პერსონალურ მონაცემთა
დაცვის სამსახური

რეკომენდაციები მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) შესახებ

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

რეკომენდაციები
მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) შესახებ

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

გამოყენებული აბრევიატურები და შემოკლებები:

AFR - სახის ავტომატური ამომცნობი;

AI - ხელოვნური ინტელექტი;

AZR - უცხოელთა ცენტრალური რეესტრი;

CJEU - ევროკავშირის მართლმსაჯულების სასამართლო;

DPIA - მონაცემთა დაცვაზე ზეგავლენის შეფასება;

GDPR - მონაცემთა დაცვის ძირითადი რეგულაცია.

შინაარსი

[1] დოკუმენტის სარეკომენდაციო ფორმა (ნიმუში) დანართის სახით ერთვის წინამდებარე რეკომენდაციებს.

შესავალი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონი (14/06/2023; №3144-XIმს-Xმპ) (შემდგომ - კანონი) ადგენს დამუშავებისთვის პასუხისმგებელ პირთა ვალდებულებებს, რომელთა შორის ერთ-ერთი მნიშვნელოვანი ადგილი მონაცემთა დაცვაზე ზეგავლენის შეფასებას (შემდგომ - ზეგავლენის შეფასება)[2] უკავია. კანონი განსაზღვრავს ზეგავლენის შეფასების წარმოების ძირითად წესებსა და ვალდებულების წარმომშობ გარემოებებს, ხოლო ამ გარემოებათა დადგენის კრიტერიუმები და შეფასების განხორციელების წესი პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტითაა[3] დადგენილი.

წინამდებარე დოკუმენტი მიზნად ისახავს, ზეგავლენის შეფასების პროცესის, როგორც დამუშავებისთვის პასუხისმგებელი პირისთვის ახალი კანონით დაკისრებული ვალდებულების გაანალიზებას და პრაქტიკული განხორციელების ხელშეწყობას.

წინამდებარე რეკომენდაციები მომზადებულია კანონისა და პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“ ნორმატიული შინაარსისა და საუკეთესო ევროპული გამოცდილების ანალიზის საფუძველზე.

ტექსტში გამოყენებულ ტერმინებს აქვთ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრული მნიშვნელობა.

[2] იხ. პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) 31-ე მუხლი.

[3] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“ - https://matsne.gov.ge/ka/document/view/6118123?publication=0

1. ზეგავლენის შეფასების ინსტიტუციური შინაარსი

1.1 ზეგავლენის შეფასების ცნება ევროპის კავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მიხედვით

თანამედროვე სამყაროში, სწრაფად განვითარებად ციფრულ ეპოქაში, სხვადასხვა ტექნოლოგიების გამოყენებით პერსონალურ მონაცემთა დამუშავება[4] სულ უფრო და უფრო კომპლექსური ხდება. აღნიშნულიდან გამომდინარე, არსებობს რისკი, რომ ამ პროცესმა ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის მომეტებული საფრთხე შექმნას.

მონაცემთა დაცვის ძირითადი რეგულაციის (შემდგომ - GDPR) 35-ე მუხლის შესაბამისად,[5] ზეგავლენის შეფასება პროცესია, რომელიც აღწერს დამუშავების მიმდინარეობას მისი აუცილებლობისა და პროპორციულობის შესაფასებლად[6]. აღნიშნული ხელს უწყობს: მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობას, მის დემონსტრირებას და შესაძლო სანქციებისგან თავის არიდებას; მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის სანდოობის განმტკიცებას საზოგადოებაში, მონაცემთა სუბიექტების დარწმუნებას, რომ მათი უფლებები არ ილახება დამუშავებისთვის პასუხისმგებელი პირის მიერ, „მონაცემთა მეტად დაფარვის პრიორიტეტის“ პრინციპის დანერგვას ახალი პროდუქტის ან მომსახურების შექმნისას; ხარჯების შემცირებას და მონაცემთა არამიზნობრივი შეგროვებისა და დამუშავების შემთხვევების აღმოფხვრას; მონაცემთა დაცვასთან დაკავშირებული რისკებისა და უსაფრთხოების თვალსაზრისით მიღებული ორგანიზაციულ-ტექნიკური ზომების ხარჯების შემცირებას.[7]

GDPR განსაზღვრავს იმ უფლებებს, რომელთა დარღვევის მაღალი რისკის არსებობა ქმნის ზეგავლენის შეფასების მექანიზმის გამოყენების წინაპირობას. მონაცემთა დაცვის ძირითადი რეგულაციის 35-ე მუხლი მოიცავს ისეთ შემთხვევებს, როდესაც ივარაუდება, რომ უახლესი ტექნოლოგიების გამოყენებით მონაცემთა კონკრეტული ტიპის დამუშავება, დამუშავების ხასიათის, მოცულობის, კონტექსტისა და მიზნების

[4] იხ. პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) მე-3 მუხლის „ვ“ ქვეპუნქტი.

[5] https://gdpr-info.eu/art-35-gdpr/;

[6] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 4.

[7] Data Protection Commission, Guide to Data Protection Impact Assessment (DPIAs), October 2019.

გათვალისწინებით, იწვევს მონაცემთა სუბიექტის ისეთი უფლებებისა და თავისუფლებების დარღვევის მაღალ რისკებს, როგორებიცაა მონაცემთა დაცვისა და კონფიდენციალურობის უფლება, აზრისა და მისი გამოხატვის თავისუფლება, მიმოსვლის თავისუფლება, დისკრიმინაციის აკრძალვა და სინდისისა და რელიგიის თავისუფლება.[8]

„პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების პერსონალური მონაცემების დაცვის შესახებ“ ევროპის საბჭოს მოდერნიზებული 108-ე კონვენციის[9] მე-10 მუხლის მე-2 პუნქტის თანახმად, ხელშემკვრელ მხარეებს მოეთხოვებათ, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა/დამუშავებაზე უფლებამოსილმა პირმა შეაფასონ შესაძლო რისკები, რომლებსაც მონაცემთა დამუშავება უქმნის მონაცემთა სუბიექტის უფლებებსა და ფუნდამენტურ თავისუფლებებს. ასეთი შეფასება დამუშავების დაწყებამდე უნდა განხორციელდეს, ხოლო შეფასების შემდეგ შემუშავდეს ისეთი მოდელი, რომლითაც შესაძლებელი იქნება დამუშავებასთან დაკავშირებული რისკების პრევენცია ან მინიმუმამდე შემცირება. [10]

1.2 ეროვნული მარეგულირებელი ჩარჩო

პერსონალურ მონაცემთა დაცვის სფეროში არსებული კანონმდებლობის ევროპულ სტანდარტებთან დაახლოების, საქართველოს მიერ საერთაშორისო ვალდებულებების შესრულებისა და საერთაშორისოდ აღიარებული პრინციპების დამკვიდრების, აგრეთვე, საჯარო და კერძო დაწესებულებებსა და სამართალდამცავ ორგანოებში არსებული გამოწვევების საპასუხოდ, 2023 წლის 14 ივნისს მიღებულ იქნა კანონი, რომელიც ახლებურად განსაზღვრავს პერსონალური მონაცემების დაცვის სამართლებრივ გარანტიებს, წესებს და, სხვა საკითხებთან ერთად, ითვალისწინებს **მონაცემთა დაცვაზე ზეგავლენის შეფასებას**, რაც პერსონალურ მონაცემთა დაცვის ქართული კანონმდებლობისთვის სიახლეს წარმოადგენს და მიზნად ისახავს ადამიანის უფლებების დარღვევის მომეტებული საფრთხეების შემცირებას.

---

[8] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 6.

[9]https://search.coe.int/cm#{%22CoEObjectId%22:[%2209000016807c65bf%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} [ვიზიტის დრო: 25.05.2024].

[10] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018, 204.

კანონის 31-ე მუხლის პირველი პუნქტის თანახმად, თუ მონაცემთა დამუშავებისას ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია წინასწარ განახორციელოს მონაცემთა დაცვაზე ზეგავლენის შეფასება.

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია დამუშავების დაწყებამდე შეაფასოს მისი შესაძლო გავლენა მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებზე, რაც ხელს შეუწყობს საფრთხეების სათანადოდ გამოვლენას, მათზე რეაგირებასა და მათ შემცირებას. ზეგავლენის შეფასება არის არაერთჯერადი ხასიათის, მიმდინარე პროცესი, განსაკუთრებით მაშინ, როდესაც მონაცემთა დამუშავებისკენ მიმართული ღონისძიება დინამიკურია და ხასიათდება პერიოდული ცვლილებით.[11] რისკების შეფასება უნდა მოიცავდეს უსაფრთხოების ღონისძიებათა დაგეგმვას გამოვლენილ საფრთხეებზე რეაგირების მიზნით[12]. თუ დადგინდება, რომ მიღებული ორგანიზაციულ-ტექნიკური ზომებით შეუძლებელია ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის არსებითად შემცირება, მონაცემთა დამუშავება არ უნდა განხორციელდეს[13].

ზეგავლენის შეფასების მიზანია:

- მონაცემთა დამუშავების საწყის ეტაპზე მონაცემთა მიმართ არსებული საფრთხეების პროაქტიულად გათვალისწინება;
- მონაცემთა დამუშავების შედეგად, ადამიანის ძირითადი უფლებებისა და თავისუფლებების მიმართ წარმოშობილი საფრთხეების იდენტიფიცირება, შეფასება და არსებითად შემცირება;
- კანონიერი და სამართლიანი გადაწყვეტილების მიღება მონაცემთა დამუშავების პროცესის დაწყების თაობაზე;

[11] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "likely to Result in a High Risk" for the Purposes of Regulation 2016/679, 2017, p. 14.

[12] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018, 205.

[13] იხ. პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) 31-ე მუხლის მე-5 პუნქტი.

- ყველა დაინტერესებული პირის ჩართვა მონაცემთა დამუშავების დაგეგმვის პროცესში;
- მონაცემთა დამუშავების გამჭვირვალობა;
- კანონის 26-ე მუხლით გათვალისწინებულ ვალდებულებებთან შესაბამისობა რაც გულისხმობს მონაცემთა მეტად დაფარვის პრიორიტეტის, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდის, გამოყენებას ახალი პროდუქტის ან მომსახურების შექმნისას.[14]

ამასთან, ზეგავლენის შეფასების პროცესში აუცილებელია პერსონალურ მონაცემთა დაცვის ოფიცრის (ასეთის არსებობის შემთხვევაში) მონაწილეობა. ასევე, რეკომენდებულია, ექსპერტებისა და დაინტერესებული მხარეების ჩართულობა. გარდა ამისა, სასურველია, ზეგავლენის შეფასების პროცესში მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა კონსულტაცია გაიაროს მონაცემთა სუბიექტებთან ან მათ წარმომადგენლებთან,[15] ხოლო კანონით განსაზღვრულ შემთხვევაში, პერსონალურ მონაცემთა დაცვის სამსახურთან.[16]

შეჯამების სახით შეიძლება ითქვას, რომ ზეგავლენის შეფასება აღქმულ უნდა იქნას როგორც მექანიზმი, რომელიც მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა დამუშავების შესახებ გადაწყვეტილების მიღებაში დაეხმარება და შესაძლებლობას მისცემს, სწორად განსაზღვროს, კონკრეტული მიზნის მისაღწევად, დამუშავების ამა თუ იმ სახის გამოყენება ნამდვილად არის თუ არა მონაცემთა დამუშავებისთვის საჭირო და ადეკვატური საშუალება.[17]

[14] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“.

[15] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is “likely to Result in a High Risk” for the Purposes of Regulation 2016/679, 2017, p. 14.

[16] იხ. პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) 31-ე მუხლის მე-5 და მე-5 პუნქტები და პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“.

[17] Information Commissioner’s Office (ICO), UK, Additional considerations for technologies other than CCTV, October 2022, p. 36.

2. ზეგავლენის შეფასების საჭიროების იდენტიფიცირება

2.1 ზეგავლენის შეფასების განხორციელების მავალდებულებელი გარემოებები

ზეგავლენის შეფასებისთვის კანონით დადგენილი მავალდებულებელი გარემოებების ანალიზით ვიღებთ ერთგვარ ტესტს იმის განსასაზღვრად, თუ რა შემთხვევაშია საჭირო და აუცილებელი ზეგავლენის შეფასების განხორციელება. ერთი მხრივ, ეს არის ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის მომეტებული საფრთხის არსებობა და მეორე მხრივ, ისეთი შემთხვევები, როდესაც დამუშავებისთვის პასუხისმგებელი პირი:

- მონაცემთა სუბიექტისთვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებს სრულად ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე (სრულად უნდა ფლობდეს ინფორმაციას იმ მექანიზმის შესახებ, რომლის საფუძველზეც მიიღება ავტომატიზებული ინდივიდუალური გადაწყვეტილება ან განხორციელდება პროფაილინგი[18], რაც ზეგავლენის შეფასების შედეგადაა შესაძლებელი);
- ამუშავებს საქართველოს მოსახლეობის არანაკლებ 3 პროცენტის განსაკუთრებული კატეგორიის მონაცემებს, რაც გამოითვლება მოსახლეობის აღწერის ბოლო შედეგების მიხედვით;
- ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში.[19]
- აღსანიშნავია, რომ კანონი დამატებით არ განმარტავს მონაცემთა სუბიექტების ქცევის სისტემატური და მასშტაბური მონიტორინგის ცნებებს, თუმცა, ამ თვალსაზრისით, საყურადღებოა პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტი[20], რომლის მიხედვით, მონაცემთა სუბიექტების

[18] პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებასთან დაკავშირებული უფლებებისა და პროფაილინგის შესახებ, გვ. 11-12.

[19] იხ. პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) 31-ე მუხლის მე-2 პუნქტი.

[20] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №22 „დამუშავებისთვის პასუხისმგებელ პირთა და დამუშავებაზე უფლებამოსილ პირთა წრის განსაზღვრის შესახებ, რომლებსაც არ აქვთ ვალდებულება დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი“.

ქცევის სისტემატურ და მასშტაბურ მონიტორინგად მიიჩნევა ისეთი აქტივობები, როგორიცაა:

ა) ინტერნეტ აქტივობის თვალთვალი, სადაც ხდება მონაცემთა სუბიექტის წინასწარი რეგისტრაცია (მომხმარებლის შექმნა/აქტივაცია);

ბ) პროფაილინგი ან ქულების მინიჭება რისკების შეფასების მიზნით;

გ) ადრეული და სკოლამდელი აღზრდისა და განათლების დაწესებულების, ზოგადსაგანმანათლებლო დაწესებულების, სპეციალური პროფესიული საგანმანათლებლო დაწესებულების, უმაღლესი საგანმანათლებლო დაწესებულების მიერ ბავშვების, მოსწავლეების, მსმენელებისა და სტუდენტების ქცევის მონიტორინგი;

დ) პერსონალურ მონაცემებზე დაფუძნებული ქცევითი რეკლამირება;

ე) სატელეკომუნიკაციო ქსელების ოპერირება.

ნორმატიული აქტით[21] განსაზღვრული კრიტერიუმების დაკმაყოფილების შემთხვევაში, მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს, ზემოთ ჩამოთვლილის გარდა, შესაძლებელია სხვაგვარი აქტივობაც წარმოადგენდეს. ამასთან, საუკეთესო პრაქტიკის გათვალისწინებით, მეტ-ნაკლებად დადგენილია ზეგავლენის შეფასების აუცილებლობის განსაზღვრის ევროპული პრაქტიკის შესაბამისი სტანდარტის საორიენტაციო მაგალითები, რაც აღნიშნული სფეროთი დაინტერესებულ პირებს დაეხმარება პრაქტიკული საკითხების მეტად გააზრებაში.

ვინაიდან ქართული კანონმდებლობისთვის ზეგავლენის შეფასების ცნება სიახლეა, თავად ამ პროცედურის მნიშვნელოვნებასა და მის აუცილებლობაზე საინტერესოა ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკის მიმოხილვა:

- *შპს ,,ციფრული უფლებები ირლანდია" ირლანდიის კომუნიკაციების სამინისტროს წინააღმდეგ*[22]

[21] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №22 „დამუშავებისთვის პასუხისმგებელ პირთა და დამუშავებაზე უფლებამოსილ პირთა წრის განსაზღვრის შესახებ, რომლებსაც არ აქვთ ვალდებულება დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი".

[22] CJEU - C-293/12 and C-594/12 - Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others - GDPRhub.

- ევროკავშირის მართლმსაჯულების სასამართლომ ძალადაკარგულად გამოაცხადა დირექტივა მონაცემთა დაცვის შესახებ, რომლითაც საკომუნიკაციო ქსელების პროვაიდერებს ეკისრებოდათ მხარეებს შორის კომუნიკაციის დროისა და ხანგრძლივობის შესახებ ინფორმაციის შეგროვების ვალდებულება - ე.წ. „ტრაფიკის მონაცემები“ და საკომუნიკაციო მოწყობილობის ადგილმდებარეობის შესახებ ინფორმაცია.

სასამართლოს გადაწყვეტილების თანახმად, მიუხედავად იმისა, რომ გაუქმებული დირექტივა კომუნიკაციის შინაარსის მოპოვებას არ ითვალისწინებდა, არსებული ინფორმაცია უკავშირდებოდა პირად ცხოვრებას. შესაბამისად, დადგენილი ვალდებულება მოიაზრებდა პირადი ცხოვრების და კომუნიკაციის პატივისცემის უფლებაში ჩარევას, რაც გარანტირებულია ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-7 და GDPR მე-8 მუხლის შესაბამისად. სასამართლომ განმარტა, რომ უფლებაში ჩარევა მხოლოდ ეროვნული უსაფრთხოების მიზნით შეიძლება განხორციელდეს. მოცემულ შემთხვევაში კი, არსებული სამართლებრივი რეგულაცია ვერ აკმაყოფილებდა პროპორციულობის კრიტერიუმს. ამ და სხვა გარემოებებზე დაყრდნობით, სასამართლომ დაადგინა, რომ ძირითად უფლებებში დირექტივით გათვალისწინებული ჩარევის ფარგლები არ იყო იმდენად შეზღუდული, რომ უფლებებში ჩარევა მხოლოდ მკაცრად აუცილებელი მოცულობით მომხდარიყო. ზემოხსენებულის გათვალისწინებით, **სასამართლომ ხაზი გაუსვა მონაცემთა ამგვარი ფართომასშტაბიანი დამუშავებისას ზეგავლენის შეფასების განხორციელების აუცილებლობას.**

- *„ბრიჯისი სამხრეთ უელსის პოლიციის წინააღმდეგ“*[23]

- აღნიშნულ საქმეზე სამხრეთ უელსის სააპელაციო სასამართლოს გადაწყვეტილებით დადგინდა, რომ სახის ავტომატური ამოცნობის (automated facial recognition (AFR)) ტექნოლოგიის გამოყენება სამხრეთ უელსის პოლიციის მიერ წარმოადგენდა ჩარევას კონფიდენციალურობის უფლებაში, რომელიც გათვალისწინებულია ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლით. საჯარო სივრცეში, პირთა თანხმობის გარეშე, მათი სახეების განურჩევლად სკანირება მნიშვნელოვანი ჩარევა იყო და ქმნიდა **მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების აუცილებლობას,** რაც თავის მხრივ, უზრუნველყოფს ვინაობის

[23] https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

დამდგენი საშუალებების სამართლებრივ და პროპორციულ გამოყენებასა და პირთა კონფიდენციალურობის უფლებების დაცვას.

სასამართლომ დაადგინა, რომ სამხრეთ უელსის პოლიციის მიერ განხორციელებული ზეგავლენის შეფასება სათანადოდ ვერ აფასებდა და ამსუბუქებდა კონფიდენციალურობის AFR ტექნოლოგიის გამოყენებასთან დაკავშირებულ რისკებს. უფრო კონკრეტულად, სათანადოდ ვერ იქნა გათვალისწინებული მონაცემთა მასობრივი შეგროვებისა და მათი პოტენციური არამიზნობრივი გამოყენების შედეგები. სამხრეთ უელსის პოლიციამ ვერ დაასაბუთა, რომ AFR ტექნოლოგიების გამოყენება იყო მათი მიზნების მიღწევის აუცილებელი და პროპორციული საშუალება. ამ ტექნოლოგიების გამოყენება საკმარისად არ იყო გამართლებული დანაშაულის პრევენციისა და საზოგადოებრივი უსაფრთხოების დაცვის მიზნებით, განსაკუთრებით, თუ გავითვალისწინებთ ადამიანის პირად ცხოვრებაში სახის ამოცნობით გამოწვეული ჩარევის ხასიათს. სააპელაციო სასამართლოს ამ გადაწყვეტილებას დიდი როლი მიუძღვის სამართალდამცავი ორგანოების მიერ სამეთვალყურეო ტექნოლოგიების გამოყენებისთვის საზღვრების დადგენაში. მან კიდევ ერთხელ **დაადასტურა მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების აუცილებლობა და ხაზი გაუსვა კონფიდენციალურობის დამრღვევი ტექნოლოგიების გამოყენებისას მკაფიო სამართლებრივი საფუძვლების არსებობის აუცილებლობას.**

- „შრემსი ირლანდიაში Facebook-ის შვილობილი კომპანიის წინააღმდეგ“ [24]

- ევროკავშირის მართლმსაჯულების სასამართლომ განიხილა საქმე, რომელიც ეხებოდა ირლანდიაში Facebook-ის შვილობილი კომპანიის მიერ პერსონალური მონაცემების გადაცემას ამერიკის შეერთებულ შტატებში განთავსებულ სერვერებზე შემდგომი დამუშავებისთვის. მომჩივანმა ევროკავშირის მართლმსაჯულების სასამართლოს მიმართა იმ მოტივით, რომ მოპასუხე მხარე ევროკავშირიდან აშშ-ში სრულიად ავტომატიზებულად გადასცემდა მომხმარებლების პერსონალურ მონაცემებს და აშშ არ აკმაყოფილებდა პერსონალურ მონაცემთა დაცვის სამართლის ევროპულ მოთხოვნებს, რაც ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის მაღალ საფრთხეს ქმნიდა. სასამართლომ დაადგინა, რომ უსაფრთხოების საშუალებათა სქემის (Safe Harbour scheme) საფუძველზე, უზრუნველყოფილი არ იყო

[24] Facebook Ireland Ltd v. Schrems (Schrems II) (Case C-311/18).

მონაცემთა ადეკვატური დაცვა, რადგან აშშ-ს მეთვალყურეობის შესახებ კანონები იძლეოდა მონაცემთა არაპროპორციული შეგროვების საშუალებას და არ გააჩნდა ევროკავშირის მოქალაქეებისთვის სამართლებრივი უზრუნველყოფის საკმარისი მექანიზმები. სასამართლომ ხაზი გაუსვა მონაცემთა დაცვის სტანდარტებსა და ზედამხედველობის ეროვნულ პრაქტიკებს შორის შესაბამისობის კრიტიკულ აუცილებლობას, რაც უზრუნველყოფს პირთა კონფიდენციალობის უფლებების უსაფრთხოებისათვის ყველა ზომის მიღებას მონაცემთა ტრანსსასაზღვრო გადაცემისას. გადაწყვეტილების თანახმად, **ორგანიზაციებმა თითოეულ საერთაშორისო გადაცემაზე ინდივიდუალურად უნდა განახორციელონ ზეგავლენის შეფასება, რათა დადგინდეს, უზრუნველყოფს თუ არა მონაცემთა მიმღები ქვეყნის კანონმდებლობა ადეკვატური დაცვის გარანტიას,** თუ დამატებითი ორგანიზაციულ-ტექნიკური ზომებით შეუძლებელია ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის არსებითად შემცირება, მონაცემთა დამუშავება არ უნდა განხორციელდეს.

დასახელებული მაგალითები ცხადჰყოფს სხვადასხვა ხასიათის მონაცემთა დამუშავებისას ზეგავლენის შეფასების მნიშვნელობასა და აუცილებლობას, რამდენადაც პროცესი გულისხმობს მონაცემთა დამუშავების სრულ ციკლთან დაკავშირებული რისკების სათანადოდ და სრულყოფილად შეფასების, იდენტიფიცირების, პრევენციისა და სამომავლო აღმოფხვრის გზების მოძიების შესაძლებლობას.

2.2 საფრთხის იდენტიფიცირება

ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის მაღალი ალბათობის დასადგენად აუცილებელია ქვემოთ ჩამოთვლილი გარემოებებიდან **სულ მცირე ორის ერთდროულად** არსებობა[25]:

- 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

[25] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“.

სარგებლის მიღებას, დასაქმებულთა მიერ შესრულებული სამუშაოს ხარისხის შეფასებას ან ადამიანური რესურსების მართვასთან დაკავშირებულ სხვა აქტივობებს, გარკვეულ ადგილებზე ფიზიკურ წვდომას ან გადაადგილებას;

მაგალითი: *მომხმარებლის გადახდისუნარიანობის შესაფასებლად, საკრედიტო ისტორიების ბიურო აგროვებს გარკვეულ მონაცემებს, როგორიცაა ინფორმაცია მომხმარებლის საკრედიტო და გადახდების ისტორიის შესახებ. შემდგომ, ეს პერსონალური მონაცემები მუშავდება სპეციალური ალგორითმის მეშვეობით, რომელიც მომხმარებელს ანიჭებს გადახდისუნარიანობის შესაბამის ქულას, რომლის გათვალისწინებითაც მიიღება შესაბამისი გადაწყვეტილება.*

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

მაგალითი: *სოციალური მედიაკომპანიები და საძიებო სისტემები დამუშავების პროცესში ახორციელებენ მონაცემთა სუბიექტების ფართომასშტაბიან, რეგულარულ და სისტემატურ მონიტორინგს. ასეთი კომპანიების ბიზნესმოდელი ეფუძნება დიდი მოცულობის პერსონალურ მონაცემთა დამუშავებას. მათი შემოსავლის წყაროა მიზნობრივი სარეკლამო მომსახურების, ასევე კომპანიებისთვის თავიანთ ვებგვერდებზე რეკლამების გამოქვეყნების შეთავაზება. მიზნობრივი რეკლამა გულისხმობს მის განთავსებას დემოგრაფიის, ასევე, მომხმარებელთა მსყიდველობითი ისტორიისა და ქცევის საფუძველზე, რაც საჭიროებს სისტემატურ მონიტორინგს მონაცემთა სუბიექტების ონლაინჩვევებსა თუ ქცევაზე.*[26]

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

მაგალითი: *Facebook-ის მომხმარებელმა, საკუთარი ანგარიშის გვერდზე ოჯახური მდგომარეობის შესახებ ინფორმაციის გამოქვეყნების შემდეგ, მის საცხოვრებელ*

[26] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018. 200.

არეალში მდებარე სავაჭრო ობიექტების მომსახურების შესახებ შეთავაზებები მიიღო. რეკლამის შექმნისას, აღნიშნული მაღაზიები კონკრეტულ პარამეტრებს ნიშნავენ, რათა შეძლონ ისეთ მომხმარებლებთან წვდომა, რომლებიც იმ ადგილთან ახლოს ცხოვრობენ, სადაც რეკლამის განმათავსებელი მაღაზიები მდებარეობს და გარდა ამისა, მათი ინტერესის სფერო ემთხვევა სავაჭრო ობიექტების საქმიანობის მიმართულებებს. შესაბამისად, მომხმარებელი პროფილზე შესვლისთანავე ხედავს რეკლამას.[27]

- ახალი ტექნოლოგიის დანერგვა ან ინოვაციური გამოყენება;

მაგალითი: *ქალაქი გეგმავს ჭკვიანი სათვალთვალო სისტემის დანერგვას საზოგადოებრივ თავშეყრის ადგილებში, აღნიშნული ტექნოლოგია კი მონიტორინგისთვის იყენებს ხელოვნურ ინტელექტს (AI). ხსენებული პროცედურის მეშვეობით ვიდეომეთვალყურეობის საშუალებას შესაძლებლობა აქვს ამოიცნოს სახეები, თვალყური ადევნოს ადამიანთა და საგანთა მოძრაობას, დააფიქსიროს საეჭვო ქცევა დანაშაულის თავიდან აცილების, მისი გამოვლენის, საზოგადოებრივი უსაფრთხოების, პირის უსაფრთხოებისა და საკუთრების დაცვის მიზნით.*

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

მაგალითი: *სამედიცინო დაწესებულება გეგმავს, რომ ორი სხვადასხვა წყაროდან - კლინიკური შემოწმების მონაცემთა ბაზიდან და პაციენტის გეგმური კვლევების შესახებ რეესტრიდან - მოიპოვოს პაციენტის მონაცემები. მითითებული წყაროებიდან ინფორმაციის მოპოვების მიზანია პოტენციური კანდიდატების იდენტიფიცირება, რათა ჩატარდეს ახალი კვლევები და გაუმჯობესდეს მკურნალობის გეგმა. კლინიკური შემოწმებების მონაცემთა ბაზა იმართება კვლევითი დეპარტამენტის მიერ, ხოლო გეგმური კვლევების რეესტრი - სამედიცინო დაწესებულების ადმინისტრაციის მიერ. აღნიშნული პროცესი წარმოადგენს საფრთხის შემცველ გარემოებას, რადგანაც მუშავდება განსაკუთრებული კატეგორიის მონაცემები, რომლიც დაკავშირებულია სხვადასხვა წყაროდან მიღებული მონაცემების ახალი მიზნებისთვის გაერთიანებასთან.*

[27] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018. 201.

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

მაგალითი: *გერმანიაში მცხოვრები ავსტრიის მოქალაქე, მიგრაციისა და ლტოლვილთა ფედერალური სამსახურისგან მოითხოვდა თავისი მონაცემების წაშლას „უცხოელთა ცენტრალური რეესტრიდან“ (AZR). რეესტრი შეიცავს პერსონალურ მონაცემებს გერმანიის მოქალაქეობის არმქონე პირების შესახებ, რომლებიც გერმანიაში ცხოვრობენ სამ თვეზე მეტხანს, და გამოიყენება სტატისტიკური მიზნებით, ასევე, სასამართლო ორგანოების მიერ - დანაშაულებრივი ან საზოგადოებრივი უსაფრთხოებისათვის სარისკო ქმედებების გამოსაძიებლად და გასახსნელად. CJEU-მ აღნიშნა, რომ სტატისტიკური მიზნებისთვის მოთხოვნილ უნდა იქნას მხოლოდ ანონიმური ინფორმაცია, და დაადგინა, რომ AZR არ შეესაბამება მონაცემთა დამუშავების აუცილებლობის კრიტერიუმს. რაც შეეხება მონაცემთა ბაზაში დაცული ინფორმაციის გამოყენებას დანაშაულთან ბრძოლის მიზნით, CJEU-მ დაადგინა, რომ რადგან რეესტრი არ შეიცავს პერსონალურ მონაცემებს გერმანიის მოქალაქეების შესახებ, ასეთი განსხვავებული მოპყრობა დისკრიმინაციაა.*[28]

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

მაგალითი: *ელექტრონული ვაჭრობის კომპანია გეგმავს დანერგოს მონაცემთა დამუშავების სისტემა, რომელიც გააანალიზებს მომხმარებელთა მიერ განხორციელებული ძიების (Search History) და შესყიდვების შესახებ ისტორიას, აგრეთვე, დემოგრაფიულ ინფორმაციას, რათა უშუალოდ მათზე მორგებული პროდუქტების შეთავაზებები გასცეს. გარდა ამისა, მომხმარებლების პროფილის გაანალიზების შედეგად, შესაძლოა, ზოგიერთ მათგანს წვდომა შეეზღუდოს კონკრეტულ შეთავაზებებზე, მათ შორის, სარეკლამო ფასდაკლებებზე.*

- დამუშავებისთვის პასუხისმგებელი პირის თანამშრომლების, სამედიცინო დაწესებულების პაციენტების, არასრულწლოვნების, შეზღუდული

[28] Heinz Huber v Bundesrepublik Deutschland, Case C-524/06

შესაძლებლობისა და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე პირების მონაცემების დამუშავება.[29]

მაგალითი: *კლინიკების, სადაზღვევო ორგანიზაციების, საპენსიო და სოციალური მომსახურების სააგენტოების მიერ ბენეფიციარების პერსონალურ მონაცემთა დამუშავება.*
სასწავლო დაწესებულების მიერ მოსწავლეთა (მათ შორის, სპეციალური საგანმანათლებლო საჭიროების მქონე მოსწავლეთა), სტუდენტთა, მასში დასაქმებულ პირთა ელექტრონული გაზის წარმოება.

2.3 გარემოებები, რომელთა არსებობის დროსაც ზეგავლენის შეფასების განხორციელების ვალდებულება არ არსებობს

აღსანიშნავია, რომ მონაცემთა დამუშავების ყველა პროცესი არ საჭიროებს ზეგავლენის შეფასებას. ეროვნული კანონმდებლობა[30] ამომწურავად განსაზღვრავს იმ გარემოებებს, რომელთა არსებობის შემთხვევაშიც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია განახორციელოს ზეგავლენის შეფასება. ამასთან, კანონმდებელი არ განსაზღვრავს ისეთ შემთხვევებს, როდესაც ზეგავლენის შეფასების ჩატარება არ მოითხოვება. ზეგავლენის შეფასებისათვის აუცილებელი გარემოებების არარსებობის შეფასებისა და მტკიცების ტვირთი ეკისრება დამუშავებისთვის პასუხისმგებელ პირს.

GDPR-ის მიხედვით, ზეგავლენის შეფასების განხორციელება არ არის საჭირო, როდესაც დამუშავება „სავარაუდოდ არ იწვევს ფიზიკური პირების უფლებებისა და თავისუფლებების შელახვის მაღალ რისკს“ ან დამუშავების ბუნება, ფარგლები,

[29] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“.

[30] იგულისხმება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი და პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“.

კონტექსტი და მიზნები ძალიან ჰგავს დამუშავებას, რომლისთვისაც უკვე განხორციელდა ზეგავლენის შეფასება.[31]

მაგალითი: *ორგანიზაცია ადამიანური რესურსების მართვის მიზნით ამუშავებს თანამშრომლების ისეთ პერსონალურ მონაცემებს, როგორიცაა მათი სახელები, სახელფასო განაკვეთი და სამსახურში გამოცხადება, აღნიშნული დამუშავების ხასიათი შეიცავს მინიმალურ რისკებს თანამშრომლების კონფიდენციალურობისათვის, რის გამოც შესაძლოა ზეგავლენის შეფასების განხორციელების აუცილებლობა არ დადგეს.*

მაგალითი: *კომპანია აგროვებს ანონიმურ მონაცემებს თავისი ვებსაიტის ვიზიტორებისგან შიდა ანალიტიკური მიზნებისთვის, როგორიცაა ვებგვერდის ე.წ. „ტრაფიკის“ შაბლონების ანალიზი ან მომხმარებლის გამოცდილების გაუმჯობესება. ვინაიდან, მონაცემები ანონიმურია და არ ავლენს პირებს, ხოლო ანალიტიკა განკუთვნილია მხოლოდ შიდა გამოყენებისთვის, მონაცემთა გაზიარების გარეშე, ზეგავლენის შეფასება შეიძლება არ იყოს საჭირო.*

სხვა შემთხვევაში, მონაცემთა ნებისმიერი დამუშავება, რომლის განხორციელების პირობები (ფარგლები, მიზანი, შეგროვებული პერსონალური მონაცემები, დამუშავებისთვის პასუხისმგებელი პირების ან მიმღებების ვინაობა, მონაცემთა შენახვის ვადა, ტექნიკური და ორგანიზაციული ღონისძიებები და ა.შ.) არსებითად შეიცვალა/გაიზარდა და სავარაუდოდ, მაღალი რისკის შემცველია, უნდა დაექვემდებაროს ზეგავლენის შეფასებას.[32]

[31] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 12.
[32] იქვე, 13.

3. ზეგავლენის შეფასების განხორციელების ეტაპები

3.1 მონაცემთა დამუშავების პროცესისა და მასშტაბის აღწერა

როგორც ზემოთ აღინიშნა, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია დამუშავების დაწყებამდე შეაფასოს დამუშავების პროცესის შესაძლო გავლენა ადამიანის ფუნდამენტური უფლებებისა და თავისუფლებების დაცვაზე, რაც ხელს შეუწყობს საფრთხეების სათანადოდ გამოვლენას, მათზე რეაგირებასა და მათ შემცირებას. საწყის ეტაპზე უნდა გამოირკვეს მონაცემთა დამუშავების მთლიანი ციკლის შემადგენელი ელემენტები, ასევე დადგინდეს, აქვს თუ არა მონაცემთა სუბიექტს მოლოდინი, რომ დამუშავდება მისი პერსონალური მონაცემები, განხორციელდება თუ არა მისი ინფორმირება, ხდება თუ არა მონაცემთა გაზიარება მესამე პირთათვის და სხვა.

აღნიშნულის შემდგომ, უნდა მოხდეს დამუშავების მასშტაბის იდენტიფიცირება. თითოეული დამუშავების სახისთვის ცალ-ცალკე უნდა განისაზღვროს დამუშავების სამართლებრივი საფუძველი და მონაცემთა შენახვის ვადა. ეს ეტაპი ეხმარება დამუშავებისთვის პასუხისმგებელ პირს მოახდინოს დამუშავების სისტემურობის და მასშტაბურობის განსაზღვრა, ხოლო ამ კონტექსტში მნიშვნელოვანია დადგინდეს, მუშავდება თუ არა არასრულწლოვანთა ან სხვა მოწყვლადი ჯგუფის მონაცემები, რა სიხშირით ხდება მონაცემთა დამუშავება, ასევე, მონაცემთა დამუშავების გეოგრაფიული არეალი.

მონაცემთა დამუშავების პროცესის კანონიერად მიჩნევისათვის, საჭიროა, როგორც დამუშავების სათანადო საფუძვლის იდენტიფიცირება, ასევე, კანონით გათვალისწინებულ ყველა ვალდებულებასთან დამუშავების პროცესის შესაბამისობის უზრუნველყოფა. მათ შორის, განსაკუთრებული ადგილი უჭირავს მონაცემთა დამუშავების პრინციპებს. დამუშავებისთვის პასუხისმგებელი პირი პასუხისმგებელია მონაცემთა დამუშავებისას კანონის მე-4 მუხლით განსაზღვრული პრინციპების დაცვაზე და მან უნდა შეძლოს დამუშავების პროცესის მათთან შესაბამისობის დასაბუთება. კერძოდ, დამუშავების დაწყებამდე უნდა განსაზღვროს, სჭირდება თუ არა კონკრეტული პერსონალური მონაცემების დამუშავება შესაბამისი მიზნების მისაღწევად. ამ თვალსაზრისით, მონაცემთა დამუშავების მიზნის იდენტიფიცირება და დამუშავების პრინციპების დაცვის საკითხის დადგენა, უმთავრესი ამოცანაა. ამასთან, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა

გამოარკვიოს, არის თუ არა მონაცემთა დამუშავება შესაბამისი მიზნის პროპორციული და შედეგის გათვალისწინებით მიიღოს გადაწყვეტილება - დაამუშავებს თუ არა პერსონალური მონაცემების შემცველ ინფორმაციას.

3.2 დამუშავების შედეგად შესაძლო რისკების და საფრთხეების ხარისხობრივი შეფასება

ზეგავლენის შეფასების შემდეგი ეტაპი გულისხმობს საფრთხეების იდენტიფიცირებას და მათი ხარისხის შეფასებას. აღნიშნული პროცესი, თავის მხრივ, იყოფა რამდენიმე ქვე-ეტაპად:

- საფრთხეებისა და მათი წყაროების იდენტიფიცირება: **აღნიშნულ ეტაპზე ხორციელდება თითოეული შესაძლო მაღალი ალბათობის საფრთხის გამოვლენა და მისი გამომწვევი წყაროს იდენტიფიცირება;**
- საფრთხეების ხარისხობრივი ანალიზი: **ხორციელდება შესაძლო საზიანო შედეგებისა და ადამიანის ძირითად უფლებებსა და თავისუფლებებზე მათი გავლენის ხარისხის შეფასება;**
- საფრთხეებზე რეაგირება: **დამუშავებისთვის პასუხისმგებელი პირის მიერ, საფრთხეების შემცირებისკენ მიმართული კონკრეტული ღონისძიებების დაგეგმვა და განხორციელება, რაც შეიძლება ემსახურებოდეს მონაცემთა სუბიექტისთვის შესაძლო საზიანო შედეგების აღმოფხვრას ან ამგვარი შედეგების დადგომის მაღალი ალბათობის შემცირებას;**
- საფრთხეების აღრიცხვა: **ამ ეტაპზე დამუშავებისთვის პასუხისმგებელი პირის მიერ ხორციელდება იდენტიფიცირებული საფრთხეების, მათი წყაროების, მათზე რეაგირების ღონისძიებების, საფრთხეების შემცირებისთვის გატარებული ღონისძიებებისა და მიღწეული შედეგების დოკუმენტური აღრიცხვა.**

თუ ზეგავლენის შეფასების შედეგად გამოვლინდება ადამიანის ძირითად უფლებათა და თავისუფლებათა დარღვევის მაღალი საფრთხე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მიიღოს ყველა აუცილებელი ზომა ასეთი შედეგის არსებითად შესამცირებლად და ამ დროს საჭიროების შემთხვევაში, კონსულტაციის მიზნით მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს.

3.3 დამუშავების შედეგების განსაზღვრა

საფრთხეების ხარისხობრივი ანალიზის შედეგად ფასდება იდენტიფიცირებული საფრთხეების შესაძლო საზიანო შედეგები და ადამიანის უფლებებსა და თავისუფლებებზე მათი გავლენის ხარისხი. ამგვარი შესაძლო საზიანო შედეგებია:

- **ვინაობის მითვისება ან გაყალბება** - *პერსონალური მონაცემების მითვისება (Identity theft), ვინაობის მოპარვის ფენომენი, გულისხმობს ერთი პირის მიერ მეორის (დაზარალებულის) ინფორმაციის, მონაცემების ან დოკუმენტების მოპოვებას და თავის საკუთრებად გასაღებას, ამ პირის სახელით საქონლისა და სერვისების მისაღებად[33];*
- **ფინანსური დანაკარგი** - მაგ.: *დაზარალებულის ფინანსურ მონაცემებზე ან დოკუმენტებზე წვდომა, რომელიც შესაძლებლია გამოყენებულ იქნას თაღლითური გადახდის ოპერაციებისთვის;*
- **რეპუტაციის შელახვა** - *მაგ.: საქმეში Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni მოსარჩელე ითხოვდა თავისი პერსონალური მონაცემების წაშლას სარეიტინგო კომპანიის რეესტრიდან, ვინაიდან აღნიშნულ გაზაში რეგისტრაცია გამოწვეული იყო მის შესახებ არასწორი მონაცემების დამუშავებით და შედეგად ზიანი ადგებოდა მის პროფესიულ რეპუტაციასა და კვალიფიკაციას[34];*
- **პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალობის დარღვევა** - *მაგ.: მონაცემთა სუბიექტის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის გამჟღავნება სამედიცინო დაწესებულების პერსონალის მიერ, რომელსაც პროფესიული საიდუმლოს შენახვის ვალდებულება ეკისრება;*
- **ფსევდონიმიზებული პერსონალური მონაცემების უკანონო გამჟღავნება** - *დეპერსონალიზაციისგან განსხვავებით, ფსევდონიმიზებული მონაცემი კვლავ პერსონალური მონაცემია, რადგან პიროვნების ვინაობასთან კავშირი არსებობს იმ ფორმით, რომელიც ერთდროულად მოიცავს როგორც ფსევდონიმის, ისე დაშიფვრის გასაღებს. შესაბამისად, მათთვის, ვისაც აქვს დაშიფვრის კოდის გამოყენების უფლებამოსილება, პირის ხელახალი იდენტიფიცირება მარტივია. დაშიფვრის კოდი განსაკუთრებით დაცული უნდა იყოს არაუფლებამოსილი*

[33] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018, 418.

[34] CJEU, C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, EUR-Lex - 62015CJ0398 - EN - EUR-Lex (europa.eu)

პირების მიერ გამოყენებისაგან[35]*, ამ ვალდებულების დარღვევა კი, თავის მხრივ, საფრთხის შემცველია ადამიანის პირადი ცხოვრების ხელშეუხებლობისა და უსაფრთხოებისთვის;*

- **ჯანმრთელობის მდგომარეობის გაუარესება** - მაგ.: *სამედიცინო პერსონალის მიერ განსაკუთრებული კატეგორიის მონაცემების არასათანადო დამუშავების შედეგად მონაცემთა სუბიექტისათვის არასწორი მკურნალობის დანიშვნა;*
- **სასიცოცხლო მნიშვნელობის ინფრასტრუქტურაზე წვდომის შეზღუდვა** - *სამედიცინო დაწესებულების მიერ არასწორად გადაგზავნილი განსაკუთრებული კატეგორიის მონაცემების შედეგად პაციენტის შეზღუდვა კონკრეტულ მედიკამენტებზე;*
- **სხვა სახის მნიშვნელოვანი ფიზიკური, ქონებრივი ან არაქონებრივი ღირებულების მატერიალური ან არამატერიალური ზიანი**[36] - მაგ.: მონაცემთა დამუშავების შედეგად, სხვა ისეთი სახის საზიანო შედეგის დადგომა/გამოწვევა, რომელიც მნიშვნელოვნად (საგრძნობლად და არსებითად) აუარესებს მონაცემთა სუბიექტის ფიზიკურ, ქონებრივ ან არაქონებრივ მდგომარეობას როგორც მატერიალური, ასევე არამატერიალური ზარალის მიყენებით.

იდენტიფიცირებული საფრთხეების შესაძლო საზიანო შედეგებისა და ადამიანის ძირითად უფლებებსა და თავისუფლებებზე მათი გავლენის ხარისხი წარმოშობს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, შესაბამისი რეაგირება მოახდინოს მათზე. საფრთხეებზე რეაგირება, უპირველეს ყოვლისა, გულისხმობს დამუშავებისთვის პასუხისმგებელი პირის მიერ საფრთხეების შემცირებისკენ მიმართული კონკრეტული ღონისძიებების დაგეგმვასა და განხორციელებას, რაც უნდა ემსახურებოდეს საფრთხის შემცველი შედეგების გამორიცხვას ან/და ასეთი შედეგების დადგომის მაღალი ალბათობის შემცირებას.

[35] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018, 110.

[36] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“.

3.4 ზეგავლენის შეფასების განხორციელების მეთოდოლოგია, პერიოდულობა და პასუხისმგებელი პირები

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია ზეგავლენის შეფასება განახორციელოს წინასწარ, მონაცემთა დამუშავების დაწყებამდე. აღნიშნული პროცესი შესაძლოა წარიმართოს მოწვეული პირის მიერაც, მაგრამ პროცესის გამართულობაზე პასუხისმგებელი მაინც უშუალოდ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირია, რომელმაც, საუკეთესო ევროპული პრაქტიკის მიხედვით,[37] მეტი ეფექტიანობისთვის, სათანადო კონსულტაციისა და რეკომენდაციის მიღების მიზნით, პროცესში უნდა ჩართოს პერსონალურ მონაცემთა დაცვის ოფიცერი (ასეთის არსებობის შემთხვევაში). პერსონალურ მონაცემთა დაცვის ოფიცერმა ასევე უნდა აკონტროლოს ზეგავლენის შეფასების ვალდებულების შესრულება.

ეროვნული კანონმდებლობა ითვალისწინებს ზეგავლენის შეფასების სხვადასხვა ეტაპზე გამოსაყენებელ მეთოდებსა და ინსტრუმენტებს. ეს შეიძლება იყოს „SWOT“ ანალიზი, ინდივიდუალური და ჯგუფური დისკუსიები, მონაცემთა დამუშავების პროცესის სამიზნე ჯგუფებთან შეხვედრები, სამუშაო შეხვედრები/სემინარები და სხვა. ამ კუთხით, ასევე, აღსანიშნავია, კანონით მკაფიოდ განსაზღვრულ შემთხვევაში, პერსონალურ მონაცემთა დაცვის სამსახურთან კონსულტირების მექანიზმის გამოყენება. კერძოდ, თუ ზეგავლენის შეფასების შედეგად გამოვლინდება მაღალი საფრთხე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მიიღოს ყველა აუცილებელი ზომა საფრთხეების არსებითად შესამცირებლად და, საჭიროების შემთხვევაში, კონსულტაციის მიზნით მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს,[38] რომელსაც უნდა წარუდგინოს:

ა) დამუშავებისთვის პასუხისმგებელი პირის, თანადამუშავებისთვის პასუხისმგებელი პირებისა და დამუშავებაზე უფლებამოსილი პირის უფლებამოსილების შესახებ ინფორმაცია;
ბ) დაგეგმილი მონაცემთა დამუშავების მიზნებისა და საშუალებების შესახებ ინფორმაცია;

[37] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 15.
[38] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“.

გ) მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დასაცავად განსაზღვრული უსაფრთხოების ზომების შესახებ ინფორმაცია;
დ) პერსონალურ მონაცემთა დაცვის ოფიცრის (ასეთის არსებობის შემთხვევაში) საკონტაქტო ინფორმაცია;
ე) ზეგავლენის შეფასება;
ვ) სხვა (დამატებითი) ინფორმაცია პერსონალურ მონაცემთა დაცვის სამსახურის მიერ მოთხოვნის არსებობის შემთხვევაში.

რაც შეეხება ზეგავლენის შეფასების განხორციელების დროსა და პერიოდულობას, აღნიშნულს კანონი ზუსტად ადგენს და პროაქტიულ ხასიათს უკავშირებს. როგორც ზემოთ არაერთგზის აღინიშნა, ზეგავლენის შეფასება უნდა განხორციელდეს წინმსწრებად, მონაცემთა დამუშავების დაწყებამდე. რაც შეეხება დამუშავების პროცესში ზეგავლენის შეფასების შემდგომ გადასინჯვას, ამ თვალსაზრისით დამუშავებისთვის პასუხისმგებელ პირს ეკისრება ზეგავლენის პროცესის მუდმივი მეთვალყურეობისა და არსებული მიდგომებისა თუ ვითარების ცვლილებათა გათვალისწინებით - შეფასების გადახედვის/ახლებურად ჩამოყალიბების ვალდებულება.

3.5 პასუხისმგებლობა ზეგავლენის შეფასების განხორციელების ვალდებულების დარღვევისთვის

ბუნებრივია, მხოლოდ სამართლებრივი ინსტრუმენტების შემოღება და დადგენა არ არის საკმარისი პერსონალურ მონაცემთა დასაცავად. მონაცემთა დაცვის წესების ეფექტიანობისთვის, საჭიროა ისეთი გარანტიების შექმნა, რომლებიც მონაცემთა სუბიექტებს საშუალებას მისცემს, შეეწინააღმდეგონ უფლებების დარღვევას და მოითხოვონ განცდილი ზიანის ანაზღაურება. GDPR-ის თანახმად, მნიშვნელოვანია ისიც, რომ საზედამხედველო ორგანოს მიერ დაკისრებული ადმინისტრაციული სახდელი, მათ შორის - ჯარიმა, ყველა ინდივიდუალურ შემთხვევაში იყოს ეფექტური, პროპორციული და შემაკავებელი ძალის მქონე.[39]

[39] სახელმძღვანელო პრინციპები 04/2022 მონაცემთა დაცვის ძირითადი რეგულაციის მიხედვით ადმინისტრაციული ჯარიმის გამოანგარიშების წესის შესახებ, 2023 წლის 24 მაისი.

შედარებისთვის საინტერესოა ზეგავლენის შეფასების განუხორციელებლობისთვის, შესაძლო პასუხისმგებლობის ზომები GDPR-ისა და ეროვნული კანონმდებლობის მიხედვით:

ინსპექტირება და გაფრთხილება: თუ მონაცემთა დაცვის ორგანო შეიტყობს, რომ დამუშავებისთვის პასუხისმგებელმა პირმა არ განახორციელა მონაცემთა დაცვაზე ზეგავლენის შეფასება, მას შეუძლია დაიწყოს ინსპექტირება, რომლის შედეგად, მონაცემთა დაცვის ორგანო უფლებამოსილია გასცეს გაფრთხილებები ან რეკომენდაციები, რათა დამუშავებისთვის პასუხისმგებელმა პირმა უზრუნველყოს მონაცემთა დაცვაზე ზეგავლენის შეფასების მოთხოვნებთან შესაბამისობა და მიიღოს მაკორექტირებელი ზომები.

ადმინისტრაციული ჯარიმები: ზეგავლენის შეფასების მოთხოვნებთან შეუსაბამობა მიიჩნევა GDPR-ის დარღვევად, აღნიშნული დარღვევის სიმძიმისა და სხვა გარემოების გათვალისწინებით კი, შესაძლოა გამოიწვიოს ადმინისტრაციული სახდელების დაკისრება, რომელთა ოდენობა განისაზღვრება დარღვევის ხასიათის, სიმძიმისა და ხანგრძლივობის, ასევე, სხვა ისეთი ფაქტორების გათვალისწინებით, როგორიცაა დამუშავებისთვის პასუხისმგებელი პირის თანამშრომლობა მონაცემთა დაცვის ორგანოსთან და სხვა დარღვევები. მონაცემთა დაცვაზე ზეგავლენის შეფასებასთან დაკავშირებული ისეთი დარღვევებისთვის, როგორიცაა სისტემური ხარვეზები მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელებისას მაღალრისკიანი დამუშავების საქმიანობასთან მიმართებით, ან GDPR-ის ძირითადი პრინციპების დარღვევა - მონაცემთა დაცვის ორგანოებმა შესაძლოა დააკისრონ ჯარიმები 20 მილიონ ევრომდე ოდენობით.

მაკორექტირებელი ზომები და შესაბამისობის ბრძანებები: ჯარიმებთან ერთად, საზედამხედველო ორგანოებმა შეიძლება გასცენ ბრძანებები მაკორექტირებელი ქმედებების განხორციელებასთან დაკავშირებით, რომლებიც მოითხოვენ ორგანიზაციისგან საჭირო მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელებას, რისკების შემსუბუქებასა და GDPR-ის მოთხოვნებთან შესაბამისობის უზრუნველყოფას. ასეთი ბრძანების შეუსრულებლობამ შეიძლება გამოიწვიოს დამატებითი სანქციებისა და ჯარიმების დაკისრება.

რაც შეეხება სანქციების შესახებ ინფორმაციის ხელმისაწვდომობას, ევროპული კანონმდებლობის მიხედვით, საზედამხედველო ორგანო უფლებამოსილია უზრუნველყოს GDPR-ის დარღვევისთვის, მათ შორის, ზეგავლენის შეფასების

განუხორციელებლობისთვის, დაკისრებული სანქციების გასაჯაროება,[40] აღნიშნული ემსახურება საზოგადოებისა და სხვა ორგანიზაციების ინფორმირებას კონკრეტული შემთხვევის პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან შეუსაბამობის თაობაზე. ასევე, მას შეიძლება ჰქონდეს მომავალი დარღვევებისგან შემაკავებელი, პრევენციული ხასიათი.

GDPR-ს დაქვემდებარებული ორგანიზაციები უნდა დარწმუნდნენ, რომ მათთვის ცხადია ზეგავლენის შეფასების მოთხოვნები, უნდა განახორციელონ აღნიშნული შეფასებები მაღალი რისკის მქონე დამუშავების დროს, მიიღონ შესაბამისი ზომები ასეთი რისკების შესამცირებლად და უზრუნველყონ მონაცემთა დაცვის რეგულაციებთან შესაბამისობა, რათა თავიდან აიცილონ სანქციები და ჯარიმები.[41]

ეროვნული კანონმდებლობა:

ევროპული კანონმდებლობის სულისკვეთების იდენტურად, ქართველმა კანონმდებელმა გაამკაცრა ადმინისტრაციული პასუხისმგებლობა პერსონალურ მონაცემთა კანონმდებლობის მოთხოვნათა დარღვევებისთვის. ახალი კანონის მიღების შედეგად, გაიზარდა და დაზუსტდა ადმინისტრაციული სამართალდარღვევების ჩამონათვალი და შინაარსი, ახლებურად ჩამოყალიბდა ადმინისტრაციული პასუხისმგებლობის მომწესრიგებელი ნორმებიც, გაიზარდა ჯარიმების ოდენობაც.

ზეგავლენის შეფასების ვალდებულების შეუსრულებლობისთვის, ევროპული სტანდარტის მსგავსად, პერსონალურ მონაცემთა დაცვის სამსახურს, მიღებული შეტყობინების საფუძველზე ან თავისი ინიციატივით შეუძლია დაიწყოს ***ინსპექტირება/შემოწმება.*** თუ საზედამხედველო ორგანო შეიტყობს, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა არ განახორციელა ზეგავლენის შეფასება, მას შეუძლია დაიწყოს ინსპექტირება, რომლის ფარგლებშიც უფლებამოსილია გამოიყენოს გაფრთხილება, გასცეს სავალდებულო ხასიათის დავალებები ან რეკომენდაციები, რათა დამუშავებისთვის პასუხისმგებელმა პირმა სამომავლოდ უზრუნველყოს ზეგავლენის შეფასების კანონმდებლობით დადგენილ მოთხოვნებთან შესაბამისობა და მიიღოს სათანადო ზომები.

[40] https://gdpr-info.eu/issues/fines-penalties/

ასევე, კანონის მე-80 მუხლი განსაზღვრავს პასუხისმგებლობას ზეგავლენის შეფასების ვალდებულების შეუსრულებლობისთვის. აღნიშნული მუხლის პირველი პუნქტის თანახმად, მითითებული სამართალდარღვევა იწვევს:

ა) ფიზიკური პირის, საჯარო დაწესებულების, არასამეწარმეო (არაკომერციული) იურიდიული პირის, აგრეთვე იურიდიული პირის, უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის, რომელთა წლიური ბრუნვა 500 000 ლარს არ აღემატება, გაფრთხილებას ან დაჯარიმებას 2 000 ლარის ოდენობით;

ბ) იურიდიული პირის (გარდა არასამეწარმეო (არაკომერციული) იურიდიული პირისა), უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის, რომელთა წლიური ბრუნვა 500 000 ლარს აღემატება, გაფრთხილებას ან დაჯარიმებას 3 000 ლარის ოდენობით.

იგივე სამართალდარღვევა, ჩადენილი დამამძიმებელი გარემოებ(ებ)ის არსებობისას, გამოიწვევს:

ა) ფიზიკური პირის, საჯარო დაწესებულების, არასამეწარმეო (არაკომერციული) იურიდიული პირის, აგრეთვე იურიდიული პირის, უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის, რომელთა წლიური ბრუნვა 500 000 ლარს არ აღემატება, დაჯარიმებას 3 000 ლარის ოდენობით;

ბ) იურიდიული პირის (გარდა არასამეწარმეო (არაკომერციული) იურიდიული პირისა), უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის, რომელთა წლიური ბრუნვა 500 000 ლარს აღემატება, დაჯარიმებას 5 000 ლარის ოდენობით.

ამასთან, კანონის 62-ე მუხლი განსაზღვრავს კანონით გათვალისწინებული ადმინისტრაციული სამართალდარღვევებისთვის ადმინისტრაციული პასუხისმგებლობის დამამძიმებელ გარემოებებს. ზემოთ აღნიშნული სამართალდარღვევების კონტექსტში ადმინისტრაციული პასუხისმგებლობის დამამძიმებელ გარემოებებაა 1 წლის განმავლობაში იმავე ადმინისტრაციული სამართალდარღვევის განმეორებით ჩადენა, რომლის გამოც დამუშავებისთვის პასუხისმგებელ პირს უკვე დაედო ადმინისტრაციული სახდელი.[42]

[42] იხ. პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) 62-ე მუხლის მე-2 პუნქტი.

4. ზეგავლენის შეფასების შედეგების გამოყენება მონაცემთა დაცვის მიზნებისთვის

როგორც ზემოთ აღინიშნა, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია დამუშავების დაწყებამდე შეაფასოს მონაცემთა დამუშავების პროცესის შესაძლო გავლენა, რაც ხელს შეუწყობს საფრთხეების სათანადოდ გამოვლენას, მათზე რეაგირებასა და მათ შემცირებას. თუ საფრთხეების ხარისხობრივი ანალიზის ეტაპზე დადგინდება, რომ დამუშავების შედეგად არსებობს ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის შექმნის მაღალი ალბათობა, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია საფრთხეებზე მოახდინოს სათანადო რეაგირება. რისკების შეფასებას თან უნდა მოჰყვეს უსაფრთხოების ადეკვატურ ღონისძიებათა დაგეგმვა გამოვლენილი საფრთხეების საპასუხოდ[43].

ამგვარი საფრთხეების ალბათობის შემამცირებელი ღონისძიებების მაგალითებია[44]:

- მონაცემთა შენახვის ვადების მინიმუმამდე დაყვანა;
- დასაქმებულთა ცნობიერების ასამაღლებელი ტრენინგების ან/და კურსების ორგანიზება პერსონალურ მონაცემთა დაცვის კუთხით;
- პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტის შემუშავება/დახვეწა;
- ორგანიზაციაში ან კონკრეტული პროექტის ფარგლებში ფიზიკური ან ინფორმაციული ტექნოლოგიური უსაფრთხოების შეფასება და, საჭიროების შემთხვევაში, შესაბამისი ზომების მიღება;
- ახალი ინფორმაციული ტექნოლოგიების სისტემების საჭიროების შეფასება პერსონალური მონაცემების უსაფრთხოდ დამუშავებისა და შენახვის უზრუნველყოფის მიზნით;
- დეპერსონალიზებული ან ფსევდონიმიზებული მონაცემების გამოყენების შესაძლებლობის შეფასება;

[43] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018, 205.

[44] Data Protection Commission, Guide to Data Protection Impact Assessment (DPIAs), October 2019, 20-21.

- მონაცემთა სუბიექტის ინფორმირება თუ რა მოცულობის პერსონალური მონაცემი მუშავდება კონკრეტული, წინასწარ განსაზღვრული მიზნის მისაღწევად;
- პერსონალურ მონაცემების დამუშავებასთან დაკავშირებული ნებისმიერი გადაწყვეტილება მიღებულ უნდა იქნეს ეროვნულ კანონმდებლობასთან შესაბამისობაში.

საფრთხეებზე რეაგირების ზემოთ აღნიშნული მაგალითები მიმართულია დამუშავებისთვის პასუხისმგებელი პირის მიერ კონკრეტული ღონისძიებების დაგეგმვისა და განხორციელებისკენ, რაც შეიძლება ემსახურებოდეს საფრთხის შემცველი საზიანო შედეგების გამორიცხვას ან/და ასეთი შედეგების დადგომის მაღალი ალბათობის შემცირებას.

აქვე გასათვალისწინებელია, რომ თუ დამატებითი ორგანიზაციულ-ტექნიკური ზომებით შეუძლებელია ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის არსებითად შემცირება, **მონაცემთა დამუშავება არ უნდა განხორციელდეს.**

მაგალითი: *გერმანიაში, ბავშვთა პირადი ცხოვრების ხელშეუხებლობის უფლების რეალიზაციის მიზნით, აიკრძალა კონკრეტული, ინტერნეტთან დაკავშირებული სათამაშოს გაყიდვა, ვინაიდან მისი საშუალებით, შესაძლებელი იყო ბავშვისა და მის სიახლოვეს მყოფი ზრდასრული ადამიანების კომუნიკაციების ჩაწერა და ინტერნეტ აპლიკაციისთვის გადაგზავნა. მარეგულირებელი ორგანოების მოთხოვნით, სათამაშოს მწარმოებლებს დაევალათ უსაფრთხოების სათანადო ზომების მიღება და სამომავლოდ, მონაცემთა დამუშავების პროცესის ხელახლა დაწყებამდე - ზეგავლენის შეფასების პროცესის სრულყოფილად განხორციელება.*[45]

[45] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018, 416.

5.მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი

5.1 მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის სარეკომენდაციო ფორმა (ნიმუში)[46] და მისი სტრუქტურა

ეროვნული კანონმდებლობა, GDPR-ის მსგავსად, აწესებს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, აწარმოოს ზეგავლენის შეფასების დოკუმენტი, სადაც: აღრიცხავს მისი პასუხისმგებლობის ქვეშ არსებულ დამუშავების შესახებ ინფორმაციას, მათ შორის, მონაცემთა კატეგორიებს, მათი დამუშავების მიზნებს, პროპორციულობას; აღწერს დამუშავების პროცესსა და საფუძვლებს; ასახავს ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის ალბათობის შეფასებას და მონაცემთა უსაფრთხოების დაცვის მიზნით გათვალისწინებული ტექნიკურ და ორგანიზაციულ ზომებს[47]. აღნიშნული გამომდინარეობს ანგარიშვალდებულებისა და გამჭვირვალობის პრინციპიდან.[48]

ზეგავლენის შეფასების დოკუმენტში აღინიშნება:

- **დამუშავებისთვის პასუხისმგებელი პირის მონაცემები** - სახელწოდება, სამართლებრივი ფორმა, მათ შორის, პერსონალურ მონაცემთა დაცვის ოფიცრის (არსებობის შემთხვევაში) ვინაობა და საკონტაქტო ინფორმაცია;

- **მონაცემთა დამუშავების პროცესის (სრული ციკლის) აღწერა** - მონაცემთა დამუშავების შემადგენელი ყველა ფორმის და ოპერაციის აღწერა (შეგროვება, მოპოვება, მათზე წვდომა, მათი ფოტოგადაღება, ვიდეომონიტორინგი ან/და აუდიომონიტორინგი, ორგანიზება, დაჯგუფება, ურთიერთდაკავშირება, შენახვა, შეცვლა, აღდგენა, გამოთხოვა, გამოყენება, დაბლოკვა, წაშლა ან განადგურება, აგრეთვე მონაცემთა გამჟღავნება მათი გადაცემით, გასაჯაროებით, გავრცელებით

[46] დოკუმენტის სარეკომენდაციო ფორმა (ნიმუში) დანართის სახით ერთვის წინამდებარე რეკომენდაციებს.

[47] იხ.პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) 31-ე მუხლის მე-3 პუნქტი; მონაცემთა დაცვის ძირითადი რეგულაცია, 30-ე მუხლის პირველი პუნქტი.

[48] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 18.

ან სხვაგვარად ხელმისაწვდომად გახდომით[49]); მათ შორის, აქვს თუ არა მონაცემთა სუბიექტს მოლოდინი, რომ მუშავდება მისი პერსონალური მონაცემები და ხდება თუ არა მონაცემთა გაზიარება მესამე პირთათვის;

დამუშავების პროცესის სრული ციკლის აღწერისას მხედველობაში უნდა იქნას მიღებული შემდეგი კომპონენტები:

- დამუშავების ბუნება, ფარგლები, კონტექსტი და მიზნები;
- პერსონალური მონაცემები, მიმღებები და პერიოდი, რომლის განმავლობაშიც შეინახება მონაცემები;
- დამუშავების ოპერაციის ფუნქციური აღწერა;
- იდენტიფიცირებული აქტივები, რომლებსაც ეყრდნობა პერსონალური მონაცემები (ტექნიკა, პროგრამული უზრუნველყოფა, ქსელები, ადამიანური რესურსი);
- ქცევის კოდექსებთან შესაბამისობის საკითხი;
- დამუშავების აუცილებლობისა და პროპორციულობის შეფასება.

- **მონაცემთა დამუშავების მასშტაბი** - აღნიშნულის მართებულად განსაზღვრის მიზნით უნდა მიექცეს ყურადღება და დოკუმენტში აისახოს ინფორმაცია იმის შესახებ, მუშავდება თუ არა არასრულწლოვანთა ან სხვა მოწყვლადი ჯგუფის მონაცემები, რა სიხშირით ხდება მონაცემთა დამუშავება და მონაცემთა დამუშავების გეოგრაფიული არეალი, ასევე, სხვა მნიშვნელოვანი ინფორმაცია, რაც ხელს შეუწყობს მონაცემთა დამუშავების მასშტაბების იდენტიფიცირებას.

- **დამუშავების სამართლებრივი საფუძველი** (კანონის მე-5 და მე-6 მუხლების მიხედვით) - აუცილებელია დამუშავების სამართლებრივი საფუძვლის მკაფიოდ იდენტიფიცირება თითოეული მონაცემისთვის და მონაცემთა შენახვის ვადის განსაზღვრა, კანონის მე-4 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტის მოთხოვნის გათვალისწინებით;

- **მონაცემთა დამუშავების მიზანი და პრინციპები** - დოკუმენტში ცხადად უნდა განიმარტოს, თუ რა კონკრეტული მიზნით ხდება მონაცემთა

[49] იხ.პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) მე-3 მუხლის „ვ“ ქვეპუნქტი

დამუშავება, დაცულია თუ არა კანონის მე-4 მუხლით დადგენილი დამუშავების პრინციპები, მათ შორის, მონაცემთა დამუშავება შესაბამისი ლეგიტიმური მიზნის პროპორციულია თუ არა;

- **ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეები და მათი ხარისხობრივი ანალიზი** - დოკუმენტში უნდა აღინიშნოს მონაცემთა დამუშავების სახე(ები) და კანონმდებლობის შესაბამისად, განხორციელდეს დამუშავების შედეგად ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის შექმნის ალბათობის შეფასება. ხსენებული საფრთხე მაღალია, თუ ერთდროულად არსებობს კანონმდებლობით განსაზღვრული[50] მინიმუმ ორი გარემოება;

- **მონაცემთა დამუშავების შედეგი** - დამუშავების შედეგად თუ იკვეთება ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის საფრთხის შექმნის მაღალი ალბათობა, ზეგავლენის შეფასების დოკუმენტში უნდა მიეთითოს მონაცემთა დამუშავების შესაძლო უარყოფითი შედეგების შესახებ;

- **ორგანიზაციულ-ტექნიკური ზომების აღწერა** - დოკუმენტში მიეთითება დამუშავებისთვის პასუხისმგებელი პირის მიერ განხორციელებული/დაგეგმილი კონკრეტული ღონისძიებები, რომლებიც მიმართულია ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეების აღმოფხვრისკენ ან/და ამცირებს მათი დადგომის მაღალ ალბათობას;

- **პერსონალურ მონაცემთა დაცვის სამსახურთან წინასწარი კონსულტაცია** - (საფრთხის მაღალი ალბათობის არსებობის შემთხვევაში, საჭიროების მიხედვით) - უნდა აღიწეროს ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეებზე რეაგირების ეტაპზე მოხდა თუ არა პერსონალურ მონაცემთა დაცვის სამსახურთან კონსულტაცია და აისახოს მიღებული კონსულტაციის შედეგი;

[50] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის ბრძანება №21 „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ“, მე-5 მუხლი.

- **ინფორმაცია ზეგავლენის შეფასების პროცესში ჩართული პირების და გამოყენებული მეთოდოლოგიის შესახებ და სხვა რელევანტური საკითხები.**

დამატებით, აღსანიშნავია, რომ შინაარსით, მასშტაბითა და კონტექსტით ერთმანეთთან დაკავშირებული მონაცემთა დამუშავების რამდენიმე პროცესის მიმართ შეიძლება მომზადდეს ზეგავლენის შეფასების ერთი (საერთო) დოკუმენტი. ***მაგალითად,*** *მუნიციპალურ ორგანოთა რამდენიმე სტრუქტურულ ერთეულს, რომლებიც იდენტური მიზნით ამონტაჟებენ ერთი და იმავე ვიდეომონიტორინგის სისტემას, ზეგავლენის შეფასების ცალ-ცალკე განხორციელების ნაცვლად, შეუძლიათ მოამზადონ ზეგავლენის შეფასების ერთიანი დოკუმენტი, რომელიც სხვადასხვა დამუშავებისთვის პასუხისმგებელი პირის მიერ დაგეგმილ მსგავს მონაცემთა დამუშავების პროცესს ერთობლივად შეაფასებს.* იგივე შეიძლება ითქვას, **მაგ.,** *რკინიგზის სისტემის ოპერატორზე, რომელსაც შეუძლია რკინიგზის ყველა სადგურზე განხორციელებული ვიდეომონიტორინგის პროცესი მოაქციოს ზეგავლენის შეფასების ერთიან დოკუმენტში.*[51]

პერსონალურ მონაცემთა დაცვის სამსახურმა, დამუშავებისთვის პასუხისმგებელ პირთათვის დახმარებისა და აღნიშნულ საკანონმდებლო სიახლესთან ადაპტირების ხელშეწყობის მიზნით, შეიმუშავა ზეგავლენის შეფასების დოკუმენტის სარეკომენდაციო ფორმა (ნიმუში), რომელიც დანართის სახით ერთვის წინამდებარე რეკომენდაციებს და ორგანიზაციის ბიზნეს პროცესების შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირებს აძლევს შესაძლებლობას იხელმძღვანელონ მის შესაბამისად, აგრეთვე, საკუთარი საჭიროების მიხედვით, მოახდინონ დოკუმენტის სარეკომენდაციო ნიმუშის ადაპტირება, შეცვალონ იგი საკუთარი შეხედულებით ან შეადგინონ ზეგავლენის შეფასების სხვაგვარი ფორმის დოკუმენტი.

5.2 ზეგავლენის შეფასების დოკუმენტის საჯაროობა და მისი შენახვის ვადები

ეროვნული კანონმდებლობის მიხედვით, ზეგავლენის შეფასების დოკუმენტის გასაჯაროების ვალდებულება რეგლამენტირებული არ არის. კანონი განსაზღვრავს იმ გარემოებებს, რომელთა არსებობის დროსაც დოკუმენტი არ ექვემდებარება გასაჯაროებას. თუ არსებობს სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესების,

[51] პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები ვიდეომონიტორინგისა და აუდიომონიტორინგის განხორციელების თაობაზე, გვ.21.

საზოგადოებრივი უსაფრთხოების ინტერესების, დანაშაულის თავიდან აცილების, ოპერატიულ-სამძებრო საქმიანობის, დანაშაულის გამოძიების, სისხლისსამართლებრივ დევნის, მართლმსაჯულების განხორციელების, პატიმრობისა და თავისუფლების აღკვეთის აღსრულების, არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის, ქვეყნისთვის მნიშვნელოვანი ფინანსური ან ეკონომიკური (მათ შორის, მონეტარული, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესების, დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის აღმატებული ლეგიტიმური ინტერესების შელახვის საფრთხე, დოკუმენტი არ ექვემდებარება გასაჯაროებას.[52]

მართალია, კანონმდებელი იმპერატიულად არ ავალდებულებს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს, საჯარო გახადონ ზეგავლენის შეფასების დოკუმენტი, თუმცა არსებობს მისი გამოქვეყნების დადებითი და მასტიმულირებელი გარემოებები, როგორიცაა მაგალითად, საზოგადოებაში მაღალი ნდობის მქონე დაწესებულების რეპუტაციის მოპოვების, კანონმდებლობასთან შესაბამისობის, ანგარიშვალდებულებისა და გამჭვირვალობის პრინციპების დაცვის დემონსტრირების ინტერესი.[53]

მონაცემთა დამუშავების ძირითადი რეგულაცია არ მიუთითებს გასაჯაროების შემზღუდველ კონკრეტულ გარემოებებზე. რეგულაციის თანახმად, დოკუმენტის გამოქვეყნება დამოკიდებულია დამუშავებისთვის პასუხისმგებელი პირის გადაწყვეტილებაზე. თუმცა, მის მიმართ სანდოობის ხარისხის გაზრდისა და კანონმდებლობის მოთხოვნებთან შესაბამისობის ხაზგასმის მიზნით, მიზანშეწონილია დოკუმენტის ძირითადი ნარატივების გამოქვეყნება ან უბრალოდ მითითება იმაზე, რომ ზეგავლენის შეფასება განხორციელებულია.[54]

რაც შეეხება დოკუმენტის შენახვის ვადებს, კანონმდებელი დამუშავებისთვის პასუხისმგებელ პირს აკისრებს ცალსახა ვალდებულებას, ზეგავლენის შეფასების

[52] იხ. პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) 31-მუხლის მე-8 პუნქტი.

[53] Data Protection Commission, Guide to Data Protection Impact Assessment (DPIAs), October 2019, 24;

[54] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 18.

დოკუმენტი შეინახოს მონაცემთა დამუშავების მთელი პერიოდის განმავლობაში, ხოლო მონაცემთა დამუშავების შეწყვეტის შემთხვევაში – არანაკლებ 1 წლის ვადით.[55]

დასკვნა

პერსონალურ მონაცემთა დაცვის ეროვნული და საერთაშორისო კანონმდებლობა, ასევე, პრეცედენტული სამართალი ცხადყოფს, რომ პერსონალურ მონაცემთა დამუშავების სფეროში არსებული გამოწვევები, ძირითადად, უკავშირდება ინფორმაციული და საკომუნიკაციო ტექნოლოგიების განვითარებას, დიდი მოცულობის პერსონალური მონაცემების დამუშავების პრაქტიკას.

მარეგულირებელი აქტების მიღებისა და საზედამხედველო ორგანოების საქმიანობის მიზანია, მონაცემთა დამუშავებისას უზრუნველყოფილ იქნას პერსონალურ მონაცემთა დაცვის სათანადო სტანდარტი. ამ კონტექსტში მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა ნათლად დაინახონ ზეგავლენის შეფასების, როგორც პრევენციული და დამუშავების პროცესში მონაცემთა უსაფრთხოების პრინციპის რეალიზაციის მექანიზმის სასარგებლო და პოზიტიური გავლენა, რომელიც შემდგომში მნიშვნელოვნად განაპირობებს მონაცემთა დამუშავების კანონიერებას.

კანონმდებლობით განსაზღვრული მავალდებულებელი გარემოებების არარსებობის შემთხვევებშიც, რეკომენდირებულია მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ, საკუთარი ინიციატივით, ზეგავლენის შეფასების განხორციელება წინმსწრებად, მონაცემთა დამუშავების დაწყებამდე, რაც მხოლოდ ხელს შეუწყობს მონაცემთა დამუშავების პროცესში მაღალი სტანდარტების დანერგვას. აღნიშნული კი, თავის მხრივ, განამტკიცებს დამუშავების პროცესის კანონიერებას.

[55] იხ. პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) 31-მუხლის მე-4 პუნქტი.

მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის სარეკომენდაციო ფორმა (ნიმუში)

წინამდებარე სარეკომენდაციო ფორმა არის ნიმუში იმისა, თუ როგორი შეიძლება იყოს (რა ინფორმაციას შეიცავდეს) მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი. ორგანიზაციის ბიზნეს პროცესების შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირებს შესაძლებლობა აქვთ იხელმძღვანელონ აღნიშნული ფორმის შესაბამისად, აგრეთვე, საკუთარი საჭიროების მიხედვით, მოახდინონ დოკუმენტის სარეკომენდაციო ნიმუშის ადაპტირება, შეცვალონ იგი საკუთარი შეხედულებით ან შეადგინონ ზეგავლენის შეფასების სხვაგვარი ფორმის დოკუმენტი.

ამასთან, დოკუმენტის შედგენისას გათვალისწინებულ უნდა იქნას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი და „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის №21 ბრძანება.

თუ დოკუმენტი ან მისი რომელიმე ნაწილი შეიცავს სახელმწიფო საიდუმლოებას მიკუთვნებულ ან კონფიდენციალურ ინფორმაციას, ან დოკუმენტში აღნიშნული ინფორმაციის გამჟღავნებამ შესაძლოა საფრთხე შეუქმნას სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესებს, საზოგადოებრივი უსაფრთხოების ინტერესებს, დანაშაულის თავიდან აცილებას, ოპერატიულ - სამძებრო საქმიანობას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას, მართლმსაჯულების განხორციელებას, პატიმრობისა და თავისუფლების აღკვეთის აღსრულებას, არასაპატიმრო სასჯელთა აღსრულებას და პრობაციას, ქვეყნისთვის მნიშვნელოვან ფინანსურ ან ეკონომიკურ (მათ შორის, მონეტარულ, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესებს, დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის აღმატებულ ლეგიტიმურ ინტერესებს, ზეგავლენის შეფასების დოკუმენტი არ ექვემდებარება გასაჯაროებას.

დამუშავებისთვის პასუხისმგებელი პირი	
სახელწოდება	
სამართლებრივი ფორმა	
მონაცემთა დაცვის ოფიცერი (არსებობის შემთხვევაში)	
საკონტაქტო პირი	

ნაწილი I - მონაცემთა დამუშავების პროცესი

მონაცემთა დამუშავების პროცესის აღწერა
როგორ ხდება მონაცემთა შეგროვება, შენახვა და წაშლა/განადგურება (დამუშავების მთლიანი ციკლის აღწერა)? აქვს თუ არა მონაცემთა სუბიექტს მოლოდინი, რომ მუშავდება მისი პერსონალური მონაცემები? ხდება თუ არა მონაცემთა გაზიარება მესამე პირთათვის?

მონაცემთა დამუშავების მასშტაბი		
მონაცემთა სახე	მონაცემთა დამუშავების საფუძველი	მონაცემთა შენახვის ვადა

მონაცემთა დამუშავების მასშტაბთან დაკავშირებული სხვა დამატებითი ინფორმაცია

მუშავდება თუ არა არასრულწლოვანთა ან სხვა მოწყვლადი ჯგუფის მონაცემები? რა სიხშირით ხდება მონაცემთა დამუშავება? მონაცემთა დამუშავების გეოგრაფიული არეალი. სხვა მნიშვნელოვანი ინფორმაცია მონაცემთა დამუშავების მასშტაბების განსასაზღვრად.

მონაცემთა დამუშავების მიზანი და პრინციპები

რა მიზნით ხდება მონაცემთა დამუშავება? დაცულია თუ არა დამუშავების პრინციპები? არის თუ არა მონაცემთა დამუშავება შესაბამისი მიზნის პროპორციული?

ნაწილი II

ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეები და მათი ხარისხობრივი ანალიზი

მონაცემთა დამუშავების სახე[1]:	
❖ დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტისთვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებს სრულად ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე;	
❖ დამუშავებისთვის პასუხისმგებელი პირი ამუშავებს დიდი რაოდენობით (საქართველოს მოსახლეობის არანაკლებ 3 პროცენტისა, რომელიც გამოითვლება მოსახლეობის აღწერის ბოლო შედეგების მიხედვით) მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემებს;	
❖ დამუშავებისთვის პასუხისმგებელი პირი ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში;	
❖ ხორციელდება 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, თანამშრომელთა 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) სისტემატური და მასშტაბური მონიტორინგი გარკვეული ელექტრონული სისტემის/ტექნოლოგიის მეშვეობით, ან ასეთი მონიტორინგი მიმდინარეობს დასაქმებულთა მიმართ;	

[1] მონაცემთა დამუშავების შედეგად ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის შექმნის ალბათობა მაღალია, როდესაც ერთდროულად არსებობს ჩამოთვლილთაგან მინიმუმ ორი გარემოება:

❖ გამოიყენება ელექტრონული პროდუქტი, რომელიც მიზნად ისახავს მომხმარებლისათვის პროდუქტის ან მომსახურების შეთავაზებას ან/და მიწოდებას და რომლის მეშვეობითაც, მუშავდება მომხმარებლის ფინანსური მონაცემები ან/და რეალურ დროში მომხმარებელთა ადგილსამყოფელის შესახებ მონაცემები;	
❖ ახალი ტექნოლოგიის დანერგვა ან ინოვაციური გამოყენება;	
❖ მონაცემთა ბაზების შედარება ან გაერთიანება, რომელიც წარმოიქმნება ორი ან მეტი სხვადასხვა მონაცემთა დამუშავების პროცესიდან, სხვადასხვა მიზნებისთვის ან/და სხვადასხვა დამუშავებისთვის პასუხიმგებელი პირის მიერ;	
❖ მონაცემთა დამუშავებას შედეგად შესაძლოა, მოჰყვეს მონაცემთა სუბიექტის დისკრიმინაცია;	
❖ მონაცემთა სუბიექტის პერსონალური მონაცემების დამუშავებას შედეგად, შესაძლოა მოჰყვეს უარი პროდუქტის ან მომსახურების შეთავაზებაზე ან მონაცემთა სუბიექტის უფლების შეზღუდვა;	
❖ მონაცემთა სუბიექტები არიან მოწყვლადი პირები, მათ შორის, დამუშავებისათვის პასუხისმგებელი პირის თანამშრომლები, სამედიცინო დაწესებულების პაციენტები, არასრულწლოვნები, შეზღუდული შესაძლებლობის მქონე პირები და სხვა.	

მონაცემთა დამუშავების შესაძლო შედეგები		მაღალი ალბათობა
❖ ვინაობის მითვისება (ე.წ. Identity Theft) ან გაყალბება		
❖ ფინანსური დანაკარგი		
❖ მონაცემთა სუბიექტის რეპუტაციის შელახვა		
❖ პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალობის დარღვევა		
❖ ფსევდონიმიზებული პერსონალური მონაცემების უკანონო გამჟღავნება		
❖ სხვა სახის მნიშვნელოვანი სოციალური ან/და ეკონომიკური ზიანი		

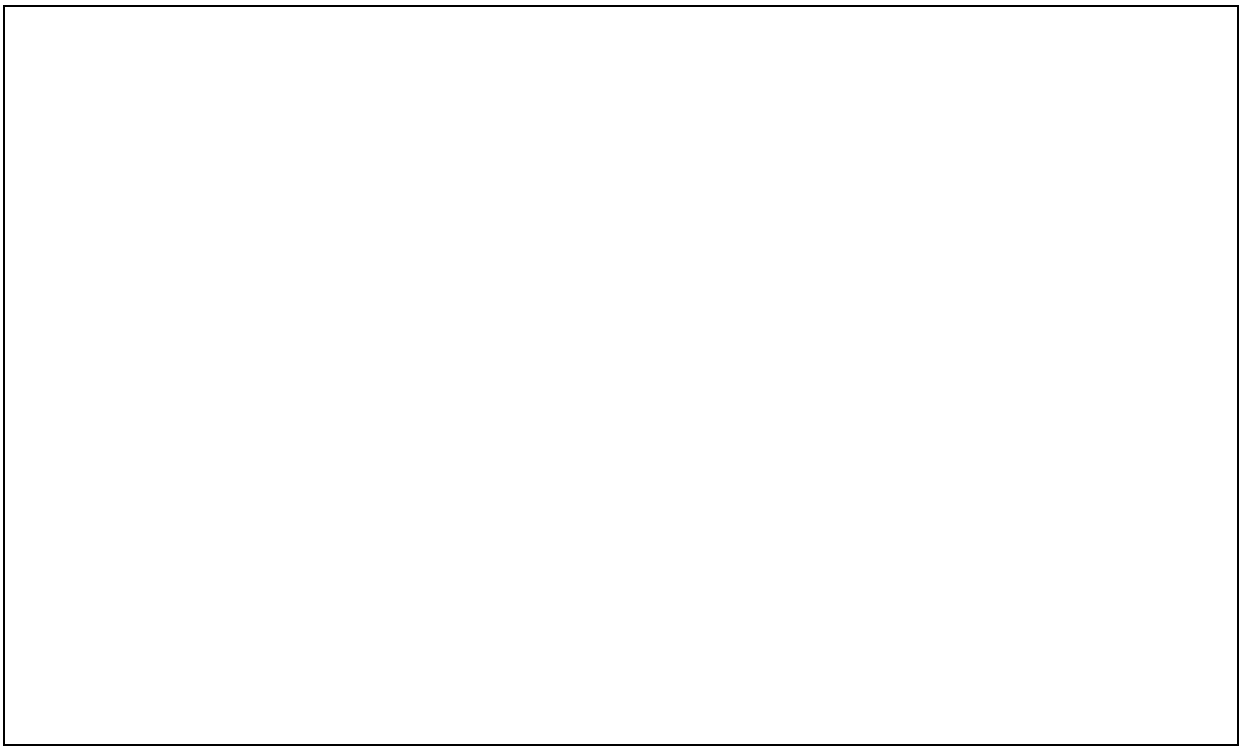
იმ შემთხვევაში, თუ საფრთხეების ხარისხობრივი ანალიზის ეტაპზე დადგინდება, რომ არსებობს ზემოაღნიშნული ერთ-ერთი შედეგის დადგომის მაღალი ალბათობა, სახეზეა პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის 31-ე მუხლის მე-5 პუნქტით გათვალიწინებული მაღალი საფრთხე და დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია საფრთხეებზე მოახდინოს რეაგირება.

საფრთხეებზე რეაგირება გულისხმობს დამუშავებისთვის პასუხისმგებელი პირის მიერ საფრთხეების შემცირებისკენ მიმართული კონკრეტული ღონისძიებების დაგეგმვასა და განხორციელებას, რაც შეიძლება ემსახურებოდეს საფრთხის შემცველი შედეგების გამორიცხვას ან/და ასეთი შედეგების დადგომის მაღალი ალბათობის შემცირებას.

ნაწილი III

საფრთხეებზე რეაგირება

ორგანიზაციულ-ტექნიკური ზომების აღწერა
დამსაქმებლისთვის პასუხისმგებელი პირის მიერ განხორციელებული/დაგეგმილი კონკრეტული ღონისძიებები, რომლებიც აღმოფხვრის ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეებს ან/და ამცირებს მათი დადგომის მაღალ ალბათობას.



პერსონალურ მონაცემთა დაცვის სამსახურთან წინასწარი კონსულტაცია (ასეთის არსებობის შემთხვევაში)

ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეებზე რეაგირების ეტაპზე მოხდა თუ არა პერსონალურ მონაცემთა დაცვის სამსახურთან კონსულტაცია? მიღებული კონსულტაციის შედეგი.

ნაწილი IV

ინფორმაცია ზეგავლენის შეფასების პროცესში ჩართული პირების, მათი მოსაზრებებისა და გამოყენებული მეთოდოლოგიის შესახებ

ზეგავლენის შეფასების პროცესში ჩართული პირები და მათი მოსაზრებები

ზეგავლენის შეფასებისას გამოყენებული მეთოდოლოგია

მიღებული გადაწყვეტილებები

ზეგავლენის შეფასების გადასინჯვის შემთხვევები