წინათქმა

საქართველოს საერთაშორისო უნივერსიტეტის (ჯიუ) ინტერდისციპლინური სამეცნიერო ჟურნალის მე-3 ტომის პირველი ნომერი აერთიანებს კვლევებს სამართლის, ეკონომიკის, ბიზნესის, სოციალური და ჰუმანიტარული მეცნიერებების სფეროებში. ნომერში წარმოდგენილია ჟურნალის სამიზნე პროფილის შესაბამისი, ინტერდისციპლინური ხასიათის ნაშრომები.

ნაშრომების მნიშვნელოვანი ნაწილი შეეხება ხელოვნური ინტელექტის გავლენას სხვადასხვა სფეროზე, ეკონომიკურ ზრდასა და ბიზნეს-ინოვაციებზე, შრომის ბაზარსა და სამუშაო ადგილების ტრანსფორმაციაზე, მედიაინდუსტრიასა და კრიზისების მართვაზე, ბიზნესის ადმინისტრირებასა და მეორე ენის სწავლებას. ნომერში ასევე შესულია კვლევები პერსონალურ მონაცემთა დაცვის, ციფრული მარკეტინგის, ენისა და მეტყველების სოციალური ფენომენისა და პოლიტიკური პროცესების შესახებ.

წინამდებარე ნომერი ასახავს ქართველი ავტორების, მათ შორის ახალგაზრდა მკვლევართა, კვლევით შედეგებს და მიზნად ისახავს დარგთაშორისი აკადემიური დისკუსიის გაღრმავებას.

Preface

Volume 3, Issue 1 of the GIU Interdisciplinary Scientific Journal brings together research in law, economics, business, social sciences, and the humanities. The issue presents interdisciplinary papers consistent with the journal's target scope.

A significant part of the papers addresses the impact of artificial intelligence across several fields — economic growth and business innovation, the labor market and job transformation, the media industry and crisis management, business administration, and second language acquisition. The issue also includes research on personal data protection, digital marketing, language and speech as a social phenomenon, and political processes.

This issue reflects the research results of Georgian authors, including early-career researchers, and aims to further deepen interdisciplinary academic discussion.

პერსონალურ მონაცემთა დაცვა უმაღლეს საგანმანათლებლო დაწესებულებებში: არსებული რეგულაცია და გამოწვევები

Personal Data Protection in Higher Education Institutions: Existing Regulation and Challenges[1]

თათია დოლიძე Tatia Dolidze
აფილირებული პროფესორი, საქართველოს საერთაშორისო უნივერსიტეტი ჯიუ
Affiliated Professor, Georgian International University (GIU)
tatuli.dolidze@giu.edu.ge
ნინო ბოჭორიშვილი Nino Botchorishvili
აფილირებული პროფესორი, საქართველოს საერთაშორისო უნივერსიტეტი ჯიუ
Affiliated Professor; Georgian International University (GIU)
nino.botchorishvili@giu.edu.ge
ლიკა საჯაია Lika Sajaia
პროფესორი, საქართველოს საერთაშორისო უნივერსიტეტი ჯიუ
Professor, Georgian International University (GIU)
lika.sajaia@giu.edu.ge
https://doi.org/10.61950/giu.3.2025.12104

აბსტრაქტი

სტატია იკვლევს პერსონალურ მონაცემთა დაცვის სამართლებრივ და პრაქტიკულ ჩარჩოს საქართველოს უმაღლეს საგანმანათლებლო დაწესებულებებში და მის შესაბამისობას ევროპულ სტანდარტებთან, განსაკუთრებით GDPR-თან. თეორიულად, ნაშრომი აყალიბებს მონაცემთა დაცვის კონცეპტუალურ საფუძვლებს (ფუნდამენტური უფლება, ღირსებასთან კავშირი, პრინციპები), ემპირიულად კი აანალიზებს უნივერსიტეტების შიდა დოკუმენტაციას პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით და მიმდინარე პრაქტიკას (მონაცემთა სუბიექტის თანხმობის კანონით დადგენილი სტანდარტები, შენახვის ვადები, უსაფრთხოების ზომები, მონაცემების გადაცემა და აშ). შედარებით-სამართლებრივი მიდგომით განიხილულია გერმანიის, პოლონეთისა და ესტონეთის მაგალითები და გამოვლენილია მსგავსებები/განსხვავებები საქართველოს რეგულაციებთან.

კვლევა ასკვნის, რომ მიუხედავად "პერსონალურ მონაცემთა დაცვის შესახებ" 2023 წლის 14 ივნისი კანონის ჰარმონიზაციისა მონაცემთა დაცვის ევროპულ რეგულაციასთან, უნივერსიტეტებში რჩება სისტემური ხარვეზები: თანხმობის ფორმალიზებული მართვა, DPO-ის ინსტიტუციური სისუსტე, მონაცემთა უსაფრთხოების პროტოკოლების არასრულობა,

[1] *კვლევითი ნაშრომი დამუშავებულია საქართველოს საერთაშორისო უნივერსიტეტი ჯიუ-ს 2025 წლის მიზნობრივი სამეცნიერო-კვლევითი საგრანტო პროექტის* ***„პერსონალური მონაცემთა დაცვა უმაღლეს საგანმანათლებლო დაწესებულებებში"*** *ფარგლებში.*

სტუდენტთა ინფორმაციაზე ხელმისაწვდომობის რეგულირება, ცნობიერების დაბალი დონე და აკადემიურ თავისუფლებასთან დაკავშირებით არსებული გამოწვევები.

რეკომენდაციებია: პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული შიდა დოკუმენტაციები დეტალური გაწერა და მონაცემთა სუბიექტისთვის გამჭვირვალობა; პერსონალისა და სტუდენტების ცნობიერების ამაღლება, მათ შორის რეგულარული ტრენინგებით, DPO-ის დამოუკიდებლობისა და რესურსების გაძლიერება, შიდა რეგულაციების ჰარმონიზაცია GDPR-ის პრინციპებთან და ტექნიკური სტანდარტების (ISO 27001/27701) დანერგვა. ეს ნაბიჯები გააძლიერებს პასუხისმგებლობისა და ნდობის კულტურას საუნივერსიტეტო სივრცეში და წაახალისებს საქართველოს ინტეგრაციას ევროპულ საგანმანათლებლო ეკოსისტემაში.

საკვანძო სიტყვები: უნივერსიტეტი, დამუშავება, ინფორმაცია

Abstract

This article investigates the legal and practical framework of personal data protection in Georgian higher education institutions and evaluates its alignment with European standards, particularly the GDPR. Theoretically, the study establishes the conceptual foundations of data protection, including fundamental rights, the connection to human dignity, and core principles. Empirically, it analyzes universities' internal documentation concerning personal data processing and examines current practices, including the standards for obtaining data subject consent, data retention periods, security measures, and data transfers. From a comparative-legal perspective, the study explores examples from Germany, Poland, and Estonia, highlighting similarities and differences with Georgian regulations.

The findings indicate that, despite the harmonization of Georgia's "Law on Personal Data Protection" (14 June 2023) with European data protection standards, systemic challenges persist within universities. These include formalized consent management, institutional weaknesses of the Data Protection Officer (DPO), incomplete data security protocols, insufficient regulation of access to student information, low awareness among staff and students, and issues related to academic freedom.

Based on these findings, the study recommends: the comprehensive elaboration of internal documentation related to personal data processing and ensuring transparency for data subjects; raising awareness among staff and students through regular training; strengthening the independence and resources of the DPO; harmonizing internal policies with GDPR principles; and implementing recognized technical standards (ISO 27001/27701). Collectively, these measures are expected to enhance a culture of accountability and trust within the university environment and facilitate Georgia's integration into the European higher education ecosystem.

Keywords: university, data processing, information

კვლევითი ნაშრომი დამუშავებულია საქართველოს საერთაშორისო უნივერსიტეტი ჯიუ-ს მიზნობრივი სამეცნიერო-კვლევითი პროექტის საგრანტო კონკურსის პროექტის „პერსონალური მონაცემთა დაცვა უმაღლეს საგანმანათლებლო დაწესებულებებში“ ფარგლებში.

კვლევის აქტუალობა:

თანამედროვე ეპოქაში, ინფორმაციული ტექნოლოგიებისა და ციფრული სისტემების სწრაფი განვითარების გამო, არსებითად გაიზარდა პერსონალური მონაცემების დამუშავების მასშტაბი და სიხშირე. აღნიშნული პრაქტიკულად შეეხო ყველა სფეროს, როგორც კერძო ისე საჯარო სექტორს. არც საგანმანათლებლო სფეროა ამ მხრივ გამონაკლისი და გადაჭარბებული არ იქნება თუ ვიტყვით, რომ ამ სფეროში პერსონალურ მონაცემთა დაცვის საკითხი ერთ ერთი დიდი გამოწვევაა, რადგან უნივერსიტეტები პრაქტიკულად ყოველდღიურ რეჟიმში ამუშავებენ სტუდენტების, პერსონალის და სხვა პირთა დიდი მოცულობის პერსონალურ მონაცემებს. მათ შორის პირად საქმეებს, შეფასებებს, ლექცია/სემინარების ვიდეო ჩანაწერებს. შესაბამისად, უმაღლესი საგანმანათლებლო დაწესებულებები იქცნენ მონაცემთა დამუშავებაზე პასუხისმგებელ პირებად, რომლებიც ამუშავებენ დიდი რაოდენობის მონაცემებს, ახორციელებენ სტუდენტთა ქცევის მონიტორინგს და რომელთაც ეკისრებათ როგორც სამართლებრივი, ისე ეთიკური ვალდებულება პერსონალური მონაცემების დაცვის საკითხში.

თანამედროვე სამართლებრივი სახელმწიფო ემყარება პრინციპს, რომლის მიხედვითაც ადამიანი, მისი ღირსება, პირადი ცხოვრება და თავისუფლება წარმოადგენს უმაღლეს ღირებულებას. ადამიანის პირადი სივრცის ხელშეუხებლობა ადამიანის ფუნდამენტურ უფლებას წარმოადგენს, რომელიც აღიარებულია ეროპნულ და საერტაშორისო დონეზე.[2] ამ კონტექსტში, ერთ-ერთი უმნიშვნელოვანესი საკითხია პერსონალური მონაცემების დაცვა, ვინაიდან ინდივიდის შესახებ ინფორმაციის დამუშავება პირდაპირ უკავშირდება პირადი ცხოვრების თავისუფლებას. საქართველოს კონსტიტუციის მე-15 მუხლით აღიარებულია პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებები.[3] კონსტიტუციით აღიარებული პერსომალური მონაცემების დაცვის სამართლებრივ მექანიზმს წარმოადგენს 2023 წელს საქართველოს პარლამენტის მიერ დამტკიცებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, რომლის მიზანია პერსონალური მონაცემების დამუშავებისას ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის, პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცვა. პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მიღებით ქართული სისტემა არსებითად დაუახლოვდა პერსონალურ მონაცემთა სფეროში ევროკავშირის ზოგადი რეგულაციით გათვალისწინებულ სტანდარტებს (GDPR).[4]

GDPR-ის სტანდარტებთან საქართველოს დაახლოება ასოცირების შეთანხმებიდან გამომდინარე ვალდებულებას წარმოადგენდა. ასოცირების შეთანხმებით[5] საქართველომ აიღო ვალდებულება შეექმნა ევროკავშირის სტანდარტებთან შესაბამისი მონაცემთა დაცვის

[2] European Court of Human Rights. (2003). Peck v. the United Kingdom, Application no. 44647/98.

[3] საქართველოს კონსტიტუცია, 24 აგვისტო, 1995, საქართველოს საკანონმდებლო მაცნე.

[4] საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ, 14.06.2023წ, საქართველოს საკანონმდებლო მაცნე.

[5] ასოცირების შესახებ შეთანხმება ერთის მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებსა და მეორეს მხრივ, საქართველოს შორის, 27/06/2014

სისტემა. ამ ვალდებულების შესრულება მოიცავდა GDPR-ის პრინციპების, სტანდარტებისა და მექანიზმების ინტეგრირებას ეროვნულ კანონმდებლობაში. აღნიშნული ვალდებულების ფარგლებში, 2023 წელს მიღებული ცვლილებებით „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონში მნიშვნელოვანი სიახლეები დაინერგა, რომლებიც მიზნად ისახავს GDPR-ის პრინციპების, სამართლებრივი საფუძვლების, გამჭვირვალობის, ანგარიშვალდებულებისა და მონაცემთა სუბიექტის უფლებების უზრუნველყოფას. ამ ცვლილებებმა არსებითად გააძლიერა მონაცემთა დაცვის ზედამხედველ ორგანოს დამოუკიდებლობა და გააფართოვა მისი უფლებამოსილებები. ამავე დროს მნიშვნელოვნად გაამკაცრა პერსონალურ მონაცემთა დაცვის სტანდარტები.

GDPR-ის გავლენამ უნივერსიტეტების საქმიანობაზეც განსაკუთრებული კვალი დატოვა. ევროკავშირის რეგულაცია მკაფიოდ განსაზღვრავს მონაცემთა დამუშავების პრინციპებს, მათ შორის - კანონიერებას, სამართლიანობას, გამჭვირვალობას, სიზუსტეს, მიზნის შეზღუდვისა და მონაცემთა მინიმიზაციის მოთხოვნებს, რომელთა დაცვა აუცილებელია ყველა ორგანიზაციისთვის, მათ შორის საგანმანათლებლო დაწესებულებებისთვისაც[6]. უნივერსიტეტებში მონაცემთა დამუშავება მოიცავს არა მხოლოდ ადმინისტრაციულ პროცესებს, არამედ კვლევით საქმიანობას, საერთაშორისო გაცვლით პროგრამებსა და ონლაინ სწავლებას, რაც ქმნის მონაცემთა დაცვის ახალი ტიპის გამოწვევებს. აუცილებელია ისეთი მექანიზმების უზრუნველყოფა, რომლებიც ერთდროულად დაიცავს მონაცემთა სუბიექტის უფლებებს და ხელს არ შეუშლის განათლების გლობალიზაციას, აკადემიური თანამშრომლობისა და ინოვაციური განვითარების შესაძლებლობების განვითარებას.

ამასთან, საქართველოს უმაღლესი საგანმანათლებლო სივრცე, ევროპულ სტანდარტებთან ჰარმონიზაციის პროცესში, თანდათან ცდილობს პერსონალურ მონაცემთა დაცვის მექანიზმების დახვეწას, თუმცა პრაქტიკაში რჩება სირთულეები - ინფორმირებული თანხმობის მოპოვებიდან დაწყებული, მონაცემთა შენახვის ვადებისა და უსაფრთხოების წესების დაცვამდე. სწორედ ამ რეალობის ფონზე კვლევის მიზანია, გამოიკვეთოს პერსონალურ მონაცემთა დაცვის არსებული სამართლებრივი ჩარჩო უმაღლეს საგანმანათლებლო დაწესებულებებში, შეფასდეს მისი შესაბამისობა საერთაშორისო სტანდარტებთან და განისაზღვროს ძირითადი გამოწვევები, რომლებიც მონაცემთა დაცვის ეფექტიან განხორციელებას უშლის ხელს.

კვლევის საგანი:

კვლევის საგანს წარმოადგენს პერსონალურ მონაცემთა დაცვის სამართლებრივი და ინსტიტუციური სისტემა უმაღლეს საგანმანათლებლო დაწესებულებებში, რაც მოიცავს როგორც საქართველოს კანონმდებლობასა და მასთან დაკავშირებულ რეგულაციებს, ისე უნივერსიტეტების შიდა პოლიტიკებსა და მონაცემთა დამუშავების პრაქტიკას. განსაკუთრებული ყურადღება ექცევა იმ ასპექტებს, რომლებიც დაკავშირებულია სტუდენტთა, აკადემიური და ადმინისტრაციული პერსონალის პერსონალურ მონაცემთა

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation — GDPR), 27 April 2016.

შეგროვებასთან, შენახვასთან, წვდომასთან, გადაცემასა და წაშლასთან. ამასთან, კვლევა მოიცავს საერთაშორისო ხელშეკრულებების, მათ შორის GDPR-ის, შედარებით ანალიზს, რათა გამოიკვეთოს საქართველოს რეგულაციების შესაბამისობა ევროპულ სტანდარტებთან. შესაბამისად, კვლევა ეფუძნება როგორც ნორმატიული რეგულაციების თეორიულ-იურიდიულ შეფასებას, ისე მათი პრაქტიკული განხორციელების ფორმების შესწავლას საუნივერსიტეტო სივრცეში.

კვლევის მიზანი:

მოცემული კვლევის მიზანია გაანალიზდეს პერსონალურ მონაცემთა დაცვის მოქმედი სამართლებრივი ჩარჩო უმაღლეს საგანმანათლებლო დაწესებულებებში, განისაზღვროს მისი შესაბამისობა საერთაშორისო სტანდარტებთან, განსაკუთრებით კი ევროკავშირის ზოგად მონაცემთა დაცვის რეგულაციასთან (GDPR), და გამოიკვეთოს ის ძირითადი სამართლებრივი და პრაქტიკული გამოწვევები, რომლებიც უნივერსიტეტებში მონაცემთა დამუშავების პროცესის ეფექტიან განხორციელებას აფერხებს. კვლევა ისახავს მიზნად არა მხოლოდ არსებული ნორმატიული საფუძვლის აღწერასა და შეფასებას, არამედ საგანმანათლებლო და აკადემიურ სივრცეში სისტემური ხარვეზების გამოვლენასაც. კვლევის ძირითადი მიზანია შემუშავდეს რეკომენდაციები სამართლებრივი ჩარჩოსა და ინსტიტუციური პრაქტიკის სრულყოფისათვის, რათა მონაცემთა დამუშავების პროცესი უმაღლეს სასწავლებლებში იყოს თანხვედრაში ევროპულ და საერთაშორისო მოთხოვნებთან, ამავდროულად კი უზრუნველყოფდეს აკადემიური თავისუფლებისა და მონაცემთა დაცვის უფლებებს შორის ბალანსს.

კვლევის ამოცანები:

დასახული მიზნის მისაღწევად, კვლევა ადგენს რამდენიმე ამოცანას: პირველ რიგში, აუცილებელია პერსონალურ მონაცემთა დაცვის ფუნდამენტური პრინციპების - სამართლიანობის, კანონიერების, გამჭვირვალობის, მიზნის შეზღუდვის, მონაცემთა მინიმიზაციისა და ანგარიშვალდებულების - შინაარსობრივი გაანალიზება სამართლებრივი თვალსაზრისით.

მეორე ეტაპზე საჭიროა საქართველოს კანონმდებლობის დეტალური შესწავლა და მისი შედარება GDPR-ის შესაბამის დებულებებთან, რათა გამოიკვეთოს თანხვედრა და განსხვავება.

შემდგომი ამოცანაა უნივერსიტეტებში მონაცემთა დამუშავების რეალური პრაქტიკის შესწავლა, მათ შორის თანხმობის მართვის, ინფორმაციის უსაფრთხოების და მესამე პირებთან მონაცემთა გაზიარების მექანიზმების შეფასება.

კვლევის ამოცანაა სამართლებრივი და პრაქტიკაში არსებული ხარვეზების იდენტიფიცირება, რომლებიც ხელს უშლის მონაცემთა დაცვის ეფექტიანი მექანიზმების დანერგვას, და ბოლოს - შესაბამისი რეკომენდაციების შემუშავებას ეროვნული კანონმდებლობისა და პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული უმაღლესი საგანმანათლებლო დაწესებულებების დოკუმენტაციის სრულყოფის მიზნით.

კვლევის მეთოდოლოგია:

მოცემული კვლევა ეფუძნება შერეულ მეთოდოლოგიურ მიდგომას, რომელიც აერთიანებს როგორც დოქტრინალურ (თეორიულ-იურიდიულ), ისე ემპირიულ კვლევის მეთოდებს. კვლევის პროცესში გამოყენებულია შემდეგი ძირითადი მეთოდები:

1. **დოქტრინალური (სამართლის-დოგმატური) ანალიზი:**

განხორციელდა პერსონალურ მონაცემთა დაცვის სამართლებრივი ჩარჩოს სიღრმისეული ანალიზი. განხილულია საქართველოს კონსტიტუცია, კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, უნივერსიტეტების შიდა რეგულაციები და საერთაშორისო სამართლებრივი დოკუმენტები, მათ შორის, ევროპის საბჭოს, 108-ე კონვენცია, ევროკავშირის მონაცემთა დაცვის რეგულაცია (GDPR), ადამიანის უფლებათა დაცვის ევროპული კონვენცია და სხვა. დოქტრინალური მეთოდის მიზანია არსებული ნორმების შინაარსობრივი გაანალიზება და მათი შესაბამისობის შეფასება საერთაშორისო სტანდარტებთან, განსაკუთრებით GDPR-ის პრინციპებთან.

2. **შედარებითი სამართლის მეთოდი:**

კვლევაში გამოყენებულია შედარებით ანალიზი, რომლის საფუძველზეც შესწავლილია თანხმვედრა და განსხვავება საქართველოს კანონმდებლობასა და ევროკავშირის რეგულაციებს შორის. ასევე შესწავლილია ევროკავშირის ზოგიერთი წევრი ქვეყნის (მაგ. გერმანია, ესტონეთი, პოლონეთი) უნივერსიტეტების მონაცემთა დაცვის პრაქტიკა, რაც საშუალებას იძლევა შეფასდეს საქართველოს სამართლებრივი ჩარჩოს პრაქტიკული ეფექტიანობა ევროპულ კონტექსტში.

3. **ემპირიული (პრაქტიკული) კვლევის მეთოდი:**

კვლევის ფარგლებში გაანალიზებულია კონკრეტული უმაღლესი საგანმანათლებლო დაწესებულებების შიდა დოკუმენტები, მონაცემთა დაცვის პოლიტიკის დუკუმენტები, თანხმობის ფორმები, მონაცემთა შენახვის და წვდომის პროცედურები. საჭიროებისამებრ გამოყენებულია ინტერვიუებისა და კითხვარების ანალიზი უნივერსიტეტების ადმინისტრაციული პერსონალთან და მონაცემთა დაცვის ოფიცრებთან, რათა დადგინდეს პრაქტიკული სირთულეები და არსებული მექანიზმების ეფექტიანობა.

4. **სისტემური და ინტერპრეტაციული მეთოდები:**

გამოყენებულია სამართლებრივი ნორმების სისტემური ინტერპრეტაცია, რაც გულისხმობს მონაცემთა დაცვის კანონმდებლობის ურთიერთკავშირს სხვა სამართლის დარგებთან - მათ შორის განათლების სამართალთან, შრომით სამართალთან და ა.შ. აღნიშნული მიდგომა აუცილებელია იმისათვის, რომ დადგინდეს პერსონალურ მონაცემთა დაცვის წესების გავლენა უნივერსიტეტის საერთო მმართველობით სისტემაზე.

5. **ანალიტიკურ-შეფასებითი მეთოდი**

კვლევა აერთიანებს კრიტიკულ ანალიზს და შეფასებას, რაც მიმართულია მონაცემთა დაცვის არსებული პრაქტიკის ძლიერი და სუსტი მხარეების იდენტიფიცირებისკენ. აღნიშნული

მეთოდი საშუალებას იძლევა ჩამოყალიბდეს დასკვნები და შემუშავდეს პრაქტიკული რეკომენდაციები კანონმდებლობისა და საუნივერსიტეტო მმართველობის სრულყოფისათვის.

ჯამში, მეთოდოლოგია ორიენტირებულია არა მხოლოდ ნორმატიული ბაზის აღწერასა და შედარებაზე, არამედ მისი პრაქტიკული განხორციელების შეფასებაზე, რაც უზრუნველყოფს კვლევის შედეგების მრავალმხრივობასა და გამოყენებით ღირებულებას.

თავი I. კვლევის თეორიული საფუძველი და სამართლებრივი ჩარჩო

1.1. პერსონალური მონაცემების დაცვის კონცეპტუალური საფუძვლები მონაცემთა დაცვის უფლება როგორც ადამიანის ფუნდამენტური უფლება

თანამედროვე სამყაროში პერსონალური მონაცემების დაცვა წარმოადგენს არა მხოლოდ ტექნიკურ თუ ადმინისტრაციულ, არამედ ადამიანის ფუნდამენტური უფლებების დაცვის საკითხს. მონაცემთა დაცვის უფლება მჭიდროდ უკავშირდება პირად ცხოვრებაში ჩარევისგან დაცვის კონსტიტუციურ გარანტიას და ადამიანის ღირსებას. სწორედ ამ ორი ღირებულების სინთეზზე დაფუძნდა ევროპული სამართლის ტრადიციაში პერსონალური მონაცემთა დაცვის ცნება[7]. ადამიანის უფლებათა დაცვის ევროპული კონვენციის მე-8 მუხლი ადგენს ადამიანის უფლებას პირად და ოჯახურ ცხოვრებაში ჩარევისგან დაცვისა, რაც შემდგომ ინტერპრეტაციით გახდა პერსონალური მონაცემების დაცვის სამართლებრივი საფუძველი[8]. ადამიანის უფლებათა ევროპულმა სასამართლომ არაერთხელ ხაზგასმით აღნიშნა, რომ სახელმწიფოს პოზიტიური ვალდებულებაა, შექმნას ისეთი სამართლებრივი ჩარჩო, რომელიც უზრუნველყოფს ინდივიდის პირადი ინფორმაციის დაცვას თვით კერძო პირების მხრიდანაც[9]. ევროკავშირის სამართალმა ეს უფლება დამოუკიდებელ სტატუსად განავითარა: ლისაბონის ხელშეკრულების მიღების შემდეგ, ევროკავშირის ფუნდამენტური უფლებების ქარტიის მე-8 მუხლი ცალსახად აღიარებს „პერსონალურ მონაცემთა დაცვის უფლებას“, რაც მას განაცალკევებს მხოლოდ „პირად ცხოვრებაზე“ მუხლიდან და აძლევს დამოუკიდებელ კონსტიტუციურ მნიშვნელობას[10].

საქართველოს სამართლებრივ სისტემაშიც მონაცემთა დაცვის უფლება აღიარებულია კონსტიტუციურად: საქართველოს კონსტიტუციის მე-15 მუხლი ადგენს პირად ცხოვრებაში ჩარევისგან დაცვის გარანტიას, ხოლო „პერსონალურ მონაცემთა დაცვის შესახებ“ ამ უფლების განხორციელების სამართლებრივ მექანიზმებს დეტალურად აწესებს[11].

ამგვარად, პერსონალურ მონაცემთა დაცვის უფლება ჩამოყალიბდა როგორც თანამედროვე ადამიანის უფლებათა დაცვის სისტემის ერთ-ერთი ცენტრალური ელემენტი, რომელიც იცავს

[7] Gutwirth, S. & De Hert, P. (2010). Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power. Springe

[8] European Convention on Human Rights, Article 8

[9] Case of Z v. Finland, European Court of Human Rights, 1997

[10] Charter of Fundamental Rights of the European Union, Article 8.

[11] საქართველოს კონსტიტუცია, მუხლი 15; კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, საქართველოს პარლამენტი, 2023.

ინდივიდს არა მხოლოდ სახელმწიფოსაგან, არამედ კერძო სექტორის მხრიდან არასათანადო მონაცემთა დამუშავებისგანაც.

მონაცემთა დაცვისა და ადამიანის ღირსების ურთიერთკავშირი: პერსონალური მონაცემების დაცვის კონცეფცია წარმოუდგენელია ადამიანის ღირსების პრინციპის გარეშე. ადამიანის ღირსება წარმოადგენს იმ ღერძს, რომელზეც აშენებულია ევროპული სამართლისა და ადამიანის უფლებათა მთელი არქიტექტურა. მონაცემთა დაცვის მიზანი საბოლოო ჯამში არის პიროვნების ღირსებისა და იდენტობის დაცვა ინფორმაციულ საზოგადოებაში[12]. განსაკუთრებით მნიშვნელოვანია აღინიშნოს, რომ პერსონალურ მონაცემთა დაცვის უფლების დარღვევა იწვევს არა მხოლოდ პირადი ინფორმაციის გავრცელებას, არამედ პიროვნული ავტონომიისა და ღირსების შელახვას- რაც გამოიხატება სოციალურ სტიგმაში, დისკრიმინაციას ან ფსიქოლოგიურ ზიანში[13]. ამდენად, მონაცემთა დაცვის პრინციპები ემსახურება არა მხოლოდ ტექნიკური უსაფრთხოების უზრუნველყოფას, არამედ ადამიანის ღირსების რეალურ დაცვას თანამედროვე ტექნოლოგიურ სამყაროში.

ევროპის საბჭოს, 108-ე კონვენცია რომელიც განახლდა 2018 წელს, პირდაპირ ხაზს უსვამს ამ საკვანძო კავშირს. კონვენციაში ხაზგასმულია, რომ პერსონალური მონაცემების დამუშავება უნდა ემსახურებოდეს „ადამიანის ღირსებისა და პიროვნების თავისუფლების პატივისცემას“[14]. ანალოგიური მიდგომა აისახა GDPR-ის პრეამბულაშიც, სადაც აღნიშნულია, რომ მონაცემთა დაცვა არ უნდა განიხილებოდეს როგორც იზოლირებული ტექნიკური მოვლენა, არამედ როგორც ადამიანის უფლებათა ფართო სისტემის განუყოფელი ნაწილი[15]. “პერსონალურ მოანეცმტა დაცვის შესახებ” საქართველოს კანონის მე-4 მუხლშიც ხაზგასმულია, რომ პერსონალური მონაცემები უნდა დამუშავდეს მონაცემთა სუბიექტის ღირსების შეულახავად.

1.2. პერსონალურ მონაცემთა დაცვის პრინციპები

პერსონალური მონაცემთა დაცვის სამართლებრივი სისტემის ბირთვს წარმოადგენს რამდენიმე ძირითადი პრინციპი, რომლებიც განსაზღვრავს მონაცემთა დამუშავების ლეგიტიმურ და ეთიკურ ჩარჩოს. აღნიშნული პრინციპები ჩამოყალიბებულია როგორც GDPR-ის 5-ე მუხლში, ასევე საქართველოს კანონში „პერსონალურ მონაცემთა დაცვის შესახებ“[16]. ეს პრინციპებია:

- **კანონიერებისა და სამართლიანობის პრინციპი** მონაცემთა დამუშავება დაშვებულია მხოლოდ კანონიერ საფუძველზე - მაგალითად, სუბიექტის თანხმობის, სამართლებრივი ვალდებულების, გარიგების შესრულების ან საჯარო ინტერესის საფუძველზე.

[12] Bygrave, L. A. (2014). Data Privacy Law: An International Perspective. Oxford University Press.
[13] olove, D. J. (2008). Understanding Privacy. Harvard University Press
[14] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), 2018
[15] European Parliament and Council of the European Union. Regulation (EU) 2016/679 ... (General Data Protection Regulation – GDPR), Recital 4
[16] European Parliament and Council of the European Union. Regulation (EU) 2016/679 ... (General Data Protection Regulation – GDPR). Article 5; კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 4

უნივერსიტეტების შემთხვევაში ეს შეიძლება იყოს სტუდენტებთან და თანამშრომლებთან არსებული სამართლებრივი ურთიერთობები ან კანონით განსაზღვრული ვალდებულებები[17]. აღნიშნული პრინციპი ასევე მოიცავს, რომ პერსონალური მონაცემები უნდა დამუშავდეს არადისკრიმინაციულად და ადამიანის ღირსების შეულახავად.

- **გამჭვირვალობის პრინციპი** დამუშავების პროცესში აუცილებელია სუბიექტის ინფორმირება მონაცემთა შეგროვების მიზნისა და მოცულობის შესახებ. გამჭვირვალობა ზრდის ნდობას ორგანიზაციასა და მონაცემთა სუბიექტს შორის[18].

- **მიზნის შეზღუდვის პრინციპი** მონაცემთა შეგროვება უნდა ხდებოდეს კონკრეტული, მკაფიო და ლეგიტიმური მიზნისთვის და მათი შემდგომი დამუშავება უნდა შეესაბამებოდეს ამ მიზანს. უნივერსიტეტებში ეს პრინციპი განსაკუთრებით მნიშვნელოვანია, რადგან მონაცემები ხშირად გამოიყენება ადმინისტრაციული და აკადემიური მიზნებისთვის[19].

- **მონაცემთა მინიმიზაციის პრინციპი:** უნივერსიტეტმა უნდა შეაგროვოს მხოლოდ ის ინფორმაცია, რომელიც აუცილებელია კონკრეტული მიზნის მისაღწევად. ზედმეტი მონაცემების დამუშავება არღვევს სუბიექტის პირად სივრცეს და ზრდის უფლების დარღვევის რისკებს[20].

- **უსაფრთხოების პრინციპი:** მონაცემები უნდა იყოს დაცული არასანქცირებული წვდომის, დაკარგვის ან განადგურებისგან. უსაფრთხოების უზრუნველყოფა მოიცავს როგორც ტექნიკურ, ისე ორგანიზაციულ ზომებს (პაროლები, დაშიფვრა, წვდომის კონტროლი)[21].

- **ანგარიშვალდებულების პრინციპი:** მონაცემთა დამმუშავებელი ორგანიზაცია ვალდებულია დაადასტუროს, რომ ყველა ზემოაღნიშნული პრინციპი დაცულია და შესაბამისი პროცედურები განხორციელებულია. ეს პრინციპი აძლიერებს მმართველობით პასუხისმგებლობასა და გამჭვირვალობას[22].

აღნიშნული პრინციპები ქმნის იმ საფუძველს, რომლის დაცვაც აუცილებელია ყველა ორგანიზაციისთვის, მათ შორის უმაღლესი საგანმანათლებლო დაწესებულებებისთვისაც, რომლებიც ყოველდღიურად ამუშავებენ სტუდენტთა და თანამშრომელთა დიდი მოცულობის მონაცემებს. მონაცემთა დამუშავების პრინციპების დაცვა უნდა ხდებოდეს მონაცემთა დამუშავების თითოეულ ეტაპზე -მოგროვების, წვდომის, გადაცემის, წაშლის დროს და თითოეულ ეტაპზე ყველა პრინციპი უნდა იყოს დაცული, რისი მტკიცების ვალდებულებაც აქვს უნივერსიტეტს- მონაცემთა დამუშავებაზე პასუხისმგებელ პირს.

თავი II. პერსონალურ მონაცემთა დაცვის ეროვნული და საერთაშორისო სამართლებრივი ჩარჩო

[17] European Data Protection Board (EDPB), Guidelines on the Legal Bases for Processing, 2020
[18] ICO (UK Information Commissioner's Office), Principles of Transparency, 2022.
[19] Article 29 Data Protection Working Party, Opinion on Purpose Limitation, 2013
[20] GDPR, Article 5(1)(c)
[21] ENISA, Technical Guidelines on Data Security, 2021
[22] GDPR, Article 5(2); OECD Privacy Guidelines, 2013

2.1. ეროვნული სამართლებრივი ჩარჩო

საქართველოს სამართლებრივი სისტემა პერსონალური მონაცემთა დაცვის მიმართულებით თანმიმდევრულად ვითარდება და ევროპული სტანდარტებისკენ მიისწრაფის. აღნიშნული სფერო მოიცავს როგორც კონსტიტუციურ საფუძველს, ასევე სპეციალურ კანონმდებლობას, კანონქვემდებარე აქტებსა და ინსტიტუციურ მექანიზმებს, რომლებიც მიზნად ისახავს ინდივიდის პირადი სივრცის დაცვასა და ინფორმაციის უსაფრთხოების უზრუნველყოფას.

პერსონალურ მონაცემთა დაცვის უფლება კონსტიტუციურად გარანტირებულია საქართველოს კონსტიტუციის მე-15 მუხლით, რომლის თანახმადაც ადამიანის პირადი ცხოვრება, პირადი სივრცე და კომუნიკაცია ხელშეუხებელია[23]. პერსონალურ მონაცემთა დაცვის თვალსაზრისით არანაკლებ მნიშვნელოვანია კონსტიტუციის მე-18 მუხლი, რომლის თანახმადაც, ყველას აქვს უფლება კანონით დადგენილი წესით გაეცნოს საჯარო დაწესებულებაში მასზე არსებულ ან სხვა ინფორმაციას ან ოფიციალურ დოკუმენტს, გარდა იმ შემთხვევისა თუ არ არსებობს შეზღუდვის კონსტიტუციით დადგენილი ლეგიტიმური საფუძვლები. იგივე მუხლი განამტკიცებს საჯარო სტუქტურებში არსებული პერსონალური მონაცემების დაცვას. კერძოდ, ოფიციალურ ჩანაწერებში არსებული ინფორმაცია, რომელიც დაკავშირებულია ადამიანის ჯანმრთელობასთან, ფინანსებთან ან სხვა პირად საკითხებთან, არავისთვის უნდა იყოს ხელმისაწვდომი თვით ამ ადამიანის თანხმობის გარეშე, გარდა კანონით გათვალისწინებული შემთხვევებისა, როდესაც ეს აუცილებელია სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, საჯარო ინტერესების, ჯანმრთელობის ან სხვათა უფლებების დასაცავად.

აღნიშნული ნორმები ქმნიან სამართლებრივ საფუძველს და ძირითად პრინციპებს ნებისმიერი შემდგომი რეგულაციისთვის, რომელიც უკავშირდება ინდივიდის პირადი ინფორმაციის მოპოვებასა და გამოყენებას. კონსტიტუციური სამართლის დონეზე ეს გარანტია განიხილება ადამიანის ღირსებისა და პირად ცხოვრებაში ჩარევის დაუშვებლობის პრინციპის კონტექსტში, რაც საქართველოს უზენაესი სასამართლოს პრაქტიკაშიც არაერთხელ ყოფილა განმტკიცებული[24].

კონსტიტუციური ნორმის კონკრეტიზაცია განხორციელდა „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონში[25]. აღნიშნული კანონი წარმოადგენს მნიშვნელოვან ეტაპს საქართველოს სამართლებრივი სისტემის ევროპულ სამართალთან ჰარმონიზაციის პროცესში, ვინაიდან იგი არსებითად ეყრდნობა ევროკავშირის ზოგადი მონაცემთა დაცვის რეგულაციის (GDPR) პრინციპებსა და სტრუქტურას[26].

---

[23] საქართველოს კონსტიტუცია, მუხლი 15 (საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება №2/1/504, 2013).

[24] საქართველოს უზენაესი სასამართლო, საქმე №ას-236-2018, გადაწყვეტილება 2018 წლის 12 აპრილი

[25] კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მიღებული საქართველოს პარლამენტის მიერ 2023 წლის 1 მარტს, ამოქმედდა 2023 წლის 15 მარტს.

[26] Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), Official Journal of the European Union, 2016

კანონი ადგენს მონაცემთა დამუშავების ძირითად პრინციპებს, მათ შორის კანონიერებისა და სამართლიანობის, გამჭვირვალობის, მიზნის შეზღუდვისა და მონაცემთა მინიმიზაციის მოთხოვნებს, განსაზღვრავს დამუშავების სამართლებრივ საფუძვლებს, მონაცემთა სუბიექტის უფლებებსა და მონაცემთა დამმუშავებლის ვალდებულებებს.

პერსონალურ მონაცემთა დაცვაზე ზედამხედველობას ახორციელებს პერსონალურ მონაცემთა დაცვის სამსახური, რომლის საქმიანობაც ემყარება, როგორც ეროვნულ, ისე საერთაშორისო თანამშრომლობას. განსაკუთრებით აღსანიშნავია ევროპულ ზედამხედველ ორგანოებთან (მაგალითად, European Data Protection Board - EDPB) თანამშრომლობა, რაც საშუალებას აძლევს საქართველოს ეტაპობრივად დააახლოვოს თავისი სტანდარტები ევროკავშირის რეგულაციებთან[27].

დამატებით, კანონის საფუძველზე შემუშავდა რიგი აქტები, რომლებიც განსაზღვრავენ მონაცემთა დამუშავების სპეციფიკურ წესებს სხვადასხვა სფეროში. მაგალითად, განათლების სექტორში მოქმედებს პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შემუშავებული სახელმძღვანელო დოკუმენტები, რომლებიც განმარტავენ სტუდენტთა, აბიტურიენტთა და აკადემიური პერსონალის მონაცემთა დამუშავების პრაქტიკულ ასპექტები. ამასთანავე, უმაღლესი საგანმანათლებლო დაწესებულებებს ევალებათ საკუთარი შიდა დოკუმენტებისა და რეგლამენტების შემუშავება, რომლებიც უნდა იყოს შესაბამისობაში როგორც ეროვნულ კანონმდებლობასთან, ისე GDPR-ის სტანდარტებთან[28].

უმაღლეს საგანმანათლებლო დაწესებულებებს ევალებათ შეიმუშავონ პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული ყველა აუცილებელი დოკუმენტი, მათ შორის განსაკუთრებით აღსანიშნავია: პოლიტიკის დოკუმენტი, უსაფრთხოების ტექნიკური და ორგანიზაციული ზომების აღწერა, პერსონალურ მონაცემთა დამუშავებაზე თანხმობის დოკუმენტი და ვიდეომონიტორინგის წესის აღწერა. ეს დოკუმენტები ხშირად მხოლოდ ფორმალურ ხასიათს ატარებს და არ ხდება მათი შექმნის პროცესში ყველა არსებითი დეტალების გააზრება და შემდგომ დოკუმენტის პრაქტიკაშისწორად შესრულება.

ამრიგად, საქართველოს სამართლებრივი ჩარჩო პერსონალური მონაცემთა დაცვის სფეროში შესაბამისობაშია საუკეთესო საერტაშორისო სტანდარტებთან. თუმცა, მიუხედავად რეგულაციების სრულყოფისა, პრაქტიკაში კვლავ არსებობს საჭიროება მათი ეფექტური დანერგვისა და მონიტორინგის.

2.2. საერთაშორისო სამართლებრივი ჩარჩო

პერსონალურ მონაცემთა დაცვის რეგულირება საერთაშორისო სამართალში ჩამოყალიბდა ადამიანის ფუნდამენტური უფლებების დაცვის სისტემის განუყოფელ ნაწილად. ეს სფერო მოიცავს მრავალმხრივ ინსტიტუციურ და ნორმატიულ ჩარჩოს, რომელიც ეფუძნება ადამიანის ღირსებისა და პირად ცხოვრებაში ჩარევისგან დაცვის პრინციპებს. მისი

[27] European Data Protection Board (EDPB) – Cooperation with Third Countries, Annual Report, 2023
[28] European Commission, Adequacy Decisions and GDPR Alignment Reports, Brussels, 2022

განვითარება ეტაპობრივად ხდებოდა — საწყისი მოდელი ჩამოყალიბდა ევროპის საბჭოს ფარგლებში, შემდგომ ევროკავშირის სამართალში და მოგვიანებით გლობალურ დონეზეც.

პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ 108-ე კონვენცია მონაცემთა დაცვის თაობაზე პირველ და ამ სფეროში სავალდებულო იურიდიული ძალის მქონე უმნიშვნელოვანეს საერთაშორისო სამართლებრივ ინსტრუმენტს წარმოადგენს. საქართველოს პარლამენტმა ამ კონვენციის რატიფიცირება 2005 წელს მოახდინა, ხოლო ძალაში 2006 წლის 1 აპრილს შევიდა.

პირადი ცხოვრების ხელშეუხებლობის უფლებასთან დაკავშირებული მზარდი გამოწვევების ფონზე საჭირო გახდა 108-ე კონვენციის განახლება. მისი მოდერნიზების პროცესი ორ ძირითად საკითხზე იყო ორიენტირებული: კონვენციას სათანადოდ უნდა ეპასუხა ციფრული ეპოქის გამოწვევებისათვის და უნდა დანერგილიყო მისი ეფექტური აღსრულების მექანიზმი. მოდერნიზების პროცესი დასრულდა კონვენციის CETS No. 223 შესწორების ოქმის მიღებით. აღნიშნული ოქმი (რომლის საფუძველზეც კონვენციას მოიხსენებენ როგორც „108+ კონვენციას“) 2018 წლის 10 ოქტომბერს გაიხსნა ხელმოსაწერად. დღეის მდგომარეობით, დოკუმენტის რატიფიცირება 33- ქვეყანამ მოახდინა. საქართველოს ჯერ ოქმის არც ხელმოწერა და არც რატიფიცირება არ განუხორციელებია.[29]

უდიდესი მნიშვნელობა აქვს ასევე ევროკავშირის ზოგად მონაცემთა დაცვის რეგულაციას (Regulation (EU) 2016/679 – GDPR), რომელიც 2018 წლის 25 მაისიდან ამოქმედდა და გახდა მონაცემთა დაცვის სფეროში გლობალური ეტალონი[30]. რეგულაციამ პირველად ჩამოაყალიბა ერთიანი სამართლებრივი ჩარჩო ევროკავშირის მასშტაბით, გააძლიერა ინდივიდის უფლებები და გაამკაცრა ორგანიზაციების პასუხისმგებლობა მონაცემთა დამუშავებისას. GDPR-ის მნიშვნელობა სცდება ევროკავშირის საზღვრებს - იგი იქცა მოდელურ სტანდარტად მესამე ქვეყნებისათვისაც, რომლებიც საკუთარ კანონმდებლობას ევროპულ სამართალთან ჰარმონიზაციას უქმნიან. საქართველოს ახალი კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, რომრლიც ძალაში 2024 წლის 1 მარტს შევიდა სწორედ ამ რეგულაციის პრინციპებს ეფუძნება და მნიშვნელოვნად მიუახლოვდა მის სტრუქტურასა და ტერმინოლოგიას[31].

განსაკუთრებით მნიშვნელოვანია მონაცემთა სუბიექტის უფლებების სისტემა, რომელიც მოიცავს ინფორმაციის მიღების, წვდომის, გასწორების, წაშლის („დავიწყების უფლება“), დამუშავების შეზღუდვისა და გადატანის უფლებებს[32]. აღნიშნული უფლებები ზრდის ინდივიდის კონტროლს საკუთარ მონაცემებზე და ამყარებს ნდობის ახალ სტანდარტს მონაცემთა დამუშავების პასუხისმგებელ პირებსა და მონაცემთა სუბიექტებს შორის.

---

[29] ხელმომწერი ქვეყნების სია: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223

[30] Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), Official Journal of the European Union, 2016.

[31] კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, საქართველოს პარლამენტი, 2023, განმარტებითი ბარათი.

[32] GDPR, Articles 12–22

გლობალურ დონეზე მონაცემთა დაცვის პრინციპები აისახა ასევე სხვა საერთაშორისო დოკუმენტებში. მაგალითად, გაეროს გენერალურმა ასამბლეამ 1990 წელს მიიღო რეზოლუცია 45/95, „ინსტრუქციები პერსონალური მონაცემების კომპიუტერიზებული ფაილების რეგულირებისთვის", რომელიც დაეფუძნა OECD-ის რეკომენდაციებს და იქცა უნივერსალურ ჩარჩოდ, განსაკუთრებით განვითარებადი ქვეყნებისათვის[33]. ხოლო OECD-ის კონფიდენციალურობის სახელმძღვანელო პრინციპები (OECD Privacy Guidelines, 2013) ითვალისწინებს მონაცემთა ხარისხის, მიზნობრიობისა და უსაფრთხოების მინიმალურ მოთხოვნებს და წარმოადგენს გლობალური სამართლიანობის სტანდარტს, რომელსაც მრავალი ქვეყანა იყენებს საკუთარი კანონმდებლობის მოდელირებისთვის[34].

საერთაშორისო სამართლის ამ მრავალდონიან სისტემაში საქართველოსთვის განსაკუთრებული მნიშვნელობა აქვს ევროპულ მოდელთან შესაბამისობას, ვინაიდან ქვეყნის კანონმდებლობა დაფუძნებულია ასოცირების ხელშეკრულებით აღებულ ვალდებულებებზე ევროკავშირთან. შესაბამისად, პერსონალურ მონაცემთა დაცვის სფეროში საერთაშორისო ჩარჩო არამარტო დოკუმენტური ან ნორმატიული საფუძველია, არამედ საქართველოს ევროპული ინტეგრაციის პროცესის პრაქტიკული ინსტრუმენტი.

ამგვარად, საერთაშორისო სამართლებრივი ჩარჩო ქმნის უნივერსალურ ბაზისს, რომლის მიზანია პიროვნების ინფორმაციული ავტონომიის დაცვა გლობალური მასშტაბით. მისი ძირითადი ღირებულებები, როგორიცაა ადამიანის ღირსება, გამჭვირვალობა, ანგარიშვალდებულება და მონაცემთა უსაფრთხოება წარმოადგენენ იმ სტანდარტებს, რომელიც ასახული უნდა იყოს ეროვნულ კანონმდებლობაში.

თავი III. პერსონალურ მონაცემთა დამუშავება საუნივერსიტეტო სივრცეში

3.1. მონაცემთა კატეგორიები და დამუშავების მიზნები უნივერსიტეტებში

უმაღლესი საგანმანათლებლო დაწესებულებები პერსონალურ მონაცემებს ამუშავებენ საგანმანათლებლო, ადმინისტრაციულ და სამეცნიერო პროცესებთან დაკავშირებით. ამდენად, უნივერსიტეტებში პერსონალური მონაცემების დამუშავება მოიცავს როგორც სტუდენტთა, ისე აკადემიური და ადმინისტრაციული პერსონალის ინფორმაციას, აგრეთვე სხვა დამატებით მონაცემებსაც, რომლებიც წარმოიქმნება კვლევის ან ონლაინ სწავლების პროცესში[35].

სტუდენტთა მონაცემები მოიცავს პირად ინფორმაციას (სახელი, გვარი, პირადი ნომერი, საკონტაქტო ინფორმაცია), აკადემიურ ჩანაწერებს (შეფასებები, საგნების დასწრება, საგანმანათლებლო პროგრამის პროგრესი), ფინანსურ მონაცემებს (სწავლის გადასახადები, სტიპენდიები, დაფინანსების წყაროები), ასევე ზოგიერთ შემთხვევაში ჯანმრთელობის ინფორმაციას - მაგალითად, შშმ სტუდენტთა მხარდაჭერის მიზნით. აღნიშნული მონაცემები

[33] United Nations General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, Resolution 45/95, 1990

[34] OECD, Privacy Guidelines: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013

[35] European Data Protection Board (EDPB), Guidelines on Data Protection in Educational Institutions, 2021.

მუშავდება სწავლების ადმინისტრირების, შეფასების, საერთაშორისო გაცვლით პროგრამებში მონაწილეობისა და აკადემიური ხარისხის მართვის მიზნებით[36].

პერსონალურ მონაცემთა დამუშავებისას გასათვალისწინებელ პრინციპებს შორის განსაკუთრებით აღსანიშნავია მიზნის შეზღუდვისა და მონაცემთა მინიმიზაციის პრინციპები. უნივერსიტეტების მიერ მონაცემთა შეგროვება უნდა ხდებოდეს მხოლოდ განსაზღვრული მიზნებისთვის და არ უნდა აღემატებოდეს მიზნისთვის აუცილებელ მოცულობას[37]. მაგალითად, სტუდენტის ფოტო ან ვიდეოჩანაწერი შეიძლება დამუშავდეს მხოლოდ იმ შემთხვევაში, თუ ეს აუცილებელია აკადემიური პროცესის ან უსაფრთხოების უზრუნველსაყოფად. ხოლო თუ ამგვარი მონაცემების დამუშავება უნივერსიტეტს ჭირდება მარკეტინგული მიზნებისათვის ამაზე სტუდენტის მხრიდან ცალკე უნდა იყოს თანხმობა აღებული.

აკადემიური და ადმინისტრაციული პერსონალის მონაცემები უნივერსიტეტების შრომითი ურთიერთობების ბუნებიდან გამომდინარე, კიდევ ერთი მნიშვნელოვანი კატეგორიაა. აღნიშნული მონაცემები მოიცავს პირად ინფორმაციას, შრომით ხელშეკრულებებს, ანაზღაურებას, სამეცნიერო აქტივობებს, შეფასების შედეგებსა და დისციპლინურ დოკუმენტებს[38]. მონაცემთა დამუშავება ეფუძნება შრომითი ურთიერთობების სამართლებრივ საფუძველს, რაც გულისხმობს დამსაქმებლის ვალდებულებას კონტრაქტის შესრულებისა და ადმინისტრაციული გამჭვირვალობის უზრუნველყოფის მიზნით[39].

თანამედროვე ციფრულ გარემოში უნივერსიტეტების მიერ დამუშავებულ მონაცემთა რაოდენობა მნიშვნელოვნად გაიზარდა ვიდეოჩანაწერების, ონლაინ სწავლების პლატფორმებისა და კვლევითი მონაცემების გამოყენების შედეგად[40]. ონლაინ სწავლებისას მუშავდება სტუდენტთა მონაწილეობასთან დაკავშირებული ინფორმაცია — ვიდეო და აუდიო ჩანაწერები, პლატფორმის აქტივობის ისტორია, IP მისამართები, ჩათებში გაკეთებული კომენტარები და სხვა მეტამონაცემები[41].

GDPR-ის მე-32 მუხლისა და საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ მოთხოვნების შესაბამისად, უნივერსიტეტები ვალდებულნი არიან უზრუნველყონ შესაბამისი ტექნიკური და ორგანიზაციული ზომები — დაშიფვრა, წვდომის კონტროლი და უსაფრთხო არქივირება[42].

კვლევითი მონაცემების დამუშავება, თავის მხრივ, დაკავშირებულია სამეცნიერო მიზნებთან და ხშირად მოიცავს გამოკითხვებს, ბიომეტრიულ ან ჯანმრთელობის მონაცემებს, სოციალური და დემოგრაფიული ინფორმაციის ანალიზს. GDPR-ის მე-89 მუხლი ასეთ

[36] Regulation (EU) 2016/679 (GDPR), Article 5(1)(b
[37] GDPR, Article 5(1)(c).
[38] OECD, Employment Data Processing Principles, Paris, 2020
[39] საქართველოს ორგანული კანონი, შრომის კოდექსი
[40] ENISA, Data Protection and Remote Learning Environments, 2021
[41] European Commission, Online Education and Data Governance Report, Brussels, 2022
[42] Regulation (EU) 2016/679 (GDPR), Article 32; კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 26

შემთხვევებში ითვალისწინებს გამონაკლისებს კვლევის ინტერესებიდან გამომდინარე, თუმცა მაინც მოითხოვს მონაცემთა ანონიმიზაციას და ინფორმირებული თანხმობის დაცვას[43].

ამრიგად, უნივერსიტეტებში მონაცემთა კატეგორიების მრავალფეროვნება მოითხოვს მკაფიოდ განსაზღვრულ მიზნებს, მკაცრ უსაფრთხოების წესებს და შესაბამის სამართლებრივ საფუძველს, რათა უზრუნველყოს როგორც განათლების ხარისხი, ისე ინდივიდის ინფორმაციული ავტონომია.

განსაკუთრებით მნიშვნელოვანია, რომ უნივერსიტეტმა მონაცემთა სუბიექტის თანხმობის მიღებისას ნათლად, მკაფიოდ და ამომწურავად განსაზღვროს ყველა მიზანი, რისთვისაც უნდა დამუშავდეს მონაცემი და ამ გზით ერთის მხრივ დაიცვას მონაცემთა მინიმაზიის პრინციპი და მეორეს მხრივ ხელი არ შეეშალოს უნივერსიტეტის სამეცნიერო საქმიანობასა თუ ეფექტურ ადმინისტრირებას.

3.2. მონაცემთა დამუშავების სამართლებრივი საფუძვლები უნივერსიტეტებში

პერსონალური მონაცემების დამუშავება დაშვებულია მხოლოდ იმ შემთხვევაში, თუ არსებობს შესაბამისი სამართლებრივი საფუძველი, რაც განსაზღვრულია როგორც ევროკავშირის ზოგად რეგულაციაში (GDPR), ისე საქართველოს კანონში „პერსონალურ მონაცემთა დაცვის შესახებ“. უნივერსიტეტებში მონაცემთა დამუშავების ყველაზე გავრცელებული სამართლებრივი საფუძვლებია: ინფორმირებული თანხმობა, კანონით დადგენილი ვალდებულება, ხელშეკრულების დადება ან შესრულება და საჯარო ინტერესი[44].

ინფორმირებული თანხმობა წარმოადგენს ერთ-ერთ მთავარ მექანიზმს მონაცემთა დამუშავების კანონიერების უზრუნველსაყოფად. GDPR-ის მე-6 მუხლის თანახმად, თანხმობა უნდა იყოს თავისუფლად გაცემული, ინფორმირებული, კონკრეტული და მკაფიო[45]. სტუდენტებმა ან თანამშრომლებმა უნდა იცოდნენ, რა მონაცემებს ამუშავებს უნივერსიტეტი, ვინ არის უფლებამოსილი პირი, რა მიზნებისთვის მუშავდება მონაცემები და რა ვადით ინახავს მათ უნივერსიტეტი. პრაქტიკაში ხშირად გვხვდება პრობლემა, როდესაც თანხმობის აღება ფორმალურ ხასიათს ატარებს და არ ხორციელდება სათანადო ინფორმირება დამუშავების მოცულობასა და შედეგებზე[46].

უნივერსიტეტების მიერ მონაცემთა დამუშავების გავრცელებული ლეგიტიმური საფუძველია კანონით დაკისრებული ვალდებულების შესრულება. უნივერსიტეტები რიგ შემთხვევებში მონაცემთა დამუშავებას ახორციელებენ კანონის მოთხოვნის საფუძველზე, მაგალითად, სახელმწიფო სტატისტიკური მიზნებისთვის, განათლების ხარისხის უზრუნველყოფის სააგენტოსთვის ინფორმაციის მიწოდების მიზნით ან განათლების სამინისტროსადმი

[43] GDPR, Article 89(1); European Research Council, Ethical Data Guidelines, 2020
[44] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 6, 2023
[45] GDPR, Article 6(1)(a)
[46] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, 2018

ანგარიშგებისათვის[47]. ასეთ შემთხვევებში დამუშავება არ საჭიროებს თანხმობას, თუმცა აუცილებელია გამჭვირვალობისა და მიზნობრიობის დაცვა[48].

ასევე გავრცელებული საფუძველია სტუდენტთან ან დასაქმებულთან ხელშეკრულების დადება და შესრულება. სტუდენტთან დადებული სასწავლო ხელშეკრულება ითვალისწინებს მონაცემთა დამუშავებას ადმინისტრაციული მიზნებისთვის - სწავლის რეგისტრაციის, შეფასების, ფინანსური ოპერაციების ან გაცვლით პროგრამებში ჩართვისათვის[49]. თანამშრომლების შემთხვევაში კი მონაცემთა დამუშავება აუცილებელია შრომითი ვალდებულებების შესრულებისა და ანაზღაურების პროცესის სამართლებრივი უზრუნველყოფისთვის[50].

ზოგიერთ შემთხვევაში უნივერსიტეტი შეიძლება დაეყრდნოს ლეგიტიმურ ინტერესს - მაგალითად, კამერებით სივრცის მონიტორინგისას უსაფრხოების დაცვის მიზანს, თუმცა GDPR მკაცრად მოითხოვს, რომ ასეთი დამუშავება არ არღვევს მონაცემთა სუბიექტის ძირითად უფლებებს და მოხდეს ინტერესების დაბალანსება[51].

შესაბამისად უნივერსიტეტებში პერსონალური მონაცემების დამუშავება რთული პროცესია, რომელიც მოითხოვს მკაფიო სამართლებრივ საფუძველს. თითოეული მოქმედება - იქნება ეს სტუდენტის რეგისტრაცია, თანამშრომლის ხელფასის გაცემა თუ უსაფრთხოების კამერების მუშაობა - უნდა ეფუძნებოდეს GDPR-ითა და ქართული კანონმდებლობით გათვალისწინებულ ერთ-ერთ საფუძველს.

ინფორმირებული თანხმობა რჩება ყველაზე მნიშვნელოვან ინსტრუმენტად, მაგრამ მას სჭირდება რეალური ინფორმირება, არა მხოლოდ ფორმალური ხელმოწერა. ხშირ შემთხვევებში უნივერსიტეტს შეუძლია დაეყრდნოს კანონით დაკისრებულ ვალდებულებას ან სასწავლო-შრომით ხელშეკრულებას, რაც აღარ საჭიროებს ცალკე თანხმობას. მთავარია, რომ ნებისმიერ შემთხვევაში დაცული იყოს გამჭვირვალობა, მიზნობრიობა და მონაცემთა სუბიექტის ფუნდამენტური უფლებები.

3.3. მონაცემთა უსაფრთხოება და შენახვის ვადები

მონაცემთა უსაფრთხოება წარმოადგენს პერსონალურ მონაცემთა დაცვის სისტემის ერთ-ერთ ფუნდამენტურ ელემენტს, განსაკუთრებით ისეთ დაწესებულებებში, სადაც დიდი მოცულობის ინფორმაციის დამუშავება ყოველდღიურ რეჟიმში ხდება. უნივერსიტეტებში უსაფრთხოების უზრუნველყოფა მოიცავს როგორც ტექნიკურ, ისე ორგანიზაციულ ზომებს, რომლებიც უნდა იყოს ადეკვატური მონაცემთა დამუშავების რისკების მიმართ[52].

[47] საქართველოს განათლებისა და მეცნიერების სამინისტრო, მონაცემთა მიწოდების წესები, 2022
[48] European Data Protection Supervisor (EDPS), Opinion on Public Sector Data Processing, 2021
[49] პერსონალურ მონაცემთა დაცვის ინსპექტორი, Data Protection in Student Contracts, თბილისი, 2024
[50] საქართველოს ორგანული კანონი შრომის კოდექსი
[51] European Court of Justice (CJEU), Case C-13/16, Rīgas satiksme v. Datu valsts inspekcija, 201
[52] ENISA, Cybersecurity in Higher Education, 2023

ტექნიკური ზომები გულისხმობს დაშიფვრას, სერვერების დაცვას, ავტორიზაციის მექანიზმებს, ქსელის უსაფრთხოებასა და მონაცემთა არქივების რეგულარულ მონიტორინგს[53]. ორგანიზაციული ზომები კი მოიცავს მონაცემთა დაცვის პოლიტიკის შემუშავებას, თანამშრომელთა ტრენინგებს, წვდომის კონტროლის რეგლამენტირებასა და მონაცემთა დაცვის ოფიცრის ინსტიტუტის არსებობას.

მონაცემთა შენახვის ვადები განისაზღვრება დამუშავების მიზნებიდან გამომდინარე. GDPR-ის მე-5 მუხლის შესაბამისად, მონაცემები უნდა ინახებოდეს მხოლოდ იმ ვადით, რაც აუცილებელია მიზნის მისაღწევად, ხოლო შემდგომ უნდა განადგურდეს ან მოხდეს მათი დეპერსონალიზება[54]. უნივერსიტეტებმა უნდა შეიმუშაონ შიდა დოკუმენტი — *Data Retention Policy*, სადაც განსაზღვრული იქნება კონკრეტული ვადები: მაგალითად, სტუდენტთა შეფასების ჩანაწერები ინახება სწავლების დასრულებიდან რამდენიმე წლის განმავლობაში, ხოლო ფინანსური დოკუმენტები — ბუღალტრული ანგარიშგების ვადის ამოწურვამდე[55].

განსაკუთრებული ყურადღება ეთმობა მესამე პირებთან მონაცემთა გაზიარების რეგულაციებს. უნივერსიტეტები ხშირად თანამშრომლობენ პარტნიორ ორგანიზაციებთან, დამსაქმებლებთან ან საერთაშორისო უნივერსიტეტებთან გაცვლითი პროგრამების ფარგლებში. ასეთ შემთხვევაში მონაცემთა გადაცემა დაშვებულია მხოლოდ სათანადო დაცვის გარანტიების არსებობისას - მაგალითად, ევროკავშირის სტანდარტული საკონტრაქტო პირობების ან მონაცემთა დაცვის სამსახურის წინასწარი ნებართვის საფუძველზე[56].

საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსს ბრძანებით აქვს დამტკიცებული უსაფრთხო ქვეყნების ნუსხა.[57] ამჟამინდელი მონაცემებით ნუსხაში 49 ქვეყანა არის შეტანილი, მათ შორის ევროკავშირის ყველა წევრის ქვეყანა. აღინიშნულ ქვეყნებში პერსონალურ მონაცემთა დაცვის მაღალი სტანდარტები არსებობს და სწორედ ამიტომ ამ ქვეყნებში პერსონალურ მონაცემთა გადაცემისას არ არის საჭირო პერსონალურ მონაცემთა დაცვის სამსახურის თანხმობა.

უნივერსიტეტებში მონაცემთა უსაფრთხოებისა და შენახვის წესების დაცვა წარმოადგენს არა მხოლოდ სამართლებრივ, არამედ ეთიკურ ვალდებულებასაც. მონაცემთა დაცვის კულტურა უნდა გახდეს სასწავლო და ადმინისტრაციული მმართველობის განუყოფელი ნაწილი, რათა უზრუნველყოფილ იქნეს როგორც სტუდენტთა და თანამშრომელთა უფლებების დაცვა, ისე ინსტიტუციური ნდობის შენარჩუნება.

[53] ISO/IEC 27001:2022, Information Security Management Systems
[54] GDPR, Article 5(1)(e)
[55] ICO (UK Information Commissioner's Office), Data Retention and Deletion Guidance, 2022
[56] European Commission, Standard Contractual Clauses for Data Transfers, 2021
[57] საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსს ბრძანება #23, 2024 წლის 29 თებერვალი. იხ. https://pdps.ge/files/content/%E1%83%91%E1%83%A0%E1%83%AB%E1%83%90%E1%83%9C%E1%83%94%E1%83%91%E1%83%90%20%E2%84%9623_1709550754.pdf

თავი IV. საერთაშორისო გამოცდილების შედარებითი ანალიზი

4.1. GDPR-ის განხორციელება ევროკავშირის ქვეყნებში (გერმანია, პოლონეთი, ესტონეთი)

ევროკავშირის ზოგადი მონაცემთა დაცვის რეგულაცია (GDPR) გახდა ევროპული სამართლისათვის ერთ-ერთი ყველაზე გავლენიანი ინსტრუმენტი, რომელმაც წევრ ქვეყნებში მონაცემთა დაცვის სამართლებრივი კულტურა საფუძვლიანად შეცვალა. რეგულაციის პრაქტიკული განხორციელება განსხვავებულია სახელმწიფოების ადმინისტრაციული სტრუქტურის, განათლების სისტემის მოდელისა და უნივერსიტეტების ავტონომიის ხარისხის მიხედვით[58].

გერმანიაში მონაცემთა დაცვის ზედამხედველობა ფედერალური სტრუქტურის შესაბამისადაა ორგანიზებული. მოქმედებს როგორც ფედერალური, ასევე ადგილობრივი ზედამხედველობის ორგანოები, რომლებიც საჯარო უნივერსიტეტებში უზრუნველყოფენ GDPR-ისა და *Bundesdatenschutzgesetz (BDSG)*-ის შესრულებას[59]. გერმანიის უნივერსიტეტებს ეკისრებათ მოვალეობა დანიშნონ მონაცემთა დაცვის ოფიცერი (Data Protection Officer – DPO), აწარმოონ მონაცემთა დამუშავების რეესტრი და შეაფასონ მონაცემთა დაცვის გავლენა (DPIA) მაღალი რისკის შემთხვევებში[60].

პოლონეთში, GDPR-ის განხორციელება მოხდა ეროვნული კანონის — *Ustawa o ochronie danych osobowych* (2018). პოლონეთის უნივერსიტეტებს ევალებათ სტუდენტთა და თანამშრომელთა მონაცემთა დამუშავებისას არა მხოლოდ ინფორმირებული თანხმობის უზრუნველყოფა, არამედ ინფორმაციის გამჭვირვალე მიწოდება მონაცემთა სუბიექტებისთვის, მათ შორის ონლაინ ფორმატში[61].

ესტონეთი გამოირჩევა ერთ-ერთი ყველაზე განვითარებული ციფრული ინფრასტრუქტურით ევროპაში. GDPR ინტეგრირებულია ფართო ელექტრონულ მმართველობის მოდელში (*e-Estonia*), სადაც უნივერსიტეტების მონაცემთა სისტემები დაკავშირებულია სახელმწიფო ციფრულ რეესტრებთან. მონაცემთა უსაფრთხოება უზრუნველყოფილია ბლოკჩეინ-ტექნოლოგიაზე დაფუძნებული სისტემა KSI Blockchain-ის მეშვეობით[62]. ესტონეთის უნივერსიტეტები იყენებენ ავტომატურ წვდომის კონტროლის მექანიზმებსა და სტუდენტური ჩანაწერების დაშიფვრას, რაც ევროკავშირის საუკეთესო პრაქტიკად მიიჩნევა[63].

ამრიგად, ევროკავშირის ქვეყნებში GDPR-ის განხორციელება უნივერსიტეტებში ხასიათდება სამართლებრივი სტანდარტების მკაცრი ინტეგრაციით, მონაცემთა დაცვის ოფიცრების

[58] Bygrave, L. A. (2021). Data Protection Law: Approaching its Rationale, Logic and Limits. Oxford University Press
[59] Bundesdatenschutzgesetz (BDSG), Federal Republic of Germany, 2018.
[60] Federal Commissioner for Data Protection and Freedom of Information (BfDI), University Data Protection Guidelines, 2021
[61] Ustawa o ochronie danych osobowych, Republic of Poland, 2018
[62] Ministry of Economic Affairs and Communications of Estonia, e-Governance and Data Security Report, 2022
[63] European Data Protection Board (EDPB), Best Practices in Higher Education under GDPR, 2023

ინსტიტუციური გაძლიერებით და ტექნოლოგიური უსაფრთხოების სისტემების განვითარებით.

4.2. უნივერსიტეტების პერსონალურ მონაცემთა დამუსავებასთან დაკავშირებული შიდა დოკუმენტაციის მაგალითები

ევროკავშირის ქვეყნების უნივერსიტეტების უმეტესობას შემუშავებული აქვს შიდა დოკუმენტები, რომლებიც განსაზღვრავს პერსონალურ მონაცემთა დამუშავების წესებს, პასუხისმგებლობებსა და სტუდენტთა ინფორმირების მექანიზმებს. ყველაზე გავრცელებული დოკუმენტებია პერსონალურ მონაცემთა პოლიტიკის დოკუმენტი, კონფიდენციალობის განაცხადი და მონაცემთა განადგურების პოლიტიკა., რომლებიც GDPR-ის მოთხოვნებთან თანხვედრაშია შემუშავებული[64].

მაგალითად, კემბრიჯის უნივერსიტეტის მონაცემთა დაცვის პოლიტიკა განსაზღვრავს მონაცემთა დამუშავების სამართლებრივ საფუძვლებს, დამუშავების მიზნებს, მონაცემთა შენახვის ვადებსა და მონაცემთა სუბიექტის უფლებების გამოყენების პროცედურებს[65]. პოლიტიკა ხაზს უსვამს ანგარიშვალდებულების პრინციპს - უნივერსიტეტი ვალდებულია არა მხოლოდ დაიცვას წესები, არამედ დაამტკიცოს მათი შესრულება შესაბამისი დოკუმენტაციით.

ბერლინის ჰუმბოლდტის უნივერსიტეტში მოქმედი პერსონალურ მონაცემთა დაცვის წესები (*Datenschutzordnung)* დეტალურად აღწერს სტუდენტთა მონაცემთა დამუშავების პროცესს, მათ შორის ლექციების ვიდეოჩანაწერებისა და ონლაინ სწავლების გარემოში მიღებული ინფორმაციის რეგულაციებს[66]. უნივერსიტეტს ჰყავს მონაცემთა დაცვის ოფიცერი, რომელიც დამოუკიდებელია ადმინისტრაციული მენეჯმენტისგან და ანგარიშვალდებულია უშუალოდ უნივერსიტეტის საბჭოს წინაშე.

ტარტუს უნივერსიტეტში (ესტონეთი) მოქმედი კონფიდენციალურობის განაცხადი (*Privacy Notice)* გამჭვირვალობის მაღალ სტანდარტს აწესებს - ყველა სტუდენტს და თანამშრომელს ონლაინ აქვს წვდომა იმ მონაცემებზე, რასაც უნივერსიტეტი ამუშავებს მათ შესახებ[67].

აღნიშნული მაგალითები აჩვენებს, რომ ევროპული უნივერსიტეტების შიდა დოკუმენტაცია აგებულია GDPR-ის პრინციპებზე დაყრდნობითა და გამჭვირვალობის მაღალი სტანდარტის დაცვით.

4.3. საერთაშორისო პრაქტიკის გაზიარების შესაძლებლობა საქართველოს უმაღლეს საგანმანათლებლო სივრცეში

საქართველოს უმაღლესი საგანმანათლებლო დაწესებულებები უკანასკნელი წლებია მნიშვნელოვან პროგრესს განიცდიან პერსონალურ მონაცემთა დაცვის თვალსაზრისით, რაც ერთი მხრივ კანონმდებლობის გამკაცრებითაა განპირობებული, ხოლო მეორე მხრივ

[64] EDPB, Guidelines on Data Protection by Design and by Default, 2020
[65] University of Cambridge, Data Protection Policy, 2023
[66] Humboldt-Universität zu Berlin, Datenschutzordnung, 2022
[67] University of Tartu, Privacy Notice for Students and Staff, 2023

ცნობიერების ამაღლების დონით. თუმცა კვლავ რჩება მნიშვნელოვანი გამოწვევები, რომლებთან გასამკლავებლადაც მნიშვნელოვანია საუკეთესო საერთაშორისო პრაქტიკის გაზიარება.

მნიშვნელოვანია გადაიდგას ეფექტური ნაბიჯები შემდეგი მიმართულებით:

1. ინსტიტუციური ჩარჩოს გაძლიერება - მონაცემთა დაცვის ოფიცრების ინსტიტუტის გაძლიერება და მათთვის შესაბამისი რესურსების გამოყოფა;

2. სასწავლო პროგრამებში მონაცემთა დაცვის ინტეგრაცია - GDPR-ისა და ეთიკური ნორმების სწავლება როგორც სამართლის, ისე საინფორმაციო ტექნოლოგიების ფაკულტეტებზე[68];

3. ტექნიკური ინფრასტრუქტურის მოდერნიზაცია — მონაცემთა უსაფრთხოების სერტიფიცირებული სტანდარტების დანერგვა (ISO 27001, ISO 27701), დაშიფვრისა და წვდომის კონტროლის სისტემების გაუმჯობესება[69].

გარდა ამისა, მნიშვნელოვანია ევროპულ უნივერსიტეტებთან თანამშრომლობა ერთობლივი კვლევითი პროექტების ფარგლებში, სადაც გამოყენებული იქნება მონაცემთა დაცვის ერთიანი ჩარჩოები და ინსტრუმენტები (მაგალითად, *GDPR Toolbox for Universities*)[70].

ამრიგად, საერთაშორისო პრაქტიკის მექანიკური გადმოტანა არასაკმარისია - საჭიროა მისი ადაპტაცია საქართველოს სამართლებრივ და ტექნოლოგიურ რეალობასთან. მნიშვნელოვანია დოკუმენტების შედგენა თუ პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნა არ ატარებდეს ფორმალურ ხასიათს და მონაცემთა დამუშავებამდე ხდებოდეს, რისკების შესწავლა და მონაცემთა დამუშავების ზეგავლენის შეფასება ადამიანის უფლებებზე. მხოლოდ ამ გზით შეძლებს ქვეყანა უნივერსიტეტებში ისეთი მონაცემთა დაცვის მოდელის ჩამოყალიბებას, რომელიც სრულად შეესაბამება ევროპულ ღირებულებებს და ამავდროულად იცავს აკადემიური თავისუფლების პრინციპებს.

V. პრაქტიკული და სამართლებრივი გამოწვევები საქართველოში

5.1. ინფორმირებული თანხმობის მართვის სირთულეები

ინფორმირებული თანხმობა პერსონალური მონაცემთა დაცვის ერთ-ერთი ძირითადი ლეგიტიმური საფუძველია, რომელიც უზრუნველყოფს გამჭვირვალობის პრინციპის რეალიზებას და სუბიექტის მონაწილეობას საკუთარი პერსონალური მონაცემების დამუშავების პროცესში. GDPR-ისა და საქართველოს ახალი კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ თანახმად, თანხმობა უნდა იყოს თავისუფლად გაცემული, კონკრეტული, ინფორმირებული და მკაფიო[71]. თუმცა საქართველოს უმაღლეს საგანმანათლებლო

[68] European University Association (EUA), Data Protection and Ethics in Higher Education, 2022
[69] ISO/IEC 27701:2019, Privacy Information Management Systems
[70] European Commission, GDPR Toolbox for Universities Project, 2023
[71] Regulation (EU) 2016/679 (GDPR), Article 6(1)(a

დაწესებულებებში აღნიშნული პრინციპის პრაქტიკული განხორციელება ხშირად სერიოზულ სირთულეებს აწყდება.

პირველი პრობლემა დაკავშირებულია თანხმობის ფორმალიზებულ ხასიათთან. უნივერსიტეტების უმეტესობაში თანხმობა მოითხოვება რეგისტრაციის ან სტუდენტთან ხელშეკრულების გაფორმებისას, თუმცა ეს პროცესი უმეტესად ტექნიკურ ფორმალობად რჩება და არ უზრუნველყოფს სტუდენტების ინფორმირებას მონაცემთა დამუშავების მიზნებისა და შედეგების შესახებ[72]. ხშირად უნივერსიტეტი მხოლოდ ერთიან დოკუმენტში უთითებს, რომ სტუდენტი ეთანხმება მონაცემთა დამუშავებას საგანმანათლებლო მიზნებისთვის, რაც ვერ აკმაყოფილებს GDPR-ის მოთხოვნას თანხმობის ინფორნირებულობისა და მიზნობრიობის შესახებ[73].

არანაკლები პრობლემაა, როდესაც უნივერსიტეტი იღებს თანხმობას იმ შემთხვევაშიც, როდესაც არსებობს მონაცემთა დამუშავების სხვა ლეგიტიმური საფუძველი, მაგ. მონაცემთა დამუშავება კანონითაა გათვალისწინებული (“კანონი უმაღლესი განათლების შესახებ” და სხვა ნორმატიული აქტები, რომელიც ითვალისწინებს მონაცემთა სავალდებულო აღრიცხვასა და განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტროსთვის გადაცემას) ან მონაცემთა დამუშავება აუცილებელია განათლების შესახებ მომსახურების ხელშეკრულების დასადებად. როდესაც არსებობს მონაცემთა დამუშავების სხვა ლეგიტიმური საფუძველი და მაინც ხდება თანხმობის მიღება ეს პრაქტიკაში წარმოშობს სხვა პრობლემებს. GDPR მოითხოვს, რომ სუბიექტს ნებისმიერ დროს ჰქონდეს უფლება გააუქმოს თანხმობა იმავე ფორმით რა ფორმითაც მისცა თანხმობა[74]. თანხმობის გამოხმობის შემდეგ მონაცემთა დამუშავება უნდა შეწყდეს. თუ თანხმობა იმ შემთხვევაშია მოპოვებული, როდესაც არსებობდა მონაცემთა დამუშავების სხვა ლეგიტიმური საფუძველი, მონაცემთა სუბიექტს უჩნდება არასწორი აღქმა, რომ თანხმობის გამოხმობის შემთხვევაში შეწყდება მონაცემების დამუშავება. ამ შემთხვევაში თანხმობის გამოხმობის უფლება ვერ რეალიზდება. მაგ. თუკი სტუდენტი მოითხოვს რომ მისი მონაცემები წაიშალოს განათლების სამინისტროს ბაზებიდან ეს უფლება ვერ განხორციელდება.

თანხმობა სტუდენტისაგან მხოლოდ იმ შემთხვევაში უნდა იყოს მოთხოვნილი თუკი მონაცემთა დამუშავება არ არის გათვალისწინებული კანონით ან არ არსებობს სხვა ლეგიტიმური საფუძველი, მაგალითად იმ შემთხვევაში, როდესაც უნივერსიტეტს სტუდენტის მონაცემები ჭირდება სტატეგიული განვითარებისათვის კვლევის ჩასატარებლად ან სტუდენტის ფოტო/ვიდეო გამოსახულება ჭირდება სოციალურ მედიაში განსათავსებლად მარკეტინგული მიზნებისათვის.

[72] პერსონალურ მონაცემთა დაცვის ინსპექტორი, წლიური ანგარიში 2023, თბილისი, 2024
[73] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, 2018
[74] GDPR, Recital 42–43

მონაცემების ნებისმიერი დამუშავებისას, მიუხედავად იმისა თუ რა საფუძვლით მუშავდება მონაცემები მნიშვნელოვანია დაცული იყოს მონაცემთა მინიმიზაციის პრინციპი[75].

კვლევის ფარგლებში გამოიკვეთა, რომ სასწავლო ელექტრონულ პლატფორმებსა და პირად საქმეებში ხშირად მოითოვება დედის, მამის ტელეფონის ნომერი და პერსონალური მონაცემები, აღნიშნული დასაბუთებულია იმით რომ საჭიროების შემთხვევაში როდესაც ვერ ხდება სტუდენტთან დაკავშირება გამოიყენება ეს მონაცემები თუმცა მაინც სადავოა ასეთი ინფორმაციის დამუშავების პროპორციულობა.

პრობლემა განსაკუთრებით მწვავედ იჩენს თავს ონლაინ სწავლებისას, სადაც ლექციების ჩაწერა და სტუდენტთა გამოსახულების დაფიქსირება ხშირ შემთხვევაში ხდება წინასწარი თანხმობის გარეშე[76]. პერსონალურ მონაცემთა დაცვის სამსახურის ანგარიშების მიხედვით, ეს პრაქტიკა წარმოადგენს ერთ-ერთ ყველაზე გავრცელებულ დარღვევას განათლების სფეროში.

ამრიგად, ინფორმირებული თანხმობის მექანიზმის არასრულყოფილება საქართველოში უნივერსიტეტებში ქმნის რეალურ საფრთხეს როგორც სამართლებრივი, ისე ეთიკური თვალსაზრისით.

5.2. მონაცემთა დაცვის ოფიცრის ინსტიტუტის ფორმალური ან არასაკმარისი ფუნქციონირება

საქართველოს ახალი კანონმდებლობა ითვალისწინებს მონაცემთა დაცვის ოფიცრის (Data Protection Officer – DPO) დანიშვნის ვალდებულებას იმ ორგანიზაციებისთვის, რომლებიც ახორციელებენ დიდი რაოდენობით მონაცემთა დამუშავებას ან ახორციელებენ მონაცემთა სუბიექტების ქცევის სისტემურ და მასშტაბურ მონიტორინგს[77].

უნივერსიტეტებს სწორედ ზემოთაღნიშნული კრიტერიუმიდან გამომდინარე ევალება ჰყავდეს პერსონალურ მონაცემთა დაცვის ოფიცერი. მიუხედავად ამისა ბევრ უნივერსიტეტში DPO-ის პოზიცია ან არ არსებობს, ან მხოლოდ ფორმალურად, სხვა ადმინისტრაციულ თანამდებობასთან შეთავსებით ფუნქციონირებს რაც არღვევს GDPR-ის მოთხოვნას ოფიცრის დამოუკიდებლობისა და კომპეტენტურობისა შესახებ[78]. ამ გზით დანიშნული ოფიცრები/ოფიცერი ვერ ახორციელებს ეფექტიან ზედამხედველობას უნივერსიტეტის მონაცემთა დამუშავების პროცესებზე და ვერ ახდენს კვალიფიციურ კონსულტაციას.

ხშირია შემთხვევა როდესაც უნივერსიტეტები აფორმებენ მომსახურების ხელშეკრულებას კომპანიასთან ან კერძო პირთან პერსონალურ მონაცემთა ოფიცრის მომსახურების შესახებ. ხშირია შემთხვევა, როდესაც თანხების დაზოგვის მიზნით უნივერსიტეტები ნაკლები კვალიფიკაციის პირებსა თუ ორგანიზაციებზე აკეთებენ არჩევანს რაც შემდომ ამ უკანასკნელთა საქმიანობის ეფექტურობაზეც აისახება.

---

[75] Bygrave, L. A. (2021). Data Protection Law: Approaching its Rationale, Logic and Limits. Oxford University Press

[76] ENISA, Data Protection and Remote Learning Environments, 2021

[77] კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 44, საქართველოს პარლამენტი, 2023

[78] Regulation (EU) 2016/679 (GDPR), Article 38

ოფიცრების უმეტესობას არ გააჩნია სპეციალური ცოდნა მონაცემთა დაცვის სამართლის ან ინფორმაციული უსაფრთხოების სფეროში. შედეგად, მათ მიერ მომზადებული შიდა რეგულაციები ხშირად მხოლოდ ფორმალური შინაარსისაა და არ ითვალისწინებს ტექნიკურ რისკებს ან რეალურ საჭიროებებს[79].

ევროპული უნივერსიტეტების პრაქტიკა გვიჩვენებს, რომ DPO-ის ეფექტიანი ფუნქციონირება მოითხოვს მისთვის დამოუკიდებელი სტატუსის მინიჭებას, ანგარიშვალდებულების დადგენას უშუალოდ რექტორის ან სამეთვალყურეო საბჭოს წინაშე და პროფესიული განვითარების მექანიზმების დანერგვას[80].

პერსონალურ მონაცემთა დაცვის სამსახურის 2024 წლის ანგარიშში უნივერსიტეტემთან მიმართებით არაერთ პრობლემაზეა ხაზგასმა, მათ შორის თანხმობების არასწორად მოპოვება, მონაცემთა დაცვის პრინციპების დარღვევა, უსაფრთხოების ზომების დარღვევა, მონაცემთა უვადოდ შენახვა და აშ.[81] ყოველივე ეს ნათლად მიუთითებს, რომ უნივერსიტეტების დიდ ნაწილს არ ჰყავს კვალიფიციური ოფიცერი, რომელიც სწორ რეკომენდაციებს მიცემდა.

5.3. მონაცემთა შენახვის ვადებისა და უსაფრთხოების პროტოკოლების დარღვევები

მონაცემთა ორგანიზაციულ-ტექნიკური უსაფრთხოების ზომების დაცვა და მონაცემთა შენახვის ვადები წარმოადგენს ერთ-ერთ ყველაზე პრობლემურ მიმართულებას საქართველოს უმაღლეს საგანმანათლებლო დაწესებულებებში. GDPR-ის მე-5 მუხლის „ვადის შეზღუდვის“ პრინციპის თანახმად, მონაცემები უნდა ინახებოდეს მხოლოდ იმ ვადით, რაც აუცილებელია მიზნის მისაღწევად, ხოლო შემდგომ უნდა განადგურდეს ან შენახული იყოს დეპერსონალიზებული ფორმით[82].

საქართველოში უმეტესს უნივერსიტეტს არ აქვს შემუშავებული მონაცემთა განადგურების წესი (*Data Retention Policy*), რის გამოც ინფორმაცია ხშირად ინახება გაურკვეველი ვადით, ზოგჯერ წლების განმავლობაში, მიზნის ამოწურვის შემდეგაც. ეს არღვევს როგორც კანონის მოთხოვნას, ისე ინფორმაციის უსაფრთხოების ფუნდამენტურ პრინციპებს. საკითხს ართულებს ისიც, რომ დოკუმენტბრუნვისა და მათი შენახვის წესები დგინდება პრეზიდენტის ბრძანებულებით[83], საქმისწარმოების ერთიანი წესების დამტკიცებისა და ამოქმედების შესახებ, რომელიც მიღებულია 1999 წლი 01 ივლისს. დღესდღეობით საქართველოში მოქმედი აღნიშნული ბრძანებულება ძალზე მოძველებულია და საჭიროებს განახლებას.

განსაკუთრებული სირთულე წარმოიქმნება ტექნიკური ინფრასტრუქტურის სიმწირის გამო — უნივერსიტეტების უმეტესობას არ აქვს დაცული სერვერები ან დაშიფვრის სისტემა.

---

[79] პერსონალურ მონაცემთა დაცვის ინსპექტორი, DPO ინსტიტუტის პრაქტიკული შეფასება, თბილისი, 2024

[80] European Data Protection Board (EDPB), Guidelines on Data Protection Officers, 2020

[81] პერსონალურ მონაცემთა დაცვის სამსახური, წლიური ანგარიში 2024, https://pdps.ge/files/content/PDPS%20%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%98%202024_1743494187.pdf

[82] Regulation (EU) 2016/679 (GDPR), Article 5(1)(e)

[83] საქართველოს პრეზიდენტის ბრძანებულება N414, საქმისწარომების ერთიანი წესების დამტკიცებისა და ამოქმედების შესახებ. 01.07.1999

შედეგად, სტუდენტთა და თანამშრომელთა მონაცემები ინახება ღია ფორმატებში, ხშირად ხშირად იგზავნება ელ-ფოსტის ან google drive საშუალებით, რაც ზრდის ინფომაციის უკონტროლო გავრცელების რისკს.[84]

ევროპული კიბერუსაფრთხოების სააგენტოს (ENISA) 2023 წლის ანგარიშის თანახმად, ევროპულ უნივერსიტეტებში მონაცემთა გავრცელების 42% გამოწვეული იყო არასაკმარისი წვდომის კონტროლითა და არქივაციის სისტემების სისუსტით[85]. მსგავსი ტენდენცია შეინიშნება საქართველოშიც — პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ ჩატარებულმა მონიტორინგმა არაერთხელ დააფიქსირა შემთხვევები, როდესაც უნივერსიტეტებში არ ხორციელდებოდა რეგულარული უსაფრთხოების შეფასება.

პრობლემის გადაჭრა მოითხოვს უსაფრთხოების სტანდარტების დანერგვას, როგორიცაა ISO/IEC 27001 და 27701, მონაცემთა დაშიფვრის მექანიზმების დანერგვას და უსაფრთხო წაშლის (secure deletion) პოლიტიკის შემოღებას. ამასთან, აუცილებელია თანამშრომელთა რეგულარული ტრენინგი მონაცემთა უსაფრთხოების საკითხებზე, რათა დაცული იყოს არა მხოლოდ კანონმდებლობა, არამედ სტუდენტთა ნდობაც.

5.4. პერსონალის ცნობიერების დაბალი დონე მონაცემთა დაცვის საკითხებში

მონაცემთა დაცვის ეფექტიანობა უნივერსიტეტებში მნიშვნელოვნად დამოკიდებულია პერსონალის ცოდნასა და ცნობიერებაზე. უნივერსიტეტში პერსონალურ მონაცემთა ეფექტიანად დაცვისათვის მნიშვნელოვანია არა მხოლოდ ოფიცრის კომპეტენტურობა არამედ სხვა დასაქმებულთა ცნობიერების ამაღლება. ამისათვის კი საუკეთესო გზა არის თანამშრომელთა ტრენინგი პერსონალურ მონაცემთა დაცვსი სფეროში.

ბევრ უნივერსიტეტში თანამშრომლებს არ აქვთ მინიმალური ცოდნა მონაცემთა დაცვის პრინციპების, ინფორმირებული თანხმობის, ან უსაფრთხოების ზომების შესახებ. შედეგად, ხშირია შემთხვევები, როდესაც მონაცემები გაზიარებულია დაუცველ არხებზე ან დამუშავებულია არალეგიტიმურად.

ევროპული გამოცდილება აჩვენებს, რომ მონაცემთა დაცვის კულტურის ჩამოყალიბება იწყება განათლებიდან — მაგალითად, ფინეთისა და დანიაში უნივერსიტეტები თანამშრომლებს სთავაზობენ სავალდებულო ელექტრონულ კურსებს GDPR-ზე და ინფორმაციული ეთიკის საფუძვლებზე[86].

საქართველოში ამ მიმართულებით საჭიროა სისტემური მიდგომა:

1. უნივერსიტეტებმა უნდა დანერგონ შიდა ტრენინგ-პროგრამები, რომლებიც მოიცავს სამართლებრივ და ტექნოლოგიურ მოდულებს;

2. განათლების სამინისტრომ უნდა შექმნას ერთიანი სახელმძღვანელო მონაცემთა დაცვის ტრენინგის მინიმალური სტანდარტებისთვის;

[84] ISO/IEC 27701:2019, Privacy Information Management Systems
[85] ENISA, Cybersecurity in Higher Education Report, 2023
[86] European University Association (EUA), Data Protection Training in Higher Education, Brussels, 2022

3. პერსონალურ მონაცემთა დაცვის სამსახურმა უნდა განახორციელოს მონიტორინგი ტრენინგების შედეგების შესახებ.

ცნობიერების ამაღლება არა მხოლოდ ამცირებს დარღვევების რისკს, არამედ აყალიბებს პასუხისმგებლობის კულტურას, რაც უნივერსიტეტებში მონაცემთა დაცვის ერთ-ერთ ძირითად გარანტიად შეიძლება იქცეს.

5.5. აკადემიური თავისუფლებისა და მონაცემთა დაცვის უფლებებს შორის ბალანსის მოძებნის გამოწვევა

უმაღლესი განათლების სივრცეში ერთ-ერთი ყველაზე დელიკატური საკითხია აკადემიური თავისუფლებისა და პერსონალურ მონაცემთა დაცვის უფლების შორის ბალანსის დაცვა. აკადემიური თავისუფლება გულისხმობს სწავლების, კვლევის და აზრის თავისუფლებას, რაც ზოგჯერ მოითხოვს მონაცემთა ფართო გამოყენებას კვლევით მიზნებისთვის[87].

მონაცემთა დაცვის ევროპული კანონმდებლობა აცნობიერებს მეცნიერების განსაკუთრებულ მნიშვნელობასაც საზოგადოებისათვის. მონაცემთა დაცვის ზოგადი რეგულაცია და მოდერნიზებული 108-ე კონვენცია პერსონალურ მონაცემთა ხანგრძლივად შენახვის შესაძლებლობას იძლევა, თუ ისინი მუშავდება სამეცნიერო ან ისტორიული კვლევისათვის. ამასთან, დამუშავების კონკრეტული აქტივობის თავდაპირველი მიზნის მიუხედავად, პერსონალური მონაცემების შემდგომი გამოყენება სამეცნიერო კვლევისათვის არ უნდა ითვლებოდეს შეუთავსებელ მიზნად.[88]

GDPR-ის მე-89 მუხლი ითვალისწინებს გამონაკლისებს სამეცნიერო და სტატისტიკური მიზნებისთვის მონაცემთა დამუშავებისას, თუმცა ეს გამონაკლისები არ ნიშნავს მონაცემთა დაცვის პრინციპების გაუქმებას. პირიქით, რეგულაცია მოითხოვს ანონიმიზაციისა და ფსევდონიმიზაციის გამოყენებას, რათა დაცული იყოს პიროვნების იდენტობა[89].

უმაღლესი საგანმანათლებლო დაწესებულებები ხშირად დგანან ამ დილემის წინაშე აკადემიური თავისუფლების ხელშეწყობა თუ მონაცემთა დაცვის რეგულაციების მკაცრი დაცვა. მაგალითად, სტუდენტთა შეფასებების ან კვლევითი გამოკითხვების საჯაროდ გამოქვეყნება ზოგჯერ არღვევს კონფიდენციალობის პრინციპს[90].

ამ გამოწვევასთან გასამკლავებლად მნიშვნელოვანია კვლევითი პროექტების განხორციელებამდე ჩატარდეს ზეგავლენის შეფასება (DPIA) და მინიმამუმდე იყოს დაყვანილი პერსონალურ მონაცემთა უკანონოდ დამუშავების რისკები.

სწორი ბალანსის მოსაძებნად საჭიროა აკადემიური გარემოსთვის მორგებული სახელმძღვანელოს შექმნა, რომელიც განსაზღვრავს, რა პირობებშია დაშვებული მონაცემთა გამოყენება კვლევისთვის ისე, რომ არ დაირღვეს კონფიდენციალურობის უფლება.

---

[87] UNESCO, Recommendation Concerning the Status of Higher-Education Teaching Personnel, 1997

[88] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 5 (1) (ბ) და 108-ე მოდერნიზებული კონვენცია, მუხლი 5(4)(ბ)

[89] GDPR, Article 89.

[90] European Research Council, Ethical Guidelines for Data Protection in Research, 2021.

ამრიგად, მონაცემთა დაცვისა და აკადემიური თავისუფლების ბალანსი წარმოადგენს არა მხოლოდ სამართლებრივ, არამედ ღირებულებით გამოწვევას - მისი წარმატებით გადაჭრა განაპირობებს უნივერსიტეტის ეფექტურ მართვას, სამეცნიერო საქმიანობის დაუბრკოლებლად განხორციელებას და პერსონალურ მონაცემთა დაცვას საერთაშორისო სტანდარტების შესაბამისად.

დასკვნები და რეკომენდაციები

დასკვნები

პერსონალურ მონაცემთა დაცვის საკითხი საქართველოს უმაღლეს საგანმანათლებლო სივრცეში თანდათან იქცა ერთ-ერთ უმნიშვნელოვანეს სამართლებრივ და ეთიკურ გამოწვევად. ციფრული ტრანსფორმაციისა და ონლაინ სწავლების ზრდამ მნიშვნელოვნად გააფართოვა დამუშავებული მონაცემების მოცულობა, რაც საჭიროებს სამართლებრივი რეგულაციების პრაქტიკულ და არა მხოლოდ ფორმალურ განხორციელებას.

კვლევის შედეგად გამოიკვეთა, რომ საქართველოს კანონმდებლობის დაახლოებისა ევროკავშირის ზოგად მონაცემთა დაცვის რეგულაციასთან (GDPR), პრაქტიკაში ვერ ხორციელდება ახალი რეგულაციების ეფექტურად განხორციელება. უმაღლესი საგანმანათლებლო დაწესებულებებისთვის გამოწვევად რჩება ინფორმირებული თანხმობის მართვა, ოფიცრის ინსტიტუტის ფორმალური ფუნქციონირება, უსაფრთხოების პროტოკოლების სისუსტე და პერსონალის არასაკმარისი ცოდნა მონაცემთა დაცვის საკითხებში.

ამავე დროს, უნივერსიტეტებისათვის დამახასიათებელია გარკვეული ღირებულებითი დილემა - აკადემიური თავისუფლებისა და მონაცემთა დაცვის უფლების ბალანსის უზრუნველყოფა. ამ კონტექსტში განსაკუთრებით მნიშვნელოვანია ის, რომ უნივერსიტეტებმა დაიცვან კვლევითი თავისუფლების პრინციპი ისე, რომ არ დაირღვეს ინდივიდთა უფლებები პერსონალურ მონაცემთა დაცვაზე.

დასკვნის სახით შეიძლება ითქვას, რომ პერსონალური მონაცემთა დაცვის სისტემა საქართველოს უმაღლეს საგანმანათლებლო სივრცეში დგას გარდამავალ ეტაპზე: ფორმალური შესაბამისობიდან რეალური დაცვისკენ. ამ პროცესის წარმატება დამოკიდებულია სამ ძირითად ფაქტორზე: სამართლებრივ თანმიმდევრულობაზე, ეფექტიან შიდა მმართველობასა და ცნობიერების ამაღლებაზე.

თუ აღნიშნული რეკომენდაციები განხორციელდება, საქართველოს უნივერსიტეტებს ექნებათ შესაძლებლობა შექმნან ისეთი გარემო, რომელიც არა მხოლოდ აკმაყოფილებს ევროპულ სამართლებრივ სტანდარტებს, არამედ აყალიბებს პასუხისმგებლობისა და ნდობის კულტურას. ეს კი გრძელვადიან პერსპექტივაში განამტკიცებს როგორც განათლების ხარისხს, ისე ქვეყნის ინტეგრაციას ევროპულ საგანმანათლებლო სივრცეში.

რეკომენდაციები

საქართველოს უმაღლეს საგანმანათლებლო დაწესებულებებში პერსონალური მონაცემთა დაცვის მექანიზმების გაუმჯობესება მოითხოვს არა მხოლოდ სამართლებრივ ჩარჩოს

დახვეწას, არამედ ეფექტიანი ინსტიტუციური პოლიტიკის ჩამოყალიბებას. არსებული მდგომარეობის ანალიზის საფუძველზე შესაძლებელია ჩამოყალიბდეს რამდენიმე ძირითადი რეკომენდაცია, რომელთა განხორციელებაც მნიშვნელოვნად გააძლიერებს მონაცემთა დაცვის კულტურას უნივერსიტეტებში:

აუცილებელია უნივერსიტეტებში მონაცემთა დაცვის პოლიტიკის გაძლიერება და გამჭვირვალობის ზრდა. უნივერსიტეტებმა უნდა შეიმუშაონ მკაფიო და ხელმისაწვდომი პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტი, რომელიც განსაზღვრავს მონაცემთა დამუშავების მიზნებს, სამართლებრივ საფუძვლებს, შენახვის ვადებსა და სუბიექტთა უფლებების განხორციელების წესს. აღნიშნული დოკუმენტი უნდა იყოს საჯაროდ გამოქვეყნებული უნივერსიტეტის ვებგვერდზე და ხელმისაწვდომი ყველა დაინტერესებული პირისთვის. ასევე საჭიროა მონაცემთა დაცვის წლიური ანგარიშების შემოღება, რაც გაზრდის გამჭვირვალობასა და ანგარიშვალდებულებას სტუდენტებისა და დასაქმებული პირების წინაშე.

უნდა დაინერგოს პერსონალისა და სტუდენტების რეგულარული ტრენინგები მონაცემთა დაცვის საკითხებზე. კვლევამ აჩვენა, რომ ინფორმირებულობის ნაკლებობა ერთ-ერთი ყველაზე გავრცელებული მიზეზია საგანმანათლებლო სექტორში მონაცემთა დაცვის დარღვევების. ტრენინგები უნდა მოიცავდეს როგორც სამართლებრივ, ისე პრაქტიკულ კომპონენტებს — მაგალითად, მონაცემთა უსაფრთხოების მინიმალურ წესებს, თანხმობის მართვის მექანიზმებსა და მონაცემთა გაზიარების ეთიკას. ამასთან, მიზანშეწონილია შესაბამისი კურსების ინტეგრაცია უნივერსიტეტის სასწავლო გეგმებში, განსაკუთრებით იურიდიული, სოციალური და საინფორმაციო ტექნოლოგიების ფაკულტეტებზე.

მონაცემთა დაცვის ოფიცრის (DPO) პოზიცია ინსტიტუციურ დონეზე უნდა გაძლიერდეს. უმაღლეს სასწავლებლებში ოფიცერი უნდა იყოს დამოუკიდებელი ადმინისტრაციული ზეწოლისგან და ჰქონდეს საკმარისი რესურსი საკუთარი ფუნქციების შესასრულებლად. მიზანშეწონილია, რომ DPO ანგარიშვალდებული იყოს უშუალოდ უნივერსიტეტის მმართველ ორგანოს - აკადემიურ საბჭოს ან რექტორის წინაშე.

მიზანშეწონილია განხორციელდეს უნივერსიტეტების შიდა რეგულაციების ჰარმონიზაცია GDPR-ის პრინციპებთან. მიუხედავად იმისა, რომ საქართველოს ახალი კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ არსებითად ეფუძნება GDPR-ის მოდელს, შიდა დოკუმენტებში კვლავ შეინიშნება არასრული შესაბამისობა, განსაკუთრებით მონაცემთა შენახვის ვადების, თანხმობის ფორმებისა და კვლევითი გამონაკლისების გამოყენების ნაწილში. აუცილებელია განათლებისა და მეცნიერების სამინისტროსა და პერსონალურ მონაცემთა დაცვის ინსპექტორის ერთობლივი სახელმძღვანელოს შემუშავება, რომელიც განსაზღვრავს უნივერსიტეტებისთვის მინიმალურ სტანდარტებს მონაცემთა დაცვისა და უსაფრთხოების პოლიტიკისთვის.

მიზანშეწონილია ერთიანი ციფრული პლატფორმის შექმნა თანხმობის მართვისა და ინფორმაციის უსაფრთხოების მონიტორინგისთვის, რაც უნივერსიტეტებს საშუალებას მისცემს უფრო ეფექტიანად განახორციელონ მონაცემთა დამუშავების კონტროლი. ასეთი

სისტემის დანერგვა გაამარტივებს სტუდენტებისა და თანამშრომლებისთვის თავიანთი უფლებების რეალიზებას, მაგალითად, თანხმობის გაუქმებას ან მონაცემთა წაშლის მოთხოვნას.

საქართველოს უმაღლეს საგანმანათლებლო დაწესებულებებში ერთ-ერთი პრიორიტეტული მიმართულება უნდა იყოს მონაცემთა დაცვის რისკების რეგულარული შეფასება (DPIA). მნიშვნელოვანია, რომ უნივერსიტეტებმა სისტემურად განახორციელონ ზეგავლენის შეფასება ყველა იმ პროცესზე, რომელიც დაკავშირებულია მაღალი რისკის მქონე მონაცემთა დამუშავებასთან - მათ შორის სტუდენტების მონიტორინგის სისტემებზე, ვიდეოთვალთვალის კამერების გამოყენებაზე, განსაკუთრებული კატეგორიის მონაცემების შემცველ კვლევით პროექტებზე და ახალი IT ინფრასტრუქტურის დანერგვაზე.

უნივერსიტეტებმა უნდა განსაზღვრონ ინფორმაციული უსაფრთხოების მკაფიო ტექნიკური სტანდარტები რომელიც გააერთიანებს მონაცემთა უსაფრთხოებისთვის აუცილებელ მინიმალურ მოთხოვნებს. ასეთ მოთხოვნებად განიხილება მონაცემთა დაშიფვრა როგორც გადაცემის, ასევე შენახვის ეტაპზე, წვდომის უფლებების მკაცრად დიფერენცირება „need-to-know“ პრინციპით, ორეტაპიანი აუთენტიფიკაციის კომპიუტერული პროგრამით სარგებლობისას და მონაცემთა სარეზერვო ასლების წარმოება. აღნიშნული ზომები მნიშვნელოვნად ზრდის მონაცემთა უსაფრთხოებას და ამცირებს შემთხვევითი ან მიზანმიმართული დარღვევების ალბათობას.

უნივერსიტეტებმა განსაკუთრებული ყურადღება უნდა დაუთმონ მონაცემთა დამუშავების შესაბამისი ლეგიტიმური საფუძვლის სწორად განსაზღვრას და თითოეული პროცესის მიზანშეწონილობის შეფასებას. პრაქტიკაში ხშირად აღინიშნება, რომ თანხმობა გამოიყენება ფორმალურად, მაშინ როდესაც მონაცემთა დამუშავება შეიძლება ხორციელდეს სხვა, უფრო შესაფერის სამართლებრივ საფუძველზე, როგორიცაა კანონით დადგენილი ვალდებულება, ხელშეკრულების შესრულება ან საჯარო/ლეგიტიმური ინტერესი. მნიშვნელოვანია, რომ უნივერსიტეტმა არ მოითხოვოს თანხმობა იმ შემთხვევებში, როდესაც დამუშავება დამოუკიდებლად დასაშვებია სხვა სამართლებრივი საფუძვლით, რადგან ასეთ გარემოებაში რეალურად ვერ ხერხდება თანხმობის გამოხმობა და სუბიექტს არ ეძლევა მისი გამოყენების შესაძლებლობა. სწორი სამართლებრივი საფუძვლის შერჩევა უზრუნველყოფს გამჭვირვალობას და უფლებების დაცვას მაღალი სტანდარტებით.

მონაცემთა კანონიერად დამუშავებისთვის აუცილებელია იმ საკანონმდებლო ბაზის განახლება რომელიც შეეხება დოკუმენტბრუნვასა და საქმისწარმოების წესებს. მნიშვნელოვანია ისიც, რომ უნივერისტეტების დიდი ნაწილი დოკუმენტბრუნვას ახორციელებს ელექტრონული პროგრამის (e-flow) საშუალებით, სასურველია აღნიშნული პროგრამის განახლება ისე რომ გათვალისწინებულ იქნას მონაცემთა დამუშავების სტანდარტები და მიზანშეწონილია შესაბამისი პროგრამის შექმნა რომელიც უზრუნველყოფს ელექტრონული არქივის სათანდო დონეზე წარმოებას.

ამგვარი ნაბიჯები შექმნის მონაცემთა დაცვის მდგრად კულტურას, რომელიც დაეფუძნება არა მხოლოდ კანონმდებლობას, არამედ პასუხისმგებლობისა და ეთიკის პრინციპებსაც.

ბიბლიოგრაფია

მონოგრაფიები, ნორმატიული აქტები

1. Bygrave, Lee A. *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press, 2014.
2. Bygrave, Lee A. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Oxford: Oxford University Press, 2021.
3. Gutwirth, Serge, and Paul De Hert. *Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power*. Dordrecht: Springer, 2010.
4. Solove, Daniel J. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.
5. საქართველოს კონსტიტუცია. საქართველოს საკანონმდებლო მაცნე, 24 აგვისტო, 1995.
6. საქართველოს ორგანული კანონი „საქართველოს შრომის კოდექსი“. საქართველოს საკანონმდებლო მაცნე.
7. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“. საქართველოს საკანონმდებლო მაცნე, 14 ივნისი, 2023.
8. საქართველოს პრეზიდენტის ბრძანებულება №414 „საქმისწარმოების ერთიანი წესების დამტკიცებისა და ამოქმედების შესახებ“. 1 ივლისი, 1999.
9. საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება №23. „პერსონალურ მონაცემთა დაცვის სამსახურის საქმიანობასთან დაკავშირებული ადმინისტრაციული აქტის დამტკიცების შესახებ.“ 29 თებერვალი, 2024.
10. Association Agreement between the European Union and the European Atomic Energy Community and Their Member States, of the One Part, and Georgia, of the Other Part. Signed June 27, 2014.
11. Charter of Fundamental Rights of the European Union. Official Journal of the European Union, 2012/C 326/02.
12. Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+).* Strasbourg, 2018.
13. European Convention on Human Rights. Rome, November 4, 1950.
14. European Parliament and Council of the European Union. *Regulation (EU) 2016/679 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 (General Data Protection Regulation).* Official Journal of the European Union L119 (2016).
15. Bundesdatenschutzgesetz (BDSG). Federal Republic of Germany, 2018.
16. Republic of Poland. *Act on the Protection of Personal Data (Ustawa o ochronie danych osobowych).* 2018.
17. United Nations General Assembly. *Guidelines for the Regulation of Computerized Personal Data Files.* Resolution 45/95. New York, 1990.
18. Organisation for Economic Co-operation and Development (OECD). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Paris: OECD Publishing, 2013.
19. International Organization for Standardization (ISO). *ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements.* Geneva: ISO, 2022.
20. International Organization for Standardization (ISO). *ISO/IEC 27701:2019 – Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management.* Geneva: ISO, 2019.
21. UNESCO. *Recommendation concerning the Status of Higher-Education Teaching Personnel.* Paris, 1997.

22. სასამართლო პრაქტიკა
23. საქართველოს საკონსტიტუციო სასამართლო. გადაწყვეტილება №2/1/504. 2013.
24. საქართველოს უზენაესი სასამართლო. საქმე №ას-236-2018. გადაწყვეტილება, 12 აპრილი, 2018.
25. *Peck v. the United Kingdom*. Application no. 44647/98. Judgment of 28 January 2003.
26. *Z v. Finland*. Application no. 22009/93. Judgment of 25 February 1997.
27. *Rīgas satiksme v. Datu valsts inspekcija*. Case C-13/16. Judgment of the Court of Justice of the European Union, 2017.
28. საერთაშორისო ორგანიზაციების ანგარიშები, რეკომენდაციები და სახელმძღვანელოები
29. European Data Protection Board. *Best Practices in Higher Education under the GDPR*. Brussels, 2023.
30. European Data Protection Board. *Cooperation with Third Countries: Annual Report*. Brussels, 2023.
31. European Data Protection Board. *Guidelines on Data Protection by Design and by Default*. Brussels, 2020.
32. European Data Protection Board. *Guidelines on Data Protection in Educational Institutions*. Brussels, 2021.
33. European Data Protection Board. *Guidelines on Data Protection Officers*. Brussels, 2020.
34. European Data Protection Board. *Guidelines on the Legal Bases for Processing Personal Data*. Brussels, 2020.
35. European Commission. *Adequacy Decisions and GDPR Alignment Reports*. Brussels, 2022.
36. European Commission. *GDPR Toolbox for Universities Project*. Brussels, 2023.
37. European Commission. *Online Education and Data Governance Report*. Brussels, 2022.
38. European Commission. *Standard Contractual Clauses for Data Transfers*. Brussels, 2021.
39. European Data Protection Supervisor. *Opinion on Public Sector Data Processing*. Brussels, 2021.
40. European Union Agency for Cybersecurity (ENISA). *Cybersecurity in Higher Education*. Heraklion, 2023.
41. European Union Agency for Cybersecurity (ENISA). *Data Protection and Remote Learning Environments*. Heraklion, 2021.
42. European Union Agency for Cybersecurity (ENISA). *Technical Guidelines on Data Security*. Heraklion, 2021.
43. European Research Council. *Ethical Data Guidelines*. Brussels, 2020.
44. European Research Council. *Ethical Guidelines for Data Protection in Research*. Brussels, 2021.
45. European University Association. *Data Protection and Ethics in Higher Education*. Brussels, 2022.
46. European University Association. *Data Protection Training in Higher Education*. Brussels, 2022.
47. Organisation for Economic Co-operation and Development (OECD). *Employment Data Processing Principles*. Paris: OECD Publishing, 2020.
48. Information Commissioner's Office. *Data Retention and Deletion Guidance*. Wilmslow, 2022.
49. Information Commissioner's Office. *Principles of Transparency*. Wilmslow, 2022.
50. Federal Commissioner for Data Protection and Freedom of Information (BfDI). *University Data Protection Guidelines*. Bonn, 2021.
51. Ministry of Economic Affairs and Communications of Estonia. *e-Governance and Data Security Report*. Tallinn, 2022.

52. University of Cambridge. *Data Protection Policy*. Cambridge, 2023.
53. Humboldt-Universität zu Berlin. *Datenschutzordnung*. Berlin, 2022.
54. University of Tartu. *Privacy Notice for Students and Staff*. Tartu, 2023.