პერსონალურ მონაცემთა
დაცვის სამსახური

მონაცემთა დაცვის

ბზამკვლევი

ვებსაიტის შექმნის მსურველთათვის

შინაარსი

რეკომენდაცია ემსახურება პერსონალურ მონაცემთა დაცვის საუკეთესო პრაქტიკის დამკვიდრების ხელშეწყობას. იგი არ წარმოადგენს სამართლებრივ აქტს, არის სარეკომენდაციო ხასიათის და არ წარმოშობს დამატებით უფლებებსა და ვალდებულებებს.

განმარტებები და აბრევიატურები

პერსონალური მონაცემი - ნებისმიერი სახის ინფორმაცია, რომელიც იდენტიფიცირებულ/იდენტიფიცირებად ფიზიკურ პირს უკავშირდება. მაგალითად, სახელი, გვარი, პირადი ნომერი, მისამართი, გეოლოკაციის მონაცემი.

დამუშავებისთვის პასუხისმგებელი პირი - ფიზიკური/იურიდიული პირი/საჯარო დაწესებულება, რომელიც განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს.

დამუშავებაზე უფლებამოსილი პირი - ფიზიკური/იურიდიული პირი/საჯარო დაწესებულება, რომელიც მონაცემებს ამუშავებს დამუშავებისთვის პასუხისმგებელი პირისთვის/მისი სახელით.

მონაცემთა დამუშავება - მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედება, მაგალითად, მოპოვება, შეგროვება, გადაცემა, შენახვა.

განსაკუთრებული კატეგორიის მონაცემი - პერსონალურ მონაცემთა დაცვის შესახებ კანონის მე-3 მუხლის „ბ“ ქვეპუნქტით განსაზღვრული ინფორმაცია. მაგალითად, რასობრივ ან ეთნიკურ კუთვნილებასთან, მრწამსთან, ჯანმრთელობასთან დაკავშირებული ინფორმაცია და სხვა.

საერთაშორისო გადაცემა - მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა.

კანონი - „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი (3144-XIმს-Xმპ, 14.6.2023).

სამსახური - პერსონალურ მონაცემთა დაცვის სამსახური.

GDPR – ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“.

DPIA – მონაცემთა დაცვაზე ზეგავლენის შეფასება.

EDPB – მონაცემთა დაცვის ევროპული საბჭო.

შესავალი

დღესდღეობით, იმის გათვალისწინებით რომ შესაბამისი მომსახურებების, ბიზნესოპერაციების მარტივად ხელმისაწვდომობის უზრუნველსაყოფად უმეტესად ციფრული მეთოდები გამოიყენება. შესაბამისად, უდიდესი მნიშვნელობა გააჩნია ციფრულ სამყაროში მონაცემთა დამუშავებას, რომლის ერთ-ერთ მაგალითსაც ვებსაიტის მეშვეობით მომხმარებლების/ვიზიტორების თაობაზე ინფორმაციის მოპოვება/შეგროვება თუ სხვაგვარი დამუშავება წარმოადგენს.

წინამდებარე რეკომენდაციის მიზანია მონაცემთა დაცვის ეროვნული კანონმდებლობის, საერთაშორისო აქტებისა და საუკეთესო პრაქტიკის გათვალისწინებით, ვებსაიტის შექმნის მსურველებს მიაწოდოს ის ძირითადი ინფორმაცია, რაც მომხმარებელთა უფლებების დაცვაზე ორიენტირებული მიდგომებისა და პროდუქტის ჩამოყალიბებაში დაეხმარება.

აღნიშნულ დოკუმენტში განხილულია მნიშვნელოვანი საკითხები, რაც ვებსაიტის შექმნის ეტაპიდანვე მის მფლობელს, ასევე დეველოპერებს დაეხმარება მონაცემთა დაცვის საორიენტაციო საკითხების განსაზღვრაში და სათანადო ღონისძიებების ეტაპობრივად დაგეგმვაში. რეკომენდაცია მოიცავს რამდენიმე თავს, რომელიც შეეხება მონაცემთა დამუშავების საფუძვლებს, მიზნებს, პრინციპებს, მონაცემთა დაცვაზე ზეგავლენის შეფასებას, მონაცემთა მეტად დაფარვის პრიორიტეტს, ინფორმაციის აღრიცხვის ვალდებულებას, მზა-ჩანაწერების გამოყენებას, სუბიექტების ინფორმირებას, ინციდენტის შეტყობინების ვალდებულებას, საერთაშორისო გადაცემას, მესამე პირების ჩართულობით მონაცემთა დამუშავებას, სუბიექტის უფლებებს და აღნიშნულ საკითხებთან დაკავშირებულ პრაქტიკულ რეკომენდაციებს/მაგალითებს.

ვებსაიტის მეშვეობით მონაცემთა დამუშავება

ვებსაიტი მსოფლიო კომპიუტერული ქსელის, ინტერნეტის მეშვეობით ხელმისაწვდომი ფაილების და მასთან დაკავშირებული წყაროების, ვებგვერდების[1] ერთობლიობაა. იგი მასობრივი კომუნიკაციისა და მასობრივი მედიის ერთ-ერთი ძირითადი საშუალებაა[2] და ინფორმაციის დიდი რაოდენობით პირთათვის მიწოდების/გავრცელების ეფექტურ გზას წარმოადგენს. პირის/ორგანიზაციის საქმიანობის სპეციფიკიდან გამომდინარე ვებსაიტის შექმნის მიზანი, მისი დანიშნულება შესაძლოა განსახვავებული იყოს, შესაბამისად მისი ფუნქციონალებიც სწორედ აღნიშნულ საკითხებზე იყოს დამოკიდებული. პრაქტიკაში გავრცელებულია შემდეგი ტიპის ვებსაიტები: *ბლოგები (კონკრეტული საკითხის ან სფეროს შესახებ ინფორმაციის მიწოდების მიზანი); ელექტრონული კომერციის გვერდები (ხშირად ცნობილი როგორც ონლაინ მაღაზიები - ნივთების/მომსახურების შესყიდვა, ონლაინ გადარიცხვები); პორტფოლიოს ტიპის ვებგვერდები (პროფესიული საქმიანობა); საინფორმაციო ვებსაიტები (კონკრეტული პირის, პროდუქტის/მომსახურების/ობიექტის, ასევე შესაბამისი თემატიკის შესახებ ინფორმაციის მიწოდების მიზანი); დასაქმების პლატფორმები; საგანმანათლებლო პლატფორმები; ვებპორტალები (მაგალითად, უნივერსიტეტის, სკოლის ან სხვა დაწესებულების ვებგვერდი, სადაც პირებს - სტუდენტებს, დასაქმებულ პირებს - მათთვის განკუთვნილ კონკრეტულ ინფორმაციაზე წვდომისთვის ესაჭიროებათ მომხმარებლის ანგარიშში შესვლა); სოციალური ქსელები; ფორუმები და სხვა.*

სწორედ ვებსაიტის შექმნის მიზანსა და დანიშნულებაზეა დამოკიდებული თუ რა სახის პერსონალური მონაცემები დამუშავდება აღნიშნული პლატფორმის მეშვეობით. ამასთან, აუცილებელია **წინასწარ მოხდეს მონაცემთა დამუშავების თითოეული პროცესის იდენტიფიცირება და უკვე შემდგომ განისაზღვროს რა სახისა და კატეგორიის მონაცემების დამუშავებაა აუცილებელი თითოეულ შემთხვევაში.**

მაგალითად, ონლაინ სავაჭრო პლატფორმაზე, საქმიანობის სპეციფიკიდან გამომდინარე, მომხმარებლის შექმნის, მისთვის მომსახურების გაწევის მიზნებისთვის, კომპანიას შესაძლოა ესაჭიროებოდეს ისეთი ინფორმაცია, როგორიცაა სახელი, გვარი, მობილურის ნომერი, ელექტრონული ფოსტის მისამართი, მისამართი და სხვა. ცალკეულ შემთხვევებში, ვებსაიტს მოქალაქეთა განცხადების მიღების ფუნქცია გააჩნია - შესაბამისად, შესაძლოა მისი მეშვეობით გროვდებოდეს ისეთი ინფორმაცია როგორიცაა სახელი, გვარი, პირადი ნომერი, ელ-ფოსტის მისამართი, ასევე განცხადებაში მითითებული მონაცემები.

[1] ციფრული ფაილები, რომლებიც ჰიპერტექსტის მარკირების ენით, HTML - ის მეშვეობით იქმნება. იხ. GeeksForGeeks, What is website? <https://www.geeksforgeeks.org/blogs/what-is-a-website/>.

[2] The Editors of Encyclopedia Britannica, "Website", *Encyclopedia Britannica*, 24 Mar. 2025, https://www.britannica.com/technology/website. Accessed 10 July 2025.

↳ გაითვალისწინეთ:

IP-ი მისამართები და ონლაინ იდენტიფიკატორები პერსონალურ მონაცემთა დაცვის კანონმდებლობის მიზნებისთვის პერსონალურ მონაცემებად მიიჩნევა, ვინაიდან კონკრეტული ფიზიკური პირის - მომხმარებლის იდენტიფიცირების შესაძლებლობას იძლევა. ავსტრიის მონაცემთა დაცვის საზედამხედველო ორგანოს თანახმად, პირის ფაქტობრივი იდენტიფიცირება არ არის აუცილებელი[3], იმისათვის რომ IP მისამართის ინფორმაცია პერსონალურ მონაცემად იქნეს მიჩნეული. ზოგიერთ შემთხვევაში პირის მაიდენტიფიცირებელი ინფორმაცია, შესაძლოა არ იყოს ერთი ორგანიზაციის ხელში, თუმცა მონაცემთა ერთობლიობა, რომლის ობიექტური და გონივრული გაერთიანების შესაძლებლობაც გააჩნიათ მათ მფლობელებს - კონკრეტული პირის იდენტიფიცირების საშუალებას იძლეოდეს.[4]

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

ნებისმიერი ახალი პროდუქტის თუ მომსახურების შექმნას, რომლის ფუნქციონირების პროცესში პერსონალური მონაცემები მუშავდება, მომხმარებელთა უფლებების შეზღუდვის საფრთხეები ახლავს სამომავლო რისკების, დროისა თუ ფინანსური რესურსების არამიზნობრივი დანახარჯების შემცირებისა და კანონშესაბამისობის წინმსწრებად უზრუნველსაყოფად მნიშვნელოვანია ახალი პროდუქტის/მომსახურების შემუშავების ეტაპიდანვე მონაცემთა დაცვა მხედველობაში იქნას მიღებული, როგორც ერთ-ერთი პრიორიტეტული საკითხი.

პერსონალურ მონაცემთა დაცვის შესახებ კანონის 26-ე მუხლი მონაცემთა მეტად დაფარვის პრიორიტეტის ვალდებულებას ითვალისწინებს, რომელიც საერთაშორისო კანონმდებლობით ცნობილია, როგორც “By Design and By Default”[5]-ის მიდგომა. აღნიშნული მხედველობაშია მისაღები ვებსაიტის, როგორც ახალი პროდუქტის/მომსახურების შექმნის შემთხვევაშიც.

“Privacy By Design” - ახალი პროდუქტის/მომსახურების შექმნისას დამუშავებისთვის პასუხისმგებელმა პირმა, როგორც **დამუშავების საშუალებების განსაზღვრის,** ისე **უშუალოდ დამუშავების პროცესში** უნდა მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები (მათ შორის, ფსევდონიმიზაცია ან/და სხვა). მათი განსაზღვრისთვის მხედველობაში უნდა იქნეს მიღებული:

[3] The Datenschutzbehörde (DSB (Austria)), 2021-0.586.257 (D155.027), 22.12.2021, <https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2021-0.586.257>.

[4] CJEU, Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, 19.10.2016, §§44-45.

[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 (GDPR)), Article 25.

- ახალი ტექნოლოგიები - იგულისხმება *როგორც ტექნიკური, ასევე ორგანიზაციული ზომების კუთხით გაზარზე ხელმისაწვდომი უახლესი მეთოდების გამოყენების საჭიროება;*
- მათი განხორციელების ხარჯები - რომელიც უნდა შეფასდეს *ფინანსური, ადამიანური და დროის რესურსების გათვალისწინებით;*
- დამუშავების ხასიათი, მასშტაბი, კონტექსტი და მიზნები - ორგანიზაციამ *უნდა გაითვალისწინოს მონაცემთა დამუშავების პროცესის მოცულობა და ფარგლები, სპეციფიკური მახასიათებლები, მიზნები, ასევე გარემოებები, რომლებიც შესაძლოა გავლენას ახდენდეს მონაცემთა სუბიექტის უფლებებსა და მოლოდინებზე;*
- მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისთვის მოსალოდნელი რისკები - *უნდა შეფასდეს ყველა ის პოტენციური საფრთხე, რაც სუბიექტებს შესაძლოა მიადგეთ ახალი პროდუქტით/მომსახურებით სარგებლობისას მონაცემთა დამუშავების პროცესში*;
- მონაცემთა დამუშავების პრინციპები.

სათანადო ტექნიკურ და ორგანიზაციულ ზომებში მოიაზრება არამხოლოდ უახლესი ტექნოლოგიური გადაწყვეტილებები, არამედ დასაქმებული პირების საბაზისო ტრენინგებიც.[6] აღნიშნული საკითხი უფრო დეტალურად განხილული იქნება მონაცემთა უსაფრთხოების თავში.

Ϟ გაითვალისწინეთ:

სათანადო ტექნიკური და ორგანიზაციული ზომების მიღება უნდა უზრუნველყოფდეს მონაცემთა დამუშავების პროცესში კანონმდებლობით გათვალისწინებული პრინციპების ეფექტიან იმპლემენტაციას და მონაცემთა სუბიექტის უფლებების დასაცავად აუცილებელი მექანიზმების ინტეგრირებას.

მონაცემთა დამუშავების პრინციპები „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებულ ვალდებულებას წარმოადგენს, რომელიც მონაცემთა დამუშავების თითოეულ პროცესში უნდა იყოს დაცული. აღნიშნული მოიცავს, მონაცემთა დამუშავებას:

- ✓ კანონიერად, სამართლიანად, გამჭვირვალედ და ღირსების შეულახავად;
- ✓ მკაფიო, კონკრეტული და ლეგიტიმური მიზნებისთვის;
- ✓ ნამდვილი, ზუსტი და განახლებული მონაცემების უზრუნველყოფით;
- ✓ მონაცემთა მინიმიზაციას - ლეგიტიმური მიზნის პროპორციული მოცულობით;
- ✓ ლეგიტიმური მიზნის შესაბამისი ვადით შენახვით;
- ✓ მონაცემთა უსაფრთხოების უზრუნველყოფით.

დამატებით, იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლი.

[6] European Data Protection Board (EDPB), Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 20 October 2020, §9.

“Privacy By Default” - მონაცემთა **რაოდენობის**, მონაცემთა **დამუშავების მასშტაბის, შენახვის ვადებისა** და მონაცემებზე **წვდომის განსაზღვრისას** „პირველად პარამეტრად“ უნდა განისაზღვროს, რომ ავტომატურად დამუშავდეს მხოლოდ ის მონაცემები, რომლებიც კონკრეტული მიზნისთვისა არის აუცილებელი.

„პირველად პარამეტრად“ (Default) მოიხსენიება აპლიკაციის, კომპიუტერული პროგრამის ან მოწყობილობის პარამეტრების წინასწარ არსებული/შერჩეული მახასიათებელი, რომელთა შეცვლა შემდგომში მომხმარებლის მიერ არის შესაძლებელი.[7] ვებსაიტის შექმნის პროცესში, *მაგალითად, როდესაც მომხმარებლის რეგისტრაციის ფუნქციონალით ხდება მისი აღჭურვა,* „პირველად პარამეტრად“ უნდა განისაზღვროს იმ მოცულობის/რაოდენობის მონაცემების დამუშავება, ასევე მათი შენახვის ისეთი ვადა, რომელიც მკაცრად აუცილებელია აღნიშნულ შემთხვევაში დასახული, კანონიერი მიზნისთვის. ზემოხსენებული პირდაპირ კავშირშია მონაცემთა დამუშავების პრინციპების დაცვის ვალდებულებასთან. ამასთან, წინასწარ უნდა განისაზღვროს იმ კონკრეტულ პირთა წრე, ვინც უფლებამოსილი იქნებიან, მათი უშუალო ფუნქციებიდან გამომდინარე განახორციელონ წვდომა ვებგვერდის მეშვეობით მოპოვებულ/შეგროვებულ მონაცემებზე.

➪ დამატებით, იხ. პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია „მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას“.

➪ პერსონალურ მონაცემთა დაცვის სამსახურის პოდკასტი N15.

მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვის ვალდებულება

ვებსაიტის მეშვეობით მონაცემთა დამუშავების პროცესები შესაძლოა ერთმანეთისგან სრულიად განსხვავებული იყოს. კანონშესაბამისობის დემონსტრირებისა და დამუშავებისას ეფექტური თვითკოორდინირებისთვის, მნიშვნელოვანია მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვის ვალდებულება, რომელსაც კანონის 28-ე მუხლი ითვალისწინებს. აღნიშნულ შემთხვევაში, მნიშვნელოვანია გაიმიჯნოს დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის მიერ აღსარიცხავი მონაცემები.

დამუშავებისთვის პასუხისმგებელმა პირმა უნდა აღრიცხოს ინფორმაცია:

[7] იქვე. §40.

- ✓ *დამუშავებისთვის პასუხისმგებელი პირის/ სპეციალური წარმომადგენლის/ პერსონალურ მონაცემთა დაცვის ოფიცრის/თანადამუშავებისთვის პასუხისმგებელი პირების/დამუშავებაზე უფლებამოსილი პირის* **ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია**;
- ✓ მონაცემთა დამუშავების **მიზნების** შესახებ;
- ✓ მონაცემთა **სუბიექტებისა** და **მონაცემთა** კატეგორიების შესახებ;
- ✓ მონაცემთა **მიმღების** კატეგორიების შესახებ;
- ✓ მონაცემთა **საერთაშორისო გადაცემის შესახებ** (პერსონალურ მონაცემთა დაცვის სამსახურის ნებართვის თაობაზე, ასეთის არსებობისას);
- ✓ მონაცემთა **შენახვის ვადების** შესახებ ან განსაზღვრის კრიტერიუმების თაობაზე (თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია);
- ✓ მიღებული **ორგანიზაციულ-ტექნიკური ზომების** ზოგადი აღწერა;
- ✓ **ინციდენტების** შესახებ ინფორმაცია (ასეთის არსებობის შემთხვევაში).

დამუშავებაზე უფლებამოსილმა პირმა უნდა აღრიცხოს ინფორმაცია:

- ✓ *დამუშავებაზე უფლებამოსილი პირის/პერსონალურ მონაცემთა დაცვის ოფიცრის/დამუშავებისთვის პასუხისმგებელი პირის/თანადამუშავებისთვის პასუხისმგებელი პირების/სპეციალური წარმომადგენლის* **ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია**;
- ✓ დამუშავებისთვის პასუხისმგებელი პირისთვის ან მისი სახელით განხორციელებული მონაცემთა დამუშავების სახეების შესახებ;
- ✓ საერთაშორისო გადაცემის თაობაზე ინფორმაცია, თუ იგი მონაწილეობს სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის მონაცემთა გადაცემის პროცესში;
- ✓ მიღებული ორგანიზაციულ-ტექნიკური ზომების ზოგადი აღწერა;
- ✓ ინციდენტების შესახებ ინფორმაცია (ასეთის არსებობის შემთხვევაში).

აღრიცხვის შაბლონური ფორმა არ არის დადგენილი, დამოკიდებულია თავად ორგანიზაციაზე და მნიშვნელოვანია შინაარსობრივად სრულყოფილად ასახავდეს ზემოხსენებულ ინფორმაციას.

↳ გაითვალისწინეთ:

აღრიცხვას ორგანიზაცია შიდაუწყებრივად ახორციელებს, ამასთან, იგი ვალდებულია პერსონალურ მონაცემთა დაცვის სამსახურს მონაცემთა დამუშავებასთან დაკავშირებით აღრიცხული ინფორმაცია წარუდგინოს მოთხოვნისთანავე, არაუგვიანეს სამი დღისა.

➪ დამატებით, იხ. პერსონალურ მონაცემთა დაცვის სამსახურის საგანმანათლებლო პლატფორმის „მოდული 5: მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა“

➪ „პერსონალურ მონაცემთა დაცვის ოფიცრის დღიური“ N2.

ინფორმაციის აღრიცხვის სანიმუშო ფორმა

*აღნიშნული ცხრილი არის ინფორმაციის აღრიცხვის ერთ-ერთი მაგალითი. რეკომენდებულია ორგანიზაციის საქმიანობიდან გამომდინარე ინდივიდუალურად, წინა თავში განხილული ინფორმაციის შესაბამისად, შეადგინოთ და განსაზღვროთ თქვენზე მორგებული ფორმატი.

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი	• *სახელწოდება/ვინაობა:* • *საიდენტიფიკაციო/პირადი ნომერი:* • *იურიდიული/ფაქტობრივი მისამართი:* • *ტელეფონის ნომერი:* • *ელექტრონული ფოსტის მისამართი:*
პერსონალურ მონაცემთა დაცვის ოფიცერი *(მიუთითეთ ასეთის არსებობის შემთხვევაში)*	• *სახელწოდება/ვინაობა:* • *საიდენტიფიკაციო/პირადი ნომერი:* • *იურიდიული/ფაქტობრივი მისამართი:* • *ტელეფონის ნომერი:* *ელექტრონული ფოსტის მისამართი:*
თანადამუშავებისთვის პასუხისმგებელი პირები *(მიუთითეთ ასეთის არსებობის შემთხვევაში)*	• *სახელწოდება/ვინაობა:* • *საიდენტიფიკაციო/პირადი ნომერი:* • *იურიდიული/ფაქტობრივი მისამართი:* • *ტელეფონის ნომერი:* • *ელექტრონული ფოსტის მისამართი:*
დამუშავებაზე უფლებამოსილი პირის *(მიუთითეთ ასეთის არსებობის შემთხვევაში)*	• *სახელწოდება/ვინაობა:* • *საიდენტიფიკაციო/პირადი ნომერი:* • *იურიდიული/ფაქტობრივი მისამართი:* • *ტელეფონის ნომერი:*

	• *ელექტრონული ფოსტის მისამართი:*
მონაცემთა დამუშავების მიზანი	
მონაცემთა სუბიექტის კატეგორიები	
მონაცემთა კატეგორიები	
მონაცემთა მიმღების კატეგორიები	
საერთაშორისო გადაცემა	
შენახვის ვადები	*მითითება: მონაცემების შენახვის ვადა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად უნდა იყოს აუცილებელი. *მაგალითად, აღნიშნული შესაძლებელია უკავშირდებოდეს სამართლებრივი ურთიერთობის ხანდაზმულობის ვადებს ან უშუალოდ იყოს განსაზღვრული ეროვნული კანონმდებლობით.*
უსაფრთხოების ზომები	*მითითება: უნდა აღირიცხოს ორგანიზაციულ-ტექნიკური ზომების ზოგადი აღწერა, მაგალითად, ისეთი მეთოდების გამოყენება როგორიცაა დეპერსონალიზაცია, ფსევდონიმიზაცია, დასაქმებულ პირთა ტრენინგები, ინფორმირება და სხვა.*

ინციდენტის შესახებ ინფორმაცია *(ასეთის არსებობის შემთხვევაში)*	

მონაცემთა დამუშავების პრინციპები

მონაცემთა დამუშავების პრინციპები, არის ზოგადი წესებისა და სახელმძღვანელო დებულებების ერთობლიობა, რომელთა დაცვას ვებსაიტის ფუნქციონირებისას, მონაცემთა დამუშავების ნებისმიერ პროცესში, თითოეულ ეტაპზე უდიდესი მნიშვნელობა გააჩნია. აღსანიშნავია, რომ მონაცემთა დამუშავების კანონშესაბამისობისთვის აუცილებელია დამუშავებისთვის პასუხისმგებელმა პირმა თავად უზრუნველყოს ყველა მონაცემთა დამუშავების პრინციპის დაცვა და შეძლოს თითოეულ მათგანთან შესაბამისობის დასაბუთება.

❒ კანონიერების, გამჭვირვალობის, სამართლიანობის პრინციპი

ფიზიკური პირის შესახებ ინფორმაცია უნდა დამუშავდეს კანონიერად. სამართლიანად, მონაცემთა სუბიექტისთვის გამჭვირვალედ[8] და მისი ღირსების შეულახავად.

დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა **კანონიერად** დამუშავების უზრუნველსაყოფად უნდა განსაზღვროს მონაცემთა დამუშავების სათანადო სამართლებრივი საფუძველი, გაატაროს ღონისძიებები, რომელიც უზრუნველყოფს დამუშავების მთლიანი პროცესის კანონთან შესაბამისობას.

სამართლიანობა ყოვლისმომცველი პრინციპია, რომელიც მოიაზრებს რომ მონაცემთა სუბიექტისთვის მის შესახებ ინფორმაციის დამუშავება არ უნდა იყოს გაუმართლებელი ზიანი მომტანი, დისკრიმინაციული, ღირსების შემლახავი, არაეთიკური, არაგონივრული, შეცდომაში შემყვანი. მონაცემთა დამუშავების პროცესის სამართლიანად წარმართვისთვის, ასევე აუცილებელია სუბიექტის უფლებების სრულყოფილად დაცვა.[9]

გამჭვირვალობა გულისხმობს, რომ პირისთვის მარტივად აღქმადი, ხელმისაწვდომი და გასაგები უნდა იყოს მონაცემთა დამუშავების პროცესის შესახებ ინფორმაცია. ამასთან, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს რომ ინფორმაცია სუბიექტს უნდა მიეწოდოს დროულად, მონაცემთა დამუშავების პროცესის შესაფერისი ფორმით, იგი უნდა იყოს ყოვლისმომცველი და ხელმისაწვდომი სხვადასხვა წყაროს მეშვეობით.[10] აღნიშნული პრინციპი პირდაპირ კავშირშია მონაცემთა სუბიექტის ინფორმირების

[8] მონაცემთა დამუშავების გამჭვირვალობის ვალდებულება არ ვრცელდება პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონით დადგენილ გამონაკლის შემთხვევებზე.

[9] European Data Protection Board (EDPB), Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 20 October 2020, §§69-70.

[10] იქვე, §§65 – 66.

ვალდებულებასთან[11] და კანონის მე-3 თავით განსაზღვრულ სუბიექტის უფლებებთან.

❐ მიზნის შეზღუდვის პრინციპი

მონაცემთა შეგროვებამდე/მოპოვებამდე უნდა განისაზღვროს კონკრეტული, მკაფიო, ლეგიტიმური მიზნები, რომელსაც მონაცემთა დამუშავების ინდივიდუალური პროცესი ემსახურება. აღნიშნულ მიზანზე არის დამოკიდებული თუ რა სახის პერსონალური მონაცემები, რა მოცულობით უნდა დამუშავდეს, ასევე მათი შემდგომი შენახვის ვადაც.

↳ გაითვალისწინეთ:

დაუშვებელია მონაცემები დამუშავდეს სხვა, დამუშავების თავდაპირველ მიზანთან შეუთავსებელი მიზნით.

❐ მონაცემთა მინიმიზაციის პრინციპი

მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად და იყოს აღნიშნული მიზნის თანაზომიერი. აღნიშნული მოიაზრებს, რომ მონაცემები რომლებიც სუბიექტის შესახებ დამუშავდება საჭირო და აუცილებელი უნდა იყოს წინასწარგანსაზღვრული კონკრეტული, მკაფიო და ლეგიტიმური მიზნის მისაღწევად. სხვაგვარად, უფრო ნაკლები მოცულობით მონაცემთა დამუშავების შემთხვევაში ეს მიზანი ვერ უნდა მიიღწეოდეს.

❐ მონაცემთა ნამდვილობისა და სიზუსტის პრინციპი

მონაცემები უნდა იყოს ნამდვილი, ზუსტი და, საჭიროების შემთხვევაში, განახლებული, ხოლო არაზუსტი მონაცემების შემთხვევაში დამუშავებისთვის პასუხისმგებელმა პრიმა უნდა მიიღოს ყველა გონივრული ზომა, რათა ისინი გასწორდეს, წაიშალოს ან განადგურდეს გაუმართლებელი დაყოვნების გარეშე.

➦ მაგალითი:

ვებსაიტის მეშვეობით მონაცემთა შეგროვებისას, სუბიექტის შესახებ ინფორმაციის სიზუსტის, ნამდვილობის უზრუნველსაყოფად შესაძლოა გამოყენებულ იქნეს ვერიფიკაციის მექანიზმები (მაგალითად, მობილურის ნომერზე, ელექტრონული ფოსტის მისამართზე ერთჯერადი კოდის გაგზავნით). ვებსაიტზე მომხმარებლის რეგისტრაციის შემთხვევაში კი კონფიდენციალურობის პარამეტრები შესაძლებელს უნდა ხდიდეს, რომ მომხმარებელმა თავად შეძლოს მის შესახებ მოწოდებული ინფორმაციის შესწორება/ განახლება.

[11] იხილეთ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 24-ე მუხლი.

❒ შენახვის ვადის შეზღუდვის პრინციპი

მონაცემთა დამუშავების თითოეულ პროცესში, ფიზიკური პირის შესახებ მოპოვებული ინფორმაცია შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც ლეგიტიმური მიზნის მისაღწევად არის აუცილებელი. აღნიშნული მიზნის მიღწევის შემდეგ კი ისინი უნდა წაიშალოს, განადგურდეს ან შენახული უნდა იქნეს დეპერსონალიზებული ფორმით. თუ მონაცემთა დამუშავება კანონით ან კანონქვემდებარე ნორმატიული აქტითაა განსაზღვრული, აღნიშნულ შემთხვევაზე ზემოხსენებული შეზღუდვა არ გავრცელდება.

პირი თავად აფასებს და ასაბუთებს მონაცემთა შენახვის საჭიროებას და კონკრეტულ ვადას, რომლის ფარგლებშიც მონაცემები აუცილებელია შეინახოს. აღნიშნული, შესაძლოა ზოგიერთ შემთხვევაში პირდაპირ რეგულირდებოდეს კანონმდებლობით.

↳ გაითვალისწინეთ:

მონაცემებზე წვდომის განხორციელების თითოეული შემთხვევა („ლოგები“), ისევე, როგორც სხვა მონაცემები შენახული უნდა იქნეს წინასწარ განსაზღვრული ვადით.[12]

↳ ვებსაიტის მეშვეობით მონაცემთა დამუშავებისას მნიშვნელოვანია ავტომატური წაშლის მექანიზმის არსებობა, რომელიც წინასწარ განსაზღვრული ვადის დადგომის შემდეგ მონაცემების წაშლას/განადგურებას/დეპერსონალიზებას უზრუნველყოფს. ამასთან, შესაძლოა აუცილებელი გახდეს ავტომატური წაშლის პროცესების „ლოგების“ შენახვა შესაბამისი ფაქტის დასადასტურებლად. [13]

↳ მომხმარებლების შესახებ არსებული ინფორმაცია არ უნდა დამუშავდეს განუსაზღვრელი ვადით, ასევე თუ აღარ არსებობს მონაცემთა დამუშავების მიზანი. ხანგრძლივი პერიოდის განმავლობაში არააქტიური მომხმარებლის არსებობის შემთხვევაში, რეკომენდებულია არსებობდეს ანგარიშის ავტომატური დეაქტივაციის მექანიზმი, რომლის თაობაზეც წინასწარ უნდა მოხდეს ვებსაიტის მომხმარებლის - მონაცემთა სუბიექტის ინფორმირება.[14]

თუ მონაცემთა წაშლა შესაძლოა დამოკიდებული იყოს სუბიექტის ნებაზე და იგი მომხმარებლის სახით რეგისტრირდება ვებსაიტზე, აუცილებელია, მას კონფიდენციალურობის პარამეტრების მეშვეობით მიეცეს აღნიშნულის განხორციელების საშუალება.

[12] Commission nationale de l'informatique et des libertés (CNIL), Developer's Guide - Sheet n°7: Minimize the Data Collection, 2020, <https://www.cnil.fr/en/sheet-ndeg7-minimize-data-collection>.

[13] იქვე.

[14] Commission nationale de l'informatique et des libertés (CNIL), 2023, 2, 7, <https://www.edpb.europa.eu/system/files/2023-10/fr_2023-06decisionpublic_redacted.pdf>

❒ მონაცემთა უსაფრთხოების პრინციპი

მონაცემების უსაფრთხოების დაცვის მიზნით მიღებულ უნდა იქნეს ისეთი ტექნიკური და ორგანიზაციული ზომები, რომლებიც სათანადოდ უზრუნველყოფს მონაცემთა დაცვას. აღნიშნულში, მათ შორის, მოიაზრება იმგვარი ღონისძიებების გატარება, რომელიც მონაცემთა უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვის, განადგურების ან/და დაზიანების პრევენციას მიემართება. მონაცემთა უსაფრთხოების პრინციპის დაცვა განსაკუთრებით მნიშვნელოვანია, როდესაც მონაცემთა შეგროვება/მოპოვება/შენახვა თუ სხვაგვარი ფორმით დამუშავება ელექტრონული საშუალებებით - ციფრულად ხდება (კიბერუსაფრთხოებასთან დაკავშირებული გამოწვევების გათვალისწინებით). შესაბამისად, აღნიშნული ორგანიზაციულ-ტექნიკური ზომების განსაზღვრისას თავდაპირველად უნდა შეფასდეს ის რისკები რაც არსებული გამოწვევების, მდგომარეობის გათვალისწინებით შეიძლება ახლდეს მონაცემთა დამუშავების კონკრეტულ პროცესს, ხოლო შემდგომ განისაზღვროს ის მოწინავე და ხელმისაწვდომი მეთოდები, რომელიც უზრუნველყოფს აღნიშნული გამოწვევების პროპორციულ დაცვას. უფრო დეტალურად მონაცემთა უსაფრთხოების უზრუნველყოფის საკითხზე შემდეგ თავებში იქნება განხილული.

ვებგვერდის მეშვეობით მონაცემთა დამუშავების საფუძველი

წინა თავში განხილული საკითხების (როგორიცაა ვებსაიტის მეშვეობით მონაცემთა დამუშავების პროცესების, მათი მიზნების, მოცულობის იდენტიფიცირება) შეფასების შემდეგ, აუცილებელია განისაზღვროს რა სამართლებრივი საფუძველი არსებობს მონაცემთა დამუშავების თითოეულ პროცესში.

კანონი მონაცემთა დამუშავების საფუძვლებს მონაცემთა კატეგორიების მიხედვით განასხვავებს, კერძოდ ზოგადად პერსონალური მონაცემების დამუშავება დასაშვებია მე-5 მუხლით გათვალისწინებული ერთ-ერთი გარემოების არსებობისას, ხოლო განსაკუთრებული კატეგორიის მონაცემების შემთხვევებში კი მე-6 მუხლით განსაზღვრული წინაპირობა უნდა არსებობდეს.

როგორც წესი, ვებსაიტის შექმნისას, მისი ფუნქციონალების გათვალისწინებით მონაცემთა დამუშავება შესაძლოა ხდებოდეს:

- მონაცემთა სუბიექტის თანხმობით;
- მონაცემთა სუბიექტის განცხადების განსახილველად;

- ხელშეკრულებით ნაკისრი ვალდებულებების შესაბამისად ან ასეთი გარიგების დასადებად;
- პირდაპირ კანონით/კანონმდებლობით იყოს გათვალისწინებული;
- ლეგიტიმური ინტერესის შესაბამისად;

↳ გაითვალისწინეთ:

მონაცემთა დამუშავების სამართლებრივი საფუძვლის დასაბუთების ვალდებულება ეკისრება დამუშავებისთვის პასუხისმგებელ პირს.

დამუშავებისთვის პასუხისმგებელმა პირებმა, მონაცემთა დამუშავების პროცესის გამჭვირვალობის ვალდებულებების შესაბამისად, უნდა მიიღონ შესაბამისი ზომები, რათა სამართლებრივ საფუძველთან დაკავშირებით გაუგებრობა/ბუნდოვანება თავიდან იქნეს აცილებული.[15] პრაქტიკაში ხშირად პრობლემურია მონაცემთა დამუშავებაზე თანხმობის, ხელშეკრულებაზე თანხმობის გამიჯვნა, მიუხედავად იმისა რომ შინაარსობრივად ისინი მონაცემთა დამუშავების დამოუკიდებელ საფუძველს წარმოადგენენ და სხვადასხვა სამართლებრივ შედეგებს შეიძლება უკავშირდებოდნენ.

ხელშეკრულებით ნაკისრი ვალდებულებების შესასრულებლად მონაცემთა დამუშავება

თუ ვებსაიტის მეშვეობით მონაცემთა დამუშავება მომხმარებელთან დადებული **ხელშეკრულებით ნაკისრი ვალდებულებებიდან გამომდინარეობს**, დამუშავებისთვის პასუხისმგებელ პირს უნდა შეეძლოს აღნიშნულის აუცილებლობის დასაბუთება. მონაცემთა დამუშავების აუცილებლობა უნდა შეფასდეს არამხოლოდ ორგანიზაციის პერსპექტივიდან, არამედ იგი მონაცემთა სუბიექტის გონივრულ მოლოდინებთან იყოს შესაბამისობაში. კერძოდ, მისთვის როგორც მხარისთვის ობიექტურად რამდენად აღქმადია მონაცემთა დამუშავების საჭიროება სახელშეკრულებო ურთიერთობაში შესვლამდე, და შესაძლებელია თუ არა ზემოხსენებული ვალდებულებები შესრულდეს კონკრეტულ მონაცემთა დამუშავების გარეშე. შესაბამისად, აუცილებელია აღნიშნულ საკითხს დამუშავებისთვის პასუხისმგებელმა პირმა შეხედოს როგორც თავისი, ისე მონაცემთა სუბიექტის პერსპექტივიდან.[16]

➦ მაგალითი:

მომხმარებელი ყიდულობს ნივთს ონლაინ მაღაზიიდან, პროდუქტის საფასურს იხდის საბანკო ბარათით, ხოლო მათი მიწოდება კი სურს კონკრეტულ მისამართზე. იმისათვის, რომ ონლაინ მაღაზიამ შეძლოს მომხმარებლისთვის მომსახურების გაწევა და ხელშეკრულებით ნაკისრი ვალდებულებების

[15] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 2019, §20.
[16] იქვე, §32.

შესრულება, მას დაჭირდება მონაცემთა სუბიექტის გარკვეული ინფორმაციის დამუშავება საგადასახადო და ადრესატისთვის პროდუქტის ჩაბარების მიზნებისთვის. ამასთან, თუ სუბიექტს არ სურს ნივთის ადგილზე მიწოდება და თავად აიღებს ამანათს მაღაზიის ფილიალიდან - მისი მისამართის დამუშავების აუცილებლობა ხელშეკრულების შესრულებისთვის არ იარსებებს. [17]

➦ მაგალითი:

ონლაინ მაღაზიას სურს დაიმახსოვროს მომხმარებლის პრეფერენციების თაობაზე ინფორმაცია ვებსაიტზე განხორციელებული შესყიდვების თუ ვიზიტების გათვალისწინებით. **პროფაილინგის განხორციელება** აღნიშნულ შემთხვევაში **ვერ იქნება** სახელშეკრულებო ვალდებულების შესასრულებლად აუცილებელი მონაცემთა დამუშავება და ამისათვის მაღაზიას უნდა ჰქონდეს დამოუკიდებელი სამართლებრივი საფუძველი.[18]

თუ ხელშეკრულება სხვადასხვა დამოუკიდებელ მომსახურებას შეეხება, ან მომსახურების სხვადასხვა კომპონენტებს მოიცავს, თითოეულთან მიმართებით ინდივიდუალურად უნდა შეფასდეს რამდენად არის აუცილებელი და გონივრული მომხმარებლის, როგორც მონაცემთა სუბიექტის შესახებ ინფორმაციის დამუშავება კონკრეტულ შემთხვევებში. მაგალითად, შესაძლოა გამოიკვეთოს რომ მონაცემთა დამუშავება ზოგიერთი სერვისის მისაწოდებლად, ხელშეკრულებით ნაკისრი ვალდებულებიდან გამომდინარეობს, მაშინ როცა ცალკეული მონაცემების დამუშავება მხოლოდ კონკრეტული კომპანიის ბიზნეს მოდელის განვითარებისთვის იყო საჭირო და აღნიშნულისთვის სრულიად დამოუკიდებელი სამართლებრივი საფუძველი უნდა არსებობდეს.[19]

მონაცემთა სუბიექტის თანხმობის საფუძველზე მონაცემთა დამუშავება

თუ პერსონალური მონაცემების დამუშავების სხვა სპეციალური საფუძველი არ არსებობს, მონაცემები შესაძლოა დამუშავდეს მხოლოდ მონაცემთა სუბიექტის თანხმობით. ამასთან, იმისათვის რომ აღნიშნული თანხმობა ნამდვილად, ხოლო მონაცემთა დამუშავება დასაშვებად იქნას მიჩნეული რამდენიმე საკითხის გათვალისწინებაა აუცილებელი.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი,[20] ასევე GDPR-ი[21] თანხმობის შემადგენელ აუცილებელ ელემენტებს განსაზღვრავს:

[17] იქვე, §34, Example 1.
[18] იქვე, §35, Example 2.
[19] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 2019, §30.
[20] იხ. კანონის მე-3 მუხლის „მ“ და „ნ“ ქვეპუნქტები.
[21] GDPR, Article 4 (11).

- ✓ ნებაყოფლობითობა;
- ✓ კონკრეტულობა;
- ✓ ინფორმირებულობა;
- ✓ მონაცემთა სუბიექტის სურვილის მკაფიოობა;
- ✓ გამოხატული აქტიური ქმედებით.

↳ გაითვალისწინეთ:

თუ მონაცემთა დამუშავება შესაძლოა მოხდეს სხვა სამართლებრივი საფუძვლით, მაგალითად, ხელშეკრულებით ნაკისრი ვალდებულებების შესასრულებლად, კანონმდებლობით პირდაპირ იყოს გათვალისწინებული, ანუ არსებობს მონაცემთა დამუშავების უფრო სპეციალური და კონკრეტული საფუძველი, მონაცემთა სუბიექტისგან დამუშავებაზე თანხმობის მოთხოვნა/მოპოვება შეცდომაში შემყვანი და დასაწყისიდანვე უსამართლო იქნება.

დამუშავებისთვის პასუხისმგებელმა პირმა, მონაცემთა დამუშავებამდე სათანადო გულისხმიერებით, წინაწარ უნდა შეაფასოს, ინდივიდუალური გარემოებების გათვალისწინებით, რა საფუძვლით დაამუშავებს პერსონალურ მონაცემებს და სუბიექტს სწორი ინფორმაცია მიაწოდოს აღნიშნულის თაობაზე.[22]

თანხმობის ნებაყოფლობითობა მოიაზრებს, რომ მონაცემთა სუბიექტს უნდა მიეცეს რეალური არჩევანისა და გადაწყვეტილების მიღების შესაძლებლობა. თუ პირი იძულებული იქნება განაცხადოს მონაცემთა დამუშავებაზე თანხმობა, ან უარის თქმა/არ დათანხმება მისთვის უარყოფითი შედეგის მომტანი იქნება - აღნიშნული ვერ ჩაითვლება მისი ნების თავისუფალ გამოხატულებად.[23] თუ რაიმე სახის მომსახურების მისაღებად პირს ესაჭიროება მონაცემთა დამუშავებაზე თანხმობის გაცხადება, რაც რეალურად არ არის აუცილებელი მხარის მიერ გარიგებით ნაკისრი ვალდებულებების შესასრულებლად ანდა მომსახურების გასაწევად, ხოლო მონაცემთა დამუშავებაზე/თანხმობის გაცემაზე უარის თქმა მომსახურების მიღებას შეუზღუდავს - მსგავს შემთხვევებში გაცემული თანხმობა ვერ იქნება მიჩნეული ნებაყოფლობითად და მონაცემთა დამუშავების წინაპირობად.[24]

➦ მაგალითი:

ვებსაიტის პროვაიდერმა ტექსტური ფაილის - „სკრიპტის“ მეშვეობით შეზღუდა შიგთავსის („კონტენტის“) ხილვადობა პირისთვის. ერთადერთი, რაც პირისთვის ხილვადია არის მზა-ჩანაწერების („ქუქი-ფაილი“) შესახებ ინფორმაცია და მათზე დათანხმების ფუნქციონალი. ვებგვერდის ძირითად შიგთავსზე წვდომას და მომსახურების მიღებას ვიზიტორი/მომხმარებელი მხოლოდ მზა-ჩანაწერების

[22] ICO, For Organisations/ UK GDPR Guidance and Resources/ Lawful Basis/ Consent/ When is Consent Appropriate - When is consent inappropriate? , <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/>.

[23] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 4 May 2020, §13.

[24] იხ. კანონის 32-ე მუხლის მე-2 პუნქტი.

განთავსებაზე დათანხმების შემთხვევაში შეძლებს - აღნიშნული კი ვერ იქნება მიჩნეული ნებაყოფლობითად გაცემულ თანხმობად, ვინაიდან სუბიექტის თავისუფალ ნებას არ ეფუძნება.[25]

თანხმობის კონკრეტულობა გულისხმობს რომ სუბიექტმა თავისი ნება უნდა გამოხატოს დამუშავების კონკრეტულ პროცესთან და მიზანთან მიმართებით. თუ მონაცემები სხვადასხვა მიზნით დამუშავდება, შესაძლოა აუცილებელი იყოს თითოეული მათგანის მიმართ თანხმობის დამოუკიდებლად გაცხადება.

↳ გაითვალისწინეთ:

თუ მონაცემთა სუბიექტის წერილობითი თანხმობის მიღება ხდება დოკუმენტით, რომელიც დამატებით სხვა საკითხებს შეეხება, აღნიშნულ დოკუმენტში მონაცემთა დამუშავებაზე თანხმობის შესახებ ტექსტი უნდა იყოს მკაფიო, მარტივი და გასაგები ენით ჩამოყალიბებული, დოკუმენტის სხვა ნაწილებისგან განცალკევებული.

თანხმობის ინფორმირებულობა პირდაპირ კავშირშია მონაცემთა სუბიექტის ინფორმირების ვალდებულებასთან, რომელიც ადგენს მისთვის მისაწოდებელი მინიმალური ინფორმაციის ჩამონათვალს.

კერძოდ, პირისგან ინფორმაციის შეგროვებისას მას უნდა მიეწოდოს შემდეგი ინფორმაცია:

- დამუშავებისთვის პასუხისმგებელი პირის/ მისი წარმომადგენლის/ დამუშავებაზე უფლებამოსილი პირის (ასეთის არსებობის შემთხვევაში) ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია;
- მონაცემთა დამუშავების მიზნებისა და სამართლებრივი საფუძვლის შესახებ;
- პერსონალურ მონაცემთა დაცვის ოფიცრის (ასეთის არსებობის შემთხვევაში) ვინაობა და საკონტაქტო ინფორმაცია;
- მონაცემთა მიმღების ვინაობა/მონაცემთა მიმღებების კატეგორიები (ასეთის არსებობის შემთხვევაში);
- საერთაშორისო გადაცემასთან დაკავშირებული ინფორმაცია - მონაცემთა დაგეგმილი გადაცემისა და მონაცემთა დაცვის სათანადო გარანტიების არსებობის შესახებ, მათ შორის, მონაცემთა გადაცემაზე ნებართვის თაობაზე (ასეთის არსებობის შემთხვევაში);
- მონაცემთა შენახვის ვადის შესახებ ან ვადის განსაზღვრის კრიტერიუმების თაობაზე (თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია);

[25] იქვე, §§40 – 41.

- მონაცემთა სუბიექტის უფლებების შესახებ.[26]

თანხმობის მიღებამდე უნდა მოხდეს სუბიექტის ინფორმირება მის მიერ **თანხმობის გამოხმობის უფლების** და შესაბამისი მექანიზმის თაობაზე, რომელიც უნდა იყოს:

- უსასყიდლო;
- მარტივი;
- ხელმისაწვდომი;
- უზრუნველყოს თანხმობის გამოხმობის შესაძლებლობა იმავე ფორმით, რომლითაც გაიცა თანხმობა.[27]

თანხმობის მოპოვების შემთხვევებში, ორგანიზაციამ უნდა უზრუნველყოს რომ სუბიექტს თითოეულ ჯერზე ინფორმაცია მიეწოდა მკაფიო და მარტივი ენით, რომელიც გასაგები იქნება ჩვეულებრივი ადამიანისთვის, ვისაც არ აქვს სამართლებრივი განათლება მიღებული.[28] იმ შემთხვევებში როდესაც ვებგვერდის მომსახურების მიმღები პოტენციურად შეიძლება იყოს არასრულწლოვანი პირი, მისაწოდებელი ინფორმაციის ფორმა მისი ასაკის, სავარაუდო განვითარების ეტაპის ადეკვატური უნდა იყოს.

მონაცემთა სუბიექტის მკაფიოდ გამოხატული სურვილი, კერძოდ, პირმა მისი სურვილი მონაცემების დამუშავებასთან დაკავშირებით უნდა გამოხატოს აქტიური მოქმედებით ან განცხადებით.

სუბიექტის მონაცემების დამუშავებასთან დაკავშირებული თანხმობა ვერ იქნება მიჩნეული ნამდვილად თუ იგი არ არის გამიჯნული ხელშეკრულების პირობებზე ან მომსახურების ძირითად პირობებზე დათანხმებისგან, ასევე თუ მას ბლანკეტური, ზოგადი ხასიათი გააჩნია.

ჯ გაითვალისწინეთ:

ვებსაიტით სარგებლობისას პირს არ უნდა უწევდეს წინასწარ მონიშნული თანხმობის უჯრის/ველის მეშვეობით უარის თქმა მისი მონაცემების დამუშავებაზე, როდესაც აღნიშნულის ფუნქციაა მისი თანხმობის მოპოვება მონაცემთა დამუშავების კონკრეტულ პროცესთან მიმართებით. მან თავად, საკუთარი გადაწყვეტილების საფუძველზე, აქტიური მოქმედებით უნდა მონიშნოს ან შეავსოს კონკრეტული უჯრა/ველი, რომელიც მონაცემთა დამუშავებაზე სუბიექტის თანხმობის მოპოვებას ემსახურება.

მონაცემთა სუბიექტის აქტიურ ქმედებად და ნების გამოხატულებად ასევე ვერ იქნება მიჩნეული პირის დუმილი, ანდა მომსახურების მიღების გაგრძელება[29],

[26] კანონის 24-ე მუხლის პირველი პუნქტი.
[27] კანონის 32-ე მუხლის მე-8 პუნქტი.
[28] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 2020, §67.
[29] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 2020, §79.

მაგალითად ვებგვერდზე რაიმე ქმედების განხორციელება, „სქროლვა“ სხვა ველებზე გადასვლა და ა.შ.[30]

თანხმობა შესაძლოა მიღებული იქნეს არამხოლოდ წერილობითი ფორმით, ხელმოწერით, არამედ ელექტრონული ფორმითაც[31] - მაგალითად, კონკრეტული უჯრის მონიშვნით, ეკრანზე რაიმე მოქმედების შესრულებით, როგორიცაა ნიშნულის გადაწევა და ა.შ.[32] აღნიშნულ შემთხვევაში განხორციელებული ქმედება შესაძლოა სუბიექტის მიერ გაცხადებულ თანხმობად იქნას მიჩნეული თუ პირს მიეწოდა ინფორმაცია არამხოლოდ მონაცემთა დამუშავებასთან დაკავშირებით, არამედ იმისა თაობაზეც, რომ მისი კონკრეტული ქმედება მიჩნეული იქნება თანხმობად. მაგალითად, რომ ნიშნულის გადაწევით/უჯრის მონიშვნით იგი თანხმობას აცხადებს მისი მონაცემები დამუშავდეს წინასწარ მიწოდებული ინფორმაციის შესაბამისად.[33]

↳ გაითვალისწინეთ:

არასრულწლოვნის მონაცემთა - თანხმობის საფუძველზე - დამუშავების შემთხვევაში უნდა დაიცვათ შემდეგი წესები:

❑ არასრულწლოვანის შესახებ მონაცემთა დამუშავება მისი თანხმობის საფუძველზე დასაშვებია - **თუ მან 16 წლის ასაკს მიაღწია.**

❑ **16 წლამდე არასრულწლოვანის** შესახებ მონაცემთა დამუშავება დასაშვებია – მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობით. გამონაკლისია, როდესაც კანონი პირდაპირ ითვალისწინებს სხვა რეგულირებას.

❑ დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მიიღოს გონივრული და ადეკვატური ზომა არასრულწლოვანის მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობის არსებობის დასადასტურებლად.

❑თანხმობა არ ჩაითვლება ნამდვილად, თუ მონაცემთა დამუშავება საფრთხეს უქმნის ან ზიანს აყენებს არასრულწლოვანის საუკეთესო ინტერესებს.

❑16 წლამდე არასრულწლოვანის მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობის არსებობის დასადასტურებლად ხელმისაწვდომი ტექნოლოგიების გათვალისწინებით მიღებულ უნდა იქნას ყველა გონივრული ზომა.[34]

❑მონაცემთა დამუშავებისას, ორგანიზაცია ვალდებულია გაითვალისწინოს და დაიცვას **არასრულწლოვანის საუკეთესო ინტერესები.**

[30] იქვე, 86.
[31] იხ. კანონის მე-3 მუხლის „მ“ და „ნ“ ქვეპუნქტები.
[32] The Autoriteit Persoonsgegevens (AP), Home/ Themes/ Basic GDPR/ GDPR basics/ Legal Basis of Consent, <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/legal-basis-of-consent>.
[33] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 2020, §85.
[34] Data Protection Commission (DPC), Guidance Note: Legal Bases for Processing Personal Data December 2019, 9.

თანხმობის გამოხმობა

თუ თანხმობა მიღებულია ელექტრონული საშუალებით, *მაგალითად, ღილაკზე თითის დაჭერით, მონიშვნით და სხვა ელექტრონული ქმედების განხორციელებით,* აღნიშნულის თანატოლი/პროპორციული მექანიზმი უნდა განისაზღვროს თანხმობის გამოხმობისთვისაც. ამასთან აღნიშნული მექანიზმი უნდა იყოს **სუბიექტისთვის** ხელმისაწვდომი და უსასყიდლო.[35]

❑მონაცემთა სუბიექტის მიერ თანხმობის გამოხმობის შემთხვევაში დაუყოვნებლივ შეწყდეს მონაცემთა დამუშავება, ხოლო დამუშავებული მონაცემები წიშალოს/ განადგურდეს.[36]

❑მონაცემთა სუბიექტის მიერ თანხმობის გამოხმობა არ იწვევს თანხმობის გამოხმობამდე და თანხმობის ფარგლებში წარმოშობილი სამართლებრივი შედეგების გაუქმებას.[37]

❑ პირს უნდა მიეწოდოს თანხმობის გამოხმობის შედეგების შესახებ ინფორმაცია თუ **მისი მოთხოვნის** საფუძველზე ან **თუ მისთვის**, როგორც მონაცემთა სუბიექტისთვის თანხმობის გამოხმობა **წარმოშობს სამართლებრივ, ფინანსურ ან სხვა სახის არსებითი მნიშვნელობის მქონე შედეგს.**[38]

↳ გაითვალისწინეთ:

პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავება მხოლოდ პირის თანხმობის საფუძველზეა დასაშვები.

ᲞᲘᲠᲓᲐᲞᲘᲠᲘ ᲛᲐᲠᲙᲔᲢᲘᲜᲒᲘᲡ ᲐᲠᲘᲡ:

❑ ფოსტით ან ნებისმიერი ელექტრონული საშუალებით (მათ შორის, ელ-ფოსტით, ტელეფონით)

❑ მონაცემთა სუბიექტისთვის ინფორმაციის პირდაპირი და უშუალო მიწოდება

❑ ფიზიკური პირის ან/და იურიდიული პირის, საქონლის, იდეის, მომსახურების, სამუშაოს ან/და წამოწყების, აგრეთვე საიმიჯო და სოციალური თემატიკისადმი

❑ ინტერესის ფორმირების, შენარჩუნების, რეალიზაციის ან/და მხარდაჭერის მიზნით.

✎ მაგალითად, როდესაც ვებგვერდის მეშვეობით მოიპოვებთ მომხმარებლის მონაცემებს მისთვის რაიმე სახის შეთავაზების გაგზავნა, ან სიახლეების თაობაზე

[35] იქვე, 114, ასევე კანონის 32-ე მუხლის მე-8 პუნქტი.
[36] კანონის მე-32 მუხლის მე-4 პუნქტი.
[37] კანონის მე-32 მუხლის მე-6 პუნქტი.
[38] კანონის მე-32 მუხლის მე-7 პუნქტი.

ინფორმაციის მიწოდება, ასევე პლატფორმის მეშვეობით მსგავსი შეტყობინებების გაგზავნა, მისი პრეფერენციების გათვალისწინებით პროდუქტების შეთავაზება მხოლოდ მისი წინასწარი თანხმობის შემთხვევაში ჩაითვლება კანონიერად.

პირდაპირი მარკეტინგის განხორციელებისას უნდა დაიცვათ შემდეგი წესები:

❑ **თანხმობის მიღებამდე** - პირს დეტალურად უნდა მიეწოდოს ინფორმაცია:

✓ რა მიზნით (მაგალითად, ახალი პროდუქტების თაობაზე, ვებგვერდზე გამოქვეყნებულ სიახლეებზე, ფასდაკლებების თაობაზე) დამუშავდება მისი მონაცემები;

✓ დამუშავებისთვის პასუხისმგებელი პირის, მისი წარმომადგენლის ან/და დამუშავებაზე უფლებამოსილი პირის, პერსონალურ მონაცემთა დაცვის ოფიცრის (ასეთის არსებობის შემთხვევაში) ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია;

✓ მონაცემთა შენახვის ვადის ან მისი განსაზღვრის კრიტერიუმების შესახებ;

✓ მონაცემთა მიმღების, მათი კატეგორიების შესახებ (ასეთის არსებობისას);

✓ მისი უფლებების შესახებ.

❑ **თანხმობის გამოხმობის უფლება** - პირს ნათლად, მარტივ და მისთვის გასაგებ ენაზე უნდა განემარტოს თანხმობის ნებისმიერ დროს გამოხმობის უფლება და ამ უფლების განხორციელების მექანიზმი/წესი (მაგალითად, შიდა პარამეტრების მეშვეობით მომხმარებლის შესაძლებლობა ე.წ. Opt-out-ის ფუნქციით გამოიხმოს მის მიერ უკვე გაცემული თანხმობა) - თანხმობის მიღებამდე და პირდაპირი მარკეტინგის განხორციელებისას; მონაცემთა დამუშავების შეწყვეტისთვის გათვალისწინებული საშუალება უნდა იყოს მარტივი.

❑ **თანხმობის გაცემის დრო და ფაქტი** უნდა აღრიცხოს და შეინახოს პირდაპირი მარკეტინგის განხორციელების ვადით.

❑ **თანხმობის გაცემის/გამოხმობის დრო და ფაქტი** უნდა აღირიცხოს პირდაპირი მარკეტინგის განხორციელების შეწყვეტიდან 1 წლის განმავლობაში.

„მზა-ჩანაწერების“ გამოყენება

ვებსაიტების ფუნქციონირებაში მნიშვნელოვანი როლი აქვს „მზა-ჩანაწერებს“ (“cookies”), მცირე ზომის ტექსტურ ფაილებს, რომლებიც მომხმარებლის მოწყობილობაზე (პერსონალურ კომპიუტერზე, პლანშეტზე, მობილურ ტელეფონზე და ა.შ.) თავსდება. აღნიშნული ტექნოლოგიები სხვადასხვა მნიშვნელოვანი ფუნქციის შესრულებას, მათ შორის, მომხმარებლის და ვებსაიტზე მისი ინტერაქციის დამახსოვრებას ემსახურება. ისინი შესაძლოა გამოიყენებოდეს

მაგალითად, ონლაინ მაღაზიის ციფრულ "ურიკაში" განთავსებული ნივთების „მიდევნებისთვის" ("tracking") ან ონლაინაპლიკაციის ფორმაში მითითებული ინფორმაციის დასამახსოვრებლად. ასევე, საბანკო ან სხვა მსგავსი ონლაინსერვისებით სარგებლობის პროცესში მნიშვნელოვანი როლი შეიძლება ჰქონდეს ავთენტიფიკაციის „მზა-ჩანაწერებს" - მომხმარებლების იდენტიფიცირების მიზნებისთვის. ზოგიერთი ტიპის "cookie" ვებგვერდების სწრაფად ჩამოტვირთვისთვის და ინფორმაციის ქსელური განაწილებისთვის გამოიყენება. „მზა-ჩანაწერების" მიერ შენახული ინფორმაცია შესაძლოა მოიცავდეს პერსონალურ მონაცემებს, როგორიცაა IP მისამართი, მომხმარებლის სახელი ("username"), უნიკალური იდენტიფიკატორები, ელექტრონული ფოსტის მისამართი.[39] გარდა აღნიშნულისა, ისინი ვებსაიტის სარგებლობისას გამოყენებული მოწყობილობის ტიპთან ან ენის პარამეტრებთან დაკავშირებულ ინფორმაციას ამუშავებენ.[40]

"მზა-ჩანაწერები", რომელთა მოქმედების ვადაც ვებბრაუზერის სესიის ბოლოს იწურება - „სესიის მზა-ჩანაწერებს" წარმოადგენს, ხოლო იმგვარი ფაილები, რომელიც მოწყობილობაში ხანგრძლივი ვადით ინახება, „ხანგრძლივი მზა-ჩანაწერებია".

"Cookie" ფაილების რამდენიმე ტიპი შეიძლება განვასხვავოთ:

შენახვის ვადის მიხედვით:

სესიის „მზა-ჩანაწერები" შესაძლოა გამოყენებულ იქნას მაგალითად, უსაფრთხოების მიზნებისთვის - როდესაც მომხმარებელი შედის ინტერნეტბანკის ან მისი ელ-ფოსტის ანგარიშში. ასევე შესაძლოა მიემართებოდეს მომხმარებლის ქმედებების ერთმანეთთან დაკავშირებას, იმ ინფორმაციის დამახსოვრებას, რაც ვებგვერდით სარგებლობისას შეავსო და სხვა.

ხანგრძლივი „მზა-ჩანაწერები" შესაძლოა გამოიყენებოდეს ვებსაიტის გამოყენებისას მომხმარებლის არჩევნების, იმ პროდუქტების/თემატიკის დასამახსოვრებლად რომელსაც უპირატესობას ანიჭებს ან მიზნობრივი რეკლამირებისთვის. „მზა-ჩანაწერების" განთავსებასა და მოქმედების ამოწურვას შორის არსებული დროის ხანგრძლივობას თავად ვებსაიტის ოპერატორი განსაზღვრავს. ამასთან, მომხმარებელს შეუძლია განთავსებული „ხანგრძლივი მზა-

[39] "GDPR"-ის თანახმად, ფიზიკურ პირთან დაკავშირებული ონლაინ იდენტიფიკატორები პერსონალურ მონაცემებს წარმოადგენს. *იხ.* 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), Article 4 (1).

[40] Data Protection Commission (DPC), Guidance Note: Cookies and Other Tracking Technologies, 2020, 3.

ჩანაწერები“ თავად წაშალოს ან ბრაუზერის პარამეტრები განსაზღვროს და კონკრეტული პერიოდულობით წაიშალოს ავტომატურად.[41]

განმთავსებლის მიხედვით:

პირველი მხარის „მზა-ჩანაწერები“ (“first party cookies”) უშუალოდ ვებსაიტის მიერ განთავსებული ფაილებია.

მესამე პირთა „მზა-ჩანაწერები“ (“third party cookies”) ვებსაიტის სხვა მომსახურების გამწევი პირების მიერ განთავსდება და შესაძლოა უკავშირდებოდეს მაგალითად, ანალიტიკას, რეკლამირებას, სოციალურ მედიას და სხვა.[42]

სავალდებულოობის მიხედვით:

სავალდებულო „მზა-ჩანაწერები“ ტექნიკური სახის ფაილები, რომლებიც ვებსაიტის ფუნქციონირებისათვის და მომხმარებლისთვის შესაბამისი მომსახურების მიწოდებისთვის არის აუცილებელი.

არასავალდებულო „მზა- ჩანაწერები არატექნიკური სახის ფაილებია, რომელთა გამოყენება ვებსაიტის ფუნქციონირებისთვის და მომსახურების გაწევისთვის აუცილებელი არ არის. მისი მიზანი ძირითადად შეიძლება იყოს მეტად მორგებული მომსახურება, ასევე მიზნობრივი რეკლამირება, მომსახურების გაუმჯობესება ან სხვა.[43]

„მზა-ჩანაწერების“ მეშვეობით მონაცემთა დამუშავების საფუძველი

„მზა-ჩანაწერების“ მეშვეობით პერსონალურ მონაცემთა დამუშავება საჭიროებს მონაცემთა დამუშავების პროცესში გასათვალისწინებელი საკითხების უზრუნველყოფას, მისი ფუნქციონირების სპეციფიკის გათვალისწინებით.

თავდაპირველად უნდა შეფასდეს რა სახის პერსონალური მონაცემები დამუშავდება „მზა-ჩანაწერების“ მეშვეობით, რა მიზანი გააჩნია აღნიშნულს და რა ფუნქციური დანიშნულება აქვს - რამდენად აუცილებელია მისი მეშვეობით ვებსაიტის მომხმარებლების მონაცემების დამუშავება, შესაბამისად რა საფუძველი ექნება „მზა-ჩანაწერების“ ფუნქციონირებას. როგორც წესი, აღნიშნული შეიძლება იყოს თანხმობა, ან ცალკეულ შემთხვევებში მომსახურების გაწევის თუ ვებსაიტის ფუნქციონირებისთვის აუცილებელი ლეგიტიმური მიზნებიდან გამომდინარეობდეს.

[41] Information Commissioner’s Office (ICO), Guidance on the Use of Cookies and Similar Technologies, 2019, 5-6.
[42] Data Protection Commission (DPC), Guidance Note: Cookies and Other Tracking Technologies, 2020, 3.
[43] Garante per la protezione dei dati personali (GPDP), Guidelines on Cookies and Other Tracking Tools Executive Summary.

თუ “cookie” ფაილები, მათი დანიშნულებიდან გამომდინარე, **აუცილებელია ვებგვერდის ძირითადი ფუნქციების შესასრულებლად,** იმისათვის რომ მომხმარებელს/ვიზიტორს შესაბამისი მომსახურება გაეწიოს, დამატებით თანხმობის მოპოვება არ არის აუცილებელი.

➦ მაგალითი:

ვებსაიტის თანხმობა შესაძლოა არ იყოს აუცილებელი „მზა-ჩანაწერებისთვის“ რომელიც:

✓ ონლაინმაღაზიის ვებსაიტზე „ურიკაში“ განთავსებული ნივთების/პროდუქტების დასამახსოვრებლად ან თანხის გადასახდელადა არის აუცილებელი;

✓ მომხმარებლის მიერ მოთხოვნილი ონლაინ მომსახურების - მაგალითად, ინტერნეტ ბანკინგის - პროცესში ინფორმაციის უსაფრთხოების უზრუნველყოფისთვისაა აუცილებელი;

✓ ვებგვერდის „კონტენტის“ დროულ ჩამოტვირთვას უზრუნველყოფს.[44]

თუ “cookie” ფაილების დანიშნულება კავშირში არ არის მომსახურების გაწევის, ვებგვერდის ფუნქციონირების მიზანთან, ხოლო მისი მეშვეობით მომხმარებლის/ვიზიტორის შესახებ ინფორმაციის დამუშავება **აუცილებლობას არ წარმოადგენს** და მიემართება მაგალითად, სერვისის განვითარებას, ქცევით რეკლამირებას, ანალიტიკას და ა.შ. მონაცემთა სუბიექტის შესახებ ინფორმაციის დამუშავებისთვის შესაძლოა უშუალოდ მისი თანხმობა იყოს აუცილებელი.[45]

„მზა-ჩანაწერების“ მეშვეობით მონაცემთა დამუშავებაზე თანხმობა უნდა აკმაყოფილებდეს იმავე წინაპირობებს (ინფორმირების შედეგად, ნებაყოფლობითად, მკაფიო, კონკრეტული მიზნით, აქტიური მოქმედებით იყოს გამოხატული), რაც წინა თავში იყო განხილული, მათი სპეციფიკის გათვალისწინებით. კერძოდ, თანხმობა მოპოვებულ უნდა იქნეს ვებსაიტზე შესვლისთანავე, სანამ ისინი მომხმარებლის მოწყობილობაზე განთავსდება, მაგალითად, „cookie” ბანერების მეშვეობით. მონაცემთა დამუშავების თითოეულ მიზანთან მიმართებით (რეკლამირების, ანალიტიკის და ა.შ.) თანხმობა განცალკევებული უნდა იყოს და სუბიექტმა ინდივიდუალურად უნდა განაცხადოს იგი.

„მზა-ჩანაწერების“ მეშვეობით მონაცემთა დამუშავების თაობაზე ინფორმირება

[44] Information Commissioner’s Office (ICO), Cookies and similar technologies, https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/cookies-and-similar-technologies/# [5.8.2025].
[45] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 2019, §55.

მიუხედავად იმისა თუ რა ტიპის „მზა-ჩანაწერები“ გამოიყენება, ასევე რა საფუძვლით ხდება მონაცემების დამუშავება, ვებგვერდის მომხმარებელს სრულყოფილი ინფორმაცია უნდა მიეწოდოს „cookie”-ის გამოყენების თაობაზე. აღნიშნული უზრუნველყოფს კანონმდებლობით გათვალისწინებული გამჭვირვალობის პრინციპის დაცვას, რაც გულისხმობს რომ დამუშავების პროცესი მარტივად აღქმადი უნდა იყოს მონაცემთა სუბიექტისთვის. ამასთან, იგი პირის შესახებ ინფორმაციის დამუშავებაზე თანხმობის ნამდვილობისთვის ერთ-ერთ აუცილებელ წინაპირობას წარმოადგენს.

ვიზიტორის ინფორმირების ვალდებულება მოიცავს როგორც „მზა-ჩანაწერების“ პოლიტიკის მეშვეობით (“Cookie Policy”) მომხმარებლისთვის დეტალური ინფორმაციის მიწოდებას, ისე პირველად ინფორმირებას კონკრეტული „მზა-ჩანაწერების“ დანიშნულების თაობაზე (მაგალითად, ბანერზე განთავსებული ზოგადი ინფორმაციით).

ინფორმაცია “cookie” ფაილების თაობაზე უნდა მოიცავდეს:

- რა სახის „მზა-ჩანაწერები“ გამოყენება ვებსაიტის მიერ;
- რა კონკრეტული მიზნით ხდება მათი განთავსება;
- აუცილებელია თუ არა მათი განთავსება ვებგვერდის ფუნქციონირებისთვის, რა საფუძვლით მოხდება მათი მეშვეობით მონაცემთა დამუშავება - *მაგალითად ვიზიტორის თანხმობით თუ აღნიშნული ვებსაიტის ლეგიტიმურ ინტერესს ან მომსახურების გაწევას მიემართება.*
- რა ვადით ხდება „მზა-ჩანაწერის“ განთავსება, მათ შორის, “სესიის მზა-ჩანაწერები“ გამოიყენება თუ „ხანგრძლივი მზა-ჩანაწერები“;
- მონაცემთა დამუშავების პროცესში არიან თუ არა ჩართული სხვა პირები, რომლებიც არ ფლობენ ვებსაიტს, ახორციელებს თუ არა სხვა ორგანიზაცია ვებსაიტის ვიზიტორის მონაცემებზე წვდომას - მაგალითად, გამოიყენება თუ არა მესამე პირთა „მზა-ჩანაწერები“;
- რა გზით ხდება გაცხადებული თანხმობის გამოხმობა ან “cookie”-ის წაშლა მისი განთავსების შემდგომ.

✎ სამართლიანი და გამჭვირვალე მონაცემთა დამუშავების პროცესის უზრუნველსაყოფად სხვა ინფორმაციასთან ერთად, ვებსაიტის მომხმარებლებისთვის „მზა-ჩანაწერების“ ფუნქციონირების ხანგრძლივობის თაობაზე, ასევე მესამე პირების მიერ მათზე წვდომის თაობაზე ინფორმირების აუცილებლობა, ასევე, ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკით არის დადგენილი. [46]

[46] Court of Justice of the European Union (CJEU), C-673/17, 1.9.2019, Planet49 GmbH., §§72-81.

მნიშვნელოვანია რომ “cookie”-ის შესახებ ინფორმაცია პირს მიეწოდოს მარტივი, გასაგები და მკაფიო ფორმით, რომელიც საშუალო მომხმარებლისთვისაც იქნება აღქმადი. თავიდან უნდა იქნეს არიდებული ზედმეტად ტექნიკური დეტალები, რამაც შესაძლოა ინფორმაციული გადატვირთულობა და დაბნეულობა გამოიწვიოს. რაც შეიძლება მარტივად უნდა განემარტოს სუბიექტს თუ რას წარმოადგენს თითოეული მზა-ჩანაწერი, რა მიზნით გამოიყენება და ა.შ.[47] ვებგვერდზე განთავსებულ ბანერზე გამოყენებული საშუალებები არ უნდა იყოს შეცდომაში შემყვანი. აღნიშნულში მოიაზრება, როგორც მონაცემთა დამუშავების საფუძვლებთან, მიზნებთან, აუცილებლობასთან დაკავშირებით ინფორმაციის მიწოდება, ასევე ტექნიკური ხრიკების (მაგალითად, მცირე ზომის, დამალული ტექსტის გამოყენება, ან ზოგიერთი ღილაკის გაბუნდოვანდება) გამოყენება. ხსენებული კანონმდებლობასთან შესაბამისად ვერ მიიჩნევა, ვინაიდან მომხმარებლის სათანადო ინფორმირება, მათ შორის მონაცემთა დამუშავების პრინციპების სრულყოფილი დაცვა (მათ შორის სამართლიანობის პრინციპის გათვალისწინებით)[48] არ იქნება უზრუნველყოფილი.

✎ საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთი ცნობილი ონლაინმაღაზია „cookie” ფაილების მეშვეობით მონაცემთა დამუშავების პროცესში შემდეგი ვალდებულებების დაუცველობისთვის დააჯარიმა:

✗მომხმარებლების თანხმობის არარსებობა - სარეკლამო მზაჩანაწერები მომხმარებლის ვიზიტისთანავე, მათი თანხმობის გარეშე თავსდებოდა;

✗საინფორმაციო ბანერები, რომელიც მზა-ჩანაწერების მართვას უკავშირდებოდა არ შეიცავდა სრულყოფილ ინფორმაციას, ხოლო „COOKIE SETTING”-ის ღილაკზე დაჭერით მომხმარებელს არ მიეწოდებოდა ინფორმაცია მესამე პირების ვინაობის შესახებ, რომელთა მზა-ჩანაწერებიც სავარაუდოდ გამოიყენებოდა ვებსაიტზე.

✗თანხმობის გამოხმობის და უარის თქმის არასათანადო მექანიზმი - როდესაც მომხმარებელი ბანერზე განთავსებულ უარის თქმის ღილაკს აჭერდა ან როდესაც მის მიერ უკვე გაცემული თანხმობის გამოხმობას ცდილობდა, ძველი მზა-ჩანაწერები კვლავ რჩებოდა, და ახალი თავსდებოდა მის მოწყობილობაზე.[49]

[47] Agencia Española de Protección de Datos (AEPD), Guide on Use of Cookies, 2021, 18-19. <https://www.aepd.es/guides/guide-on-use-of-cookies.pdf>

[48] The Autoriteit Persoonsgegevens (AP), Themes - Internet and smart devices – Cookies - Clear cookie banners, <https://www.autoriteitpersoonsgegevens.nl/en/themes/internet-and-smart-devices/cookies/clear-cookie-banners#which-information-should-be-on-the-first-layer-of-my-cookie-banner> [6.8.2025].

[49] EDPB, French SA: Cookies placed without consent: SHEIN fined 150 000 000 EUR by the CNIL, 4.9.2025,, <https://www.edpb.europa.eu/news/national-news/2025/french-sa-cookies-placed-without-consent-shein-fined-150-000-000-eur-cnil_en>

„მზა-ჩანაწერების“ გამოყენების გავრცელებული არასწორი პრაქტიკა[50]

✗ მხოლოდ „თანახმა ვარ“ ღილაკის გამოყენება, დამუშავების მიზნების დიფერენცირების და პარამეტრების ინდივიდუალურად მორგების გარეშე.

✗ გამოხმობის მექანიზმის არარსებობა.

✗ თანხმობის მისაღებად ვებმისამართის გამოყენება ღილაკის ნაცვლად.

✗ მომხმარებელს/ვიზიტორს არ უნდა დარჩეს შთაბეჭდილება, რომ მხოლოდ „მზა-ჩანაწერებზე“ დათანხმების შემდეგ შეძლებს ვებსაიტით სარგებლობას.[51]

✗ “მზა-ჩანაწერების“ სავალდებულოობის არასწორი კლასიფიცირება.

✗ წინასწარ მონიშნული უჯრები.

✗ შეცდომაში შემყვანი ფერების ან შეცდომაში შემყვანი კონტრასტები.

[50] European Data (EDPB), Report of the Work Undertaken by the Cookie Banner Taskforce Adopted on 17 January 2023.
[51] Agencia Española de Protección de Datos (AEPD), Guide on Use of Cookies, 2024, 21 <https://www.aepd.es/guias/guia-cookies.pdf> .

მონაცემთა სუბიექტების ინფორმირება

გამჭვირვალობა მონაცემთა დამუშავების ერთ-ერთი უმნიშვნელოვანესი პრინციპია, რაც სუბიექტებისთვის დამუშავების პროცესების აღქმადობას უზრუნველყოფს და მათი უფლებების რეალიზაციას უწყობს ხელს. სწორედ აღნიშნული პრინციპიდან გამომდინარეობს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულება, მონაცემთა სუბიექტს მიაწოდოს ინფორმაცია მონაცემთა დამუშავების პროცესის შესახებ. კერძოდ, **სუბიექტისგან მონაცემების შეგროვებისას** პირს უნდა მიეწოდოს სულ მცირე შემდეგი ინფორმაცია:

- დამუშავებისთვის პასუხისმგებელი პირის, მისი წარმომადგენლის ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია (მაგალითად, ელ-ფოსტის მისამართი, სატელეფონო ნომერი, მისამართი);

- პერსონალურ მონაცემთა დაცვის ოფიცრის (ასეთის არსებობის შემთხვევაში) ვინაობა და საკონტაქტო ინფორმაცია;

- დამუშავებაზე უფლებამოსილი პირის არსებობის შემთხვევაში - მისი ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია;

- მონაცემთა დამუშავების მიზნებისა და სამართლებრივი საფუძვლის შესახებ;

- მონაცემთა მისთვის მიწოდების სავალდებულოობის შესახებ. თუ მონაცემთა მიწოდება სავალდებულოა – მონაცემთა მიწოდებაზე უარის თქმის სამართლებრივი შედეგების თაობაზე.

- თუ მონაცემთა შეგროვება/მოპოვება გათვალისწინებულია საქართველოს კანონმდებლობით ან აუცილებელი პირობაა ხელშეკრულების დასადებად - ინფორმაცია აღნიშნულის შესახებ.

- თუ მონაცემები მუშავდება კანონის მე-5 მუხლის პირველი პუნქტის „ი“ ქვეპუნქტის შესაბამისად - დამუშავებისთვის პასუხისმგებელი პირის/მესამე პირის მნიშვნელოვანი ლეგიტიმური ინტერესების შესახებ ;

- თუ შესაძლოა, რომ მონაცემები გადაეცეს სხვა პირს - მონაცემთა მიმღების ვინაობა ან მონაცემთა მიმღებების კატეგორიები;

- მონაცემთა დაგეგმილი გადაცემისა და მონაცემთა დაცვის სათანადო გარანტიების არსებობის შესახებ. თუ დამუშავებისთვის პასუხისმგებელი პირი გეგმავს მონაცემთა სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის გადაცემას - მონაცემთა გადაცემაზე ნებართვის თაობაზე (ასეთის არსებობის შემთხვევაში);

❑ მონაცემთა შენახვის ვადის შესახებ. თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, სუბიექტს უნდა ეცნობოს ვადის განსაზღვრის კრიტერიუმების თაობაზე;

❑ მონაცემთა სუბიექტის უფლებების შესახებ[52] და შესაბამისი მექანიზმის თაობაზე, რითიც შეძლებს აღნიშნული უფლებით სარგებლობას (მაგალითად, კონფიდენციალურობის პარამეტრი, ვებსაიტში ინტეგრირებული ფუნქციონალი ან ელექტრონული ფოსტის მისამართი სადაც შესაბამისი მოთხოვნის გაგზავნას შეძლებს).

შესაბამისად, თითოეულ ვებსაიტზე უნდა იყოს განთავსებული პერსონალურ მონაცემთა დაცვის შესახებ დოკუმენტი (მაგალითად, პერსონალურ მონაცემთა დაცვის პოლიტიკა), რომელიც სუბიექტებს მონაცემთა დამუშავების პროცესზე მიაწვდის ინფორმაციას. ვებსაიტის თითოეული გვერდის ვიზიტისას მასზე გადამყვანი ბმული ვიზიტორისთვის მარტივად ხელმისაწვდომი და იდენტიფიცირებადი უნდა იყოს (მაგალითად, "footer"-ში განთავსებით). ისეთი ფერების, კონტრასტების, თუ ადგილმდებარეობის შემთხვევაში, როდესაც ტექსტი/ბმული ნაკლებად თვალსაჩინოა, ან სხვაგვარად ართულებს დოკუმენტის მოძიებას - პოლიტიკის დოკუმენტი ვერ იქნება მიჩნეული მარტივად ხელმისაწვდომად. ასევე, მნიშვნელოვანია, ინფორმაცია ხელმისაწვდომი იყოს იმავე გვერდზე, რომელზეც სუბიექტის მონაცემები გროვდება (მაგალითად, რეგისტრაციისას).[53] რეკომენდებულია, რომ ცალკეულ შემთხვევაში, პირის რეგისტრაცია ან შესაბამისი სერვისის მიწოდება მონაცემთა დაცვის პოლიტიკის გაცნობაზე თანხმობის გაცხადების (მაგალითად, შესაბამისი გრაფის მონიშვნით) შემდეგ იყოს ხელმისაწვდომი.

↳ გაითვალისწინეთ:

მონაცემთა დამუშავების **პროცესში ცვლილებების შემთხვევაში** აუცილებელია შესაბამისი ინფორმაცია განახლდეს ვებსაიტზე განთავსებულ მონაცემთა დაცვის პოლიტიკაში, ამასთან რეგისტრირებული მომხმარებლების შემთხვევაში, შესაბამისი წყაროს გამოყენებით ეცნობოთ აღნიშნული ცვლილების თაობაზე.

სუბიექტის ინფორმირებულობისთვის, პრაქტიკული თვალსაზრისით, მნიშვნელოვანია, მხედველობაში იქნეს მიღებული დოკუმენტის ადრესატები - მონაცემთა სუბიექტები, ინფორმაცია იყოს მათთვის მარტივად გასაგებ ენაზე, მკაფიო, კონკრეტული და ვებგვერდზე ადვილად მიგნებადი. ამასთან, რეკომენდებულია, ვებსაიტი შეიცავდეს ხელმისაწვდომობის ფუნქციებს ("accessibility tools") და იყოს მომხმარებლის/ვიზიტორის საჭიროებებზე

[52] „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, მუხლი 24.
[53] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017, Revised and Adopted on 11 April 2018, §11.

ადაპტირებული, რათა მონაცემთა დამუშავებასთან, სუბიექტის უფლებებთან დაკავშირებული ინფორმაცია მათთვის წაიკითხავდი იყოს.

➪ დამატებით, იხ. პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები „კონფიდენციალურობის პოლიტიკის დოკუმენტების შემუშავების თაობაზე“.

მონაცემთა უსაფრთხოება

უსაფრთხოება მონაცემთა დამუშავების ერთ-ერთი უმნიშვნელოვანესი პრინციპია, რომლის ძირითადი წესები კანონმდებლობითაა[54] გათვალისწინებული. იგი გულისხმობს ისეთი ღონისძიებების გატარებას, რომელიც უზრუნველყოფს მონაცემთა დაცვას არაუფლებამოსილ პირთა მიერ წვდომისგან და დამუშავებისგან, შემთხვევით დაკარგვისგან, განადგურებისგან ან დაზიანებისგან. ციფრული პროდუქტის შექმნისას, ზემოაღნიშნულის აუცილებელი კომპონენტი და დღესდღეობით აქტუალური გამოწვევაა - კიბერუსაფრთხოება, რაც მონაცემებზე გარეშე პირთა მხრიდან ზემოქმედებისგან დაცვაზე უნდა იყოს ორიენტირებული.

პირველ ეტაპზე, აუცილებელია გაანალიზდეს მონაცემთა კატეგორიები და მის უსაფრთხოებასთან დაკავშირებული რისკები, მათ შორის მონაცემთა სუბიექტის უფლებებზე გავლენის ქონის თვალსაზრისით.

შესაბამისი საფრთხეების იდენტიფიცირების შემდეგ უნდა შემუშავდეს და განისაზღვროს უსაფრთხოების ღონისძიებები, რომლებიც მომხმარებლების/ვიზიტორების შესახებ ინფორმაციის დაცულობას უზრუნველყოფს. მნიშვნელოვანია შესაბამისი „ტესტირებების“ ჩატარება, აღნიშნული ზომების ეფექტურობაში დარწმუნებისთვის და შესაბამისი სუსტი მხარეების დასაიდენტიფიცირებლად. მონაცემთა უსაფრთხოების უზრუნველმყოფი ტექნიკური ზომები თავდაპირველად, შექმნისთანავე უნდა იყოს ვებსაიტში ინტეგრირებული. მნიშვნელოვანია, რომ ვებსაიტის მეშვეობით მონაცემთა დამუშავების პროცესში გატარებული უსაფრთხოების ღონისძიებები უნდა აკმაყოფილებდეს საერთაშორისო დონეზე აღნიშნულ სფეროში დამკვიდრებულ სტანდარტებსა და საუკეთესო პრაქტიკას. გასათვალისწინებელია შემდეგი საკითხები:

- არსებული სისტემების, მომსახურებების, მოწყობილობების, პროგრამული უზრუნველყოფის რეგულარული გადახედვა და ტესტირება, რათა დროულად მოხდეს შესაბამისი ხარვეზების, სუსტი მხარეების იდენტიფიცირება;

[54] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლი.

- წვდომის უფლებების მართვა, რაც გულისხმობს, რომ მხოლოდ იმ პირებს აქვთ წვდომა („უფლებამოსილი პირები“) მონაცემებზე, რომლებსაც შესაბამისი საქმიანობიდან, ფუნქციებიდან გამომდინარე ესაჭიროებათ აღნიშნული. დამუშავებისთვის პასუხისმგებელმა პირმა ერთმანეთისგან უნდა გამიჯნოს დასაქმებულ პირთა წვდომის უფლებების მასშტაბი. წვდომის შეზღუდვა, ერთი მხრივ, გულისხმობს რომ მხოლოდ მინიმალური რაოდენობის პირებს უნდა ჰქონდეთ შეზღუდული, მათი ფუნქციებისთვის აუცილებელი წვდომის უფლება პერსონალურ მონაცემებზე, ხოლო, მეორე მხრივ, მოიაზრებს, რომ შესაბამის პირებს მხოლოდ იმ მინიმალური რაოდენობის მონაცემებზე/მონაცემთა ნაკრებზე(dataset) უნდა ჰქონდეთ წვდომა, რაც რეალურად აუცილებელია შესაბამისი ღონისძიებების გასატარებლად. წვდომის სეგრეგაცია გულისხმობს, რომ მონაცემთა დამუშავების პროცესი უნდა ჩამოყალიბდეს იმ ფორმით, რომ არცერთ ინდივიდს არ ექნება ყოვლისმომცველი წვდომა ფიზიკურ პირთა შესახებ არსებულ ინფორმაციაზე; ამასთან აღნიშნულ პირებს უნდა ჰქონდეთ განპიროვნებული მომხმარებელი, რაც მონაცემთა მიმართ განხორციელებულ თითოეულ ქმედებასთან დაკავშირებით მათ იდენტიფიცირებას გახდის შესაძლებელს.
- უსაფრთხო გადაცემისათვის მიღებულ უნდა იქნეს ყველა პრევენციული ზომა არაუფლებამოსილ პირთა მიერ განზრახი თუ შემთხვევითი წვდომისგან და შეცვლისგან დასაცავად;
- მონაცემები უნდა იქნეს შენახული იმგვარად, რომ არაუფლებამოსილ პირებს არ შეეძლოთ მათზე წვდომის განხორციელება და შეცვლა. მნიშვნელოვანია ისეთი პროცედურების მიღება, რომლებიც მონაცემთა ცენტრალიზებული ან დეცენტრალიზებული შენახვის რისკების შეფასებას უზრუნველყოფს, ასევე დამატებითი უსაფრთხოების ზომების მიღება ზოგიერთ მონაცემებთან მიმართებით, რომლებიც ამას საჭიროებს (მაგალითად, იმ ინფორმაციასთან დაკავშირებით, რომელიც განსაკუთრებული სენსიტიურობით ხასიათდება);
- ინფორმაციის ფსევდონიმიზაცია ერთ-ერთი მნიშვნელოვანი გზაა, რომელიც ამცირებს პოტენციური ინციდენტების რისკებს (მაგალითად, დაშიფვრის (“encryption”) ან „ჰეშინგის“ (“hashing”) მეშვეობით);
- მონაცემთა მიმართ განხორციელებული თითოეული ქმედების (ჩამოწერა, ნახვა, ძებნა და ა.შ), „ლოგირებების“, შენახვა მონაცემთა უსაფრთხოების ერთ-ერთი აუცილებელი ზომაა,[55] აღნიშნული გულისხმობს მონაცემის მიმართ კონკრეტულ დროს იმ მომხმარებლების/პირების თაობაზე ინფორმაციის პროგრამულ შენახვას/აღრიცხვას, რომლებმაც აღნიშნულის მიმართ განახორციელეს რაიმე სახის ქმედება. აუცილებელია როგორც მინიმუმ ინახებოდეს ყველაზე მეტად განხორციელებადი ქმედებები,

[55] European Data Protection Board (EDPB), Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 20 October 2020, §85.

როგორიცაა დათვალიერება, შეცვლა, გაერთიანება, ჩამოტვირთვა, გამჟღავნება/გადაცემა, წაშლა[56]. აღნიშნული ხელს უწყობს მონაცემების მიმართ შესრულებული ქმედებების მიკვლევადობას და უსაფრთხოებასთან დაკავშირებული შემთხვევების აღმოჩენას.[57] მნიშვნელოვანია, რომ თავად „ლოგირებების“ შესახებ ინფორმაციის გადამოწმება არ უნდა ხდებოდეს არამიზნობრივად და შესაბამის საფუძველს საჭიროებს (მაგალითად, მონაცემთა დამუშავების კანონიერების დემონსტრირება, მონაცემთა მთლიანობის, უსაფრთხოების უზრუნველსაყოფად, მონიტორინგის განსახორციელებლად, და სხვა).[58]

- უსაფრთხოებასთან დაკავშირებულ ინციდენტზე ეფექტიანი რეაგირებისთვის აუცილებელია არსებობდეს პროცედურები, რომლებიც უზრუნველყოფს მათ აღმოჩენას, შეჩერებას, შესწავლასა და მართვას. სათანადო რეაგირება, ასევე, მოიცავს ინციდენტის თაობაზე საზედამხედველო ორგანოსათვის, ასევე მონაცემთა სუბიექტისთვის შეტყობინების პროცედურების შიდაორგანიზაციულ მოწესრიგებას.[59]
- რეკომენდებულია მომხმარებლის ვებსაიტზე რეგისტრაციის შემთხვევაში სავალდებულო იყოს რთული პაროლის გამოყენება, ასევე მოხდეს მათი ინფორმირება გარკვეული პერიოდულობით ანგარიშის პაროლის განახლების საჭიროებასთან დაკავშირებით.[60]

ვებსაიტის მეშვეობით მონაცემთა დამუშავებისას მნიშვნელოვანია ისეთი ტექნიკური ღონისძიებების გატარება, რომლებიც უზრუნველყოფს მავნე პროგრამების (“malware”) იდენტიფიცირებას, საეჭვო აქტივობების მონიტორინგს და სარეზერვო ასლების (“backups”) რეგულარულ წარმოებას, ასევე მმართველობითი პროცესების უზრუნველყოფას, როგორიცაა მონაცემთა დამუშავებაზე უფლებამოსილი პირის და მის მიერ გატარებული ორგანიზაციულ-ტექნიკური ზომების მონიტორინგი.[61]

ნებისმიერი თანამშრომელი რომელიც მონაწილეობს მონაცემთა დამუშავებაში/აქვთ წვდომა მონაცემებზე, არ უნდა გასცდეს მისთვის მინიჭებული

---

[56] ICO, For Organisations - Law Enforcement - Guide to Law Enforcement Processing -Accountability and governance – Logging, <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/accountability-and-governance/logging/>, [9.9.2025].

[57] EDPB, one-stop-shop case digest on Security of Processing (Art. 32 GDPR) and Data Breach Notification (Art. 33 & 34 GDPR), 2024, 12-13, <https://www.edpb.europa.eu/system/files/2024-01/one_stop_shop_case_digest_security_data_breach_en.pdf>.

[58] ICO, For Organisations - Law Enforcement - Guide to Law Enforcement Processing -Accountability and governance – Logging, <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/accountability-and-governance/logging/>, [9.9.2025].

[59] European Data Protection Board (EDPB), Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 20 October 2020, §85.

[60]Commission nationale de l'informatique et des libertés (CNIL), 2023, 8, <https://www.edpb.europa.eu/system/files/2023-10/fr_2023-06decisionpublic_redacted.pdf>.

[61] Annual Report of the Data Protection Commissioner of Ireland , Case Study 17 - Data Breach at an Online Retailer, 50-51, 2016, <https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Annual%20Report%202016.pdf>.

უფლებამოსილების ფარგლებს, დაიცვას მონაცემთა საიდუმლოება და კონფიდენციალურობა, მათ შორის, სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგ. უსაფრთხოების ორგანიზაციული ღონისძიებების ფარგლებში, აუცილებელია მოხდეს თითოეული დასაქმებული პირის ინფორმირება, კონფიდენციალურობის დებულებების გათვალისწინება შესაბამის დოკუმენტებში, საინფორმაციო შეხვედრები/ტრენინგები ცნობიერების ამაღლებისა და მათზე დაკისრებული პასუხისმგებლობების გასააზრებლად. მონაცემთა უსაფრთხოების უზრუნველსაყოფად არ არის საკმარისი მხოლოდ შესაბამისი „წვდომის“ უფლებამოსილებების განაწილება, არამედ სავალდებულოა ადეკვატური ღონისძიებების გატარება თანამშრომელთა მიერ მონაცემთა უკანონო დამუშავების ფაქტების თავიდან ასაცილებლად, გამოსავლენად და აღსაკვეთად.

↳ გაითვალისწინეთ:

ვებსაიტის მეშვეობით მონაცემთა მოპოვებისას/შენახვისას, თუ სხვა დამუშავებისას აუცილებლად უნდა გაითვალისწინოთ აღნიშნული პროცესის თანმდევი რისკები არამხოლოდ საწყის ეტაპზე, არამედ მონაცემთა დამუშავების მთლიანი პერიოდის განმავლობაში. ამასთან უნდა შეიმუშავოთ ისეთი ორგანიზაციული თუ ტექნიკური ზომები, რომლებიც უზრუნველყოფს აღნიშნული საფრთხეებისგან მონაცემთა სუბიექტების დაცვას და იქნება არსებულ გამოწვევებთან გამკლავების ეფექტიანი საშუალება.

➪ დამატებით, იხ. პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია **“მონაცემთა უსაფრთხოების დაცვის სტანდარტის შესახებ”.**

ინციდენტის შეტყობინების ვალდებულება

ინციდენტი არის მონაცემთა უსაფრთხოების დარღვევა, რომელიც იწვევს მონაცემების არამართლზომიერ/შემთხვევით დაზიანებას, დაკარგვას, უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას/მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას.[62] ვებსაიტის მეშვეობით მონაცემთა დამუშავების სპეციფიკის, ციფრულ სამყაროში უსაფრთხოებასთან დაკავშირებით არსებული გამოწვევების გათვალისწინებით მნიშვნელოვანია ინციდენტის პრევენციისთვის შესაბამისი ღონისძიებების გატარება, რაც წინა თავში არის განხილული. ამასთან, არანაკლებ მნიშვნელოვანია პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შემთხვევაში მისი დროული იდენტიფიცირება, შეფასება და შესაბამისი ზომების გატარება. შესაბამისად, აუცილებელია სათანადო შიდაორგანიზაციული პროცედურებისა თუ პროტოკოლების შემუშავება, რაც გაამარტივებს ზემოაღნიშნულ პროცესს და

[62] კანონის მე-3 მუხლის „წ“ ქვეპუნქტი.

ინციდიენტის დადგომის შემთხვევაში, მისი შეტყობინების კანონმდებლობით გათვალისწინებული ვალდებულების შესრულება.

ინციდენტს შედეგად შესაძლოა მოჰყვეს ფიზიკური, ქონებრივი ან არაქონებრივი ღირებულების მატერიალური ან არამატერიალური ზიანი. ინციდენტი აღმოჩენილად, ხოლო დამუშავებისთვის პასუხისმგებელი პირი ინციდენტის შესახებ ინფორმირებულად ითვლება იმ მომენტიდან, როდესაც მან შეიტყო ინციდენტის შესახებ.[63]

ინციდენტის შემდეგი სახეები არსებობს:

კონფიდენციალურობის დარღვევა

- პერსონალური მონაცემების უნებართვო *გამჟღავნება, წვდომა*;

მთლიანობის დარღვევა

- პერსონალური მონაცემების უნებართვო *შეცვლა*;
- მონაცემთა არამართლზომიერი ან შემთხვევითი *დაზიანება, დაკარგვა.*

ხელმისაწვდომობის დარღვევა

- პერსონალურ მონაცემებზე *წვდომის დაკარგვა* ან *შეზღუდვა;*
- მონაცემების *განადგურება/წაშლა.*

მას შემდეგ, რაც დამუშავებისთვის პასუხისმგებელი პირი აღმოაჩენს ზემოხსენებულ უსაფრთხოების დარღვევას, აღმოჩენისთანავე უნდა დაიწყოს ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობისა და სიმძიმის შეფასება. ხოლო ალბათობის ხარისხის გათვალისწინებით უნდა შეაფასოს მონაცემთა სუბიექტის, პერსონალურ მონაცემთა დაცვის სამსახურის ინფორმირების ვალდებულების წარმოშობის საკითხი კანონის 29-ე და 30-ე მუხლების შესაბამისად.

I საფრთხის შექმნის სიმძიმე ფასდება შემდეგი კრიტერიუმებით:

- ინციდენტის სახე (პერსონალურ მონაცემთა კონფიდენციალურობის, მთლიანობის თუ ხელმისაწვდომობის დარღვევა);
- პერსონალური მონაცემების კატეგორია, რომლებზეც გავლენას ახდენს ინციდენტი;
- სახეზე არის თუ არა არასრულწლოვნის, შეზღუდული შესაძლებლობის მქონე პირის ან სხვა განსაკუთრებული სოციალური თუ სამართლებრივი

[63] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №19 „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ“, მუხლი 4, პუნქტები 1 და 3.

დაცვის საჭიროების მქონე მონაცემთა სუბიექტის პერსონალურ მონაცემებთან დაკავშირებული ინციდენტი;

- მონაცემთა სუბიექტის მესამე პირთა მიერ იდენტიფიცირების შესაძლებლობის ხარისხი;
- დამუშავებისთვის პასუხისმგებელი პირის საქმიანობის განსაკუთრებული ხასიათი, რასაც შესაძლოა ახლდეს მომეტებული საფრთხე;
- ინციდენტის მასშტაბი, მონაცემთა სუბიექტის ან/და პერსონალური მონაცემის რაოდენობის ან/და მოცულობის თვალსაზრისით;
- სხვა ისეთი გარემოება, რამაც შესაძლოა არსებითი გავლენა მოახდინოს ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შექმნის ალბათობის სიმძიმეზე.[64]

II მნიშვნელოვანი ზიანი სახეზე იქნება ერთ-ერთი შედეგის დადგომის ან მისი ალბათობის შემთხვევაში:

- მონაცემთა სუბიექტის *დისკრიმინაცია,* მისი *ვინაობის მითვისება/ გაყალბება*;
- პირისთვის *ფინანსური ზიანი,* მონაცემთა სუბიექტის *რეპუტაციის შელახვა;*
- პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალურობის დარღვევა, ან *სხვა სახის მნიშვნელოვანი სოციალური ან/და ეკონომიკური ზიანი*;
- კანონით გათვალისწინებული *მონაცემთა სუბიექტის უფლებების რეალიზებისათვის ხელის შეშლა,* მათ შორის, მონაცემთა სუბიექტის უფლებების კანონით დადგენილ ვადებში რეალიზების შეზღუდვა;
- პერსონალური მონაცემების იმგვარი *წაშლა/განადგურება, რომელიც არ ექვემდებარება აღდგენას,* ან მისი აღდგენა *არაპროპორციულად დიდ დროსა და ძალისხმევას საჭიროებს,* გარდა იმ შემთხვევისა, როდესაც პერსონალური მონაცემების (გარდა განსაკუთრებული კატეგორიის პერსონალური მონაცემისა) დამუშავების მიზნიდან გამომდინარე, მათი წაშლის/განადგურების შედეგად მონაცემთა სუბიექტს ამ მუხლის „ა“, „ბ“, „დ“, „ე“ და „ვ“ ქვეპუნქტებით გათვალისწინებული ან სხვა მნიშვნელოვანი ზიანი არ ადგება;
- *განსაკუთრებული კატეგორიის მონაცემების* უკანონო გამჟღავნება;
- *ფიზიკური ზიანი,* მათ შორის, სამედიცინო მომსახურების მიღების შეზღუდვა, თუ აღნიშნული იწვევს სამედიცინო მანიპულაციის ან ოპერაციის გადადებას, რაც პაციენტის მკურნალობაზე ახდენს უარყოფით გავლენას;
- *არასრულწლოვნის, შეზღუდული შესაძლებლობების მქონე პირისა* და სხვა *განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების*

[64] იქვე, მუხლი 5.

მქონე მონაცემთა სუბიექტის პერსონალური მონაცემების უკანონო დამუშავება.[65]

III **ინციდენტის შედეგად მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა არის:**

დაბალი - თუ ნაკლებსავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს;

საშუალო - თუ ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნისა და ასეთი ზიანის/საფრთხის არარსებობის ალბათობა მეტნაკლებად თანაბარია;

მაღალი - თუ ინციდენტი დიდი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

IV თუ ინციდენტი **საშუალო/მაღალი ალბათობით** მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს ინციდენტის აღმოჩენიდან **არაუგვიანეს 72 საათისა** აღნიშნულის თაობაზე უნდა ეცნობოს პერსონალურ მონაცემთა დაცვის სამსახურს.[66]

სამსახურის ინფორმირება ხდება წერილობით[67] ან სამსახურის ვებგვერდზე განთავსებული, ინციდენტის შეტყობინების მართვის ელექტრონულ სისტემის მეშვეობით.

თუ ინციდენტი **მაღალი ალბათობით** გამოიწვევს მნიშვნელოვან ზიანს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, გაუმართლებელი დაყოვნების გარეშე აღნიშნულის თაობაზე უნდა ეცნობოს მონაცემთა სუბიექტს. **მას უნდა მიეწოდოს შემდეგი ინფორმაცია:**

- ინციდენტისა და მასთან დაკავშირებული გარემოებების ზოგადი აღწერა;
- სავარაუდო/დამდგარი ზიანის შესამცირებლად ან აღმოსაფხვრელად განხორციელებული ან დაგეგმილი ღონისძიებების შესახებ;

[65] იქვე, მუხლი 6.
[66] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მუხლი 29.
[67] იხ. პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის 28 თებერვლის ბრძანება №19 „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ“, მუხლი 11.

❑პერსონალურ მონაცემთა დაცვის ოფიცრის/სხვა პირის საკონტაქტო მონაცემები.[68]

➦ მაგალითი:

ვებსაიტზე კიბერთავდასხმის შედეგად მომხმარებლების სახელები, პაროლები, შესყიდვების ისტორია საჯაროდ ხელმისაწვდომი გახდა. აღნიშნულმა შესაძლოა მაღალი ალბათობით გამოიწვიოს/შექმნას ადამიანის უფლებებისადმი და თავისუფლებებისადმი მნიშვნელოვანი ზიანის და საფრთხე. შესაბამისად, უნდა მოხდეს როგორც მონაცემთა დაცვის საზედამხედველო ორგანოს, ისე მომხმარებლების (მონაცემთა სუბიექტის) ინფორმირება. რეკომენდებულიa დროულად იქნეს მიღებული საფრთხეების/ზიანის შემაჩერებელი თუ შემამცირებელი ღონისძიებები, მაგალითად როგორიცაა მომხმარებლების ანგარიშების პაროლების განულება (reset).[69]

➪ დამატებით, იხ. პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია „ინციდენტთან დაკავშირებული ღონისძიებების განხორციელების თაობაზე“.

[68] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მუხლი 30.
[69] EDPB, Guidelines 9/2022 on personal data breach notification under GDPR ,Ver. 2.0, 28 March 2023, 32.

მესამე პირების ჩართულობა მონაცემთა დამუშავების პროცესში

ვებსაიტის მეშვეობით მონაცემთა დამუშავების პროცესში შესაძლოა ჩართული იყვნენ სხვა პირები, რომლებიც არ არიან დამუშავებისთვის პასუხისმგებელ პირთა დასაქმებულები. ასეთი შესაძლოა იყოს „ვებჰოსტინგის“, ასევე სასერვერო მომსახურების გამწევი კომპანიები, მარკეტინგული მომსახურების ორგანიზაციები და სხვა.

თუ დამუშავებისთვის პასუხიმგებელი პირის სახელით ან მისთვის ვებსაიტის მეშვეობით მოპოვებულ მონაცემთა დამუშავებას სხვა პირი უზრუნველყოფს, იგი დამუშავებაზე უფლებამოსილ პირს წარმოადგენს.

დამუშავებაზე უფლებამოსილმა პირმა მონაცემები შეიძლება დაამუშაოს მხოლოდ სამართლებრივი აქტის/დამუშავებისთვის პასუხისმგებელ პირთან დადებული წერილობითი შეთანხმების საფუძველზე[70], რომლითაც უნდა განისაზღვროს:

- ❑ მონაცემთა დამუშავების საფუძვლები და მიზნები;
- ❑ დასამუშავებელ მონაცემთა კატეგორიები;
- ❑ მონაცემთა დამუშავების ვადა;
- ❑ დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის უფლებები და ვალდებულებები.

ზემოხსენებული წერილობითი შეთანხმება **დამუშავებაზე უფლებამოსილი პირის** შემდეგ **ვალდებულებებს** უნდა ითვალისწინებდეს:

- ❑ დაამუშაოს მონაცემები მხოლოდ დამუშავებისთვის პასუხისმგებელი პირის წერილობითი დავალების ან მითითების შესაბამისად;
- ❑ უზრუნველყოს, რომ იმ ფიზიკურ პირს, რომელიც უშუალოდ მონაწილეობს მონაცემთა დამუშავებაში, ჰქონდეს კონფიდენციალურობის დაცვის ვალდებულება;
- ❑ უზრუნველყოს მონაცემთა უსაფრთხოება პერსონალურ მონაცემთა დაცვის შესახებ კანონის შესაბამისად;
- ❑ წაშალოს ან დამუშავებისთვის პასუხისმგებელ პირს გადასცეს მონაცემები შეთანხმების გაუქმების ან მოქმედების შეწყვეტის შემთხვევაში, აგრეთვე წაშალოს

[70] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მუხლი 36.

მათი ასლები, თუ მათი შენახვის ვალდებულება საქართველოს კანონმდებლობით არ არის დადგენილი;

❑ პერსონალურ მონაცემთა დაცვის შესახებ კანონით დადგენილ ვალდებულებებთან შესაბამისობის უზრუნველსაყოფად დამუშავებისთვის პასუხისმგებელ პირს მიაწოდოს სათანადო ინფორმაცია და ხელი შეუწყოს მის მიერ მონაცემთა დამუშავების მონიტორინგის განხორციელებას.

თავის მხრივ, **დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია** დამუშავებაზე უფლებამოსილ პირს წინასწარ მოსთხოვოს ინფორმაცია მონაცემთა კანონის შესაბამისად დამუშავების შესახებ და მონიტორინგი გაუწიოს დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავებას.

დამუშავებაზე უფლებამოსილმა პირმა შესაძლოა **თავისი უფლება-მოვალეობები სრულად/ნაწილობრივ გადასცეს სხვა პირს** მხოლოდ დამუშავებისთვის პასუხისმგებელი პირის წინასწარი წერილობითი თანხმობით, რაც მას არ ათავისუფლებს შესაბამისი ვალდებულებებისა და პასუხისმგებლობისგან.

დამუშავებაზე უფლებამოსილი პირი ვალდებულია მიიღოს სათანადო ორგანიზაციულ-ტექნიკური ზომები დამუშავებისთვის პასუხისმგებელ პირის მიერ მონაცემთა სუბიექტის უფლებების განხორციელებასთან დაკავშირებული ვალდებულებების შესრულებაში დასახმარებლად. ამასთან, მასთან დაცული ინფორმაციის ფარგლებში იგი ვალდებულია, უზრუნველყოს მონაცემთა სუბიექტის მოთხოვნის შესაბამისად, მისი უფლებების რეალიზება, მათ შორის, მიიღოს ყველა ზომა ამავე კანონის მოთხოვნებთან შესაბამისობის და, საჭიროების შემთხვევაში, მათი დემონსტრირების მიზნით.[71]

➪ დამატებით, იხ. პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია „დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებული ხელშეკრულების არსებითი და სტანდარტული პირობების შესახებ“.

მონაცემთა საერთაშორისო გადაცემა

მონაცემთა საერთაშორისო გადაცემის ზუსტ განმარტებას კანონმდებლობა არ იძლევა, თუმცა აღნიშნულში მოიაზრება ის შემთხვევები, როდესაც საქართველოს ტერიტორიიდან მონაცემები გადაეცემა უცხო ქვეყნის ტერიტორიაზე რეგისტრირებულ ორგანიზაციას, სხვა სახელმწიფოს და საერთაშორისო ორგანიზაციას. მონაცემთა დაცვის ევროპულმა საბჭომ განსაზღვრა სამი კუმულატიური კრიტერიუმი, რომლის შესაბამისადაც პროცესი საერთაშორისო გადაცემად იქნება მიჩნეული, კერძოდ:

[71] იქვე, მუხლი 23, პუნქტი 1.

- ✓ მონაცემთა გადამცემი დაწესებულების მიერ მონაცემთა დამუშავებაზე უნდა ვრცელდებოდეს “GDPR”;
- ✓ გადამცემი დაწესებულება გადაცემით ან სხვა გზით პერსონალურ მონაცემებს ხელმისაწვდომს უნდა ხდიდეს მონაცემთა მიმღებისთვის, იქნება ეს დამუშავებისთვის პასუხისმგებელი/თანადამუშავებისთვის პასუხისმგებელი თუ დამუშავებაზე უფლებამოსილი პირი;
- ✓ მონაცემთა მიმღები პირი უნდა იმყოფებოდეს უცხო ქვეყანაში ან იყოს საერთაშორისო ორგანიზაცია.[72]

საქართველოს კანონმდებლობით მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვებია, თუ არსებობს მონაცემთა დამუშავების კანონით გათვალისწინებული მოთხოვნები და შესაბამის სახელმწიფოში/საერთაშორისო ორგანიზაციაში უზრუნველყოფილია მონაცემთა დაცვისა და მონაცემთა სუბიექტის უფლებების დაცვის სათანადო გარანტიები.

სხვა სახელმწიფოში ან/და საერთაშორისო ორგანიზაციაში მონაცემთა დაცვის სათანადო გარანტიების არსებობას აფასებს პერსონალურ მონაცემთა დაცვის სამსახური, ხოლო იმ სახელმწიფოებისა და საერთაშორისო ორგანიზაციების ნუსხა, რომლებშიც უზრუნველყოფილია მონაცემთა დაცვის სათანადო გარანტიები, განისაზღვრება პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტით[73].

თუ ქვეყანა, სადაც ვებსაიტის მეშვეობით ხდება მონაცემთა გადაცემა არ წარმოადგენს სათანადო გარანტიების მქონე ნუსხით გათვალისწინებულ ერთ-ერთ სახელმწიფოს, მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვები იქნება თუ:

- ✓ მონაცემთა გადაცემა გათვალისწინებულია საქართველოს საერთაშორისო ხელშეკრულებითა და შეთანხმებით;
- ✓ დამუშავებისთვის პასუხისმგებელი პირი უზრუნველყოფს მონაცემთა დაცვის სათანადო გარანტიებს დამუშავებისთვის პასუხისმგებელ პირსა და შესაბამის სახელმწიფოს, ასეთი სახელმწიფოს სათანადო საჯარო დაწესებულებას, იურიდიულ პირს ან ფიზიკურ პირს ან საერთაშორისო ორგანიზაციას შორის დადებული ხელშეკრულებით, რომელთან

[72] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Ver. 2.0, 14 February 2023, §9.

[73] იხ. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის ბრძანება №23 „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“.

დაკავშირებითაც მოიპოვებს პერსონალურ მონაცემთა დაცვის სამსახურის ნებართვას საერთაშორისო გადაცემაზე.[74]

- ✓ შესაბამის სახელმწიფოში მონაცემთა დაცვის სათანადო გარანტიების არარსებობისა და შესაძლო საფრთხეების შესახებ ინფორმაციის მიღების შემდეგ მონაცემთა სუბიექტი განაცხადებს წერილობით თანხმობას.
- ✓ მონაცემთა გადაცემა აუცილებელია მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად და მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად უნარი არა აქვს, მონაცემთა დამუშავებაზე თანხმობა განაცხადოს;
- ✓ მონაცემთა გადაცემა გათვალისწინებულია საქართველოს სისხლის სამართლის საპროცესო კოდექსით (საგამოძიებო მოქმედების განხორციელების მიზნით), „უცხოელთა და მოქალაქეობის არმქონე პირთა სამართლებრივი მდგომარეობის შესახებ“ საქართველოს კანონით, „სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის შესახებ“ საქართველოს კანონით, „სამართალდაცვით სფეროში საერთაშორისო თანამშრომლობის შესახებ“ საქართველოს კანონით, „საქართველოს ეროვნული ბანკის შესახებ“ საქართველოს ორგანული კანონის ან „ფულის გათეთრებისა და ტერორიზმის დაფინანსების აღკვეთის ხელშეწყობის შესახებ“ საქართველოს კანონის საფუძველზე მიღებული ნორმატიული აქტით;
- ✓ არსებობს კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესი (მათ შორის, დანაშაულის თავიდან აცილება, გამოძიება, გამოვლენა და სისხლისსამართლებრივი დევნა, სასჯელის აღსრულება და ოპერატიულ-სამძებრო ღონისძიებების განხორციელება) და მონაცემთა გადაცემა აუცილებელი და პროპორციული ზომაა დემოკრატიულ საზოგადოებაში.

ჯ გაითვალისწინეთ:

მონაცემთა სუბიექტის თანხმობა, როგორც საერთაშორისო გადაცემის წინაპირობა საგამონაკლისო შემთხვევას წარმოადგენს, რომელიც მხოლოდ სპეციფიურ გარემოებებში შეიძლება იქნეს გამოყენებული, თუ სათანადო გარანტიების არსებობა შესაბამის ქვეყანაში ან მისი უზრუნველყოფა ორგანიზაციებს შორის გაფორმებული შესაბამისი შეთანხმებით გამორიცხულია.[75]

[74] იხ. პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 1 მარტის ბრძანება №33 „პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე ნებართვის გაცემის წესის და პერსონალურ მონაცემთა სხვა სახელმწიფოს ან/და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე განაცხადის ფორმის დამტკიცების შესახებ”.

[75] EDPB, Data Protection Guide For Small Businesses, International Data Transfers - Data transfers on the Basis of Derogations, <https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en#toc-6>. ასევე GDPR, Article 49.

მონაცემთა საერთაშორისო გადაცემის წინაპირობებთან ერთად, აუცილებელია არსებობდეს დამუშავების შესაბამისი სამართლებრივი საფუძველი, დაცულ იქნეს თითოეული პრინციპი და მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული სხვა ვალდებულებები.

მონაცემთა დაცვაზე ზეგავლენის შეფასება პერსონალური მონაცემების დამუშავების პროცესში ერთ-ერთი მნიშვნელოვანი გზაა, იმისათვის რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა სისტემურად და ყოვლისმომცველად გააანალიზოს მონაცემთა დამუშავების პროცესი, რომლის ფარგლებში მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე, ასევე, მოახდინოს აღნიშნული რისკების იდენტიფიცირება, შეფასება, პროაქტიულად გათვალისწინება, მიიღოს სათანადო ზომები მათი შემცირებისათვის, უზრუნველყოს კანონიერი და სამართლიანი გადაწყვეტილების მიღება მონაცემთა დამუშავების პროცესის დაწყების თაობაზე, ასევე დამუშავების გამჭვირვალობა, ყველა დაინტერესებული პირის ჩართვა აღნიშნულ პროცესში და კანონის 26-ე მუხლით გათვალისწინებულ ვალდებულებებთან[76] შესაბამისობა.

↳ გაითვალისწინეთ:

[76] იხ, ქვეთავი „მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას“.

თუ მონაცემთა დამუშავებისას *ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით,* მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია წინასწარ განახორციელოს მონაცემთა დაცვაზე ზეგავლენის შეფასება.[77]

ზემოხსენებული საფრთხის **მაღალი ალბათობის დასადგენად** აუცილებელია ქვემოთ ჩამოთვლილთაგან სულ მცირე ორი გარემოების ერთდროულად არსებობა:

❑პროფაილინგი, რომლის შედეგების გათვალისწინებაც ხდება ისეთი გადაწყვეტილების მიღებისას, რომელიც სამართლებრივ შედეგს წარმოშობს მონაცემთა სუბიექტის მიმართ, ან ასეთი გადაწყვეტილება ეხება მონაცემთა სუბიექტისთვის პროდუქტის ან მომსახურების შეთავაზებას, გარკვეული სარგებლის მიღებას, დასაქმებულთა მიერ შესრულებული სამუშაოს ხარისხის შეფასებას ან ადამიანური რესურსების მართვასთან დაკავშირებულ სხვა აქტივობებს, გარკვეულ ადგილებზე ფიზიკურ წვდომას ან გადაადგილებას;

❑მონაცემთა სუბიექტების ქცევის ან მდგომარეობის (მათ შორის, ფიზიკური/ჯანმრთელობის მდგომარეობის) სისტემატური და მასშტაბური მონიტორინგი ელექტრონული სისტემის/ტექნოლოგიის მეშვეობით, ან როცა ასეთი მონიტორინგი მიმდინარეობს დასაქმებულთა მიმართ;

❑ელექტრონული სისტემის გამოყენება, რომელიც მიზნად ისახავს მომხმარებლისათვის პროდუქტის ან მომსახურების შეთავაზებას ან/და მიწოდებას და რომლის მეშვეობითაც მუშავდება მომხმარებლის ფინანსური მონაცემები ან/და რეალურ დროში მომხმარებელთა ადგილსამყოფლის შესახებ მონაცემები;

❑ახალი ტექნოლოგიის დანერგვა ან ინოვაციური გამოყენება;

❑იმ მონაცემთა ბაზების შედარება ან გაერთიანება, რომელიც წარმოიქმნება ორი ან მეტი სხვადასხვა მონაცემთა დამუშავების პროცესიდან, სხვადასხვა მიზნისთვის ან/და სხვადასხვა დამუშავებისთვის პასუხიმგებელი პირის მიერ;

❑მონაცემთა დამუშავება, რომელსაც შედეგად შესაძლოა მოჰყვეს მონაცემთა სუბიექტის დისკრიმინაცია;

❑მონაცემთა დამუშავება, რომელსაც შედეგად შესაძლოა მოჰყვეს უარი პროდუქტის/მომსახურების შეთავაზებაზე ან მონაცემთა სუბიექტის უფლების შეზღუდვა;

[77] "პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, მუხლი 31.

❑მუშავდება დამუშავებისთვის პასუხისმგებელი პირის თანამშრომლების, სამედიცინო დაწესებულების პაციენტების, არასრულწლოვნების, შეზღუდული შესაძლებლობისა და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე პირების მონაცემები.

მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელება ასევე, სავალდებულოა, თუ დამუშავებისთვის პასუხისმგებელი პირი:

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

ზეგავლენის შეფასების პროცესში ჩართული პირ(ებ)ი	სავალდებულოა	ნებაყოფლობითია
პროდუქტის/მომსახურების შექმნასა თუ ბანახღებაზე პასუხისმგებელი პირი	✓ *არსებობის შემთხვევაში	
პერსონალურ მონაცემთა დაცვის ოფიცერი	✓ *არსებობის შემთხვევაში	
ინფორმაციულ უსაფრთხოებაზე პასუხისმგებელი პირი	✓ *არსებობის შემთხვევაში	
საინფორმაციო ტექნოლოგიებზე პასუხისმგებელი პირი	✓ *არსებობის შემთხვევაში	
ექსპერტი		✓
მონაცემთა სუბიექტები/მათი წარმომადგენლები		✓
სხვა პირი, რომლის მონაწილეობა მნიშვნელოვანია ზეგავლენის შეფასების პროცესში		✓
პერსონალურ მონაცემთა დაცვის სამსახური	✓ *მაღალი საფრთის არსებობის შემთხვევაში	

მონაცემთა დაცვაზე ზეგავლენის შეფასების შედეგად ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის მაღალი საფრთხის გამოვლენის შემთხვევაში დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია:

- მიიღოს ყველა აუცილებელი ზომა საფრთხეების არსებითად შესამცირებლად;
- კონსულტაციის მიზნით მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს. თუ დამატებითი ორგანიზაციულ-ტექნიკური ზომებით შეუძლებელია ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის არსებითად შემცირება, მონაცემთა დამუშავება არ უნდა განხორციელდეს.

თუ დამატებითი ორგანიზაციულ-ტექნიკური ზომებით შეუძლებელია საფრთხის არსებითად შემცირება, მონაცემები არ უნდა დამუშავდეს.
მონაცემთა დაცვაზე ზეგავლენის შეფასება პირმა შესაძლოა, ასევე, ნებაყოფლობით განახორციელოს, რაც მას დამუშავების პროცესში სავარაუდო საფრთხეების იდენტიფიცირებასა და დროულ პრევენციაში დაეხმარება.

↳ გაითვალისწინეთ:

ზეგავლენის პროცესი მუდმივ მეთვალყურეობას საჭიროებს და დროთა განმავლობაში შესაძლოა აუცილებელი გახდეს ზეგავლენის შეფასების არსებული დოკუმენტის გადასინჯვა.

➪ დამატებით, იხ. პერსონალურ მონაცემთა დაცვის სამსახურის სახელმძღვანელო რეკომენდაცია „მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) შესახებ“.

➪ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21.

მონაცემთა სუბიექტის უფლებები

მონაცემთა დამუშავების თითოეულ პროცესში აუცილებელია უზრუნველყოფილ იქნეს მონაცემთა სუბიექტის უფლებები და მათი რეალიზაციის ქმედითი საშუალებები. ვებსაიტის მეშვეობით მონაცემთა შეგროვებისას მნიშვნელოვანია ციფრული სამყაროს მახასიათებლების გათვალისწინება და აღნიშნულზე მორგებული მექანიზმების შემუშავება. მაგალითად, იმ შემთხვევაში თუ ვებსაიტის მეშვეობით ხდება მომხმარებლის რეგისტრირება, ანგარიშის შექმნა და ამ გზით ხდება მონაცემების დამუშავება - კონფიდენციალურობის პარამეტრების განსაზღვრით, რომლის ცვლილება თუ შესაბამისი მოთხოვნის გაგზავნა მარტივად იქნება შესაძლებელი ვებსაიტის მეშვეობით. თუ ანგარიშის შექმნა არ ხდება, თუმცა

სუბიექტის ინფორმაცია ვებსაიტზე სხვაგვარად მუშავდება, შესაძლოა მონაცემთა დაცვის პოლიტიკის დოკუმენტში, საკონტაქტო ინფორმაციის ველში მიეთითოს შესაბამისი ელექტრონული ფოსტის მისამართი, სადაც მონაცემთა სუბიექტი მოთხოვნას გააგზავნის. ასევე, შესაძლოა ვებსაიტის შესაბამისი გვერდი ინტეგრირდეს, რომლის მეშვეობითაც, ვებფორმის შევსებით სუბიექტს თავისი უფლებების განხორციელების შესაძლებლობა - შესაბამისი მოთხოვნის გაგზავნა შეეძლება. ინტერნეტში არსებული რისკების გათვალისწინებით აუცილებელია არსებობდეს ვერიფიკაციის შესაბამისი მექანიზმი, რომლის მეშვეობითაც მოხდება სუბიექტის იდენტიფიცირება და მოთხოვნის ნამდვილობის დადასტურება.

მონაცემთა სუბიექტს შემდეგი უფლებები გააჩნია:

მონაცემებზე წვდომის უფლება[78]

პირს, რომლის შესახებ ინფორმაციაც მუშავდება უფლება აქვს მიიღოს ინფორმაცია მონაცემთა დამუშავების შესახებ, გაეცნოს მის შესახებ არსებულ პერსონალურ მონაცემებს და უსასყიდლოდ მიიღოს ამ მონაცემების ასლები.
სუბიექტმა, მოთხოვნის შემთხვევაში, უსასყიდლოდ უნდა მიიღოს ინფორმაცია:

- ✓ მისი მონაცემის თაობაზე, რომელიც მუშავდება, ასევე მათი დამუშავების საფუძვლისა და მიზნის შესახებ;
- ✓ მონაცემთა შეგროვების/მოპოვების წყაროს შესახებ;
- ✓ მონაცემთა შენახვის ვადის (დროის) შესახებ. თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, ვადის განსაზღვრის კრიტერიუმების თაობაზე;
- ✓ მონაცემთა სუბიექტის უფლებების შესახებ;
- ✓ მონაცემთა გადაცემის სამართლებრივი საფუძვლისა და მიზნების, მონაცემთა დაცვის სათანადო გარანტიების შესახებ - თუ მონაცემები გადაეცემა სხვა სახელმწიფოს ან საერთაშორისო ორგანიზაციას;
- ✓ მონაცემთა მიმღების ვინაობის ან მონაცემთა მიმღებების კატეგორიების შესახებ. ინფორმაცია მონაცემთა გადაცემის საფუძვლისა და მიზნის თაობაზე, თუ მონაცემები მესამე პირს გადაეცემა;
- ✓ ავტომატიზებული დამუშავების, (მაგალითად, პროფაილინგის) შედეგად მიღებული გადაწყვეტილების, ასევე ლოგიკის შესახებ, რომელიც გამოიყენება ამგვარი გადაწყვეტილების მისაღებად, აგრეთვე მონაცემთა დამუშავებაზე მისი გავლენისა და დამუშავების მოსალოდნელი/ სავარაუდო შედეგის თაობაზე.

[78] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მუხლები 13 და 14.

↳ გაითვალისწინეთ:

სუბიექტმა აღნიშნული ინფორმაცია, ასევე მოთხოვნის შემთხვევაში, შესაბამისი ასლები უნდა მიიღოს **მოთხოვნიდან არაუგვიანეს 10 სამუშაო დღისა.**

ეს ვადა განსაკუთრებულ შემთხვევებში და სათანადო დასაბუთებით შეიძლება გაგრძელდეს არაუმეტეს 10 სამუშაო დღით, რის შესახებაც მონაცემთა სუბიექტს დაუყოვნებლივ უნდა ეცნობოს.

რეკომენდებულია ვებსაიტის მომხმარებლის (ასეთს არსებობის შემთხვევაში) პარამეტრის შემუშავება, რომელიც აღნიშნული ინფორმაციის მიღებასა და ჩამოტვირთვას უზრუნველყოფს.

მონაცემთა წაშლის უფლება[79]

მონაცემთა სუბიექტს უფლება აქვს მოითხოვოს მის შესახებ მონაცემთა დამუშავების შეწყვეტა, წაშლა ან განადგურება.

მონაცემთა სუბიექტს უფლება აქვს, მის შესახებ მონაცემთა საჯაროდ ხელმისაწვდომი ფორმით დამუშავების შემთხვევაში, დამატებით მოითხოვოს მონაცემთა ხელმისაწვდომობის შეზღუდვა ან/და მონაცემთა ასლების ან მონაცემებთან დამაკავშირებელი **ნებისმიერი ინტერნეტბმულის წაშლა.**

↳ გაითვალისწინეთ:

მოთხოვნიდან არაუგვიანეს 10 სამუშაო დღისა უნდა შეწყდეს მონაცემთა დამუშავება/მონაცემები უნდა წაიშალოს ან განადგურდეს ან მონაცემთა სუბიექტს უნდა ეცნობოს მოთხოვნაზე უარის თქმის საფუძველი (ასეთის არსებობისას) და განემარტოს უარის გასაჩივრების წესი.

დამუშავების **შეწყვეტის, წაშლის ან განადგურების შესახებ ინფორმაცია** სუბიექტს უნდა მიეწოდოს შესაბამისი მოქმედების განხორციელებისთანავე, არაუგვიანეს 10 სამუშაო დღისა.

შესაძლებელია მომხმარებლის პროფილი შეიცავდეს იმგვარ ფუნქციონალს, რომელიც უზრუნველყოფს სუბიექტის მიერ შესაბამისი პარამეტრების მეშვეობით მისი ინფორმაციის წაშლას, აღნიშნულის თაობაზე შესაბამისი პირების (მაგალითად, დამუშავებაზე უფლებამოსილი პირის) ავტომატურ ინფორმირებას.

მონაცემთა დაბლოკვის უფლება[80]

მონაცემთა სუბიექტს უფლება აქვს მოითხოვოს მონაცემთა დაბლოკვა, თუ:

❑იგი სადავოს ხდის მონაცემების ნამდვილობას/სიზუსტეს;

[79] იქვე, მუხლი 16.
[80] იქვე, მუხლი 17.

❑მონაცემთა დამუშავება უკანონოა, თუმცა მონაცემთა სუბიექტი ეწინააღმდეგება მათ წაშლას და ითხოვს მონაცემთა დაბლოკვას;

❑მონაცემები საჭირო აღარ არის მათი დამუშავების მიზნის მისაღწევად, თუმცა მონაცემთა სუბიექტს ისინი სჭირდება საჩივრის/სარჩელის წარსადგენად;

❑იგი მოითხოვს მონაცემთა დამუშავების შეწყვეტას, წაშლას ან განადგურებას და მიმდინარეობს ამ მოთხოვნის განხილვა;

ვებსაიტის ადმინისტრატორებს უნდა ჰქონდეთ ტექნიკურად შესაძლებლობა, რომ მოთხოვნის შემთხვევაში უზრუნველყონ ინფორმაციის დაბლოკვა, იმგვარად რომ ისინი არ დამუშავდეს შესაბამისი ვადის განმავლობაში.

თანხმობის ბათოხმობის უფლება[81]

მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, ყოველგვარი განმარტების/დასაბუთების გარეშე გამოიხმოს მის მიერ გაცემული თანხმობა. მას უნდა ჰქონდეს შესაძლებლობა თანხმობა გამოიხმოს იმავე ფორმით, რომლითაც იგი განაცხადა, ხოლო გამოხმობამდე უფლება აქვს, მიიღოს ინფორმაცია გამოხმობის შესაძლო შედეგების შესახებ.

↳ გაითვალისწინეთ:

სუბიექტის მოთხოვნის შესაბამისად, მონაცემთა დამუშავება უნდა შეწყდეს ან/და დამუშავებული მონაცემები წაიშალოს ან განადგურდეს მოთხოვნიდან არაუგვიანეს 10 სამუშაო დღისა, *თუ მონაცემთა დამუშავების სხვა საფუძველი არ არსებობს.*

მონაცემთა ბასწორების უფლება[82]

მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს მის შესახებ მცდარი, არაზუსტი ან/დაარასრული მონაცემებისგასწორება, განახლება ან/და შევსება.

↳ გაითვალისწინეთ:

მოთხოვნის წარდგენიდან არაუგვიანეს 10 სამუშაო დღისა, მონაცემები უნდა გასწორდეს, განახლდეს ან/და შეივსოს ან მონაცემთა სუბიექტს ეცნობოს მოთხოვნაზე უარის თქმის საფუძველი და განემარტოს უარის გასაჩივრების წესი.

მომხმარებელს, მაგალითად ანგარიშის არსებობის შემთხვევაში, უნდა შეეძლოს მონაცემების მოდიფიკაცია შესაბამისი პარამეტრების მეშვეობით.

[81] იქვე, მუხლი 20.
[82] იქვე, მუხლი 15.

მონაცემთა გადატანის უფლება[83]

მე-5 მუხლის პირველი პუნქტის „ა“ (სუბიექტის თანხმობა) და „ბ“ (გარიგებით ნაკისრი ვალდებულებების შესასრულებლად/გარიგების დასადებად) ქვეპუნქტებითა და მე-6 მუხლის პირველი პუნქტის „ა“ (სუბიექტის წერილობითი თანხმობა) ქვეპუნქტით გათვალისწინებული საფუძვლებით მონაცემთა ავტომატური დამუშავების[84] შემთხვევაში, თუ ეს ტექნიკურად შესაძლებელია, მონაცემთა სუბიექტს უფლება აქვს მიიღოს მის მიერ მიწოდებული მონაცემები ან მოითხოვოს მათი სხვა დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემა:

- ✓ სტრუქტურიზებული,
- ✓ საზოგადოდ გამოყენებადი,
- ✓ მანქანურად წაკითხვადი ფორმატით.

ვებსაიტის მომხმარებლის კონფიდენციალურობის პარამეტრი შესაძლოა ითვალისწინებდეს მონაცემთა ჩამოტვირთვის ფუნქციონალს, სტრუქტურიზებული, მანქანურად წაკითხვადი (CSV, XML, JSON და სხვა) და საზოგადოდ ხელმისაწვდომი ფორმატით.[85]

შესაბამისად, ვებსაიტის შექმნისას მონაცემთა დაცვასთან დაკავშირებული ვალდებულებები, აღნიშნულ პროცესში გასათვალისწინებელი საკითხები საკმაოდ ფართოა და ინდივიდუალურ მიდგომას საჭიროებს, მათ შორის უშუალოდ ვებსაიტის დანიშნულებიდან გამომდინარე. წინამდებარე რეკომენდაციებში განხილული საკითხები მნიშვნელოვანია როგორც მომხმარებლების უფლებების დაცვის კუთხით, ასევე უშუალოდ ვებსაიტის შემქმნელთა თუ მფლობელთა მიერ კანონშესაბამისობის უზრუნველსაყოფად, პროცესის გამართულად წარმართვის დემონსტრირებისთვის, რაც ემსახურება არამხოლოდ ანგარიშვალდებულების პრინციპს, არამედ პოზიტიურად მოქმედებს შესაბამისი ორგანიზაციის იმიჯზე.

[83] იქვე, მუხლი 18.

[84] მონაცემთა დამუშავება ინფორმაციული ტექნოლოგიების გამოყენებით.

[85] Commission nationale de l'informatique et des libertés (CNIL), Developer's Guide - Sheet n°13: Prepare for the exercise of people's rights, 2020, <https://www.cnil.fr/en/sheet-ndeg13-prepare-exercise-peoples-rights> [7.9.2025].

ᲕᲔᲠᲡᲝᲜᲐᲚᲣᲠ ᲛᲝᲜᲐᲪᲔᲛᲗᲐ ᲓᲐᲪᲕᲘᲡ ᲡᲐᲛᲡᲐᲮᲣᲠᲘ
2025