფორმაცია კანონით გათვალისწინებული სიახლეების, მათ შორის პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულების შესახებ.

3.2. შიდა საკონსულტაციო შეხვედრები

ახალი კანონის მიღების პერიოდიდან, პერსონალურ მონაცემთა დაცვის სამსახური დაინტერესებული პირებისგან უწყვეტ რეჟიმში იღებს კონკრეტულ საკონსულტაციო შეკითხვებს, როგორც წერილობით, ისე სატელეფონო გზით, რის საპასუხოდაც სამსახურმა გასცა ასობით ინდივიდუალური კონსულტაცია, მათ შორის პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულებასთან დაკავშირებით.

გარდა ამისა, სამსახურმა შეიმუშავა შეხვედრების ფორმატი, რომლის ფარგლებშიც, ნებისმიერი დაწესებულების პერსონალურ მონაცემთა დაცვის ოფიცრებს და სხვა დაინტერესებულ პირებს ეძლევათ შესაძლებლობა, სამსახურის პერსონალურ მონაცემთა დაცვის ოფიცერთან პირისპირ შეხვედრის ფორმატში მიიღონ პასუხი ახალი კანონის იმპლემენტაციასთან დაკავშირებულ მათთვის საინტერესო ნებისმიერ შეკითხვაზე. აღნიშნული ფორმატის ფარგლებში დეტალური კონსულტაცია უკვე მიიღო 40-მდე (ორმოცამდე) პირმა.

4. საგანმანათლებლო აქტივობები

4.1. ზოგადი სასწავლო კურსები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული სიახლეების, მათ შორის, პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული ვალდებულების შესახებ დეტალური ინფორმირების მიზნით, პერსონალურ მონაცემთა დაცვის სამსახურის ორგანიზებით სასწავლო შეხვედრები ჩატარდა, რომლებსაც 1335-მდე (ათას სამას ოცდათხუთმეტი) პირი დაესწრო.

4.2. პერსონალურ მონაცემთა დაცვის ოფიცრებთან განხორციელებული შეხვედრები

სამსახურმა დამატებითი სასწავლო შეხვედრები დაუთმო უშუალოდ მოქმედი მონაცემთა დაცვის ოფიცრებისა და აღნიშნული პროფესიით დაინტერესებული პირების ინფორმირებას პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქცია-მოვალეობების და საქმიანობის განხორციელებისას გასათვალისწინებელი პრაქტიკული რჩევების შესახებ, რის ფარგლებშიც გადამზადება 640-მა (ექვსას ორმოცმა) პირმა გაიარა.

გარდა ამისა, მოცემული დროისთვის, წარმატებით მიმდინარეობს ამავე მიზნით პერსონალურ მონაცემთა დაცვის სამსახურისა და ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის თანამშრომლობის ფარგლებში შექმნილი სასერტიფიკატო კურსი პერსონალურ მონაცემთა დაცვის ოფიცრებისთვის, რაც ასევე ხელს შეუწყობს შრომით ბაზარზე გაჩენილი მზარდი მოთხოვნის დასაკმაყოფილებლად შესაბამისი კვალიფიციური კადრების მომზადებას.

4.3. სასწავლო პუბლიკაციები

დაინტერესებული პირების სათანადო ინფორმაციული რესურსით აღჭურვის მიზნით, პერსონალურ მონაცემთა დაცვის სამსახური აქტიურად მუშაობს შესაბამისი თემატური სახელმძღვანელოების შექმნასა და გავრცელებაზე. კერძოდ, სამსახურმა შეიმუშავა და გამოაქვეყნა „რეკომენდაციები პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ“; ხოლო ამერიკის შეერთებული შტატების საერთაშორისო განვითარების სააგენტოს (DAI/USAID) „საჯარო მმართველობის პროგრამის“ მხარდაჭერითა და მოწვეულ ექსპერტთან თანამშრომლობით — „მინიმალური სტანდარტი პერსონალურ მონაცემთა დაცვის ოფიცრებისთვის“. შემუშავებულ სახელმძღვანელო რეკომენდაციებში დეტალურად არის მიმოხილული პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულების ფარგლები და ორგანიზაციების მიერ მისი შესრულების წესი მონაცემთა დაცვის ოფიცრის პოზიციაზე დასაქმებული პირის ცოდნისა და უნარების მიმართ არსებული მოთხოვნები.

საკითხით დაინტერესებული პირებისთვის, ასევე, ხელმისაწვდომია პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულებასთან დაკავშირებით პერსონალურ მონაცემთა დაცვის სამსახურის მიერ მომზადებული 3 (სამი) ვიდეო პოდკასტი.

IV თავი. კანონის იმპლემენტაციის პროცესში გამოვლენილი სირთულეები

1. სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლთან დაკავშირებით

2022 წლის 24 მაისის საქართველოს №1575 კანონის საფუძველზე, სისხლის სამართლის საპროცესო კოდექსში განხორციელებული ცვლილების შედეგად, 136-ე მუხლით განსაზღვრულ საგამოძიებო მოქმედებაზე აღარ ვრცელდება ამავე კოდექსის XVI1 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, მაგრამ არაუგვიანეს 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 4^{1} ნაწილი, რომლის თანახმად, ამ მუხლით გათვალისწინებულ საგამოძიებო მოქმედებაზე ვრცელდება ამ კოდექსის 111-ე, 112-ე და 134-ე მუხლების დებულებები, რაც 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 ეგზემპლარს, 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 არაუგვიანეს 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.

ხსენებული დათქმები არ შეცვლილა 2024 წლის პირველ მარტს ამოქმედებულ, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით და მოწესრიგდა ამ კანონის 28-ე მუხლის მე-4, მე-5 და მე-6 პუნქტებით. საკანონმდებლო ცვლილებების შედეგად, დოკუმენტის ან ინფორმაციის — მათ შორის, კომპიუტერულ სისტემასა და კომპიუტერულ მონაცემთა შესანახ საშუალებაში არსებული მონაცემების — გამოთხოვაზე აღარ ვრცელდება სსსკ ფარული საგამოძიებო მოქმედებების თავით (მათ შორის, 143[3] მუხლით) დადგენილი ნორმები. თავის მხრივ, 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 მუხლით, ფარული საგამოძიებო მოქმედებების ჩატარებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების, ელექტრონული კომუნიკაციების კომპანიების კონტროლი პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ხორციელდება სამსახურის კონტროლის ელექტრონულ და კონტროლის სპეციალური ელექტრონულ სისტემაში — მონაცემთა დამუშავების კანონიერების შემოწმებით, მონაცემთა დამმუშავებლის/უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების შემოწმებით — ინსპექტირებით.

ამავე მუხლის მე-2 პუნქტის შესაბამისად, საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე-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, პერსონალურ მონაცემთა დაცვის სამსახური გარკვეული პრობლემების წინაშე დააყენა კანონმდებლობით განსაზღვრული საზედამხედველო კონტროლის სრულყოფილად განხორციელების ფარგლებში. სამსახურს, რომელიც ამ ინფორმაციათა შედარებით აწარმოებდა კონტროლს, მოაკლდა შესაძლებლობა, ზედამხედველობა გაუწიოს კომპანიების მოქმედებას მონაცემთა გადაცემის სისწორის შესახებ.

აღსანიშნავია პრაქტიკული სირთულეებიც, რომელიც წამოიჭრა, მაგალითად, 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, წარმოედგინათ ინფორმაცია — 2023 წლის პირველი იანვრიდან 2023 წლის 20 მაისამდე პერიოდში, სამართალდამცავი ორგანოების მიერ კომპანიის ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი

მონაცემების, სსსკ 136-ე მუხლით დადგენილი წესით გამოთხოვის შესახებ — გაცემული განჩინებების რაოდენობის შესახებ ან გადმოეგზავნათ გაცემული განჩინებების ასლები (რეკვიზიტები და სარეზოლუციო ნაწილი).

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

ინფორმაციის მოუწოდებლობამ გაართულა ელექტრონული კომუნიკაციის კომპანიის მიერ სამსახურისათვის შეტყობინების წარმოდგენის ვალდებულების შესწავლის პროცესი, შესაბამისად, სამსახურმა ვერ შეძლო სრულყოფილად გადაემოწმებინა, თუ რამდენი განჩინება გასცა სასამართლომ და მათ საფუძველზე, რამდენ შემთხვევაში და რა სახის ინფორმაცია გადასცა კომპანიამ სამართალდამცავ ორგანოს. ამასთან, შექმნა საჭიროება სასამართლოთა მხრიდან ინფორმაციის მიუწოდებლობის ფაქტზე არაგეგმური შემოწმებისა, რომლის შედეგად დადგინდა სამართალდარღვევა, მაგრამ აღნიშნული არ შეიძლება იქნეს მიჩნეული პრევენციისათვის გასატარებელ ღონისძიებად, რის გამოც შესაბამისად საკითხს შემდგომი საქმიანობის ობიექტურად და სრულყოფილად წარმართვისათვის ვერ მოაგვარებს.

საქართველოს სისხლის სამართლის საპროცესო კოდექსსა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში არსებული წინააღმდეგობებისა და ხარვეზების აღმოფხვრის მიზნით, სამსახურმა, 2022 წლის 23 აგვისტოს № PDPS 3 22 00004257 წერილით, მიმართა საქართველოს პარლამენტს, საკანონმდებლო ცვლილებების შემუშავების შესახებ, რომლითაც, სამართალდამცავი ორგანოების მიერ ელექტრონული კომუნიკაციის კომპანიებიდან ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების გამოთხოვისას, სასამართლოებისთვის და პროკურატურისათვის სავალდებულო გახდებოდა შესაბამისი განჩინებებისა და დადგენილებების (მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილის გათვალისწინებით) პერსონალურ მონაცემთა დაცვის სამსახურისთვის წარდგენა. აქვე, სამსახურს

ჰქონდა ინიციატივა დოკუმენტაციის წარმოდგენის კანონით დადგენილი ფორმისა და დროის შეცვლაზე. კერძოდ, ნაცვლად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლის მე-6 პუნქტით (2024 წლის პირველ მარტამდე მოქმედი კანონის მე-20 მუხლის მე-5 პუნქტი) დადგენილი გადაუდებელი აუცილებლობის შემთხვევაში, ფარული საგამოძიებო მოქმედების ჩატარების შესახებ პროკურორის დადგენილების, ფარული საგამოძიებო მოქმედების დადგენილებაში მითითებული დაწყების დროიდან, პროკურორის ან პროკურორის დავალებით გამომძიებლის მიერ, არაუგვიანეს 12 საათში წარმოდგენისა, შესაძლებლად მივიჩნევდით ამ ვადის გაზრდას, დადგენილების მიღებიდან 24 საათის, ხოლო განჩინების გამოტანიდან — 48 საათის გათვალისწინებით. ამასთან, სამსახური თანახმა იყო მატერიალური (დოკუმენტური) სახით წარდგენის ვალდებულების იმპერატიული დათქმის გაუქმებაზე და უშვებდა ან მატერიალური, ან ელექტრონული ფორმით წარმოდგენის შესაძლებლობას.

ვინაიდან, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლის მე-5 ნაწილის 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, სისხლის სამართლის საპროცესო კოდექსში განხორციელებული ზემოხსენებული საკანონმდებლო ცვლილებები, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს მოქმედი კანონით განსაზღვრულ ნორმებთანაც წინააღმდეგობრივ კოლიზიაშია, რაც სამსახურს მომავალშიც შეუქმნის მსგავს მნიშვნელოვან დაბრკოლებებს, საზედამხედველო კონტროლის უფლებამოსილების განხორციელების პროცესში.

სამართალდამცავი ორგანოები სხვადასხვა საპოლიციო ღონისძიების ჩატარების, დანაშაულის გამოძიების, სისხლისსამართლებრივ დევნასა და სასჯელის აღსრულებასთან დაკავშირებით, ამუშავებენ დიდი მოცულობით, მათ შორის, განსაკუთრებული კატეგორიის, პერსონალურ მონაცემებს, ხელი მიუწვდებათ არაერთ საინფორმაციო ბაზაზე, ვიდეო-სათვალთვალო სისტემების ჩანაწერებზე, ღია და ფარული მეთოდებით მოპოვებულ მონაცემებზე, რაც ზრდის პერსონალური მონაცემების კანონის მოთხოვნათა დარღვევით დამუშავების რისკებს.

გასათვალისწინებელია ის გარემოებაც, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 48-ე მუხლის მე-3 პუნქტის შესაბამისად, საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-138-ე მუხლებით გათვალისწინებული საგამოძიებო მოქმედებებისა და იმავე კოდექსის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული ფარული საგამოძიებო მოქმედებების ჩატარების კონტროლის შედეგების შესახებ ანგარიშს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი წელიწადში ერთხელ წარუდგენს საქართველოს პარლამენტის ბიუროს მიერ საქართველოს პარლამენტის რეგლამენტით დადგენილი წესით განსაზღვრულ პარლამენტის კომიტეტსა და ნდობის ჯგუფს.

ზემოაღნიშნული მიმართულია სამსახურის კონტროლის მექანიზმისა და საქმიანობის სრულყოფის ბერკეტების გაზრდისაკენ, რამაც ხელი უნდა შეუწყოს არაკანონიერი დამუშავებით მონაცემთა სუბიექტების უფლებების მნიშვნელოვანი დაზიანების რისკების შემცირებას და თავიდან იქნეს აცილებული მონაცემთა სუბიექტის ღირსების/რეპუტაციის/შელახვა, მათ მიმართ დისკრიმინაციული მოპყრობა ან სხვა მძიმე შედეგი.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, სამსახური მიზანშეწონილად მიიჩნევს, საკანონმდებლო დონეზე მოწესრიგდეს კონტროლის მექანიზმები, კომპიუტერულ სისტემასა და კომპიუტერულ მონაცემთა შემნახავ საშუალებებიდან ინფორმაციის გამოთხოვის შედეგებზე პერსონალური მონაცემების დაცვის სამსახურისათვის სავალდებულო შეტყობინების შესახებ და ზემოხსენებული წინააღმდეგობების საკანონმდებლო წესით გასწორების მიზნით, განახლდეს საკითხის განხილვა.

პერსონალურ მონაცემთა დაცვის სამსახური გამოთქვამს სრულ მზადყოფნას, ხარვეზის მოწესრიგების ფარგლებში, აქტიურად ითანამშრომლოს საქართველოს პარლამენტთან.

2. იურიდიული პირის, უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის წლიური ბრუნვის საკითხი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის IX და X თავებით დადგენილი რეგულაციები სრულიად ახლებურად აწესრიგებენ პერსონალურ მონაცემთა დამუშავების სფეროში ჩადენილ

სამართალდარღვევებზე პასუხისმგებლობის დადგენისა და სახდელის სახით დაკისრებული ჯარიმის ოდენობის განსაზღვრის წესებს.

აღნიშნული დანაწესების მიხედვით, სამართალდამრღვევისათვის დასაკისრებელი ჯარიმის ოდენობა, სამსახურმა უნდა განსაზღვროს იურიდიული პირის, უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის წლიური ბრუნვის მიხედვით, ხოლო ჯარიმების საერთო ოდენობა არ უნდა აღემატებოდეს:

- 10 000 ლარს ფიზიკური პირის, საჯარო დაწესებულების, არასამეწარმეო (არაკომერციული) იურიდიული პირის შემთხვევაში, აგრეთვე იურიდიული პირის, უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის შემთხვევაში, რომელთა წლიური ბრუნვა 500 000 ლარს არ აღემატება;
- 20 000 ლარს იურიდიული პირის (გარდა არასამეწარმეო (არაკომერციული) იურიდიული პირისა), უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის შემთხვევაში, რომელთა წლიური ბრუნვა 500 000 ლარს აღემატება.

ზემოაღნიშნულიდან გამომდინარე, ცხადია, რომ სამსახურის პერსონალურ მონაცემთა დამუშავების კანონიერებაზე ზედამხედველობის განმახორციელებელ სტრუქტურულ ერთეულებს - საჯარო სექტორზე ზედამხედველობის, კერძო სექტორზე ზედამხედველობის, გეგმური ინსპექტირების და სამართალდამცავ ორგანოებზე ზედამხედველობის დეპარტამენტებს 2024 წლის პირველი მარტიდან სავალდებულო წესით ესაჭიროებათ აღნიშნულ ინფორმაციაზე წვდომა თითოეული სამართალდარღვევის საქმის შესწავლის ფარგლებში.

სწორედ ამ მიზნით, პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის 64-ე მუხლის მე-7 პუნქტი პირდაპირ ადგენს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის უფლებამოსილებას ამ კანონით გათვალისწინებული ადმინისტრაციული პასუხისმგებლობის დაკისრების მიზნებისთვის საჯარო სამართლის იურიდიული პირისგან – შემოსავლების სამსახურისგან გამოითხოვოს იურიდიული პირის, უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის წლიური ბრუნვის შესახებ ინფორმაცია, მიიღოს იგი და აგრეთვე ჰქონდეს წვდომა საჯარო სამართლის იურიდიული პირის – შემოსავლების სამსახურის შესაბამის ელექტრონულ მონაცემთა ბაზაზე.

მოცემული მომენტისთვის, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების/უფლებამოსილი პირების წლიური ბრუნვის შესახებ ინფორმაციის

პირდაპირ წერილობით გამოთხოვის მექანიზმი მოქმედებს. რაც შეეხება სამსახურის უფროსის წვდომას საჯარო სამართლის იურიდიული პირის – შემოსავლების სამსახურის შესაბამის ელექტრონულ მონაცემთა ბაზაზე, აღნიშნული მექანიზმი ამჟამად ჯერ კიდევ ტექნოლოგიური დამუშავების ეტაპზეა და არ არის რეალიზებული, თუმცა სამსახურის მხრიდან გადადგმულია ყველა შესაძლო საამისო ნაბიჯი.

გარდა ამისა, წლიური ბრუნვის შესახებ ინფორმაციის წერილობით გამოთხოვის მოქმედი მექანიზმის ფარგლებშიც გამოიკვეთა სერიოზული ხარვეზები მოწოდებული ინფორმაციის სისრულის და სიზუსტის თვალსაზრისით, რასაც შემოსავლების სამსახურის წარმომადგენლები გარკვეული მეთოდოლოგიური მიზეზებით თუ ბრუნვის განსაზღვრის ცალკეული კრიტერიუმებით ხსნიან. კერძოდ, თუ პირი დამატებითი ღირებულების გადასახადის გადამხდელია, მაშინ როგორც წესი პრობლემა არ არსებობს, მაგრამ თუ პირი არ არის ამ სახის გადასახადის გადამხდელი, ინფორმაცია წლიური ბრუნვის შესახებ ან საერთოდ არ მოეწოდება სამსახურს ან გარკვეულ შემთხვევებში არასრული და არაზუსტია.

განსაკუთრებით მნიშვნელოვანია ამ კუთხით რა ვითარებაა ცალკეულ სექტორებთან დაკავშირებით. მაგალითად, საგანმანათლებლო, ჯანდაცვის, სათამაშო ბიზნესის მიმართულებებით, უფრო ხშირია წლიური ბრუნვის შესახებ არასრული ან უზუსტ და ზოგჯერ საქმიანობის მასშტაბისათვის შეუსაბამო ინფორმაციის მოწოდების შემთხვევებიც. ასე მაგალითად, ცნობილი სადიაგნოსტიკო ლაბორატორიის (რომელიც ქვეყნის ფარგლებს გარეთაც სარგებლობს ევროპული ქვეყნების ლაბორატორიების მომსახურებით) შემთხვევაში, სამსახურს ვერ მოეწოდა ინფორმაცია მისი წლიური ბრუნვის შესახებ, მაშინ როცა სხვა, ანალოგიური ტიპის სადიაგნოსტიკო კლინიკის შემთხვევაში, გაზიარებულ იქნა ინფორმაცია.

ამასთან, ერთ-ერთი ფინანსური ბიუროს შემთხვევაში, სამსახურმა მიიღო ინფორმაცია მისი წლიური ბრუნვის 500 000 ლარზე ნაკლებობის შესახებ, რაც ამ ტიპის ორგანიზაციის საქმიანობის სახის გათვალისწინებით ნამდვილად შეუსაბამოა. რთული წარმოსადგენია, მაგრამ ერთ-ერთი ცნობილი სამორინის შემთხვევაშიც იგივე განმეორდა.

ასევე, რთული ვითარებაა კერძო საგანმანათლებლო დაწესებულებების წლიური ბრუნვის შესახებ ინფორმაციის მიღებასთან დაკავშირებითაც. ამ სექტორის შესახებ სამსახური, როგორც წესი, გამონაკლისი შემთხვევების გარდა, საერთოდ

ვერ იღებს მათი წლიური ბრუნვის შესახებ ინფორმაციას, ამგვარი ინფორმაციის სსიპ შემოსავლების სამსახურში არარსებობის გამო.

სსიპ — შემოსავლების სამსახურიდან დადასტურდა, რომ გადასახადის გადამხდელის შესახებ კონკრეტული პერიოდის მიხედვით, შესაძლებელია გაიცეს ინფორმაცია ბრუნვების შესახებ დღგ-ს ყოველთვიური დეკლარაციების/საკონტროლო-სალარო აპარატის (აპარატების) ფისკალური მეხსიერების/გადამხდელის მიერ გამოწერილი რეალიზაციის სასაქონლო ზედნადებების/„გადახდის წყაროსთან დაკავებული გადასახადების დეკლარაციების, განხორციელებული ექსპორტის საბაჟო პროცედურის (ასეთების არსებობის შემთხვევაში) მიხედვით.

სამსახურის წარმომადგენლების მიერ არაერთი შეხვედრა/კომუნიკაცია შედგა შემოსავლების სამსახურის უფლებამოსილ წარმომადგენლებთან აღნიშნულ თემაზე. ზემოთდასახელებული მაგალითები კონკრეტულადაა განხილული მათთან. შედეგად იკვეთება, რომ აღნიშნული პრობლემა არსებობს არა მხოლოდ სამსახურთან მიმართებაში, არამედ ყველა იმ მაკონტროლებელ/ზედამხედველ ორგანოებთან მიმართებაშიც, რომლებიც სამართალდამრღვევს ფულად სახდელს აკისრებენ მისი წლიური ბრუნვის ოდენობის მიხედვით, რადგან მსგავსი საკანონმდებლო რეგულაციები, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის გარდა, გვხვდება „მომხმარებელთა უფლებების დაცვის შესახებ“ და „ელექტრონული კომერციის შესახებ“ საქართველოს კანონებშიც.

ამდენად, გარდა იმისა, რომ სამართალდამრღვევის წლიური ბრუნვის შესახებ უზუსტო ინფორმაციის მიღება ან ამგვარი ინფორმაციის მიუღებლობა, შეიძლება გახდეს კანონით გათვალისწინებულ, რეალურად კუთვნილზე ნაკლები ფულადი სახდელის (სახელმწიფო ბიუჯეტში გადასახდელი ჯარიმა) დაკისრების წინაპირობა, ასევე აღნიშნული დასაკისრებელი ჯარიმის ოდენობის სამართლიანად და კანონით დადგენილი ფარგლების დაცვით განსაზღვრის შესაძლებლობას ზღუდავს, რამაც საბოლოოდ სამსახურის მიერ ჩატარებული ინსპექტირების მთლიანი პროცესის კანონშესაბამისობა შეიძლება ეჭვქვეშ დააყენოს.

სამსახური მიიჩნევს, რომ მიზანშეწონილია ყველა კომპეტენტური ორგანოს ჩართულობით შემუშავდეს პრაქტიკული და საჭიროების შემთხვევაში, სათანადო ნორმატიული მექანიზმები აღნიშნული პრობლემის სრულად აღმოსაფხვრელად.

3. სპეციალური წარმომადგენლები

ახალი კანონის 34-ე მუხლი ადგენს, რომ საქართველოს ფარგლებს გარეთ რეგისტრირებული დამუშავებისთვის პასუხისმგებელი პირის/დამუშავებაზე უფლებამოსილი პირის მიერ საქართველოში არსებული ტექნიკური საშუალებებით მონაცემთა დამუშავების შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირი/დამუშავებაზე უფლებამოსილი პირი ვალდებულია, საქართველოში არსებული ტექნიკური საშუალებების გამოყენებით მონაცემთა დამუშავებამდე საქართველოში დანიშნოს ან განსაზღვროს სპეციალური წარმომადგენელი, რომელიც რეგისტრირდება პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მიერ გამოცემული ნორმატიული აქტით დადგენილი წესით.

საგულისხმოა, რომ დამუშავებისთვის პასუხისმგებელ /დამუშავებაზე უფლებამოსილ პირს მონაცემთა დამუშავების უფლება წარმოეშობა მხოლოდ სპეციალური წარმომადგენლის რეგისტრაციის შემდეგ, ხოლო სპეციალური წარმომადგენლის განსაზღვრასთან/დანიშვნასთან დაკავშირებული ვალდებულების შეუსრულებლობა, კანონის 83-ე მუხლის თანახმად, გამოიწვევს სამართალდამრღვევის გაფრთხილებას ან დაჯარიმებას 3 000 ლარის ოდენობით, იგივე ქმედება კი, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მიერ ადმინისტრაციული სახდელის დადებიდან 1 წლის განმავლობაში – გამოიწვევს სამართალდამრღვევის დაჯარიმებას 5 000 ლარის ოდენობით.

გასათვალისწინებელია, რომ სპეციალური წარმომადგენლის დანიშვნის/რეგისტრაციის ვალდებულება არ ვრცელდება იმ დამუშავებისთვის პასუხისმგებელ პირზე/დამუშავებაზე უფლებამოსილ პირზე, რომელიც დაფუძნებულია ევროკავშირის წევრ სახელმწიფოებში, ევროკავშირის მიერ აღიარებულ მონაცემთა ადეკვატური დაცვის მქონე სახელმწიფოში და მასზე ვრცელდება ევროკავშირში მოქმედი პერსონალურ მონაცემთა დაცვის წესები.

სპეციალური წარმომადგენლის რეგისტრაცია ხორციელდება „პერსონალურ მონაცემთა დაცვის სამსახურის მიერ სპეციალური წარმომადგენლის რეგისტრაციის წესის დამტკიცების შესახებ“ ბრძანების[7] საფუძველზე და სარეგისტრაციოდ წარსადგენი განაცხადისა და თანდართული დოკუმენტაციის

[7] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №20 პერსონალურ მონაცემთა დაცვის სამსახურის მიერ სპეციალური წარმომადგენლის რეგისტრაციის წესის დამტკიცების შესახებ.

წარდგენის წესიც ამავე ბრძანებით განისაზღვრება. პერსონალურ მონაცემთა დაცვის სამსახური ამოწმებს განაცხადს თანდართულ დოკუმენტაციასთან ერთად და იღებს გადაწყვეტილებას საქართველოს ფარგლებს გარეთ რეგისტრირებული დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირის სპეციალური წარმომადგენლის რეგისტრაციის, რეგისტრაციაზე უარის თქმის ან განაცხადზე ხარვეზის დადგენის შესახებ. სამსახური ასევე უფლებამოსილია გამოითხოვოს განმცხადებლისაგან დამატებითი დოკუმენტაცია სპეციალური წარმომადგენლის რეგისტრაციის მიზნებისათვის. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ სპეციალური წარმომადგენლის დანიშვნის შესახებ მიღებული განაცხადების განხილვის ვადებიც ზემოხსენებული ბრძანებით არის განსაზღვრული.

საგულისხმოა, რომ სპეციალური წარმომადგენლის დანიშვნის ვალდებულება, ერთი მხრივ მონაცემთა დამუშავების გამჭვირვალობის პრინციპის დაცვასა და მონაცემთა სუბიექტის ინფორმირების უფლების რეალიზაციას მიემართება, ხოლო მეორე მხრივ — ემსახურება საზედამხედველო ორგანოს მანდატის სრულყოფილად გავრცელებისა და მისი ფუნქციების შეუფერხებლად განხორციელების შესაძლებლობას, თუმცა პრაქტიკული თვალსაზრისით, არსებობს გარკვეული გამოწვევები, რაც კანონით გათვალისწინებული ამ ვალდებულების შესრულებაზე ზედამხედველობას ართულებს.

უპირველეს ყოვლისა, ამ თვალსაზრისით უნდა აღინიშნოს ის ფაქტი, რომ კანონის ამ კონკრეტული დანაწესის ამოქმედებიდან დღემდე, სამსახურში არ დაფიქსირებულა არც ერთი მომართვა სპეციალური წარმომადგენლის რეგისტრაციის მოთხოვნით და შესაბამისად არ განხორციელებულა ადმინისტრაციული წარმოება ამ მიზნებისთვის. აღნიშნულის განმაპირობებელ გარემოებად შესაძლოა დასახელდეს ცნობიერების ნაკლებობა, რამდენადაც კანონის 34-ე მუხლის რეგულაცია ადგენს იმ დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირების ვალდებულებებს, რომლებიც არ არიან საქართველოში დაფუძნებული და არც საქართველოში არსებული ტექნიკური საშუალებების გამოყენებით ახორციელებენ მონაცემთა დამუშავებას, შესაბამისად არ ფლობენ სახელმწიფო ენას, რომ წინმსწრებად გაეცნონ სამსახურის უფროსის შესაბამის ბრძანებას სპეციალური წარმომადგენლის რეგისტრაციის წესისა და პირობების თაობაზე. ხსენებული დაბრკოლების აღმოფხვრის თვალსაზრისით, დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი ორგანიზაციებისა თუ პირების ცნობიერების ამაღლებისა და მათი ინფორმირების მიზნით, სამსახურმა მიმართა საქართველოს საკანონმდებლო მაცნეს კანონის გარდამავალი დებულებების

შესაბამისად, კანონით დადგენილ ვადაში, 2024 წლის პირველ მარტამდე გამოცემული და საქართველოს საკანონმდებლო მაცნეს ვებგვერდზე გამოქვეყნებული ოთხი მნიშვნელოვანი კანონქვემდებარე ნორმატიული აქტის („ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება №19 (2024 წლის 28 თებერვალი); „პერსონალურ მონაცემთა დაცვის სამსახურის მიერ სპეციალური წარმომადგენლის რეგისტრაციის წესის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება №20 (2024 წლის 28 თებერვალი); „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება №21 (2024 წლის 28 თებერვალი); პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება №22 იმ „დამუშავებისთვის პასუხისმგებელ პირთა და დამუშავებაზე უფლებამოსილ პირთა წრის განსაზღვრის შესახებ, რომლებსაც არ აქვთ ვალდებულება დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი“ (2024 წლის 28 თებერვალი)) ინგლისურ ენაზე თარგმნის, რედაქტირებისა და გამოქვეყნების თხოვნით, რაც შესაბამისად განხორციელდება 2025 წლის იანვრის თვეში.

სპეციალური წარმომადგენლის კანონით განსაზღვრული ვალდებულების შესრულებაზე სამსახურის საზედამხედველო მანდატის სრულყოფილად გავრცელებასთან დაკავშირებით კიდევ ერთ გამოწვევას წარმოადგენს ხსენებული ვალდებულების შეუსრულებლობის გამო სამსახურის უფროსის მიერ კონკრეტული დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირის დაჯარიმების შესახებ მიღებული გადაწყვეტილების აღსრულების საკითხი. კერძოდ, „სააღსრულებო წარმოებათა შესახებ“ საქართველოს კანონის მე-2 მუხლის „ძ“ ქვეპუნქტის თანახმად, სამსახურის უფროსის ინდივიდუალური სამართლებრივი აქტი სახდელის სახით ჯარიმის დაკისრების ნაწილში ექვემდებარება აღსრულებას, თუმცა იმის გათვალისწინებით, რომ სამართალდამრღვევი არ წარმოადგენს საქართველოში დაფუძნებულ სამართალსუბიექტს და არც ქონებას ფლობს საქართველოს ტერიტორიაზე, სააღსრულებო წარმოება ფერხდება.

სპეციალური წარმომადგენლის კონცეფცია, როგორც ქართულ სამართლებრივ რეალობაში, აგრეთვე ევროპის ქვეყნების მხრიდან მონაცემთა დაცვის

მიზნებისთვის, დაინერგა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ იმ პასუხისმგებელი ან უფლებამოსილი პირების მიმართ ეფექტიანი სააღსრულებო მანდატის გასავრცელებლად, რომლებიც არ ექცევიან რეგულაციის ტერიტორიული გავრცელების არეალში და გულისხმობს ევროპულ საზედამხედველო ორგანოების შესაძლებლობას გამოიყენონ მაკორექტირებელი ზომები ან ადმინისტრაციული სახდელები და ჯარიმები იმ პასუხისმგებელი ან უფლებამოსილი პირის წინააღმდეგ, რომელიც სხვა ქვეყანაშია დაფუძნებული. მსგავსად ქართული სამართლებრივი რეალობისა, რეგულაციის გავრცელების შედეგად სპეციალური წარმომადგენლის დაურეგისტრირებლობის გამო დაკისრებული ჯარიმების აღსრულება რამდენიმე გამოწვევის წინაშე დგას, მათ შორისაა იურისდიქციის შეზღუდვები ევროკავშირის არაწევრი სუბიექტების მიმართ, იურისდიქციებს შორის საპასუხო აღსრულების შეთანხმებების არარსებობა და ევროკავშირის ზედამხედველობის ორგანოების რესურსების შეზღუდვა[8].

ზემოხსენებულის გათვალისწინებით, უცხო ქვეყანაში რეგისტრირებული დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირის ადგილობრივი წარმომადგენლის არარსებობა არა მხოლოდ საქართველოს სამართლებრივ რეალობაში, არამედ - ევროკავშირის ტერიტორიულ ფარგლებშიც აფერხებს მონაცემთა დამუშავების პროცესების კანონიერების შემოწმებასა და გამოვლენილი სამართალდარღვევისთვის დაკისრებული ჯარიმის უშუალო აღსრულებას და ასუსტებს სანქციის ამ სახის შემაკავებელ ეფექტს. მართალია, საზედამხედველო ორგანოს ყოველთვის აქვს შესაძლებლობა, ჯარიმის დაკისრებასთან ერთად დაავალდებულოს სამართალდამრღვევი, დანიშნოს სპეციალური წარმომადგენელი, ხოლო ამ ვალდებულების შესრულებამდე აუკრძალოს მას მონაცემთა დამუშავების პროცესის წარმოება, თუმცა აღსრულების თვალსაზრისით ეს საკითხიც ფერხდება, ვინაიდან დავალების შეუსრულებლობის შემთხვევისთვის გათვალისწინებული სანქციაც ჯარიმას წარმოადგენს, თუმცა ამ გარემოებას კვლავ ფულადი ვალდებულებების იძულებით გადახდევინების მექანიზმის ნაკლოვანებასთან მივყავართ.

ამდენად, საზედამხედველო ორგანოს გაძლიერებული მანდატის ფარგლებში, მისი საქმიანობის ეფექტიანად და სრულყოფილად წარმართვისა და კანონით

[8] შდრ. https://www.adamsandreese.com/news-knowledge/gdpr-guidelines-finalized-but-how-will-they-be-enforced-for-non-eu-companies; https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement; https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm.

დასახული მიზნების ზედმიწევნით შესრულების თვალსაზრისით მიზანშეწონილია, სამსახურის უფროსის გადაწყვეტილების აღსრულების მექანიზმებთან კავშირში მყოფ ყველა კომპეტენტურ ორგანოსა და პარტნიორ საერთაშორისო ორგანიზაციებთან ურთიერთთანამშრომლობით დაიდენტიფიცირდეს სააღსრულებო წარმოების განხორციელებისთვის ხელისშემშლელი ფაქტორები, ნაკლოვანების აღმოფხვრის კონკრეტული საშუალებები და გაიწეროს გარკვეული გეგმა, რომელიც ერთი მხრივ გამოკვეთს პრობლემური საკითხის გადასაჭრელად აუცილებელ საჭიროებებსა და სამართლებრივი მოწესრიგების გზებს, ხოლო მეორე მხრივ — საუკეთესო საერთაშორისო პრაქტიკაზე დაყრდნობით, განსაზღვრავს საკითხის მიმართ კომპლექსურ და კოორდინირებულ მიდგომას.

4. პერსონალურ მონაცემთა დაცვის ოფიცრებთან დაკავშირებით

4.1. ძირითადი სირთულეები

საკონსულტაციო-საგანმანათლებლო ფორმატების მეშვეობით დაინტერესებული პირების ინფორმირების პარალელურად, პერსონალურ მონაცემთა დაცვის სამსახური კერძო და საჯარო დაწესებულებების მიერ პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულების შესრულებას კანონით მინიჭებული უფლებამოსილების ფარგლებში ზედამხედველობს.

არსებული მდგომარეობით, პერსონალურ მონაცემთა დაცვის სამსახურში წარმოდგენილია სხვადასხვა დაწესებულების 2365 (ორი ათას სამას სამოცდახუთი) შეტყობინება პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულების შესრულებასთან დაკავშირებით. სამსახურში წარმოდგენილი აღნიშნული ინფორმაციიდან იკვეთება, რომ მონაცემთა დამმუშავებელი ორგანიზაციების მნიშვნელოვანი ნაწილი ხსენებული ვალდებულების შესრულებას პასუხისმგებლობით მოეკიდა. დადებითი ტენდენციის ამსახველი ზემოაღნიშნული მაჩვენებლის მიუხედავად, საყურადღებოა ის რიგი გამოწვევები, რომლებიც პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ჩატარებული შემოწმებების შედეგად გამოიკვეთა.

არსებული მდგომარეობით, პერსონალურ მონაცემთა დაცვის სამსახურმა პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული ვალდებულების შესრულების საკითხის შესწავლა 73 (სამოცდაცამეტი) შემოწმების ფარგლებში დაასრულა.

პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულების შეუსრულებლობა შემოწმებების შედეგად 16 (თექვსმეტ) შემთხვევაში დადგინდა. შესაბამისი დაწესებულებები სამართალდამრღვევებად იქნენ ცნობილნი, დაეკისრათ ადმინისტრაციული სახდელი და დაევალათ ვალდებულების შესრულება სამსახურის მიერ განსაზღვრულ გონივრულ ვადაში.

აღნიშნული შემოწმებების ფარგლებში სამსახურის მიერ გამოვლენილი სხვა ნაკლოვანებები უკავშირდებოდა ინტერესთა კონფლიქტის თავიდან არიდებას, ოფიცრად დანიშნული პირების კომპეტენციას და ოფიცრის შესახებ ინფორმაციის ხელმისაწვდომობასთან დაკავშირებით კანონით განსაზღვრული მოთხოვნების შესრულებას. კერძოდ, 9 (ცხრა) დაწესებულების შემთხვევაში გამოირკვა, რომ პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციები მათ შეთავსებული ჰქონდათ საკუთარი თანამშრომლებისთვის, თუმცა აღნიშნული თანამშრომლების სხვა ფუნქციებთან მიმართებით ვერ იყო თავიდან აცილებული ინტერესთა კონფლიქტი. შემოწმებების ფარგლებში დადგინდა, რომ თანამშრომლები, რომლებსაც აღნიშნულ შემთხვევებში პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციები დაეკისრათ, მათი სხვა ფუნქცია-მოვალეობების ფარგლებში პარალელურად მონაწილეობდნენ მონაცემთა დამუშავების მიზნებისა და საშუალებების განსაზღვრაში. შედეგად კი, სათანადოდ ვერ იყო უზრუნველყოფილი პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციების შესრულებისას მათი დამოუკიდებლობა და მიუკერძოებლობა. 2 (ორი) დაწესებულების შემთხვევაში დადგინდა, რომ პერსონალურ მონაცემთა დაცვის ოფიცრად დანიშნულ პირებს არ ჰქონდათ არავითარი ცოდნა მონაცემთა დაცვის სფეროში, რაც, ცხადია, გამორიცხავდა მათ მიერ საქმიანობის კვალიფიციურად და ეფექტიანად განხორციელების შესაძლებლობას.

13 (ცამეტი) დაწესებულების შემთხვევაში გამოიკვეთა, რომ მათ კანონით დადგენილ ვადაში ჰყავდათ დანიშნული პერსონალურ მონაცემთა დაცვის ოფიცერი, თუმცა არ ჰქონდათ დაცული ოფიცრის ვინაობისა და საკონტაქტო ინფორმაციის პერსონალურ მონაცემთა დაცვის სამსახურისთვის მოწოდების ან/და საჯაროდ ხელმისაწვდომი საშუალებებით გამოქვეყნების ვადები. აღნიშნული კი აფერხებდა ხსენებულ პოზიციაზე განსაზღვრული პირების შესახებ ინფორმაციის საზედამხედველო ორგანოსთვისა და მონაცემთა სუბიექტებისთვის სათანადო ხელმისაწვდომობას.

პერსონალურ მონაცემთა დაცვის სამსახურის გადაწყვეტილებებით, დაწესებულებებს მიეცათ შესაბამისი დავალებები ინტერესთა კონფლიქტთან,

ოფიცრად დანიშნული პირების კომპეტენციასთან და ოფიცრის შესახებ ინფორმაციის ხელმისაწვდომობასთან დაკავშირებული ზემოხსენებული ნაკლოვანებების აღმოსაფხვრელად.

4.2. პრეცედენტული გადაწყვეტილებები

- **მცხეთის მუნიციპალიტეტის საკრებულო**

სამსახურმა გეგმური შემოწმების ფარგლებში შეისწავლა მცხეთის მუნიციპალიტეტის საკრებულოს მიერ პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულების შესრულების ფაქტი. მცხეთის მუნიციპალიტეტის საკრებულო საჯარო დაწესებულებას წარმოადგენს, შესაბამისად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 33-ე მუხლის თანახმად, იგი ვალდებულია, დანიშნოს პერსონალურ მონაცემთა დაცვის ოფიცერი.

შემოწმების ფარგლებში დადგინდა, რომ საკრებულომ პერსონალურ მონაცემთა დაცვის ოფიცრად განსაზღვრა საკრებულოს ადამიანური რესურსების მართვის დეპარტამენტის უფროსი, რომელსაც ოფიცრის ფუნქციები დააკისრა თავის ძირითად სამსახურებრივ უფლებამოსილებებთან შეთავსებით. ადამიანური რესურსების განყოფილების ხელმძღვანელი, მისთვის დაკისრებული ფუნქციებიდან გამომდინარე, ზედამხედველობდა მის დაქვემდებარებაში მყოფი პირების მხრიდან განხორციელებულ მონაცემთა დამუშავების პროცესებს. კერძოდ, საკრებულოს ადამიანური რესურსების მართვის განყოფილების უფლებამოსილებებს, მათ შორის საკრებულოს თანამდებობის პირების, საკრებულოს წევრების, საკრებულოში დასაქმებული საჯარო მოსამსახურეების პირადი საქმეების შექმნა, შენახვა და ადამიანური რესურსების მართვასთან დაკავშირებული დოკუმენტაციის მომზადება, საკრებულოს თავმჯდომარის ინდივიდუალური ადმინისტრაციულ-სამართლებრივი აქტების პროექტების მომზადება, ადამიანური რესურსების მართვის ელექტრონულ პროგრამაში მუშაობა (საკრებულოში დასაქმებულ საჯარო მოსამსახურეთა შესახებ მონაცემების პროგრამაში ატვირთვა), საკრებულოს აპარატის ადამიანური რესურსების მართვის განყოფილებაში შემოსული კორესპონდენციის დამუშავება, ანალიზი და მათზე პასუხების მომზადება.

შესაბამისად, დადგინდა, რომ საკრებულოს პერსონალურ მონაცემთა დაცვის ოფიცერი, რომელიც იმავდროულად ასრულებდა პერსონალური მონაცემების დამმუშავებელი სტრუქტურული ერთეულის — ადამიანური რესურსების

მართვის განყოფილების უფროსის უფლებამოსილებებს, ხელმძღვანელობდა მის დაქვემდებარებაში მყოფი პირების მიერ ისეთი ფუნქციების განხორციელებას, რაც მოიცავდა პერსონალურ მონაცემთა დამუშავებას, ჰქონდა პერსონალურ მონაცემებზე წვდომა, ჩართული იყო მონაცემთა დამუშავების პროცესში და ჰქონდა დამუშავების პროცესებთან დაკავშირებული გადაწყვეტილებების მიღების შესაძლებლობა.

აღნიშნულის გათვალისწინებით, პერსონალურ მონაცემთა დაცვის სამსახურმა მიიჩნია, რომ იმ პირობებში, როდესაც საკრებულოს პერსონალურ მონაცემთა დაცვის ოფიცერი იმავდროულად ითავსებდა ზემოაღნიშნულ უფლებამოსილებებს და საკრებულოს მიერ არ იყო დაცული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრული წესი პერსონალურ მონაცემთა დაცვის ოფიცრის განსაზღვრისას ინტერესთა კონფლიქტის თავიდან აცილების შესახებ.

სამსახურის გადაწყვეტილებით, საკრებულოს დაევალა უზრუნველყოს პერსონალურ მონაცემთა დაცვის ოფიცრად მხოლოდ ისეთი პირის საქმიანობა, რომელსაც თავისი უფლებამოსილებების განხორციელების პროცესში არ ექნება ინტერესთა კონფლიქტი.

- **საგარეჯოს მუნიციპალიტეტის მერია**

სამსახურმა ასევე შეისწავლა საგარეჯოს მუნიციპალიტეტის მერიის მიერ პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულების შესრულების ფაქტი. საგარეჯოს მუნიციპალიტეტის მერიას, როგორც საჯარო დაწესებულებას, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 33-ე მუხლის თანახმად, ასევე ეკისრება პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულება.

შემოწმების შედეგად დადგინდა, რომ მერიას პერსონალურ მონაცემთა დაცვის ოფიცრად განსაზღვრული ჰყავდა მერიის იურიდიული სამსახურის სპეციალისტი, რომელიც არ გათავისუფლებულა მისი ძირითადი ფუნქცია-მოვალეობებისგან. როგორც შემოწმების ფარგლებში დადგინდა, აღნიშნული პირი მისთვის, როგორც იურიდიული სამსახურის სპეციალისტისთვის დაკისრებული ფუნქციების ფარგლებში, ახორციელებდა მერიის წარმომადგენლობას სასამართლოში და სხვა ადმინისტრაციულ ორგანოებში უზრუნველყოფდა სარჩელებისა და შესაგებლების მომზადებას და ხელს აწერდა სასამართლო

დოკუმენტებს. აღნიშნული პირი ხელმძღვანელთან შეთანხმებით, წარმოების ფარგლებში, თავად განსაზღვრავდა სასამართლოში წარსადგენი მტკიცებულებების სახესა და მოცულობას. ასევე დადგინდა, რომ ოფიცრად განსაზღვრულ პირს, შესაძლოა, პერიოდულად ასევე დაჰკისრებოდა ისეთი ფუნქციები, როგორებიცაა: მოქალაქეთა წერილებისა და განცხადებების განხილვა, საჯარო ინფორმაციის ხელმისაწვდომობის უზრუნველყოფა, მერიაში შექმნილი სხვადასხვა კომისიის მუშაობაში მონაწილეობა და სხვა.

აღნიშნულის გათვალისწინებით, პერსონალურ მონაცემთა დაცვის სამსახურმა მიიჩნია, რომ მერიის მიერ პერსონალურ მონაცემთა დაცვის ოფიცრად განსაზღვრული პირისთვის პარალელურად დაკისრებული ზემოხსენებული ფუნქციები განაპირობებდა მონაცემთა დამუშავების მიზნებისა და საშუალებების განსაზღვრაში მის მონაწილეობას, რაც ქმნიდა ინტერესთა კონფლიქტს. სამსახურის გადაწყვეტილებით მერიას დაევალა, პერსონალურ მონაცემთა დაცვის ოფიცრად ისეთი პირის საქმიანობის უზრუნველყოფა, რომელსაც არ ექნება ინტერესთა კონფლიქტი.

დადგინდა, რომ მერიას პერსონალურ მონაცემთა დაცვის სამსახურისთვის კანონის შესაბამისად არ ჰქონდა წარდგენილი ინფორმაცია ოფიცრად განსაზღვრული პირის ვინაობისა და საკონტაქტო ინფორმაციის შესახებ, დაწესებულებას ასევე დაევალა აღნიშნული ინფორმაციის საზედამხედველო ორგანოსთვის წარმოდგენა.

- **ა(ა)იპ — დედოფლისწყაროს მუნიციპალიტეტის ხელოვნების სკოლა**

ერთ-ერთი შემოწმების ფარგლებში პერსონალურ მონაცემთა დაცვის სამსახურმა ასევე შეისწავლა ა(ა)იპ — დედოფლისწყაროს მუნიციპალიტეტის ხელოვნების სკოლის მიერ პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული ვალდებულების შესრულების ფაქტი.

აღსანიშნავია, რომ სკოლაზე, როგორც დედოფლისწყაროს მუნიციპალიტეტის მიერ დაფუძნებულ და ნაწილობრივ ადგილობრივი ბიუჯეტიდან დაფინანსებულ საჯარო დაწესებულებაზე, ვრცელდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულება.

შემოწმების შედეგად დადგინდა, რომ სკოლას პერსონალურ მონაცემთა დაცვის ოფიცრად განსაზღვრული ჰყავდა პირი, რომელიც სკოლაში პარალელურად დასაქმებული იყო ფორტეპიანოს პედაგოგისა და სავიოლინო და საგუნდო განყოფილების კონცერტმეისტერის პოზიციაზე. ინტერესთა კონფლიქტის შესაძლო არსებობის შეფასებისას, პერსონალურ მონაცემთა დაცვის სამსახურმა მხედველობაში მიიღო ის გარემოება, რომ პედაგოგიური საქმიანობის ფარგლებში, მასწავლებლები, როგორც ფორმალურ, საგაკვეთილო პროცესში, ისე არაფორმალურ გარემოში, მუდმივად მონაწილეობენ მონაცემების დამუშავებაში. გარდა ამისა, სკოლის თითოეული პედაგოგი, წარმოადგენს სკოლის პედაგოგიური საბჭოს წევრს. თავის მხრივ, პედაგოგიური საბჭო არის სკოლაში შექმნილი კოლეგიური ორგანო, რომელიც გადაწყვეტილებას იღებს მიმდინარე/განსახორციელებელ მნიშვნელოვან ღონისძიებებზე, როგორიცაა სამუშაო და სასწავლო გეგმები, რაც თავის მხრივ, მოიცავს მონაცემთა დამუშავების მრავალმხრივ პროცესებს.

შესაბამისად, პერსონალურ მონაცემთა დაცვის სამსახურმა დაადგინა, რომ რამდენადაც პერსონალურ მონაცემთა დაცვის ოფიცრად განსაზღვრული პირი ამავდროულად იყო სკოლის პედაგოგი, რომელიც უშუალოდ მონაწილეობდა სკოლის მიზნების შესრულებაში და სკოლაში მონაცემთა დამუშავებასთან დაკავშირებული კონკრეტული პროცესების დაგეგმვაში, სახეზე იყო ინტერესთა კონფლიქტი.

შემოწმების ფარგლებში ასევე გამოირკვა, რომ პერსონალურ მონაცემთა დაცვის ოფიცრად განსაზღვრული პირი არ ფლობდა მონაცემთა დაცვის სფეროს მარეგულირებელი კანონმდებლობის შესახებ საბაზისო ცოდნას. აღნიშნული მიმართულებით მას არც დაწესებულებისგან ჰქონდა რაიმე ინფორმაცია მიღებული და არც რაიმე სასწავლო კურსი ჰქონდა გავლილი, რაც ოფიცრად განსაზღვრული პირის კომპეტენციასთან მიმართებით კანონმდებლობით განსაზღვრულ წესთან შეუსაბამობაზე მიანიშნებდა.

სამსახურის გადაწყვეტილებით სკოლას დაევალა პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნა ინტერესთა კონფლიქტთან და სათანადო ცოდნასთან დაკავშირებით კანონით განსაზღვრული მოთხოვნების დაცვით.

- **სენაკის მუნიციპალიტეტის საკრებულო**

სამსახურის მიერ ასევე შემოწმდა სენაკის მუნიციპალიტეტის საკრებულოს მიერ პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული ვალდებულების შესრულების ფაქტი. საკრებულოს, როგორც საჯარო დაწესებულებას, ასევე გააჩნია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრული ხსენებული ვალდებულება.

შემოწმების შედეგად დადგინდა, რომ საკრებულოს პერსონალურ მონაცემთა დაცვის ოფიცრად განსაზღვრული ჰყავდა საკრებულოს აპარატის უფროსი ისე, რომ იგი არ იყო გათავისუფლებული მისი ძირითადი ფუნქცია-მოვალეობებისგან. კერძოდ, გამოირკვა, რომ ოფიცრად განსაზღვრული პირი, როგორც აპარატის უფროსი, ახდენდა მის დაქვემდებარებაში მყოფი თანამშრომლების მიერ მომზადებული წერილობითი კორესპონდენციის შეთანხმებას და მის ვიზირებას. ასევე დადგინდა, რომ აღნიშნული პირი მის დაქვემდებარებაში მყოფი იურიდიული მიმართულების სპეციალისტის მიერ საკრებულოს ინტერესების სასამართლოში დაცვის შემთხვევაში, თავადაც ჩართული იყო სასამართლოში წარსადგენი მტკიცებულებების სახისა და მოცულობის შესახებ გადაწყვეტილებების მიღებაში. ამასთან, საკრებულოს დებულების მიხედვით, აპარატის უფროსის ფუნქციები დაკავშირებული იყო რიგი მმართველობითი გადაწყვეტილებების მიღებასთან, რაც პერსონალური მონაცემების დამუშავების საკითხების გადაწყვეტასაც გულისხმობს. მაგალითად, აღნიშნული პირის, როგორც აპარატის უფროსის ფუნქციები მოიცავდა თანამდებობაზე დასანიშნად და თანამდებობიდან გასათავისუფლებლად აპარატის შესაბამისი მოხელეების საკრებულოს თავმჯდომარისთვის წარდგენას, რაც დაკავშირებული იყო შესაბამისი ადმინისტრაციული ხასიათის გადაწყვეტილებების მისაღებად საჭირო პერსონალური მონაცემების მოცულობის განსაზღვრასთან, მათი მოპოვების და გამოყენების ზედამხედველობასთან. ოფიცრად განსაზღვრული პირის უფლებამოსილებები ასევე მოიცავდა ხელმძღვანელის როლით ჩართვას სხვადასხვა საორგანიზაციო პროცესში, მათ შორის მოსახლეობასთან და მედიასთან შეხვედრების დაგეგმვა/განხორციელებაში, დაწესებულებაში შექმნილი სხვადასხვა კომისიის მუშაობაში მონაწილეობას, საკადრო დოკუმენტაციის სრულყოფილად წარმოებასთან და საჯარო ინფორმაციის პროაქტიულად გამოქვეყნებასთან დაკავშირებული საკითხების გადაწყვეტას.

აღნიშნულის გათვალისწინებით, პერსონალურ მონაცემთა დაცვის სამსახურმა დაადგინა, რომ პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციების შეთავსება პირისთვის, რომელიც პარალელურად ასრულებს აპარატის უფროსისთვის

განსაზღვრულ ზემოაღნიშნულ ფუნქციებს, რის ფარგლებშიც ჩართულია მონაცემთა დამუშავების მნიშვნელოვან პროცესებში და აქვს მათთან დაკავშირებული გადაწყვეტილებების მიღების შესაძლებლობა, ქმნის ინტერესთა კონფლიქტს.

სამსახურმა ასევე დაადგინა, რომ პერსონალურ მონაცემთა დაცვის ოფიცრის ვინაობა და საკონტაქტო მონაცემები საკრებულოს ვებგვერდზე გამოქვეყნებული იყო საკრებულოს აპარატის სხვა თანამშრომლების შესახებ ინფორმაციას შორის და დაინტერესებული პირი მის მოძიებას მხოლოდ ვებგვერდის დეტალურად დათვალიერების შემთხვევაში შეძლებდა.

სამსახურის გადაწყვეტილებით საკრებულოს დაევალა პერსონალურ მონაცემთა დაცვის ოფიცრად ისეთი პირის საქმიანობის უზრუნველყოფა, რომელსაც თავისი უფლებამოსილებების განხორციელების პროცესში არ ექნებოდა ინტერესთა კონფლიქტი. ამასთან, საკრებულოს ასევე დაევალა ოფიცრის ვინაობისა და საკონტაქტო მონაცემების გამოქვეყნება საზოგადოებისთვის ადვილად ხელმისაწვდომი, სხვა ინფორმაციისგან განცალკევებული ფორმით.

მის.: საქართველო, თბილისი, ნ. ვაჩნაძის №7, 0105
ბათუმი, ბაქოს ქუჩა, №48, 6010
www.pdps.ge
ტელ.: (+995 32) 242 1000
E-mail: office@pdps.ge