პერსონალურ მონაცემთა
დაცვის ინსპექტორის აპარატი

პერსონალური მონაცემების დაცვის მინიმალური მოთხოვნები

დოკუმენტი განკუთვნილია საჯარო დაწესებულებებისთვის და მიზნად ისახავს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის იმპლემენტაციის, ევროპის კავშირთან სავიზო რეჟიმის ლიბერალიზაციის სამოქმედო გეგმის მეორე ფაზით გათვალისწინებული ვალდებულებების შესრულების ხელშეწყობასა და შემფასებელი მისიის ვიზიტისათვის მომზადებას.

1. პერსონალურ მონაცემთა დაცვის შიდა სტანდარტები და რეგულაცია

ვინაიდან „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ადგენს პერსონალურ მონაცემთა დაცვის ზოგად სტანდარტს, საჯარო დაწესებულებას, მისი კომპეტენციისა და სპეციფიკის გათვალისწინებით, შემუშავებული უნდა ჰქონდეს **შიდა დოკუმენტი (პოლიტიკა, ინსტრუქცია, დებულება, სახელმძღვანელო წესები)**, რომელშიც გაწერილი იქნება მის ხელთ არსებული პერსონალური მონაცემების (მონაცემთა ბაზები/ ფაილური სისტემები, საშვთა ბიუროს მონაცემები, არქივი, საქმისწარმეობის პროგრამაში არსებული მონაცემები და ა.შ.) **დამუშავების წესი და უსაფრთხოების ორგანიზაციულ-ტექნიკური ზომები.**[1] შიდა რეგულაციის სტრუქტურა დამოკიდებულია დამუშავებული პერსონალურ მონაცემების მოცულობასა და კატეგორიაზე.

შიდა დოკუმენტი მიზნად უნდა ისახავდეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილ ვალდებულებებთან სრული შესაბამისობის მიღწევას და **შესასრულებლად სავალდებულო** უნდა იყოს ყველა თანამშრომლისთვის, რომელიც ჩართული ან პასუხისმგებელია მონაცემთა დამუშავებაზე. ამასთან, დოკუმენტი უნდა ითვალისწინებდეს შიდა კონტროლის მექანიზმსა და პასუხისმგებლობას მისი დარღვევისათვის.

2. თანამშრომლების ინფორმირებულობა და ცნობიერების დონე

უწყების ყველა თანამშრომელი, რომელიც ჩართულია პერსონალური მონაცემების დამუშავების პროცესში (თუნდაც მინიმალური შეხება ჰქონდეს პერსონალური მონაცემების შემცველ ბაზასთან), ინფორმირებული უნდა იყოს კანონისა და შიდა რეგულაციის შესახებ,

[1] თუ უსაფრთხოების წესები უკვე ამომწურავად არ არის გაწერილი ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტში, რომელიც „ინფორმაციული უსაფრთხოების შესახებ“ კანონის საფუძველზე არის მიღებული.

უნდა შეეძლოს პასუხის გაცემა კითხვაზე, თუ რა მიზნით, რა საფუძვლით და რა ვადით ხდება პერსონალური მონაცემების დამუშავება. *მაგალითად, ამა თუ იმ ორგანიზაციის საშვთა ბიუროს თანამშრომელმა უნდა იცოდეს, რა მიზანს ემსახურება მის მიერ პერსონალური მონაცემების დამუშავება, მათ შორის, მონაცემთა გადამოწმება სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ელექტრონულ გაზაში და რა ვადით ინახება ეს მონაცემები.*

ამ მიზნით ორგანიზაციის შიგნით შექმნილი დოკუმენტი მაქსიმალურად მარტივი და გასაგები უნდა იყოს თანამშრომლებისა და გარე პარტნიორებისათვის. დოკუმენტის მოცულობა, სტრუქტურა და სირთულე, როგორც წესი, პირდაპირპროპორციულია პერსონალურ მონაცემთა იმ ოდენობისა ან/და კატეგორიებისა, რომელსაც ორგანიზაცია ამუშავებს.

3. მონაცემთა დამუშავების მიზანი და საჭიროება

საჯარო დაწესებულებამ უნდა განსაზღვროს მონაცემთა **დამუშავების მკაფიო და კონკრეტული მიზანი** *(მაგალითად, მოქალაქის განცხადების განხილვა, ამა და ამ კანონით განსაზღვრული ვალდებულების შესრულება და ა.შ.)*. მიზანი არ შეიძლება იყოს აბსტრაქტული და ზოგადი ხასიათის. *მაგალითად, მოქალაქეს, რომელმაც განცხადებით მიმართა საჯარო დაწესებულებას, სთხოვენ მისთვის საპასუხო წერილის გაგზავნისა თუ დამატებითი ინფორმაციის მიღების მიზნით მიუთითოს მისამართი და ტელეფონის ნომერი.* გარდა იმისა, რომ უწყებას უნდა ჰქონდეს ამ ინფორმაციის შეგროვების მიზანი *(დასახელებულ მაგალითში: მოქალაქის განცხადებაზე რეაგირება),* მან მოქალაქეს უნდა განუმარტოს, რატომ ხდება ამ ინფორმაციის მოთხოვნა.

მონაცემთა დამმუშავებელმა დეტალურად უნდა განსაზღვროს, **რა სახის და რა მოცულობის** მონაცემთა დამუშავებაა **აუცილებელი კონკრეტული მიზნის მისაღწევად**. დამუშავებული პერსონალური მონაცემები უნდა იყოს იმ მიზნის **ადეკვატური და პროპორციული,** რომლის მისაღწევადაც ისინი გროვდება/მუშავდება. დაუშვებელია ზედმეტი ინფორმაციის შეგროვებ/შენახვა. *მაგალითად, განცხადების განმხილველმა ადმინისტრაციულმა ორგანომ არ უნდა შეაგროვოს განმცხადებლის შემოსავლის ან ოჯახის წევრების შესახებ ინფორმაცია, თუ მოქალაქის განცხადების განხილვისთვის ეს ინფორმაცია აუცილებელი არ არის.*

4. მონაცემთა დამუშავების საფუძველი

თითოეული მონაცემთა დამმუშავებელი უნდა დარწმუნდეს, რომ ის მონაცემთა დამუშავებას ახდენს **„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული მონაცემთა დამუშავების ერთ-ერთი საფუძვლით (კანონის მე-5 მუხლი)**. ნებისმიერმა თანამშრომელმა, რომელიც უშუალოდაა ჩართული დამუშავების პროცესში, უნდა იცოდეს, რა სამართლებრივი საფუძვლით ხდება ინფორმაციის დამუშავება. *მაგალითად, სსიპ სოციალური მომსახურების სააგენტო მოქალაქის განცხადების (მონაცემთა*

სუბიექტის თანხმობა) განხილვისა და შესაბამისი გადაწყვეტილების მიღების მიზნით ახდენს მისი მონაცემების დამუშავებას; ცესკო საქართველოს ორგანული კანონით „საარჩევნო კოდექსი“ მასზე დაკისრებული მოვალეობების შესასრულებლად ამუშავებს მოქალაქეთა პერსონალურ მონაცემებს; სსიპ საჯარო რეესტრი ვებგვერდზე ასაჯაროებს უძრავ ქონებასთან დაკავშირებული უფლებების რეგისტრაციის დროს შეგროვებულ მონაცემებს „საჯარო რეესტრის შესახებ“ საქართველოს კანონის საფუძველზე.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, განსაკუთრებული კატეგორიის მონაცემების დამუშავება აკრძალულია, თუმცა ამავე მუხლის მე-2 პუნქტით განსაზღვრულია ის გამონაკლისი შემთხვევები, როდესაც შესაძლებელია ამ კატეგორიის მონაცემთა დამუშავება. შესაბამისად, ამა თუ იმ დაწესებულების მიერ განსაკუთრებული კატეგორიის მონაცემების დამუშავება უნდა შეესაბამებოდეს დადგენილი გამონაკლისებიდან ერთ-ერთს მაინც. *მაგალითად, საჯარო დაწესებულება უფლებამოსილია „საჯარო სამსახურის შესახებ“ საქართველოს კანონის საფუძველზე საჯარო მოხელის დანიშვნამდე კანდიდატს მოსთხოვოს ნასამართლობის შესახებ ცნობის წარმოდგენა.*

5. მონაცემთა შენახვის ვადა

პერსონალური მონაცემების შენახვისას, ისევე როგორც პერსონალური მონაცემების დამუშავების სხვა შემთხვევებში, აუცილებელია კანონით გათვალისწინებული პრინციპების დაცვა. იმ შემთხვევაში, თუ მონაცემთა შენახვის ვადა კანონმდებლობით არ არის განსაზღვრული, უწყებამ თავად უნდა განსაზღვროს მის შიგნით დამუშავებული მონაცემების (როგორც ქაღალდზე, ისე - ელექტრონულ სახით არსებული მონაცემების), შენახვის ვადა. მონაცემები შენახულ უნდა იქნას იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა დაიბლოკოს, წაიშალოს ან განადგურდეს ან შენახულ იქნას პირის იდენტიფიცირების გამომრიცხავი ფორმით. მნიშნელოვანია, განისაზღვროს შესაბამისი ვადის გასვლის შემდგომ პერსონალური მონაცემების წაშლის, განადგურების ან დეპერსონალიზაციის მეთოდები და საშუალებები. გასათვალისწინებელია, რომ პერსონალურ მონაცემთა განადგურება ყოველთვის არ არის აუცილებელი, რადგანაც არსებობს მონაცემთა დეპერსონალიზაციის რამდენიმე ალტერნატიული საშუალება (მაგალითად, ანონიმიზაცია, ფსევდონიმით ან კრიპტოგრაფიული მეთოდით გარდაქმნა იდენტიფიკაციის გამომრიცხველი ფორმატით), რომელიც მონაცემთა სუბიექტის უფლებათა დაცვის თვალსაზრისით იგივე შედეგების მომტანია, როგორც მონაცემთა წაშლა.

6. მონაცემთა ნამდვილობა და სიზუსტე

საჯარო დაწესებულება პასუხისმგებელია დამუშავებული პერსონალური მონაცემების სისწორეზე. შესაბამისად, თუ მისთვის ცნობილი გახდა მონაცემთა განახლების შესახებ, ის ვალდებულია, განაახლოს მასთან არსებული ინფორმაცია და ასევე უზრუნველყოს ამ ინფორმაციის განახლება იმ შემთხვევაში, თუ კი მონაცემთა დამუშავების პროცესში

ჩართულია სხვა უწყება. *მაგალითად, მოქალაქემ საიდენტიფიკაციო დოკუმენტებში ცვლილების შესახებ ინფორმაცია მიაწოდა იმ დაწესებულებას, სადაც განიხილება მისი ადმინისტრაციული საჩივარი. ადმინისტრაციულმა ორგანომ უნდა განაახლოს მასთან დაცული ინფორმაცია.*

7. ვიდეოთვალთვალის განხორციელება, ბიომეტრული მონაცემების დამუშავება

იმ შემთხვევაში, თუ ორგანიზაცია ამუშავებს ისეთ პერსონალურ მონაცემების, როგორიცაა ვიდეო/აუდიო ჩანაწერები და ბიომეტრული მონაცემები, განსაზღვრული უნდა იყოს **ამ ტიპის მონაცემების დამუშავების წესი.**

მონაცემთა დამმუშავებლის მიერ **ვიდეოთვალთვალის** სისტემის გამოყენების შემთხვევაში, ორგანიზაციის მიერ მონაცემთა დაცვასთან დაკავშირებით შემუშავებულ დოკუმენტში გათვალისწინებული უნდა იყოს შემდეგი საკითხები:

- ვიდეოთვალთვალის სისტემის გამოყენების მიზანი და პირობები.
- ვიდეო/აუდიო ჩანაწერების შენახვის ვადა;
- სად და რა ფორმით უნდა მოხდეს გამაფრთხილებელი ნიშნების განთავსება; აუდიო ჩანაწერის მიმდინარეობისას უზრუნველყოფილი უნდა იყოს განსხვავებული გამაფრთხილებელი ნიშნის არსებობა;
- განსაზღვრული უნდა იყოს იმ თანამშრომელთა ნუსხა, რომლებსაც წვდომა აქვთ ვიდეოთვალთვალის შედეგად მოპოვებულ ჩანაწერებზე. ასევე, რა შემთხვევაშია შესაძლებელი ვიდეო ჩანაწერის მესამე პირისათვის გადაცემა;
- ვიდეოთვალთვალის სისტემის უსაფრთხოების გარანტიები და უსაფრთხოებაზე პასუხისმგებელი პირები.

დოკუმენტში გაწერილი უნდა იყოს ვიდეოთვალთვალის განხორციელების კანონით გათვალისწინებული მიზანი, ხაზგასმული უნდა იყოს სისტემის სხვა მიზნით გამოყენების დაუშვებლობა.

მონაცემთა დამმუშავებლის მიერ შენობის ვიდეოთვალთვალის განხორციელებისას, კანონის მოთხოვნების შესაბამისად, უნდა შეიქმნას **ვიდეოჩანაწერების შენახვისათვის განკუთვნილი ფაილური სისტემა**.[2]

თუ ორგანიზაცია ამუშავებს **ბიომეტრულ მონაცემებს,** აუცილებელია, განსაზღვროს ამ მონაცემების დამუშავების მიზანი. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, საჯარო დაწესებულების მიერ ბიომეტრული მონაცემების დამუშავება შესაძლებელია მხოლოდ პირის უსაფრთხოებისა და საკუთრების დაცვის მიზნებისათვის, აგრეთვე საიდუმლო ინფორმაციის გამჟღავნების თავიდან აცილების მიზნით. თითოეულმა

[2] დეტალური ინფორმაციისათვის იხილეთ რეკომენდაციები ვიდეოთვალთვალის განხორციელების შესახებ: http://personaldata.ge/res/docs/recommendation/video%20surviellance-recommendation-final.pdf.

მონაცემთა დამმუშავებელმა, რომელიც აღნიშნული მიზნებისათვის ახდენს ბიომეტრული მონაცემების დამუშავებას, უნდა დაასაბუთოს, რომ აღნიშნული მიზნის მიღწევა სხვა საშუალებით შეუძლებელია ან/და დაკავშირებულია დიდ ძალისხმევასთან. *მაგალითად, დაწესებულებამ, რომელიც არ წარმოადგენს* კრიტიკული ინფორმაციული ინფრასტრუქტურის ნაწილს, *არ უნდა მოახდინოს თანამშრომელთა შენობაში შესვლისა და შენობიდან გასვლის აღრიცხვის მიზნით მათი ბიომეტრული მონაცემების დამუშავება.*

საჯარო დაწესებულების მიერ მკაცრად უნდა იყოს შემოფარგლული იმ პირთა წრე, ვისაც წვდომა აქვს ბიომეტრულ მონაცემებზე და ასევე, დადგენილი უნდა იყოს ამ სახის მონაცემთა უსაფრთხოების ზომები.

8. მონაცემთა უსაფრთხოების სტანდარტი

მონაცემთა უსაფრთხოება გულისხმობს ორგანიზაციის ოპერაციული, ფუნქციური და სტრატეგიული კონტროლის მექანიზმების გამოყენებას, რომელიც ემსახურება პერსონალურ მონაცემთა მთლიანობის, კონფიდენციალობისა და ხელმისაწვდომობის დაცვას.

პერსონალურ მონაცემთა და მონაცემთა დამუშავების სისტემების **უსაფრთხოების** მინიმალური სტანდარტი შეიძლება არსებობდეს როგორც ცალკე დოკუმენტის სახით, ისე წარმოადგენდეს პერსონალურ მონაცემთა დაცვის შიდა პოლიტიკის ნაწილს. უსაფრთხოების სტანდარტი მორგებული უნდა იყოს დაწესებულების საქმიანობის სპეციფიკასა და მის მიერ დამუშავებული პერსონალური მონაცემების კატეგორიაზე. აღნიშნულ დოკუმენტში დეტალურად უნდა გაიწეროს:

- მონაცემთა დამუშავებასთან დაკავშირებული რისკები;
- ფიზიკური და ტექნიკური უსაფრთხოების ზომები, მათ შორის ინფორმაციული ტექნოლოგიების უსაფრთხოება;
- პერსონალური მონაცემების შემცველ ბაზებზე თანამშრომელთა დაშვება და დაშვების დონეები;
- კონტროლის მექანიზმები;
- პასუხისმგებლობა უსაფრთხოების ზომების უგულებელყოფისთვის.

კონტროლის მექანიზმები უნდა პასუხობდეს ისეთ რისკებს, როგორებიცაა მონაცემზე არასანქცირებული წვდომა, მონაცემთა განადგურება, უკანონო გამოყენება, ცვლილება, გახმაურება ან დაკარგვა, ასევე, სხვა მნიშვნელოვან საფრთხეებს, რომელიც რისკის შეფასების პროცესში დადგინდა და განისაზღვრა პრიორიტეტულად.

9. მონაცემთა სუბიექტის უფლებების დაცვა

პერსონალური მონაცემების დაცვის უზრუნველსაყოფად და კანონის მოთხოვნების პრაქტიკაში დასანერგად მნიშვნელოვანია იმ პირთა უფლებების დაცვა, ვისი პერსონალური მონაცემებიც მუშავდება. ორგანიზაციის ყველა თანამშრომელი ინფორმირებული უნდა იყოს

მონაცემთა სუბიექტის უფლებებისა და მონაცემთა დამმუშავებლის ვალდებულებების შესახებ.

ეფექტურობის მისაღწევად, სასურველია, ორგანიზაციებმა შეიმუშაონ მონაცემთა სუბიექტის უფლებების რეალიზების ეფექტური მექანიზმი (მაგალითად ცალკე განცხადების ფორმა, ცხელი ხაზი, მონაცემთა დაცვის საკითხებზე პასუხისმგებელი პირის განსაზღვრა და სხვა), რათა სწრაფად და კანონით დადგენილ ვადებში მოხდეს სუბიექტისათვის ინფორმაციის მიწოდება, მონაცემთა დამუშავების ხარვეზების აღმოფხვრა და აუცილებლობის შემთხვევაში - მონაცემთა დამუშავების შეწყვეტა/დაბლოკვა.