USAID
ამერიკელი ხალხისგან

პერსონალურ მონაცემთა
დაცვის სამსახური

მინიმალური სტანდარტი
პერსონალურ მონაცემთა დაცვის ოფიცრებისთვის

თბილისი, 2024

წინამდებარე დოკუმენტი მომზადდა ამერიკის შეერთებული შტატების საერთაშორისო სააგენტოს (USAID) ფინანსური მხარდაჭერით. დოკუმენტის შინაარსზე პასუხისმგებელია „პერსონალურ მონაცემთა დაცვის სამსახური“ და იგი შესაძლოა, არ ასახავდეს USAID-ის და ამერიკის შეერთებული შტატების მთავრობის შეხედულებებს.

სარჩევი

რეკომენდაციების მიზანი

წინამდებარე რეკომენდაციების მიზანია, უზრუნველყოს მონაცემთა დაცვის ოფიცრების შერჩევისა და მომზადების მინიმალური სტანდარტები, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად. საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის ნორმატიულ აქტებთან და რეკომენდაციებთან ერთად, წინამდებარე რეკომენდაციების მიზანია მონაცემთა დაცვის პრაქტიკის გაუმჯობესება, პირადი ცხოვრების უფლების დაცვა და კანონთან შესაბამისობის უზრუნველყოფა.

წინამდებარე დოკუმენტი უზრუნველყოფს მკაფიო და სტანდარტიზებულ მიდგომებს, რომლებსაც ორგანიზაციები გამოიყენებენ მონაცემთა დაცვის ოფიცრების დანიშვნისას ან განსაზღვრისას. გარდა ამისა, დოკუმენტი, მონაცემთა დაცვის ოფიცრებისთვის, განსაზღვრავს მინიმალურ მოთხოვნებს ცოდნის, უნარებისა და პიროვნული მახასიათებლების კუთხით. ამასთან, წინამდებარე დოკუმენტი განკუთვნილია მონაცემთა დაცვის ოფიცრების მომზადებისთვის შემუშავებული ტრენინგების შესაბამისობისა და ხარისხის უზრუნველყოფისთვის.

რეკომენდაციები შემუშავებულია ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაციის გათვალისწინებით და შეესაბამება ხარისხისა და პროფესიონალიზმის ევროპულ სტანდარტებს. მისი მიზანია, უზრუნველყოს მონაცემთა დაცვის ოფიცრებისა და მათთვის განკუთვნილი სასწავლო პროგრამების ეფექტურობა, შესაბამისობა და მაღალი ხარისხი. აღნიშნული სტანდარტი დაეხმარებათ პერსონალურ მონაცემთა დაცვის ოფიცრებს ეფექტიანად უზრუნველყონ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნათა დაცვა.

მეთოდოლოგია

რეკომენდაციები შედგენილია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიზნებისა და მოთხოვნების შესაბამისად. რეკომენდაციები ასევე, ითვალისწინებს საუკეთესო საერთაშორისო პრაქტიკასა და დაინტერესებული მხარეების მოსაზრებებს.

ახალი კანონის მიღებითა და მისი მოქმედებით, საქართველო უერთდება იმ მსოფლიო იურისდიქციების რიგს, რომლებიც აღიარებენ მონაცემთა დაცვის ოფიცრების უმნიშვნელოვანეს როლს ორგანიზაციის მიერ პერსონალური მონაცემების გამოყენების მართლზომიერად წარმართვაში. ევროკავშირის წევრი ქვეყნების გარდა, რომლებშიც მონაცემთა დაცვის ძირითადი რეგულაცია (შემდგომში “GDPR”) მოქმედებს, მონაცემთა დაცვის ოფიცრის ინსტიტუტი ასევე აქტუალურია ავსტრალიაში, ბრაზილიაში, სინგაპურში, დიდ ბრიტანეთსა და ბევრ სხვა ქვეყანაში.

რეკომენდაციები შემუშავებულია მონაცემთა დაცვაზე საზედამხედველო ორგანოების საუკეთესო პრაქტიკაზე დაყრდნობით, მათ შორის:

- 29-ე სამუშაო ჯგუფის სახელმძღვანელო პრინციპები მონაცემთა დაცვის ოფიცრების შესახებ (დამტკიცებულია მონაცემთა დაცვის ევროპული საბჭოს მიერ)
- „ევროკავშირის მონაცემთა დაცვის ზედამხედველის“ პოზიცია მონაცემთა დაცვის ოფიცრის როლის თაობაზე
- “CNIL”-ის სახელმძღვანელო მონაცემთა დაცვის ოფიცრების შესახებ
- “ICO”-ის გზამკვლევი მონაცემთა დაცვის ოფიცრების შესახებ

რეკომენდაციებში გათვალისწინებულია წამყვანი საერთაშორისო ორგანიზაციების (როგორებიცაა: Microsoft, Mastercard და მსოფლიო ბანკი) მოსაზრებები მონაცემთა დაცვის ოფიცრებისთვის საჭირო კვალიფიკაციისა და უნარების შესახებ. გარდა ამისა, ეს რეკომენდაციები ეფუძნება საუკეთესო პრაქტიკას, რომლითაც ხელმძღვანელობს „IAPP“ და „CIPL“.

გარდა ამისა, რეკომენდაციებზე გავლენა მოახდინა მონაცემთა დაცვის ოფიცრის როლის შესახებ შემდეგი დაინტერესებული მხარეების მიერ გამოთქმულმა შეხედულებებმა და მოსაზრებებმა:

- პერსონალურ მონაცემთა დაცვის სამსახური;
- ევროკომისიის საერთაშორისო ციფრული თანამშრომლობის პროექტი;
- სამართლისა და საჯარო პოლიტიკის ცენტრი;
- ელექტრონული კომერციის ასოციაცია;
- გრიგოლ რობაქიძის სახელობის უნივერსიტეტი;
- ინფორმაციის თავისუფლების განვითარების ინსტიტუტი;
- იურიდიული სწავლების ცენტრი “LS”;
- საქართველოს ბანკი;

- განათლების ხარისხის განვითარების ეროვნული ცენტრი;
- სახელმწიფო სერვისების განვითარების სააგენტო.

შესავალი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიზანია, უზრუნველყოს პერსონალური მონაცემების დამუშავებისას ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის დაცვა.“[1] ამ მიზნის მისაღწევად, კანონი ორგანიზაციებს განუსაზღვრავს ვალდებულებას, რომ მონაცემები დაამუშაონ კანონიერად, კეთილსინდისიერად და მონაცემთა სუბიექტების უფლებების ჯეროვანი გათვალისწინებით. ორგანიზაციები ვალდებულნი არიან, მიიღონ შესაბამისი ტექნიკური და ორგანიზაციული ზომები, რათა უზრუნველყონ მონაცემთა კანონის შესაბამისად დამუშავება. ამასთან, კანონის მოთხოვნებთან შესაბამისობის დასადასტურებლად, ორგანიზაციებმა უნდა აწარმოონ შესაბამისი დოკუმენტაცია.

კანონი საჯარო დაწესებულებებს, კონკრეტულ სფეროებში საქმიანობის განმახორციელებელ სუბიექტებს, აგრეთვე, იმ დამუშავებისთვის პასუხისმგებელ პირს/დამუშავებაზე უფლებამოსილ პირს, რომელიც ამუშავებს დიდი რაოდენობით სუბიექტების მონაცემებს ან ახორციელებს მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს, ავალდებულებს, დანიშნონ ან განსაზღვრონ მონაცემთა დაცვის ოფიცერი. ამასთანავე, კანონი ადგენს მონაცემთა დაცვის ოფიცრის ძირითად პასუხისმგებლობებს და განსაზღვრავს, ვის წინაშე უნდა იყოს მონაცემთა დაცვის ოფიცერი ანგარიშვალდებული ორგანიზაციის ფარგლებში. კანონი ასევე ადგენს მონაცემთა დამუშავებასთან დაკავშირებით ორგანიზაციის მიერ გადაწყვეტილებების მიღების პროცესში მონაცემთა დაცვის ოფიცრის ჩართულობის აუცილებლობას.

პერსონალურ მონაცემთა დაცვის ოფიცერს უნდა ჰქონდეს „სათანადო ცოდნა მონაცემთა დაცვის სფეროში.“[2] ამ სტანდარტის დაკმაყოფილების მიზნით, საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის მოთხოვნის თანახმად, პირს, რომელიც მონაცემთა დაცვის ოფიცრად ინიშნება ან განისაზღვრება, უნდა გააჩნდეს (ან დანიშვნიდან/განსაზღვრიდან უმოკლეს დროში უნდა შეიძინოს) შემდეგი:

- კანონის სიღრმისეული ცოდნა;
- მონაცემთა დაცვის ოფიცრისთვის განსაზღვრული კონკრეტული დავალებების შესასრულებლად აუცილებელი უნარები;
- პიროვნული თვისებები, რათა ხელი შეუწყოს, მხარი დაუჭიროს და მიაღწიოს ორგანიზაციის შესაბამისობას კანონის მოთხოვნებთან;
- კანონთან შესაბამისობის დასადასტურებლად საჭირო დოკუმენტაციის ცოდნა (და ორგანიზაციის შეხედულებისამებრ, ამ დოკუმენტაციის შექმნა).

მონაცემთა დაცვის ოფიცერს ასევე უნდა ჰქონდეს საბაზისო ცოდნა საინფორმაციო ტექნოლოგიების, მონაცემთა უსაფრთხოებისა და ხელოვნური ინტელექტის სფეროებში; უნდა იცნობდეს ორგანიზაციის საქმიანობას, მის ორგანიზაციულ

[1] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 1.
[2] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 33(5).

სტრუქტურასა და დარგის რეგულაციებს, ხოლო საჯარო დაწესებულებებში საქმიანობის შემთხვევაში, დეტალურად უნდა იცნობდეს ამ დაწესებულებების საქმიანობის მარეგულირებელ საკანონმდებლო და კანონქვემდებარე აქტებს.

ქვემოთ მოცემული არასავალდებულო მინიმალური სტანდარტები გამიზნულია მონაცემთა დაცვის ოფიცრის შერჩევისა და შესაბამისი ტრენინგის სახელმძღვანელოდ გამოსაყენებლად.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ზოგადი მიმოხილვა

პერსონალური მონაცემების დაცვისა და პირადი ცხოვრების ხელშეუხებლობის სტანდარტებისა და გარანტიების განმტკიცების მიზნით, საქართველოს პარლამენტმა 2023 წლის 14 ივნისს მიიღო კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, რომლის ძირითადი ნაწილი მიმდინარე წლის 1 მარტს შევიდა ძალაში. ახალი კანონი ადგენს პერსონალური მონაცემების დაცვის საერთაშორისოდ აღიარებულ სტანდარტებს, რაც მნიშვნელოვანი ნაბიჯია ევროპის კანონმდებლობასთან ჰარმონიზაციის მიმართულებით. იგი განსაზღვრავს საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის, როგორც სახელმწიფო ორგანოს, ინსტიტუციურ დამოუკიდებლობას და ადგენს მთელ რიგ ახალ ინსტიტუტებსა და საკანონმდებლო ინოვაციებს.

პერსონალური მონაცემების დაცვასთან დაკავშირებული საკანონმდებლო ბაზის ჰარმონიზაციისა და კონსოლიდაციის ვალდებულება საქართველომ ევროკავშირთან ასოცირების შეთანხმებისა და ასოცირების პროგრამის ფარგლებში იკისრა. საქართველოსთვის, როგორც ევროპული სამართლებრივი კულტურისა და ევროინტეგრაციის პროცესში მყოფი ქვეყნისთვის, უაღრესად მნიშვნელოვანია პერსონალური მონაცემების დაცვის შესახებ საქართველოს კანონმდებლობის ევროკავშირის კანონმდებლობასთან ჰარმონიზაცია და შესაბამისად, ახალი დემოკრატიული სტანდარტების დანერგვა ეროვნულ დონეზე. ახალ კანონში ინტეგრირებულია “GDPR”-ის ღირებულებები და სტანდარტები. „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის დანერგვის შედეგად, პერსონალური მონაცემების დაცვის საკანონმდებლო ბაზა ევროკავშირის კანონმდებლობის შესაბამისი იქნება. აღნიშნული უზრუნველყოფს ადამიანის უფლებებისა და თავისუფლებების, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის ეფექტიან დაცვას პერსონალური მონაცემების დამუშავებისას, ასევე, მონაცემთა დაცვის დამოუკიდებელი საზედამხედველო ორგანოს შესაბამისი მექანიზმებითა და უფლებამოსილებებით აღჭურვას.

ახალი კანონი მნიშვნელოვნად ზრდის მონაცემთა სუბიექტების უფლებებს და აფართოებს მათი დაცვის გარანტიებს. საკანონმდებლო სიახლეები ასევე ეხება, მათ შორის, პირდაპირი მარკეტინგის მიზნით მონაცემების დამუშავების წესებს. გარდა ამისა, ახალი კანონი ასევე ითვალისწინებს აუდიო მონიტორინგის გზით მონაცემთა დამუშავების პროცესის მარეგულირებელ სპეციალურ დებულებებს, ადგენს კონკრეტულ სამართლებრივ საფუძვლებსა და მოთხოვნებს.

ევროკავშირის “GDPR”-ის შესაბამისად, საქართველოს კანონი ადგენს საჯარო დაწესებულებებსა და კერძო ორგანიზაციებში პერსონალური მონაცემების დაცვის ოფიცრის დანიშვნის ან განსაზღვრის ვალდებულებას, განსაზღვრავს ოფიცრის ცნებას და აწესრიგებს მასთან დაკავშირებულ სხვა ძირითად საკითხებს.

პერსონალურ მონაცემთა დაცვის ოფიცერი

2018 წელს, ევროკავშირში „მონაცემთა დაცვის ძირითადი რეგულაციის“ ძალაში შესვლის შემდეგ,[3] მონაცემთა დაცვის ოფიცრის როლმა საკვანძო მნიშვნელობა შეიძინა ორგანიზაციის პერსონალური მონაცემების მართვაში. ქვემოთ შეჯამებულია მონაცემთა დაცვის ოფიცრის ის პასუხისმგებლობები, რომლებიც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით არის განსაზღვრული.

სუბიექტები, რომლებიც ვალდებულნი არიან, დანიშნონ მონაცემთა დაცვის ოფიცერი[4]

კანონის თანახმად, საჯარო დაწესებულება, სადაზღვევო ორგანიზაცია, კომერციული ბანკი, მიკროსაფინანსო ორგანიზაცია, საკრედიტო ბიურო, ელექტრონული კომუნიკაციის კომპანია, ავიაკომპანია, აეროპორტი, სამედიცინო დაწესებულება, აგრეთვე ორგანიზაცია, რომელიც ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან ახორციელებს მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს, ვალდებულია, დანიშნოს ან განსაზღვროს პერსონალურ მონაცემთა დაცვის ოფიცერი.[5] სხვა ორგანიზაციებს უფლება აქვთ, საკუთარი შეხედულებისამებრ, დანიშნონ პერსონალურ მონაცემთა დაცვის ოფიცერი. დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირები ვალდებულნი არიან, მონაცემთა დაცვის ოფიცრის ვინაობა და საკონტაქტო ინფორმაცია აცნობონ პერსონალურ მონაცემთა დაცვის სამსახურს.[6]

მონაცემთა დაცვის ოფიცრის ფუნქციები

მონაცემთა დაცვის ოფიცერს მნიშვნელოვანი როლი ეკისრება ორგანიზაციის მიერ მონაცემთა დაცვის მოთხოვნებთან შესაბამისობის უზრუნველყოფაში. მონაცემთა დაცვის ოფიცერს ევალება ორგანიზაციის ინფორმირება და კონსულტირება, ახორციელებს ორგანიზაციის მიერ სამართლებრივი ვალდებულების შესრულების მონიტორინგს, აგრეთვე მოქმედებს, როგორც საკონტაქტო პირი საზედამხედველო ორგანოსა და მონაცემთა სუბიექტებთან ურთიერთობაში.

---

[3] “GDPR”-ის მიღებამდე, მონაცემთა დაცვის ოფიცრის დანიშვნის პრაქტიკა ევროკავშირის რამდენიმე წევრ ქვეყანაში დაინერგა. ის ანგარიშვალდებულების ერთგვარი ქვაკუთხედის ფუნქციას ასრულებდა, რამდენადაც მიიჩნეოდა, რომ მონაცემთა დაცვის ოფიცრის დანიშვნა ხელს უწყობს ორგანიზაციის მიერ კანონის დაცვას და უზრუნველყოფს მის კონკურენტულ უპირატესობას.

[4] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 33.

[5] იხილეთ 2024 წლის 2 თებერვალს გამოცემული, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება „დამუშავებისთვის პასუხისმგებელ პირთა და დამუშავებაზე უფლებამოსილ პირთა წრის განსაზღვრის შესახებ, რომლებსაც არ აქვთ ვალდებულება, დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი“. <https://matsne.gov.ge/ka/document/view/6117102?publication=0>.

[6] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 33(8).

მონაცემთა დაცვის ოფიცრის პასუხისმგებლობაა ორგანიზაციის მოქმედებების კანონთან შესაბამისობის ხელშეწყობა და მონიტორინგი. კერძოდ, მონაცემთა დაცვის ოფიცერი უზრუნველყოფს:

- მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე ორგანიზაციებისა და მათი თანამშრომლების ინფორმირებას;

- მონაცემთა დამუშავებასთან დაკავშირებული შიდა რეგულაციების შემუშავებაში მონაწილეობას;

- მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის შემუშავებასა და აღნიშნული დოკუმენტით განსაზღვრული ღონისძიებების განხორციელებაში მონაწილეობას;

- ორგანიზაციის მიერ მონაცემთა დამუშავებასთან დაკავშირებული შიდა რეგულაციების შესრულების მონიტორინგს;

- მონაცემთა დამუშავებასთან დაკავშირებით შემოსული განცხადებებისა და საჩივრების ანალიზსა და შესაბამისი რეკომენდაციების გაცემას;

- ორგანიზაციის წარმომადგენლობას პერსონალურ მონაცემთა დაცვის სამსახურთან ურთიერთობაში, მისი მოთხოვნით ინფორმაციისა და დოკუმენტების წარდგენასა და მისი დავალებებისა და რეკომენდაციების შესრულების კოორდინაციასა და მონიტორინგს;

- მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში, მისთვის მონაცემთა დამუშავების პროცესებისა და მისი უფლებების შესახებ ინფორმაციის მიწოდებას;

- მონაცემთა დამუშავების სტანდარტების ამაღლების მიზნით სხვა ფუნქციების შესრულებას.[7]

ზოგადი პრინციპები მონაცემთა დაცვის ოფიცრისთვის

კომპეტენცია

კანონი მონაცემთა დაცვის ოფიცრებს ავალდებულებს, ჰქონდეთ შესაბამისი ცოდნა მონაცემთა დაცვის სფეროში,[8] მაგრამ არ განსაზღვრავს კონკრეტულ საკვალიფიკაციო მოთხოვნებს. ეს მიდგომა შეესაბამება “GDPR”-ს, რომლის თანახმად, მონაცემთა დაცვის

[7] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 33(1)(ა-ვ).
[8] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 33(5).

ოფიცრის დანიშვნის საფუძველია პირის „პროფესიული თვისებები, კერძოდ, მონაცემთა დაცვის კანონმდებლობისა და პრაქტიკის ექსპერტული ცოდნა და [მონაცემთა დაცვის ოფიცრის] ამოცანების შესრულების უნარი“.[9] კანონის მსგავსად, “GDPR” პირდაპირ არ განსაზღვრავს მონაცემთა დაცვის ოფიცრებისთვის აუცილებელ საკვალიფიკაციო მოთხოვნებს.

ევროპის ქვეყნები, რომლებზეც ვრცელდება “GDPR”, ამ საკითხთან დაკავშირებით, განსხვავებულ მიდგომებს იყენებენ. საფრანგეთმა და ლატვიამ დაამკვიდრეს იმგვარი ღონისძიებები, რომლებიც ითვალისწინებს მონაცემთა დაცვის ოფიცრების კვალიფიკაციის დადასტურებას სერტიფიცირების ან საკვალიფიკაციო გამოცდის გზით. გაერთიანებულ სამეფოს, გერმანიასა და ესპანეთს არ აქვთ პირდაპირ განსაზღვრული სერტიფიცირების ან ლიცენზირების მოთხოვნები.[10]

მიუხედავად იმისა, სავალდებულოა თუ არა სერტიფიცირება, დაინტერესებულ პირებს შეუძლიათ გაიარონ საერთაშორისო ონლაინ სერტიფიცირების კურსები, როგორებიცაა: Apave Certification, IAPP-ის სერტიფიცირება, ITCERTS, EU GDPR ტრენინგი და სერტიფიცირება.[11]

<u>დამოუკიდებლობა და მიუკერძოებლობა</u>

კანონი აღიარებს მონაცემთა დაცვის ოფიცრის ფუნქციების შესრულებისას დამოუკიდებლობისა და მიუკერძოებლობის მნიშვნელობას, ასევე, ინტერესთა კონფლიქტის თავიდან აცილების აუცილებლობას.[12] ამ მიზნის მისაღწევად, კანონი ითვალისწინებს, რომ პერსონალურ მონაცემთა დაცვის ოფიცერი, კონკრეტული გარემოებების გათვალისწინებით, ანგარიშვალდებული უნდა იყოს ორგანიზაციის ფარგლებში მაქსიმალურად მაღალი დონის მმართველობის სტრუქტურის წინაშე.[13] მონაცემთა დაცვის ოფიცრის როლი შეიძლება შეასრულოს ორგანიზაციის თანამშრომელმა ან აღნიშნული ფუნქციების განხორციელება, მომსახურების ხელშეკრულების საფუძველზე, დაევალოს გარეშე მესამე პირს. შესაძლებელია, მონაცემთა დაცვის ოფიცერი ორგანიზაციაში იმავდროულად ითავსებდეს სხვა ფუნქციებს, ასევე, მონაცემთა დაცვის ოფიცრის ფუნქცია-მოვალეობებს ახორციელებდეს ერთზე მეტ ორგანიზაციაში, თუ ამის შედეგად არ წარმოიქმნება ინტერესთა კონფლიქტი.

დამოუკიდებლობის, მიუკერძოებლობისა და ინტერესთა კონფლიქტის თავიდან აცილების მნიშვნელობა ხაზგასმულია, როგორც “GDPR”-ში,[14] ისე ევროკავშირის

[9] ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 37(5).
[10] რეკომენდაციები პერსონალური მონაცემების დაცვის ოფიცრებისთვის, PDPS: <https://shorturl.at/qW2dZ>
[11] იქვე.
[12] აღნიშნული ასევე შეესაბამება “GDPR”-ს. *იხილეთ* ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 38.
[13] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 33(6).
[14] *იხილეთ ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 38.*

სხვადასხვა ქვეყნის საზედამხედველო ორგანოების პოზიციებში. მაგალითად, ევროკავშირის ქვეყნების საზედამხედველო ორგანოები მიიჩნევენ, რომ:

- ინტერესთა კონფლიქტი ჩნდება, როდესაც მონაცემთა დაცვის ოფიცერს შეუძლია მიიღოს მნიშვნელოვანი გადაწყვეტილებები მონაცემთა დამუშავების პროცესთან დაკავშირებით;

- მონაცემთა დაცვის ოფიცრის დამოუკიდებლობას და მიუკერძოებლობას შეიძლება საფრთხე შეექმნას იმ შემთხვევაში, თუ მონაცემთა დაცვის ოფიცერი ამავდროულად ასრულებს შესაბამისობის ოფიცრის, აუდიტისა და რისკის მართვის ხელმძღვანელის ფუნქციას;

- მონაცემთა დაცვის ოფიცერსა და აღმასრულებელი დონის მენეჯმენტს შორის არსებული ორი იერარქიული დონე ხელს უშლის მონაცემთა დაცვის ოფიცერს, უშუალო კავშირი დაამყაროს უმაღლეს ხელმძღვანელობასთან, ისეთ შემთხვევაშიც კი, როდესაც მონაცემთა დაცვის ოფიცერი რეგულარულად მართავს შეხვედრებს დირექტორთა საბჭოსთან.

<u>უფლებები და პასუხისმგებლობა</u>

კანონის თანახმად, მონაცემთა დაცვის ოფიცერმა უნდა მიიღოს მონაწილეობა მონაცემთა დამუშავებასთან დაკავშირებით მნიშვნელოვანი გადაწყვეტილებების მიღების პროცესში, უზრუნველყოფილი იყოს შესაბამისი რესურსებით, აგრეთვე უზრუნველყოფილი იყოს მისი დამოუკიდებლობა საქმიანობის განხორციელებისას.[15]

მონაცემთა დაცვის ოფიცერი პირადად არ არის პასუხისმგებელი ორგანიზაციის მიერ კანონის დაცვაზე. კანონის დაცვა ორგანიზაციის პასუხისმგებლობაა.[16] კანონის თანახმად, მონაცემთა დაცვის ოფიცერი უზრუნველყოფს „ინფორმირებას“, „მონაწილეობას“, „მონიტორინგს“ და „აანალიზებს“ ორგანიზაციის მიერ წარმართული მონაცემთა დამუშავების პროცესების კანონთან შესაბამისობას. მონაცემთა დაცვის ოფიცერი ვალდებულია, ამ როლისთვის განსაზღვრული სამსახურებრივი მოვალეობები შეასრულოს ჯეროვნად, ორგანიზაციის საქმიანობისა და დისციპლინური სტანდარტების შესაბამისად.

შენიშვნა საფრთხეების, საფრთხეების ანალიზისა და საფრთხის შემცირების შესახებ

საფრთხეების ადეკვატური ანალიზი და საფრთხის შესამცირებლად შესაბამისი ღონისძიებების გატარება მნიშვნელოვან როლს თამაშობს მონაცემთა დაცვისა და

[15] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 33(7).

[16] ეს ასევე შესაბამისობაშია “GDPR”-სა და მონაცემთა დაცვის ევროპულ საბჭოსთან. *იხილეთ* მუხლი 29, მონაცემთა დაცვის ოფიცერთა სამუშაო ჯგუფის სახელმძღვანელო პრინციპები (დამტკიცებულია მონაცემთა დაცვის ევროპული საბჭოს მიერ), დანართი (12).

პირადი ცხოვრების ხელშეუხებლობის სფეროში. საფრთხეებზე ორიენტირებული მიდგომა ეფექტიანი ინსტრუმენტია და უზრუნველყოფს პირთა უფლებებისა და თავისუფლებების დაცვის უმაღლეს დონეს, ორგანიზაციის ინტერესების მხედველობაში მიღების და ინოვაციების ხელშეწყობის პარალელურად.

არსებული საფრთხეების ანალიზის აუცილებლობა კანონის არაერთ დანაწესში ფიგურირებს. მაგალითად, მონაცემთა უსაფრთხოების უზრუნველსაყოფად, აუცილებელია, გათვალისწინებული იყოს მონაცემთა სუბიექტის უფლებების დარღვევის შესაძლო საფრთხეები.[17] თუ მონაცემთა დამუშავებისას არსებობს ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის მაღალი ალბათობა, სავალდებულოა მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის შექმნა.[18] მონაცემთა დამუშავება დასაშვებია ორგანიზაციის ლეგიტიმური ინტერესების დასაცავად, გარდა იმ შემთხვევისა, თუ არსებობს მონაცემთა სუბიექტის უფლებების დაცვის აღმატებული ინტერესი.[19]

საფრთხეების ანალიზისას უნდა შეფასდეს მონაცემთა დამუშავების შესაძლო უარყოფითი შედეგები და ამ შედეგების საპირწონე სარგებელი. აუცილებელია, გააზრებულ იქნას იმ უარყოფითი შედეგების ალბათობა და სიმძიმე, რომელიც მონაცემთა სუბიექტს შეიძლება მიადგეს ორგანიზაციის მიერ პერსონალური მონაცემების დამუშავების შედეგად. ამასთანავე, საფრთხეს უნდა აბალანსებდეს მონაცემთა დამუშავებით მიღებული სარგებელი. „ალბათობის“ დადგენა გულისხმობს იმის განსაზღვრას, თუ რამდენად სავარაუდოა საფრთხის ან საფრთხის შედეგების რეალურად დადგომა. „სიმძიმე“ კი აღნიშნავს საფრთხის მატერიალიზების შემთხვევაში მისი უარყოფითი ზემოქმედების ხარისხს. მონაცემთა სუბიექტების მიმართ დამდგარი უარყოფითი შედეგები ან ზიანი შეიძლება იყოს ფიზიკური, ფსიქოლოგიური, ეკონომიკური, რეპუტაციის შემლახავი, დისკრიმინაციული ან ავტონომიური.

თუ მონაცემთა დამუშავების თანმდევი საფრთხეების ანალიზის შედეგად გამოვლინდა, რომ საფრთხის დონე დაუშვებლად მაღალია, გათვალისწინებული უნდა იყოს საფრთხის შემცირებისკენ მიმართული სათანადო ღონისძიებები. ამგვარი ღონისძიებები შეიძლება მოიცავდეს: მონაცემთა ფსევდონიმიზაციას; მონაცემებზე წვდომების შეზღუდვას; მონაცემთა მესამე პირებისთვის გადაცემის შეზღუდვას; გეოგრაფიული დაფარვის შეზღუდვას; შემდგომი დამუშავების შეზღუდვას; გამჭვირვალობის გაზრდას; უსაფრთხოების ახალი ან გაძლიერებული ზომების მიღებას; მონაცემთა დამუშავებაში ჩართულ თანამშრომელთა გადამზადებას; გადაწყვეტილების მიღებას გარკვეული ტიპის მონაცემების დაუმუშავებლობის შესახებ; შენახვის ვადების შეზღუდვას; მონაცემების უსაფრთხო და სამუდამოდ წაშლის უზრუნველყოფას; იმგვარი სისტემების გამოყენებას, რომლებიც მონაცემთა სუბიექტებს მონაცემების მიღებას უმარტივებს; ორგანიზაციის მიერ მონაცემთა დამუშავების პროცესების შესახებ მონაცემთა სუბიექტების სრულყოფილად ინფორმირებას და ორგანიზაციასთან

[17] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 27(3).
[18] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 31(1).
[19] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 5(1)(ი).

კომუნიკაციის გამარტივებას; პროცესში დამუშავებაზე უფლებამოსილი პირის ჩართვას მხოლოდ სათანადო წერილობითი შეთანხმებების (რომლებიც შეიცავს სათანადო სავალდებულო წესებსა და აკრძალვებს) საფუძველზე; მონაცემთა გადაცემის პროცესების რეგულირებას ხელშეკრულებებით, რომლებიც მკაფიოდ განსაზღვრავს, თუ რა სახის ინფორმაცია იქნება გაზიარებული, როგორ და ვისთან; გამოვლენილი საფრთხეების შესაბამის სხვა სპეციფიკური ღონისძიებებს.

მონაცემთა დაცვის ოფიცერი მნიშვნელოვნად ეხმარება ორგანიზაციას პერსონალური მონაცემების დამუშავებასთან დაკავშირებული საფრთხეების იდენტიფიცირების, შეფასებისა და მართვის პროცესში.

ცოდნა, უნარები და პიროვნული თვისებები

ცოდნა: „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ცოდნა

მონაცემთა დაცვის ოფიცერს საფუძვლიანად უნდა ესმოდეს კანონის მოთხოვნები და მათი მიმართება კონკრეტული ორგანიზაციის საქმიანობასთან. უაღრესად მნიშვნელოვანია შემდეგ საკითხებთან დაკავშირებული რეგულაციების შესწავლა.[20]

კანონის მიზანი:	პერსონალური მონაცემების დამუშავებისას, ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის, პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცვა.
კანონის მოქმედების სფერო:	• საქართველოს ტერიტორიაზე მონაცემთა ავტომატური საშუალებებით დამუშავება • იმ მონაცემთა დამუშავება, რომლებიც ფაილური სისტემის ნაწილია ან ფაილურ სისტემაში შესატანად მუშავდება • საქართველოს ფარგლების გარეთ რეგისტრირებული დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა საქართველოში არსებული ტექნიკური საშუალებების გამოყენებით დამუშავება, გარდა იმ შემთხვევისა, როდესაც ტექნიკური საშუალებები მხოლოდ მონაცემთა ტრანზიტისთვის გამოიყენება • გამონაკლისი: ○ ფიზიკური პირების მიერ მონაცემთა პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში დამუშავება ○ სახელმწიფო უსაფრთხოება ○ სახელმწიფო საიდუმლოებები ○ სასამართლო სამართალწარმოება ○ მასობრივი ინფორმაციის საშუალებები ○ აკადემიური, სახელოვნებო და ლიტერატურული მიზნები

[20] კანონის ზოგიერთი სხვა ნაწილის კარგი ცოდნა სასურველია, მაგრამ არ აქვს გადამწყვეტი მნიშვნელობა მონაცემთა დაცვის ოფიცრის როლისთვის მინიმალური სტანდარტების დადგენისას.

(შერჩეული) განმარტებები:	• პერსონალური მონაცემი
	• განსაკუთრებული კატეგორიის მონაცემი
	  • ჯანმრთელობასთან დაკავშირებული მონაცემი
	  • ბიომეტრიული მონაცემი
	  • გენეტიკური მონაცემი
	• მონაცემთა დამუშავება
	• მონაცემთა ავტომატური საშუალებებით დამუშავება
	• ფაილური სისტემა
	• მონაცემთა სუბიექტი
	• მონაცემთა სუბიექტის თანხმობა
	• დამუშავებისთვის პასუხისმგებელი პირი
	• დამუშავებაზე უფლებამოსილი პირი
	• ვიდეომონიტორინგი
	• აუდიომონიტორინგი
	• პირდაპირი მარკეტინგი
	• პროფაილინგი
	• მონაცემთა დეპერსონალიზაცია
	• მონაცემთა ფსევდონიმიზაცია
	• ინციდენტი

მონაცემთა დამუშავების პრინციპები:	• კანონიერება, სამართლიანობა და გამჭვირვალობა • კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზნები • აუცილებლობა და თანაზომიერება • სიზუსტე • შენახვასთან დაკავშირებული შეზღუდვა • უსაფრთხოება • მიზნის შეზღუდვა (და გამონაკლისები)

მონაცემთა დამუშავების საფუძვლები	• თანხმობაზე დაფუძნებული დამუშავება
	• დამუშავება, რომელსაც მოითხოვს:
	  ○ სახელშეკრულებო ვალდებულება
	  ○ კანონით გათვალისწინებული მოვალეობა
	  ○ მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დაცვა (მაგ., პანდემია)
	  ○ მაღალი საზოგადოებრივი ინტერესი (მაგ., დანაშაულის თავიდან აცილებისთვის)
	• საჯაროდ ხელმისაწვდომი მონაცემების დამუშავება

	• საქართველოს კანონმდებლობით განსაზღვრული დამუშავება • განსაკუთრებული კატეგორიის მონაცემების დამუშავება
დამუშავების სპეციალური წესები	• ისეთი მონაცემების დამუშავება, რომლებიც ეხება: ○ არასრულწლოვან პირებს ○ გარდაცვლილ პირებს ○ ბიომეტრიას • ვიდეომონიტორინგის წესები • აუდიომონიტორინგის წესები • პირდაპირი მარკეტინგის წესები
მონაცემთა სუბიექტის უფლებები:	• მონაცემთა დამუშავების შესახებ ინფორმაციის მიღების უფლება • მონაცემთა გაცნობისა და ასლის მიღების უფლება • მონაცემთა გასწორების, განახლებისა და შევსების უფლება • მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლება • მონაცემთა დაბლოკვის უფლება • მონაცემთა გადატანის უფლება • ავტომატიზებული წესით მიღებულ გადაწყვეტილებაზე დაქვემდებარებაზე უარის განცხადების უფლება • მონაცემთა დამუშავებაზე თანხმობის გამოხმობის უფლება • მონაცემთა სუბიექტის უფლებების შეზღუდვა ○ გასაჩივრების უფლება
დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის ვალდებულებები:	• ყოვლისმომცველი ვალდებულება მონაცემთა სუბიექტების უფლებების დაცვის შესახებ • მონაცემთა სუბიექტების ინფორმირება მონაცემთა დამუშავების შესახებ ○ როდესაც მონაცემების შეგროვება უშუალოდ მისგან ხდება ○ როდესაც მონაცემების შეგროვება უშუალოდ მისგან არ ხდება ○ მონაცემთა სუბიექტის თანხმობის მიღების პროცესში

	• მონაცემების მეტად დაფარვის პრიორიტეტად განსაზღვრის ვალდებულება ახალი პროდუქტის ან მომსახურების შექმნისას • სათანადო ტექნიკური და ორგანიზაციული ზომების მიღების ვალდებულება, რომლებიც: ○ უზრუნველყოფს მონაცემთა დაცვას კანონის შესაბამისად, მათ დაცვას დაკარგვისგან, უკანონო დამუშავებისგან, მათ შორის, განადგურებისგან, წაშლისგან, შეცვლისგან, გამჟღავნებისგან ან გამოყენებისგან • მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვის ვალდებულება • ინციდენტის (განსაზღვრული სახის) შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისთვის და მონაცემთა სუბიექტისთვის შეტყობინების ვალდებულება • მონაცემთა დაცვაზე ზეგავლენის შეფასებათა განხორციელების ვალდებულება • პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულება; • სპეციალური წარმომადგენლის დანიშვნის ან განსაზღვრის ვალდებულება; • როდესაც მონაცემთა დამუშავებაში ჩართულია თანადამუშავებისთვის პასუხისმგებელი პირი ან დამუშავებაზე უფლებამოსილი პირი, რომელიც მონაცემებს ამუშავებს დამუშავებისთვის პასუხისმგებელი პირის სახელით — თითოეული ასეთი პირის ვალდებულებებისა და პასუხისმგებლობის წინასწარ წერილობით განსაზღვრის ვალდებულება • ვალდებულებები, რომლებიც უკავშირდება ორგანიზაციის ურთიერთობას პერსონალურ მონაცემთა დაცვის სამსახურთან.
მონაცემთა საერთაშორისო გადაცემა:	• მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის კანონიერი გადაცემა; • პერსონალურ მონაცემთა დაცვის სამსახურის მიერ განსაზღვრული მონაცემთა დაცვის სათანადო გარანტიების მქონე სახელმწიფოები და ორგანიზაციები

პერსონალურ მონაცემთა დაცვის სამსახურის ძირითადი უფლება-მოვალეობები:	• პერსონალურ მონაცემთა დაცვის სამსახურის მიერ მონაცემთა დამუშავების კანონიერების მონიტორინგი საქართველოში • კონსულტაციების გაცემა მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე • მონაცემთა დაცვასთან დაკავშირებული განცხადებების (მონაცემთა სუბიექტებისგან) განხილვა • მონაცემთა დამუშავების კანონიერებას შემოწმება • მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე საზოგადოების ინფორმირება და ცნობიერების ამაღლება
ადმინისტრაციული სამართალდარღვევები, პასუხისმგებლობა და საზედამხედველო ორგანოს მიერ გამოყენებული ღონისძიებები	• კანონის დარღვევისთვის პერსონალურ მონაცემთა დაცვის სამსახურს შეუძლია: ○ დაავალოს დარღვევ(ებ)ის გამოსწორება ○ დაავალოს მონაცემთა დამუშავების შეჩერება ○ დაავალოს მონაცემთა დამუშავების შეწყვეტა ○ დაავალოს მონაცემთა სხვა სახელმწიფოსთვის და საერთაშორისო ორგანიზაციისთვის გადაცემის შეწყვეტა ○ გასცეს წერილობითი რჩევები და რეკომენდაციები ○ დააკისროს ადმინისტრაციული პასუხისმგებლობა • ადმინისტრაციულ სამართალდარღვევებზე პასუხისმგებლობა გამომდინარეობს სამართალდარღვევის თავისებურებიდან

უნარები: მონაცემთა დაცვის ოფიცრის უნარების გამომუშავება

მონაცემთა დაცვის ოფიცრის როლი შეიძლება დაიყოს რამდენიმე განსხვავებულ ფუნქციად: ინფორმირება და ცნობიერების ამაღლება, კონსულტირება, ორგანიზება, თანამშრომლობა და კანონთან შესაბამისობის უზრუნველყოფა. აუცილებელია, რომ მონაცემთა დაცვის ოფიცერს გააჩნდეს ამ ფუნქციების შესასრულებლად საჭირო უნარები.

ინფორმირებისა და ცნობიერების ამაღლების ფუნქცია	• მიმდინარე სტრატეგიის განსაზღვრა და განხორციელება, ორგანიზაციაში კანონით გათვალისწინებული ვალდებულებების, პასუხისმგებლობისა და ამოცანების შესახებ ინფორმირებისთვის, მაგალითად, შემდეგი საშუალებების გამოყენებით:

	○ საინფორმაციო შეტყობინებები და შეხსენების ბარათები თანამშრომლებისთვის ○ ტრენინგ სესიები ○ ინდივიდუალური კომუნიკაცია სტრუქტურულ ერთეულებთან ○ ვებგვერდ(ებ)ი ○ მონაცემთა დაცვის დღისადმი მიძღვნილი ღონისძიებები[21] • შესაბამისი სტრუქტურული ერთეულების დახმარება მონაცემთა კონფიდენციალობასთან დაკავშირებული შეტყობინებების შემუშავებაში, გამოქვეყნებასა და განახლებაში: ○ ყველა კატეგორიის მონაცემთა სუბიექტებისთვის (მაგ. თანამშრომლები და პოტენციური თანამშრომლები, კლიენტები და პოტენციური კლიენტები, ვებგვერდების მომხმარებლები) ○ მონაცემთა შეგროვების კონკრეტული პროცესის სპეციფიკაზე მორგებული ინფორმაციით.[22] ○ კონკრეტული ინფორმაციით, დამუშავების საფუძვლად გამოყენებული მონაცემთა სუბიექტის თანხმობის მოპოვების პროცესებში
საკონსულტაციო ფუნქცია:	• ორგანიზაციისთვის კონსულტაციის გაწევა მონაცემთა დაკარგვისა და უკანონო დამუშავების რისკების შემცირებისთვის კონფიდენციალურობის დაცვის შესაბამისი ტექნოლოგიებისა და ორგანიზაციული ზომების შესახებ, მაგალითად: ○ მონაცემთა კლასიფიკაცია (საჯარო, კონფიდენციალური, შეზღუდული) ○ მონაცემთა ფსევდონიმიზაცია ○ მონაცემთა შენიღბვა ○ მონაცემთა დეიდენტიფიკაცია ○ წვდომის შეზღუდვები ○ მონაცემთა მინიმიზაცია ○ მონაცემთა შენახვა და წაშლა ○ ფიზიკური დაცვის მექანიზმები

[21] *იხილეთ, მაგ.,* <https://www.edps.europa.eu/data-protection/our-work/publications/events/european-data-protection-day-0_en.>

[22] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლები 24 და 25.

	• ინციდენტის შემთხვევაში, ორგანიზაციის კონსულტირება შეტყობინების ვალდებულების თაობაზე, მათ შორის: ○ შეტყობინების ვადები ○ პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინებების მიწოდება ○ მონაცემთა სუბიექტების ინფორმირება, როდესაც არსებობს მაღალი ალბათობა იმისა, რომ ინციდენტი გამოიწვევს მნიშვნელოვან ზიანს ან მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს ○ შეტყობინებების შინაარსი ○ ინციდენტის შესახებ ინფორმირება მარტივი და გასაგები ფორმით • ორგანიზაციისთვის კონსულტაციის გაწევა მონაცემთა დაცვაზე ზეგავლენის შეფასების ჩატარების თაობაზე ○ მონაცემთა დაცვაზე ზეგავლენის შეფასება სავალდებულოა იმ შემთხვევაში, თუ არსებობს ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის მაღალი ალბათობა ▪ მონაცემთა დაცვაზე ზეგავლენის შეფასება უნდა მოხდეს მონაცემთა დამუშავების პროცესის დაწყებამდე ▪ გასათვალისწინებელია ახალი ტექნოლოგიები, მონაცემთა კატეგორია და მოცულობა, ასევე დამუშავების მიზნები და საშუალებები. ○ მონაცემთა დაცვაზე ზეგავლენის შეფასება სავალდებულოა, როდესაც 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 ▪ ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში. ○ მონაცემთა დაცვაზე ზეგავლენის შეფასების ჩატარების სათანადო მეთოდოლოგია

	○ მონაცემთა კატეგორიის, მიზნების, პროპორციულობის, პროცედურისა და მონაცემთა დამუშავების საფუძვლების აღმწერი დოკუმენტაციის შემუშავება; ადამიანის ძირითადი უფლებებისა და თავისუფლებების დარღვევის საფრთხეების შეფასება; მონაცემთა უსაფრთხოების უზრუნველსაყოფად განხორციელებული ორგანიზაციული და ტექნიკური ღონისძიებების აღწერა ○ რა გარანტიები (მათ შორის: ორგანიზაციული და ტექნიკური ზომები) უნდა იქნას გამოყენებული მონაცემთა სუბიექტების უფლებებისა და ინტერესებისადმი წარმოქმნილი რისკის შესამცირებლად ○ როდის უნდა მოხდეს პერსონალურ მონაცემთა დაცვის სამსახურთან კონსულტაციის გავლა ○ სწორად ჩატარდა თუ არა მონაცემთა დაცვაზე ზეგავლენის შეფასება ○ შეესაბამება თუ არა მონაცემთა დაცვაზე ზეგავლენის შეფასების დასკვნები კანონის მოთხოვნებს • კონსულტირება და რეკომენდაციების გაცემა, როდესაც მონაცემთა სუბიექტს შემოაქვს განცხადება ან საჩივარი ორგანიზაციის მიერ მონაცემთა დამუშავებასთან დაკავშირებით
ორგანიზაციული ფუნქცია:	• შიდა პოლიტიკის, პროცედურებისა და სახელმძღვანელო პრინციპების შემუშავებაში და განხორციელებაში მონაწილეობა, რომლებიც: ○ განსაზღვრავს როლებს, პასუხისმგებლობებსა და ანგარიშგების სტრუქტურებს მონაცემთა დამუშავებისთვის თითოეულ სტრუქტურულ ერთეულში ○ განსაზღვრავს იმ ინდივიდუალურ კოორდინატორებს ან ლიდერებს თითოეულ სტრუქტურულ ერთეულში, რომლებსაც მონაცემთა დაცვის ოფიცერთან ურთიერთობა ევალება ○ აწესებს სტანდარტებს, პრაქტიკებსა და პროტოკოლებს ორგანიზაციისთვის, რათა უზრუნველყოს ორგანიზაციის მიერ მონაცემების დამუშავება კანონის მოთხოვნებთან შესაბამისობაში • მონაწილეობს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვაში და

	სათანადო აღრიცხვის დოკუმენტის/რეესტრის შექმნასა და წარმოებაში, რომელიც შეიცავს შემდეგ ინფორმაციას: ○ დამუშავებისთვის პასუხისმგებელი პირის, სპეციალური წარმომადგენლის, მონაცემთა დაცვის ოფიცრის, თანადამმუშავებლისა და დამუშავებაზე უფლებამოსილი პირის ვინაობა და საკონტაქტო მონაცემები; ○ მონაცემთა დამუშავების მიზნები; ○ მონაცემთა სუბიექტები და მონაცემთა კატეგორიები ○ მონაცემთა მიმღებების კატეგორიები; ○ მონაცემთა ნებისმიერი გადაცემა სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის, მონაცემთა დაცვის გარანტიებით და პერსონალურ მონაცემთა დაცვის სამსახურის მიერ გაცემული ნებისმიერი ნებართვით ○ მონაცემთა შენახვის ვადა; ○ მონაცემთა უსაფრთხოების უზრუნველსაყოფად განხორციელებული ორგანიზაციული და ტექნიკური ღონისძიებების ზოგადი აღწერა; ○ ინფორმაცია ინციდენტების შესახებ (ასეთის არსებობის შემთხვევაში); • მონაწილეობა დამუშავებაზე უფლებამოსილი პირების ჩართულობასა და მართვაში; ○ მომსახურების მომწოდებელთა შეფასება, რათა დადგინდეს დამუშავებაზე უფლებამოსილი პირის უნარი, დააკმაყოფილოს კანონმდებლობისა და ორგანიზაციის შიდა წესების მოთხოვნები; ○ ორგანიზაციის ვალდებულებების შესრულების უზრუნველსაყოფად ხელშეკრულებებში სათანადო პირობების გათვალისწინება; • ინციდენტებზე რეაგირების პროცედურების შემუშავებასა და განხორციელებაში მონაწილეობა შემდეგი მიზნებისთვის: ○ ინციდენტის რისკის შეფასება; ○ ინციდენტის შეკავება; ○ მაკორექტირებელი ღონისძიებების იდენტიფიცირება და განხორციელება; ○ პერსონალურ მონაცემთა დაცვის სამსახურისთვისა და მონაცემთა სუბიექტებისთვის შეტყობინება; ○ ინციდენტის შემდგომი მოკვლევის ჩატარება და მომავალი რისკების შემცირება; ○ ინციდენტების რეესტრისა და დაკავშირებული დოკუმენტაციის წარმოება;

	○ ინციდენტზე რეაგირების პროცედურების გასაუმჯობესებლად პერიოდული მოდელირებული სავარჯიშოების ჩატარება.
თანამშრომლობის ფუნქცია:	• ორგანიზაციის საკონტაქტო პირის ფუნქციის შესრულება მონაცემთა დაცვის საკითხებში, შემდეგ პირებთან ურთიერთობისას: ○ ორგანიზაციის თანამშრომლები და ხელმძღვანელობა; ○ მონაცემთა სუბიექტები; ○ პერსონალურ მონაცემთა დაცვის სამსახური; • პერსონალურ მონაცემთა დაცვის სამსახურთან კონსულტაცია, როდესაც მონაცემთა დაცვაზე ზეგავლენის შეფასება მიუთითებს, რომ მონაცემთა დამუშავება, მაღალი ალბათობით, ქმნის ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხეს; • მონაცემთა სუბიექტების მიერ განცხადების შემოტანისას მათი ინფორმირება მონაცემების დამუშავებისა და მათი უფლებების შესახებ.
კანონთან შესაბამისობის უზრუნველყოფის ფუნქცია:	• კანონის დაცვის ხელშემწყობი კულტურის წახალისება • შიდა პოლიტიკის, პროცედურებისა და ინსტრუქციების შემუშავების და განახლების ინიცირება; • კანონმდებლობის მოთხოვნების განმარტება და იმის უზრუნველყოფა, რომ ორგანიზაციის შიდა პოლიტიკა, პროცედურები და მითითებები იყოს კანონთან შესაბამისი;კანონის მოთხოვნებთან შესაბამისობის შესახებ მუდმივი ტრენინგისა და კომუნიკაციის უზრუნველყოფა; • ორგანიზაციის საქმიანობის კანონის მოთხოვნებთან თავსებადობის და არსებული პრობლემების შესახებ შიდა ანგარიშების წარმოება; • კანონის მოთხოვნათა დაცვისკენ მიმართული წახალისების სისტემისა და დისციპლინის დანერგვა; • კანონთან შეუსაბამობის შესაძლო შემთხვევების გამოძიება და გამოსწორება; • იმ მესამე პირებთან ურთიერთობების კომპლექსური შესწავლა და ზედამხედველობა, რომელთა ქმედებებმა

	შეიძლება წარმოქმნას კანონთან შეუსაბამობის მნიშვნელოვანი რისკი; • ორგანიზაციის კანონთან შესაბამისობის მონიტორინგი და შემოწმება.

პიროვნული თვისებები: მონაცემთა დაცვის ოფიცრის პიროვნული თვისებები

მონაცემთა დაცვის ოფიცერს უნდა გააჩნდეს ისეთი პიროვნული თვისებები, როგორიცაა: კეთილსინდისიერება, განვითარებაზე ორიენტირებულობა, პრობლემების გადაჭრის, რისკების ეფექტურად ანალიზის და ეფექტური კომუნიკაციის უნარი.

კეთილსინდისიერება:	მონაცემთა დაცვის ოფიცერმა პერსონალური მონაცემების დამუშავების პროცესში ჩართულობისას უნდა შეინარჩუნოს პროფესიული ეთიკისა და კონფიდენციალურობის მაღალი დონე.
განვითარებაზე ორიენტირებულობა:	მონაცემთა დაცვის ოფიცერი მუდმივად უნდა ეცნობოდეს მონაცემთა დაცვის წესების დამდგენი კანონების, რეგულაციებისა და საუკეთესო პრაქტიკის სიახლეებს, რათა გაითვალისწინოს ისინი საკუთარ საქმიანობაში.
პრობლემების გადაჭრის უნარი:	მონაცემთა დაცვის ოფიცერს უნდა შეეძლოს, გააანალიზოს მონაცემთა დაცვის კომპლექსური საკითხები და შეიმუშაოს გამოკვეთილი პრობლემების გადაჭრის პრაქტიკული გზები, რომლებიც ორგანიზაციის მიზნებსა და ღირებულებებს შეუსაბამებს საკანონმდებლო მოთხოვნებს.
რისკების ანალიზი:	მონაცემთა დაცვის ოფიცერს უნდა შეეძლოს, შეაფასოს რისკები, რა დროსაც უნდა გაითვალისწინოს, ერთი მხრივ, ორგანიზაციის ინტერესები — მათ შორის, პერსონალური მონაცემების გამოყენების სურვილი — და, მეორე მხრივ, მონაცემთა სუბიექტებისთვის ზიანის მიყენების ალბათობა, რომელიც ასეთი გამოყენების შედეგად შეიძლება წარმოიქმნას.
კომუნიკაციის უნარები:	მონაცემთა დაცვის ოფიცერს უნდა შეეძლოს ეფექტური კომუნიკაცია, ფლობდეს ახალი იდეების

	პოპულარიზების და დარწმუნების უნარს, სკეპტიციზმის ან პრიორიტეტებს შორის კონფლიქტის პირობებში.

დოკუმენტაცია

ორგანიზაციების საქმიანობის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან თავსებადობის უზრუნველყოფის საკვანძო ნაწილია სათანადო დოკუმენტაციის წარმოება. მაგალითად, კანონის თანახმად, ორგანიზაცია ვალდებულია, აწარმოოს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა და, საჭიროების შემთხვევაში, მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტაცია, უზრუნველყოს მონაცემთა სუბიექტების ინფორმირება, ასევე, ინციდენტის შემთხვევაში — პერსონალურ მონაცემთა დაცვის სამსახურისთვის და მონაცემთა სუბიექტებისთვის დადგენილი წესით შეტყობინება.

მონაცემთა დამუშავების პროცესების აღმწერი და მომწესრიგებელი შიდა დოკუმენტაცია მონაცემთა დაცვის ოფიცრისთვის მნიშვნელოვანი საინფორმაციო წყაროა კონკრეტულ ორგანიზაციაში მონაცემთა დამუშავების თვალსაზრისით არსებული აქტივობების შესახებ. გარდა ამისა, ამგვარი დოკუმენტაცია შესაძლებელს ხდის, დამუშავების პროცესები დაიგეგმოს კანონის მოთხოვნებთან შესაბამისად. მიუხედავად იმისა, რომ აღნიშნული დოკუმენტაციის წარმოება დამუშავებისთვის პასუხისმგებელი ორგანიზაციის ვალდებულებაა, პრაქტიკაში აღნიშნული ამოცანის შესრულებაში მთავარ როლს მონაცემთა დაცვის ოფიცერი ასრულებს. როლებისა და პასუხისმგებლობების ნათლად განსაზღვრისათვის, მონაცემთა დაცვის ოფიცრის ფუნქცია-მოვალეობების დამდგენ სამუშაო აღწერილობებში და სხვა დოკუმენტებში ხშირად არის მითითებული, რომ დოკუმენტების შექმნა მონაცემთა დაცვის ოფიცრის ერთ-ერთი მოვალეობაა. ამგვარი ვალდებულების მონაცემთა დაცვის ოფიცრისთვის განსაზღვრის შემთხვევაში, ორგანიზაცია ვალდებულია, მიაწოდოს მას ასეთი დოკუმენტაციის შექმნისთვის საჭირო ყველა შესაბამისი ინფორმაცია.

ქვემოთ მოცემულია ძირითადი სახელმძღვანელო მითითებები, რომლებიც ეხება მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვას, მონაცემთა დაცვაზე ზეგავლენის შეფასებას, კონფიდენციალურობის შესახებ შეტყობინებებსა და ინციდენტებზე რეაგირებას.

მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა[23]

ორგანიზაციაში მიმდინარე მონაცემთა დამუშავების პროცესებთან დაკავშირებული ინფორმაციის აღრიცხვის მიზნით შექმნილი დოკუმენტი/რეესტრი მონაცემთა დაცვის ოფიცრის ერთ-ერთი მთავარი ინსტრუმენტია. ამგვარ დოკუმენტში აღრიცხული უნდა იყოს ინფორმაცია ორგანიზაციის მიერ განხორციელებული პერსონალური მონაცემების დამუშავების ყველა პროცესის შესახებ. აღნიშნული დოკუმენტი არის ინსტრუმენტი, რომელიც გამოიყენება მონაცემთა დამუშავების პროცესის კანონთან შესაბამისად წარმართვის კოორდინირებისთვის, სათანადო მონიტორინგის აქტივობების

[23] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 28.

დაგეგმვისთვის და კანონთან შესაბამისობის დემონსტრირებისთვის. ის ასევე ეხმარება მონაცემთა დაცვის ოფიცერს, განსაზღვროს ის პროცესები, რომლებთან მიმართებითაც მიზანშეწონილია ორგანიზაციის შემდგომი ინფორმირება და კონსულტირება.

დამუშავებისთვის პასუხისმგებელ პირებს, სპეციალურ წარმომადგენლებსა და დამუშავებაზე უფლებამოსილ პირებს მოეთხოვებათ, წერილობით ან ელექტრონულად უზრუნველყონ მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა. დამუშავებისთვის პასუხისმგებელი პირებისა და სპეციალური წარმომადგენლების მიერ ამ მიზნით შექმნილი დოკუმენტი უნდა შეიცავდეს, სულ მცირე, შემდეგ ინფორმაციას:

- დამუშავებისთვის პასუხისმგებელი პირის, სპეციალური წარმომადგენლის, მონაცემთა დაცვის ოფიცრის, თანადამუშავებისთვის პასუხისმგებელი პირების და დამუშავებაზე უფლებამოსილი პირის ვინაობა და საკონტაქტო მონაცემები;

- მონაცემთა დამუშავების მიზნები;

- მონაცემთა სუბიექტები და მონაცემთა კატეგორიები;

- მონაცემთა მიმღებების კატეგორიები;

- მონაცემთა გადაცემა სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის, ასევე მონაცემთა დაცვის გარანტიები და პერსონალურ მონაცემთა დაცვის სამსახურის მიერ გაცემული ნებისმიერი ნებართვა;

- მონაცემთა შენახვის ვადა;

- მონაცემთა უსაფრთხოების უზრუნველსაყოფად განხორციელებული ორგანიზაციული და ტექნიკური ღონისძიებები;

- ინფორმაცია ინციდენტების შესახებ.

დამუშავებაზე უფლებამოსილი პირისთვის, აღრიცხვის დოკუმენტი უნდა შეიცავდეს:

- დამუშავებაზე უფლებამოსილი პირის, მონაცემთა დაცვის ოფიცრის, დამუშავებისთვის პასუხისმგებელი პირის, თანადამუშავებისთვის პასუხისმგებელი პირების და სპეციალური წარმომადგენლის ვინაობასა და საკონტაქტო მონაცემებს;

- დამუშავებისთვის პასუხისმგებელი პირისთვის განხორციელებული მონაცემთა დამუშავების სახეები;

- ინფორმაცია მონაცემთა სხვა სახელმწიფოსთვის თუ საერთაშორისო ორგანიზაციისთვის გადაცემის შესახებ;

- მონაცემთა უსაფრთხოების უზრუნველსაყოფად განხორციელებული ორგანიზაციული და ტექნიკური ღონისძიებები; და

- ინფორმაცია ინციდენტების შესახებ.

დამუშავებისთვის პასუხისმგებელი პირები, რომლებიც ამუშავებენ ბიომეტრიულ მონაცემებს ან ახორციელებენ ვიდეო ან აუდიომონიტორინგს, ვალდებულნი არიან წერილობით განსაზღვრონ ასეთი დამუშავების მიზანი და კანონით განსაზღვრული სხვა დეტალები.[24] ეს ინფორმაცია ასევე შეიძლება შეტანილი იყოს დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დამუშავების შესახებ ინფორმაციის აღრიცხვის მიზნით შექმნილ დოკუმენტში.

მიზანშეწონილია, მონაცემთა დამუშავების შესახებ ინფორმაციის აღრიცხვის მიზნით შექმნილი დოკუმენტი ასევე შეიცავდეს დამატებით ინფორმაციას, როგორიცაა, მაგალითად: დამუშავების საფუძვლები — მათ შორის, ინფორმაცია მონაცემთა სუბიექტის თანხმობაზე (თუკი მონაცემები თანხმობის საფუძველზე მუშავდება).

აღრიცხვის მიზნით შექმნილ დოკუმენტში/რეესტრში ცალ-ცალკე უნდა იყოს იდენტიფიცირებული მონაცემთა დამუშავების თითოეული აქტივობა. პრაქტიკაში, ამგვარი სახის რეესტრის შესაქმნელად, მონაცემთა დაცვის ოფიცერმა უნდა ითანამშრომლოს ორგანიზაციის თითოეულ სტრუქტურულ ერთეულთან, რათა მიიღოს სათანადო ინფორმაცია მათ მიერ წარმართული მონაცემთა დამუშავების პროცესების შესახებ.

მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვისთვის შექმნილი დოკუმენტის სავალდებულო ფორმა დადგენილი არ არის და მას თავად ორგანიზაცია განსაზღვრავს. ორგანიზაცია ვალდებულია, აღნიშნული დოკუმენტი წარუდგინოს პერსონალურ მონაცემთა დაცვის სამსახურს, მისი მოთხოვნის შემთხვევაში.

მონაცემთა დაცვაზე ზეგავლენის შეფასება[25]

მონაცემთა დაცვის ოფიცერი აქტიურად მონაწილეობს მონაცემთა დამუშავების თანმდევი რისკების შეფასებაში. მონაცემთა დაცვაზე ზეგავლენის შეფასება არის პროცესი, რომლის დახმარებითაც დამუშავებისთვის პასუხისმგებელ პირს შეუძლია სისტემურად შეაფასოს და განსაზღვროს მის მიერ დანერგილი ამა თუ იმ პროდუქტისა და მომსახურების გავლენა კონფიდენციალურობასა და მონაცემთა დაცვაზე. ის

[24] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლები 9, 10 და 11.
[25] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 31.

საშუალებას აძლევს ორგანიზაციას, განსაზღვროს და მიიღოს შესაბამისი ზომები, რათა თავიდან აიცილოს ან მინიმუმამდე დაიყვანოს ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე.

ახალი ტექნოლოგიების, მონაცემთა კატეგორიებისა და მოცულობის, აგრეთვე დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, კანონი მონაცემთა დაცვაზე ზეგავლენის შეფასებას შემდეგ შემთხვევებში მოითხოვს:[26]

- მონაცემთა დამუშავება, მაღალი ალბათობით, ქმნის ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხეს;

- დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტისთვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებს სრულად ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე;

- დამუშავებისთვის პასუხისმგებელი პირი ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემებს;

- დამუშავებისთვის პასუხისმგებელი პირი ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში.

მონაცემთა დაცვაზე ზეგავლენის შეფასებისას დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია შექმნას წერილობითი დოკუმენტი, რომელიც შეიცავს:

- მონაცემთა კატეგორიის, მათი დამუშავების მიზნების, პროპორციულობის, პროცესისა და საფუძვლების აღწერას;

- ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეების შეფასებასა; და

- მონაცემთა უსაფრთხოების უზრუნველსაყოფად განხორციელებული და დაგეგმილი ორგანიზაციული და ტექნიკური ღონისძიებების აღწერას.

დამუშავებისთვის პასუხისმგებელი პირების მიერ ამგვარი დოკუმენტაციის წარმოების და ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის შემცირების მიზნით ღონისძიებების დაგეგმვის მთავარი მიზანია იმის წარმოჩენა, რომ

[26] *იხილეთ აგრეთვე,* პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მიერ გამოცემული ნორმატიული აქტი, რომელიც ადგენს მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობ კრიტერიუმებსა და მონაცემთა დაცვაზე ზეგავლენის შეფასების წესს.

ორგანიზაციამ ყურადღებით განიხილა ყველა რისკი (მათ შორის, იურიდიული, კორპორაციული, სამოქალაქო და რეპუტაციული) და გაითვალისწინა სათანადო ზომები ამ რისკების შემცირებისთვის. თითოეულ რისკთან მიმართებით უნდა არსებობდეს შიდა კონტროლის კონკრეტული მექანიზმი, რაც უზრუნველყოფს რისკის შესამცირებლად გათვალისწინებული ღონისძიებების ჯეროვნად აღსრულებას და დოკუმენტირებას. ცალკე უნდა შეფასდეს მონაცემთა სხვადასხვა კატეგორიები, ასევე კონკრეტული პროდუქტები თუ მომსახურებები. გარდა ამისა, ორგანიზაციებმა უნდა განსაზღვრონ პირი, რომელიც პასუხისმგებელია გამოვლენილი რისკის შემცირების მიზნით დაგეგმილი კონკრეტული ღონისძიებების განხორციელებაზე.

საუკეთესო პრაქტიკის შესწავლის საფუძველზე შემუშავდა ქვემოთ მოყვანილი ზოგადი მითითებები მონაცემთა დაცვაზე ზეგავლენის შეფასების წარმართვისა და დოკუმენტირებისთვის:

- <u>განსაზღვრეთ მონაცემთა დაცვაზე ზეგავლენის შეფასების საჭიროება</u>: ზოგადი სახით აღწერეთ დაგეგმილი პროექტის მიზანი და განსაზღვრეთ, რა სახის დამუშავებას მოითხოვს იგი. შეიძლება დაგეხმაროთ სხვა დოკუმენტები, როგორიცაა: საპროექტო გეგმა. მოკლედ აღწერეთ, რამ განაპირობა მონაცემთა დაცვაზე ზეგავლენის შეფასების საჭიროება.

- <u>აღწერეთ დამუშავების პროცესი</u>: როგორ შეაგროვებს, გამოიყენებს, შეინახავს და გაანადგურებს ორგანიზაცია მონაცემებს? რა არის მონაცემთა წყარო? აპირებთ თუ არა მონაცემების ვინმესთვის გაზიარებას? ხშირად, სასარგებლოა ვიზუალური დიაგრამის ან მონაცემთა ნაკადების ასახვის სხვა საშუალებების გამოყენება. მაღალი საფრთხის შემცველი დამუშავების რომელი ტიპებია გამოყენებული?

- <u>აღწერეთ დამუშავების მასშტაბი</u>: აღწერეთ მონაცემების სახეები — იგეგმება თუ არა განსაკუთრებული კატეგორიის მონაცემების დამუშავება? რა მოცულობის მონაცემების შეგროვებას და გამოყენებას გეგმავთ? რა სიხშირით? რა დროის მანძილზე შეინახავთ მათ? რამდენ ადამიანს შეეხება? რა გეოგრაფიულ ტერიტორიას მოიცავს?

- <u>აღწერეთ დამუშავების კონტექსტი</u>: რა სახის ურთიერთობა გაკავშირებთ იმ ადამიანებთან, რომელთა მონაცემებსაც დაამუშავებთ? რა სახის კონტროლი ექნებათ მათ ამ პროცესზე? მოსალოდნელია თუ არა მათთვის, რომ მათ მონაცემებს ამ გზით გამოიყენებთ? მოიცავს თუ არა პროცესი ბავშვების ან სხვა მოწყვლადი ჯგუფების მონაცემების დამუშავებას? არსებობს თუ არა წარსული უარყოფითი გამოცდილება ამ ტიპის დამუშავების ან უსაფრთხოების ხარვეზების შესახებ? არის თუ არა ამგვარი დამუშავება სიახლე, ნებისმიერი თვალსაზრისით? როგორია თანამედროვე ტექნოლოგიების მდგომარეობა ამ სფეროში? არსებობს თუ არა დამუშავების ამ პროცესთან მიმართებით საზოგადოებისთვის აქტუალური ისეთი საკითხები, რომლებიც უნდა გაითვალისწინოთ? ხართ თუ არა

რაიმე ქცევის კოდექსის ან სერტიფიცირების პროგრამის ხელმომწერი (მას შემდეგ, რაც ის დამტკიცდა)?

- <u>აღწერეთ დამუშავების მიზანი ან მიზნები</u>: რისი მიღწევა გსურთ? რა მოსალოდნელ გავლენას მოახდენს ის ადამიანებზე? რა სარგებელი მოაქვს დამუშავებას, როგორც უშუალოდ თქვენთვის, ისე — უფრო ფართო მასშტაბით?

- <u>განსაზღვრეთ შეფასების პროცესში მონაწილე პირები</u>: მოიფიქრეთ, თუ როგორ უნდა ჩართოთ შეფასების პროცესში შესაბამისი დაინტერესებული მხარეები: აღწერეთ, როდის და როგორ გაიგებთ მონაცემთა სუბიექტების მოსაზრებებს — ან დაასაბუთეთ, თუ რატომ არ არის ამის გაკეთება მიზანშეწონილი. ვისი ჩართულობა გჭირდებათ თქვენი ორგანიზაციიდან? გჭირდებათ თუ არა თქვენი დამუშავებაზე უფლებამოსილი პირების დახმარება? გეგმავთ თუ არა ინფორმაციის უსაფრთხოების ექსპერტებთან ან სხვა ექსპერტებთან კონსულტაციას?

- <u>დეტალურად დაასაბუთეთ დამუშავების აუცილებლობა და თანაზომიერება</u>: აღწერეთ შესაბამისობისა და პროპორციულობის ზომები, კერძოდ: დამუშავების რა კანონიერი საფუძველი გაქვთ? აღწევს თუ არა დამუშავება თქვენს მიზანს? არსებობს თუ არა სხვა გზა იმავე შედეგის მისაღწევად? როგორ აიცილებთ თავიდან თავდაპირველ მიზანთან შეუთავსებელი მიზნით დამუშავებას? როგორ უზრუნველყოფთ მონაცემთა ხარისხს და მონაცემთა მინიმიზაციას? რა ინფორმაციას მიაწვდით მონაცემთა სუბიექტებს? როგორ შეუწყობთ ხელს მათი უფლებების დაცვას? რა ზომებს იღებთ დამუშავებაზე უფლებამოსილი პირების მოქმედებების კანონთან შესაბამისობის უზრუნველსაყოფად? როგორ იცავთ მონაცემებს საერთაშორისო გადაცემების დროს?

- <u>გამოავლინეთ და შეაფასეთ საფრთხეები</u>: აღწერეთ საფრთხის წყარო(ები) და მონაცემთა სუბიექტებზე პოტენციური ზემოქმედების ხასიათი. საჭიროებისამებრ, დაურთეთ შესაბამისობასთან დაკავშირებული და კორპორაციული რისკები. როგორია საფრთხის ალბათობა — დაბალი, საშუალო თუ მაღალი? როგორი იქნება ზიანის სიმძიმე — მინიმალური, მნიშვნელოვანი თუ სერიოზული?

- <u>შეამცირეთ საფრთხეები</u>: განსაზღვრეთ საშუალო ან მაღალი საფრთხეების შემცირების ან აღმოფხვრის ზომები. რა შედეგი აქვს საფრთხეების შემცირების ზომებს: საფრთხეები აღმოიფხვრა, შემცირდა თუ დასაშვებად ჩაითვალა? როგორია ნარჩენი საფრთხე — დაბალი, საშუალო თუ მაღალი? დამტკიცდა თუ არა საფრთხის შემცირების ზომები და თუ არა — რატომ?

არსებობს თუ არა ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის მაღალი ალბათობა?
თუ მონაცემთა დაცვაზე ზეგავლენის შეფასება მიუთითებს, რომ მონაცემთა დამუშავება, მაღალი ალბათობით, ქმნის ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხეს, აუცილებელია, მიღებულ იქნას ყველა საჭირო ზომა ამ რისკების მნიშვნელოვნად შესამცირებლად. დამუშავება დაუშვებელია, თუ ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის შემცირება შეუძლებელია ორგანიზაციული და ტექნიკური ღონისძიებების გატარებით. მკაცრად რეკომენდებულია კონსულტაციების გავლა პერსონალურ მონაცემთა დაცვის სამსახურთან, რათა განისაზღვროს, არსებობს თუ არა ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის მაღალი რისკი და არის თუ არა რისკების შემცირების ეს ზომები საკმარისი.

- <u>მიუთითეთ, როგორ განხორციელდა მონაცემთა დაცვაზე ზეგავლენის შეფასება</u>: აღრიცხეთ, ვინ დაუჭირა მხარი ან უარყო საფრთხის შემცირებისთვის განკუთვნილი ესა თუ ის ღონისძიება. შეიტანეთ დამტკიცებული ღონისძიებები პროექტის გეგმაში, მიუთითეთ მათი დასრულების თარიღები და განსაზღვრეთ მათ შესრულებაზე პასუხისმგებლობა. აღრიცხეთ, ვინ მიიჩნია არსებული საფრთხეები სათანადოდ შემცირებულად. აღრიცხეთ შეფასების პროცესში მონაწილე პირების მოსაზრებები. აღრიცხეთ მონაცემთა დაცვის ოფიცრის პოზიცია, მათ შორის, საფრთხის შემცირების ზომების, ასევე, დამუშავების პროცესის კანონშესაბამისობის შესახებ. აღრიცხეთ, გათვალისწინებულ იქნა თუ არა მონაცემთა დაცვის ოფიცრის რეკომენდაციები.

მონაცემთა დამუშავების გამჭვირვალობის უზრუნველყოფა[27]

გამჭვირვალობა არის კანონით გათვალისწინებული ყოვლისმომცველი პრინციპი, რომელიც არსებითად უკავშირდება სამართლიანობისა და ანგარიშვალდებულების პრინციპებს და მიზნად ისახავს მონაცემთა სუბიექტების ნდობის ჩამოყალიბებას მათი მონაცემების დამუშავების პროცესების მიმართ. კანონით განსაზღვრული გამჭვირვალობის პრინციპის დაცვის უზრუნველყოფის ინსტრუმენტად შეიძლება გამოყენებულ იქნეს ამ მიზნით შექმნილი დოკუმენტაცია - კონფიდენციალობის პოლიტიკები, კონფიდენციალობასთან დაკავშირებული შეტყობინებები, იგივე, კონფიდენციალურობის განცხადებები.[28] კონფიდენციალობასთან დაკავშირებული შეტყობინებები მონაცემთა სუბიექტებს საშუალებას აძლევს, მიიღონ ინფორმაცია მათი

[27] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლები 4, 13, 24, 25 და 32.
[28] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 4.

მონაცემების დამუშავების პროცესების შესახებ და, საჭიროების შემთხვევაში, სადავოდ გახადონ ეს პროცესები.

კონფიდენციალობასთან დაკავშირებული შეტყობინებების მიზანია, მიაწოდოს მონაცემთა სუბიექტებს სათანადო ინფორმაცია, რათა ხელი შეუწყოს მათი უფლებების რეალიზებას. მონაცემთა დამუშავების პროცესის შესახებ კანონით გათვალისწინებული ინფორმაცია მონაცემთა სუბიექტებს უნდა მიეწოდოთ მონაცემთა შეგროვებამდე ან შეგროვების დაწყებისთანავე, მარტივ და გასაგებ ენაზე. ამ ინფორმაციის მიწოდება შეიძლება ზეპირად ან წერილობით.[29] კანონის თანახმად, მონაცემთა სუბიექტებს უნდა მიეწოდოთ, სულ მცირე, შემდეგი ინფორმაცია:

- დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის (ასეთის არსებობის შემთხვევაში) ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია;

- ინფორმაცია მონაცემთა დამუშავების მიზნებისა და სამართლებრივი საფუძვლების შესახებ;

- სავალდებულოა თუ არა მონაცემების მიწოდება;

- დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური ინტერესები (თუ ეს წარმოადგენს დამუშავების საფუძველს);

- პერსონალურ მონაცემთა დაცვის ოფიცრის ვინაობა და საკონტაქტო ინფორმაცია;

- მონაცემთა მიმღების ვინაობა;

- ინფორმაცია მონაცემთა დაგეგმილი გადაცემის შესახებ;

- რამდენ ხანს შეინახება მონაცემები; და

- მონაცემთა სუბიექტების უფლებები.

აუცილებელია, მონაცემთა სუბიექტებს მიეწოდოთ პროცესის სრულყოფილად აღქმისთვის საკმარისი ინფორმაცია, თუმცა, ამავდროულად, ეს ინფორმაცია უნდა იყოს ლაკონური, გამჭვირვალე, გასაგები და ადვილად ხელმისაწვდომი — ასეთ დროს

[29] ინფორმაციის მიწოდება შეიძლება ზეპირად ან წერილობით (მათ შორის, ელექტრონულად), გარდა იმ შემთხვევისა, როდესაც მონაცემთა სუბიექტი ინფორმაციის წერილობით მიღებას ითხოვს. *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 24(5). ინფორმაციის ზეპირად მიწოდების შემთხვევაში, რეკომენდებულია წერილობით აღირიცხოს მიწოდებული ინფორმაციის შინაარსი, თარიღი და მეთოდი.

მნიშვნელოვანია სათანადო ბალანსის დაცვა. ორგანიზაციებს შეუძლიათ შემოქმედებითად მიუდგნენ ამ ამოცანას და ამ ბალანსის დასაცავად, საჭიროების შემთხვევაში, გამოიყენონ ინფორმაციის მიწოდების ისეთი მეთოდები, როგორებიცაა ხატულები, „ემოჯიები“, დიაგრამები, აუდიო და ვიდეო მასალები და სხვა საშუალებები.

ინფორმაციის სისრულესა და აღქმადობას შორის ბალანსის დასაცავად, კონფიდენციალურობის შესახებ შეტყობინებები მონაცემთა სუბიექტებს შეიძლება მიეწოდოთ ე.წ. „მრავალშრიანი“ მიდგომით, სხვადასხვა ინფორმაციის შემცველი ბმულების სათანადო ადგილზე დართვით. ამგვარი მეთოდის გამოყენებისას, მომხმარებელი თავად შეძლებს მისთვის სასურველი ინფორმაციის არჩევასა და გაცნობას.

ინციდენტები[30]

მონაცემთა დაცვის ოფიცრის საქმიანობა ინციდენტების თავიდან აცილებაში საკვანძო როლს თამაშობს, რამდენადაც მას აკისრია ორგანიზაციის მრჩევლისა და კანონთან შესაბამისობის ზედამხედველობის ფუნქციები. პერსონალურ მონაცემებთან დაკავშირებული ინციდენტის დადგომის შემთხვევაში, მონაცემთა დაცვის ოფიცერი უნდა იყოს ინციდენტზე რეაგირებისთვის პასუხისმგებელ პირთა ჯგუფის წევრი. მონაცემთა დაცვის ოფიცერი ჩართული უნდა იყოს ისეთ ამოცანებში, როგორიცაა: ინციდენტზე რეაგირების პროცედურებთან დაკავშირებული დოკუმენტაციისა და ინციდენტების შესახებ ინფორმაციის აღრიცხვის წარმოება, ასევე პერსონალურ მონაცემთა დაცვის სამსახურისთვის და მონაცემთა სუბიექტებისთვის შეტყობინებების მომზადება.

ინციდენტი არის „მონაცემთა უსაფრთხოების დარღვევა, რომელიც იწვევს მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას/მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას“.[31] ინციდენტების მაგალითებია:

- მესამე პირის მიერ მონაცემებზე უნებართვო წვდომა;
- დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის წინასწარგანზრახული ან უნებლიე ქმედება (ან უმოქმედობა);
- პერსონალური მონაცემების არასწორი მიმღებისთვის გაგზავნა;
- პერსონალური მონაცემების შემცველი მოწყობილობების დაკარგვის ან მოპარვის ფაქტი;

[30] *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლები 29, 30.
[31] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 3(წ).

- პერსონალური მონაცემების შეცვლა ნებართვის გარეშე; ასევე
- პერსონალური მონაცემების ხელმისაწვდომობის დაკარგვა,
- და სხვა.

ორგანიზაციის მიერ დოკუმენტურად განსაზღვრული ინციდენტებზე რეაგირების წესები უნდა მოიცავდეს ინფორმაციას იმის შესახებ, თუ როგორ უზრუნველყოფს ორგანიზაცია: ინციდენტის შედეგად წარმოქმნილი ზიანის იდენტიფიცირებას, მასზე რეაგირებას და მის შემცირებას. ამგვარი წესების არსებობა მნიშვნელოვანია, რამდენადაც, მათი არსებობის პირობებში, მკაფიოდ არის განსაზღვრული ინციდენტის აღმოჩენის შემთხვევაში ორგანიზაციის მიერ გასატარებელი ღონისძიებები. ინციდენტზე რეაგირების პროცედურები უნდა აღწერდეს იმ ნაბიჯებს, რომლებიც უნდა გადაიდგას ინციდენტის აღმოჩენის შემდეგ. მაგალითად:

- <u>ნაბიჯი პირველი: დადგინდეს, ეხება თუ არა ინციდენტი პერსონალურ მონაცემებს</u>. გახსოვდეთ, რომ პერსონალური მონაცემები არის ნებისმიერი ინფორმაცია, რომელიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს, მაგალითად, სახელები, გვარები და მისამართები. პერსონალური მონაცემების შემცველად ასევე შეიძლება ჩაითვალოს ფოტოები, სოციალურ მედიაში დატოვებული კომენტარები, სხვა ჩანაწერები და ა.შ.

- <u>ნაბიჯი მეორე: დადგინდეს, რა სახის პერსონალური მონაცემების უსაფრთხოება დაირღვა</u>. განსაზღვრეთ, რა ტიპის და მოცულობის პერსონალურ მონაცემებს შეეხო ინციდენტი. ამის დადგენისთვის, შესაძლოა, სასარგებლო იყოს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვის მიზნით შექმნილ რეესტრში მოცემული ინფორმაციის გაცნობა. გასათვალისწინებელია პერსონალური მონაცემების ტიპი და ოდენობა, რამდენადაც რისკის შეფასებისთვის საჭირო იქნება კონკრეტული ფაქტობრივი მოცემულობის შესაფერისი მეთოდის შერჩევა. მაგალითად, მნიშვნელოვანი ზიანის გამომწვევ ინციდენტად ჩაითვლება ისეთი შემთხვევები, როდესაც უსაფრთხოება დაირღვა მოწყვლადი პირების სენსიტიურ ინფორმაციასთან მიმართებით, ან ისეთ ფინანსურ ინფორმაციასთან მიმართებით, რომლის არამართლზომიერმა გამოყენებამ შეიძლება ვინაობის მითვისება გამოიწვიოს. რაც უფრო სენსიტიურია მონაცემები, მით მაღალია მათი უსაფრთხოების დაცვის აუცილებლობა და მათდამი დამდგარი ინციდენტისგან მომდინარე შესაძლო უარყოფითი შედეგის სიმძიმე.

- <u>ნაბიჯი მესამე: განისაზღვროს, ვის შეიძლება მოეპოვებინა წვდომა პერსონალურ მონაცემებზე</u>. თუ ინციდენტის შედეგად არაუფლებამოსილმა პირმა მიიღო მონაცემებზე წვდომა ან ადგილი ჰქონდა მონაცემების დაკარგვას/მოპარვას, შეაფასეთ, ვის შეიძლება ჰქონდეს წვდომა მონაცემებზე ახლა. იმ შემთხვევაში, თუ პერსონალური მონაცემები ვინმეს შეცდომით გაეგზავნა ან ინფორმაციაზე

თქვენი ნებართვის გარეშე ჰქონდათ წვდომა ან ინფორმაცია დაიკარგა/მოიპარეს — მნიშვნელოვანი ზიანის გამოწვევის რისკის ხარისხს დიდწილად ის განაპირობებს, თუ ვინ მოიპოვა მონაცემებზე წვდომა. მაგალითად, თუ შეცდომით გაგზავნილი ელ-ფოსტის ადრესატი თქვენივე ორგანიზაციის ერთ-ერთი განყოფილებაა, მაშინ რისკი იმაზე მცირეა, ვიდრე იგივე ელ-ფოსტის კომპანიის გარეთ, უცნობ პირთან გაგზავნის შემთხვევაში იქნებოდა.

- ნაბიჯი მეოთხე: განისაზღვროს, რამდენ ადამიანს შეეხო ინციდენტი. მნიშვნელოვანია, დადგინდეს, რამდენი ადამიანის პერსონალურ მონაცემების მიმართ დადგა ინციდენტი. ინციდენტი, მისი სპეციფიკის გათვალისწინებით, შეიძლება მხოლოდ რამდენიმე პირის პერსონალურ მონაცემებს შეეხოს, ან იყოს უფრო მასშტაბური ხასიათის და ასობით ათასი ადამიანის მონაცემების უსაფრთხოების დარღვევაში გამოიხატოს.

- ნაბიჯი მეხუთე: შეფასდეს მონაცემთა სუბიექტებზე ინციდენტის შესაძლო გავლენის სიმძიმე. დაადგინეთ, რა შეიძლება მოჰყვეს ინციდენტს მონაცემთა სუბიექტების უფლებებისა და ინტერესების მიმართ, კერძოდ — მოსალოდნელია თუ არა რაიმე სახის ზიანი. ინციდენტის შესაძლო შედეგების შეფასება დაგეხმარებათ გადაწყვიტოთ, რა უნდა მოიმოქმედოთ, რათა შეამციროთ უარყოფითი გავლენა და დაიცვათ ადამიანები შესაძლო შემდგომი ზიანისგან. მაგალითად, დააზუსტეთ, არიან თუ არა ინციდენტში ჩართული მოწყვლადი ზრდასრულები ან ბავშვები; ჩააყენებს თუ არა ინციდენტი ვინმეს სახიფათო მდგომარეობაში; ემუქრება თუ არა ადამიანებს ინციდენტის შედეგად ფულის, სამუშაოს ან საცხოვრებლის დაკარგვის რისკი; იმოქმედებს თუ არა ინციდენტი ადამიანების ჯანმრთელობასა და კეთილდღეობაზე.

- ნაბიჯი მეექვსე: აღირიცხოს ინციდენტთან დაკავშირებული ინფორმაცია. დეტალურად აღრიცხეთ, თუ რა რეაგირება განახორციელა ორგანიზაციამ კონკრეტულ ინციდენტზე. მათ შორის, ინფორმაცია იმის შესახებ, თუ როგორ მოხდა ინციდენტის გამოვლენა და კონტროლი, როგორ შემცირდა მონაცემთა სუბიექტებისთვის ზიანის მიყენების რისკი, რა ღონისძიებები იქნა გატარებული დარჩენილი რისკის სამართავად. გარდა ამისა, მიუთითეთ განხორციელებული ღონისძიებები და ნაბიჯები, რომლებიც განხილული იყო, თუმცა, არ გადადგმულა. აღნიშნული ინფორმაცია საჭირო იქნება პერსონალურ მონაცემთა დაცვის სამსახურისთვის და მონაცემთა სუბიექტებისთვის შეტყობინების ვალდებულების შესასრულებლად, აგრეთვე, მონაცემთა დამუშავების შესახებ ინფორმაციის აღრიცხვის მიზნით შექმნილ რეესტრში შესატანად.

- ნაბიჯი მეშვიდე: შეფასდეს მონაცემთა სუბიექტებისა და სხვა პირებისთვის ზიანის დადგომის ალბათობა.[32] მონაცემთა სუბიექტებისთვის ზიანის მიყენების

[32] *იხილეთ* პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მიერ გამოცემული ნორმატიული აქტი, რომელიც განსაზღვრავს ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი

ალბათობის შეფასებისას გათვალისწინებულ უნდა იქნას როგორც ინციდენტის თავდაპირველი აღმოჩენის მომენტისთვის არსებული, ისე შემდგომი ფაქტობრივი მდგომარეობა.

ინციდენტის შედეგად მნიშვნელოვანი ზიანის მიყენების ან/და ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შექმნის ალბათობის შეფასებისას დაფიქრდით, ვინ შეიძლება დაზარალდეს, რა არის ასეთ პირთა რიცხოვნობა და როგორ აისახება ეს მათზე. ინციდენტმა შეიძლება დაბალი, საშუალო ან მაღალი ალბათობით დააზარალოს ადამიანების უფლებები და თავისუფლებები და/ან მნიშვნელოვანი საფრთხე შეუქმნას ამ უფლებებსა და თავისუფლებებს.

ალბათობის გათვალისწინება ინციდენტის შეფასებისას:		
დაბალი	ნაკლებად სავარაუდოა, რომ ინციდენტი გამოიწვევს მნიშვნელოვან ზიანს და/ან მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს	მაგალითად, მონაცემთა სუბიექტებს შეიძლება ინციდენტი საერთოდ არ შეეხოს ან მხოლოდ უმნიშვნელოდ შეეხოს (დასჭირდეთ სისტემაში ხელახლა შესვლა, ახალი პაროლის დაყენება და ა.შ.)
საშუალო	ინციდენტმა შეიძლება გამოიწვიოს მნიშვნელოვანი ზიანი და/ან მნიშვნელოვანი საფრთხე შეუქმნას ადამიანის ძირითად უფლებებსა და თავისუფლებებს, ამასთან, ასეთი ზიანის/საფრთხის არსებობისა და არარსებობის ალბათობები მეტ-ნაკლებად თანაბარია.	მაგალითად, მონაცემთა სუბიექტებს შეიძლება შეექმნათ მნიშვნელოვანი პრობლემები, რომლებსაც ისინი გადალახავენ გარკვეული სირთულეების მიუხედავად (დამატებითი ხარჯები, არააუცილებელ მომსახურებაზე ხელმისაწვდომობის დროებით დაკარგვა, სტრესი, შიში და ა.შ.)
მაღალი	ინციდენტი დიდი ალბათობით გამოიწვევს მნიშვნელოვან ზიანს და/ან მნიშვნელოვან საფრთხეს	მაგალითად, მონაცემთა სუბიექტებს შეიძლება მიადგეთ მნიშვნელოვანი ზიანი, რომლის დაძლევაც სერიოზულ სირთულეებთან არის

საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებსა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესს.

	შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს	დაკავშირებული (ჯანმრთელობის გაუარესება, სამუშაოს ან სახსრების დაკარგვა, ქონების დაზიანება და ა.შ.) ან შეუქცევადი ზიანი, რომლის დაძლევაც შეუძლებელია (სოლიდური ვალი, გრძელვადიანი ფსიქოლოგიური პრობლემები, ფიზიკური დაზიანება ან სიკვდილი და ა.შ.)

- <u>ნაბიჯი მერვე: შეტყობინებების ვალდებულების შესრულება</u>.[33] დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს შესაბამისი შეტყობინების ვალდებულებების შესრულება, თუ ინციდენტი საშუალო ან მაღალი ალბათობით გამოიწვევს მნიშვნელოვან ზიანს ან მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ასეთი ინციდენტის აღმოჩენიდან არაუგვიანეს 72 საათისა, მის შესახებ წერილობით ან ელექტრონულად შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს. შეტყობინება უნდა შეიცავდეს დეტალურ ინფორმაციას ინციდენტისა და მის სამართავად მიღებული ზომების შესახებ. თუ ინციდენტი მაღალი ალბათობით გამოიწვევს ამგვარ ზიანს, დამუშავებისთვის პასუხისმგებელი პირი ასევე ვალდებულია ინციდენტის შესახებ დაუყოვნებლივ აცნობოს მონაცემთა სუბიექტებს, რომელთაც ეს ინციდენტი შეეხო. აღსანიშნავია, რომ დამუშავებაზე უფლებამოსილი პირი ვალდებულია ინციდენტის შესახებ დაუყოვნებლივ აცნობოს დამუშავებისთვის პასუხისმგებელ პირს.

მონაცემთა დაცვის ოფიცრის პასუხისმგებლობაა, იზრუნოს იმაზე, რომ ორგანიზაციაში დასაქმებულმა პირებმა იცოდნენ ინციდენტზე რეაგირების პროცედურებისა და მექანიზმების არსებობის შესახებ და აცნობიერებდნენ საკუთარ როლს. სასურველია, ორგანიზაციის მიერ განსაზღვრული ინციდენტებზე რეაგირების წესების ეფექტიანობა რეგულარულად მოწმდებოდეს იმიტირებული სავარჯიშოების მეშვეობით. აღნიშნულ წესებში, საჭიროებისამებრ, უნდა შედიოდეს სათანადო ცვლილებები, პრაქტიკაში გამოვლენილი ნაკლოვანებების აღმოსაფხვრელად.

[33] გაითვალისწინეთ, რომ ინციდენტის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურის შეტყობინების წესს ადგენს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი. *იხილეთ* საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლები 29(9) და 30(4).

რეკომენდაციების შეჯამება

პერსონალურ მონაცემთა დაცვის ოფიცერი უმნიშვნელოვანეს როლს ასრულებს ორგანიზაციის საქმიანობის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან შესაბამისობის უზრუნველყოფისა და აღნიშნულის დემონსტრირების თვალსაზრისით. მონაცემთა დაცვის ოფიცერი, როგორც მონაცემთა დაცვასთან დაკავშირებული საკითხების ექსპერტი, ეხმარება ორგანიზაციას მონაცემთა კანონშესაბამისად დამუშავების მიმართ არსებული რისკების ამოცნობაში, ამ რისკების ანალიზსა და მათ შემცირებაში.

მონაცემთა დაცვის ოფიცერი ხელს უწყობს ორგანიზაციის მიერ წარმართული მონაცემთა დამუშავების პროცესების კანონთან შესაბამისობას, მათ შორის, ანგარიშვალდებულების ისეთი ინსტრუმენტების დანერგვაში ჩართულობის გზით, როგორებიცაა მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა და, საჭიროების შემთხვევაში, მონაცემთა დაცვაზე ზეგავლენის შეფასება. მონაცემთა დაცვის ოფიცერი ორგანიზაციას აწვდის ინფორმაციას მონაცემთა დაცვასთან დაკავშირებული წესების შესახებ და უზრუნველყოფს სათანადო კვალიფიციურ კონსულტაციას, ეხმარება კანონთან შესაბამისობის უზრუნველსაყოფად მისაღები ზომების განსაზღვრაში, აგრეთვე მოქმედებს, როგორც საკონტაქტო პირი პერსონალურ მონაცემთა დაცვის სამსახურსა და მონაცემთა სუბიექტებთან ურთიერთობაში.

პერსონალურ მონაცემთა დაცვის სამსახურის მიერ გაცემული ამ სარეკომენდაციო მინიმალური სტანდარტების თანახმად, სათანადო ცოდნის მქონე მონაცემთა დაცვის ოფიცერი, მისი ამ პოზიციაზე განსაზღვრის ან დანიშვნის მომენტისთვის უნდა ფლობდეს (ან დანიშვნიდან/განსაზღვრიდან უმოკლეს დროში უნდა შეიძინოს) შემდეგს:

- <u>ცოდნა</u>: „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის დანაწესის ცოდნა, რათა შეძლოს ამ კანონის მოთხოვნების ინტერპრეტირება და მათზე დაყრდნობით სათანადო რეკომენდაციების მიწოდება, დაეხმაროს ორგანიზაციას, პერსონალური მონაცემები დაამუშაოს კანონისა და პერსონალურ მონაცემთა დაცვის სამსახურის ხელმძღვანელის, მათ შორის, შემდეგი ნორმატიული აქტების შესაბამისად:
    - ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმები და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესი;
    - მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმები და შეფასების წესი;
    - იმ პირთა წრის განსაზღვრის შესახებ, რომლებსაც არ აქვთ ვალდებულება დანიშნონ/განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი;

- პერსონალურ მონაცემთა დაცვის სამსახურში სპეციალური წარმომადგენლის რეგისტრაციის პროცედურა.

- უნარები: მონაცემთა დაცვის ოფიცრის როლისთვის განსაზღვრული სხვადასხვა ფუნქციების შესრულების უნარი:

  - ინფორმირებისა და ცნობიერების ამაღლების ფუნქცია;

  - საკონსულტაციო ფუნქცია;

  - ორგანიზაციული ფუნქცია;

  - თანამშრომლობის ფუნქცია;

  - კანონთან შესაბამისობის უზრუნველყოფის ფუნქცია.

- პიროვნული თვისებები: კეთილსინდისიერება და მონაცემთა დაცვის ოფიცრის ფუნქცია-მოვალეობების შესრულებისთვის საჭირო უნარები.

პერსონალურ მონაცემთა დაცვის ოფიცერს უნდა ჰქონდეს სიღრმისეული ცოდნა ორგანიზაციის მიერ წარმართული მონაცემთა დამუშავების პროცესების კანონთან შესაბამისობის დემონსტრირებისთვის შესამუშავებელი დოკუმენტაციის წარმოების შესახებ.