პერსონალურ მონაცემთა
დაცვის სამსახური

# რეკომენდაციები
## პერსონალურ მონაცემთა დამუშავების
# პრინციპების შესახებ

www.pdps.ge

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

შინაარსი

## შესავალი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, ევროპის კავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მსგავსად, ითვალისწინებს პერსონალურ მონაცემთა დამუშავების პრინციპებს.[1] საკანონმდებლო სიახლეს წარმოადგენს პერსონალურ მონაცემთა დამუშავების ორი პრინციპის — მონაცემთა დამუშავების გამჭვირვალობისა და მონაცემთა უსაფრთხოების დაცვის, მოწესრიგება. ამასთანავე, კანონის მე-4 მუხლით გათვალისწინებულ იქნა მონაცემთა შეგროვების, მოპოვების მიზნისგან განსხვავებული მიზნით მონაცემთა დამუშავების საკითხები. საგულისხმოა, რომ დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია უზრუნველყოს მონაცემთა დამუშავებისას შესაბამის პრინციპებთან შესაბამისობა, რაზეც მტკიცების ტვირთი მას აკისრია.

წინამდებარე რეკომენდაციები მიზნად ისახავს მონაცემთა დაცვის საერთაშორისო სტანდარტის შესაბამისად, პერსონალურ მონაცემთა დამუშავების პრინციპების განმარტებას, რათა შესაბამისმა პასუხისმგებელმა სუბიექტებმა სრულყოფილად აღიქვან მათთვის დაკისრებული ვალდებულებების არსი და ფარგლები. რეკომენდაციებში განხილულია პერსონალურ მონაცემთა დაცვის შემდეგი პრინციპები: კანონიერება, სამართლიანობა, გამჭვირვალობა და მონაცემთა დამუშავება მონაცემთა სუბიექტის ღირსების შეულახავად; კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზანი; მონაცემთა მინიმიზაცია; მონაცემთა ნამდვილობა და სიზუსტე; მონაცემთა შენახვის ვადის შეზღუდვა; მონაცემთა დამუშავების უსაფრთხოება.

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

[1] მე-4 მუხლი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ).

## 1. კანონიერება, სამართლიანობა, გამჭვირვალობა და მონაცემთა დამუშავება მონაცემთა სუბიექტის ღირსების შეულახავად

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტის მიხედვით, *„მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად, მონაცემთა სუბიექტისთვის გამჭვირვალედ და მისი ღირსების შეულახავად. მონაცემთა დამუშავების გამჭვირვალობის ვალდებულება არ ვრცელდება ამ კანონით დადგენილ გამონაკლის შემთხვევებზე“.*[2]

### 1.1.კანონიერება

პერსონალურ მონაცემთა კანონიერი დამუშავება გულისხმობს, რომ მონაცემები უნდა დამუშავდეს მხოლოდ მაშინ, როდესაც არსებობს შესაბამისი საფუძველი[3] და დაცულია ყველა სამართლებრივი მოთხოვნა.[4] დამუშავების ოპერაციები სამართლებრივ მოთხოვნებთან სრულ შესაბამისობაში უნდა იყოს.[5] “GDPR”-ის მიხედვით, უპირველეს ყოვლისა, იმისათვის, რომ დამუშავება კანონიერად იქნეს მიჩნეული, იგი უნდა შეესაბამებოდეს მე-6 მუხლს (მონაცემთა დამუშავების კანონიერება), რომელიც მოითხოვს, რომ დამუშავების ნებისმიერი ოპერაცია ამომწურავ ჩამონათვალში მოცემული ექვსი სამართლებრივი საფუძვლიდან მინიმუმ ერთს მაინც უნდა აკმაყოფილებდეს.[6] უნდა აღინიშნოს, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლი ასევე ადგენს სამართლებრივ საფუძვლებს, რისი არსებობის შემთხვევაშიც დაშვებულია პერსონალურ მონაცემთა დამუშავება მონაცემთა დამუშავებისთვის პასუხისმგებელი („პასუხისმგებელი პირი“) თუ დამუშავებაზე უფლებამოსილი პირების („უფლებამოსილი პირი“) მიერ. მოქმედი კანონმდებლობა ასევე ითვალისწინებს განსაკუთრებული კატეგორიის მონაცემთა დამუშავების სპეციალურ საფუძვლებს.[7]

ზემოაღნიშნულის გათვალისწინებით, პერსონალურ მონაცემთა შეგროვება და დამუშავების სხვა ოპერაციების განხორციელება მხოლოდ მაშინ არის შესაძლებელი, როდესაც არსებობს დამუშავების ლეგიტიმური საფუძველი, მაგალითად, თანხმობა.

---

[2] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 3144-XIმს-Xმპ, 14/06/2023 <https://www.matsne.gov.ge/document/view/5827307?publication=0> [26.02.2024].

[3] Adv. Prashant Mali, GDPR Articles with Commentary & EU Case Laws, 15.

[4] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 314.

[5] Sanjay Sharma, PhD with research associate Pranav Menon, 2020, 126.

[6] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].

[7] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლი, 3144-XIმს-Xმპ, 14/06/2023 <https://www.matsne.gov.ge/document/view/5827307?publication=0> [26.02.2024].

თუ პერსონალური მონაცემების შეგროვება განხორციელდა არაავტორიზებული წვდომის შედეგად, დამუშავება უკანონო იქნება და, შესაბამისად, დაირღვევა კანონიერების პრინციპი.[8] გარდა ამისა, მონაცემთა დამუშავებას უნდა გააჩნდეს ლეგიტიმური მიზანი, უნდა იყოს აუცილებელი და პროპორციული დემოკრატიულ საზოგადოებაში.[9]

### მაგალითი

მონაცემთა დაცვის ახლადდანიშნულმა ოფიცერმა თავის თანამშრომლებს სთხოვა, რომ გარკვეული ინფორმაციის მონაცემთა ბაზაში შესანახად სამართლებრივი საფუძველი დაესახელებინათ. ანალიზის შედეგად დადგინდა, რომ მონაცემთა დამუშავება არ შეესაბამებოდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლით გათვალისწინებულ არცერთ საფუძველს. თანამშრომლები ამტკიცებდნენ, რომ კომპანია აქამდეც ამუშავებდა შესაბამის მონაცემებს, ისევე როგორც სხვა კონკურენტი კომპანიები.[10] მოცემულ შემთხვევაში, დარღვეულია კანონიერების პრინციპი.

## 1.2.სამართლიანობა

სამართლიანობა ყოვლისმომცველი პრინციპია,[11] რომელიც მოითხოვს, რომ პერსონალური მონაცემები მონაცემთა სუბიექტის საზიანოდ, დისკრიმინაციულად არ დამუშავდეს, არ აღმოჩნდეს მოულოდნელი ან შეცდომაში შემყვანი.[12] ამ პრინციპის მიხედვით, მონაცემთა მოპოვება ან სხვაგვარად დამუშავება უსამართლო საშუალებებით, შეცდომაში შეყვანით ან მონაცემთა სუბიექტის ცოდნის გარეშე,

[8] Adv. Prashant Mali, GDPR Articles with Commentary & EU Case Laws, 15.

[9] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 314.

[10] GDPRhub, GDPR commentary, < https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].

[11] ევროკავშირის მართლმსაჯულების სასამართლომ *"Bara"*-ს საქმეში (CJEU, Case C- 201/ 14, Bara [2015], §34) დაადგინა, რომ პერსონალური მონაცემების სამართლიანი დამუშავების მოთხოვნის თანახმად, საჯარო დაწესებულებამ მონაცემთა სუბიექტებს მათი პერსონალური მონაცემების სხვა მსგავსი ორგანოსთვის გადაცემის შესახებ უნდა აცნობოს. იხ. Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 313.

[12] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §69, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> [26.02.2024].

დაუშვებელია.[13] მნიშვნელოვანია, რომ მონაცემთა სუბიექტი ინფორმირებული იყოს მისი პერსონალური მონაცემების დამუშავების შესახებ, როგორ მოხდება მონაცემების შეგროვება, შენახვა და გამოყენება. თუმცა, გარკვეულ შემთხვევებში, დამუშავება ნებადართულია კანონით და სამართლიანად ითვლება, მიუხედავად მონაცემთა სუბიექტის ცოდნისა და სურვილისა.[14]

დამუშავების ოპერაციის სამართლიანობის საკითხი კონტექსტის მიხედვით უნდა გადაწყდეს.[15] „მონაცემთა დაცვის ევროპული საბჭოს“ („EDPB“) ერთ-ერთ სახელმძღვანელოში[16] მოცემულია სამართლიანობის გარკვეული ელემენტების არასრული ჩამონათვალი, რომლებიც პერსონალური მონაცემების დამუშავებისას უნდა იქნეს დაცული. სამართლიანობის მნიშვნელოვან ელემენტებად აღიარებულია, მონაცემთა სუბიექტის მოლოდინი,[17] მისი მონაცემების გონივრული გამოყენების შესახებ,[18] ასევე, გარკვეული ფსიქოლოგიური მდგომარეობის გამო დისკრიმინაციისაგან ან ექსპლუატაციისაგან დაცვის უფლება. “EDPB”-ის განმარტების თანახმად, იმისათვის, რომ დამუშავება „სამართლიანი“ იყოს, დაუშვებელია მოტყუებით მონაცემთა დამუშავება და ყოველი არჩევანი ობიექტური და ნეიტრალური გზით უნდა იყოს წარმოდგენილი, შეცდომაში შემყვანი ან მანიპულაციური ენის ან დიზაინის თავიდან აცილების მიზნით.[19]

---

[13] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 314.

[14] Eduardo Ustaran, CIPP/E, Partner, Hogan Lovells, European Data Protection Law and Practice, Second Edition, 2019, 128.

[15] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].

[16] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> [26.02.2024].

[17] იხ. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Convention 108, Children's Data Protection in Education Systems: Challenges and Possible Remedies, 2019, 12, <https://rm.coe.int/t-pd-2019-06final-eng-report-children/1680a01b47> [26.02.2024].

[18] “*M.S.”-ს* საქმეში (Case of M.S. v. Sweden, [1997] ECHR App. No. 74/1996/693/885) სასამართლომ გამჭვირვალობის მოთხოვნასთან დაკავშირებით აღნიშნა, რომ პერსონალურ მონაცემებთან დაკავშირებით განხორციელებული ოპერაციები (როგორიცაა მონაცემთა მესამე მხარისთვის გადაცემა) აუცილებელია, ექცეოდეს მონაცემთა სუბიექტის გონივრული მოლოდინის ფარგლებში. სასამართლომ აღნიშნა, რომ სადავო მონაცემების შემდგომი გამოყენება ემსახურებოდა განსხვავებულ მიზანს, რომელიც მომჩივნის მოლოდინს სცდებოდა და დაასკვნა, რომ განხორციელდა მომჩივნის პირადი ცხოვრების უფლებაში ჩარევა. იხ. Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 313.

[19] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].

### მაგალითი

პირდაპირი მარკეტინგის განხორციელების მიზნით პასუხისმგებელმა პირმა მოიპოვა მომხმარებელთა თანხმობები, თუმცა ადრესატთა მხოლოდ 10%-გან მიიღო დადებითი პასუხი. მომხმარებელთა აბსოლუტურ უმრავლესობას საკუთარი მონაცემების დამუშავება არ სურდა. მომხმარებელთა თანხმობის მოტყუებით მოპოვების მიზნით, პასუხისმგებელმა პირმა შეცდომაში შემყვანი შაბლონები შეიმუშავა, ვინაიდან კომპანიის ადვოკატის განცხადებით, მსგავს საქმიანობას მონაცემთა დაცვის კანონმდებლობა პირდაპირ არ კრძალავდა. დამაბნეველი მექანიზმის დანერგვის შედეგად, პასუხისმგებელმა პირმა თანხმობების კოეფიციენტი 90%-მდე გაზარდა. მოცემულ შემთხვევაში დაირღვა სამართლიანობის პრინციპი, რადგან თანხმობები მოპოვებულ იქნა მომხმარებელთა შეცდომაში შეყვანის გზით.[20]

## 1.3.გამჭვირვალობა

მონაცემთა სამართლიანად დამუშავების პრინციპთან მჭიდროდაა დაკავშირებული გამჭვირვალობის პრინციპი. "GDPR"-ის მიღებამდე გამჭვირვალობის მოთხოვნა აღიქმებოდა სამართლიანობის ცნების შემადგენელ ნაწილად.[21] გამჭვირვალობის პრინციპი პერსონალურ მონაცემთა დაცვის შიდა კანონმდებლობაშიც სიახლეს წარმოადგენს. გამჭვირვალობის ვალდებულება მჭიდროდ არის დაკავშირებული მონაცემთა სუბიექტის ინფორმირების უფლებასთან.[22] გასათვალისწინებელია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი ითვალისწინებს საგამონაკლისო შემთხვევებს, რომლებზეც არ ვრცელდება მონაცემთა დამუშავების გამჭვირვალობის ვალდებულება.[23]

გამჭვირვალობის პრინციპის მიხედვით, ფიზიკური პირებისთვის ნათელი უნდა იყოს, რომ მათთან დაკავშირებული პერსონალური მონაცემების შეგროვება, გამოყენება, გაცნობა ან სხვა სახით დამუშავება ხორციელდება.[24] ამასთანავე, თუ პირებს ორგანიზაციის მიერ გარკვეული ინფორმაცია მიეწოდებათ მათი პერსონალური

[20] იქვე.
[21] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 314.
[22] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის 24-ე და 25-ე მუხლები, 3144-XIმს-Xმპ, 14/06/2023 <https://www.matsne.gov.ge/document/view/5827307?publication=0> [26.02.2024].
[23] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-13 მუხლის მე-3 პუნქტი, 3144-XIმს-Xმპ, 14/06/2023 <https://www.matsne.gov.ge/document/view/5827307?publication=0> [26.02.2024].
[24] GDPR, Recital 39.

მონაცემების გამოყენების შესახებ, მისი მიწოდება ლაკონიური, გამჭვირვალე, გასაგები და ადვილად ხელმისაწვდომი ფორმით, მკაფიო და მარტივი ენით უნდა მოხდეს. ინფორმაციის სიცხადე განსაკუთრებით მნიშვნელოვანია, როდესაც იგი ბავშვს მიეწოდება.[25]

მნიშვნელოვანია გამჭვირვალობის შესახებ ინფორმაციის შესაბამის აუდიტორიაზე მორგება.[26] ამიტომ, გამჭვირვალობის პრინციპი მოითხოვს, რომ როდესაც პასუხისმგებელი პირების სამიზნე აუდიტორიას ბავშვები წარმოადგენენ ან მათ პროდუქციას თუ მომსახურებას განსაკუთრებით ისინი იყენებენ, ნებისმიერი ინფორმაცია და კომუნიკაცია უნდა იყოს გადმოცემული მკაფიო და მარტივი ენით ან ადვილად გასაგები საშუალებებით.[27]

### მაგალითი

ყველა ორგანიზაცია, რომელსაც აქვს საკუთარი ვებსაიტი, ვალდებულია, გამოაქვეყნოს კონფიდენციალობის შესახებ განაცხადი/შეტყობინება, ხოლო განაცხადის/შეტყობინების პირდაპირი ბმული ნათლად უნდა ჩანდეს ვებსაიტის თითოეულ გვერდზე, ფართოდ გავრცელებული ტერმინის ქვეშ (მაგ., „კონფიდენციალობის დაცვა“, „კონფიდენციალობის პოლიტიკა“ ან „მონაცემთა დაცვის შესახებ შეტყობინება“). მონაცემთა გამჭვირვალობის პრინციპს ეწინააღმდეგება ტექსტის/ბმულის განთავსება იმგვარად, რაც მას ნაკლებად შესამჩნევს ხდის ან ართულებს მის მოძიებას ვებგვერდზე.[28]

## 1.4.მონაცემთა დამუშავება მონაცემთა სუბიექტის ღირსების შეულახავად

განსახილველი პრინციპის ერთ-ერთი მნიშვნელოვანი შემადგენელი ნაწილია მონაცემთა დამუშავება მონაცემთა სუბიექტის ღირსების შეულახავად. მონაცემთა დაცვის ფუნდამენტური უფლების მიზანია ადამიანების ღირსებისა და უფლებებისთვის საზიანო მონაცემთა დამუშავების თავიდან აცილება. შესაბამისად,

[25] Data Protection Commission, Irish DPA, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 27.

[26] Morgan A., The Transparency Challenge: Making children aware of their data protection rights and the risks online, Volume 23, No.1, 2018, 3, <https://www.dataprotection.ie/sites/default/files/uploads/2019-02/TransparencyChallenge.pdf> [26.02.2024].

[27] Article 29 Working Party Guidelines on transparency under Regulation 2016/679, 2018, §14, <https://ec.europa.eu/newsroom/article29/items/622227/en> [26.02.2024].

[28] იქვე, §11.

ადამიანის ღირსება და მონაცემთა დაცვის უფლება წარმოადგენს სახელმწიფო წესრიგის საფუძველს.[29]

მონაცემთა სუბიექტის ღირსების შეულახავად მონაცემთა დამუშავების საკითხზე მითითებას არ შეიცავს ისეთი საერთაშორისო ინსტრუმენტები, როგორიცაა "GDPR"-ისა[30] და მოდერნიზებული 108-ე კონვენციის[31] ანალოგიური დებულებები. მიუხედავად ამისა, მონაცემთა დაცვის ერთ-ერთი ევროპული ქვეყნის საზედამხედველო ორგანოს პრაქტიკის მიხედვით, მონაცემთა დაცვის უფლების კონტექსტში ადამიანის ღირსებას ენიჭება უპირატესი ძალა, ქვეყნის კონსტიტუციის, საკონსტიტუციო სასამართლოს გადაწყვეტილებებისა და სამოქალაქო სამართლის დებულებების ანალიზის საფუძველზე.[32]

### მაგალითი

ერთ-ერთი სკოლის პედაგოგმა გაკვეთილის მიმდინარეობისას მოსწავლეებს გადაუღო ფოტოსურათები, რაც გაეგზავნათ არასრულწლოვნების მშობლებს. ერთ ფოტოსურათზე აღბეჭდილნი იყვნენ მერხებთან მსხდომი ის მოსწავლეები, რომლებიც გაკვეთილზე მომზადებულნი გამოცხადდნენ, ხოლო მეორე ფოტოზე ასახულნი იყვნენ დაფასთან ე. წ. „ჩაცუცქულ" მდგომარეობაში მყოფი ის მოსწავლეები, რომლებსაც არ ჰქონდათ ნასწავლი გაკვეთილი. იმ ფაქტორის გათვალისწინებით, რომ მოსწავლეთა აღნიშნული მდგომარეობა უკავშირდებოდა მათ არადამაკმაყოფილებელ მოსწრებას, როგორც „ჩაცუცქულ", ასევე „დაჩოქილ" მდგომარეობაში ყოფნა აღიქმებოდა არასრულწლოვანთა ღირსების შელახვად, რაც, თავის მხრივ, ბავშვების ჩაგვრის, ე.წ. „ბულინგის", დისკრიმინაციისა და არასათანადო მოპყრობის მსხვერპლად გახდომის საფრთხეს შეიცავდა. განსახილველი მაგალითის მიხედვით, გაკვეთილისთვის მოუმზადებელი ბავშვების მონაცემების დამუშავებისას სკოლის

[29] The Agencia Española de Protección de Datos ("AEPD"), Case No. PS/00410/2020, 17.06.2021, <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00410/2020> [26.02.2024].

[30] იხ. GDPR-ის მე-5 მუხლი, 2016, <https://personaldata.ge/cdn/2018/11/GDPR-%E1%83%97%E1%83%90%E1%83%A0%E1%83%92%E1%83%9B%E1%83%90%E1%83%9C%E1%83%98.pdf> [26.02.2024].

[31] „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ" 108-ე კონვენციის შესწორების ოქმი CETS No. 223 („მოდერნიზებული 108-ე კონვენცია"), მიღებულ იქნა ევროპის საბჭოს მინისტრთა კომიტეტის მიერ, 128-ე სხდომაზე, რომელიც 2018 წლის 17-18 მაისს გაიმართა. იხ. მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 11, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf> [26.02.2024].

[32] იხ. The Agencia Española de Protección de Datos ("AEPD"), Case No. PS/00410/2020, 17.06.2021, <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00410/2020> [26.02.2024].

პედაგოგმა არ დაიცვა მონაცემთა სუბიექტის ღირსების შეულახავად მონაცემების დამუშავების პრინციპი.[33]

## 1.5.რეკომენდაციები

- ☑ მონაცემთა დამუშავების დაწყებამდე უნდა განხორციელდეს დამუშავების კანონიერი საფუძვლის იდენტიფიცირება, მათ შორის, განსაკუთრებული კატეგორიის მონაცემების დამუშავების შემთხვევაში.
- ☑ დამუშავების ოპერაციები პერსონალურ მონაცემთა დაცვის სამართლებრივ მოთხოვნებთან სრულ შესაბამისობაში უნდა იყოს.
- ☑ უნდა შეფასდეს, რა გავლენა ექნება პერსონალურ მონაცემთა დამუშავებას მონაცემთა სუბიექტზე და უნდა დასაბუთდეს ყოველგვარი უარყოფითი ზემოქმედება მასზე.
- ☑ პერსონალური მონაცემები გამოყენებულ უნდა იქნეს მხოლოდ მონაცემთა სუბიექტის გონივრული მოლოდინის შესაბამისად ან უნდა დასაბუთდეს, თუ რატომ არის ნებისმიერი მოულოდნელი დამუშავება გამართლებული.
- ☑ მონაცემთა შეგროვება არ უნდა განხორციელდეს მონაცემთა სუბიექტის მოტყუებით ან შეცდომაში შეყვანით.
- ☑ მონაცემთა სუბიექტს ინფორმაცია მისი პერსონალური მონაცემების გამოყენების შესახებ უნდა მიეწოდოთ ლაკონიურად, გამჭვირვალედ, გასაგებად და ადვილად ხელმისაწვდომი ფორმით, მკაფიო და მარტივი ენით.[34]
- ☑ მონაცემთა დამუშავება არ უნდა მოიცავდეს იმგვარ ქმედებებს, რაც ლახავს მონაცემთა სუბიექტის ღირსებას.

[33] პერსონალურ მონაცემთა დაცვის სამსახური, არასრულწლოვანთა პერსონალურ მონაცემთა დაცვა - თეორია და პრაქტიკა, 2023, 22-23, <https://personaldata.ge/ka/recommendations> [26.02.2024].

[34] ICO, Guide to the General Data Protection Regulation (GDPR), Principles, Lawful, fair and transparent processing, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/lawfulness-fairness-and-transparency/> [26.02.2024].

## 2. კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზანი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტის მიხედვით, *„მონაცემები უნდა შეგროვდეს/მოპოვებული უნდა იქნეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზნებისთვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებელი მიზნით.“*

მიზნის შეზღუდვა შიდა კანონმდებლობასა და მონაცემთა დაცვის საზედამხედველო ორგანოს პრაქტიკაში, ისევე როგორც მონაცემთა დაცვის ევროპულ სამართალში, ერთ-ერთი ფუნდამენტური პრინციპია. დამუშავების ნებისმიერი ოპერაციის მიზნის განსაზღვრა მონაცემთა დაცვის კანონმდებლობის გამოყენებისა და მონაცემთა დაცვის გარანტიების შემუშავებისთვის პირველი ეტაპია. ამასთანავე, მიზნის განსაზღვრა სხვა მოთხოვნების დაწესების წინაპირობას წარმოადგენს. მიზნის შეზღუდვის პრინციპი ადგენს საზღვრებს, რომლის ფარგლებშიც შესაძლებელია მოცემული მიზნისთვის შეგროვებული პერსონალური მონაცემების დამუშავება და შემდგომი გამოყენება. აღნიშნული პრინციპი გულისხმობს, რომ მონაცემები უნდა შეგროვდეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზნებისთვის.[35]

### 2.1.„კონკრეტული“

მიზნის კონკრეტულობა გულისხმობს, რომ ნებისმიერ შემთხვევაში, წინასწარ, არაუგვიანეს პერსონალურ მონაცემთა შეგროვების დაწყებისა,[36] მიზანი უნდა იყოს ზუსტად და სრულად იდენტიფიცირებადი. აღნიშნული საჭიროა იმის განსასაზღვრად, თუ რა სახის დამუშავებას მოიცავს კონკრეტული მიზანი. ასევე, კონკრეტული მიზანი მისი კანონთან შესაბამისობისა და გამოყენებული მონაცემთა დაცვის მექანიზმების შეფასების შესაძლებლობას იძლევა.[37]

გასათვალისწინებელია, რომ ზედმეტად ფართო მიზნების განსაზღვრა საფრთხეს უქმნის მიზნის შეზღუდვის პრინციპის დაცულობას. ზოგადი აღწერილობები, როგორიცაა „მომხმარებლის გამოცდილების გაუმჯობესება“, „მარკეტინგი“, „კვლევა“

[35] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 315.

[36] იქვე.

[37] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2013, 39, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> [26.02.2024].

ან „IT უსაფრთხოება“ საკმარისად კონკრეტული არ არის.[38] მაგალითად, “EDPB”-მ განმარტა, რომ ვიდეომეთვალყურეობის დროს, მონიტორინგის მიზნები უნდა დაკონკრეტდეს ყველა გამოყენებული სათვალთვალო კამერისთვის და ვიდეო მეთვალყურეობა მხოლოდ „უსაფრთხოების“ ან „თქვენი უსაფრთხოების მიზნით“ არ არის საკმარისად კონკრეტული.[39]

მიუხედავად იმისა, რომ მიზანი არ უნდა იყოს ძალიან ფართო, არ არსებობს შეზღუდვა იმის შესახებ, თუ რამდენად კონკრეტული შეიძლება იყოს იგი. კონკრეტულობის ზუსტი დონე ობიექტურად განსაზღვრული არ არის, ხშირ შემთხვევაში, შესაძლებელია, ფართო მიზნების დაყოფა მრავალ, უფრო კონკრეტულ მიზნად.[40]

პრაქტიკაში, მიზნის დეტალურობა და კონკრეტულობა დამოკიდებულია მონაცემების შეგროვებისა და დასამუშავებელ პერსონალურ მონაცემთა კონტექსტზე. ზოგიერთ შემთხვევაში, მარტივი ენა საკმარისი იქნება შესაბამისი სპეციფიკაციის უზრუნველსაყოფად, ხოლო სხვა შემთხვევებში შესაძლებელია უფრო დეტალური ინფორმაციის მითითება გახდეს საჭირო.[41]

### მაგალითები

- ადგილობრივი მაღაზია, რომელიც პროდუქციას პატარა ქალაქში ადგილობრივ მოსახლეობაზე ყიდის და მისი მომხმარებლების შესახებ მხოლოდ შეზღუდულ ინფორმაციას აგროვებს, არ საჭიროებს მიზნების ისევე დეტალურად დაკონკრეტებას, როგორც დიდი საცალო კომპანია, რომელიც საქონელს ვებსაიტის საშუალებით მთელ ევროპაში ყიდის და იყენებს კომპლექსურ ანალიტიკას, რათა მომხმარებელს მათზე მორგებული რეკლამები შესთავაზოს.[42]
- პასუხისმგებელი პირი მონაცემთა სუბიექტებს უცხადებს, რომ მათი მონაცემები გამოყენებული იქნება „ბიზნეს მიზნებისთვის“. მეტი კონკრეტულობისთვის, იურისტებმა დაამატეს მიზნების არასრული ჩამონათვალი. კერძოდ, მონაცემთა დამუშავების მიზნების შესახებ დებულებაში აღნიშნულია, რომ „მონაცემები

[38] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].
[39] EDPB, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, 2020, §15, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf> [26.02.2024].
[40] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].
[41] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2013, 16, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> [26.02.2024].
[42] იქვე, 51.

დამუშავდება ბიზნესის მიზნებისთვის, როგორიცაა საგადასახადო, თაღლითობის პრევენცია და პროდუქტის გაუმჯობესება“. ამ პუნქტის თანახმად, პასუხისმგებელ პირს შეუძლია მონაცემები გამოიყენოს თითქმის ყველა მიზნით. შესაბამისად, მოცემული ფორმულირება ვერ აკმაყოფილებს კონკრეტულობის მოთხოვნას.[43]

## 2.2.„მკაფიოდ განსაზღვრული“

მიზნების მკაფიოდ განსაზღვრულობა ნიშნავს, რომ იგი უნდა იყოს ნათლად გამოვლენილი, ახსნილი ან გამოხატული რაიმე ფორმით, რათა ნებისმიერ პირს შეექმნას დამუშავების მიზნების არაორაზროვანი გაგება, კულტურული ან ენობრივი განსხვავებების მიუხედავად. შესაძლოა, არსებობდეს ისეთი მძიმე დარღვევების შემთხვევები, როდესაც პასუხისმგებელი პირი დამუშავების მიზნებს საკმარისად დეტალურად ან მკაფიო და ნათელი ენით ვერ აკონკრეტებს, ან მითითებული მიზნები შეცდომაში შემყვანია, ან არ შეესაბამება რეალობას. ნებისმიერ ასეთ სიტუაციაში, ნამდვილი მიზნების დასადგენად ყველა ფაქტი უნდა იყოს გათვალისწინებული, საქმის კონტექსტიდან გამომდინარე, მონაცემთა სუბიექტების საერთო გაგებასა და გონივრულ მოლოდინებთან ერთად. ამ მოთხოვნის საბოლოო ამოცანა ბუნდოვანებისა და გაურკვევლობის გარეშე მიზნების დაზუსტებაა.[44]

მიზნები იმგვარად უნდა იქნეს ფორმულირებული, რომ ერთგვარად იყოს აღქმადი არა მხოლოდ პასუხისმგებელი პირის და ნებისმიერი სხვა უფლებამოსილი პირის მიერ, არამედ მონაცემთა დაცვის ორგანოებისა და დაინტერესებული მონაცემთა სუბიექტების მიერ. განსაკუთრებული ყურადღება უნდა მიექცეს იმის უზრუნველყოფას, რომ მიზნის ნებისმიერი სპეციფიკაცია საკმარისად მკაფიო იყოს ყველა დაინტერესებული პირისთვის, განურჩევლად მათი განსხვავებული კულტურული თუ ენობრივი წარმოშობის, გაგების დონისა და სპეციალური საჭიროებებისა.[45]

[43] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].
[44] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2013, 17, 39 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> [26.02.2024].
[45] იქვე.

### მაგალითები

იმ სიტუაციებში, როდესაც დამუშავების მიზნები შეიძლება მკაფიოდ გამომდინარეობდეს კონტექსტიდან, ჩვეულებრივ, ნაკლები დეტალების მითითებაა აუცილებელი. თუმცა, ამ შემთხვევაშიც, გაურკვევლობის არსებობისას, უფრო ზუსტი და დეტალური ინფორმაციაა საჭირო:

- ადგილობრივ მცირე მეწარმეს ხელშეკრულების შესაბამისად ევალება, რომ მომხმარებელს მიაწოდოს და დაუმონტაჟოს გათბობის სისტემა, ასევე, უზრუნველყოს წლიური ტექნიკური მომსახურება. იგი აგროვებს ისეთ ინფორმაციას, როგორიცაა მომხმარებლის სახელი, მისამართი და ტელეფონის ნომერი, სისტემის მიწოდების/ინსტალაციისა და წლიური ტექნიკური მომსახურების დაგეგმვის მიზნით. აღნიშნულ პროცესში მონაცემთა შეგროვების საჭიროება გამომდინარეობს კონტექსტიდან, ჩვეულებიდან და ეკონომიკური ტრანზაქციის ბუნებიდან. თუმცა, რაიმე გაურკვევლობის შემთხვევაში, მაგალითად, თუ კომპანია აპირებს, რომ მომხმარებელს თავის სხვა სერვისებთან (ან სხვა კომპანიების მომსახურებებთან) დაკავშირებით გაუგზავნოს რეკლამები, აღნიშნულის შესახებ მონაცემთა სუბიექტს უნდა მიეწოდოს ინფორმაცია;
- პოტენციურმა დამსაქმებელმა, თანამშრომლის აყვანის პროცესში, კანდიდატის პროფესიული გამოცდილების შესაფასებლად მისი რეზიუმე უნდა დაამუშაოს, რაც თავისთავად გასაგებია. თუმცა, თუ რეზიუმე ასევე განკუთვნილია შიდა მობილობის სქემებსა და დაქირავების შემდგომ პროცედურებში გამოსაყენებლად, მონაცემთა შეგროვების მიზნებში აღნიშნულის შესახებ მითითება უნდა გაკეთდეს.[46]

## 2.3.„ლეგიტიმური“

პერსონალური მონაცემები ლეგიტიმური მიზნებით უნდა შეგროვდეს. იმისათვის, რომ მიზნები ლეგიტიმური იყოს, მათი დამუშავება ყველა ეტაპზე და ნებისმიერ დროს უნდა ეფუძნებოდეს მინიმუმ ერთ სამართლებრივ საფუძველს. ლეგიტიმურობა ფართო მოთხოვნაა და არ არის საკმარისი პერსონალურ მონაცემთა დაცვის კანონმდებლობის მხოლოდ რომელიმე მოთხოვნაზე მითითება. იგი მოიცავს წერილობითი და საერთო სამართლის ყველა ფორმას, პირველად და მეორად კანონმდებლობას, მუნიციპალურ დადგენილებებს, სასამართლო პრეცედენტებს,

[46] იქვე, 51-52.

კონსტიტუციურ პრინციპებს, ფუნდამენტურ უფლებებს, ზოგად სამართლებრივ პრინციპებს და სხვა. იგი ასევე ვრცელდება სამართლის სხვა სფეროებზე და უნდა განიმარტოს პერსონალურ მონაცემთა დამუშავების კონტექსტში.[47]

ის, თუ რა მიიჩნევა ლეგიტიმურ მიზნად, დამოკიდებულია კონკრეტულ გარემოებებზე, ვინაიდან მთავარი ამოცანაა, თითოეულ შემთხვევაში, ყველა შესაბამისი უფლების, თავისუფლებისა და ინტერესების დაბალანსება.[48] მიზნის ლეგიტიმურობის დადგენისას შესაძლებელია, გათვალისწინებულ იქნეს ჩვეულებითი წესები, ქცევის კოდექსები, ეთიკის კოდექსები, სახელშეკრულებო შეთანხმებები და საქმის ზოგადი კონტექსტი და ფაქტები; იგი მოიცავს პასუხისმგებელ პირსა და მონაცემთა სუბიექტებს შორის არსებული ურთიერთობის ბუნებას, იქნება ეს კომერციული თუ სხვა ხასიათის. მოცემული მიზნის ლეგიტიმურობა ასევე შეიძლება შეიცვალოს დროთა განმავლობაში, რაც დამოკიდებულია მეცნიერულ და ტექნოლოგიურ განვითარებაზე, საზოგადოებისა და კულტურული დამოკიდებულებების ცვლილებაზე.[49]

### მაგალითი

კომპანია თავის მომხმარებლებს ეთნიკური პროფილის მიხედვით ორ ჯგუფად ჰყოფს. კერძოდ, იგი უფრო მაღალ ფასებს აწესებს „თეთრი“ მომხმარებლებისთვის „აზიელებისაგან“ განსხვავებით. არაგამჭვირვალე გზით პრაქტიკის დამალვის მიზნით, აზიური გვარების მქონე მომხმარებლებისთვის გაგზავნილ კუპონებზე გამოიყენება სხვადასხვა პერსონალიზებული ფასდაკლებები. გარდა იმისა, რომ „ლოიალურობის ბარათის მონაცემები შეიძლება გამოყენებულ იქნეს მარკეტინგული მიზნებისთვის“, მომხმარებლებს სხვა სახის ინფორმაცია არ მიეწოდება.

მაგალითიდან ჩანს, რომ ლეგიტიმურობის მოთხოვნა ფართოა: მაგალითად, იგი ასევე კრძალავს მონაცემთა დამუშავებას იმ მიზნებისთვის, რამაც შეიძლება დანერგოს დისკრიმინაციული პრაქტიკა. შემთხვევა ასევე ხაზს უსვამს ლეგიტიმური დამუშავების კონტექსტში გამჭვირვალობის მნიშვნელობას: კომპანიას თვალსაჩინოდ

[47] იქვე, 19-20, 39.

[48] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10.X.2018, §48, <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> [26.02.2024].

[49] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2013, 20 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> [26.02.2024].

რომ გამოექვეყნებინა აზიური წარმოშობის პირებისთვის 10%-იანი ფასდაკლების შესახებ ბანერი, დისკრიმინაციული მოპყრობა ყველასათვის აშკარა იქნებოდა.[50]

## 2.4.მონაცემთა დამუშავება შეგროვების/მოპოვების მიზნისგან განსხვავებული მიზნით

მიზნის შეზღუდვის პრინციპმა[51] უნდა უზრუნველყოს, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა არ მოახდინონ პერსონალური მონაცემების „მეორადი გამოყენება“ („შემდგომი დამუშავება“), როდესაც ასეთი დამუშავება შეუთავსებელია თავდაპირველ მიზნებთან.[52] დამუშავების ნებისმიერ ახალ მიზანს, რომელიც თავდაპირველ მიზანს არ შეესაბამება, უნდა ჰქონდეს სამართლებრივი საფუძველი. კანონიერი დამუშავება შემოიფარგლება მხოლოდ საწყისი მიზნით და ნებისმიერი ახალი მიზანი საჭიროებს ცალკე სამართლებრივ საფუძველს.[53]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლით განსაზღვრულია გამონაკლისები, რა მიზნების არსებობის შემთხვევაშიც მონაცემთა შემდგომი დამუშავება მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებლად არ მიიჩნევა, თუ მონაცემთა დამუშავება გათვალისწინებულია კანონით ან კანონითა და მის საფუძველზე გამოცემული კანონქვემდებარე ნორმატიული აქტით. ასეთი მიზნები შეიძლება იყოს: დანაშაულის გამოძიება, სისხლისსამართლებრივი დევნა, მართლმსაჯულების განხორციელება და სხვა. ასევე, მონაცემები, რომლებიც სამართალდამცავმა ორგანომ შეაგროვა თავისი საქმიანობის ფარგლებში, შეიძლება დამუშავდეს დანაშაულებრივი საქმიანობის ზოგადი ანალიზისა და სხვადასხვა გამოვლენილ დანაშაულს შორის კავშირის დადგენის მიზნით. გარდა ამისა, მონაცემთა დამუშავების თავდაპირველ მიზანთან

---

[50] იქვე, 54-55.

[51] *“Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság”*-ის საქმეზე, მართლმსაჯულების ევროპულმა სასამართლომ “GDPR”-ის მე-5 მუხლის პირველი პუნქტის “ხ” ქვეპუნქტით გათვალისწინებული მიზნის შეზღუდვის პრინციპი განმარტა, რომლის თანახმად, აღნიშნული დებულება არ გამორიცხავს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ, ტესტირებისა და შეცდომების გასწორების მიზნებისთვის შექმნილ მონაცემთა ბაზაში იმ პერსონალურ მონაცემთა რეგისტრაციასა და შენახვას, რომლის შეგროვება და შენახვაც სხვა მონაცემთა ბაზაში მოხდა, თუკი ამგვარი დამუშავება თავსებადია თავდაპირველ მიზნებთან. გარემოებები უნდა განისაზღვროს “GDPR”-ის მე-6 მუხლის მე-4 პუნქტში მითითებული კრიტერიუმების შესაბამისად. იხ. CJEU, Case C-77/21, Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság [2022], §63.

[52] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].

[53] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 140, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf> [26.02.2024].

შეუთავსებლად არ მიიჩნევა მონაცემთა შემდგომი დამუშავება საჯარო ინტერესების შესაბამისად არქივირების, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის. თუმცა, თუ მონაცემთა მეორადი ან შემდგომი დამუშავება არ უკავშირდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრულ მიზნებს, პასუხისმგებელმა პირებმა უნდა შეაფასონ, მონაცემთა შემდგომი დამუშავების საკითხი.[54] კერძოდ, თუ მონაცემები უნდა დამუშავდეს მათი შეგროვების/მოპოვების მიზნისგან განსხვავებული მიზნით და დამუშავება მონაცემთა სუბიექტის თანხმობით ან კანონის საფუძველზე არ ხორციელდება, მონაცემთა შეგროვების/მოპოვების მიზნისგან განსხვავებული მიზნით მონაცემთა დამუშავების საკითხის გადაწყვეტისას პასუხისმგებელმა პირმა უნდა გაითვალისწინოს:

- ☑ არსებობს თუ არა მონაცემთა შეგროვების/მოპოვების თავდაპირველ მიზანსა და შემდგომ მიზანს შორის კავშირი;
- ☑ მონაცემთა შეგროვებისას/მოპოვებისას პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის არსებული ურთიერთობის ხასიათი;
- ☑ აქვს თუ არა მონაცემთა სუბიექტს მის შესახებ მონაცემთა შემდგომი დამუშავების გონივრული მოლოდინი;
- ☑ ხორციელდება თუ არა განსაკუთრებული კატეგორიის მონაცემთა დამუშავება;
- ☑ მონაცემთა სუბიექტისთვის შესაძლო შედეგები, რომლებიც შეიძლება თან ახლდეს მონაცემთა შემდგომ დამუშავებას;
- ☑ მონაცემთა ტექნიკური და ორგანიზაციული უსაფრთხოების ზომების არსებობა.

თუკი დამუშავება თავდაპირველ მიზანთან თავსებადად მიიჩნევა, ზემოაღნიშნული პირობების არსებობის შემთხვევაში, აღარ არის საჭირო სხვა სამართლებრივი საფუძვლის არსებობა, თუმცა, როდესაც დამუშავება არ არის თავსებადი თავდაპირველ მიზანთან, ცალკე სამართლებრივი საფუძვლის არსებობა აუცილებელი იქნება.[55]

### მაგალითი

დაუშვებელია, რომ ექიმმა თავისი პაციენტის შესახებ მონაცემები მოულოდნელად მარკეტინგული მიზნებისთვის დაამუშაოს, რადგან ეს იქნება „მეორადი გამოყენება“, რომელიც სცილდება თავდაპირველ მიზანს. თუმცა, ექიმმა შესაძლებელია თავისი

[54] Eduardo Ustaran, CIPP/E, Partner, Hogan Lovells, European Data Protection Law and Practice, Second Edition, 2019, 131.
[55] იქვე, 132.

ჩანაწერები სამართალწარმოების დროს გამოიყენოს, რათა დაამტკიცოს, რომ პაციენტს არ გადაუხდია სამედიცინო გადასახადები.[56]

## 2.5.რეკომენდაციები

- ☑ წინასწარ უნდა განისაზღვროს პერსონალურ მონაცემთა დამუშავების მიზანი/მიზნები.
- ☑ სასურველია, განხორციელდეს, მონაცემთა დამუშავების მიზნების/მიზნის დოკუმენტირება.
- ☑ დამუშავების მიზნების შესახებ ინფორმაციას უნდა შეიცავდეს მონაცემთა დამუშავების პოლიტიკა.
- ☑ რეგულარულად უნდა გადაიხედოს დამუშავების ოპერაციები და, საჭიროების შემთხვევაში, განახლდეს შესაბამისი დოკუმენტაცია, ასევე, ფიზიკური პირებისთვის განკუთვნილი კონფიდენციალობის შესახებ ინფორმაცია.
- ☑ თუ პასუხისმგებელი პირის მიერ მონაცემთა დამუშავება ხორციელდება შეგროვების/მოპოვების მიზნისგან განსხვავებული მიზნით, რაზეც არ ვრცელდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლით განსაზღვრული გამონაკლისები, უნდა შეფასდეს, აღნიშნული მიზნის თავდაპირველ მიზანთან შესაბამისობა.[57]

# 3. მონაცემთა მინიმიზაცია

[56] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].
[57] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/ Principle (b): Purpose limitation, < https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/purpose-limitation/> [26.02.2024].

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „გ“ ქვეპუნქტის მიხედვით, *„მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად. მონაცემები იმ მიზნის თანაზომიერი უნდა იყოს, რომლის მისაღწევადაც ისინი მუშავდება.“*

## 3.1.პრინციპის არსი

მონაცემთა მინიმიზაციის პრინციპის დაცვისათვის საჭიროა, რომ დამუშავებული მონაცემების მოცულობა იყოს:

- ☑ *ადეკვატური:* საკმარისი დასახელებული მიზნის სათანადოდ მიღწევისთვის. პერსონალური მონაცემები „ადეკვატურია“, თუ ასეთი მონაცემების კონკრეტული მიზნისთვის გამოყენება მიზანშეწონილია (მაგალითად, პირის საცხოვრებელი მისამართი არ არის მისი საკრედიტო შეფასებისთვის საჭირო ინფორმაცია);
- ☑ *შესაბამისი:* აქვს გონივრული კავშირი დასახულ მიზანთან. პერსონალური მონაცემები „შესაბამისია“, თუ ის იწვევს განსხვავებულ შედეგს მიზანთან დაკავშირებით (მაგალითად, მომხმარებლის მისამართი პროდუქტის მიწოდებისთვის შესაბამის ინფორმაციას წარმოადგენს);
- ☑ *შემოფარგლული მხოლოდ იმით, რაც აუცილებელია:* არ უნდა დამუშავდეს უფრო მეტი მონაცემი, ვიდრე მიზნის მიღწევისთვის არის საჭირო.[58] ეს კომპონენტი გულისხმობს, რომ მიზნის მიღწევა გონივრულად შეუძლებელია კონკრეტული პერსონალური მონაცემების დამუშავების გარეშე.[59] აუცილებლობის კრიტერიუმი ასევე მოითხოვს, რომ პერსონალურ მონაცემთა შენახვის ვადა შეიზღუდოს მკაცრი მინიმუმით.[60]

პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, როდესაც დამუშავების მიზნის მიღწევა, გონივრულობის ფარგლებში, შეუძლებელია სხვა საშუალებებით.[61] ამასთანავე, მონაცემთა მინიმიზაციის პრინციპი მჭიდრო კავშირშია

[58] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/ Principle (c): Data minimisation, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> [26.02.2024].
[59] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].
[60] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 313.
[61] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 143, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf> [26.02.2024].

მიზნის შეზღუდვის პრინციპთან და მისი დაცვა შესაძლებელია მხოლოდ იმ შემთხვევაში, როდესაც პასუხისმგებელი პირის მიერ კონკრეტული მიზნები მკაფიოდაა განსაზღვრული. პასუხისმგებელმა პირმა, მიზნის მიღწევის აუცილებლობის დასადგენად, უნდა გადახედოს დამუშავების ოპერაციის თითოეულ საფეხურს და მონაცემთა თითოეულ ელემენტს.[62]

პასუხისმგებელმა პირებმა უნდა განსაზღვრონ, სჭირდებათ თუ არა მათ პერსონალური მონაცემების დამუშავება შესაბამისი მიზნების მიღწევისთვის, უნდა გადაამოწმონ, შესაძლებელია თუ არა ნაკლები მოცულობის პერსონალური მონაცემების დამუშავებით, ნაკლებად დეტალური ან გაერთიანებული პერსონალური მონაცემებით ან საერთოდ პერსონალური მონაცემების დამუშავების გარეშე შესაბამისი მიზნების მიღწევა. ამგვარი შემოწმება უნდა განხორციელდეს ნებისმიერი დამუშავების დაწყებამდე, თუმცა მისი ჩატარება ასევე შესაძლებელია დამუშავების ციკლის ნებისმიერ მომენტში.[63]

მინიმიზაცია ასევე დაკავშირებულია იდენტიფიკაციის ხარისხთან. თუ დამუშავების მიზანი არ მოითხოვს, რომ მონაცემთა საბოლოო ნაკრები მითითებას იდენტიფიცირებულ ან იდენტიფიცირებად ინდივიდზე (მაგალითად, სტატისტიკის შემთხვევაში) აკეთებდეს, თუმცა პირველადი დამუშავებისას ამის საჭიროება არსებობს (მაგალითად, მონაცემთა გაერთიანებამდე), მაშინ პასუხისმგებელმა პირმა პერსონალური მონაცემები უნდა წაშალოს ან მისი ანონიმიზაცია მოახდინოს, მას შემდეგ რაც იდენტიფიკაციის საჭიროება აღარ იარსებებს. ხოლო, თუ სხვა დამუშავების აქტივობებისთვის მუდმივი იდენტიფიკაციაა საჭირო, მონაცემთა სუბიექტების უფლებების რისკის შესამცირებლად პერსონალური მონაცემების ფსევდონიმიზაცია უნდა განხორციელდეს.[64]

### მაგალითები

[62] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].
[63] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §74, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> [26.02.2024].
[64] იქვე, §75.

- ☐ დასაქმების სააგენტო კანდიდატებს უგზავნის ზოგად კითხვარს, რომელიც მოიცავს კონკრეტულ კითხვებს ჯანმრთელობის მდგომარეობის შესახებ. აღნიშნულ მონაცემთა შეგროვება აუცილებელია მხოლოდ კონკრეტული პროფესიებისთვის. შესაბამისად, იმ კანდიდატთა ჯანმრთელობის შესახებ მონაცემთა შეგროვებით, რომელთა საქმიანობისათვის არარელევანტურია ზემოაღნიშნული განსაკუთრებული კატეგორიის მონაცემები, დაირღვევა მონაცემთა მინიმიზაციის პრინციპი.[65]
- ☐ ონლაინ მაღაზია მოითხოვს, რომ ყველა მომხმარებელმა შეავსოს დაბადების ზუსტი თარიღი, იმის დასადასტურებლად, რომ მომხმარებლები სრულწლოვნები არიან. იმის გათვალისწინებით, რომ ონლაინ მაღაზიას არ შეუძლია დაბადების თარიღების გადამოწმება, მარტივი კითხვა „დიახ/არა“ შეასრულებს იმავე მიზანს, დაბადების ზუსტი თარიღების შეგროვების გარეშე.[66]

### 3.2.რეკომენდაციები

- ☑ უნდა შეგროვდეს მხოლოდ იმ რაოდენობის პერსონალური მონაცემები, რაც საჭიროა კონკრეტული მიზნის/მიზნების მისაღწევად.
- ☑ პერსონალურ მონაცემები არ უნდა შეგროვდეს იმ განზრახვით, რომ ისინი მომავალში ჰიპოთეტურად სასარგებლო აღმოჩნდება.
- ☑ შეგროვებული მონაცემები მიზნის/მიზნების მიღწევისთვის საკმარისი რაოდენობის (და არა უფრო ნაკლები) უნდა იყოს.
- ☑ პერიოდულად უნდა გადაიხედოს, რა მონაცემებს ფლობს პასუხისმგებელი პირი და თუ მონაცემთა შენახვის საჭიროება აღარ არსებობს, იგი უნდა წაიშალოს.[67]

## 4. მონაცემთა ნამდვილობა და სიზუსტე

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „დ“ ქვეპუნქტის მიხედვით, *„მონაცემები უნდა იყოს ნამდვილი,*

[65] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/ Principle (c): Data minimisation, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> [26.02.2024].
[66] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].
[67] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/ Principle (c): Data minimisation, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> [26.02.2024].

*ზუსტი და, საჭიროების შემთხვევაში, განახლებული. მონაცემთა დამუშავების მიზნების გათვალისწინებით, არაზუსტი მონაცემები უნდა გასწორდეს, წაიშალოს ან განადგურდეს გაუმართლებელი დაყოვნების გარეშე.“*

## 4.1.პრინციპის არსი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, ისევე როგორც ევროკავშირის მონაცემთა დაცვის კანონმდებლობა არ იძლევა „სიზუსტის“ დეფინიციას, თუმცა, პრაქტიკაში „არაზუსტი“ მონაცემი განიმარტება, როგორც არასწორი ან შეცდომაში შემყვანი ნებისმიერი სახის ფაქტი. არსებობს სხვადასხვა კატეგორიის ინფორმაცია, რისი განხილვაც მიზანშეწონილია ნამდვილობისა და სიზუსტის პრინციპის კონტექსტში:

☑ *პიროვნების შესახებ ობიექტური ფაქტები*

ინფორმაცია, როგორიცაა სახელი, დაბადების თარიღი ან საცხოვრებელი მისამართი შეიძლება იყოს „არაზუსტი“ და შესაბამისად, ექცევა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „დ“ ქვეპუნქტის ფარგლებში.

☑ *პროგნოზები და ვარაუდები*

სიზუსტის პრინციპი ვრცელდება პროგნოზებსა და ვარაუდებზეც, რაც განსაკუთრებით აქტუალურია ავტომატური პროფილირების თანამედროვე ფორმების, ხელოვნური ინტელექტის მეშვეობით მონაცემთა დამუშავებისა თუ სხვა თანამედროვე სისტემებისთვის. პროგნოზები შესაძლებელია ობიექტურად არაზუსტი იყოს, თუ ისინი ეფუძნება მცდარ ფაქტებს, არასწორ დასკვნებს ან მეთოდოლოგიებს. ამ შემთხვევაში, პასუხისმგებელი და უფლებამოსილი პირები სიზუსტის პრინციპს გვერდს ვერ აუვლიან.

☑ *შეფასებები*

მტკიცებულებებზე დაფუძნებული პროგნოზებისა და ვარაუდებისგან განსხვავებით, ღირებულებითი შეფასებები „არაზუსტი“ არ შეიძლება იყოს, რადგან ისინი თავისი ბუნებით არ არის ობიექტურად სწორი.[68] გასათვალისწინებელია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის მე-4 პუნქტის მიხედვით, ნამდვილობისა და სიზუსტის პრინციპის დაცვის მიზნისთვის პასუხისმგებელმა პირმა, კონტექსტიდან გამომდინარე, ფაქტებზე დაფუძნებული მონაცემები უნდა განასხვაოს იმ მონაცემებისგან, რომლებიც პირად შეფასებას

[68] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].

ეფუძნება. პირად შეფასებაზე დაფუძნებულ მონაცემებთან მიმართებით ამ პრინციპის ზედმიწევნით დაცვა სავალდებულო არ არის.

ასევე, გასათვალისწინებელია, რომ მოძველებული პერსონალური მონაცემები შესაძლებელია დროთა განმავლობაში გახდეს არაზუსტი.[69] სწორედ ამიტომ, პასუხისმგებელმა პირებმა პერიოდულად უნდა განაახლონ მათ ხელთ არსებული ინფორმაცია, მაგალითად, ელექტრონული ფოსტის მისამართები, ტელეფონის ნომრები, საცხოვრებელი მისამართები და სხვა.

მონაცემთა სიზუსტის მოთხოვნების შეფასება მონაცემთა კონკრეტული დამუშავების რისკებთან და შედეგებთან მიმართებით უნდა განხორციელდეს. არაზუსტმა პერსონალურმა მონაცემებმა შეიძლება საფრთხე შეუქმნას მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებს, მაგალითად, პიროვნების არასწორმა სურათმა შეიძლება გამოიწვიოს გადაწყვეტილებების შეუსაბამო საფუძველზე მიღება არაავტომატურად, ავტომატურად თუ ხელოვნური ინტელექტის მეშვეობით.[70] ამიტომ, პასუხისმგებელი პირი ვალდებულია, მონაცემთა სიზუსტის პრინციპი დანერგოს დამუშავების ყველა ოპერაციაში.[71]

ამასთანავე, მნიშვნელოვანია, რომ მონაცემთა დამუშავების მიზნების გათვალისწინებით, არაზუსტი მონაცემები უნდა გასწორდეს, წაიშალოს[72] ან განადგურდეს გაუმართლებელი დაყოვნების გარეშე. მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლება, თავის მხრივ, უზრუნველყოფილია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-16 მუხლით.

### მაგალითები

---

[69] იქვე.

[70] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §78, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> [26.02.2024].

[71] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 145, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf> [26.02.2024].

[72] გერმანიის ფედერალურმა ადმინისტრაციულმა სასამართლომ მონაცემთა სუბიექტის მიერ მონაცემთა გასწორების უფლების მოთხოვნასთან დაკავშირებულ საქმეზე დაადგინა, რომ პასუხისმგებელ პირს არ შეიძლება მოეთხოვოს ისეთი მონაცემების შეყვანა და შემდგომი დამუშავება, რომელთა სიზუსტის საკმარისი სარწმუნოობით დადგენა შეუძლებელია. შესაბამისად, გასაახლებელი მონაცემების სიზუსტესთან დაკავშირებით მტკიცების ტვირთი მონაცემთა სუბიექტს ეკისრება. ვინაიდან, მოცემული საქმის მიხედვით, მონაცემთა სუბიექტმა ვერ შეძლო მისი დაბადების თარიღის დადასტურება, სასამართლომ საკითხი პასუხისმგებელი პირის სასარგებლოდ გადაწყვიტა. იხ. BVerwG (Germany), 6 C 7.20, [2022], <https://gdprhub.eu/index.php?title=BVerwG_-_6_C_7.20> [26.02.2024].

- ☐ სამედიცინო მდგომარეობის არასწორი დიაგნოსტიკა კვლავ რჩება პაციენტის სამედიცინო ჩანაწერებში, დიაგნოზის გამოსწორების შემდეგაც კი, რადგან ის რელევანტურია პაციენტისთვის დანიშნული მკურნალობის დასაბუთებისთვის ან ჯანმრთელობის სხვა პრობლემებისთვის.[73]
- ☐ ერთ-ერთი საავადმყოფო ინახავს პაციენტების სამედიცინო ჩანაწერებსა და საკონტაქტო დეტალებს სპეციალურ მონაცემთა ბაზაში. ფიზიკური პირი 2016 წელს საავადმყოფოში ყოფნისას 135 კგ-ს იწონიდა, მაგრამ ახლა მისი წონა 85 კგ-მდე შემცირდა. ამ შემთხვევაში, ძველი ჩანაწერების განახლება არ არის „აუცილებელი“ და „ზუსტი“, იმის გათვალისწინებით, რომ ჩანაწერები მიზნად ისახავს ფიზიკური პირის მდგომარეობის ჩვენებას 2016 წელს, როდესაც ის საავადმყოფოში იმყოფებოდა. ამავე დროს, ფიზიკურმა პირმა შეიცვალა მისამართი. მას შეიძლება სურდეს მისი საკონტაქტო მონაცემების განახლება, როდესაც საავადმყოფოში ყოველწლიური შემოწმებისთვის დაბრუნდება.[74]

### 4.2.რეკომენდაციები

- ☑ სასურველია, დაინერგოს შესაბამისი მონაცემების სიზუსტის შემოწმების პროცედურა, ასევე, აღირიცხოს ინფორმაცია მონაცემთა მოპოვების წყაროს შესახებ.
- ☑ უნდა დაინერგოს პერსონალურ მონაცემთა განახლების პროცედურა და საჭიროების შემთხვევაში, განახლდეს არაზუსტი მონაცემები.
- ☑ მცდარი ჩანაწერების დამუშავების საჭიროების შემთხვევაში, ჩანაწერებში ნათლად უნდა იყოს მითითებული, რომ იგი წარმოადგენს შეცდომას.
- ☑ პასუხისმგებელმა პირმა პატივი უნდა სცეს მონაცემთა სუბიექტის უფლებას, მოითხოვოს მის შესახებ მონაცემთა გასწორება და ყურადღებით განიხილოს მონაცემთა სიზუსტესთან დაკავშირებული ნებისმიერი გამოწვევა.[75]

## 5. მონაცემთა შენახვის ვადის შეზღუდვა

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტის მიხედვით, „*მონაცემები შეიძლება შენახულ იქნეს*

[73] ICO, Guide to the General Data Protection Regulation (GDPR), Principles, Accuracy, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/> [26.02.2024].
[74] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].
[75] ICO, Guide to the General Data Protection Regulation (GDPR), Principles, Accuracy, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/> [26.02.2024].

*მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა წაიშალოს, განადგურდეს ან შენახული უნდა იქნეს დეპერსონალიზებული ფორმით, გარდა იმ შემთხვევისა, თუ მონაცემთა დამუშავება განსაზღვრულია კანონით ან/და კანონის შესაბამისად გამოცემული კანონქვემდებარე ნორმატიული აქტით და მონაცემთა შენახვა აუცილებელი და პროპორციული ზომაა დემოკრატიულ საზოგადოებაში აღმატებული ინტერესების დასაცავად.“*

## 5.1.პრინციპის არსი

შენახვის ვადის შეზღუდვის პრინციპი გულისხმობს, რომ პასუხისმგებელმა პირმა წინასწარ უნდა აცნობოს მონაცემთა სუბიექტს შენახვის პერიოდის შესახებ, ასევე, უნდა უზრუნველყოს პრინციპთან შესაბამისობის დემონსტრირება. შესაბამისად, შენახვის ვადები უნდა განისაზღვროს ორგანიზაციის შიგნით, მონაცემთა დამუშავების დაწყებამდე.[76]

პერსონალურ მონაცემთა დამუშავების პროცესში შენახვის ვადის შეზღუდვა მნიშვნელოვანია, ვინაიდან, როდესაც მონაცემები ინახება გადაჭარბებული ვადებით, იგი ხდება არასაჭირო, შესაბამისად, აღარ არსებობს მონაცემთა დამუშავების კანონიერი საფუძველი. უფრო პრაქტიკული თვალსაზრისით კი, პერსონალურ მონაცემთა შენახვა იმაზე მეტი ვადით, ვიდრე აუცილებელია, საჭიროებს შენახვასთან და უსაფრთხოებასთან დაკავშირებულ ზედმეტ ხარჯებს. ამასთანავე, რაც უფრო დიდი ვადით ინახება მონაცემები, მით უფრო მეტი შეიძლება იყოს მათზე მონაცემთა სუბიექტის მიერ მონაცემთა მოთხოვნისა და აღნიშნული ინფორმაციის წაშლის მოთხოვნის განცხადებები.[77]

პერსონალურ მონაცემთა შენახვის ვადების სწორად დადგენა შესაძლებელია შემდეგი ფაქტორების დახმარებით:

- ☑ პასუხისმგებელმა პირმა უნდა გაითვალისწინოს გაცხადებული მიზან(ებ)ი. მონაცემთა შენახვა შესაძლებელია მანამ, სანამ ერთ-ერთი მიზნის მისაღწევად მაინც არის იგი საჭირო, თუმცა მონაცემთა შენახვა არ იქნება გამართლებული

[76] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful> [26.02.2024].
[77] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/The principles/Storage limitation, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/#why_storage_limitation> [26.02.2024].

„ყოველი შემთხვევისთვის“ ან თუ ძალიან მცირე შესაძლებლობა არსებობს, რომ ისინი გამოდგება;

- ☑ პასუხისმგებელმა პირმა უნდა განსაზღვროს სჭირდება თუ არა სამართლებრივი ურთიერთობის შესახებ (მაგალითად, მონაცემთა სუბიექტისთვის მომსახურების მიწოდება) ჩანაწერების შენახვა მას შემდეგ, რაც სამართლებრივი ურთიერთობა დასრულდება. შესაძლებელია, ყველა მონაცემის წაშლა არ იყოს გამართლებული სამართლებრივი ურთიერთობის დასრულების შემდეგ და ინფორმაცია ან მის შესახებ მცირე დეტალები ინახებოდეს სამართლებრივი ურთიერთობის არსებობის/დასრულების დასადგენად;
- ☑ პასუხისმგებელმა პირმა უნდა გაითვალისწინოს სჭირდება თუ არა ინფორმაციის შენახვა შესაძლო სამართლებრივი ინტერესების დასაცავად. მას შეუძლია წაშალოს ინფორმაცია, რომელიც არ არის რელევანტური შესაბამისი სამართლებრივი ინტერესების დასაცავად. თუ მონაცემთა შენახვის სხვა რაიმე მიზეზი არ არსებობს, პერსონალური მონაცემები უნდა წაიშალოს, როდესაც ასეთი სამართლებრივი დაცვის საჭიროება აღარ შეიძლება გაჩნდება;
- ☑ პასუხისმგებელმა პირმა უნდა გაითვალისწინოს მის მიმართ მონაცემთა შენახვასთან დაკავშირებული სამართლებრივი მოთხოვნები. არსებობს რეგულაციები და სახელმძღვანელო მითითებები ზოგიერთი კატეგორიის მონაცემთა შენახვის შესახებ, როგორიცაა ინფორმაცია საგანმანათლებლო, საგადასახადო და აუდიტის მიზნებისთვის, ჯანმრთელობისა და უსაფრთხოების შესახებ. თუ ინფორმაციას პასუხისმგებელი პირი ამგვარი მოთხოვნებიდან გამომდინარე ინახავს, ნაკლებად არის შესაძლებელი, რომ მონაცემები ინახება გადაჭარბებული ვადით;
- ☑ პასუხისმგებელმა პირმა უნდა გაითვალისწინოს მისი საქმიანობის სფეროს შესაბამისი სტანდარტები და ინსტრუქციები. თუმცა, ასეთი სტანდარტების არსებობა თავისთავად არ ადასტურებს, რომ დაცულია შენახვის ვადის შეზღუდვის პრინციპი და პასუხისმგებელ პირს მოუწევს მათი მიზანშეწონილობის დასაბუთება;
- ☑ პასუხისმგებელმა პირმა ვადების განსაზღვრისას, უნდა იხელმძღვანელოს პროპორციული მიდგომით, რათა დაბალანსდეს მისი საჭიროებები და შენახვის ვადების გავლენა მონაცემთა სუბიექტის პირად ცხოვრებასა და მის საუკეთესო ინტერესზე. ასევე, გასათვალისწინებელია, რომ შენახვის ვადები ყოველთვის უნდა იყოს სამართლიანი და კანონიერი.[78]

[78] იქვე.

### მაგალითი

ბანკი ფლობს თავისი კლიენტების შესახებ პერსონალურ მონაცემებს, კერძოდ, თითოეული მომხმარებლის მისამართის, დაბადების თარიღისა და დედის გვარის შესახებ. ბანკი ამ ინფორმაციას უსაფრთხოების პროცედურების ფარგლებში იყენებს. ბანკისთვის მიზანშეწონილია, რომ ეს მონაცემები შეინარჩუნოს მანამ, სანამ ბანკში მომხმარებელს აქვს ანგარიში. ანგარიშის დახურვის შემდეგაც კი, ბანკს შეიძლება დასჭირდეს ამ ინფორმაციის გარკვეული ნაწილის შენახვა სამართლებრივი ან ოპერაციული მიზეზების გამო, განსაზღვრული დროის განმავლობაში.[79]

## 5.2.რეკომენდაციები

- ☑ პასუხისმგებელმა პირმა უნდა იცოდეს რა პერსონალურ მონაცემს ფლობს და რატომ სჭირდება ეს ინფორმაცია.
- ☑ პასუხისმგებელ პირს უნდა შეეძლოს დაასაბუთოს, რატომ ინახავს პერსონალურ მონაცემებს კონკრეტული ვადებით.
- ☑ სასურველია, ორგანიზაციას გააჩნდეს სტანდარტული შენახვის ვადების თაობაზე პოლიტიკის დოკუმენტი.
- ☑ პერიოდულად უნდა გადახედოს ორგანიზაციის მფლობელობაში არსებული მონაცემები და წაიშალოს/განადგურდეს ან მოხდეს ისეთი მონაცემების დეპერსონალიზაცია, რომლებიც აღარ არის საჭირო, თუ კანონით სხვა რამ არ არის განსაზღვრული.
- ☑ უნდა დაინერგოს შესაბამისი პროცედურები, რათა შესრულდეს მონაცემთა სუბიექტის მოთხოვნები მონაცემთა წაშლის/განადგურების შესახებ.[80]

# 6. მონაცემთა უსაფრთხოება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის „ვ“ ქვეპუნქტის მიხედვით, *„მონაცემების უსაფრთხოების დაცვის*

[79] იქვე.
[80] იქვე.

*მიზნით მონაცემთა დამუშავებისას მიღებული უნდა იქნეს ისეთი ტექნიკური და ორგანიზაციული ზომები, რომლებიც სათანადოდ უზრუნველყოფს მონაცემთა დაცვას, მათ შორის, უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვისგან, განადგურებისგან ან/და დაზიანებისგან.“*

## 6.1.პრინციპის არსი

პერსონალური მონაცემების უსაფრთხოების დაცვა მოითხოვს შესაბამის ზომებს, რომელთა მიზანია: მონაცემთა უსაფრთხოების დარღვევის — ინციდენტის თავიდან აცილება და მართვა; მონაცემთა დამუშავების ამოცანების სწორად შესრულება და სხვა პრინციპებთან შესაბამისობის უზრუნველყოფა; და პირთა უფლებების ეფექტიანად განხორციელების ხელშეწყობა.[81] უსაფრთხოების ზომები უნდა მოიცავდეს არა მხოლოდ კიბერუსაფრთხოებას, არამედ ფიზიკურ და ორგანიზაციულ უსაფრთხოებასაც.[82] ორგანიზაციებმა რეგულარულად უნდა შეამოწმონ, არის თუ არა მათი უსაფრთხოების ზომები განახლებული და ეფექტიანი.[83] შესაბამისად, მონაცემთა უსაფრთხოების სათანადო ზომების მიღებისას, გათვალისწინებულ უნდა იქნეს მონაცემთა უსაფრთხოების თანამედროვე მეთოდები და ტექნოლოგიები,[84] უახლესი მიღწევები, განხორციელების ხარჯები, ასევე, დამუშავების ხასიათი, ფარგლები, კონტექსტი და მიზნები. ასევე, გასათვალისწინებელია, ფიზიკური პირების უფლებებსა და თავისუფლებებზე დამუშავების ოპერაციის გავლენა.[85]

---

[81] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §83, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> [26.02.2024].

[82] *“Z v Finland”*-ის საქმეზე ( [1997], ECHR, App. No. 22009/93) ევროპულმა სასამართლომ დაადგინა, რომ შიდა კანონმდებლობამ უნდა უზრუნველყოს შესაბამისი უსაფრთხოების ზომები, რათა თავიდან იქნეს აცილებული „ადამიანის უფლებათა ევროპული კონვენციის“ მე-8 მუხლის გარანტიებთან შეუსაბამო ნებისმიერი კომუნიკაცია ან ჯანმრთელობის შესახებ მონაცემების გამჟღავნება. კერძოდ, ფინეთმა ვერ უზრუნველყო საჯარო საავადმყოფოში პაციენტის სამედიცინო მონაცემების არასანქცირებული წვდომისგან დაცვის მიზნით ადეკვატური ტექნიკური და ორგანიზაციული ზომების მიღება. იხ. Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 634.

[83] Irish DPA, Quick Guide to the Principles of Data Protection, 2019, <https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf > [26.02.2024].

[84] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10.X.2018, §63, <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> [26.02.2024].

[85] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_32_GDPR#cite_note-1> [26.02.2024].

პერსონალურ მონაცემთა უსაფრთხოების დაცვის კონტექსტში ასევე მნიშვნელოვანია შემდეგი ფაქტორები:

☑ *ორგანიზაციული ზომები*

მონაცემთა უსაფრთხოების დაცვისათვის, ორგანიზაციული ზომების ნაწილში, შესაძლებელია შემდეგი ღონისძიებების გატარება:

- ინფორმაციული უსაფრთხოების რისკების შეფასება;
- უსაფრთხოების პოლიტიკის დოკუმენტის მიღება;
- უსაფრთხოების საკითხებზე თანამშრომელთა ცნობიერების ამაღლება;
- თანამშრომლების მხრიდან კონფიდენციალობის გარანტიების მიღება;
- დაწესებულებაში კონკრეტული პირის/დანაყოფის განსაზღვრა, რომელიც პასუხისმგებელი იქნება მონაცემთა უსაფრთხოებაზე და ექნება ამისათვის საჭირო რესურსები და უფლებამოსილება და სხვ.[86]

☑ *ტექნიკური ზომები*

ტექნიკურ ზომებად ძირითადად მიიჩნევა პერსონალურ მონაცემთა დაცვა კომპიუტერებსა და ქსელებში. ტექნიკური ზომები მოიცავს ფიზიკურ და ინფორმაციულ უსაფრთხოებას (IT უსაფრთხოება).[87]

☑ *ფიზიკური უსაფრთხოება*

ფიზიკური უსაფრთხოებისთვის გასათვალისწინებელია შემდეგი ფაქტორები:

- კარების და საკეტების ხარისხი, შენობების დაცვა ისეთი საშუალებებით, როგორიცაა სიგნალიზაცია, ვიდეომეთვალყურეობა;
- როგორ ხდება შენობაში შესვლა და როგორ კონტროლდებიან ვიზიტორები;
- როგორ ნადგურდება ფურცლები და ელექტრონული ნარჩენები;
- როგორ ინახება ელექტრონული მოწყობილობა, მაგალითად, სერვერები, მობილური ტელეფონები და სხვ.[88]

☑ *ინფორმაციული უსაფრთხოება*

რაც შეეხება ინფორმაციულ უსაფრთხოებას (მას ასევე მოიხსენიებენ ტერმინით - „კიბერუსაფრთხოება“), ეს არის კომპლექსური ტექნიკური სფერო, რომელიც

[86] ICO, For organisations/UK GDPR guidance and resources/Security/A guide to data security, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/> [26.02.2024].
[87] იქვე.
[88] იქვე.

მუდმივად ვითარდება და ჩნდება ახალი საფრთხეები. ინფორმაციული უსაფრთხოების კონტექსტში, გასათვალისწინებელია შემდეგი საკითხები:

- ქსელებისა და ინფორმაციული სისტემების უსაფრთხოება;
- სისტემაში შენახული მონაცემების უსაფრთხოება, მაგალითად, წვდომის კონტროლით;
- ონლაინ უსაფრთხოება, რაც გულისხმობს გამოყენებული ვებგვერდებისა და სხვა ონლაინ სერვისების/აპლიკაციების უსაფრთხოებას;
- მოწყობილობის უსაფრთხოება და სხვ.[89]

### მაგალითი

მიკროსაფინანსო ორგანიზაცია უნდა დარწმუნდეს, რომ ფინანსური ინფორმაცია არ გავრცელდეს მისივე თანამშრომლების მიერ. ამასთანავე, მან უნდა უზრუნველყოს, რომ მონაცემები არ შეიცვალოს ან წაიშალოს. ზოგიერთ შემთხვევაში, დაწესებულებას აღნიშნულის მიღწევა ტექნიკური ზომების საშუალებით (მაგ., უსაფრთხოების სისტემები, გარკვეული პირებისთვის წვდომის შეზღუდვა) შეუძლია. თუმცა, ტექნიკური გადაწყვეტილებებით არ შეიძლება ყველა რისკის თავიდან აცილება (მაგ., ზოგიერთ პირს უნდა ჰქონდეს სრული წვდომა ინფორმაციაზე, აპარატურასა და პროგრამულ უზრუნველყოფაზე, რათა უზრუნველყოს სისტემის მუშაობა). ამ შემთხვევებში, ორგანიზაციული ღონისძიებები (მაგ., ხელშეკრულებები კონფიდენციალობის დაცვის შესახებ, სერვერის ოთახებში წვდომის შეზღუდვები) შეიძლება უფრო მიზანშეწონილი აღმოჩნდეს.[90]

## 6.2.რეკომენდაციები

☑ უნდა გაანალიზდეს, რა რისკები შეიძლება ახლდეს მონაცემთა სუბიექტის მონაცემების დამუშავებას და აღნიშნული გათვალისწინებულ იქნეს უსაფრთხოების ღონისძიებების დანერგვის პროცესში.

[89] იქვე.
[90] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_32_GDPR#cite_note-1> [26.02.2024].

- ☑ სასურველია, შემუშავებულ იქნეს კონფიდენციალობის პოლიტიკა, რომელიც პერიოდულად უნდა განახლდეს/გაუმჯობესდეს;
- ☑ შესაძლებლობის შემთხვევაში, უსაფრთხოების ზომებად გამოყენებულ უნდა იქნეს დეპერსონალიზაცია და ფსევდონიმიზაცია.
- ☑ უზრუნველყოფილ უნდა იქნეს, რომ პასუხისმგებელი და უფლებამოსილი პირების ნებისმიერმა თანამშრომელმა, რომელიც მონაწილეობს მონაცემთა დამუშავებაში, დაიცვას კონფიდენციალობის ვალდებულება.
- ☑ უნდა დაინერგოს მექანიზმი, რომელიც მონაცემთა შეცვლისაგან, გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან (მაგალითად, მონაცემების დათვალიერების, წაშლის, რედაქტირების ლოგირებით) დაცვის შესაძლებლობას იძლევა. ასევე, სასურველია, დაინერგოს უკანონოდ განადგურებული მონაცემების აღდგენის მექანიზმი.
- ☑ უნდა განისაზღვროს სისტემებში მონაცემებზე წვდომის დონეები, ვის, რა სახის მონაცემებზე ექნება წვდომა და რა მოქმედებების შესრულება შეეძლება (მაგალითად, ფაილის დამატება, წაშლა და სხვ.).
- ☑ უზრუნველყოფილ უნდა იქნეს ქსელიდან ინტერნეტში მონაცემთა გადაცემის დროს შესაბამისი უსაფრთხოება.
- ☑ სერვერის ინფორმაციული უსაფრთხოებისათვის (მაგალითად, ვიდეოჩანაწერებზე წვდომა არ უნდა იყოს შესაძლებელი ყველა კომპიუტერიდან) უნდა დაინერგოს შესაბამისი მექანიზმები.
- ☑ უსაფრთხოების ზომები პერიოდულად უნდა გადაიხედოს და საჭიროების შემთხვევაში, განახლდეს.[91]

[91] ICO, For organisations/UK GDPR guidance and resources/Security/A guide to data security, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/> [26.02.2024].

ნატო ვაჩნაძის ქუჩა N° 7, თბილისი

ბაქოს ქუჩა N° 48, ბათუმი

(+995 32) 242 1000

office@pdps.ge