მაკა ნუცუბიძე*

პერსონალურ მონაცემთა დაცვა მოქმედებების აღრიცხვის ჟურნალებში (ე.წ. „ლოგებში“)

სტატიაში განხილულია მოქმედებების აღრიცხვის ჟურნალებში (ე.წ. „ლოგებში“) პერსონალურ მონაცემთა დაცვის აქტუალური სამართლებრივი საკითხები. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის ძალაში შესვლასთან ერთად მეტი აქტუალურობით დადგა დღის წესრიგში ბალანსის აუცილებლობა მოქმედებების აღრიცხვის ჟურნალების, როგორც ინფორმაციული უსაფრთხოების სისტემის ეფექტურობასა და მასში შეგროვებული პერსონალური მონაცემების მაღალი სტანდარტით დაცულობას შორის.

საკვანძო სიტყვები: *მოქმედებების აღრიცხვის ჟურნალი, პერსონალური მონაცემები, მონაცემთა უსაფრთხოება, მონაცემთა დაცვის ძირითადი რეგულაცია, პერსონალურ მონაცემთა დაცვა.*

1. შესავალი

ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) საქმეში: “*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González”*[1] განაცხადა: „ინტერნეტის ავტომატური, მუდმივი და სისტემატური შესწავლის პროცესში, ინტერნეტში გამოქვეყნებული ინფორმაციის მოსაძიებლად, საძიებო სისტემის ოპერატორი „აგროვებს“ მონაცემებს, რომლებსაც შემდგომ „აღადგენს“, „იწერს“ და „ალაგებს“ ინდექსაციის პროგრამების ფარგლებში, „ინახავს“ სერვერებზე და საჭიროებისას, „ამჟღავნებს“ მას; ასევე, უზრუნველყოფს მასზე „წვდომას“ თავისი მომხმარებლებისათვის, საძიებო შედეგების ჩამონათვალის ფორმით.“[2] სასამართლოს დასკვნით, ამგვარი ქმედება არის „დამუშავება“, მიუხედავად იმისა, რომ საძიებო სისტემის ოპერატორი მსგავს ოპერაციებს ახორციელებს სხვა ტიპის ინფორმაციის მიმართ და ამ უკანასკნელს არ განარჩევს პერსონალური მონაცემებისაგან.“

ევროკავშირის კანონმდებლობის შესაბამისად „უახლესი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ბუნების, მოცულობის, კონტექსტისა და მიზნების, ასევე, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისათვის სავარაუდო საფრთხეების გათვალისწინებით, მონაცემთა დამუშავებისთვის

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის ასისტენტ პროფესორი, სამართლის დოქტორი.

[1] CJEU, Case 131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13/05/2014.

[2] იქვე, პუნქტი 28.

პასუხისმგებელმა და დამუშავებაზე უფლებამოსილმა პირებმა უნდა მიიღონ რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები უსაფრთხოების უზრუნველსაყოფად [...].“[3]

ეს ზომები მოიცავს შემდეგ ასპექტებს: პერსონალურ მონაცემთა ფსევდონიმიზაცია და დაშიფვრა; დამუშავების სისტემებისა და სერვისების მუდმივი კონფიდენციალობა, ხელშეუხებლობა, ხელმისაწვდომობა და მოქნილობა; ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში, პერსონალურ მონაცემთა წვდომისა და ხელმისაწვდომობის დროული აღდგენა; დამუშავების უსაფრთხოების ტექნიკურ და ორგანიზაციულ საშუალებათა ეფექტიანობის რეგულარული შემოწმება და შეფასება.

პერსონალურ მონაცემთა დაცვის საერთაშორისო სტანდარტით „ლოგირება“ განიხილება, როგორც სავალდებულო მოთხოვნა და მიიჩნევა მონაცემთა უსაფრთხოების გარანტიად.

აღსანიშნავია, რომ საქართველოს კანონმდებლობა არ იცნობს ტერმინებს „ლოგი“ და ლოგირება“. ამის მიუხედავად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი შეესაბამება ევროკავშირის, კერძოდ “GDPR”-ის სტანდარტს და დამუშავებისთვის პასუხისმგებელ პირს ავალდებულებს „უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების (მათ შორის, ინციდენტების შესახებ, მონაცემთა შეგროვების, შეცვლის, მათზე წვდომის, მათი გამჟღავნების (გადაცემის), დაკავშირებისა და წაშლის თაობაზე ინფორმაციის) აღრიცხვა“[4] - ანუ ლოგირება.

ამგვარად, საქართველოს კანონმდებლობის შესაბამისად, „ლოგირება“ გადაითარგმნა, როგორც „მოქმედებების აღრიცხვა“, ხოლო „ლოგი“ – „მოქმედებების აღრიცხვის ჟურნალი“.[5]

როგორც წესი, მოქმედებების აღრიცხვის ჟურნალის შექმნის დროს მასში თავს იყრის პერსონალური ინფორმაცია, რაც, თავის მხრივ, მოქმედებების აღრიცხვის ჟურნალებს გადააქცევს პერსონალური მონაცემების დამუშავების ადგილად. დღის წესრიგში დგება ბალანსის დაცვის აუცილებლობა მოქმედებების აღრიცხვის ჟურნალების, როგორც ინფორმაციული უსაფრთხოების სისტემის ეფექტურობასა და მასში შეგროვებული პერსონალური მონაცემების დაცულობას შორის.

ამგვარად, ჩვენი კვლევის მიზანია იმ საკანონმდებლო და პროცედურული სტანდარტების მიმოხილვა, რომლებიც ამ ბალანსის შესაძლებლობას იძლევა. შესაბამისად სტატიაში მიმოვიხილავთ მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის სტანდარტს “GDPR”-ის და საქართველოს კანონმდებლობის შესაბამისად (მეორე თავი); მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის პრინციპებს: მინიმიზაცია; ფსევდონიმიზაცია და დეპერსონალიზაცია (მესამე თავი) მოქმედებების აღრიცხვის ჟურნალებს, როგორც მონაცემთა უსაფრთხოების დაცვის გარანტს: ინციდენტის აღრიცხვა და შეტყობინება (მეოთხე თავი); ასევე, პროცედურულ მოთხოვნებს

[3] 2018 წლის 25 მაისს ძალაში შევიდა ევროპარლამენტისა და საბჭოს პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია (EU) 2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“, 27/04/2016, <https://gdpr-info.eu/> [02.07.2024]. იხ. მუხლი 5.

[4] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, მუხლი 27, პუნქტი 4.

[5] ფრანგულ ენაში, შესაბამისად საფრანგეთსა და კანადაში, ასევე არ გამოიყენება ტერმინები ლოგირება და ლოგი. მათ ნაცვლად „მოქმედებების აღრიცხვა“ და „მოქმედებების აღრიცხვის ჟურნალი“ (მ.ნ.).

მოქმედებების აღრიცხვის ჟურნალების მიმართ: შენახვის ვადები და წვდომაზე უფლებამოსილი პირები (მეხუთე თავი); დასკვნის სახით შემოგთავაზებთ რეკომენდაციებს ლოგირებისას და ლოგებში პერსონალური მონაცემების დაცვის მაღალი სტანდარტით უზრუნველსაყოფად.

2. მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის სტანდარტი "GDPR"-ის და საქართველოს კანონმდებლობის შესაბამისად

„პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის" მსგავსად ითვალისწინებს დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის ვალდებულებას უზრუნველყოს მონაცემთა უსაფრთხოება, კერძოდ, კანონის 27-ე მუხლის მე-4 პუნქტი ადგენს: „დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან უზრუნველყონ ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების (მათ შორის, ინციდენტების შესახებ, მონაცემთა შეგროვების, შეცვლის, მათზე წვდომის, მათი გამჟღავნების (გადაცემის), დაკავშირებისა და წაშლის თაობაზე ინფორმაციის) აღრიცხვა".

ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული მოქმედებების აღრიცხვა გამოიყენება უსაფრთხოების მიზნით, ინციდენტის მიზეზებისა და მის უკან მდგომი სუბიექტების შესახებ მოკვლევისა და გამოძიების უზრუნველსაყოფად. აღრიცხული მონაცემები გროვდება ოპერატორებისა და ინტერნეტთან დაკავშირებული მოწყობილობების საშუალებით.

ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული მოქმედებები ქრონოლოგიურად იწერება ელექტრონულ ჟურნალებში. მონაცემები გენერირდება ყოველთვის და ყველგან. ისინი შეიცავს ინფორმაციას მოქმედების დროისა და თარიღის შესახებ; აღრიცხავს განხორციელებულ მოქმედებას, მოქმედების მცდელობას და მომხმარებელს, ან IP მისამართს; აღრიცხავს ავტორიზებულ ან წვდომის უფლების მქონე მომხმარებელს; აღრიცხავს სად განხორციელდა მოქმედება და სად შეიცვალა ორიგინალური მონაცემები; აღრიცხავს მიაღწია თუ არა მომხმარებელმა შედეგს. წარუმატებელი მცდელობის შემთხვევაში იწერს (ინიშნავს და იმახსოვრებს) წარუმატებლობის მიზეზს.

იმავდროულად, აღრიცხვის ჟურნალებში მუშავდება პერსონალური მონაცემები განუსაზღვრელი რაოდენობით.

"GDPR"-ით და „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონით[6]: პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს უკავშირდება. ფიზიკური პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, მათ შორის, სახელით, გვარით, საიდენტიფიკაციო ნომრით, გეოლოკაციის მონაცემებით, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემებით, ფიზიკური, ფიზიოლოგიური, ფსიქიკური, ფსიქოლოგიური, გენეტიკური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლით. პერსონალურ ინფორმაციად შეიძლება ჩაითვალოს, მაგალითად,

[6] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", 14/06/2023, მუხლი 3, პუნქტი „ა".

პიროვნების განრიგი, ისევე როგორც ინფორმაცია ადგილმდებარეობის შესახებ, მათ შორის მათი IP მისამართი.

ამგვარად, მოქმედებების აღრიცხვის ჟურნალები ექვემდებარება პერსონალურ მონაცემთა დაცვის კონტროლს და მათზე ვრცელდება “GDPR”-ის მე-5 და 32-ე მუხლებით, ასევე, მონაცემთა დაცვის საქართველოს კანონმდებლობით ვალდებულებები.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლისა და „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.“

მონაცემთა მინიმიზაციის პრინციპის[7] დაცვისათვის საჭიროა, რომ დამუშავებული მონაცემების მოცულობა იყოს:

შემოფარგლული მხოლოდ იმით, რაც აუცილებელია: მოქმედებების აღრიცხვის ჟურნალებში არ უნდა დამუშავდეს უფრო მეტი მონაცემი, ვიდრე მიზნის მიღწევისთვის არის საჭირო. ეს კომპონენტი გულისხმობს, რომ მიზნის მიღწევა გონივრულად შეუძლებელია კონკრეტული პერსონალური მონაცემების დამუშავების გარეშე.

პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, როდესაც დამუშავების მიზნის მიღწევა, გონივრულობის ფარგლებში, შეუძლებელია სხვა საშუალებებით. ამასთანავე, მონაცემთა მინიმიზაციის პრინციპი მჭიდრო კავშირშია 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 მოქმედებების აღრიცხვის ჟურნალებში პერსონალური ინფორმაციის დამუშავების ოპერაციის თითოეულ საფეხურს და მონაცემთა თითოეულ ელემენტს.

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.

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

[7] იქვე, მუხლი 4.

სუბიექტების უფლებების რისკის შესამცირებლად პერსონალური მონაცემების ფსევდონიმიზაცია უნდა განხორციელდეს[8].

მოქმედებების აღრიცხვის ჟურნალები შეიცავს დიდი რაოდენობით მონაცემებს, მათი უმრავლესობა პერსონალური მონაცემებია. რაც უფრო მსხვილია ორგანიზაცია, მით მეტი პერსონალური ინფორმაცია მუშავდება და ინახება ჟურნალებში, მაგალითად, IP მისამართები და გეოლოკაციის მონაცემები. იმის გათვალისწინებით, რომ ხშირად მოქმედებების აღრიცხვის ჟურნალებში მონაცემების შენახვა კანონითაა გათვალისწინებული აპრობირებული მეთოდია მოქმედებების აღრიცხვის ჟურნალში მონაცემების გაფილტვრა, მაგალითად, ელექტრონული ფოსტის მისამართების ან ტელეფონის ნომრების რედაქტირება/წაშლა[9].

3. მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვა

ნებისმიერ შემთხვევაში, მონაცემთა დამუშავებაზე უფლებამოსილმა პირმა უნდა შექმნას ისეთი სისტემა, რომელიც უზრუნველყოფს მოქმედებების აღრიცხვის ჟურნალებში დაცული მონაცემების კონფიდენციალურობის, ხელმისაწვდომობისა და მთლიანობის გარანტიას. უფრო ზუსტად, შეგროვებული მონაცემების გამოყენება უნდა იყოს ფორმალიზებული და დოკუმენტირებული წინასწარ დადგენილი წესებითა და პროცედურებით.

იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა ინახებოდეს პირის იდენტიფიცირების გამომრიცხავი ფორმით.

უფლებამოსილი პირი, რომელსაც აქვს წვდომა დამუშავებაზე, ინფორმირებული უნდა იყოს მოქმედებების აღრიცხვის ჟურნალის გამოყენების წესების, შეგროვებული მონაცემების სახეობისა და მათი შენახვის ვადის შესახებ. ამის მიღწევა შესაძლებელია, მაგალითად, საინფორმაციო შეტყობინების საშუალებით ავტორიზაციის დროს/დაშვების წინ.

მონაცემების დამუშავებისას უზრუნველყოფილი უნდა იყოს მათი მთლიანობა, უსაფრთხოება და დაცვა უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვის, განადგურებისა და დაზიანებისგან[10].

“GDPR”-ის 32-ე მუხლი აფართოებს მე-5 მუხლში ჩამოყალიბებული მთლიანობისა და კონფიდენციალურობის ფუნდამენტურ პრინციპს და იძლევა მონაცემთა დაცვის შესაძლებლობას ფსევდონიმიზაციისა და დეპერსონალიზაციის საშუალებით, რომელიც ასევე ვრცელდება მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დამუშავებაზე.

„პერსონალურ მონაცემთა შესახებ“ საქართველოს კანონით მონაცემთა დეპერსონალიზაცია არის მონაცემთა იმგვარი დამუშავებაა, როდესაც შეუძლებელია მონაცემთა სუბიექტთან მათი დაკავშირება ან ასეთი კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას, ხარჯებს ან/და დროს საჭიროებს;[11] ხოლო მონაცემთა ფსევდონიმიზაცია – მონაცემთა იმგვარი დამუშავებაა, როდესაც

[8] რეკომენდაცია „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, პერსონალურ მონაცემთა დაცვის სამსახური, 2024.

[9] კანადის პირადი ცხოვრების დაცვის კომისარიატის გზამკვლევი მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის შესახებ, <https://www.cyber.gc.ca/sites/default/files/itsap80085-journalisation-surveillance-securite-reseau-f.pdf> [02.07.2024].

[10] იქვე.

[11] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, მუხლი 2, პუნქტი „ც“.

დამატებითი ინფორმაციის გამოყენების გარეშე შეუძლებელია მონაცემების კონკრეტულ მონაცემთა სუბიექტთან დაკავშირება და ეს დამატებითი ინფორმაცია შენახულია ცალკე და ტექნიკური და ორგანიზაციული ზომების მეშვეობით მონაცემების იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირთან დაკავშირება არ ხდება[12].

ახალი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ხასიათის, მასშტაბის, კონტექსტისა და მიზნების, აგრეთვე, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისთვის მოსალოდნელი რისკებისა და მონაცემთა დამუშავების პრინციპების გათვალისწინებით, დამუშავებისთვის პასუხისმგებელმა პირმა, როგორც დამუშავების საშუალებების განსაზღვრის, ისე უშუალოდ დამუშავების პროცესში უნდა მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები (მათ შორის, ფსევდონიმიზაცია ან/და სხვა). ამ ზომების მიღება უნდა უზრუნველყოფდეს მონაცემთა დამუშავების პრინციპების ეფექტიან იმპლემენტაციას და მონაცემთა დამუშავების პროცესში დაცვის მექანიზმების ინტეგრირებას მონაცემთა სუბიექტის უფლებების დასაცავად.[13]

4. მოქმედებების აღრიცხვის ჟურნალები, როგორც მონაცემთა უსაფრთხოების დაცვის გარანტი: ინციდენტის აღრიცხვა და შეტყობინება

“GDPR”-ის 33-ე მუხლით, ისევე როგორც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 29-ე მუხლით: „დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია აღრიცხოს ინციდენტი, დამდგარი შედეგი, მიღებული ზომები და ინციდენტის აღმოჩენიდან არაუგვიანეს 72 საათისა მის შესახებ წერილობით ან ელექტრონულად შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს, გარდა იმ შემთხვევისა, როდესაც ნაკლებსავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს“. ასევე „დამუშავებაზე უფლებამოსილი პირი ვალდებულია ინციდენტის შესახებ დაუყოვნებლივ აცნობოს დამუშავებისთვის პასუხისმგებელ პირს“.

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის[14] შესაბამისად, შეტყობინება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) ინციდენტის გარემოებების, სახისა და დროის შესახებ;

ბ) ინციდენტის შედეგად უნებართვოდ გამჟღავნებული, დაზიანებული, წაშლილი, განადგურებული, მოპოვებული, დაკარგული, შეცვლილი მონაცემების სავარაუდო კატეგორიებისა და რაოდენობის, აგრეთვე იმ მონაცემთა სუბიექტების სავარაუდო კატეგორიებისა და რაოდენობის შესახებ, რომლებსაც ინციდენტის შედეგად შეექმნათ საფრთხე.

მოქმედებების აღრიცხვის ჟურნალები, რომლებიც აღრიცხავენ სისტემის შიდა ფუნქციონირებას, წარმოადგენს ერთადერთ მონაცემთა ბაზას, რომელიც საშუალებას აძლევს დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს რეაგირებისა და შეტყობინების უზრუნველსაყოფად.

[12] იქვე, პუნქტი „ძ“.
[13] იქვე, მუხლი 26.
[14] იქვე, მუხლი 29.

5. პროცედურული მოთხოვნები მოქმედებების აღრიცხვის ჟურნალების მიმართ: შენახვის ვადები და წვდომაზე უფლებამოსილი პირები

5.1. მოქმედებების აღრიცხვის ჟურნალების შენახვის ვადები

"GDPR"-ის 30-ე მუხლი და „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის 28-ე მუხლი აწესებს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულებას, კერძოდ, დამუშავებისთვის პასუხისმგებელი პირი და მისი სპეციალური წარმომადგენელი (ასეთის არსებობის შემთხვევაში) ვალდებული არიან წერილობით ან ელექტრონულად უზრუნველყონ მონაცემთა დამუშავებასთან დაკავშირებული შემდეგი ინფორმაციის აღრიცხვა: მონაცემთა შენახვის ვადების შესახებ, ხოლო თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, მათი შენახვის ვადის განსაზღვრის კრიტერიუმების თაობაზე.

მოქმედებების აღრიცხვის ჟურნალები ხშირად დიდი ხნის განმავლობაში ინახება. მათი დანიშნულებიდან გამომდინარე შენახვის ვალდებულება უალტერნატივოა, რადგან ისინი შეიცავს მნიშვნელოვან ინფორმაციას ინციდენტის ან ინციდენტის მცდელობის შემთხვევაში ეფექტური გამოძიების ჩასატარებლად. იმავდროულად, მათში თავმოყრილი პერსონალური მონაცემების უვადოდ და გაუმართლებლად დიდი ხნით შენახვა არაგონივრული რისკია.

მართალია, "GDPR" არ აკონკრეტებს პერსონალური მონაცემების შენახვის ზუსტ ვადას, თუმცა საქმეში Digital Rights Irelan[15] ევროკავშირის მართლმსაჯულების სასამართლომ ("CJEU") იმსჯელა მონაცემთა შენახვის დირექტივის კანონიერებაზე[16]. "CJEU" შეეხო მონაცემთა შენახვის დირექტივაში ობიექტურ კრიტერიუმთა არარსებობასაც, რომელთა საფუძველზეც უნდა განისაზღვროს მონაცემთა შენახვის ზუსტი პერიოდი - მინიმალური 6 თვიდან მაქსიმალურ 24 თვემდე.

ამგვარად, მოქმედებების აღრიცხვის ჟურნალების შენახვის ვადა ევროკავშირის ქვეყნების კარგი პრაქტიკის[17] გათვალისწინებით მერყეობს 6 თვიდან - 12 თვემდე. განსაკუთრებულ შემთხვევებში ეს ვადა შესაძლებელია გაგრძელდეს 24 თვემდე.

"GDPR"-ის მე-5 მუხლისა და „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-4 მუხლის შესაბამისად მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა წაიშალოს, განადგურდეს ან

[15] CJEU, Case C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 08/04/2014.

[16] დირექტივა მიზნად ისახავდა შიდასახელმწიფოებრივი დებულებების ჰარმონიზებას ისეთი პერსონალური მონაცემების შენახვასთან დაკავშირებით, რომლებიც მოპოვებული და დამუშავებულია საჯაროდ ხელმისაწვდომი ელექტრონული საკომუნიკაციო სერვისების ან ქსელების საშუალებით და შეიძლება გადაეცეს უფლებამოსილ უწყებას ორგანიზებულ დანაშაულსა და ტერორიზმთან ბრძოლის მიზნებით. მონაცემთა დაცვის დირექტივა ადგენდა მონაცემთა შენახვას, „სულ მცირე, 6 თვის ვადით, ისე, რომ არ განარჩევდა ამავე დირექტივის მე-5 მუხლით გათვალისწინებულ მონაცემთა კატეგორიებს იმის მიხედვით, თუ რამდენად გამოსადეგი იყო დასახული მიზნის მისაღწევად ან რომელ პირებს მიემართებოდა.".

[17] საფრანგეთის ინფორმაციისა და თავისუფლების ეროვნული კომისიის ("CNIL") დადგენილება №2021-122 „მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის შესახებ".

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.

დამუშავებისთვის პასუხისმგებელი პირის მიერ შენახვის ვადის განსაზღვრისას გათვალისწინებული უნდა იქნეს მისაღწევი მიზნის პროპორციული დროის მონაკვეთი. მაქსიმალური - 24 თვიანი ვადა უნდა დასაბუთდეს. ნებისმიერ შემთხვევაში, შეუძლებელია მაქსიმალური ვადის გამართლება მხოლოდ სისხლის სამართლის დანაშაულის ხანდაზმულობის ვადით.

დამუშავებისას სხვადასხვა ფაქტორების გათვალისწინებით შესაძლებელია შენახვის მაქსიმალური ვადის განსაზღვრა ჩაითვალოს გამართლებულად[18], მაგალითად:

- როდესაც კანონმდებლობით დადგენილია ჩანაწერების შენახვის კონკრეტული ვადა;
- კონკრეტული მიზნისთვის, რომლის მიღწევა მხოლოდ მოქმედებების აღრიცხვის ჟურნალების მონაცემების გამოყენებითაა შესაძლებელი, მაგალითად, დამუშავების კონტექსტში, რომელიც საშუალებას მისცემს დავის მონაწილეებს, გაეცნონ დოკუმენტებსა და შესაბამის მასალებს, რათა უზრუნველყოფილი იქნას პროცესის გამჭვირვალობა დაინტერესებული მხარეებისთვის;
- როდესაც არსებობს თავდასხმის შემდგომი ან შეჭრის მცდელობის შემდგომი ანალიზის განხორციელების აუცილებლობა, რომელიც დაკავშირებულია სამომავლოდ, გრძელვადიან პერსპექტივაში საფრთხის გაანალიზების აუცილებლობასთან.

მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელი პირმა ზუსტად და დოკუმენტურად დაასაბუთოს ის მიზეზები, რის გამოც მას უფრო ხანგრძლივი ვადის დადგენა უწევს[19], მაგალითად, კონკრეტული სამართლებრივი ვალდებულების ან სპეციფიკის მითითებით, რომლებიც დაკავშირებულია მიზანთან. მონაცემთა უფრო ხანგრძლივად შენახვის აუცილებლობა შეიძლება ასევე გამართლებული იყოს იმით, რომ ეს ღონისძიება არის ერთადერთი გზა, რათა მოხდეს მაღალი რისკის ქვეშ მყოფი ფიზიკური პირების მიმართ მონაცემთა დაცვაზე ზემოქმედების შეფასებისა (“AIPD”) ან ექვივალენტური შესწავლის. ეს ანალიზი უნდა განხორციელდეს ინდივიდუალურად, “GDPR”-ის პრინციპების გამოყენებით, სადაც ეს შესაძლებელია, რათა განისაზღვროს საჭირო გარანტიები უსაფრთხოების პირობების, ხელმისაწვდომობისა და მონაცემთა შენახვის მიზნების თვალსაზრისით.

5.2. უფლებამოსილი პირების წვდომა მოქმედებების აღრიცხვის ჟურნალებზე

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის მე-6 პუნქტის შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან თანამშრომელთა უფლებამოსილებების შესაბამისად განსაზღვრონ მონაცემებზე წვდომის ფარგლები და განახორციელონ ადეკვატური ღონისძიებები თანამშრომელთა მიერ მონაცემთა

[18] იქვე.
[19] იქვე.

უკანონო დამუშავების ფაქტების თავიდან ასაცილებლად, გამოსავლენად და აღსაკვეთად, მათ შორის, უზრუნველყონ თანამშრომელთა ინფორმირება მონაცემთა უსაფრთხოების დაცვის საკითხების შესახებ.

პირი, რომელიც სარგებლობს მოქმედებების აღრიცხვის ჟურნალებზე წვდომის უფლებით, ვალდებულია, არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს, დაიცვას მონაცემთა საიდუმლოება და კონფიდენციალურობა, მათ შორის, სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგ[20].

თავდაპირველი მიზნისგან განსხვავებით, შეგროვებული მონაცემების ნებისმიერი ხელახალი დამუშავება ნიშნავს დამუშავების საბოლოო მიზნის ცვლილებას. ამიტომ, მიზანშეწონილია დამუშავებაზე პასუხისმგებელმა პირმა მიიღოს ტექნიკური და ორგანიზაციული ზომები, რომლებიც შესაძლებლობას მისცემს შეამციროს რისკები. მაგალითად, დაავალდებულოს მოქმედებების აღრიცხვის ჟურნალებზე წვდომაზე უფლებამოსილი პირები დაიცვან მონაცემების გამოყენების წესები (წინასწარ დადგენილი) ან სპეციალური გაფრთხილების სისტემის არსებობით მოახდინოს მოქმედებების აღრიცხვის ჟურნალებში უკანონოდ განხორციელებული ცვლილებების პრევენცია.

6. დასკვნა და რეკომენდაციები

კვლევამ აჩვენა, რომ მოქმედებების აღრიცხვის ჟურნალები წარმოადგენს შეუცვლელ და მნიშვნელოვან შესაძლებლობას ინციდენტთან დაკავშირებული საფრთხეების მისაკვლევად და გამოსავლენად, სისტემების დაცვის პრევენციული ღონისძიებების დასაგეგმად და განსახორციელებლად. თუმცა იმისათვის, რომ ჟურნალებში თავმოყრილი პერსონალური მონაცემები “GDPR”-ისა და საქართველოს კანონმდებლობის შესაბამისად მაღალი ხარისხით იქნეს დაცული, მონაცემთა დამუშავებისთვის პასუხისმგებელმა და დამუშავებაზე უფლებამოსილმა პირებმა უნდა გაითვალისწინონ და პრაქტიკაში დანერგონ შემდეგი რეკომენდაციები:

- მოქმედებების აღრიცხვის ჟურნალებში მონაცემების დამუშავება უნდა შეესაბამებოდეს შემდეგ პრინციპებს: სამართლიანობა, კანონიერება და გამჭვირვალობა;
- დამუშავების მიზანი უნდა იყოს კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური. არ შეიძლება მოქმედებების აღრიცხვის ჟურნალებში შეგროვებული მონაცემების გამოყენება სხვა მიზნით;
- მოქმედებების აღრიცხვის ჟურნალებში უნდა შეგროვდეს მხოლოდ ის მონაცემები, რომლებიც საჭიროა იმისთვის, რომ უზრუნველყოს მონაცემთა უსაფრთხოების დაცვა ინციდენტის, ან ინციდენტის მცდელობის აღსაკვეთად, გასაანალიზებლად ან გამოსაძიებლად;
- მოქმედებების აღრიცხვის ჟურნალებში მონაცემები უნდა ინახებოდეს მხოლოდ წინასწარ დადგენილი ვადით;
- მოქმედებების აღრიცხვის ჟურნალები უნდა ინახებოდეს უსაფრთხოდ, სასურველია გარე სერვერებზე. ეს მონაცემები შენახული იქნას ძირითადი სისტემისგან განცალკევებულად. წვდომა განსაზღვრული უნდა იყოს წინასწარ განსაზღვრული ფორმით მხოლოდ უფლებამოსილი პირებისთვის.

[20] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023, მუხლი 27, პუნქტი 5.

მოქმედებების აღრიცხვის სისტემა უნდა იყოს აღჭურვილი დუბლირება-კოპირების/გადაწერის პრევენციული ტექნიკური საშუალებებით;
- რეკომენდირებულია მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემები იყოს დაშიფრული.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 14/06/2023.
2. ევროპარლამენტისა და საბჭოს პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია (EU) 2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“, 27/04/2016, <https://gdpr-info.eu/> [02.07.2024].
3. კანადის პირადი ცხოვრების დაცვის კომისარიატის გზამკვლევი მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის შესახებ, <https://www.cyber.gc.ca/sites/default/files/itsap80085-journalisation-surveillance-securite-reseau-f.pdf> [02.07.2024].
4. რეკომენდაცია „პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ“, პერსონალურ მონაცემთა დაცვის სამსახური, 2024, <https://personaldata.ge> [02.07.2024].
5. საფრანგეთის ინფორმაციისა და თავისუფლების ეროვნული კომისიის (“CNIL”) დადგენილება №2021-122 „მოქმედებების აღრიცხვის ჟურნალებში პერსონალური მონაცემების დაცვის შესახებ“, <https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation_-_journalisation.pdf> [02.07.2024].
6. ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება, CJEU, Case 131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC]*, 13/05/2014.
7. ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება, CJEU, Case C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC]*, 08/04/2014.