პერსონალურ მონაცემთა
დაცვის სამსახური

რეკომენდაციები
პერსონალურ მონაცემთა დაცვის ოფიცრისთვის

www.pdps.ge

რეკომენდაციები ემსახურება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ნორმათა განმარტებას, საუკეთესო პრაქტიკის დამკვიდრების ხელშეწყობას, ის არ წარმოადგენს სამართლებრივ აქტს, არის სარეკომენდაციო ხასიათის და არ წარმოშობს დამატებით უფლებებსა და ვალდებულებებს.

შინაარსი

შესავალი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მსგავსად ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციისა“, ამკვიდრებს საჯარო დაწესებულებებსა და კერძო ორგანიზაციებში პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ან განსაზღვრის ვალდებულებას, ადგენს ოფიცრის ცნებას და აწესრიგებს მასთან დაკავშირებულ სხვა ძირითად საკითხებს.[1] წინამდებარე რეკომენდაცია განმარტავს პერსონალურ მონაცემთა დაცვის ოფიცრის ინსტიტუციურ როლს, მისი დანიშვნის ან განსაზღვრის სავალდებულო კრიტერიუმებსა და წესს, განსაზღვრავს ოფიცრის ფუნქციებს, მისი საქმიანობის ძირითად პრინციპებს, აგრეთვე, განიხილავს ოფიცრის პასუხისმგებლობის საკითხსა და გაწვევის შემთხვევებს.

წინამდებარე რეკომენდაციები მიზნად ისახავს, მათ შორის, კონკრეტულ პრაქტიკულ მაგალითებზე მითითებით, გაანალიზოს კანონმდებლობის ზემოაღნიშნული დანაწესი, რათა შესაბამისმა პასუხისმგებელმა სუბიექტებმა სრულყოფილად აღიქვან მათთვის დაკისრებული ვალდებულებების არსი და ფარგლები.

რეკომენდაციები მომზადებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) ნორმატიული შინაარსისა და „მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”) წინამორბედის — „29-ე სამუშაო ჯგუფის“ სახელმძღვანელო რეკომენდაციების[2] ისევე, როგორც საზღვარგარეთის პერსონალურ მონაცემთა დაცვის სამსახურების საუკეთესო პრაქტიკის, სხვადასხვა სამეცნიერო წყაროების ანალიზის საფუძველზე.

[1] აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 90-ე მუხლის თანახმად, 33-ე მუხლის („პერსონალურ მონაცემთა დაცვის ოფიცერი“) ამოქმედების თარიღად განსაზღვრა 2024 წლის 1 ივნისი. შეად. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 37-ე — 39-ე მუხლი, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016, 1-88.

[2] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2017, <https://ec.europa.eu/newsroom/article29/items/612048>. დამატებით პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ, იხ. „მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”) ვებგვერდი: <https://edpb.europa.eu/sme-data-protection-guide/data-protection-officer_en>.

1. პერსონალურ მონაცემთა დაცვის ოფიცრის ინსტიტუციური შინაარსი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი პერსონალურ მონაცემთა დაცვის ოფიცრის დეფინიციურ ცნებას არ ითვალისწინებს. კანონის მე-3 მუხლის „ფ“ ქვეპუნქტის თანახმად, მისი ტერმინოლოგიური განმარტება ოფიცრის მიერ განსახორციელებელ ფუნქცია-მოვალეობებს უკავშირდება. იგი არის პირი, რომელიც დამუშავებისთვის პასუხისმგებელ პირს ან დამუშავებაზე უფლებამოსილ პირს უწევს კონსულტაციას, ექსპერტულ რჩევებს პერსონალურ მონაცემთა დაცვის წესებთან შესაბამისობის შესახებ.[3]

„პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების პერსონალური მონაცემების დაცვის შესახებ“ ევროპის საბჭოს მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათის თანახმად, მონაცემთა დაცვის ოფიცრის დანიშვნა ან განსაზღვრა დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ იმ ერთ-ერთ ორგანიზაციულ-ტექნიკურ ღონისძიებას წარმოადგენს, რომლითაც შესაძლებელია მონაცემთა დაცვის წესებთან შესაბამისობის დემონსტრირება.[4] აღნიშნული უკავშირდება ანგარიშვალდებულების პრინციპს, რაც გულისხმობს მონაცემთა დამუშავებისთვის პასუხისმგებელი ან/და მონაცემთა დამუშავებაზე უფლებამოსილი პირების ვალდებულებას, მონაცემთა დამუშავების პრინციპების დაცვისა და მათთან შესაბამისობის დემონსტრირების თაობაზე.[5] ანგარიშვალდებულების გამოხატულებას წარმოადგენს სხვადასხვა ორგანიზაციულ-ტექნიკური ღონისძიებების მიღება, მაგალითად, პერსონალურ მონაცემთა დაცვის ოფიცრის განსაზღვრა ან დანიშვნა, მონაცემთა დაცვაზე ზეგავლენის შეფასების წინასწარ ჩატარება, დამუშავებული მონაცემის ფსევდონიმიზაცია და სხვა.[6] შესაბამისად, ოფიცრებს შეუძლიათ, პრევენციული ზეგავლენა მოახდინონ ორგანიზაციაზე სამართალდარღვევის არიდების მიზნით.[7]

---

[3] *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 198. *Matheson L.,* DPO Liability and Potential Insurance Coverage, <https://iapp.org/news/a/dpo-liability-and-potential-insurance-coverage/>.

[4] *Council of Europe,* Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 10.X.2018, § 87 (შემდგომში — „კონვენცია“).

[5] Art. 5(2), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016, 1-88 (შემდგომში - "GDPR").

[6] *Vrabec H. U.,* Data Subject Rights under the GDPR, with a Commentary through the Lens of the Data-driven Economy, Oxford, 2021, 225.

[7] *კატიჩი ი.,* მონაცემთა დაცვის ოფიცერი — „მონაცემთა დაცვის ძირითადი რეგულაციით“ განსაზღვრულ ამოცანებთან დაკავშირებული დარღვევების პრევენციის მექანიზმი, პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, N2, 2023, 71.

პერსონალურ მონაცემთა დაცვის ოფიცერი კლასიფიცირდება რამდენიმე ნიშნით:

- მონაცემთა დაცვის ოფიცერი შეიძლება იყოს როგორც **ფიზიკური,** ისევე **იურიდიული პირი.** ზოგიერთ შემთხვევაში, ორგანიზაციის მოცულობის და სტრუქტურის გათვალისწინებით, შესაძლოა, საჭირო იყოს ოფიცერთა გუნდის შექმნა.[8]

> ***მაგალითად,*** შესაძლებელია, ამგვარი ფუნქციით აღიჭურვოს კონკრეტული უწყების ან ინსტიტუტის სტრუქტურული ერთეული.

- მონაცემთა დაცვის ოფიცერი შესაძლებელია იყოს როგორც **შიდა ინსტიტუციური**, ისევე **გარე მოწვეული პირი**.[9] მაგალითად, შიდაინსტიტუციურ დონეზე განსაზღვრული ან დანიშნული ოფიცერი ინტეგრირებულია უწყების ან ინსტიტუტის ორგანიზაციულ სტრუქტურაში მაშინ, როდესაც გარე მოწვეული პირი გარიგებითსამართლებრივი (სახელშეკრულებო ურთიერთობის ფარგლებში) უწევს მომსახურებს მონაცემთა დამუშავებისთვის პასუხისმგებელ ან მონაცემთა დამუშავებაზე უფლებამოსილ პირებს.

> ***მაგალითად,*** მომსახურების ხელშეკრულების საფუძველზე, აუთსორსული მომსახურების გამწევი კომპანია.

- ასევე, შესაძლებელია **სავალდებულო** და **ნებაყოფლობითი ოფიცრის ინსტიტუტების** გამიჯვნა. როგორც მომდევნო თავებში იქნება განხილული, კანონმდებლობით განსაზღვრულ შემთხვევებში, ოფიცრის განსაზღვრა ან დანიშვნა სავალდებულოა[10], თუმცა აღნიშნული არ გამორიცხავს მონაცემთა დამუშავებისთვის პასუხისმგებელი ან/და მონაცემთა დამუშავებაზე უფლებამოსილი პირების მიერ ოფიცრის ნებაყოფლობით, თვითრეგულირებისა და საწესდებო ავტონომიის ფარგლებში დანიშვნას.

- დაბოლოს, შესაძლებელია **ინდივიდუალურად, ერთი ან რამდენიმე** და **საერთო** მონაცემთა დაცვის ოფიცრის ინსტიტუტის ურთიერთგამიჯვნა იქიდან გამომდინარე, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს

[8] *პერსონალურ მონაცემთა დაცვის სამსახური*, მსოფლიო პრაქტიკა, N1, 2024, 1-2. European Data Protection Board (EDPB), Designation and Position of Data Protection Officers, Adopted on 16 January 2024: <https://edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf>, [24.01.2024].

[9] *Voigt P., Bussche A.*, The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 57.

[10] მუხლი 33(1), „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 14/06/2023; შედარების მიზნით, იხ. Art. 37(1), GDPR.

კანონის 33-ე მუხლის მე-4 პუნქტის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელმა ან მონაცემთა დამუშავებაზე უფლებამოსილმა პირებმა, შესაძლებელია, განსაზღვრონ ან დანიშნონ საერთო ოფიცერი, თუკი უზრუნველყოფილი იქნება დაკისრებული ფუნქციების ჯეროვანი, სრულყოფილი შესრულება.[11]

მაგალითად, კორპორაციული კონსორციუმებისთვის, ორგანიზაციათა ჯგუფისთვის, ჰოლდინგური კომპანიებისათვის ერთი საერთო მონაცემთა ოფიცრის დანიშვნა.

შიდა მონაცემთა დაცვის ოფიცერი იძლევა რჩევებს, კონსულტაციებს მაშინ, როდესაც გარე მონაცემთა დაცვის ოფიცერი — მომსახურების გამწევი პირია. სამსახურებრივი ფუნქციის განხორციელების ეტაპზე, ორივე უზრუნველყოფს კანონშესაბამისობის საკითხზე კონსულტაციების გაცემას დამმუშავებლისათვის.

2. პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნა ან განსაზღვრა

2.1. სავალდებულო კანონისმიერი საფუძვლით

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი განსაზღვრავს სუბიექტთა იმ წრეს, ვისაც ეკისრება პერსონალურ მონაცემთა დაცვის ოფიცრის განსაზღვრის ან დანიშვნის ვალდებულება. კერძოდ, 33-ე მუხლის პირველი პუნქტის თანახმად, ყველა საჯარო დაწესებულება, სადაზღვევო ორგანიზაცია, კომერციული ბანკი, მიკროსაფინანსო ორგანიზაცია, საკრედიტო ბიურო, ელექტრონული კომუნიკაციის კომპანია, ავიაკომპანია, აეროპორტი, სამედიცინო დაწესებულება, აგრეთვე, დამუშავებისთვის პასუხისმგებელი პირი ან/და დამუშავებაზე უფლებამოსილი პირი, რომლებიც ამუშავებენ დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან ახორციელებენ მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს, ვალდებულნი არიან, დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი.

[11] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2017, 10.

ხსენებული პუნქტის განმარტების მიზნებისათვის, მნიშვნელოვანია **„დანიშვნისა“** და **„განსაზღვრის“** ტერმინოლოგიური მნიშვნელობის გამიჯვნა. გამომდინარე იქიდან, რომ ოფიცერი შესაძლებელია იყოს მომსახურების ხელშეკრულების საფუძველზე გარე მოწვეული პირიც, ეს უკანასკნელი *ინიშნება* უწყებაში ან ორგანიზაციაში აღნიშნულ პოზიციაზე[12] მაშინ, როდესაც უწყებაში ან ორგანიზაციაში დასაქმებული პირიც შესაძლებელია *განისაზღვროს* მონაცემთა დაცვის ოფიცრად[13].

ამდენად, კანონმდებლობა ითვალისწინებს იმ სექტორებს, რომლის წარმომადგენელ დაწესებულებებსაც აკისრიათ კანონისმიერი ვალდებულება, დანიშნონ/განსაზღვრონ ოფიცერი. ამავდროულად, იგივე პუნქტი მიუთითებს ოფიცრის დანიშვნის ვალდებულებაზე დამუშავებისთვის პასუხისმგებელ და დამუშავებაზე უფლებამოსილ იმ პირებთან მიმართებითაც, რომლებიც არ ექცევიან ზემოაღნიშნულ სექტორულ ჩამონათვალში, თუმცა ამუშავებენ დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან ახორციელებენ მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს.

ევროკავშირის „მონაცემთა დაცვის ზოგადი რეგულაცია“ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულებას სამ ცალკეულ შემთხვევაში ითვალისწინებს.[14] კერძო სექტორში ოპერირებად მეწარმე სუბიექტში ოფიცრის ინსტიტუტის არსებობა უკავშირდება მონაცემთა დამუშავებისთვის პასუხისმგებელი ან მონაცემთა დამუშავებაზე უფლებამოსილი პირების იმგვარ **„ძირითად საქმიანობას“**, რომლის ფარგლებში განხორციელებული ოპერაციები ფართო მასშტაბით ითვალისწინებს მონაცემთა სუბიექტის რეგულარულ, სისტემურ მონიტორინგს ან თუკი მათი ძირითადი საქმიანობა უკავშირდება განსაკუთრებული კატეგორიის მონაცემთა ფართომასშტაბიან დამუშავებას.[15] საგულისხმოა, რომ „ძირითადი საქმიანობა“ და მის ფარგლებში განხორციელებული ოპერაციების *ხარისხობრივი* და *რაოდენობრივი* მაჩვენებლები.

[12] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2017, 12.

[13] მუხლი 33(3), „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 14/06/2023.

[14] Artc. 37, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016, 1–88.

[15] იქვე, მუხლი 37(1).

მაგალითად, კომპანია აწარმოებს ონლაინ გაყიდვებს, რა მიზნითაც იგი ინახავს მომხმარებლების მონაცემებს. კომპანიის სამიზნეა ევროკავშირის მომხმარებლები, რომლებიც იმყოფებიან გერმანიაში, საფრანგეთსა და იტალიაში.

იმდენად, რამდენადაც კომპანია ამუშავებს მომხმარებლის პერსონალურ მონაცემებს, რათა წარმატებულად მართოს მისი ონლაინ მაღაზია და განახორციელოს დაკისრებული მოვალეობა, მონაცემთა დამუშავება წარმოადგენს დამატებით საქმიანობას კომპანიის ძირითად საქმიანობასთან მიმართებით. ამდენად, მას არ ევალება მონაცემთა დაცვის ოფიცრის დანიშვნა.[16]

მაგალითად, ორგანიზაცია „J“ ონლაინ სივრცეში ყიდის ავეჯს და იკვლევს ევროპულ ბაზარს მისი ბიზნესის გაფართოების მიზნით. ნებისმიერი პირი, ვინც ესტუმრება ვებგვერდს, ვალდებულია, დაეთანხმოს „მზა ჩანაწერების“ (“cookies”) გამოყენებას. „J“ აანალიზებს IP გეოლოკაციის მონაცემებს, რათა დაადგინოს ის ქვეყანა, სადაც იმყოფება მომხმარებელი (მომხმარებლის ადგილსამყოფელი). „J”-ის მიერ პერსონალური მონაცემების დამუშავების მიზანია დააიდენტიფიციროს, თუ რამდენი ევროპელი მომხმარებელი ესტუმრა ვებგვერდს და, ძირითადად, რა იყო მათი ინტერესის საგანი. მოცემულ მაგალითში, „J“ იყენებს ვებგვერდის მონიტორინგის (Tracking) მეთოდს, რათა ეტაპობრივად გააფართოვოს მისი ბიზნესი.

ვებგვერდის მონიტორინგი „J“-ს შესაძლებლობას აძლევს, შეისწავლოს ევროპული ბაზარი მისი ონლაინ მაღაზიის მეშვეობით. აქედან გამომდინარე, „J“-სთვის მონაცემთა დამუშავება წარმოადგენს მიზნის მიღწევის საშუალებას, რომლის შედეგადაც განავითარებს თავის ბიზნესს. ერთი მხრივ, „J“ ცდილობს, რომ განავითაროს ბიზნესის ახალი ხაზი, როგორც მისი ბიზნეს სტრატეგიის ნაწილი, რაც შეიძლება ჩაითვალოს „ძირითად საქმიანობად“ GDPR-ის მიხედვით. მეორე მხრივ, „J“ აკვირდება მთელ მსოფლიოში მის ვებგვერდზე შესული ნებისმიერი ადამიანის ქცევას, მათ შორის უკვე არსებული მომხმარებლების, რაც არის მარტივი ბიზნეს ანალიზი, რომელიც არ წარმოადგენს „ძირითად საქმიანობას“. თუმცა, „J“-ის დამუშავების სამიზნეა ევროპელი მომხმარებლები, რათა გააფართოვოს ბიზნესი ევროპაში. აღნიშნული არის „J“-ის ბიზნეს სტრატეგიის მნიშვნელოვანი ელემენტი. ამიტომ, **„J“-ს ეკისრება ოფიცრის დანიშვნის ვალდებულება.**[17]

[16] EU General Data Protection Regulation (GDPR) A Practical Guide, 2017, 54-55.

[17] იქვე.

2.1.1. დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემთა დამუშავება

კანონის 33-ე მუხლის პირველი პუნქტის თანახმად, თუკი მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ან/და მონაცემთა დამუშავებაზე უფლებამოსილი პირი ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტის მონაცემებს, აუცილებელია მონაცემთა დაცვის ოფიცრის დანიშვნა ან განსაზღვრა. მართალია, მონაცემთა დაცვის ოფიცრის მომწესრიგებელი ნორმა არ განსაზღვრავს მონაცემთა სუბიექტის დიდ ოდენობას, თუმცა კანონის სისტემური ანალიზის საფუძველზე[18], ამგვარ ოდენობად განისაზღვრება საქართველოს მოსახლეობის **არანაკლებ 3 პროცენტი**, რომელიც გამოითვლება მოსახლეობის აღწერის ბოლო შედეგების მიხედვით. საგულისხმოა, რომ დამუშავებისთვის პასუხისმგებელ პირთა და დამუშავებაზე უფლებამოსილ პირთა წრე, რომლებსაც არ აქვთ ვალდებულება, დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი, თანახმად კანონის 33-ე მუხლის მე-10 პუნქტისა, დგინდება პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტით, რომელიც მონაცემთა სუბიექტის დიდ ოდენობას აგრეთვე განსაზღვრავს საქართველოს მოსახლეობის არანაკლებ 3 პროცენტის ოდენობით.

მაგალითად, „სოციალური მედიაკომპანიები და საძიებო სისტემები არიან ისეთი კატეგორიის დამმუშავებლები, რომლებიც დამუშავების პროცესში ახორციელებენ მონაცემთა სუბიექტების ფართომასშტაბიან, რეგულარულ და სისტემატურ მონიტორინგს. ასეთი კომპანიების ბიზნესმოდელი ეფუძნება დიდი მოცულობის პერსონალურ მონაცემთა დამუშავებას. ისინი დიდ შემოსავალს იღებენ მიზნობრივი სარეკლამო მომსახურების შეთავაზებით, ასევე იმით, რომ კომპანიებს თავიანთ ვებგვერდებზე რეკლამების განთავსების შესაძლებლობას აძლევენ. მიზნობრივი რეკლამა გულისხმობს რეკლამის განთავსებას დემოგრაფიის, ასევე, მომხმარებელთა მსყიდველობითი ისტორიისა და ქცევის საფუძველზე, რაც საჭიროებს სისტემატურ მონიტორინგს მონაცემთა სუბიექტების ონლაინჩვევებსა და ქცევაზე.“[19]

[18] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 31-ე მუხლის მე-7 პუნქტი.

[19] *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 199-200.

2.1.2. ქცევის სისტემური და მასშტაბური მონიტორინგის განმსაზღვრელი კრიტერიუმები

აღსანიშნავია, რომ კანონი დამატებით არ განმარტავს ზემოაღნიშნულ მუხლში მოყვანილი ცალკეული ტერმინების, მათ შორის, მონაცემთა სუბიექტების ქცევის სისტემატური და მასშტაბური მონიტორინგის ცნებებს. ამ თვალსაზრისით, საყურადღებოა, რომ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტი, რომელიც ადგენს იმ კრიტერიუმებსა და გარემოებებს, რომელთა არსებობის შემთხვევაში, მონაცემთა დამუშავებისთვის პასუხისმგებელ ან/და მონაცემთა დამუშავებაზე უფლებამოსილ პირებს არ აქვთ ვალდებულება, დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი. აღნიშნული ნორმატიული აქტის მიხედვით, მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგად მიიჩნევა ისეთი აქტივობები, როგორიცაა: ა) ინტერნეტ აქტივობის თვალთვალი, სადაც ხდება მონაცემთა სუბიექტის წინასწარი რეგისტრაცია (მომხმარებლის შექმნა/აქტივაცია); ბ) პროფაილინგი ან ქულების მინიჭება რისკების შეფასების მიზნით; გ) ადრეული და სკოლამდელი აღზრდისა და განათლების დაწესებულების, ზოგადსაგანმანათლებლო დაწესებულების, სპეციალური პროფესიული საგანმანათლებლო დაწესებულების, უმაღლესი საგანმანათლებლო დაწესებულების მიერ ბავშვების, მოსწავლეების, მსმენელებისა და სტუდენტების ქცევის მონიტორინგი; დ) პერსონალურ მონაცემებზე დაფუძნებული ქცევითი რეკლამირება; ე) სატელეკომუნიკაციო ქსელების ოპერირება. თუმცა საგულისხმოა, რომ შესაძლებელია სხვაგვარი აქტივობაც წარმოადგენდეს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს ნორმატიული აქტით განსაზღვრული კრიტერიუმების დაკმაყოფილების შემთხვევაში.

მონიტორინგის სისტემატურობის შეფასებისას მხედველობაში მიიღება ისეთი კრიტერიუმები, როგორიცაა: მონაცემთა დამუშავების სიხშირე, მისი განგრძობადობა და პერიოდულად განმეორებითი ხასიათი; მონაცემთა დამუშავების წინასწარ დაგეგმილი ხასიათი, ორგანიზებულობა და თანმიმდევრულობა; მონაცემთა დამუშავება წარმოადგენს თუ არა დამუშავებისთვის პასუხისმგებელი პირის/დამუშავებაზე უფლებამოსილი პირის ძირითადი საქმიანობის ნაწილს. ხოლო რაც შეეხება მონაცემთა სუბიექტების ქცევის მონიტორინგის მასშტაბურობის შეფასებას, იგი განისაზღვრება შემდეგი გარემოებების მიხედვით: ა) მონაცემთა სუბიექტების რაოდენობა; ბ) დამუშავებული მონაცემების მოცულობა ან/და დამუშავებული მონაცემების სახეობათა სიმრავლე; გ) მონაცემთა დამუშავების

პროცესის ხანგრძლივობა; დ) მონაცემთა დამუშავების პროცესის გეოგრაფიული დაფარვა.

აქვე გასათვალისწინებელია, რომ სისტემატურ და მასშტაბურ მონიტორინგად არ მიიჩნევა დამუშავებისთვის პასუხისმგებელი პირის ან/და დამუშავებაზე უფლებამოსილი პირის ადმინისტრაციული თუ სამუშაო ადგილის ან დამხმარე ინფრასტრუქტურის ვიდეომონიტორინგის ფარგლებში მონაცემთა დამუშავება, გარდა ე. წ. „ჭკვიანი ვიდეოკამერების“ მეშვეობით მონაცემთა დამუშავებისა.

მაგალითად, ერთ-ერთი კომპანიის ვებგვერდი იყენებს ალგორითმებს, რათა საძიებო სისტემის გამოყენების საშუალებით დაადგინოს მისი მომხმარებლების ინტერესები და განხორციელებული შესყიდვები და, მიღებული ინფორმაციის საფუძველზე, მომხმარებლებს სთავაზობს რეკომენდაციებს. ვინაიდან, აღნიშნული ხორციელდება უწყვეტად და წინასწარ განსაზღვრული კრიტერიუმების მიხედვით, შეიძლება, მიჩნეულ იქნეს მონაცემთა სუბიექტების ფართომასშტაბიანი და სისტემატური მონიტორინგის მაგალითად.[20]

„მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”) წინამორბედი — „29-ე მუხლის სამუშაო ჯგუფის“ სახელმძღვანელო რეკომენდაციაში წარმოდგენილია ის ძირითადი კრიტერიუმი, რომლის მიხედვით შესაძლებელია პერსონალურ მონაცემთა დამუშავების ფართომასშტაბიანი ბუნების შეფასება:

- მონაცემთა სუბიექტების რაოდენობა;
- მონაცემთა მოცულობა ან/და კონკრეტული დამუშავებული მონაცემების მასშტაბი;
- მონაცემთა დამუშავების ხანგრძლივობა ან მუდმივობა;
- მონაცემთა დამუშავების გეოგრაფიული დაფარვა.[21]

მაგალითად, საავადმყოფოს მიერ პაციენტის მონაცემების რეგულარული დამუშავება; საზოგადოებრივი ტრანსპორტით მოსარგებლე პირთა მონაცემების დამუშავება.

[20] ICO, Data protection officers, ხელმისაწვდომია: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-officers/#ib1 [21.07.2023].

[21] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2017, 9.

2.2. ნებაყოფლობითი წესით

საჯარო უწყებებსა და კერძო ორგანიზაციებს, შეუძლიათ, დანიშნონ ან განსაზღვრონ მონაცემთა დაცვის ოფიცერი მაშინაც კი, როდესაც მათ არ აქვთ ამის სამართლებრივი ვალდებულება.[22] აღნიშნული გამომდინარეობს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 33-ე მუხლის მე-2 პუნქტიდან, რომლის თანახმად, კანონით გათვალისწინებულ ვალდებულებას დაქვემდებარებული სუბიექტების გარდა, სხვა დამუშავებისთვის პასუხისმგებელ პირებს, საკუთარი შეხედულებისამებრ, უფლება აქვთ, დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი.

ნებაყოფლობით პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ან განსაზღვრის ვალდებულების წარმომშობი პირობები, შესაძლებელია განსაზღვროს თავად მონაცემთა დამუშავებისთვის პასუხისმგებელმა ან/და მონაცემთა დამუშავებაზე უფლებამოსილმა პირებმა შიდაინსტიტუციური მონაცემთა დაცვის პოლიტიკის დოკუმენტი. შესაძლებელია, აღნიშნული დაეყრდნოს ისეთ ინდიკატორს ან საფუძვლებს როგორიცაა, მაგალითად, ორგანიზაციაში დასაქმებულ პირთა რაოდენობა, რომელსაც შემხებლობა აქვს პერსონალურ მონაცემთა ავტომატურ დამუშავებასთან,[23] ასევე, მონაცემთა იმგვარი დამუშავება, რომელიც ექვემდებარება მონაცემთა დამუშავებაზე ზეგავლენის შეფასებას ან თუკი პერსონალური მონაცემები მუშავდება კომერციული გადაცემის, ანონიმური გადაცემის ან ბაზრის, ან აზრის კვლევის მიზნებისთვის.[24]

აღსანიშნავია, რომ ნებაყოფლობით დანიშნული ან განსაზღვრული მონაცემთა დაცვის ოფიცრის მიმართ, აგრეთვე, ვრცელდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 33-ე მუხლი. [25]

[22] *Kuner Ch., Bygrave L. A., Docksey Ch.,* EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 694.

[23] იხ. მონაცემთა დაცვის შესახებ გერმანიის ფედერალური კანონის § 38, Bundesdatenschutzgesetz, (BDSG), 30/06/2017.

[24] იქვე.

[25] ანალოგიურია 29-ე სამუშაო ჯგუფის მიდგომა ნებაყოფლობით მონაცემთა დაცვის ოფიცერთან მიმართებით. იხ. *Kuner Ch., Bygrave L. A., Docksey Ch.,* EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 695.

2.3. პირთა წრე, რომლებსაც არ აქვთ ვალდებულება, დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი

როგორც აღინიშნა, კანონის 33-ე მუხლის მე-10 პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელ პირთა და დამუშავებაზე უფლებამოსილ პირთა წრე, რომლებსაც არ აქვთ ვალდებულება, დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი, განისაზღვრება პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტით. ხოლო აღნიშნულ პირთა წრის განსაზღვრისას მხედველობაში მიიღება 33-ე მუხლის პირველი პუნქტით დადგენილი კრიტერიუმები (მონაცემთა სუბიექტების რაოდენობა ან მათი ქცევის მონიტორინგის სისტემატური და მასშტაბური ხასიათი).

აღსანიშნავია, რომ ხსენებული ნორმატიული აქტის მიხედვით, პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნა და განსაზღვრა არ ევალება იმ დამუშავებისთვის პასუხისმგებელ ან/და დამუშავებაზე უფლებამოსილ პირებს, რომლებიც აკმაყოფილებენ შემდეგ პირობებს — ერთი მხრივ, ისინი არ უნდა წარმოადგენდნენ კანონის 33-ე მუხლის პირველი პუნქტით განსაზღვრულ პირთა წერს (კერძოდ, საჯარო დაწესებულებას, სადაზღვევო კომპანიას, კომერციულ ბანკს, მიკროსაფინანსო ორგანიზაციას, საკრედიტო ბიუროს, ელექტრონული კომუნიკაციის კომპანიას, ავიაკომპანიას, აეროპორტს, სამედიცინო დაწესებულებას). ასევე, დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირები ამუშავებს საქართველოს მოსახლეობის არაუმეტეს 3 პროცენტისა, რომელიც გამოითვლება მოსახლეობის აღწერის ბოლო შედეგების მიხედვით; აგრეთვე, საქართველოს მოსახლეობის არაუმეტეს 1 პროცენტის განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს, რომელიც გამოითვლება მოსახლეობის აღწერის ბოლო შედეგების მიხედვით. იგი არ ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს.

აქვე აღსანიშნავია, რომ მონაცემთა სუბიექტებად არ მიიჩნევიან დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირების დასაქმებული პირები, მიუხედავად მათი რაოდენობისა.

3. პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციები

3.1. პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციების კლასიფიკაცია

მნიშვნელოვანია, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა და მონაცემთა დამუშავებაზე უფლებამოსილმა პირებმა ხელი შეუწყონ ოფიცერს მისი ფუნქციების შესრულებაში, უზრუნველყონ აუცილებელი და სათანადო რესურსებით.[26] მონაცემთა დაცვის ოფიცერი უნდა მონაწილეობდეს რჩევების მიცემაში რისკების შეფასების შესახებ, ასევე, დამუშავებასთან დაკავშირებული ჩანაწერების წარმოებაში, ამდენად, იგი აუცილებელია, უზრუნველყოფილი იყოს სათანადო ადმინისტრაციული თუ ფინანსური რესურსებით, ინფრასტრუქტურითა და მოწყობილობით.[27] იმდენად, რამდენადაც მონაცემთა დაცვის ოფიცრის ფუნქცია, შესაძლებელია, შეითავსოს უწყების ან ორგანიზაციის არსებულმა თანამშრომელმა, მნიშვნელოვანია საკმარისი დროის გამოყოფა დაკისრებული ფუნქციების შესასრულებლად.[28] მონაცემთა დაცვის ოფიცრის ფუნქციებია:[29]

კანონშესაბამისობის უზრუნველყოფისა და პროცესის ზედამხედველობის ვალდებულება — მონაცემთა დამუშავებისთვის პასუხისმგებელი ან/და მონაცემთა დამუშავებაზე უფლებამოსილი პირებისთვის მონაცემთა დამუშავების თაობაზე სათანადო კონსულტაციის გაწევა, და ზედამხედველობის ვალდებულებებად. კანონის 33-ე მუხლის პირველი მუხლის „ა“ და „ბ“ ქვეპუნქტებზე დაყრდნობით, რაც გულისხმობს „მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე, მათ შორის, მარეგულირებელი სამართლებრივი ნორმების მიღების ან შეცვლის შესახებ, დამუშავებისთვის პასუხისმგებელი პირის, დამუშავებაზე უფლებამოსილი პირისა და მათი თანამშრომლების ინფორმირებას, მათთვის კონსულტაციისა და მეთოდური დახმარების გაწევას“; აგრეთვე, მონაცემთა დაცვის შესახებ შიდაინსტიტუციური რეგულაციებისა და მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის შემუშავებაში მონაწილეობას და დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ საქართველოს კანონმდებლობისა და შიდა ორგანიზაციული დოკუმენტების შესრულების მონიტორინგს.

---

[26] *პერსონალურ მონაცემთა დაცვის სამსახური,* მსოფლიო პრაქტიკა, N1, 2024, 1-2. European Data Protection Board (EDPB), Designation and Position of Data Protection Officers, Adopted on 16 January 2024: <https://edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf>, [24.01.2024].

[27] *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო,* მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 198.

[28] Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001, 13, <https://edps.europa.eu/sites/default/files/publication/10-10-14_dpo_standards_en.pdf> [26.04.2023].

[29] *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 60.

თანამშრომლობის ვალდებულება და წარმომადგენლობა საზედამხედველო ორგანოსთან — მონაცემთა დაცვის საზედამხედველო ორგანოსთან აქტიური კავშირი და თანამშრომლობა. კანონის 33-ე მუხლის პირველი მუხლის „დ“ ქვეპუნქტის მიხედვით, ოფიცერი უზრუნველყოფს პერსონალურ მონაცემთა დაცვის სამსახურისგან კონსულტაციების მიღებას, დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის წარმომადგენლობას სამსახურთან ურთიერთობაში, მისი მოთხოვნით ინფორმაციისა და დოკუმენტების წარდგენას და მისი დავალებებისა და რეკომენდაციების შესრულების კოორდინაციასა და მონიტორინგს.

ანალიტიკა, ინფორმირებისა და კონსულტაციების გაწევის ვალდებულება — რაშიც მოიაზრება მონაცემთა სუბიექტის საჩივრების განხილვა, მომართვის შემთხვევაში მონაცემთა სუბიექტის ინფორმირება მისი უფლებების შესახებ, მონაცემთა დამუშავებასთან დაკავშირებული განცხადებების ანალიზი და შესაბამისი რეკომენდაციების გაცემა, თანახმად კანონის 33-ე მუხლის პირველი პუნქტის „გ“ და ე“ ქვეპუნქტებისა.[30]

აღნიშნული ფუნქციების ჯეროვნად განხორციელების მიზნით, იგი უფლებამოსილია, ჩაატაროს ინსპექტირება, ჰქონდეს წვდომა პერსონალურ მონაცემებზე, გაეცნოს მონაცემთა სუბიექტების განცხადებებს და ამ მიზნით დამოუკიდებლად განახორციელოს ნებისმიერი ქმედება ეთიკის სტანდარტის ფარგლებში.[31]

ამასთანავე, აღსანიშნავია, რომ მონაცემთა დაცვის ოფიცერს, შესაძლებელია, მონაცემთა დაცვასთან დაკავშირებული სხვა ფუნქციებიც განესაზღვროს შესაძლებლობა მომსახურების ხელშეკრულების (სახელშეკრულებო თავისუფლების), უწყების დებულების ანდა ორგანიზაციის საწესდებო ავტონომიის ფარგლებში. აღნიშნულის შესაბამისად, კანონის 33-ე მუხლის პირველი პუნქტის „ვ“ ქვეპუნქტი ადგენს, რომ მონაცემთა დამუშავების სტანდარტების ამაღლების მიზნით იგი ახორციელებს სხვა ფუნქციებსაც. მაგალითად, თანამშრომლებისათვის შიდაინსტიტუციური ტრეინინგის ორგანიზება პერსონალურ მონაცემთა დაცვის თემატიკაზე.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ კომენტატორულ ლიტერატურაში წარმოდგენილია მონაცემთა დაცვის ოფიცერთა ფუნქციების ის კატეგორია, რომლებიც მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა ან/და

[30] იქვე.
[31] *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 12-13.

მონაცემთა დამუშავებაზე უფლებამოსილმა პირმა უნდა განახორციელოს მონაცემთა დაცვის ოფიცრის დახმარებით ან უშუალოდ მისი მეშვეობით:[32]

GDPR	ფუნქცია	კომენტარი
39-ე მუხლის პირველი პუნქტის “a” ქვეპუნქტი	ინფორმირება და ცნობიერების ამაღლება	„ევროპის მონაცემთა დაცვის ზედამხედველის“ (EDPS) განმარტებით, მონაცემთა დაცვის საკითხებზე ინფორმირება და ცნობიერების ამაღლება შეიძლება, განხორციელდეს თანამშრომელთა გადამზადების, შიდაინსტიტუციური რეკომენდაციების მომზადების ფორმითაც.
39-ე მუხლის პირველი პუნქტის “b” ქვეპუნქტი	კანონშესაბამისობის უზრუნველყოფა და მონიტორინგი	„29-ე მუხლის სამუშაო ჯგუფის“ განმარტებით, შესაბამისობის მონიტორინგის ფარგლებში, ოფიცერმა შეიძლება: ☑ დაამუშავოს ინფორმაცია დამუშავების საქმიანობის განსასაზღვრად; ☑ განახორციელოს დამუშავების პროცესების შესაბამისობის შემოწმება და ანალიზი; ☑ უზრუნველყოს დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირების ინფორმირება, მათთვის კონსულტაციებისა და რეკომენდაციების გაცემა.

[32] *Kuner Ch., Bygrave L. A., Docksey Ch.,* EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 713.

39-ე მუხლის პირველი პუნქტის “c” ქვეპუნქტი	კონსულტირება და საექსპერტო დასკვნის გაცემა	ოფიცერმა შეიძლება, რჩევა მისცეს ორგანიზაციას მონაცემთა დაცვის კანონმდებლობასთან დაკავშირებით ისეთ საკითხებზე, როგორიცაა: მონაცემთა დაცვაზე გავლენის შეფასება; რისკების შეფასება; ანგარიშვალდებულების პრინციპთან შესაბამისობის უზრუნველყოფა.

3.2. პერსონალურ მონაცემთა დაცვის ოფიცრის საქმიანობის ძირითადი პრინციპები

პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციებისა და ვალდებულებების სისტემური ანალიზიდან გამომდინარე, შესაძლებელია, მისი საქმიანობის შემდეგი ძირითადი პრინციპების განსაზღვრა:

3.2.1. კომპეტენტურობის პრინციპი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი არ ადგენს მონაცემთა დაცვის ოფიცრის საკვალიფიკაციო მოთხოვნებს, თუმცა 33-ე მუხლის მე-5 პუნქტის თანახმად, მას უნდა ჰქონდეს სათანადო ცოდნა მონაცემთა დაცვის სფეროში. აღნიშნული უკავშირდება მის მიერ კომპეტენტური შეფასებებისა და დასკვნების ჩამოყალიბების ვალდებულებას. დარგის საექსპერტო ცოდნა, აგრეთვე, უკავშირდება მის მიერ დაკისრებული მოვალეობის დამოუკიდებლად განხორციელების ვალდებულებას.[33] ამდენად, პერსონალურ მონაცემთა დაცვის ოფიცრის მიმართ მოქმედებს კომპეტენტურობის პრინციპი.

აღსანიშნავია, რომ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციაც“ არ ადგენს პირდაპირ მოთხოვნას მონაცემთა დაცვის ოფიცრის საკვალიფიკაციო მოთხოვნებზე, მათ შორის, ლიცენზირების საკითხზე. ევროპის კავშირის ინსტიტუციებში და ორგანოებში არსებული ოფიცრების მიმართ მოქმედი სტანდარტის თანახმად, ოფიცერს უნდა ჰქონდეს შესაბამისი კომპეტენცია, რასაც

[33] *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 56-57.

შესაძლებელია, ადასტურებდეს პროფესიული სერტიფიცირების შესაბამისი პროგრამა.[34]

სხვადასხვა ქვეყნების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების გამოცდილება:

გაერთანებულ სამეფოში სერტიფიცირება სავალდებულო არ არის[35]; "UK GDPR" მხოლოდ კვალიფიკაციის კრიტერიუმს ადგენს, რომელიც ოფიცრის კომპეტენციის მაღალ სტანდარტს აწესებს. თუმცა, არ არის დაკონკრეტებული, თუ როგორ უნდა დადასტურდეს აღნიშნული კომპეტენციის არსებობა.

გერმანიის „მონაცემთა დაცვის ფედერალურ აქტში" არ არის ცალსახად მითითებული ლიცენზირების თაობაზე. თუმცა, ამავე თავის ერთ-ერთ დებულებაში, სადაც საუბარია მონაცემთა დაცვის ოფიცრის ინსტიტუტზე, აღნიშნულია, რომ სერტიფიცირებას ახდენს ფედერალურ დონეზე არსებული საზედამხედველო ორგანო ან კონკრეტული მიწაზე არსებული საზედამხედველო ორგანო.[36]

ესპანეთის „მონაცემთა დაცვის აქტის" 34-35-ე მუხლებით რეგულირდება მონაცემთა დაცვის ოფიცრის დანიშვნის საკითხი. 35-ე მუხლი შეეხება ოფიცრის კვალიფიკაციას, რომლის თანახმად, იგი შესაძლებელია იყოს როგორც ფიზიკური, ისევე იურიდიული პირი, ხოლო მისი დანიშვნის წინაპირობებთან შესაბამისობის დადგენა შესაძლებელია ნებაყოფლობითი სერტიფიცირების მექანიზმის საფუძველზე, რომელიც მოიაზრებს შესაბამისი საუნივერსიტეტო ხარისხის არსებობას სამართალსა და მონაცემთა დაცვის დარგში.[37]

საფრანგეთის „მონაცემთა დაცვის აქტში" 2018 წელს განხორციელებული ცვლილების შესაბამისად, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო ("Commission nationale de l'informatique et des libertés") უფლებამოსილია, განსაზღვროს აკრედიტაციისა და სერტიფიცირების შესაბამისი სქემა და კრიტერიუმები, კერძოდ, იგი უფლებამოსილია, დაადგინოს იმ ორგანიზაციათა აკრედიტაციის კრიტერიუმი, რომელიც მოახდენენ მონაცემთა დაცვის ოფიცერთა შემდგომ სერტიფიცირებას. აგრეთვე, საზედამხედველო ორგანომ განსაზღვრა მონაცემთა დაცვის ოფიცერთა

[34] Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 <https://edps.europa.eu/sites/default/files/publication/10-10-14_dpo_standards_en.pdf>.

[35] <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/#ib6>.

[36] <https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0316>.

[37] <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673>.

სერტიფიცირების ის კრიტერიუმი, რომლის მიხედვით, აკრედიტირებული ორგანოები განახორციელებენ ოფიცერთა ლიცენზირებას.[38] აღსანიშნავია, რომ სერტიფიცირება სავალდებულო არ არის და მხოლოდ ნებაყოფლობითი მექანიზმია. იგი მხოლოდ უზრუნველყოფს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ დადგენილი კვალიფიკაციის მოთხოვნებთან შესაბამისობის დადასტურებას. შესაბამის ორგანოთა აკრედიტაციის ძირითადი კრიტერიუმებია: 1. უპირველესად, ასეთი ორგანო უნდა აკმაყოფილებდეს ISO (ISO/CEI 17024:2012) სტანდარტს, რომელიც პირთა სერტიფიცირების განმახორციელებელ ორგანოთა მიმართ მოქმედებს; 2. აკრედიტაციის მაძიებელმა ორგანომ უნდა წარადგინოს შესაბამისი განაცხადი მონაცემთა დაცვის საზედამხედველო ორგანოს სახელზე; 3. ოფიცრების სერტიფიცირება უნდა განახორციელოს წერილობითი გამოცდის გზით, რომლის ძირითადი ნაწილი ტესტური კითხვებია, ხოლო 30% — კაზუისტური. 4. აკრედიტაციის მაძიებელ ორგანიზაციას უნდა ჰქონდეს სერტიფიკატის გაცემის, განახლების შესაძლებლობა და საამისოდ შესაბამისი მონაცემთა ბაზა; 5. მას უნდა ჰყავდეს სერტიფიცირების კომიტეტი. აღსანიშნავია, რომ საფრანგეთს „მონაცემთა დაცვის აქტი“ არ კრძალავს აკრედიტაციის არმქონე ორგანოთა მიერ სერტიფიცირების კურსის განხორციელებას მონაცემთა ოფიცერთა ლიცენზირების ან გადამზადების მიზნით. რაც შეეხება კანდიდატთა სერტიფიცირების კრიტერიუმს, იგი განისაზღვრება ორი ძირითადი წინაპირობით: 1. *კანდიდატის სერტიფიცირების წინაპირობით:* ა) კანდიდატმა უნდა წარმოადგინოს შესაბამისი მოწმობა/დოკუმენტი, რომელიც დაადასტურებს მონაცემთა დაცვის სფეროში მის სულ მცირე ორწლიან პროფესიულ გამოცდილებას მონაცემთა დაცვის ოფიცრის პოზიციასთან მიმართებით; ბ) სულ მცირე ორწლიანი პროფესიული გამოცდილებისა და სულ მცირე 35 საათიანი პროფესიული ტრენინგის გავლის დამდასტურებელი მოწმობა, გაცემული შესაბამისი გადასამზადებელი ორგანოს მიერ. 2. *პროფესიული ცოდნისა და უნარების წინაპირობით,* რომელიც უკავშირდება მონაცემთა დაცვის სამართლის, დამუშავების პრინციპებისა და საფუძვლების, მონაცემთა დაცვაზე ზეგავლენის შეფასების, ინციდენტის ინფორმირების და სხვა დარგობრივი საკითხების სიღრმისეულ ცოდნას.[39]

ლატვიის მონაცემთა დაცვის ეროვნული კანონი არ ითვალისწინებს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციისგან“ განსხვავებულ მოთხოვნებს, თუმცა იგი ადგენს ოფიცრის სტატუსის მოპოვებისა და მონაცემთა დაცვის დარგში ცოდნის შემოწმების წესებს. „მონაცემთა დაცვის ოფიცრების კვალიფიკაციის შესახებ“ მინისტრთა კაბინეტის 2020 წლის 6 ოქტომბრის N620 დებულებით დეტალურად არის

[38] იხ. დოკუმენტის სრული ვერსია, <https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf>.
[39] <https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf>.

განსაზღვრული ოფიცრის საკვალიფიკაციო გამოცდის ჩატარების პროცედურა, გამოცდის შინაარსი და საკვალიფიკაციო გამოცდაზე გასვლის შესაბამისი საფასური. თუმცა, აღსანიშნავია, რომ საკვალიფიკაციო გამოცდის ჩაბარება სავალდებულო არ არის. გამოცდის ჩაბარების მსურველი კანდიდატი მიმართავს ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს, იხდის გამოცდის შესაბამის საფასურსა და საკვალიფიკაციო გამოცდის ჩაბარების შემდეგ, აღირიცხება საზედამხედველო ორგანოს მიერ შემუშავებულ და მის ვებგვერდზე გამოქვეყნებული კვალიფიციური ოფიცრების სიაში.[40] აღსანიშნავია ისიც, რომ საზედამხედველო ორგანო თავად უწევს სერტიფიცირების პროცესს ორგანიზებას.[41]

გარდა ზემოხსენებულისა, არსებობს არაერთი საერთაშორისო ორგანიზაცია, რომელიც დაინტერესებულ პირებს სთავაზობს ონლაინ სერტიფიცირების მექანიზმს (წერილობითი გამოცდის ჩაბარების გზით), მაგალითად: Apave Certification[42], IAPP Certification[43], ITCERTS[44], EU GDPR Training and Certification[45].

3.2.2. დამოუკიდებლობისა და მიუკერძოებლობის პრინციპი

ოფიცრის დამოუკიდებლობის უზრუნველყოფის მიზნით, დაუშვებელია მისთვის მონაცემთა დამუშავებისთვის პასუხისმგებელი ან/და მონაცემთა დამუშავებაზე უფლებამოსილის პირების მიერ რაიმე სახის ინსტრუქციის ან მითითებების მიცემა.[46] მონაცემთა დაცვის ოფიცერი უნდა იყოს აღჭურვილი შესაბამისი რესურსით, რაც უზრუნველყოფს მის მიერ ნაკისრი მოვალეობის დამოუკიდებლად, დროულად და კვალიფიციურად შესრულებას. ასევე, აკრძალულია მასზე რაიმე სახის ზეგავლენა ან ზეწოლა.

აღსანიშნავია, რომ პერსონალურ მონაცემთა დაცვის ოფიცერი არ არის უწყების ან ორგანიზაციის „თანამშრომელი“, შესაბამისად, იგი არ იმყოფება დამსაქმებელთან სუბორდინაციულ ურთიერთობაში. აღნიშნული უფრო მეტად უზრუნველყოფს მის პირდაპირ ანგარიშვალდებულებას უწყების ან ორგანიზაციის პირველი კატეგორიის მენეჯმენტთან და გამორიცხავს მათი მხრიდან ოფიცრის საექსპერტო შეფასების

[40] <https://www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=LV&c2=>.

[41]იხ. ლატვიის მონაცემთა დაცვის საზედამხედველო ორგანოს ვებგვერდი, <https://www.dvi.gov.lv/lv/datu-aizsardzibas-specialists>.

[42]<https://www.apave-certification.com/en/certification/data-protection-officer-dpo-skills-certification>.

[43] <https://iapp.org/certify/>.

[44]<https://www.itcerts.ca/certification-programs/certified-data-protection-officer/#:~:text=The%20DPO%20(Data%20Protection%20Officer,Foundation%20or%20ITC%2D34%3A%20LGPD>.

[45] <https://www.eugdpr.institute/dpo-certification/> [26.04.2023].

[46] *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 59.

საწინააღმდეგო მითითებების ან დავალებების მიცემის, ამგვარი მითითებებისა და დავალებების შეუსრულებლობის შემთხვევაში კი — მისი გაწვევის შესაძლებლობას.

მონაცემთა დაცვის ოფიცრის თაობაზე „მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”) მიერ გამოქვეყნებული უკანასკნელი კვლევის შედეგების თანახმად, მონაცემთა დაცვის ოფიცერს საკუთარი ფუნქციის განხორციელებისას უნდა ჰქონდეს სათანადო მხარდაჭერა; ამასთანავე, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებმა სხვადასხვა აქტივობის გამართვით უნდა უზრუნველყონ ოფიცერთა დამოუკიდებლობის ხარისხი; ხოლო მონაცემთა დამუშავებისთვის პასუხისმგებელმა და მონაცემთა დამუშავებაზე უფლებამოსილმა პირებმა შესაბამისად უნდა ჩართონ მონაცემთა დაცვის ოფიცრები სხვადასხვა ორგანიზაციულ საკითხში.[47]

დამოუკიდებლობისა და მიუკერძოებლობის პრინციპის ლოგიკური გაგრძელებაა სათანადო ანაზღაურების წესი, რომელიც საკანონმდებლო მოწესრიგების მიღმა, სახელშეკრულებო ურთიერთობის ფარგლებში შეთანხმების საგნად განიხილება.

3.2.3. ანგარიშვალდებულების პრინციპი

მონაცემთა დაცვის ოფიცერი ანგარიშვალდებულია უშუალოდ მონაცემთა დამუშავებისთვის პასუხისმგებელი ან მონაცემთა დამუშავებაზე უფლებამოსილი პირის პირველი რანგის ხელმძღვანელთა წინაშე.[48] საგულისხმოა, რომ კანონის 33-ე მუხლის მე-6 პუნქტის მიხედვით, პირველი რანგის ხელმძღვანელის წინაშე ანგარიშვალდებულება კონკრეტული ვითარების გათვალისწინებით განისაზღვრება. აღნიშნული, ასევე, გულისხმობს პერიოდული ანგარიშის წარდგენასაც.

„ევროპის მონაცემთა დაცვის ზედამხედველის“ (“EDPS”) რეკომენდაციის თანახმად, მონაცემთა დაცვის ოფიცერი არ უნდა იყოს უწყების ან ორგანიზაციის ვადიანი ან მოკლევადიანი ხელშეკრულებით დასაქმებული პირი; მას უნდა ჰქონდეს

[47] *პერსონალურ მონაცემთა დაცვის სამსახური,* მსოფლიო პრაქტიკა, N1, 2024, 1-2. European Data Protection Board (EDPB), Designation and Position of Data Protection Officers, Adopted on 16 January 2024: <https://edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf>, [24.01.2024].

[48] მუხლი 38(3), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016, 1–88.

ეკონომიკური სახსრების დამოუკიდებლად განკარგვის შესაძლებლობა და უნდა იყოს ანგარიშვალდებული მხოლოდ ორგანიზაციის უმაღლესი მენეჯმენტის წინაშე.[49]

3.2.4. კონფიდენციალურობის დაცვა

მონაცემთა დაცვის ოფიცერზე, ასევე, ვრცელდება კონფიდენციალურობის დაცვის ვალდებულება,[50] რაც შესაძლებელია ითქვას, შიდა ინსაიდერული ინფორმაციის დაცვის, პერსონალური მონაცემების უსაფრთოხების უზრუნველყოფის მიზანს ატარებს. აქვე, საგულისხმოა, რომ სახელშეკრულებო თავისუფლების ფარგლებში აღნიშნული ვალდებულების შეზღუდვა ან შემსუბუქება დაუშვებელია.

4. პერსონალურ მონაცემთა დაცვის სამსახურის ინფორმირება ოფიცრის დანიშვნის ან განსზღვრის შესახებ

კანონი ადგენს დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის მონაცემთა დაცვის ოფიცრის საკონტაქტო ინფორმაციის ვებგვერდზე (ასეთის არსებობის შემთხვევაში) ან სხვა ხელმისაწვდომი საშუალებით პროაქტიული გამოქვეყნების ვალდებულებას,[51] რაც, აგრეთვე, გამომდინარეობს კარგი საჯარო მმართველობისა და ანგარიშვალდებულების პრინციპიდან. აღნიშნული, უპირველესად, ემსახურება მონაცემთა სუბიექტის მიერ საკუთარი უფლებების მარტივად განხორციელებას. ამასთანავე, მონაცემთა დაცვის ოფიცრის დანიშვნის ან განსაზღვრის სამართლებრივი ნამდვილობის მნიშვნელოვანი წინაპირობაა პერსონალურ მონაცემთა დაცვის სამსახურის ინფორმირება.[52] კანონის 33-ე მუხლის მე-8 პუნქტიდან გამომდინარე, „მონაცემთა დაცვის ოფიცრის დანიშვნიდან ან განსაზღვრიდან, აგრეთვე, მისი შეცვლიდან 10 სამუშაო დღის ვადაში მისი ვინაობა და საკონტაქტო ინფორმაცია უნდა ეცნობოს პერსონალურ მონაცემთა დაცვის სამსახურს“. თავის მხრივ, სამსახური აღრიცხავს ოფიცრის ვინაობასა და მის საკონტაქტო ინფორმაციას და აქვეყნებს საჯაროდ.

---

[49] *European Data Protection Supervisor*, Data Protection Officer (DPO), <https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en> [20.01.2023].

[50] მუხლი 38(5), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016, 1–88.

[51] მუხლი 33(8), „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 14/06/2023.

[52] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2017, 10.

5. ინტერესთა კონფლიქტის აკრძალვა

კანონის 33-ე მუხლის მე-3 პუნქტის თანახმად, პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქცია შეიძლება შეასრულოს დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის თანამშრომელმა ან სხვა პირმა მომსახურების ხელშეკრულების საფუძველზე. ამასთან, პერსონალურ მონაცემთა დაცვის ოფიცერს უფლება აქვს, შეასრულოს სხვა ფუნქციაც, თუ აღნიშნული არ წარმოშობს ინტერესთა კონფლიქტს, ე. ი. ფუნქციურ შეუთავსებლობას.

დაუშვებელია, რომ მონაცემთა დაცვის ოფიცერი უწყებაში ან ორგანიზაციაში იკავებდეს იმგვარ პოზიციას ან თანამდებობას, რომელიც მას შესაძლებლობას მისცემს, განსაზღვროს მონაცემთა დამუშავების მიზანი და საშუალება.[53] შესაბამისად, იგი არ უნდა იყოს მონაცემთა დამუშავებისთვის პასუხისმგებელი ანდა მონაცემთა დამუშავებაზე უფლებამოსილი პირი. ამასთანავე, იგი არ უნდა იყოს პერსონალურ მონაცემთა დამუშავების სხვადასხვა პროცესებში ჩართული პირი.[54] ასევე, ოფიცერი პარალელურად არ უნდა ასრულებს იმგვარ ფუნქციას, რომელიც პირდაპირ წინააღმდეგობაში მოდის უწყების ან ორგანიზაციის მიერ დამუშავების პროცესების მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის უზრუნველყოფის ინტერესთან.[55]

მაგალითად, კონკრეტული პოზიციები შეიძლება, შეუთავსებელი იყოს ოფიცრის საქმიანობასთან და წარმოშვას ინტერესთა კონფლიქტი: აღმასრულებელი დირექტორი, დამუშავების მთავარი ოფიცერი, მთავარი ფინანსური ოფიცერი, მარკეტინგის დეპარტამენტის უფროსი, ადამიანური რესურსებისა თუ ინფორმაციული ტექნოლოგიების დეპარტამენტის უფროსი, საჯარო ინფორმაციის გაცემაზე პასუხისმგებელი პირი (საჯარო დაწესებულების შემთხვევაში) და ნებისმიერი სხვა თანამდებობა/ფუნქცია, რომლის ფარგლებშიც იგი, შესაძლოა, უშუალოდ იყოს ჩართული მონაცემთა დამუშავების პროცესში.[56]

აქვე, საყურადღებოა შემთხვევა, როდესაც დანიშნული მონაცემთა დაცვის ოფიცერი ამავდროულად სხვა დაწესებულებაშიც იკავებს რაიმე თანამდებობას. ასეთ დროს, დამოუკიდებლად უნდა შეფასდეს მისთვის დაკისრებული ფუნქციების განხორციელების შესაძლებლობა სხვა ფუნქციებთან მიმართებით.

[53] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2017, 24.
[54] *Voigt P., Bussche A.,* The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 60.
[55] *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 15.
[56] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2017, 16.

გასათვალისწინებელია, რომ ორგანიზაციის შიდასამართლებრივი ურთიერთობიდან ოფიცრის დანიშვნის საკითხზეც ანალოგიური წესები ვრცელდება. ინტერესთა კონფლიქტის მაგალითად შესაძლებელია დასახელდეს, ასევე, მაგალითი, როდესაც ოფიცერი ერთდროულად არის ორგანიზაციის იურიდიული მრჩეველი და მონაცემთა დაცვის ოფიცერი იმავე სექტორის სხვა უწყებაში.[57]

მაგალითად, ინტერესთა კონფლიქტის მოტივით, ბელგიის მონაცემთა დაცვის საზედამხდველო ორგანომ დამმუშავებელი 50 000 ევროს ოდენობით დააჯარიმა, რადგან მონაცემთა ოფიცრის პოზიციაზე დაინიშნა პირი, რომელიც ამავდროულად იყო კორპორაციული შესაბამისობის სამსახურის უფროსი, ფულის გათეთრების ანგარიშგების ოფიცერი.[58]

მაგალითად, სლოვენიის მონაცემთა დაცვის საზედამხედველო ორგანომ კომპანიის მთავარი აღმასრულებელი დირექტორის ან დირექტორთა ბორდის წევრის მონაცემთა დაცვის ოფიცრად დანიშვნის ფაქტი ინტერესთა კონფლიქტად ცნო და დაუშვებლად მიიჩნია. [59]

მაგალითად, 2019 წელს ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთი კორპორაცია 25 000 ევროს ოდენობით დააჯარიმა, რადგან მონაცემთა დაცვის ოფიცრის ფუნქცია შიდაკორპორაციულ სტრუქტურაში შექმნილ ორგანოს ე. წ. „მონაცემთა დაცვის შიდა ბორდს“ მიანიჭა, რომელიც დამმუშავებლის განმარტებით, სწორედ იმავე ფუნქციას ასრულებდა, რასაც მონაცემთა დაცვის ოფიცერი. [60]

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 38-ე მუხლის მე-6 პუნქტის თანახმად, შესაძლებელია, დაინიშნოს ნახევარ განაკვეთზე მომუშავე მონაცემთა დაცვის ოფიცერი, თუ სხვა მოვალეობები არ წარმოშობს ინტერესთა კონფლიქტს. თუმცა ევროკავშირის „მონაცემთა დაცვის ოფიცრის ქსელის“ (“EU DPO Network”) განმარტებით, ნახევარ განაკვეთზე მომუშავე ოფიცერს შეიძლება, არ

[57] იქვე, 706.
[58] Autorité de protection des données, Dossiernummer: DOS-2019-04309, 2020, <https://cedpo.eu/dpo-case-law/> [20.01.2023].
[59] *Informacijski pooblaščenec,* Advisory Opinion, N07121-1/2021/577, 2021, <https://gdprhub.eu/index.php?title=IP_-_07121-1/2021/577#Facts> [22.01.2023].
[60] *Agencia Española Proteccion Datós,* Resolución de procedimiento sancionador, Procedimiento Nº: PS/00417/2019, იხ.: <https://cedpo.eu/dpo-case-law/> [22.01.2023].

ჰქონდეს დროის სათანადო რესურსი სხვადასხვა პარალელური ამოცანების შესასრულებლად.[61]

„ევროპის მონაცემთა დაცვის ზედამხედველის“ (“EDPS”) მოსაზრებით, ინტერესთა კონფლიქტი სახეზეა, როდესაც ოფიცრის მიერ სხვა მოვალეობების განხორციელება ნეგატიურად აისახება პერსონალური მონაცემების დაცვაზე. აღნიშნულის საილუსტრაციოდ, „ევროპის მონაცემთა დაცვის ზედამხედველმა“ მაგალითად მოიყვანა ინტერესთა კონფლიქტის ისეთი შემთხვევა, როდესაც ოფიცერი ამავდროულად არის ადამიანური რესურსების ადმინისტრაციის უფროსი ან ინფორმაციული ტექნოლოგიების უფროსი.[62]

6. პერსონალურ მონაცემთა დაცვის ოფიცრის პასუხისმგებლობის საკითხი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ისევე, როგორც ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ არ ითვალისწინებს მონაცემთა დაცვის ოფიცრის პასუხისმგებლობის მომწესრიგებელ ცალკეულ დებულებას. პერსონალურ მონაცემთა დაცვის მომწესრიგებელ კანონმდებლობასთან შეუსაბამობისათვის ოფიცრის პირადი, პერსონალური პასუხისმგებლობა არ დგება იმდენად, რამდენადაც პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს შემოწმების სუბიექტს შესაბამისი უწყება ან ორგანიზაცია წარმოადგენს. კანონის 82-ე მუხლის თანახმად, პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან დაკავშირებული ვალდებულების შეუსრულებლობა გამოიწვევს სამართალდამრღვევის გაფრთხილებას, ხოლო პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მიერ ადმინისტრაციული სახდელის დადებიდან ერთი წლის განმავლობაში – სამართალდამრღვევის დაჯარიმებას 3 000 ლარის ოდენობით.

აღსანიშნავია, რომ მონაცემთა დაცვის ოფიცერზე ვრცელდება კეთილსინდისიერების პრინციპი სწორედ იმ უწყების ან ორგანიზაციის მიმართ, რომელშიც იგი იქნა დანიშნული ან განსაზღვრული.[63] ოფიცერი მოქმედებს შინაგანი პროფესიული რწმენის საფუძველზე და აქვს თითოეული შემთხვევის გულისხმიერად, დაყოვნების გარეშე შესწავლის ვალდებულება.[64] ამასთანავე, აღსანიშნავია, რომ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის მე-2 პუნქტი და 24-ე მუხლის პირველი პუნქტი განმარტავს, რომ დამუშავებისთვის პასუხისმგებელ პირს, და არა ოფიცერს მოეთხოვება, უზრუნველყოს და დაასაბუთოს, რომ მონაცემთა

[61] იქვე, 705.
[62] იქვე.
[63] *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 14-15.
[64] იქვე, 15.

დამუშავება ხორციელდება რეგულაციის მოთხოვნების შესაბამისად. ამასთანავე, აღსანიშნავია, რომ დაუშვებელია ოფიცრის დაჯარიმება ან პოზიციიდან გათავისუფლება მის მიერ ფუნქციების ჯეროვანი განხორციელების გამო, რაც მიუთითებს მის დამოუკიდებელ ავტონომიასა და დაცვის დამატებით გარანტიებზე.[65] მონაცემთა დამუშავებისთვის პასუხისმგებელი ან/და მონაცემთა დამუშავებაზე უფლებამოსილი პირების წინაშე ნაკისრ ვალდებულებათა არაკეთილსინდისიერი და არაჯეროვანი შესრულება მონაცემთა დაცვის ოფიცრის პირდაპირ პასუხისმგებლობას უკავშირდება. ამ თვალსაზრისით სხვადასხვა სამეცნიერო წყაროში საუბარია გარე, მოწვეული ოფიცრის სახელშეკრულებოსამართლებრივ პასუხისმგებლობაზე, ხოლო მონაცემთა სუბიექტის ჭრილში — მის დელიქტურ პასუხისმგებლობაზეც.[66]

მართალია, საერთაშორისოსამართლებრივი სტანდარტის თანახმად, ოფიცერი სარგებლობს სამართლებრივი დაცვის გარკვეული გარანტიებით, თუმცა მისი პასუხისმგებლობა არ არის სრულად შეზღუდული. სამსახურებრივი გულგრილობის, არაკომპეტენტური კონსულტაციების გაწევის შემთხვევაში, დამუშავებისთვის პასუხისმგებელ ან/და დამუშავებაზე უფლებამოსილ პირს შეუძლია, მოითხოვოს ოფიცრისგან მიყენებული იმ ზიანის ანაზღაურება, რომელიც მას საზედამხედველო ორგანოს მიერ ადმინისტრაციული პასუხისმგებლობის სახით დაეკისრა.[67] ცხადია, მოცემულ შემთხვევაში, მტკიცების ტვირთი დამმუშავებლის მხარეს დგას და მან უნდა დაამტკიცოს დამდგარ შედეგსა და ოფიცრის ქმედებას შორის მიზეზობრივი კავშირი დამდგარი ზიანის ანაზღაურების მიზნებისათვის. ამას გარდა, ოფიცერთან დადებული ხელშეკრულება შესაძლებელია, ცალკე აწესრიგებდეს აღნიშნულ საკითხს და ითვალისწინებდეს დავის გადაწყვეტის ალტერნატიულ საშუალებებსაც. უფრო მეტიც, კერძო მეწარმე სუბიექტის შემთხვევაში, შესაძლებელია, მიყენებული ზიანის ანაზღაურება მოითხოვოს კორპორაციის აქციონერმა დერივაციული სარჩელის ფარგლებშიც.[68]

აღსანიშნავია, რომ არაკომპეტენტური რჩევის ან სამსახურებრივი გულგრილობის გამოჩენის ეტაპზე, ოფიცერს ვერ დააჯარიმებს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო იმდენად, რამდენადაც საზედამხედველო ორგანოს კომპეტენცია შემოიფარგლება მონაცემთა დამუშავებისთვის პასუხისმგებელი ან/და

[65] GDPRhub Commentary, <https://gdprhub.eu/Article_38_GDPR#No_retaliation_or_penalties>.
[66] *Paal P. B., Pauly D. A.*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Kommentar, 3. Aufl., 2021, Art. 39, para. 11, 12.
[67] *Matheson L.*, DPO Liability and Potential Insurance Coverage, < https://iapp.org/news/a/dpo-liability-and-potential-insurance-coverage/>.
[68] იქვე.

მონაცემთა დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების კონტროლით, ხოლო ოფიცერი არც ერთ მათგანს წარმოადგენს.[69]

7. პერსონალურ მონაცემთა დაცვის ოფიცრის გაწვევა

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ისევე, როგორც ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ არ აწესრიგებს ოფიცრის გაწვევის, შესაბამისად, მასთან სამართლებრივი ურთიერთობის შეწყვეტის საკითხს. რეგულაციის 38(3)-ე მუხლის თანახმად, დაუშვებელია მონაცემთა დამუშავებისთვის პასუხისმგებელი ან დამუშავებაზე უფლებამოსილი პირების მიერ ოფიცრის პოზიციიდან გათავისუფლება ან მასზე რაიმე ჯარიმის დაკისრება, მასზე დაკისრებული ფუნქციების შესრულების გამო. ოფიცერი ვერ იქნება გაწვეული იმ მიზეზით, რომ მონაცემთა დამუშავების სხვადასხვა პროცესზე მის მიერ გაცემულ კონსულტაციას არ ეთანხმება მონაცემთა დამუშავებისთვის პასუხისმგებელი ან/და დამუშავებაზე უფლებამოსილი პირი.[70] აღნიშნული არ მიემართება ოფიცერთა მხრიდან უხეშ გაუფრთხილებლობას, მისი საქმიანობის რომელიმე ზემოხსენებული პრინციპის დარღვევას ან კანონდარღვევის შემთხვევებს.

საგულისხმოა, რომ მართლმსაჯულების ევროპულმა სასამართლომ 2022 წლის 22 ივნისის გადაწყვეტილებაში საქმეზე: “*Leistritz AG v. LH”* აღნიშნა, რომ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 38(3)-ე მუხლის მოთხოვნა ვრცელდება როგორც შიდა, ისე გარე ოფიცერზე; წევრი სახელმწიფოს ეროვნული კანონმდებლობა შესაძლებელია, ითვალისწინებდეს ოფიცერთან ხელშეკრულების შეწყვეტის შესაძლებლობას მხოლოდ სამართლიანი საფუძვლით, მაშინაც კი, თუკი ხელშეკრულების შეწყვეტა არ უკავშირდება ოფიცრის ამოცანების შესრულებას, რამდენადაც აღნიშნული ხელს არ უშლის ძირითადი რეგულაციით დასახული მიზნის მიღწევას.[71] აღნიშნული წარმოადგენს ოფიცრის დამოუკიდებლობის დამატებით გარანტს.[72] უფრო მეტიც, სასამართლოს შეფასებით, ეროვნული კანონმდებლობა შესაძლებელია, ითვალისწინებდეს ოფიცრის განთავისუფლებისაგან გაცილებით ძლიერი დაცვის მექანიზმს, ვიდრე ეს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციითაა“ დადგენილი.[73] ამასთანავე, ოფიცერთა დადებული

[69] იქვე.
[70] *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2017, 15.
[71] CJEU, C-534/20, *Leistritz AG v. LH* [2022], პარა. 23-24, 36.
[72] იქვე, პარა. 26.
[73] იქვე, პარა. 33-36.

ხელშეკრულება შესაძლებელია, ითვალისწინებდეს დამატებით სამართლებრივ მექანიზმს, რომელიც გულისხმობს ოფიცრის სამოქალაქო პასუხისმგებლობის დაზღვევასაც და მასთან დავის მოგვარების საშუალებებს.

ნატო ვაჩნაძის ქუჩა N° 7, თბილისი

ბაქოს ქუჩა N° 48, ბათუმი

(+995 32) 242 1000

office@pdps.ge