პერსონალურ მონაცემთა
დაცვის სამსახური

სახელმძღვანელო რეკომენდაცია

მონაცემთა მეზად დაფარვის პრიორიტეტი, რომორც აღტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას

რეკომენდაციის მიზანია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ნორმათა განმარტება და საუკეთესო პრაქტიკის დამკვიდრების ხელშეწყობა. ის არ წარმოადგენს სამართლებრივ აქტს, არის სარეკომენდაციო ხასიათის და არ წარმოშობს დამატებით უფლებებსა და ვალდებულებებს.

შინაარსი

შესავალი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, ევროპის კავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”)[1] მსგავსად, ითვალისწინებს მონაცემთა მეტად დაფარვის პრიორიტეტს, როგორც ახალი პროდუქტის ან მომსახურების შექმნისას ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებულ საწყის მეთოდს.[2] ტექნოლოგიური პროგრესისა და სხვადასხვა ელექტრონული მომსახურების განვითარებასთან დაკავშირებული რისკების პრევენციის მიზნით, კანონის 26-ე მუხლი მონაცემთა სუბიექტის უფლებების სათანადო დაცვის სტანდარტს და დამუშავებისთვის პასუხისმგებელი პირის მიერ შესასრულებელ რიგ ვალდებულებებს ადგენს.

წინამდებარე სარეკომენდაციო დოკუმენტი აანალიზებს მონაცემთა მეტად დაფარვის პრიორიტეტთან დაკავშირებულ ვალდებულებათა შინაარსს და ევროპის კავშირის „მონაცემთა დაცვის ძირითადი რეგულაციიდან“ გამომდინარე საერთაშორისო სტანდარტებს, დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირებისთვის მათთვის დაკისრებული მოვალეობების არსისა და ფარგლების განმარტების მიზნით.

რეკომენდაციები მომზადებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) ნორმატიული შინაარსის, „მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”) სახელმძღვანელო რეკომენდაციის, პერსონალურ მონაცემთა დაცვის ევროპული საზედამხედველო ორგანოების პრაქტიკისა და სხვა საერთაშორისო სტანდარტების ანალიზის საფუძველზე.

[1] 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.

[2] 26-ე მუხლი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი (14/06/2023; №3144-XIმსXმპ).

1. ახალი პროდუქტის ან მომსახურების შექმნის პროცესში „მონაცემთა მეტად დაფარვის პრიორიტეტის“ მნიშვნელობა

ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა მეტად დაფარვის პრიორიტეტი წარმოადგენს პრევენციულ ღონისძიებას, რომლის გათვალისწინება ხორციელდება მონაცემთა დამუშავების საშუალების განსაზღვრის ეტაპზე. აღნიშნული სტანდარტი ეხმარება დამუშავებისთვის პასუხისმგებელ პირს, დამუშავების პროცესის ყველა ეტაპი განახორციელოს კანონის მოთხოვნათა და მონაცემთა დამუშავების პრინციპების სრული დაცვით. სტანდარტის მიზანია კონფიდენციალურობისა და მონაცემთა დაცვის პრინციპების ინტეგრირება სისტემების შექმნის ეტაპზე და მონაცემთა დამუშავების პროცესში.

ახალი პროდუქტის ან მომსახურების შექმნისას „მონაცემთა მეტად დაფარვის პრიორიტეტთან“ დაკავშირებულ ვალდებულებებს ითვალისწინებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 26-ე მუხლი, რომლის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ახალი პროდუქტის ან მომსახურების შექმნის პროცესში, გაითვალისწინოს მონაცემთა დაცვის სტანდარტები და დანერგოს მონაცემთა დამუშავების ძირითადი პრინციპები.

დამუშავებისთვის პასუხისმგებელი პირი უნდა დარწმუნდეს, რომ მონაცემთა დამუშავება შეესაბამება პერსონალურ მონაცემთა დაცვის სტანდარტებს. ამასთან, კანონის 26-ე მუხლით გათვალისწინებული სტანდარტის შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები მონაცემთა დამუშავების პროცესში, რათა უზრუნველყოს მონაცემთა სუბიექტის უფლებების დაცულობა.[3] აღნიშნული ვალდებულება მჭიდროდაა დაკავშირებული ანგარიშვალდებულების პრინციპთან, რომლის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეძლოს მონაცემთა დაცვის მოთხოვნებთან შესაბამისობის დადასტურება.[4]

კანონის 26-ე მუხლის შესაბამისად, მონაცემთა მეტად დაფარვის პრიორიტეტი შედგება ორი კომპონენტისგან: ახალი პროდუქტის ან მომსახურების შექმნის

[3] მსგავსად ეროვნული მოწესრიგებისა, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ აგრეთვე იცნობს ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინებისა (“Privacy by Design”) და პირველად პარამეტრად მონაცემთა დაცვის (“Privacy by Default”) ვალდებულებას.

[4] Information Commissioner’s Office (ICO), Data Protection by Design and Default, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/>, [31.08.2024].

პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება (“Privacy by Design”)[5]; მონაცემთა დაცვა პირველად პარამეტრად (“Privacy by Default”)[6].

კანონის 26-ე მუხლის პირველ პუნქტით (“Privacy by Design”) განსაზღვრულია ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვასთან დაკავშირებული სტანდარტები და დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებები. მოცემულ შემთხვევაში, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს შემდეგი კრიტერიუმები: ახალი ტექნოლოგიები; განხორციელების ხარჯები;[7] დამუშავების ხასიათი, მასშტაბი, კონტექსტი და მიზანი; მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისთვის მოსალოდნელი რისკები; მონაცემთა დამუშავების პრინციპები. ამავდროულად, კონცეფციით გათვალისწინებული მოთხოვნების დანერგვისას გასათვალისწინებელია თითოეული ინდივიდუალური შემთხვევის მონაცემთა დამუშავების სპეციფიკა.[8]

კანონის 26-ე მუხლის მე-2 პუნქტი ითვალისწინებს მონაცემთა დაცვას „პირველად პარამეტრად“ (“Privacy by Default”). კერძოდ, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, პერსონალური მონაცემები დაამუშაოს კონკრეტული მიზნის შესაბამისად და ამ მიზნისთვის აუცილებლობის პრინციპით უნდა განისაზღვროს: შეგროვებულ მონაცემთა რაოდენობა; დამუშავების მასშტაბი; შენახვის ვადა; მონაცემებზე წვდომის საკითხები.

ზემოაღნიშნული კონცეფციები ერთმანეთთან მჭიდროდაა დაკავშირებული და მათი იმპლემენტაცია დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებების ნაწილია,[9] იმ შემთხვევაშიც, თუკი მონაცემთა დამუშავების პროცესში დამუშავებაზე უფლებამოსილი პირია ჩართული. კანონის 36-ე მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს ეკისრება ვალდებულება, მონიტორინგი გაუწიოს დამუშავებაზე უფლებამოსილ პირს მონაცემთა დამუშავების პროცესში. თუმცა პერსონალური მონაცემების არამართლზომიერი დამუშავების შემთხვევაში, პერსონალურ მონაცემთა დაცვის სამსახურის წინაშე, როგორც წესი, პასუხს აგებს დამუშავებისთვის პასუხისმგებელი პირი. ამასთანავე, დამუშავებაზე უფლებამოსილი პირის მეშვეობით

[5] 26-ე მუხლის პირველი პუნქტი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი.
[6] 26-ე მუხლის მე-2 პუნქტი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი.
[7] თანამედროვე ტექნოლოგიების განხორციელების ხარჯები.
[8] Swedish Authority for Privacy Protection (IMY), Privacy by design and privacy by default, <https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/privacy-by-design-and-privacy-by-default/>, [31.08.2024].
[9] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 5-6, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024]. აღნიშნული დოკუმენტის თარგმანი ქართულ ენაზე ხელმისაწვდომია პერსონალურ მონაცემთა დაცვის სამსახურის ვებგვერდზე.

მონაცემთა დამუშავება დასაშვებია მხოლოდ იმ შემთხვევაში, თუ იგი მონაცემთა სუბიექტის უფლებებისა და კანონის მოთხოვნების დასაცავად უზრუნველყოფს შესაბამისი ორგანიზაციული და ტექნიკური ზომების მიღებას[10]. აღნიშნულიდან გამომდინარე, აუცილებელია დამუშავებაზე უფლებამოსილმა პირმა, მონაცემთა დამუშავებისას, ნებისმიერ შემთხვევაში, გაითვალისწინოს კანონის მოთხოვნები.[11]

საგულისხმოა, რომ დამუშავებაზე უფლებამოსილი პირის მიერ შესრულებული მოქმედებები უნდა ექვემდებარებოდეს მუდმივ მონიტორინგს დამუშავებისთვის პასუხისმგებელი პირის მხრიდან. შესაბამისად, ხელშეკრულებით წინასწარ უნდა განისაზღვროს დამუშავებაზე უფლებამოსილი პირის ფუნქცია-მოვალეობები და მონაცემთა დამუშავებასთან დაკავშირებული შესაბამისი სტანდარტები.[12]

2. ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება (“Privacy by Design”) და მასთან დაკავშირებულ ტერმინთა დეფინიცია

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 26-ე მუხლის პირველი პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა როგორც დამუშავების საშუალებების განსაზღვრის, ისე უშუალოდ დამუშავების პროცესში, უნდა მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები. აღნიშნული ზომების შერჩევისას დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს: ტექნოლოგიური განვითარების მხრივ არსებული მდგომარეობა; უსაფრთხოების ზომების მიღებისთვის გასაწევი ხარჯები; მონაცემთა დამუშავების ხასიათი, მასშტაბი, კონტექსტი და მიზნები; მონაცემთა დამუშავების შედეგად მოსალოდნელი რისკები მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების თვალსაზრისით, მონაცემთა დამუშავების პრინციპები. თავის მხრივ, ტექნიკური და ორგანიზაციული ზომები უნდა უზრუნველყოფდეს მონაცემთა დამუშავების პრინციპების ეფექტიან იმპლემენტაციას და მონაცემთა დამუშავების პროცესში მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმების ინტეგრირებას.

---

[10] 36-ე მუხლის მე-5 პუნქტი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი.

[11] Information Commissioner’s Office (ICO), Data protection by design and default, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/>, [30.08.2024].

[12] Future of Privacy Forum, Christina Michelakaki and Sebastião Barros Vale, Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR, 2023, 10-11, <https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf?fbclid=IwY2xjawFAL9RleHRuA2FlbQIxMAABHZgKscp2JpFY9-2hARtejqzLZgLZA_WfT_ZyVdIQnelt9yCt22UgFzN9vg_aem_aBRFAWm79k_PdIn_2DAprw>, [31.08.2024].

დამუშავებისთვის პასუხისმგებელ პირს არსებული რისკების ადეკვატური ტექნიკური და ორგანიზაციული ზომების გათვალისწინების ვალდებულება დამუშავების პროცესის დაგეგმვის საწყის ეტაპზევე ეკისრება, რათა მონაცემთა დამუშავების პრინციპების დაცვა საწყისი ეტაპიდანვე იყოს უზრუნველყოფილი.[13] კერძოდ, მონაცემთა დაცვასთან დაკავშირებით კანონმდებლობით განსაზღვრული წესები გათვალისწინებული უნდა იქნეს დამუშავებისას გამოსაყენებელი ინფორმაციული ტექნოლოგიების სისტემის თუ პროცესის დაგეგმვის, შექმნის და დანერგვის პირველ ეტაპზევე, რაც უზრუნველყოფს საკანონმდებლო ვალდებულებისა და მონაცემთა სუბიექტის უფლებების სათანადო დაცულობას.[14]

კონცეფციის - „მონაცემთა დაცვის სტანდარტების გათვალისწინება პროდუქტის ან მომსახურების შექმნისას“ (“Privacy by Design)” მიზანია, დამუშავებისთვის პასუხისმგებელმა პირმა ნებისმიერი სისტემის თუ მომსახურების შექმნისას და მათი ფუნქციონირების პროცესში დანერგოს პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის სტანდარტები. აღნიშნული პრინციპი შეიძლება, ვრცელდებოდეს სხვადასხვა შემთხვევაზე, მაგალითად:

- ახალი ინფორმაციული ტექნოლოგიური სისტემების, მომსახურებისა და პროდუქტების შემუშავება, რომელთა ფუნქციონირების პროცესშიც მუშავდება პერსონალური მონაცემები;
- პირადი ცხოვრების ხელშეუხებლობის უფლებასთან კავშირში მყოფი ორგანიზაციული პოლიტიკის დოკუმენტების შემუშავება და შესაბამისი პრაქტიკის ჩამოყალიბება;
- პროდუქტების ფიზიკური მახასიათებლების განსაზღვრა;
- მონაცემთა გადაცემის/გაზიარების მომცველი პროცესის წამოწყება;
- პერსონალური მონაცემების თავდაპირველისგან განსხვავებული, ახალი მიზნებით დამუშავების შესახებ გადაწყვეტილებების მიღება.[15]

კონცეფცია “Privacy by Design“ მონაცემთა დამუშავების პროცესში ადგენს შვიდ ძირითად პრინციპს:

---

[13] European Commission, “What does data protection ‘by design’ and ‘by default’ mean?”, <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en>, [31.08.2024].

[14] Swedish Authority for Privacy Protection (IMY), Privacy by design and privacy by default, <https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/privacy-by-design-and-privacy-by-default/>, [31.08.2024].

[15] Information Commissioner’s Office (ICO), Data protection by design and default, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/>, [31.08.2024].

1. პროდუქტის ან მომსახურების შექმნისას, რისკების შესამცირებლად, პირველ რიგში, უნდა იქნას გათვალისწინებული პირადი ცხოვრების ხელშეუხებლობის უფლებასთან დაკავშირებული საკითხები;
2. უნდა შეგროვდეს მხოლოდ ის პერსონალური მონაცემები, რომლებიც აუცილებელია კანონიერი მიზნის მისაღწევად. ამასთან, მონაცემების ამგვარი დამუშავება უნდა განხორციელდეს კანონიერად და სამართლიანად;
3. პირადი ცხოვრების ხელშეუხებლობასთან დაკავშირებული საკითხები უნდა იქნეს გათვალისწინებული სისტემის ან პროცესის შექმნის საწყის ეტაპზევე;
4. უნდა დაბალანსდეს პირადი ცხოვრების ხელშეუხებლობის უფლება და მონაცემთა დამუშავების სხვა ინტერესები;
5. პერსონალური მონაცემები პროდუქტის ფუნქციონირების და მომსახურების ყველა ეტაპზე უნდა იქნეს დაცული;
6. თითოეული ტექნოლოგიის თუ პროცესის გამოყენების ფარგლებში, პერსონალური მონაცემები უნდა დამუშავდეს გამჭვირვალედ;
7. სისტემის შემმუშავებელმა პირებმა უნდა უზრუნველყონ მომხმარებლის პერსონალური მონაცემების კონფიდენციალურობა.[16]

2.1. ახალი ტექნოლოგიები

დამუშავებისთვის პასუხისმგებელ პირს მოეთხოვება, ინფორმირებული იყოს ტექნოლოგიურ პროგრესთან დაკავშირებული საკითხების შესახებ. რიგ შემთხვევებში, შეიძლება, საჭირო იყოს დარგის ექსპერტების ჩართულობა. პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების რეკომენდაციების თანახმად, აღნიშნული ცნება დინამიკურია და აუცილებელია ტექნოლოგიური პროგრესის პირობებში მათი მუდმივი შეფასება.[17] მისი სტატიკურად განსაზღვრა, დროის რომელიმე მონაკვეთში შეუძლებელია და შეფასება უნდა მოხდეს უწყვეტად. კანონის შესაბამისად, „ახალ ტექნოლოგიებზე“ მითითება დამუშავებისთვის პასუხისმგებელ პირს ავალდებულებს, სათანადო ტექნიკური და ორგანიზაციული ზომების განსაზღვრისას, გაითვალისწინოს ბაზარზე ხელმისაწვდომი ტექნოლოგიები.[18] აღნიშნული კრიტერიუმი ვრცელდება როგორც ტექნიკურ, ისე

[16] Daniela Ježová, Principle of Privacy by Design and Privacy by Default, 130, <https://rlr.iup.rs/wp-content/uploads/2020/12/10-Jezova.pdf>, [16.12.2024].

[17] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [31.08.2024].

[18] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 8,

ორგანიზაციულ ზომებზე. ორგანიზაციული ზომების მაგალითები, ასევე გულისხმობს შიდა პოლიტიკის დოკუმენტების მიღებას და მონაცემთა დაცვის მიმართულებით თანამშრომელთა გადამზადებას.[19] ამასთანავე, დამუშავებისთვის პასუხისმგებელ პირს უნდა ჰქონდეს ინფორმაცია მონაცემთა დამუშავების პროცესში ტექნოლოგიების დადებითი და უარყოფითი მხარეების შესახებ.[20]

მაგალითი:

ვებგვერდის ან აპლიკაციის შექმნის შემთხვევაში, აუცილებელია განისაზღვროს მომხმარებელთა მიერ პლატფორმით სარგებლობის შესახებ ინფორმაცია რამდენად ინახება მუდმივად. ამისათვის, სასურველია, დაინერგოს იმგვარი მექანიზმი, რომლის საშუალებითაც კონკრეტული აპლიკაციიდან სპეციალური ძალისხმევის ("Log Out") გარეშე, მომხმარებელი შეძლებს სისტემიდან გამოსვლას, მაგალითად, ვებგვერდის დატოვებით ან აპლიკაციის გამორთვით.[21]

2.2. განხორციელების ხარჯები

„განხორციელების ხარჯებში" მოიაზრება როგორც ზოგადი (მაგალითად, დრო), ასევე, ადამიანური და ფინანსური რესურსები. დამუშავებისთვის პასუხისმგებელმა პირმა სათანადო ორგანიზაციულ-ტექნიკური ზომებისა და მონაცემთა სუბიექტის უფლებების დაცვის საჭირო მექანიზმების განსაზღვრისას და გამოყენებისას, რომელთა მიზანია მონაცემთა დამუშავების პრინციპების ეფექტიანი იმპლემენტაცია, უნდა გაითვალისწინოს მათი განხორციელების ხარჯები. აღნიშნული კრიტერიუმის შესაბამისად, დამუშავებისთვის პასუხისმგებელმა პირმა მნიშვნელოვანია, ეფექტიანად მართოს ზოგადი ხარჯები. რიგ შემთხვევებში, მან შეიძლება გამოიყენოს

<https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024].

[19] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [31.08.2024].

[20] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 8, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024].

[21] Paul Voigt, The EU General Data Protection Regulation (GDPR), A Practical Guide, 63, 2017.

სხვა, ალტერნატიული ზომები, რომლებიც ნაკლებ ხარჯებთან იქნება დაკავშირებული.[22]

მაგალითი:

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთი საქმის განხილვისას, სხვა ხარვეზებთან ერთად, დაადგინა, რომ კომპანია მამხილებლებისგან ("whistleblowers") მოპოვებულ ინფორმაციას ფსევდონიმიზაციის გარეშე, კერძოდ, დაუშიფრავი ფორმით ინახავდა, რაც ვერ აკმაყოფილებდა სათანადო უსაფრთხოების ზომებს. საზედამხედველო ორგანოს შეფასებით, დამუშავებისთვის პასუხისმგებელმა პირმა ახალი პროდუქტისა და მომსახურების შექმნის პროცესში არ გაითვალისწინა მონაცემთა დაცვის სტანდარტები ("GDPR"-ის 25-ე მუხლი), რის გამოც დადგინდა დარღვევა.

ამავდროულად, საზედამხედველო ორგანომ არ გაიზიარა დამუშავებისთვის პასუხისმგებელი პირის მიერ წარმოდგენილი არგუმენტი იმის შესახებ, რომ მონაცემთა ფსევდონიმიზაციის ფორმა - დაშიფვრა დაკავშირებული იყო დიდ ხარჯებთან და, ასევე, არ წარმოადგენდა აუცილებლობას.[23] აღსანიშნავია, რომ სათანადო ზომების მიღების თაობაზე მტკიცების ტვირთი დამუშავებისთვის პასუხისმგებელ პირს ეკისრება.

2.3. დამუშავების ხასიათი, მასშტაბი, კონტექსტი და მიზნები

„დამუშავების ხასიათი" გაგებული უნდა იქნას, როგორც მონაცემთა დამუშავების თანმდევი მახასიათებლები. „მასშტაბში" იგულისხმება დამუშავების მოცულობა და ფარგლები. „კონტექსტი" დამუშავების გარემოებებს უკავშირდება, რომლებიც შესაძლოა, მონაცემთა სუბიექტის უფლებებსა და მოლოდინებზე გარკვეულ გავლენას

[22] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 8-9, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024].

[23] Future of Privacy Forum, Christina Michelakaki and Sebastião Barros Vale, Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR, 2023, 14, <https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf?fbclid=IwY2xjawFAL9RleHRuA2FlbQIxMAABHZgKscp2JpFY9-2hARtejqzLZgLZA_WfT_ZyVdIQnelt9yCt22UgFzN9vg_aem_aBRFAWm79k_PdIn_2DAprw>, [31.08.2024].

ახდენდეს, ხოლო „მიზანი“ დამუშავების ლეგიტიმურ ინტერესსა და მიზნებს მოიაზრებს. შესაბამისად, სათანადო ღონისძიებების განსაზღვრის პროცესში, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაითვალისწინოს: დამუშავების ხასიათი; მასშტაბი; კონტექსტი; მიზანი.[24]

2.4. მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისთვის მოსალოდნელი რისკები

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ არაერთი დებულებით არის გათვალისწინებული თანმიმდევრული, რისკზე დაფუძნებული მიდგომა, რომლის მიზანია სათანადო ტექნიკური და ორგანიზაციული ზომების მიღება ფიზიკური პირებისა და მათი პერსონალური მონაცემების დასაცავად. კანონის თანახმად, თუ მონაცემთა დამუშავებისას ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე, დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების ვალდებულება ეკისრება.[25] ზეგავლენის შეფასების პროცესში დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გამოავლინოს რისკები, რომლებმაც, შესაძლოა, საფრთხე შეუქმნას მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებს. შეფასების პროცესში, არსებითად მნიშვნელოვანია მონაცემთა დამუშავების პროცესის სიღრმისეული შესწავლა[26] და გამოვლენილი რისკების მინიმიზაცია.

წარმოდგენილი საკითხი მჭიდრო კავშირშია კანონის 31-ე მუხლით განსაზღვრულ მოთხოვნებთან, რომლებიც შეეხება მონაცემთა დაცვაზე ზეგავლენის შეფასებას. ამდენად, კანონით გათვალისწინებულ შემთხვევაში, დამუშავებისთვის

[24] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 9, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024].

[25] 31-ე მუხლის პირველი პუნქტი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი.

[26] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 9-10, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024].

პასუხისმგებელი პირი ვალდებულია, იხელმძღვანელოს აღნიშნული მუხლით გათვალისწინებული სტანდარტებით.[27]

მაგალითი:

საინფორმაციო ხასიათის ვებგვერდი დაინტერესებულ პირებს საშუალებას აძლევს, რომ სიახლეების შესახებ სტატიებზე წვდომა ჰქონდეთ თანხის გადახდის სანაცვლოდ. თანხის გადახდის ალტერნატივაა მომხმარებლის მიერ მისი პერსონალური მონაცემების დამუშავებაზე თანხმობა ქცევითი რეკლამის მიღების მიზნებისთვის. "GDPR"-ის 25-ე მუხლის პირველი პუნქტის შესაბამისად, რისკის შეფასებისას, მხედველობაში უნდა იქნას მიღებული ისეთი გარემოებები, როგორიცაა ნებაყოფლობითი თანხმობის გაცემის არარსებობა.

მოცემულ შემთხვევაში, მიზანშეწონილია, არსებობდეს სტატიებზე წვდომის უფასო საშუალება, რომელიც არ მოიაზრებს ქცევითი რეკლამების მიღებას.[28]

2.5. დამუშავების საშუალებების განსაზღვრისა და უშუალოდ დამუშავების პროცესში სათანადო ტექნიკური და ორგანიზაციული ზომების მიღება

ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების დანერგვა უნდა განხორციელდეს „დამუშავების საშუალებების განსაზღვრის დროს". მასში მოიაზრება დროის ის პერიოდი, როდესაც დამუშავებისთვის პასუხისმგებელი პირი იღებს გადაწყვეტილებას მონაცემთა დამუშავების განხორციელების ფორმისა და მექანიზმების შესახებ. სწორედ ამ ეტაპზე უნდა შეფასდეს მონაცემთა დამუშავების მიმართ მიღებული ღონისძიებები. აღნიშნულის მიზანი მონაცემთა სუბიექტის უფლებებისა და მონაცემთა დამუშავების პრინციპების დაცვაა. მითითებულ პროცესში უნდა იქნას გათვალისწინებული სწორედ ის კრიტერიუმები, როგორიცაა: ახალი ტექნოლოგიები; განხორციელების ხარჯები; დამუშავების ხასიათი, მასშტაბი, კონტექსტი და მიზნები; რისკები. მოცემულ შემთხვევაში, დროის პერიოდი მოიცავს მონაცემთა დამუშავებისთვის

[27] იხ. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შემუშავებული რეკომენდაციები მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) შესახებ.

[28] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [31.08.2024].

გამოსაყენებელი კომპიუტერული უზრუნველყოფის, აპარატურის და სერვისების შესყიდვისა და განხორციელების ეტაპს.[29]

უშუალოდ „დამუშავების პროცესში“ იგულისხმება მონაცემთა დაცვის მოთხოვნების შენარჩუნება და გადახედვა. დამუშავების დაწყების შემდგომ, დამუშავებისთვის პასუხისმგებელ პირს აქვს უწყვეტი ვალდებულება, უზრუნველყოს მონაცემთა დამუშავების პრინციპების ეფექტიანი იმპლემენტაცია. დამუშავების ოპერაციების ხასიათი, მასშტაბი და კონტექსტი და რისკი, შესაძლოა, დამუშავების პროცესში შეიცვალოს, რაც ნიშნავს იმას, რომ დამუშავებისთვის პასუხისმგებელმა პირმა საკუთარი დამუშავების ოპერაციები ხელმეორედ უნდა შეაფასოს.[30]

მაგალითი:

ბანკს დასაქმებული პირებისთვის მამხილებელი ინსტიტუტის (“whistleblowers”) დანერგვა სურს. კონცეფციის - “Privacy by Design” შესაბამისად (ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება), ბანკი, როგორც დამუშავებისთვის პასუხისმგებელი პირი, ვალდებულია კანონით გათვალისწინებული მონაცემთა დაცვის მოთხოვნები დამუშავების საქმიანობის ჩამოყალიბების ეტაპზევე გაითვალისწინოს. ამდენად, უნდა უზრუნველყოს მონაცემთა დამუშავების პრინციპებსა და მონაცემთა სუბიექტის უფლებებთან შესაბამისობა.[31]

2.6. სათანადო ტექნიკური და ორგანიზაციული ზომები

კანონის 26-ე მუხლის პირველ პუნქტის შესაბამისად, მონაცემთა დამუშავების პროცესში უნდა იქნას გათვალისწინებული სათანადო ტექნიკური და ორგანიზაციული ზომები. ამავე მუხლში, ერთ-ერთი ტექნიკური უსაფრთხოების ზომად დასახელებულია მონაცემთა ფსევდონიმიზაცია. ამგვარი ზომების მიღების მიზანია მონაცემთა დამუშავების პრინციპების (მაგალითად, მონაცემთა

[29] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 10, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024].

[30] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 10-11.

[31] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [27.08.2024].

მინიმიზაციის პრინციპი) ეფექტიანი იმპლემენტაცია მონაცემთა სუბიექტის უფლებების დაცვის ხელშესაწყობად.

ტერმინი „სათანადო“ მიემართება იმ ტექნიკურ ან ორგანიზაციულ ზომას, რომელიც უკავშირდება დამუშავების სპეციფიკასა და მასთან დაკავშირებულ გარემოებებს. დამუშავებისთვის პასუხისმგებელი პირის მიერ მიღებული ზომების „შესაბამისობა“ უნდა შეფასდეს კანონით გათვალისწინებული მოთხოვნების კონტექსტში.[32]

ფსევდონიმიზაციის გარდა, „მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”) სახელმძღვანელო რეკომენდაციებში წარმოდგენილია მონაცემთა დასაცავად მისაღები სხვა სათანადო ზომათა ნუსხა:

- შენახული პერსონალური მონაცემების ხელმისაწვდომობა სტრუქტურიზებული, მანქანურად წაკითხვადი ფორმატით;
- დამუშავების პროცესში მონაცემთა სუბიექტების ჩართვის შესაძლებლობის უზრუნველყოფა;
- პერსონალური მონაცემების შენახვასთან დაკავშირებით ინფორმაციის მიწოდება;
- კომპიუტერული ვირუსებისაგან დაცული სისტემების დანერგვა (“malware detection systems”);
- კიბერუსაფრთხოების საკითხებთან დაკავშირებით დასაქმებული პირების გადამზადება;
- მონაცემთა დაცვის და ინფორმაციული უსაფრთხოების მართვის სისტემების შემუშავება;
- დამუშავებაზე უფლებამოსილი პირებისათვის ხელშეკრულებით ვალდებულების დაწესება, მონაცემთა მინიმიზაციის პრაქტიკის დანერგვის თვალსაზრისით.[33]

<u>მაგალითი:</u>

ფინანსური კომპანია პროდუქტის შექმნაზე მომუშავე გუნდს ავალდებულებს, აწარმოოს საინფორმაციო ფურცელი, რომელშიც ასახული იქნება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვასთან დაკავშირებული მოთხოვნები. კონკრეტულად, შესაბამისი პირების მოვალეობაა, დამუშავებასთან დაკავშირებით კონკრეტული ინფორმაციის შეგროვება და

[32] იქვე.
[33] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [27.08.2024].

დოკუმენტში ასახვა. აგრეთვე, უნდა დასაბუთდეს მონაცემთა დამუშავების პრინციპებისა და მონაცემის სუბიექტის უფლებებთან დაკავშირებული მოთხოვნების დაცულობა.[34]

2.7. მონაცემთა დამუშავების პრინციპების ეფექტიანი იმპლემენტაცია

დამუშავებისთვის პასუხისმგებელი პირის მიერ მიღებული ტექნიკური და ორგანიზაციული ზომების საშუალებით უნდა დაინერგოს მონაცემთა დამუშავების პრინციპები. კანონის 26-ე მუხლი არ განსაზღვრავს კონკრეტულად, თუ რომელი ტექნიკური და ორგანიზაციული ზომა უნდა იქნეს მიღებული, თუმცა იმპლემენტირებული ღონისძიებები ეფექტიანად უნდა უზრუნველყოფდეს მონაცემთა დამუშავების პრინციპების დაცვას. განხორციელებული კონკრეტული ღონისძიების ეფექტიანობის შეფასებისას, გასათვალისწინებელია მონაცემთა დამუშავების კონტექსტი. სათანადო ზომების მიღების ვალდებულება ვრცელდება მონაცემთა დამუშავების სრულ პროცესზე.[35]

2.8. მონაცემთა დამუშავების პროცესში დაცვის სათანადო მექანიზმების ინტეგრირება

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მიიღოს სათანადო ზომები მონაცემთა დამუშავების პრინციპების ეფექტიანად დასაცავად და უზრუნველყოს დამუშავების პროცესში დაცვის სათანადო მექანიზმების ინტეგრირება. აღნიშნული ვალდებულება შეიძლება, იქნას გაგებული, როგორც შიდაორგანიზაციული პოლიტიკის დოკუმენტების შემუშავებისა და სხვა კონკრეტული ტექნიკური და ორგანიზაციული ზომების მიღების მოთხოვნა. დაცვის სათანადო მექანიზმების ინტეგრირება აუცილებლად მოიაზრებს, მათ შორის, მონაცემთა სუბიექტის უფლებების სათანადო რეალიზების ხელშესაწყობად კონკრეტული ღონისძიებების გატარებას.[36]

მაგალითი:

[34] იქვე.
[35] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [27.08.2024].
[36] იქვე.

მონაცემთა ბროკერი აგროვებს დიდი ოდენობის პერსონალურ მონაცემებს. მან უნდა მიიღოს შესაბამისი ტექნიკური და ორგანიზაციული ზომები, რომლებიც უზრუნველყოფს კანონის მოთხოვნების შესაბამისად მონაცემთა სუბიექტის სათანადო ინფორმირებას და, მონაცემებზე წვდომასთან დაკავშირებით მიღებულ მოთხოვნათა რაოდენობის მიუხედავად, მონაცემთა სუბიექტების უფლებების გაუმართლებელი დაყოვნების გარეშე აღსრულებას.[37]

3. მონაცემთა დაცვა პირველად პარამეტრად (“Privacy by Default”)

26-ე მუხლის მე-2 პუნქტი განმარტავს კონცეფციას — „მონაცემთა დაცვა პირველად პარამეტრად“. იგი გულისხმობს მონაცემთა დამუშავების პროცესის იმგვარად მოწესრიგებას, რომ მის ფარგლებში დამუშავებული მონაცემები აუცილებელი იყოს დასახული ლეგიტიმური მიზნის მისაღწევად. ტერმინი „პირველად პარამეტრად“ პერსონალური მონაცემების დამუშავება გულისხმობს კონფიგურაციულ მახასიათებლებთან ან დამუშავებისთვის გამოყენებულ სისტემაში (ელექტრონული აპლიკაციები, მომსახურება ან მოწყობილობა ან დამუშავების მექანიკური პროცედურა) ინტეგრირებულ ან გათვალისწინებულ ვარიანტებთან მიმართებით იმგვარი თავდაპირველი არჩევანის გაკეთებას, რომ შეგროვებული მონაცემების რაოდენობა, მათი დამუშავების მასშტაბი, შენახვის ვადა და მათი ხელმისაწვდომობა იყოს მინიმიზებული.[38] თუკი მონაცემთა სუბიექტის ნებაა, რომ მონაცემთა დამუშავების შემოთავაზებულ მოცულობაზე უფრო მეტი ოდენობით გააზიაროს მისი პერსონალური მონაცემი, ასეთ შემთხვევაში, მას ექნება შესაძლებლობა, შეცვალოს პირველადი პარამეტრი.

მონაცემთა სუბიექტისათვის შეთავაზებული მონაცემთა დამუშავების პირველადი პარამეტრი უნდა ითვალისწინებდეს მონაცემთა დაცვის უმაღლეს სტანდარტს. ამ შემთხვევაში მხედველობაში მიიღება მონაცემთა მოცულობა, კატეგორია და სენსიტიურობა.

აგრეთვე, პირველადი პარამეტრი ავტომატურად უნდა ითვალისწინებდეს დამუშავებულ მონაცემზე წვდომის შეზღუდვას, ანუ დამუშავებული მონაცემის გადაცემა ან ფართო საზოგადოებისთვის ხელმისაწვდომობა უნდა იყოს შეზღუდული და თავდაპირველადვე ავტომატურად არ უნდა ხდებოდეს. ამასთან, პირი, რომელიც

[37] იქვე.

[38] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 11, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [26.08.2024].

ამუშავებს პერსონალურ მონაცემებს, უნდა დარწმუნდეს, რომ ამუშავებს მხოლოდ საჭირო პერსონალურ ინფორმაციას მიზნის მისაღწევად.[39]

აღნიშნული პუნქტი, ერთგვარად, ავიწროებს მონაცემთა დამუშავების ფარგლებს მიზნის შესაბამისად. მითითებული კონცეფცია მჭიდრო კავშირშია მონაცემთა მინიმიზაციის, შენახვის ვადის შეზღუდვისა და მიზნის შეზღუდვის პრინციპებთან.[40]

მაგალითი:

დამუშავებისთვის პასუხისმგებელი პირის მიერ გატარებული ზომების საშუალებით, კომპანიის თანამშრომლების მხოლოდ გარკვეულ ნაწილს უნდა ჰქონდეს მონაცემთა სუბიექტის პერსონალურ მონაცემებზე წვდომა.[41]

პრინციპის მიზანია მონაცემთა სუბიექტების დაცვა მათი დიდი მოცულობის პერსონალური მონაცემების დამუშავებისგან. ასევე, მონაცემთა სუბიექტის მიერ მისი პერსონალური მონაცემების დამუშავებაზე თანხმობის მოსაპოვებლად კონკრეტული პროდუქტი „პირველად პარამეტრად“ უნდა ითვალისწინებდეს პერსონალური მონაცემების დაცვასთან დაკავშირებულ მოთხოვნებს.[42]

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, აარჩიოს დამუშავების პირველადი პარამეტრებისა და ვარიანტების იმგვარად განხორციელება, რომ დამუშავდეს მხოლოდ დასახული, კანონიერი მიზნისთვის მკაცრად აუცილებელი მონაცემი. ამასთან, მას მოეთხოვება, განსაზღვროს, თუ რა კონკრეტული, ცალსახა და ლეგიტიმური მიზნებისთვის ხორციელდება მონაცემთა შეგროვება და დამუშავება.[43] ამავდროულად, დამუშავებისთვის პასუხისმგებელმა პირმა მიზანშეწონილია:

- სისტემების შემუშავებისას იმოქმედოს პირადი ცხოვრების ხელშეუხებლობის უპირატესი მიდგომით;

---

[39] Swedish Authority for Privacy Protection (IMY), Privacy by design and privacy by default, <https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/privacy-by-design-and-privacy-by-default/>, [31.08.2024].

[40] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [31.08.2024].

[41] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 210, <https://www.echr.coe.int/documents/d/echr/Handbook_data_protection_KAT>, [31.08.2024].

[42] Paul Voigt, The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 63.

[43] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 11, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [26.08.2024].

- უზრუნველყოს, რომ მონაცემთა სუბიექტებს არ ჰქონდეთ ილუზორული არჩევანის გაკეთების შესაძლებლობა მათი პერსონალური მონაცემების დამუშავებასთან მიმართებით;
- მონაცემთა სუბიექტის თანხმობის გარეშე არ დაამუშაოს დამატებითი პერსონალური მონაცემები;
- უზრუნველყოს, რომ მონაცემთა სუბიექტის თანხმობის გარეშე მისი პერსონალური ინფორმაცია არ გახდება საჯაროდ ხელმისაწვდომი;
- მონაცემთა სუბიექტებისთვის უზრუნველყოფილი იყოს მათთვის მინიჭებული უფლებებით სარგებლობის შესაძლებლობა.[44]

3.1. ტექნიკური და ორგანიზაციული ზომების მიღება მონაცემთა დამუშავების მიზნის შესაბამისად

26-ე მუხლის მე-2 პუნქტის ფარგლებში, ტექნიკური და ორგანიზაციული ზომების მიღებისას, უნდა განისაზღვროს მონაცემთა რაოდენობა, მონაცემთა დამუშავების მასშტაბი, შენახვის ვადები და მონაცემებზე წვდომასთან დაკავშირებული საკითხები. ამგვარი ზომები მიღებული უნდა იქნას დამუშავების თითოეულ ოპერაციასთან მიმართებით.

დამუშავებისთვის პასუხისმგებელმა პირმა, როგორც დამუშავების მიზნებისა და საშუალებების განსაზღვრის, ისე პერსონალური მონაცემების დამუშავების პროცესში უნდა მიიღოს ან შესაბამისად განაახლოს ტექნიკურ-ორგანიზაციული ზომები.[45]

მაგალითი:

დამუშავებისთვის პასუხისმგებელმა პირმა „პირველად პარამეტრად“ მონაცემთა დაცვის პრინციპთან შესაბამისობის უზრუნველსაყოფად, პოლიტიკის დოკუმენტში უნდა განსაზღვროს: დამუშავების კონკრეტული მიზანი; მიზნის მისაღწევად დასამუშავებელი პერსონალური მონაცემების ოდენობა; მონაცემთა

[44] Information Commissioner's Office (ICO), Data protection by design and default, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/>, [31.08.2024].

[45] Future of Privacy Forum, Christina Michelakaki and Sebastião Barros Vale, Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR, 2023, 17, <https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf?fbclid=IwY2xjawFAL9RleHRuA2FlbQIxMAABHZgKscp2JpFY9-2hARtejqzLZgLZA_WfT_ZyVdIQnelt9yCt22UgFzN9vg_aem_aBRFAWm79k_PdIn_2DAprw>, [31.08.2024].

დამუშავების ფარგლები; მონაცემთა შენახვის აუცილებელი ვადა; მონაცემთა წვდომაზე უფლებამოსილი პირები.[46]

კონცეფცია — „მონაცემთა დაცვა პირველად პარამეტრად“, განსხვავებით „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინების“ კონცეფციისგან, არ მოიცავს ისეთ ელემენტებს, როგორიცაა: განხორციელების ხარჯები; მონაცემთა დამუშავების ხასიათი, მასშტაბი, კონტექსტი და მიზნები; მოსალოდნელი რისკები მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების მიმართულებით. თუმცა, მიუხედავად ამისა, დამუშავებისთვის პასუხისმგებელი პირის მიერ მიღებული ზომები უნდა შეესაბამებოდეს მონაცემთა დაცვის ყველა მოთხოვნას.[47]

3.2. მონაცემების მხოლოდ იმ მოცულობის ავტომატურად დამუშავება, რომელიც აუცილებელია დამუშავების კონკრეტული მიზნისთვის

მონაცემთა დამუშავება პირველად პარამეტრად კომპიუტერული მეცნიერებიდან მომდინარეობს და გულისხმობს უკვე არსებულ ან წინასწარ შერჩეულ მახასიათებელს კონფიგურირებად პარამეტრებში, რომლებიც ელექტრონულ აპლიკაციას, კომპიუტერულ პროგრამას ან მოწყობილობას მიენიჭება. ასეთ პარამეტრებს უწოდებენ „წინასწარ განსაზღვრულ“ ან „ქარხნულ“ პარამეტრებს, განსაკუთრებით, ელექტრონულ მოწყობილობებთან მიმართებით.[48]

მონაცემთა დამუშავების ოპერაციები უნდა განისაზღვროს იმგვარად, რომ საწყისი ეტაპიდანვე უზრუნველყოფილი იყოს მხოლოდ იმ მინიმალური ოდენობის პერსონალური მონაცემების დამუშავება, რომელიც აუცილებელია კონკრეტული მიზნებისთვის. აღნიშნული საკითხის გათვალისწინება განსაკუთრებით მნიშვნელოვანია მაშინ, როდესაც მონაცემებზე წვდომა უზრუნველყოფილია თანამშრომლებისთვის, რომლებსაც სხვადასხვა როლი და მონაცემებზე წვდომის განსხვავებული საჭიროება გააჩნიათ.[49]

---

[46] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [31.08.2024].

[47] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [31.08.2024].

[48] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 11, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024].

[49] იქვე, 12.

შესაბამისად, პროდუქტი ან მომსახურება უნდა მოიცავდეს მონაცემთა დაცვის კონცეფციების შესაბამის პარამეტრებს. მოწყობილობის ფუნქციონირებისას, სამართლებრივი საფუძვლის არარსებობის ან განსაზღვრულ მიზანთან შეუსაბამობის შემთხვევაში, დამუშავება უნდა შეწყდეს.[50]

3.3. მონაცემთა მინიმიზაციის პრინციპთან დაკავშირებული ვალდებულებები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 26-ე მუხლის მე-2 პუნქტში წარმოდგენილია მონაცემთა მინიმიზაციის პრინციპთან დაკავშირებულ ვალდებულებათა ჩამონათვალი მონაცემთა ავტომატური დამუშავების შემთხვევაში. აღნიშნულის შესაბამისად, „მხოლოდ კონკრეტული მიზნისთვის საჭირო პერსონალური მონაცემების დამუშავების“ მოთხოვნა ვრცელდება შეგროვებული მონაცემების რაოდენობაზე, მონაცემთა დამუშავების მასშტაბებზე, შენახვის ვადებსა და წვდომაზე.

3.3.1. შეგროვებული მონაცემების რაოდენობა

დამუშავებისთვის პასუხისმგებელმა პირმა წინასწარ უნდა განსაზღვროს დამუშავების მიზნისთვის აუცილებელი პერსონალური მონაცემების მოცულობა და კატეგორიები. პროდუქტის შემუშავებისას, უნდა იქნას გათვალისწინებული ის რისკები, რომლებიც უკავშირდება მონაცემთა უსაფრთხოებას, კონფიდენციალურობას, მონაცემთა დამუშავების პრინციპების დაცვას და ა.შ.[51]; [52]

---

[50] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [31.08.2024].

[51] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 17, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024].

[52] იხ. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შემუშავებული რეკომენდაციები „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, გვ. 18, <https://shorturl.at/yxPd0>, [13.12.2024].

3.3.2. მონაცემთა დამუშავების ფარგლები

პერსონალურ მონაცემების დამუშავების ოპერაციები უნდა შემოიფარგლებოდეს აუცილებლობის ელემენტით.[53] დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მიიღოს შესაბამისი ზომები, რათა არ გაფართოვდეს მონაცემთა დამუშავების მიზნები. დამატებით, უნდა გაითვალისწინოს, თუ რა სახის დამუშავება ექცევა მონაცემთა სუბიექტთა გონივრული მოლოდინების ფარგლებში[54] და თავიდან აირიდოს თავდაპირველი მიზნისაგან განსხვავებული მიზნით მონაცემთა შემდგომი დამუშავება.

3.3.3. მონაცემთა შენახვის ვადა

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა შენახვის ვადა შეზღუდოს მონაცემთა დამუშავების მიზნის შესაბამისად. თუკი პერსონალური მონაცემები წინასწარ განსაზღვრული მიზნისთვის აღარ არის საჭირო, უნდა წაიშალოს ან უზრუნველყოფილი იქნას მათი დეპერსონალიზაცია.[55] მონაცემთა შენახვის ვადის ხანგრძლივობა დამოკიდებულია დამუშავების კონკრეტულ მიზანზე. აღნიშნული ვალდებულება პირდაპირ კავშირშია მიზნის შეზღუდვის პრინციპთან. დამუშავებისთვის პასუხისმგებელმა პირმა, მიზანშეწონილია, დანერგოს მონაცემთა წაშლისა თუ დეპერსონალიზაციისათვის შესაბამისი პროცედურები.[56]

3.3.4. მონაცემებზე წვდომა

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, შიდაორგანიზაციულ დონეზე მაქსიმალურად შეზღუდოს პერსონალურ მონაცემებზე წვდომა. მონაცემები ხელმისაწვდომი უნდა იყოს მხოლოდ იმ პირებისთვის, ვისაც რეალურად სჭირდება.

---

[53] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [31.08.2024].

[54] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 13, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024].

[55] მე-3 მუხლის „ც“ ქვეპუნქტის შესაბამისად, მონაცემთა დეპერსონალიზაცია გულისხმობს მონაცემთა იმგვარ დამუშავებას, როდესაც შეუძლებელია მონაცემთა სუბიექტთან მათი დაკავშირება ან ასეთი კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას, ხარჯებს ან/და დროს საჭიროებს.

[56] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [31.08.2024].

მონაცემთა გადაცემის პროცესში უნდა არსებობდეს მონიტორინგის მექანიზმი.[57] მონაცემთა ბაზებთან მიმართებით, უნდა იქნას მიღებული იმგვარი ტექნიკური და ორგანიზაციული ზომები, რომელთა საშუალებითაც პერსონალურ მონაცემებზე წვდომა მხოლოდ აუცილებელი საჭიროებით შეიზღუდება.[58]

3.3.5. ალტერნატიული მიდგომის არჩევამდე პირთა განუსაზღვრელი წრისთვის მონაცემთა მხოლოდ მინიმალურ მოცულობაზე წვდომის ავტომატური უზრუნველყოფა

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 26-ე მუხლის მე-2 პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელი პირის მიერ მიღებული ტექნიკური და ორგანიზაციული ზომები იმგვარად უნდა იქნეს გამოყენებული, რომ ნებადართული ალტერნატიული მიდგომის არჩევამდე, პირთა განუსაზღვრელი წრისთვის ავტომატურად უზრუნველყოფილი იყოს მონაცემთა მხოლოდ მინიმალურ მოცულობაზე წვდომა. აღსანიშნავია, რომ პერსონალური მონაცემი პირთა განუსაზღვრელი წრისათვის არ იყოს ხელმისაწვდომი, რათა არ განხორციელდეს მონაცემთა გაუთვალისწინებელი დამუშავება.[59]

კონცეფციის პრაქტიკულ გამოხატულებას, ყველაზე ხშირად, ინტერნეტ სივრცეში, ვებგვერდის „მზა ჩანაწერები“ ე. წ. “cookies” პოლიტიკა წარმოადგენს, რომელიც განსაზღვრავს ვებგვერდის ვიზიტორის მონაცემების დამუშავების პირობებს. ამასთან, შესაძლებელია, აღინიშნოს სოციალური ქსელის შემთხვევა, რომელშიც მომხმარებლის მიერ შექმნილი გვერდის პარამეტრები თავდაპირველად ავტომატურად ისე უნდა იყოს კონფიგურირებული, რომ პირთა განუსაზღვრელი წრისთვის მინიმალური ინფორმაცია ზიარდებოდეს და მომხმარებლის მიერ ატვირთული ყველა მონაცემი თავიდანვე ავტომატურად საჯარო არ იყოს.

ინტერნეტმომხმარებელს შეთავაზებული აქვს ყველა მზა ჩანაწერის თანხმობის ან უარყოფის ღილაკი (“accept all cookies”). აღსანიშნავია, რომ ინტერნეტმომხარებელს უნდა შეეძლოს შეთავაზებული კონფიგურაციის ცვლილება. გარდა ამისა, მზა ჩანაწერებზე დათანხმება ან უარყოფა სხვადასხვა ალტერნატიული პირობით უნდა

---

[57] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, 13, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [31.08.2024].

[58] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [27.08.2024].

[59] GDPR hub, GDPR commentary, article 25, <https://gdprhub.eu/index.php?title=Article_25_GDPR>, [27.08.2024].

განხორციელდეს და მომხმარებელს შეეძლოს მისთვის მისაღები პირობებით თანხმობის გაცემა. აღნიშნული ალტერნატივა უნდა იყოს შეთავაზებული მონაცემთა სუბიექტისათვის გასაგები და მარტივი ფორმით.

4. „მონაცემთა მეტად დაფარვის პრიორიტეტის“ მოთხოვნების დარღვევა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად

მონაცემთა დამუშავების პროცესში „მონაცემთა მეტად დაფარვის პრიორიტეტის“ მოთხოვნების არსებობის შესახებ მტკიცების ტვირთი, ანგარიშვალდებულების პრინციპიდან გამომდინარე, დამუშავებისთვის პასუხისმგებელ პირს ეკისრება. აღნიშნული ვალდებულების გათვალისწინება არ უნდა იყოს ფიგურალური, იგი უნდა იყოს მონაცემთა პრინციპების დაცვის ეფექტიანი მექანიზმი და კონტექსტუალურად ემსახურებოდეს მონაცემთა სუბიექტებისათვის მონაცემთა დაცვაზე ორიენტირებული მომსახურების მიწოდებას და შეთავაზებული პროდუქტის მიმართ მათი ნდობის ზრდას.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 75-ე მუხლი განსაზღვრავს დამუშავებისთვის პასუხისმგებელი პირის პასუხისმგებლობას 26-ე მუხლით გათვალისწინებული რომელიმე ვალდებულების შეუსრულებლობისთვის. კერძოდ, მოთხოვნების დარღვევის შემთხვევაში, ფიზიკურ პირს, საჯარო დაწესებულებას, არასამეწარმეო (არაკომერციულ) იურიდიულ პირს, აგრეთვე იურიდიულ პირს, უცხო ქვეყნის საწარმოს ფილიალსა და ინდივიდუალურ მეწარმეს, რომელთა წლიური ბრუნვა 500 000 ლარს არ აღემატება, სანქციის სახით დაეკისრება გაფრთხილება ან ჯარიმა 2 000 ლარის ოდენობით. ხოლო იურიდიულ პირს (გარდა არასამეწარმეო (არაკომერციული) იურიდიული პირისა), უცხო ქვეყნის საწარმოს ფილიალსა და ინდივიდუალურ მეწარმეს, რომელთა წლიური ბრუნვა 500 000 ლარს აღემატება, დაეკისრება გაფრთხილება ან ჯარიმა 3 000 ლარის ოდენობით.

კანონი, ასევე, ქმედების ჩადენის დამამძიმებელ გარემოებებს ითვალისწინებს. კერძოდ, ფიზიკური პირი, საჯარო დაწესებულება, არასამეწარმეო (არაკომერციული) იურიდიული პირი, აგრეთვე იურიდიული პირი, უცხო ქვეყნის საწარმოს ფილიალი და ინდივიდუალური მეწარმე, რომელთა წლიური ბრუნვა 500 000 ლარს არ აღემატება, დაჯარიმდება 3 000 ლარის ოდენობით. აგრეთვე, იურიდიული პირი (გარდა არასამეწარმეო (არაკომერციული) იურიდიული პირისა), უცხო ქვეყნის საწარმოს ფილიალი და ინდივიდუალური მეწარმე, რომელთა წლიური ბრუნვა 500 000 ლარს აღემატება, დაჯარიმდება 5 000 ლარის ოდენობით.“

5. საზღვარგარეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოთა პრაქტიკის ზოგადი მიმოხილვა

საზღვარგარეთის მონაცემთა დაცვის საზედამხედველო ორგანოები საქმეების განხილვისას, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 25-ე მუხლის ფარგლებში საჭიროების შესაბამისად შეისწავლიან დამუშავებისთვის პასუხისმგებელი პირის მიერ კონცეფციების — „ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინება“ (“Privacy by Design”) და „მონაცემთა დაცვა პირველად პარამეტრად“ (“Privacy by Default”) ფარგლებში არსებული ვალდებულებების შესრულების საკითხს. ძირითად შემთხვევაში, საზედამხედველო ორგანოები მონაცემთა უსაფრთხოებასთან დაკავშირებულ საკითხებზე მსჯელობენ, რამდენადაც ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა უსაფრთხოების უზრუნველყოფა არსებით კომპონენტს წარმოადგენს.

საბერძნეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“HDPA”) მონაცემთა სუბიექტის მიმართვის საფუძველზე, დამუშავებისთვის პასუხისმგებელი პირის (მუნიციპალიტეტის) მიერ მონაცემთა უსაფრთხოების დარღვევის (ინციდენტი) შესახებ იმსჯელა. საზედამხედველო ორგანომ, სხვა დარღვევებთან ერთად, დაადგინა “GDPR”-ის 25-ე მუხლის პირველი პუნქტის დარღვევა (“Privacy by Design”), რადგან დამუშავებისთვის პასუხისმგებელმა პირმა ვებგვერდის შექმნის საწყის ეტაპზევე არ მიიღო შესაბამისი ზომები (პროდუქტის შექმნის საწყის ეტაპზევე არ გაითვალისწინა მონაცემთა დაცვის სტანდარტები) პერსონალურ მონაცემთა დაცვასთან დაკავშირებული რისკების აღმოსაფხვრელად.[60]

ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთ საქმეში, რომელიც საგანმანათლებლო დაწესებულების მიერ პერსონალური მონაცემების დამუშავების კანონიერების საკითხს შეეხებოდა, სათანადო ტექნიკური და ორგანიზაციული ზომების არარსებობის გამო, დამუშავებისთვის პასუხისმგებელი პირი სამართალდამრღვევად ცნო. საქმის ფაქტობრივი გარემოებების თანახმად, მონაცემთა სუბიექტმა სკოლის ვაკანტურ თანამდებობაზე გამოცხადებულ კონკურსში მიიღო მონაწილეობა, თუმცა ის არ იქნა შერჩეული მისთვის სასურველ პოზიციაზე. აღნიშნულის თაობაზე გადაწყვეტილება სკოლის ციფრულ პლატფორმაზე (“Smartschool”) გამოქვეყნდა, რომელზეც წვდომა სკოლის 150 თანამშრომელს ჰქონდა. წარმოდგენილი ფაქტის შემდეგ, სკოლის საბჭომ განაცხადა, რომ გამოქვეყნებული

[60] GDPR hub, HDPA (Greece) - Decision 18/2024, <https://gdprhub.eu/index.php?title=HDPA_(Greece)_-_Decision_18%2F2024&fbclid=IwZXh0bgNhZW0CMTAAAR16ksiYk_-BYeYfRfXX1vwvPQn6NVLbRH6dO3RMNQkhPSXtUimxsNr8sr0_aem_8aaeh5YPwBoSqRLnzQW8Iw>, [31.08.2024].

ინფორმაცია იყო კონფიდენციალური და შეცდომით გახდა საჯაროდ ხელმისაწვდომი. აღნიშნულთან დაკავშირებით, საზედამხედველო ორგანომ "GDPR"-ის 25-ე მუხლის დარღვევა დაადგინა.[61]

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ("Garante") დამუშავებისთვის პასუხისმგებელი პირის მიერ, სხვა დარღვევებს შორის, "GDPR"-ის 25-ე მუხლის დარღვევა დაადგინა. კონკრეტულად, ვებგვერდის საშუალებით შესაძლებელი იყო სახელით და გვარით კონკრეტული პირების საკონტაქტო ინფორმაციის მოძიება. საზედამხედველო ორგანომ "Privacy by design" და "Privacy by Default" კონცეფციების განხორციელებასთან მიმართებით აღნიშნა, რომ მიღებული ტექნიკური და ორგანიზაციული ზომები ვერ უზრუნველყოფდა მონაცემთა სუბიექტების უფლებების ჯეროვან დაცვას.[62]

ავსტრიის მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთ საქმეში დაადგინა დამუშავებისთვის პასუხისმგებელი პირის მიერ "GDPR"-ის 25-ე მუხლის პირველი პუნქტის დარღვევა, რადგან არ მიიღო სათანადო ტექნიკური და ორგანიზაციული ზომები მონაცემთა სუბიექტთა უფლებების დასაცავად. კერძოდ, საჯაროდ ხელმისაწვდომი ვებგვერდიდან ვერ უზრუნველყო პერსონალური ინფორმაციის წაშლა.[63]

ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ("AEPD") ერთ-ერთი ბანკის მიერ, "GDPR"-ის 25-ე მუხლის კონტექსტში, მონაცემთა დამუშავების მართლზომიერება შეაფასა. დამუშავებისთვის პასუხისმგებელმა პირმა არ განახორციელა მონაცემთა დაცვაზე ზეგავლენის შეფასება "GDPR"-ის მოთხოვნების შესაბამისად, კერძოდ, არ მიიღო სათანადო ტექნიკური და ორგანიზაციული ზომები მონაცემთა დამუშავების პრინციპების დასანერგად. მოცემულ საქმეში "AEPD"-მ აღნიშნა, რომ "GDPR"-ის 25-ე მუხლის პირველი და მე-2 პუნქტით

[61] GDPR hub, APD/GBA (Belgium) - 81/2024, <https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_81/2024>, [31.08.2024].

[62] GDPR hub, Garante per la protezione dei dati personali (Italy) – 9780409, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9780409>, [31.08.2024].

[63] GDPR hub, DSB (Austria) - 2023-0.592.319, <https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2023-0.592.319&fbclid=IwZXh0bgNhZW0CMTAAAR0AdNIJtt_LWAKIbmX38A8Wk-GTfa26EwGhtu1mojd_3eToZLIQId4sybs_aem_Xo8D4DcWtga-4X2Rqd2YrQ>, [31.08.2024].

გათვალისწინებული მოთხოვნების დასაცავად, პროდუქტის შექმნისას აუცილებელია მონაცემთა დაცვის მოთხოვნების გათვალისწინება.[64]

ხორვატიის მონაცემთა დაცვის საზედამხედველო ორგანომ კომპანიის მიერ პერსონალური მონაცემების დამუშავების კანონიერების საკითხებზე მიიღო გადაწყვეტილება. "GDPR"-ის 25-ე მუხლთან მიმართებით ფაქტობრივი გარემოებების შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი პერსონალურ მონაცემებს ინახავდა აუცილებელზე მეტი ვადით და აღნიშნავდა, რომ ფინანსური მონაცემები არ უნდა წაშლილიყო. ამასთან, დამუშავებისთვის პასუხისმგებელი პირის კომპანიაში დასაქმებულ პირებს წვდომა ჰქონდათ დიდი მოცულობით პერსონალურ ინფორმაციაზე. საზედამხედველო ორგანომ დაადგინა, რომ კომპანიას არ ჰქონდა სათანადო ტექნიკური და ორგანიზაციული ზომები დანერგილი მონაცემთა სუბიექტის უფლებების დასაცავად, რაც წინააღმდეგობაში მოდიოდა "GDPR"-ის 25-ე მუხლის პირველ და მე-2 პუნქტებთან.[65]

პოლონეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ("UODO") მოიკვლია სატელეფონო კომპანიის მიერ პერსონალური მონაცემების დამუშავების კანონიერებასთან დაკავშირებული საკითხები. "UODO"-მ აღნიშნა, რომ მხოლოდ დაშიფვრა და ფსევდონიმიზაცია არ არის საკმარისი "GDPR"-ის 25-ე მუხლის მოთხოვნების დაცვის უზრუნველსაყოფად. კერძოდ, აუცილებელია მიღებულ იქნას, დამატებით, სხვადასხვა ზომა მონაცემთა სუბიექტის უფლებების დასაცავად. მოცემულ საქმეში, საზედამხედველო ორგანომ დაადგინა "GDPR"-ის 25-ე მუხლის პირველი პუნქტის დარღვევა.[66]

ლატვიის მონაცემთა დაცვის საზედამხედველო ორგანომ ("DVI") შეისწავლა კომპანიის მიერ ვიდეოსამეთვალყურეო სისტემების გამოყენების მართლზომიერება. საქმის ფაქტობრივი გარემოებების შესაბამისად, იკვეთებოდა, რომ დამუშავებისთვის პასუხისმგებელ პირს შემუშავებული ჰქონდა პროცედურები, რომლებიც აწესრიგებდა პერსონალურ მონაცემებზე წვდომასთან, წვდომაზე უფლებამოსილ პირებსა და ვიდეოჩანაწერების შენახვასთან დაკავშირებულ საკითხებს. "DVI"-ის შეფასებით, დამუშავებისთვის პასუხისმგებელი პირის მიერ დანერგილი ტექნიკური და

---

[64] GDPR hub, AEPD (Spain) - PS/00331/2022, <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS%2F00331%2F2022&fbclid=IwZXh0bgNhZW0CMTAAAR3iMatALRROPpXyq3Hj2EaEGNXwB3bfVTAzpVrYNihKRIXFYj5WrgwGhfA_aem_yYLE4CCf1PrIz0WNKShu3g>, [31.08.2024].

[65] GDPR hub, AZOP (Croatia) - Decision 18-05-2023, <https://gdprhub.eu/index.php?title=AZOP_(Croatia)_-_Decision_18-05-2023&fbclid=IwZXh0bgNhZW0CMTAAAR34-zNlE-TZkODjP69D7GerdRQRfSBaICpdrHEKTUY_vGs1Mgqzm8Gckfs_aem_ksYtoT0T-wRZFhaorF2bkA>, [31.08.2024].

[66] GDPR hub, UODO (Poland) - DKN.5112.1.2020, <https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DKN.5112.1.2020&fbclid=IwZXh0bgNhZW0CMTAAAR3ZRfzhy4RvX0P6yjFv2uTl-cy_LkDS5pbDa_4zfC7OyjF9J0VFaNGRADY_aem_6SYWTRwLh4UPgZSy3QCGvg>, [31.08.2024].

ორგანიზაციული ზომები შეესაბამებოდა “GDPR”-ის 25-ე მუხლის პირველი პუნქტით დადგენილ მოთხოვნებს.[67]

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირის, ფინეთის გოლფის ასოციაციის მიერ პერსონალურ მონაცემთა დამუშავების “GDPR”-ის მოთხოვნებთან შესაბამისობის შესახებ მიიღო გადაწყვეტილება. ფაქტობრივი გარემოებების შესაბამისად, აპლიკაციაში ავთენტიფიკაციისთვის მომხმარებელს არ სჭირდებოდა პაროლი და მას მხოლოდ საიდენტიფიკაციო ნომრით შეეძლო საკუთარი ანგარიშის გააქტიურება. ხოლო საიდენტიფიკაციო ნომერი შედგებოდა იმ მონაცემებისგან, რომლებიც გენერირდებოდა მონაცემთა სუბიექტის საიდენტიფიკაციო ბარათიდან. საგულისხმოა, რომ აღნიშნული ბარათის მონაცემები ასოციაციის ვებგვერდზე საჯაროდ იყო ხელმისაწვდომი. საზედამხედველო ორგანომ მიიჩნია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა, დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 25-ე მუხლის პირველი პუნქტი და 32-ე მუხლი (მონაცემთა დამუშავების უსაფრთხოება), რადგან აპლიკაციის გამართულად ფუნქციონირებისთვის, მას არ ჰქონდა განხორციელებული სათანადო ორგანიზაციული და ტექნიკური ზომები. ასევე, აპლიკაციაში ავთენტიფიკაციის მიზნით, სათანადო პაროლის არარსებობა ქმნიდა მონაცემთა სუბიექტების საიდენტიფიკაციო ნომრების მარტივად იდენტიფიცირების შესაძლებლობას, რის შედეგადაც შესაძლებელი იყო მომხმარებელთა ანგარიშებსა და პერსონალურ მონაცემებზე არაუფლებამოსილი წვდომა.[68]

6. რეკომენდაციები კონცეფციებთან - „მონაცემთა დაცვის სტანდარტების გათვალისწინება პროდუქტის ან მომსახურების შექმნისას“ და „მონაცემთა დაცვა პირველად პარამეტრად“ მიმართებით

დამუშავებისთვის პასუხისმგებელმა პირმა, კონცეფციების — „მონაცემთა დაცვის სტანდარტების გათვალისწინება პროდუქტის ან მომსახურების შექმნისას“ და „მონაცემთა დაცვა პირველად პარამეტრად“ შესაბამისად, მიზანშეწონილია, მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები, უზრუნველყოს მონაცემთა დამუშავების პრინციპების იმპლემენტაცია და სათანადო დაცვის მექანიზმების დანერგვის გზით — მონაცემთა სუბიექტის უფლებების დაცვა. მონაცემთა

[67] GDPR hub, DVI (Latvia) - SIA "QUANTRUM", <https://gdprhub.eu/index.php?title=DVI_(Latvia)_-_SIA_%22QUANTRUM%22&fbclid=IwZXh0bgNhZW0CMTAAAR3iMatALRROPpXyq3Hj2EaEGNXwB3bfVTAzpVrYNihKRIXFYj5WrgwGhfA_aem_yYLE4CCf1PrIz0WNKShu3g>, [31.08.2024].

[68] GDPR hub, Decision of DPA (Finland), Tietosuojavaltuutetun toimisto (Finland) - TSV/955/2023, <https://gdprhub.eu/index.php?title=Tietosuojavaltuutetun_toimisto_(Finland)_-_TSV/955/2023>, [31.08.2024].

დამუშავების ინდივიდუალური სპეციფიკიდან გამომდინარე, არ არსებობს უნივერსალური მეთოდი, რომელიც უზრუნველყოფს მონაცემთა მეტად დაფარვის სტანდარტის ეფექტიან დანერგვას. მიუხედავად ამისა, დამუშავებისთვის პასუხისმგებელმა პირმა სასურველია, უზრუნველყოს: პერსონალურ მონაცემთა დამუშავების მინიმიზაცია; პერსონალური მონაცემების დროული ფსევდონიმიზაცია; პერსონალური მონაცემების დამუშავების პროცესში გამჭვირვალობა; მონაცემთა სუბიექტებისთვის სრული კონტროლის შესაძლებლობა მონაცემთა დამუშავების პროცესზე; მონაცემთა უსაფრთხოების შესაბამისი ტექნიკურ-ორგანიზაციული ზომების მიღება და, საჭიროებისამებრ, მათი გაუმჯობესება.[69] განხილული ვალდებულებების გათვალისწინება უნდა განხორციელდეს მონაცემთა დამუშავების ყველა ეტაპზე, კერძოდ: პროდუქტის ან მომსახურების შექმნა; განვითარებისა და სატესტო რეჟიმი; მონაცემების შეგროვება; მონაცემების შემდგომი დამუშავება; მონაცემების გამჟღავნება; მონაცემების შენახვა.[70]

დამატებით, იმისათვის, რომ პერსონალურ მონაცემთა დამუშავების პროცესი შესაბამისობაში იყო "Privacy by design" და "Privacy by Default" კონცეფციების მოთხოვნებთან, მიზანშეწონილია, შემდეგი რეკომენდაციების გათვალისწინება:

- ☑ ახალი პროდუქტის შექმნის პროცესში დაინერგოს პერსონალურ მონაცემთა დაცვასთან დაკავშირებული სტანდარტები;
- ☑ ახალი პროდუქტისა და მომსახურების შექმნამდე შეფასდეს მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებზე ზეგავლენა;
- ☑ დამუშავდეს მხოლოდ იმ მოცულობის პერსონალური მონაცემები, რომლებიც აუცილებელია მიზნის მისაღწევად;
- ☑ ინფორმაციული ტექნოლოგიის სისტემის, მომსახურებისა და პროდუქტის შემუშავებისას, ავტომატურად იქნეს გათვალისწინებული პერსონალურ მონაცემთა დაცვის მოთხოვნები;
- ☑ გასაგები ფორმით შემუშავდეს პოლიტიკის დოკუმენტი, რათა დაინტერესებულმა პირებმა პერსონალური მონაცემების დამუშავების თაობაზე მიიღონ სრულყოფილი ინფორმაცია;

[69] Information Commissioner's Office (ICO), Data protection by design and default, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/>, [30.08.2024].

[70] Catalan Data Protection Authority, Privacy by design and privacy by default, A guide for developers, 2024, 7, <https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD_EN.pdf?fbclid=IwZXh0bgNhZW0CMTAAAR3ZRfzhy4RvX0P6yjFv2uTl-cy_LkDS5pbDa_4zfC7OyjF9J0VFaNGRADY_aem_6SYWTRwLh4UPgZSy3QCGvg>, [31.08.2024].

- ☑ პირადი ცხოვრების ხელშეუხებლობის უზრუნველსაყოფად შემუშავდეს სათანადო დაცვის მექანიზმები;
- ☑ გამოყენებული იქნას იმგვარი ტექნოლოგიები, რომელთა საშუალებითაც მაქსიმალურად იქნება უზრუნველყოფილი პირადი ცხოვრების ხელშეუხებლობის უფლების დაცულობა.[71]

[71] Information Commissioner's Office (ICO), Data protection by design and default, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/>, [30.08.2024].

ᲛᲘᲡ.: ᲡᲐᲥᲐᲠᲗᲕᲔᲚᲝ, ᲗᲑᲘᲚᲘᲡᲘ, Ნ. ᲕᲐᲠᲜᲐᲫᲘᲡ №7, 0105
ᲑᲐᲗᲣᲛᲘ, ᲑᲐᲥᲝᲡ ᲥᲣᲩᲐ, №48, 6010
www.personaldata.ge
ᲢᲔᲚ.: (+995 32) 242 1000
E-mail: office@pdps.ge