მარიკა აბაზაძე*

პერსონალურ მონაცემთა დაცვა სამეცნიერო და აკადემიური კვლევის პროცესში

საქართველოში „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის ამოქმედებით, განსაკუთრებული აქტუალობა შეიძინა მონაცემთა უსაფრთხოების დაცვის მაღალ სტანდარტსა და აკადემიური კვლევის მიზნით მონაცემთა დამუშავების ინტერესს შორის ბალანსის დაცვამ. წინამდებარე სტატია მიმოიხილავს სამეცნიერო და აკადემიური კვლევის პროცესში გასათვალისწინებელ პერსონალურ მონაცემთა დაცვის სამართლებრივ ასპექტებს.

სტატიაში განხილულია მკვლევრების მიერ ყოველდღიურ საქმიანობაში გასათვალისწინებელი საკითხები და შესაბამისი საუკეთესო პრაქტიკა.

***საკვანძო სიტყვები:** სამეცნიერო და აკადემიური კვლევა, მონაცემთა მეორეული დამუშავება, მონაცემთა სუბიექტის თანხმობის ნამდვილობა, პერსონალურ მონაცემთა უსაფრთხოების დაცვა, მონაცემთა სუბიექტის უფლებები.*

1. შესავალი

სამეცნიერო და აკადემიური კვლევის პროცესი, ხშირ შემთხვევაში, ინფორმაციის შეგროვებას და ციფრული ან მატერიალური ფორმით შენახვას ითვალისწინებს. ამ მიმართულებით მთავარი გამოწვევა პერსონალურ მონაცემთა შემცველი ინფორმაციის, მონაცემთა დაცვის კანონმდებლობის შესაბამისად გამოყენება და გაზიარებაა.

პერსონალურ მონაცემთა დაცვა მონაცემთა სუბიექტის ძირითადი უფლებაა და შესაბამისად, მისი დაცვის საკითხი აქტუალურია აკადემიური

* მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის სამართლის მაგისტრი, დუბლინის საქალაქო უნივერსიტეტი (Dublin City University (DCU)); საზოგადოებრივ საქმეთა ინსტიტუტის (GIPA) საერთაშორისო სამართლის მაგისტრი; პერსონალურ მონაცემთა დაცვის სამსახურის საერთაშორისო ურთიერთობების, ანალიტიკისა და სტრატეგიული განვითარების დეპარტამენტის მკვლევარ-ანალიტიკოსი.

კვლევის დაგეგმვის ეტაპიდანვე, კვლევის მიზნის განსაზღვრისას.[1] საგულისხმოა, რომ მონაცემთა სუბიექტის „კონფიდენციალურობა“, როგორც ცნება, სხვადასხვა კულტურისა და კონტექსტის გათვალისწინებით სხვადასხვაგვარად შეიძლება განიმარტოს,[2] აღნიშნულიდან გამომდინარე, საჭიროა მონაცემთა დამუშავების საკითხი კვლევის კონტექსტის შესაბამისად განისაზღვროს.

მნიშვნელოვანია, რომ პერსონალურ მონაცემთა დაცვის პრიზმიდან შეფასდეს კვლევის ჩატარების მეთოდოლოგიაც. მაგალითად, მონაცემთა სუბიექტებზე ფარულად დაკვირვებისას საჭიროა ცნებების „საჯარო“ და „კერძო“ განმარტებების საკვლევ კონტექსტში გააზრება. ფარულად მიმდინარე დაკვირვების ჩატარება დასაშვებია მხოლოდ მაშინ, თუ მკვლევარს ნათლად შეუძლია აჩვენოს ამ მეთოდის დადებითი მხარეები, აგრეთვე დაასაბუთოს, რომ სხვა მეთოდის გამოყენებით სასურველი შედეგის მიღწევა ძალიან რთული ან შეუძლებელია. ამავდროულად, საჭიროა მკვლევრის მიერ დასაბუთდეს, რომ ფარული დაკვირვება მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებზე უარყოფით ზეგავლენას არ მოახდენს.

პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის ვალდებულება ვრცელდება კვლევის მიზნებისა და მეთოდოლოგიის განსაზღვრის შემდგომ, კვლევის პრაქტიკულად განხორციელების ეტაპებზეც: მონაცემთა შეგროვების; მონაცემებზე ხელმისაწვდომობის; რესპონდენტთან კომუნიკაციის და ინფორმაციის შენახვის ან/და წაშლის დროს. ზოგიერთი დაწესებულების და ორგანიზაციის მონაცემთა დაცვის სტრატეგიულ დოკუმენტში მონაცემთა სწორად შენახვის და სისწორის შენარჩუნების წესები დეტალურად არის გაწერილი. აღნიშნული დოკუმენტი აერთიანებს მონაცემთა დამუშავების წესებს მონაცემთა დამუშავების სრული ციკლის გათვალისწინებით.[3]

კვლევის პროცესი, შეიძლება, ითვალისწინებდეს მონაცემთა საერთაშორისო გადაცემას. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR”) მიზნად ისახავს მონაცემთა დაცვის წესთა ჰარმონიზაციას ევროპის მასშტაბით. თუმცა, იმ შემთხვევაში, თუ მონაცემები სტატისტიკური ან აკადემიური კვლევის მიზნით მუშავდება, შესაძლებელია საკითხის მოწესრიგება დამატებითი, ეროვნული წესების შემუშავების გზით. წევრი ქვეყნების აღნიშნული დისკრეცია ევროკავშირის მასშტაბით საკითხის საკანონმდებლო რეგულირების განსხვავებებს წარმოშობს. მაგალითისთვის, სხვადასხვა წევრი ქვეყანა „სამეცნიერო კვლევას“ სხვადასხვაგვარად განმარტავს, რაც, შესაძლოა, რიგი სამართლებრივი პრობლემის საფუძველი

[1] *European University Institute*, Guide on Good Data Protection Practice in Research, 2022, 5.
[2] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 27 (2).
[3] *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021.

გახდეს, ხელი შეუშალოს მონაცემთა საერთაშორისო გადაცემის პროცესს ან საერთაშორისო კვლევით თანამშრომლობას.[4]

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ პერსონალურ მონაცემთა დამუშავებას კვლევითი მიზნებით დასაშვებად მიიჩნევს, თუ მონაცემთა სუბიექტის უფლებების დასაცავად მიღებულია უსაფრთხოების სათანადო ტექნიკური და ორგანიზაციული ზომები. აგრეთვე, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ითვალისწინებს პერსონალურ მონაცემთა დამუშავების საკანონმდებლო მოთხოვნებს.[5]

2. პერსონალურ მონაცემთა დამუშავების პრინციპები და მოქმედებები

საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ პერსონალურ მონაცემებთან მიმართებით განხორციელებული ნებისმიერი მოქმედება მონაცემთა დამუშავებად მიიჩნევა. კვლევითი პროექტების კონტექსტში, მონაცემთა დამუშავებად ჩაითვლება: რესპონდენტთა ელექტრონული ფოსტის მისამართების ნუსხის შედგენა; მონაცემთა ბაზის შექმნა და მართვა; აგრეთვე, მონაცემთა გაზიარება მესამე მხარისათვის. კანონის თანახმად, „პერსონალურ მონაცემთა დამუშავება“ განიმარტება, როგორც, ნებისმიერი მოქმედება ან მოქმედებათა ერთობლიობა პერსონალურ მონაცემთა გამოყენებით, განუსაზღვრელად დამუშავების ფორმისა და საშუალებებისა. მონაცემები შეიძლება დამუშავდეს როგორც ავტომატური, ასევე არაავტომატური საშუალებებით და სხვადასხვა მეთოდით, როგორიცაა: მონაცემთა შეგროვება; ჩაწერა; ორგანიზება; შენახვა; ადაპტაცია ან შეცვლა; მოძიება; კონსულტაცია; გამოყენება; გამჟღავნება; გადაცემა; გავრცელება ან სხვაგვარად ხელმისაწვდომობა; გასწორება ან კომბინაცია; დაბლოკვა; წაშლა ან განადგურება და სხვა.[6]

მონაცემთა სუბიექტის თანხმობა პერსონალურ მონაცემთა დამუშავებაზე სხვადასხვა სფეროში განსხვავებულ ვალდებულებებს წარმოშობს. მაგალითად, სამეცნიერო ან კლინიკური კვლევის პროცესში, მონაცემთა შეგროვების ეტაპზე, შესაძლოა, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა ვერ შეძლოს ზუსტად განსაზღვროს მონაცემთა დამუშავების მხოლოდ ერთი, კონკრეტული მიზანი.[7] რეგულაცია განმარტავს, რომ, დამუშავების სფეროსა და კონტექსტის გათვალისწინებით, მონაცემთა სუბიექტები უფლებამოსილნი არიან დაეთანხმონ პერსონალურ მონაცემთა დამუშავებას მეტად ზოგადი მიზნებისათვისაც.[8]

---

[4] *Ducato R.,* Data protection, Scientific Research, and the Role of Information, Computer Law & Security Review, Vol. 37, 2020,14.

[5] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 4(6).

[6] იქვე, 3 (ვ).

[7] *Schaar K.,* Working Paper: What is important for Data Protection in science in the future? General and Specific Changes in Data Protection for Scientific Use Resulting from the EU General Data Protection Regulation RatSWD Working Paper, No. 258, 2016, pg 6.

[8] *Chassang G.,* The Impact of the EU General Data Protection Regulation on Scientific Research, Ecancer Medical Science, 2017, <https://pubmed.ncbi.nlm.nih.gov/28144283/> [20.02.2025].

იმ შემთხვევაში, თუ საჭიროა მონაცემთა საერთაშორისო გადაცემა ან კვლევითი პროექტი ხორციელდება საერთაშორისო ორგანიზაციის ჩართულობით, რეკომენდებულია მკვლევრებმა გაითვალისწინონ და დაიცვან პერსონალურ მონაცემთა დაცვის შესაბამისი მოთხოვნები. კერძოდ, მონაცემთა დაცვის ადგილობრივი და საერთაშორისო კანონმდებლობა და სტანდარტები, საერთაშორისო ორგანიზაციის პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტით განსაზღვრული ვალდებულებები და სხვა შესაბამისი წესები. საჭიროა მკვლევრებმა მონაცემთა დამუშავების დაწყებამდე იზრუნონ სათანადო ნებართვის მიღებაზე, შესაბამისი მონაცემთა დაცვის საზედამხედველო ორგანოს ან კომიტეტის ინფორმირებაზე და შეასრულონ რიგი სხვა ვალდებულებები, რაც მათ შეიძლება ეკისრებოდეთ.[9]

მკვლევრის ვალდებულებაა უზრუნველყოს მონაცემთა სიზუსტე და ამ მიზნით პერიოდულად განაახლოს მონაცემები. აუცილებელია მონაცემთა უსაფრთხოების ზომებისა და მონაცემთა სუბიექტების უფლებების, მათ შორის მონაცემთა წაშლის - „დავიწყების უფლების დაცვა“. საჭიროა მონაცემები შენახული იქნას ისეთი ფორმით, რომელიც მონაცემთა სუბიექტების იდენტიფიცირების საშუალებას არ იძლევა და არაუმეტეს იმ დროით, რაც საჭიროა მონაცემთა შეგროვების მიზნის შესასრულებლად.[10] კვლევის დასრულების შემდგომ, შესაძლოა, საჭირო გახდეს მონაცემებზე წვდომა სათანადო ანგარიშის მოსამზადებლად, თუმცა, ამ უკანასკნელი მიზნითაც კი, მონაცემთა განუსაზღვრელი ვადით შენახვის პრაქტიკა დასაშვებად არ მიიჩნევა.[11]

კვლევის დაგეგმვის ეტაპიდანვე მნიშვნელოვანია მონაცემთა შენახვის ვადისა და წაშლის შესახებ გეგმის შემუშავება, ასევე, საჭიროებისამებრ, მონაცემთა ავტომატიზებული წაშლის ფუნქციის დამატება. სასურველია მონაცემთა შენახვის დეტალური გეგმის დასახვა, იმ ინფორმაციასთან მიმართებით, რომლის შენახვაც იგეგმება კვლევის დასრულების შემდგომ. პერსონალურ მონაცემთა შენახვის ვადა დამოკიდებულია იმ თავდაპირველ მიზანზე, რომლის მისაღწევადაც შეგროვდა მონაცემები, ან რა მიზეზითაც მონაცემები განმეორებით დამუშავდა. აქედან გამომდინარე, როდესაც პერსონალურ მონაცემთა შენახვა კვლევის მიზნებისათვის აუცილებელი აღარ არის, აუცილებელია მონაცემები წაიშალოს ან დეპერსონალიზებული ფორმით დაარქივდეს.[12]

შედარებისთვის, საერთაშორისო პრაქტიკის თანახმად, მონაცემთა დაცვის პრინციპებთან შესაბამისობის თაობაზე მტკიცების ტვირთი მკვლევრებს, კვლევით პროექტზე პასუხისმგებელ პირებს ან/და დაწესებულებებს ეკისრებათ. გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ (“ICO”) პერსონალურ მონაცემთა უსაფრთხოების

[9] პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები კონფიდენციალურობის პოლიტიკის დოკუმენტის შემუშავების თაობაზე, 2025, 11.
[10] EDPS, *Preliminary Opinion on Data Protection and Scientific Research,* 2020, 23.
[11] ICO, Guideilne on Principle of Storage Limitation, <https://ico.org.uk/> [20.02.2025].
[12] European University Institute, Guide on Good Data Protection Practice in Research, 2022.

დარღვევის მიზეზით გრინვიჩის უნივერსიტეტს ადმინისტრაციული ჯარიმა დააკისრა. დარღვევის საფუძველი სტუდენტის მიერ წამოწყებული კვლევითი პროექტი გახდა.[13] კერძოდ, აღნიშნულმა სტუდენტმა ვერ უზრუნველყო კვლევასთან დაკავშირებული გვერდის გამართვა უსაფრთხოების სათანადო ზომებით. შედეგად, ჰაკერული თავდასხმის გზით 20 000 მონაცემთა სუბიექტის განსაკუთრებული კატეგორიის პერსონალური მონაცემები არაავტორიზებულ პირთათვის გახდა ხელმისაწვდომი. აღნიშნული საქმე ხაზს უსვამს რისკების საფუძვლიანი შეფასების, მონაცემთა უსაფრთხოების პოლიტიკის დანერგვისა და პერსონალურ მონაცემთა დამუშავების წესებთან შესაბამისობის მიმართებით კონტროლის განხორციელების აუცილებლობას.

აკადემიური კვლევის მიზნებისათვის განსაკუთრებული კატეგორიის მონაცემთა დამუშავების საფუძველი, ძირითადად, მონაცემთა სუბიექტის აშკარად გამოხატული თანხმობაა. განსაკუთრებული კატეგორიის მონაცემია (მათ შორის): ინფორმაცია რასობრივი ან ეთნიკური წარმომავლობის; პოლიტიკური შეხედულებების; რელიგიური ან ფილოსოფიური მრწამსის; პროფკავშირის წევრობის; გენეტიკურ მონაცემების; ბიომეტრიულ მონაცემების; ჯანმრთელობის შესახებ მონაცემების და სექსუალური ორიენტაციის ან აქტივობის შესახებ.[14] განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავების შემთხვევაში, საჭიროა მონაცემთა დამუშავების სათანადო საფუძვლის წარდგენა შესაბამის ეთიკის კომიტეტთან. მნიშვნელოვანია, რომ კვლევითი პროექტის ფარგლებში განიმარტოს მონაცემთა შეგროვების საჭიროების შესახებ, ასევე ჩატარდეს მონაცემთა დამუშავების პროპორციულობის შეფასება. საყურადღებოა, რომ სხვადასხვა წყაროდან შეგროვებული პერსონალური მონაცემები მხოლოდ მაშინ შეიძლება გაერთიანდეს, როდესაც აღნიშნული კანონის მიერ დაშვებულია.

3. ინფორმირებული თანხმობის მიღება პერსონალურ მონაცემთა დამუშავებაზე

იმისათვის, რომ მონაცემთა დამუშავება კანონიერი იყოს, აუცილებელია მონაცემთა სუბიექტის თანხმობა პერსონალურ მონაცემთა დამუშავებაზე. პერსონალურ მონაცემთა თანხმობის გარეშე დამუშავება დასაშვებია მხოლოდ ცალკეულ შემთხვევებში: მაგალითად, როდესაც მონაცემთა დამუშავებას ინდივიდის ლეგიტიმურ ინტერესებზე უარყოფითი გავლენა არ აქვს; კვლევითი პროექტის განხორციელების საჯარო ინტერესი აღემატება მონაცემთა სუბიექტის ლეგიტიმურ ინტერესებს; კვლევის მიზანი სხვაგვარად ვერ მიიღწევა ან მისი მიღწევა შესაძლებელია მხოლოდ არაპროპორციული

[13] *Lallie H.S., Thompson A., Titis E., Stephens P.,* Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector, 2025, 20.

[14] Article 9, 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).

ძალისხმევით. თანხმობის გარეშე მონაცემთა დამუშავების კანონიერება ხშირად დამოკიდებულია კონფიდენციალურობის უფლებასა და კვლევის სარგებელს შორის ურთიერთბალანსზე.[15] საგულისხმოა, რომ ზოგიერთ სიტუაციაში, ძირითადი რეგულაციის თანახმად, დამუშავების ზუსტი მიზნების განსაზღვრის გარეშეც მონაცემთა დამუშავება შესაძლოა კანონიერი იყოს[16], მაგალითად, პანდემიის დროს, იმ პირობით, რომ დაცული იქნება კვლევის ეთიკური სტანდარტები.[17]

მონაცემთა სუბიექტს ნებისმიერ დროს აქვს თანხმობაზე უარის გაცხადების უფლება, შესაბამისი მიზეზის გაცხადების გარეშე. აგრეთვე, მისი უფლებაა დამუშავებული ინფორმაციის წაშლისა და დაბლოკვის მოთხოვნაც.[18] მკვლევარი, შეიძლება იურიდიული გამოწვევების ან პასუხისმგებლობის წინაშე აღმოჩნდეს, თუ მის მიერ მონაცემთა სუბიექტისგან მიღებული თანხმობა არ არის ნამდვილი. მონაცემთა სუბიექტის „ნამდვილი“ თანხმობა ნიშნავს ნებისმიერ თავისუფლად გაცემულ, კონკრეტულ, ინფორმირებულ და ცალსახა მითითებას პერსონალური მონაცემთა დამუშავებაზე თანხმობის შესახებ. [19]

თანხმობა ნამდვილია იმ შემთხვევაში, თუ მონაცემთა სუბიექტს გააჩნდა მონაცემთა შეგროვებასთან დაკავშირებით რეალური არჩევანის გაკეთების საშუალება. ნამდვილ თანხმობას გამორიცხავს ისეთი პრაქტიკები როგორიც არის მონაცემთა სუბიექტზე ნებისმიერი ფორმით ზემოქმედება, მათ შორის მისი შეცდომაში შეყვანა,[20] დაშინება ან იძულება. რესპონდენტის თანხმობა საჭიროა იყოს კონკრეტული, ნათლად გამოვლენილი, ზუსტად პასუხობდეს და ეთანხმებოდეს მონაცემთა დამუშავების მიზანს და შედეგებს.[21] მონაცემთა დამუშავებამდე, საჭიროა მონაცემთა სუბიექტის ინფორმირება იმის შესახებ, თუ რა ტიპის ინფორმაცია მუშავდება. სხვადასხვა დამუშავების მოქმედებათა განსახორციელებლად მონაცემთა სუბიექტისგან თანხმობის ერთხელ მიღება საკმარისია, თუ მონაცემთა სუბიექტს, გამომდინარე იმ ინფორმაციიდან რაც მან მიიღო, აქვს გონივრული მოლოდინი, რომ მისი მონაცემების გამოყენებით წინამდებარე ღონისძიებები განხორციელდება.[22]

---

[15] *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021, 26.

[16] *Malgieri G.,* Data Protection and Research: A Vital Challenge in the Era of COVID-19 Pandemic, Computer Law & Security Review, 2020, 3.

[17] Recital 33, 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).

[18] სახელმძღვანელო რეკომენდაცია 05/2020 თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით, 9.

[19] Recital 32, 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).

[20] EDPS, A Preliminary Opinion on Data Protection and Scientific Research, 2020, 19.

[21] სახელმძღვანელო რეკომენდაცია 05/2020 თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით, 21.

[22] WP29-ის სახელმძღვანელო პრინციპები ავტომატური ინდივიდუალური გადაწყვეტილების მიღების და პროფაილინგის შესახებ, 2016/679 (WP251) რეგულაციის მიზნებისთვის, პუნქტი IV.B, მე-20 და შემდგომი გვერდები.

საჭიროა კვლევის რესპონდენტებს მიეცეთ სრული და სწორი ინფორმაცია მონაცემთა დამუშავების მიზნების, დამუშავებულ მონაცემთა კატეგორიის, მეორეული დამუშავების, გადაცემის, შენახვის ვადის და მონაცემთა სუბიექტის თანამდევი უფლებების შესახებ, აგრეთვე, ინფორმაცია მონაცემთა დამუშავებაზე უარის თქმის უფლების შესახებ - მონაცემთა სუბიექტი თავისუფალია არჩევანში დაეთანხმოს ან უარი უთხრას შესაბამის პირს პერსონალურ მონაცემთა დამუშავებაზე.[23]

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებაა ამტკიცოს, რომ მონაცემთა სუბიექტი დაეთანხმა პერსონალურ მონაცემთა დამუშავებაზე და მისი პერსონალური მონაცემების გამოყენებაზე კონკრეტული კვლევასთან დაკავშირებული მიზნით.[24] ამ მიმართულებით გასათვალისწინებელი საკითხებია: სუბიექტთა ურთიერთმიმართება - როგორიცაა: ფაქტობრივი ან იურიდიული იერარქია; ეკონომიკური დამოკიდებულება მკვლევარსა და კვლევის მონაწილეს შორის; კვლევის მონაწილის მოწყვლადობა და კვლევის შედეგი პიროვნებაზე ან საზოგადოებაზე.

4. პერსონალურ მონაცემთა „მეორეული დამუშავება“

პერსონალურ მონაცემთა განმეორებით დამუშავებისას, პირველადი დამუშავების მიზნისაგან განსხვავებული მიზნით, სახეზეა მონაცემთა მეორეული დამუშავების შემთხვევა. მონაცემთა მეორეული დამუშავება უკანონოა თუ მონაცემები შეგროვდა ერთი კვლევითი პროექტისათვის და სხვა კვლევისათვის იქნა გამოყენებული, ისე, რომ მონაცემთა სუბიექტმა არ იცოდა ახალი კვლევის შესახებ და არ განუცხადებია შესაბამისი თანხმობა მონაცემთა დამუშავებაზე.[25]პერსონალურ მონაცემთა მეორეული დამუშავება კანონიერად ჩაითვლება იმ შემთხვევაში, თუ მონაცემთა პირველადი დამუშავებისას მიღებული მონაცემთა სუბიექტების თანხმობა მოიცავს ახალი კვლევის მიზნებისათვის პერსონალურ მონაცემთა დამუშავებაზე თანხმობასაც, ან ახალი კვლევის წარმოებისას მკვლევრები უზრუნველყოფენ თანხმობის მიღებას ახალი კვლევის მიზნებისათვის.[26]

მკვლევრის ვალდებულებაა მონაცემთა სუბიექტის სრულად ინფორმირება ინფორმაციის შეგროვებისას, მათ შორის, ინფორმირებული თანხმობის მნიშვნელობის შესახებ. აგრეთვე, თუ კვლევის პროცესში გამოიყენება საჯაროდ ხელმისაწვდომი ინფორმაცია, რეკომენდებულია

[23] ასევე, იხ. GDPR-ის პრეამბულა, 42-ე პუნქტი: „[...] იმისთვის, რომ თანხმობა ინფორმირებული იყოს, მონაცემთა სუბიექტისთვის, საჭიროა ცნობილი იყოს, სულ მცირე, დამუშავებისთვის პასუხისმგებელი პირის ვინაობა და მონაცემთა დამუშავების მიზანი. [...].“

[24] Article 7 and Recital 32, 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).

[25] იქვე, Recital 50.

[26] European University Institute, Guide on Good Data Protection Practice in Research, 2022, 7.

მიეთითოს შესაბამისი წყაროს შესახებ. კვლევის პროცესში, საჭიროა პერსონალურ მონაცემთა კატეგორიის სწორად განსაზღვრა და მათი სათანადოდ დაცვა. პერსონალურ მონაცემთა კატეგორიას მიეკუთვნება: (მათ შორის) მონაცემთა სუბიექტის სახელი; სახლის მისამართი; ელექტრონული ფოსტის მისამართი, გეოგრაფიული მდებარეობის შესახებ ინფორმაცია. განსაკუთრებული კატეგორიის პერსონალური მონაცემების მაგალითად კი გამოდგება ინფორმაცია, რომელიც ეხება რელიგიურ, პოლიტიკურ შეხედულებებს ან სამედიცინო მონაცემებს. მათი დამუშავებისას მეტი სიფრთხილის გამოჩენაა საჭირო, ვინაიდან აღნიშნული ინფორმაციის გამჟღავნებით მონაცემთა სუბიექტების უფლებებს შესაძლოა მეტი ზიანი მიადგეს.[27]

პერსონალურ მონაცემთა დაცვის ტექნიკური და ორგანიზაციული ზომების განსაზღვრისას მნიშვნელოვანია გამოკითხულთა ვინაობის გათვალისწინება, რადგან, მონაცემთა სუბიექტების სხვადასხვა კატეგორიის გამოკითხვის შემთხვევაში შეიძლება საჭირო გახდეს პერსონალურ მონაცემთა დაცვის სხვადასხვა ზომის გამოყენება. მაგალითისთვის, კვლევითი პროექტის გამოკითხულთა კატეგორიებია: პაციენტი, მოხალისე (გამოკითხვისთვის, სამედიცინო კვლევისთვის და ა.შ.) თანამშრომელი (მაგალითად, კვლევითი ლაბორატორიის პერსონალი), კვლევაში ჩართული სხვა მკვლევარი, არასრულწლოვანი, ბავშვი ან მოზარდი და სხვა.[28]

როდესაც მონაცემთა მეორეული დამუშავება არ ეფუძნება მონაცემთა სუბიექტის თანხმობას ან კანონის მოთხოვნას, დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია დაამუშაოს პერსონალური მონაცემები დამუშავების პირველად მიზანთან „შესაბამისობის ტესტის“ საფუძველზე. წინამდებარე ტესტის საშუალებით, შესაძლოა, დადგინდეს, თუ რამდენად შეესაბამება მონაცემთა დამუშავების ახალი მიზანი მონაცემთა დამუშავების პირველად მიზანს.[29] აღნიშნულის დასადგენად კი დამუშავებისთვის პასუხისმგებელმა პირმა საჭიროა გაითვალისწინოს კავშირი მონაცემთა დამუშავების პირველად და ახალ მიზნებს შორის, მონაცემთა შეგროვების კონტექსტი, განსაკუთრებულ კატეგორიათა დამუშავების საკითხი, დამუშავების ზეგავლენა მონაცემთა სუბიექტების უფლებებზე, და მონაცემთა დაცვის გარანტიათა შესაბამისობა[30] მათი დამუშავების რისკებთან.[31]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლით განსაზღვრულია გამონაკლისი სფეროები, რომელთა

[27] პერსონალურ მონაცემთა დაცვის სამსახური, პერსონალურ მონაცემთა დაცვის სახელმძღვანელო რეკომენდაციები მცირე და საშუალო ზომის მეწარმე სუბიექტებისათვის, 2024, 11.

[28] პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, 2024, 17.

[29] *Mészáros J., Ho Chih-hsing,* Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR, 2018,4.

[30] მუხლი 89, 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).

[31] იქვე, მუხლი 5(1).

მიზნებისათვის მონაცემთა შემდგომი დამუშავება მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებლად არ მიიჩნევა. წინამდებარე გამონაკლისთა ჩამონათვალში ექცევა მონაცემთა შემდგომი დამუშავება საჯარო ინტერესების შესაბამისად არქივირების, სამეცნიერო, ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის.[32] საყურადღებოა, რომ ამ უკანასკნელი მიზნითაც პერსონალურ მონაცემთა მეორეული დამუშავებისას, პასუხისმგებელმა პირებმა საჭიროა შეაფასონ, მონაცემთა შემდგომი დამუშავების კანონიერების საკითხი. კერძოდ, რეკომენდებულია შეფასდეს მეორეული დამუშავების მიზნის შესაბამისობა დამუშავების პირველად მიზანთან.

5. კვლევის დაგეგმვისა და განხორციელების ეტაპზე გასათვალისწინებელი საკითხები

მონაცემთა დაცვის საკანონმდებლო მოთხოვნებთან შესაბამისობის მიზნებისათვის საჭიროა დეტალურად იყოს გააზრებული ის ინფორმაცია, რასაც მკვლევარი მიაწვდის კვლევაში ჩართულ რესპონდენტს. აუცილებელია ინფორმაციის მარტივი და ადვილად გასაგები ენით მიწოდება, რათა აღნიშნულმა ინფორმაციამ მონაცემთა სუბიექტს კვლევაში მონაწილეობის შესახებ თავისუფალი არჩევანის გაკეთების საშუალება მისცეს. რესპონდენტთა ინფორმირების ერთ-ერთი მეთოდია კვლევის შესახებ წინასწარ მომზადებული საინფორმაციო ფურცლის[33] გადაცემა კვლევის მონაწილისათვის, ისევე როგორც კითხვარზე ინფორმირებული თანხმობის პროტოკოლის დართვა.[34]

მონაცემთა დამუშავების შესახებ ინფორმირების მიმართულებით მნიშვნელოვანი საკითხია რესპონდენტების გაცნობა, და მათთან პირველი კომუნიკაციის დამყარება კვლევაში ჩართვის მოთხოვნით. იმ შემთხვევაშიც კი, როდესაც რესპონდენტი ოჯახის წევრი ან მეგობარია, მნიშვნელოვანია შესაბამისი ინფორმაციის გაზიარება და მათი თანხმობის მიღება პერსონალური მონაცემების დამუშავების თაობაზე. თუ პიროვნებას არ შეუძლია დაეთანხმოს მონაცემთა დამუშავებაზე, მაგალითად, არასრულწლოვანების გამო, აუცილებელია თანხმობის მიღება მათი მშობლების, მეურვის ან სხვა კანონიერი წარმომადგენლისაგან.

იმ შემთხვევაში, თუ კვლევა მოიცავს საველე სამუშაოს, ინფორმირებული თანხმობის მიღება შეიძლება არა ერთჯერადი, არამედ განგრძობითი პროცესი გახდეს, რომელიც, შესაძლოა განსხვავდებოდეს, კვლევის დაწყებამდე დაგეგმილ პროცესთან. დასაშვებია, მკვლევარს მოუხდეს თანხმობის შესახებ ხელახალი მოლაპარაკების წარმოება, იმ შემთხვევაში,

[32] პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, 2024,17.

[33] *Katulic T., Katulic A.,* GDPR and the Reuse of Personal Data in Scientific Research, International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, 1311-1316.

[34] European University Institute, Guide on Good Data Protection Practice in Research, 2022, 15.

თუ აღმოჩნდა, რომ კვლევის პროცესში წინასწარ განუსაზღვრელი, ახალი საკითხები წარმოიშვა. ასევე, იმ შემთხვევაში, თუ ინტერვიუს ჩატარების ან კითხვარის შევსების დროს საჭირო გახდა დამატებითი ინფორმაციის გაცემა ან მიღება. საუბრის დასაწყისშივე, რეკომენდებულია რესპონდენტებს მიეწოდოთ ინფორმაცია იმ გამონაკლისების შესახებ, რასაც გულისხმობს ინფორმირებული თანხმობის მიღება. საჭიროა მონაცემთა სუბიექტებს ეცნობოთ, რომ შეიძლება საჭირო გახდეს თანხმობის შესახებ ხელახალი მოლაპარაკება, საუბრის მიმდინარეობიდან, ან განხილული თემატიკიდან წარმოშობილი საჭიროებებიდან გამომდინარე.

საჭიროა გამოსაკითხ საზოგადოებაში დამკვიდრებული კულტურული და ეთიკური ნორმების მხედველობაში მიღება. წერილობითი თანხმობა შეიძლება ეწინააღმდეგებოდეს რესპონდენტთა ეთიკურ ნორმებს, ან რესპონდენტთაგან თანხმობის მიღება შეუძლებელი აღმოჩნდეს სხვა მიზეზით. აღნიშნულ შემთხვევაში, რეკომენდებულია ალტერნატიული თანხმობის მექანიზმების შეთავაზება, როგორიცაა, მაგალითად, ვერბალური თანხმობის ჩანაწერის მომზადება ან მოწმის დასწრება. ნებისმიერი მეთოდის არჩევის შემთხვევაში, აუცილებელია გამოყენებული პროცედურის შესახებ შესაბამისი დოკუმენტების წარმოება. ისეთ შემთხვევაში, როდესაც რესპონდენტს არ შეუძლია საკუთარი სურვილის ნათლად გამოხატვა ან ინფორმაციის სათანადოდ გაგება, საჭიროა ინფორმირებული თანხმობა სხვა შესაბამისი საშუალებით ჩანაცვლდეს.

დაკვირვებითი კვლევის შემთხვევაში, კვლევის დაწყებამდე საჭიროა მიღებულ იქნას ინფორმირებული თანხმობა როგორც მონაცემთა სუბიექტთაგან, ასევე სხვა ზედამხედველი, მეურვე ან პასუხისმგებელი პირებისგან. საჯარო სივრცეში ადამიანებზე დაკვირვება, შესაძლოა, არ სჭირდებოდეს თანხმობის მიღებას. ამ მოცემულობაში, მკვლევრებს ევალებათ დაამტკიცონ, რომ მათ მიერ ჩატარებული კვლევა არ შეცვლის ან მოახდენს ნეგატიურ ზემოქმედებას ადამიანების ქცევაზე, და არ შელახავს მათი კონფიდენციალურობის უფლებას. აუცილებელია კვლევის ფარგლებში მონაცემთა დამუშავების შესახებ ბავშვთა ინფორმირების კუთხით შემუშავდეს სტრატეგია მათთვის მარტივად გასაგები მეთოდების გამოყენებით, მაგალითად, აუდიო ან ვიდეო მასალის გამოყენებით, ან ბავშვისთვის მარტივად აღსაქმელი საინფორმაციო ბროშურების მომზადების გზით.[35]

კიდევ ერთი საკვანძო საკითხია მკვლევრის უფლებამოსილება პერსონალურ მონაცემთა დამუშავების მიმართულებით. თუ მონაცემები განმეორებით მუშავდება, რომელიც პირველად სხვა კვლევისათვის დამუშავდა, საჭიროა პირველი კვლევის ჩატარებისას მიღებული თანხმობის მიღება განმეორებით, ახალი კვლევის მიზნებისათვის. როდესაც არსებობს სხვა კვლევითი პროექტისათვის შექმნილი მონაცემთა ბაზა, მნიშვნელოვანია გათვალისწინებულ იქნას სხვადასხვა საკითხი. მაგალითად, ვრცელდება თუ არა განმეორებით მონაცემთა დამუშავებაზე პირველად მიღებული

[35] იქვე.

მონაცემთა სუბიექტის ინფორმირებული თანხმობა. აღნიშნულ საკითხებზე კონსულტაციის გაწევა კომპანიის ან დაწესებულების ეთიკის კომისიის, მონაცემთა დაცვის ოფიცრის, ან პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს კომპეტენციაა.

6. მონაცემთა უსაფრთხოება

პერსონალურ მონაცემთა უსაფრთხოდ დამუშავების მიზნით, აუცილებელია სათანადო ტექნიკური და ორგანიზაციული ზომების მიღება, რათა თავიდან იქნას არიდებული არაავტორიზებული წვდომა პერსონალურ მონაცემებზე. [36]აკადემიური და სამეცნიერო კვლევის პროცესში, მონაცემთა უსაფრთხოების დაცვის პრაქტიკული მეთოდი შეიძლება იყოს, მაგალითად, ჩანაწერების წარმოება წვდომის თაობაზე, რაც ცნობილია როგორც ინფორმაციის „ლოგირება“ და მიანიშნებს იმაზე თუ ვინ, როდის და რა ინფორმაციაზე განახორციელა წვდომა. ასევე, შესაძლოა კვლევის კონტექსტიდან გამომდინარე მონაცემების დასაცავად გამოყენებული იქნას სხვა შემდეგი მიდგომები: მომხმარებლის იდენტობის გადამოწმება ავტორიზაციის გზით; ელექტრონული ფაილების დაცვა პაროლებით (მაგალითად, პაროლით დაცული დოკუმენტის შენახვა); მონაცემთა ბაზის დაშიფვრა ანუ, მონაცემთა ისეთი ფორმით შენახვა, რომელიც გაუგებარს ხდის მას, და იგი გასაგები ხდება მხოლოდ ავტორიზებული პირისთვის, რომელსაც აქვს ე.წ. „გასაღები“ (პაროლი, რომლის საშუალებითაც ინფორმაცია კვლავ გახდება გასაგები).

მიუხედავად მონაცემთა შენახვის ადგილისა, კანონის მოთხოვნები მონაცემთა დაცვის მიმართულებით (იქნება ეს პერსონალური კომპიუტერი, მეხსიერების ბარათი, თუ „ქლაუდ“ ტექნოლოგია) თანაბრად ვრცელდება. საჭიროა პერსონალურ მონაცემებზე უსაფრთხო წვდომის წესი ნათლად ჩამოყალიბდეს და პერიოდულად განახლდეს და იყოს პროპორციული მოსალოდნელ უსაფრთხოების რისკებთან და დამუშავებულ მონაცემთა კატეგორიასთან. მაგალითად, განსაკუთრებული კატეგორიის მონაცემი, დაუცველი რესპონდენტი ან/და მკვლევარი შესაძლოა სხვა რესპონდენტებთან შედარებით მაღალი ხარისხის დაცვას საჭიროებდეს, მონაცემთა დამუშავების კონტექსტიდან და თანამდევი რისკებიდან გამომდინარე. რეკომენდებულია აღნიშნული დოკუმენტი, რომელშიც გაწერილი იქნება დამუშავებულ მონაცემებზე წვდომის წესი, მოიცავდეს ინფორმაციას გამოყენებულ დაცვის საშუალებებზე, მაგალითად, დაშიფვრა, დამცავი პაროლის გამოყენება და სხვა შესაბამისი საშუალებები.[37]

[36] *EDPS,* Preliminary Opinion on Data Protection and Scientific Research, 2020, 24.

[37]Article 4(13), (14) and (15) andArticle 9 and Recitals (51) to (56), 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).

არაავტორიზებული წვდომისაგან დაცვის მიზნით შესაძლოა საჭირო გახდეს მონაცემთა განცალკევება სხვა ინფორმაციისაგან. აღნიშნულის მაგალითია მონაცემთა ბაზების დაყოფა, რათა მონაცემთა სუბიექტების იდენტიფიცირება შეუძლებელი გახდეს არაავტორიზებულ პირთათვის. შეიძლება, განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა სხვა პერსონალური მონაცემებისაგან დამოუკიდებლად შენახვა მათი დაცვის მიზნით. ასევე, შესაძლებელია საჭირო გახდეს სამოქმედო გეგმის შემუშავება იმ მონაცემებთან დაკავშირებით, რომელთა შეგროვებაც წინასწარ არ იყო განსაზღვრული და მკვლევრისთვის ხელმისაწვდომი გახდა დაუგეგმავად, კვლევის პროცესში.

მონაცემთა გადაცემისას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია შეაფასოს მონაცემთა მიმღების პერსონალურ მონაცემთა დაცვის სისტემის ადეკვატურობა. მნიშვნელოვანია კვლევის მონაწილეებმა იცოდნენ იქნება თუ არა მათი მონაცემები გადაცემული მესამე ქვეყნებში. მონაცემთა დამუშავებაზე პასუხისმგებელმა პირმა შესაძლოა ვერბალურად აუხსნას მონაცემთა სუბიექტს მონაცემთა საერთაშორისო გადაცემის საკითხი. უკანასკნელ შემთხვევაში რთულდება მონაცემთა სუბიექტის მიერ გაცემული თანხმობის დოკუმენტებში ასახვა ან/და მტკიცებულების წარმოდგენა მიღებული თანხმობის თაობაზე. შესაძლებელია მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა შეიმუშაოს წერილობითი დოკუმენტი, რომელშიც ასახულია რესპონდენტთა თანხმობა პერსონალურ მონაცემთა დამუშავების შესახებ. საჭიროა მონაცემთა დაცვის ხარისხის შეფასება მესამე ქვეყანაში, სადაც იგეგმება ინფორმაციის გადაცემა, იმ მონაცემთა გადაცემის მეთოდების გათვალისწინებით, რა მეთოდებითაც იგეგმება ინფორმაციის გადაცემა. [38] სხვა სახელმწიფოში ან/და საერთაშორისო ორგანიზაციაში მონაცემთა დაცვის სათანადო გარანტიების არსებობას აფასებს და მის შესახებ გადაწყვეტილებას იღებს პერსონალურ მონაცემთა დაცვის სამსახური მონაცემთა დამუშავების მომწესრიგებელი კანონმდებლობისა და პრაქტიკის ანალიზის საფუძველზე.[39]

პერსონალურ მონაცემთა უსაფრთხოების დაცვის კუთხით სასარგებლო ინსტრუმენტია მონაცემთა დეპერსონალიზაცია, ვინაიდან იგი იძლევა კვლევათა ჩატარების შესაძლებლობას, რომელთა განხორციელება შეუძლებელი იქნებოდა მათი კონფიდენციალურობის მიზეზით.[40] პერსონალურ მონაცემთა დეპერსონალიზაცია გულისხმობს პირდაპირი იდენტიფიცირების ისეთი საშუალებების ამოღებას ტექსტიდან, როგორიცაა მონაცემთა სუბიექტის სახელი, დაბადების თარიღი, ან მისამართი, თუმცა, ამ გზით სრულად ვერ გამოირიცხება მონაცემთა სუბიექტთა რეიდენტიფიცირების შესაძლებლობა. საყურადღებოა, რომ პირდაპირი იდენტიფიკატორების მოშორება ტექსტიდან, ავტომატურად არ ნიშნავს რომ

[38] *ცაგარეიშვილი ნ.,* პერსონალურ მონაცემთა საერთაშორისო გადაცემის სამართლებრივი მოწესრიგება (საერთაშორისო და ეროვნული სტანდარტები), პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, 1/2024, 84.

[39] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 42.

[40] რეკომენდაციები პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ, 2024, 27.

მონაცემთა სუბიექტთა რეიდენტიფიცირება შეუძლებელია, ვინაიდან, არსებობს მათი რეიდენტიფიცირების შანსი სხვადასხვა ინფორმაციის გაერთიანების გზით.[41]

დეპერსონალიზაციის ხშირად გამოყენებული მეთოდია შემთხვევითი შერჩევის პრინციპი, რაც გულისხმობს მონაცემთა სუბიექტსა და ინფორმაციას შორის კავშირის წაშლას. თუ მონაცემები საკმარისად გაურკვევლად არის წარმოდგენილი, იგი ვეღარ დაუკავშირდება პიროვნებას.[42] დეპერსონალიზაციის ერთ-ერთი პრინციპია განზოგადება.[43] განზოგადების მიდგომის გამოყენებით ნაკლებია მონაცემთა იდენტიფიკაციის შანსი. მონაცემთა განზოგადების მაგალითად შესაძლოა მოვიყვანოთ მონაცემთა სუბიექტის საცხოვრებელი ქალაქის ან დაბის ნაცვლად, მიეთითოს რეგიონი, მეტად განზოგადებული გეოგრაფიული მდებარეობის ერთეული. ასევე, რესპონდენტის კონკრეტული ასაკის მითითების ნაცვლად, მინიშნება გაკეთდეს ასაკობრივ ჯგუფზე რომელშიც რესპონდენტი მოექცევა. საყურადღებოა, რომ მონაცემთა სუბიექტის ხელახალ იდენტიფიცირებასთან დაკავშირებული ყველა პრობლემის გადაწყვეტის საშუალებად არც ეს მეთოდი გამოდგება, ამიტომაც, სასურველია მონაცემთა დამუშავების კონკრეტულ კონტექსტზე მორგებული მონაცემთა დაცვის მეთოდის შერჩევა.

პერსონალურ მონაცემთა მინიმიზაციისა და უსაფრთხოების პრინციპების გათვალისწინება კვლევის ეთიკის მნიშვნელოვანი საკითხებია. მაგალითისთვის, შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ უმეას უნივერსიტეტის დაჯარიმების საქმე წარმოაჩენს პერსონალურ მონაცემთა უსაფრთხოების სათანადო ტექნიკური და ორგანიზაციული ზომების გატარების მნიშვნელობას. უნივერსიტეტი განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა უსაფრთხოების წესების გათვალისწინების გარეშე ღრუბლოვან პლატფორმაზე შენახვის გამო დაჯარიმდა. აღნიშნულმა გადაწყვეტილებამ გამოკვეთა მკვლევრების ვალდებულება, განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავებისას უზრუნველყოს მონაცემთა დაცვის შესაბამისი მექანიზმების გამოყენება, როგორიცაა, მაგალითად, პერსონალურ მონაცემთა დაშიფვრა ან ანონიმიზაცია.[44]

კვლევის პროცესში დამუშავებული პერსონალური მონაცემების შემცველი ინფორმაციის დასაცავად კიდევ ერთი საშუალებაა პერსონალურ მონაცემთა ფსევდონიმიზაცია,[45] რომელიც გულისხმობს უნიკალური მახასიათებლების ჩანაცვლებას სხვა მახასიათებლით, მაგალითად, კოდით.[46] იმ შემთხვევაში, თუ ინფორმაციას მესამე პირი ინახავს ან ან იგი შენახულია

[41] იქვე, მუხლი 3(ც).
[42] AEPD, 10 Misunderstandings relating to Anonymisation, 2021, 5.
[43] Article 29 WP Opinion on Anonymisation Techniques, 2014.
[44] Decision of the DPA (Sweden), DI-2019-9432, 2020, <https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-9432> [24.02.2025].
[45] *Manis M. L.,* The Processing of Personal Data in the Context of Scientific Research, The New Regime under the EU-GDPR, BioLaw Journal, 3/2017, 344.
[46] EDPB Guidelines 01/2025 on Pseudonymisation, 2025, 36.

„ქლაუდ“ სისტემაში, საჭიროა გადამოწმდეს, რომ აღნიშნული მონაცემები უსაფრთხოდ წაიშალა. აგრეთვე, როდესაც, ინფორმაცია გადაიცა მესამე პირთან, რეკომენდებულია გადამოწმდეს, რომ მათ წინამდებარე ინფორმაცია დასახული მონაცემთა დამუშავების მიზნის შესრულების შემდგომ წაიშალა.

7. დასკვნა

„პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის ამოქმედებით მონაცემთა უსაფრთხოების მაღალი სტანდარტის დაცვისა და კვლევითი ინტერესების დაბალანსების საკითხმა განსაკუთრებული მნიშვნელობა შეიძინა. ამ მოცემულობაში, მკვლევრებს წარმოეშობათ მტკიცების ტვირთი იმის შესახებ, რომ იცავენ მონაცემთა დამუშავების კანონით განსაზღვრულ მოთხოვნებს როგორც კვლევის დაგეგმვის, ასევე მისი განხორციელების ყველა ეტაპზე.

მონაცემთა სუბიექტის კონფიდენციალურობის პატივისცემა და მისგან ინფორმირებული თანხმობის მიღება კვლევის პროცესის განუყოფელი ნაწილია. აკადემიურ და სამეცნიერო კვლევის პროცესში ხშირია მონაცემთა მეორეული დამუშავება, რაც გულისხმობს მონაცემთა გამოყენებას სხვა მიზნებისთვის, გარდა თავდაპირველად განსაზღვრულისა. ასეთ შემთხვევაში, საჭიროა მონაცემთა სუბიექტისაგან ახალი თანხმობის მიღება ან კანონით განსაზღვრული საფუძვლის არსებობა.

აუცილებელია პერსონალური მონაცემები დამუშავდეს მონაცემთა დამუშავების ძირითადი პრინციპების გათვალისწინებით; კანონიერად და გამჭვირვალედ; შეგროვდეს კონკრეტული, ნათელი და ლეგიტიმური მიზნების მისაღწევად, იყოს ზუსტი და საჭიროების შემთხვევაში განახლებული, ინახებოდეს იმ ფორმით, რომელიც იძლევა მონაცემთა სუბიექტის იდენტიფიცირების საშუალებას არაუმეტეს იმ დროისა, რაც საჭიროა დამუშავების მიზნებისთვის და იქნას მიღებული შესაბამისი ტექნიკური და ორგანიზაციული ზომები მონაცემთა უსაფრთხოების უზრუნველსაყოფად. განსაკუთრებული კატეგორიის მონაცემთა (მაგალითად, ჯანმრთელობის, ან/და რელიგიური შეხედულებების შესახებ ინფორმაციის) დამუშავებისას რეკომენდებულია დამატებითი სიფრთხილის გამოჩენა და მონაცემთა სუბიექტისაგან გამოხატული თანხმობის მიღება.

პერსონალურ მონაცემთა უსაფრთხოების უზრუნველსაყოფად აუცილებელია ტექნიკური და ორგანიზაციული ზომების მიღება, როგორიცაა მონაცემების დაშიფვრა, პაროლებით დაცვა და წვდომის კონტროლი. ასევე, მნიშვნელოვანია მონაცემთა დეპერსონალიზაცია ან ფსევდონიმიზაცია, რათა შემცირდეს მონაცემთა სუბიექტის იდენტიფიცირების რისკი.

პერსონალურ მონაცემთა დამუშავების პრინციპების დაცვა სამეცნიერო და აკადემიურ კვლევათა წარმოების მიზნით არა მხოლოდ სამართლებრივი ვალდებულება, არამედ ეთიკური პასუხისმგებლობაც არის, რომელიც მონაცემთა სუბიექტების უფლებების პატივისცემას და კვლევის სანდოობას უზრუნველყოფს.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Aata, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.
3. პერსონალურ მონაცემთა დაცვის სამსახური, რეკომენდაციები პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ, 2024, 7.
4. პერსონალურ მონაცემთა დაცვის სამსახური, პერსონალურ მონაცემთა დაცვის სახელმძღვანელო რეკომენდაციები მცირე და საშუალო ზომის მეწარმე სუბიექტებისათვის, 2024, 11.
5. პერსონალურ მონაცემთა დაცვის სამსახური, რეკომენდაციები კონფიდენციალურობის პოლიტიკის დოკუმენტის შემუშავების თაობაზე, 2025.
6. სახელმძღვანელო რეკომენდაცია 05/2020 თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით.
7. *ცაგარეიშვილი ნ.,* პერსონალურ მონაცემთა საერთაშორისო გადაცემის სამართლებრივი მოწესრიგება (საერთაშორისო და ეროვნული სტანდარტები), პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი, №1, 2024.
8. 29-ე სამუშაო ჯგუფის სახელმძღვანელო პრინციპები ავტომატური ინდივიდუალური გადაწყვეტილების მიღების და პროფაილინგის შესახებ, 2016/679 (WP251) რეგულაციის მიზნებისთვის.
9. *Chassang G.,* The Impact of the EU General Data Protection Regulation on Scientific Research, Ecancer Medical Science, 2017, <https://pubmed.ncbi.nlm.nih.gov/28144283/> [20.02.2025].
10. *Ducato R.,* Data protection, Scientific Research, and the Role of Information, Computer Law & Security Review, Vol. 37, 2020.
11. EDPB Guidelines 01/2025 on Pseudonymisation, 2025.
12. EDPS, Preliminary Opinion on Data Protection and Scientific Research, 2020.
13. European University Institute, Guide on Good Data Protection Practice in Research, 2022.
14. ICO, Guideline on Principle of Storage Limitation, <https://ico.org.uk/> [20.02.2025].
15. *Katulic T., Katulic A.,* GDPR and the Reuse of Personal Data in Scientific Research, International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018.
16. *Lallie H.S., Thompson A., Titis E., Stephens P.,* Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector, 2025, 20.

17. *Manis M. L.,* The Processing of Personal Data in the Context of Scientific Research, The New Regime under the EU-GDPR, BioLaw Journal, 3/2017.
18. *Malgieri G.,* Data Protection and Research: A Vital Challenge in the Era of COVID-19 Pandemic, Computer Law & Security Review, 2020.
19. *Mészáros J., Ho Chih-hsing,* Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR, 2018.
20. *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021.
21. *Schaar K.,* Working Paper: What is important for Data Protection in science in the future? General and Specific Changes in Data Protection for Scientific Use Resulting from the EU General Data Protection Regulation RatSWD Working Paper, No. 258, 2016.
22. Decision of the DPA (Sweden), 2020, <https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-9432> [24.02.2025].