პერსონალურ მონაცემთა დამუშავების პრინციპების რეალიზება მიმდინარე შრომით ურთიერთობებში

ეთერ შერმადინი

წარმოდგენილია სამართლის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

სულხან-საბა ორბელიანის სასწავლო უნივერსიტეტი
თბილისი 0164, საქართველო სექტემბერი 2020

სულხან-საბა ორბელიანის სასწავლო უნივერსიტეტი

სამართლის ფაკულტეტი

ვადასტურებ, რომ გავეცანი ეთერ შერმადინის მიერ შესრულებულ სამაგისტრო ნაშრომს დასახელებით: პერსონალურ მონაცემთა დამუშავების პრინციპების რეალიზება მიმდინარე შრომით ურთიერთობებში და ვაძლევ რეკომენდაციას სულხან-საბა ორბელიანის სასწავლო უნივერსიტეტის სამართლის ფაკულტეტის საგამოცდო კომისიაში მის განხილვას სამართლის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად.

თარიღი: 03.09.2020

ხელმძღვანელი: კახაბერ გოშაძე

სულხან-საბა ორბელიანის სასწავლო უნივერსიტეტი

სამართლის ფაკულტეტი

განაცხადი წარმოდგენილ ნაშრომში პლაგიატის არარსებობის შესახებ

როგორც წარმოდგენილი ნაშრომის ავტორი, ვაცხადებ, რომ ნაშრომი წარმოადგენს ჩემს ორიგინალურ ნამუშევარს და არ შეიცავს სხვ ავტორების მიერ აქამდე გამოქვეყნებულ, გამოსაქვეყნებლად მიღებულ ან დასაცავად წარდგენილ მასალებს, რომლებიც ნაშრომში არ არის მოხსენიებული ან ციტირებული სათანადო წესების შესაბამისად.

სტუდენტი: ეთერ შერმადინი

თარიღი: 03.09.2020

ანოტაცია

ნაშრომში მოცემულია პერსონალურ მონაცემთა დამუშავების პრინციპების იმპლემენტირების საკითხი მიმდინარე შრომით ურთიერთობებში, მათი არსი. დანიშნულება და მნიშვნელობა. ასევე, განხილულია პრინციპების რეალიზებისა და კანონმდებლობაში არსებული ხარვეზების აღმოფხვრის გზები.

ნაშრომის ძირითად საკითხს წარმოადგენს პერსონალურ მონაცემთა დაცვის პრინციპების ზოგადი რეალიზება მიმდინარე შრომით ურთიერთობებში დამმუშავებლის მიერ, მონაცემთა აუთსორსი დამუშავების პრინციპების შესაბამისად, მონაცემთა დაცვის ოფიცრის ინსტიტუტის არსი, მნიშვნელობა და დანიშნულება. თემის განხილვის პროცესში გაანალიზებულია ის საკანონმდებლო ნორმები, რომელიც აღნიშნულ ინსტიტუტებს აწესრიგებს.

ნაშრომის მიზანია განსაზღვროს პერსონალურ მონაცემთა დამუშავების პრინციპების იმპლემენტირების თავისებურებები შრომით სახელშეკრულებო ურთიერთობებში, ასევე წარმოაჩინოს ძირითადი პრობლემები და გამოწვევები, რომელიც არის ადგილობრივ კანონმდებლობასა და პრაქტიკაში, ასევე მიმდინარე შრომით ურთიერთობებში პერსონალურ მონაცემთა დამუშავების პრინციპების ანალიზის პერსპექტივიდან განხილული იქნეს მათი იმპლემენტირების საკითხი.

Abstract

The paper covers a subject of the implementation of the principles of personal data processing in the actual (ongoing) labor relations. The essence of the implementation process, purpose and significance are also reviewed, considering that the volume of the personal data processed in labor relations in relatively large. The ways to implement the principles and eliminate gaps in the legistation are also discussed.

The paper mainly focuses on the methods of implementation of the general principles of personal data processing by the controller and processor in the actual labor relations. In the regard, principles are thoroughly analyzed and reviewed in a way that gives the reader clear view on the overall purpose and importance.

The aim of the paper is to identify the peculiarities of implementing those principles in labor relations as well as to present main problems and challenges, existing in local legislation and practice.

სარჩევი

შესავალი 2

1. პერსონალურ მონაცემთა დაცვის კონცეფცია 6

1.1 მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის ევოლუცია 9

1.2 პერსონალურ მონაცემთა დამუშავების პრინციპების დანიშნულება და მიმართება დამუშავების წესებთან 13

2. მონაცემთა დამუშავების პრინციპების მოქმედება მიმდინარე შრომით ურთიერთობებში 23

2.1 მონაცემთა დამუშავების პრინციპების ზოგადი რეალიზება დამმუშავებლის მიერ 25

2.1.1. დამუშავების პროცესის კანონიერების, სამართლიანობისა და ღირსების დაცვის უზრუნველყოფა 26

2.1.2. მიზნის მკაფიოდ განსაზღვრა, როგორც პროპორციული დამუშავების უზრუნველყოფის წინაპირობა 31

2.1.3. მონაცემთა მიზნობრივი განახლება და სისწორის დაცვა 37

2.1.4. დამუშავების მთელი პროცესის უსაფრთხოდ უზრუველყოფა 41

2.1.5. მონაცემთა დამმუშავებლის მიერ ანგარიშვალდებულებისა და გამჭვირვალობის დემონსტრირება 44

2.2 მონაცემთა დამუშავების აუთსორსის ურთიერთმიმართბეა დამუშავების პრინციპებთან 46

2.2.1. დამმუშავებლის ვალდებულებები აუთსორსის წინარე პერიოდსა და მიმდინარე პროცესში 48

2.2.2. მონაცემთა აუთსორსი მონაცემთა საერთაშორისო გადაცემის კონტექსტში 50

3. მონაცემთა დაცვის ოფიცერი, როგორც დამუშავების ანგარიშვალდებულების პრინციპის რეალიზების ეფექტური გზა ..... 54 დასკვნა .....

58 ბიბლიოგრაფია: .....
66

შესავალი

ტექნოლოგიების განვითარებასთან ერთად იზრდება პერსონალური მონაცემების დაცვის საჭიროება. აუცილებელია შესაბამისი საკანონმდებლო ბაზისა და მის საფუძველზე ქმედითი საშუალებების შემუშავება, რომელიც ხელს შეუწყობს და დაავალდებულებს საჯარო და კერძო სექტორს უზრუნველყოს კანონმდებლობით გათვალისწინებული დებულებების პრაქტიკული იმპლემენტირება პერსონალური მონაცმების დაცვასთან დაკავშირებით. ორგანიზაციების მიერ ყოველდღიურად მარტივდება მონაცემთა დამუშავება და მათზე წვდომის შესაძლებლობა, რამაც, თავის მხრივ, წარმოშვა პერსონალური მონაცემების არამართლზომიერი გამოყენების რისკები.

როგორც წესი, პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის აღსრულება მეტად ეფექტურად შეინიშნება საჯარო სექტორში, ვიდრე კერძო ორგანიზაციებში (ამას მოწმობს სახელმწიფო ინსპექტორის მიერ გამოცემული წლიური ანგარიშები). მონაცემთა დამუშავება მეტად ინტენსიურად კერძო სექტორის მიერ ხორციელდება. ეს ვლინდება ორი მიმართულებით: 1. საჯარო დაწესებულებებთან შედარებით მათი რაოდენობა დიდია და 2. ბიზნეს პროცესის განვითარებასთან ერთად ხშირად გამოიყენება მონაცემთა დამუშავების მრავალფეროვანი მეთოდები. ამდენად, განსაკუთრებული მნიშვნელობა ენიჭება მონაცემთა დამუშავების ფუძემდებლური პრინციპების დაცვას, განსაკუთრებით კი, მიმდინარე შრომითსამართლებრივ ურთიერთობებში, სადაც პერსონალურ მონაცემთა დამუშავება საკმაოდ ინტენსიურია. ამ მხრივ, აუცილებელია

შიდაორგანიზაციულად ჩამოყალიბებული იყოს მონაცემთა დამუშავების შესაბამისი სტანდარტები, რომელიც თანხვედრაში იქნება მონაცემთა დაცვის მარეგულირებელ კანონმდებლობასთან. შესაბამისად, მნიშვნელოვანია განისაზღვროს პერსონალურ მონაცემთა დამუშავების მიზანი და მისი დამუშავების აუცილებლობა, ასევე როგორ გამოიყენებს დამსაქმებელი დამუშავებულ მონაცემებს და რა შედეგი შეიძლება მოჰყვეს მას, ასევე რა სახის პერსონალური მონაცემების დამუშავების საშუალებას აძლევს კანონი და რა არის დამუშავების მიზანი (მაგ: განსაკუთრებული კატეგორიის პერსონალური მონაცემი, ბიომეტრიული მონაცემი და ა.შ), მნიშვნელოვანია განისაზღვროს დამუშავების წყარო, ანუ საიდან მუშავდება ესა თუ ის პეროსნალური მონაცემი დამსაქმებლის მიერ, ხდება თუ არა პერსონალური მონაცემების გაცემა მესამე პირებზე, (მაგ: უფლებამოსილი პირი) გაცემის საფუძველი და მიზანი. აუცილებელია განისაზღვროს პერსონალურ მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის დადებული ხელშერკულებით გათვალისწინებული პერსონალური მონაცემების დამუშავების ფარგლები, და კანონით რომელი თავდაცვის მექანიზმები გააჩნია მონაცემთა დამუშავების სუბიექტს. მხარეთა თანასწორუფლებიანობა და ნების ავტონომია წამყვანი პრინციპებია ურთიერთობის წარმოშობისა და მიმდინარეობისას. სხვა სიტყვებით, საინტერესოა განისაზღვროს თუ რა ოდენობით იჭრება მონაცემთა დამუშავების იმპერატიული, ამავდროულად, პრინციპული მოთხოვნები შრომით სახელშეკრულებო ურთიერთობებში.

გარდა ამისა, ზოგიერთ შემთხვევაში მხოლოდ შიდა ორგანიზაციული დამუშავების პროცედურები ვერ იქნება ეფექტიანი თუ არ იქნება დანერგილი მონაცემთა სუბიექტის უფლებების ეფექტური რეალიზაციის გზები, რაც, მაგალითად, შესაძლებელია განხორციელდეს ორგანიზაციაში მონაცემთა დაცვის ოფიცრის განსაზღვრითა და შესაბამისი უფლებების მინიჭებით.

ზემოაღნიშნულიდან გამომდინარე, წინამდებარე ნაშრომის მიზანია განისაზღვროს პერსონალურ მონაცემთა დამუშავების პრინციპების იმპლემენტირების თავისებურებები შრომით სახელშეკრულებო ურთიერთობებში, ასევე, წარმოაჩინოს პერსონალურ მონაცემთა დაცვის პრინციპების მნიშვნელობა და დანიშნულება. გარდა ამისა, ნაშრომი ითვალისწინებს იმ ძირითადი პრობლემებისა და გამოწვევების წარმოჩენას, რომელიც არის ადგილობრივ კანონმდებლობასა და პრაქტიკაში, ნაშრომის მიზანია აგრეთვე შედარებითი ანალიზის საფუძველზე შეფასდეს ევროპული სტანდარტები და მათი დანერგვა ქართულ კანონმდებლობაში, პრინციპების გამოყენებასთან დაკავშირებით, ასევე შრომით სახელშეკრულებო ურთიერთობებში პერსონალურ მონაცემთა დამუშავების პრინციპების ანალიზის პერსპექტივიდან განხილულ იქნეს მათი იმპემენტირების საკითხი.

გამომდინარე იქედან, რომ პერსონალურ მონაცემთა დამუშავების პრინციპებს გააჩნია კუმულაციური ხასიათი, მნიშვნელოვანია თითოეული პრინციპის არსი სწორად იქნეს გაგებული. საკითხი საინტერესოა იმდენად, რამდენადაც თავისი არსით მონაცემთა დაცვის უფლება, ძირითადი უფლებაა, რომელსაც უშუალო მოქმედების გამოვლინება გააჩნია კერძო სამართლებრივ, განსაკუთრებით კი შრომით სამართლებრივ ურთიერთობებში. ამდენად, საინტერესოა რამდენად ერევა იმპერატიული ნორმები შრომით სამართლებრივ ურთიერთობებში.

გარდა ამისა, მონაცემთა დამუშავების პრინციპები თავისი ბუნებით აღმატებულია დამუშავების საფუძვლებზე, ეს ნიშნავს, რომ თუ მხარეები შეთანხმდნენ გარკვეულ საკითხზე, რომელსაც შემხებლობა აქვს მონაცემთა გამოყენებასთან, დამუშავების პრინციპების ბუნებიდან გამომდინარე, ისინი სავალდებულოდ უნდა იქნეს გათვალისწინებული, წინააღმდეგ შემთხვევაში დამუშავების კანონიერება შესაძლოა სადავო გახდეს მონაცემთა დაცვის პერსპექტივიდან გამომდინარე.

ნაშრომში დასახული ამოცანების გადასაწყვეტად, წარმოდგენილ იქნება სამეცნიერო სფეროში გავრცელებული კვლევის მეთოდები. ეს მეთოდებია, ისტორიულ-შედარებითი, ლოგიკური, სისტემურ-სტრუქტურული, სოციოლოგიური, ფუნქციური, სინთეზის, სიტუაციური ანალიზი, დოკუმენტების შესწავლა-შედარება და პროგნოზირება. შედარებითსამართლებრივი კვლევის მეთოდი იძლევა სხვადასხვა ქვეყნის კანონმდებლობის დადებითი და უარყოფითი მხარეების შედარების საშუალებასა და შეჯერების მეშვეობით ლოგიკურ და თანამიმდევრულ დასკვნამდე იქნეს მსჯელობა წაყვანილი. ანალიტიკური კვლევის მეთოდი, თავისთავად, გულისხმობს პრობლემათა ანალიზს, რაც, კვლავ, მსჯელობის ლოგიკურ თანამიმდევრობას, განსაზღვრავს და იძლევა რაციონალური დასკვნის განხორციელების შესაძლებლობას. ისტორიული კვლევის მეთოდი კი პერსონალურ მონაცემთა დამცავი კანონმდებლობის განვითარების ეტაპებს წარმოაჩენს. რაც შეეხება სოციოლოგიური კვლევის მეთოდს, მისი გამოყენება აუცილებელიცაა, ვინაიდან პერსონალური მონაცემი თავისი არსით სოციუმს უკავშირდება და სოციუმში მყოფ თითოეულ პიროვნებას გააჩნია ის.

1. პერსონალურ მონაცემთა დაცვის კონცეფცია

პერსონალურ მონაცემთა დაცვა უზრუნველყოფს პირადი ცხოვრების ინფორმაციული ასპექტის დაცვას, რა დროსაც, პერსონალური მონაცემები უნდა დაექვემდებაროს კანონიერ დამუშავებას, პარალელურად კი, უზრუნველყოფილი იყოს მონაცემთა სუბიექტების - ფიზიკური პირების პერსონალური მონაცემების დაცვა. პერსონალურ მონაცემთა დაცვის აქტუალობა, დამატებით, გამოწვეულია ტექნოლოგიური პროგრესითა და მისგან გამომდინარე გამოწვევებით.

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ ადგენს პერსონალური მონაცემის დეფინიციას, რომელიც შეესაბამება საერთაშორისოდ აღიარებულ სტანდარტს, კერძოდ, პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ და იდენტიფიცირებად ფიზიკურ პირს, ხოლო პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ[1]. კანონის მოქმედება ვრცელდება მხოლოდ ფიზიკურ პირებზე[2], ასევე, დეფინიციაში გამოყოფილია, რომ ნებისმიერი ინფორმაცია შეიძლება ჩაითვალოს პერსონალურ მონაცემად, მაგრამ აუცილებელია, რომ ამით ფიზიკური პირის იდენტიფიცირება მოხდეს. საქართველოს უზენაესმა სასამართლომ ერთ-ერთ გადაწყვეტილებაში ხელფასის ოდენობა მიიჩნია პერსონალურ მონაცემად, რადგან საკითხი ეხებოდა მაიდენტიფიცირებელ ინფორმაციას[3], CJEU გაერთიანებულ საქმეებში აღნიშნავს, რომ ელექტრონული საკომუნიკაციო საშუალებებით მიღებული ყოველდღიური ცხოვრების ჩვევების, მუდმივი ან დროებითი საცხოვრებელი ადგილების შესახებ ინფორმაციის, ყოველდღიური ან სხვა სახის მოძრაობების, განხორციელებული საქმიანობის, სუბიექტთა

[1] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მუხლი 2, ა პუნქტი.

[2] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მუხლი 3.

[3] საქართველოს უზენაესი სასამართლოს სამოქალაქო საქმეთა პალატის 2015 წლის 22 მაისის გადაწყვეტილება საქმე №ას-243-230-2015.

სოციალური ურთიერთობების და მათი სოციალური გარემოს შესახებ მონაცემები იძლევა ძალიან ზუსტი დასკვნების გაკეთების შესაძლებლობას, რომ ეს წარმოადგენს პირად ცხოვრებასთან დაკავშირებულ ინფორმაციას[4] და ამ შემთხვევაში საქმე ეხება სწორედ პერსონალურ მონაცემების დამუშავებას [5] . ასევე ადამიანის უფლებათა ევროპულმა სასამართლომ პეროსონალურ მონაცემად მიიჩნია გაზეთში გამოქვეყნებული ინფორმაცია საგადასახადო მონაცემების დამუშავებასთან დაკავშირებით [6] , კერძოდ დასაბეგრ და მიუღებელ შემოსავალზე, ასევე დასაბეგრ წმინდა აქტივებზე[7].

ცნების განმარტებისთვის, ასევე, საინტერესოა, რომ პერსონალურ მონაცემთა დაცვის ინსპექტორმა სააფთიაქო ქსელში აუდიო-ვიდეო მონიტორინგი უკანონოდ ცნო, ვინაიდან მედიკამენტების შეძენით (ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია, რომელიც არის განსაკუთრებული კატეგორიის მონაცემი) შესაძლებელი იყო პირის იდენტიფიცირება პირდაპირი ან არაპირდაპირი გზით [8] . შესაბამისად, კანონი ფართო ინტერპრეტაციის საშუალებას იძლევა იმის თაობაზე, თუ რა შეიძლება ჩაითვალოს პერსონალურ მონაცემად. პერსონალური მონაცემად ჩაითვლება ფიზიკური პირის მონაცემები, რომლის საფუძველზეც ხდება მისი იდენტიფიცირება, მაგალითად მისთვის დამახასიათებელი ნიშნები: თვალის ფერი, სახის მოყვანილობა, სისხლის ჯგუფი, ნასამართლეობა, პროფესია, ჰობი, და ა. შ[9]. „ნებისმიერ ინფორმაციით“ იდენტიფიცირება დამოკიდებულია ასევე ინფორმაციის სისწორეზე, წინააღმდეგ შემთხვევაში ასეთი მონაცემი ექვემდებარება წაშლას, დაბლოკვას, განადგურებას [9] .

---

[4] CJEU, In Joined Cases C 293/12 and C 594/12, Digital Rights Ireland Ltd (C 293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, 8 April, 2014, პარაგრაფი 27.

[5] იხ. იქვე პარაგრაფი 29.

[6] ადამიანის უფლებათა ევროპული სასამართლოს 2017 წლის 27 ივნისის გადაწყვეტილება საქმეზე Satakunnan Markkinaporssi oy and Satamedia oy v. Finald, პარაგრაფი 13-14.

[7] იხ, იქვე პარაგრაფი 20-22.

[8] იხ. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის 20 მაისის გადაწყვეტილება შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N: გ-1/143/2015, გვ.6.

[9] იხ.„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მუხლი 2, პუნქტი ა, ბ.

[9] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მუხლი 4.

ტექნოლოგიების და განსაკუთრებით კი ინტერნეტსივრცის ფართო მაშტაბიანმა განვითარებამ ხელი შეუწყო ინფორმაციაზე მარტივად წვდომას, რამაც საფრთხის ქვეშ დააყენა პერსონალური მონაცემების უსაფრთხოდ დაცვის საკითხი. ამასთანავე აღსანიშნავია, რომ პერსონალურ მონაცემთა დაცვა ემსახურება უფლებრივი ბალანსის უზრუნველყოფას დამმუშავებელსა და სუბიექტს შორის.

ამავდროულად, პერსონალური მონაცემები დაკავშირებულია პირადი ცხოვრების ხელშეუხებლობის უფლებასთან. ადამიანის უფლებათა ევროპული სასამართლო ხაზგასმით აღნიშნავს რომ, „პირადი ცხოვრება“ არის ფართო ტერმინი, რომლის ამომწურავი განმარტება არ არსებობს, ასევე შესაძლებელია „პირადი ცხოვრების“ ფართო განმარტება, როგორიც არის ინდივიდის მიერ საკუთარი პიროვნული იდენტურობის განვითარების შესაძლებლობა, ასევე „პირადი ცხოვრება“ შესაძლოა დაკავშირებული იყოს, როგორც პროფესიულ საქმიანობასთან, ასევე საზოგადოებაში მიმდინარე ნებისმიერ ღონისძიებასთან [10] , მათ შორის სამსახურებრივ ურთიერთობასაც [11] . პერსონალური მონაცემების დაცვაში საბოლოოდ პრიორიტეტი ენიჭება არა მგრძნობიარობის, არამედ იდენთიფიკაციის კრიტერიუმს[12]. კანონმდებლობის მიზანი სწორედ ის არის, რომ მონაცემთა დამუშავებისას უზრუნველყოფილ იქნეს ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის დაცვა[13].

ამდენად, ნათელია, რომ პერსონალურ მონაცემთა დაცვა აქცენტს აკეთებს

---

[10] ადამიანის უფლებათა ევროპული სასამართლოს ადამიანის უფლებათა ევროპული 2017 წლის 5 სექტემბრის გადაწყვეტილება საქმეზე Barbulescu v. Romania, პარაგრაფი N:70-71.

[11] პირადი და ოჯახური ცხოვრების პატივისცემის უფლება და სახელმწიფოს ვალდებულებები, ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკისა და საქართველოს საკონსტიტუციო სასამართლოს პრაქტიკის მიმოხილვა., ოქტომბერი, 2017, 48, იხ. ციტირება ნიმიტცი გერმანიის წინააღმდეგ (Niemietz v. Germany) , 16 დეკემბერი, 1992, § 29, Series A no. 251-B-ე პარაგრაფი ; ჰალფორდი გაერთიანებული სამეფოს წ ინააღმდეგ (Halford v. the United Kingdom) , 25 ივნისი, 1997, § 42-46, Reports of Judgments and Decisions 1997-III.

[12] თბილისის სააპელაციო სასამართლოს ადმინისტრაციულ საქმეთა პალატის 2016 წლის 26 აპრილის გადაწყვეტილება N3ბ/1059-15.

[13] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მუხლი 1.

პერსონალური ინფორმაციის კანონიერი ცირკულაციაზე.

1.1 მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის ევოლუცია

აუცილებელია აღინიშნოს, რომ პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობა საზოგადოებრივი ურთიერთობების განვითარებასთან ერთად განვითარდა, რიგი განმაპირობებელი ერთ-ერთი ფაქტორი ტექნოლოგიური პროგრესი იყო. „პერსონალურ მონაცემთა დაცვასთან დაკავშირებით პირველი კანონი ამოქმედდა ჰესეში, გერმანიაში, ამ პროცესს მოჰყვა კანონის ამოქმედება შვედეთში 1973 წელს, ამერიკის შეერთებულ შტატებში 1974 წელს, გერმანიაში 1977 წელს, საფრანგეთსა და ნორვეგიაში 1978 წელს[14]“.

1960-იან წლებში ინფორმაციული ტექნოლოგიების გამოჩენასთან ერთად, გაიზარდა მოთხოვნა პერსონალურ მონაცემთა დაცვის დეტალური წესების შემუშავებაზე[15], ხოლო 1981 წელს კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ (108-ე კონვენცია) გაიხსნა ხელმოსაწერად [16] . კონვენცია რატიფიცირებულია ევროკავშირის ყველა წევრი სახელმწიფოს მიერ[18], ხოლო საქართველოს პარლამენტის მიერ მისი რატიფიცირება მოხდა 2015 წლის 28 ოქტომბრის N 2010 – IIს დადგენილებით, რომელიც ძალაშია 2006 წლის 1 აპრილიდან[17]. საქართველოს პარლამენტის მხრიდან კონვენციის რატიფიცირებას უდიდესი მნიშვნელობა ენიჭება, რადგან ის ასახავს იმ საერთაშორისო

---

[14] წერეთელი მ., პერსონალურ მონაცმეების დაცვის სამართლებრივი მნიშვნელობა და დაცვის სტანდარტები ბიზნეს ურთიერთობებში,თბილისი, 2019, 8, იხ. ციტირება „ადამიანის უფლებათა დაცვის ეროვნული და საერთაშორისო მექანიზმები (სტატიათა კრებული)“, ქალდანი თ., სარიშვილი ნ., 2016 წელი“

[15] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი 2018, 29.

[16] იქვე. გვ 29, იხ. ციტირება ევროპის საბჭო, კონვენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ CETS No. 108, 1981. [18] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი 2018, 30.

[17] იხ. კონვენცია “პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“.

სტანდარტებს და რეგულაციებს, რომელიც აუცილებლად შესასრულებელია მონაცემთა დამმუშავებლის მხრიდან. „კონვენცია ვრცელდება ყველა სახის მონაცემთა დამუშავებაზე, განხორციელებული როგორც კერძო, ასევე საჯარო სექტორის მიერ“ [18]. კონვენცია უზრუნველყოფს პერსონალური მონაცემების დამუშავებისას უსაფრთხოების გარანტიების შექმნას, იცავს დამუშავების სუბიექტის უფლებებს მონაცემთა შეგროვების და დამუშავების ეტაპზე, განსაზღვრავს სუბიექტის უფლებას ინფორმაციის მიღებაზე, ასევე ითვალისწინებს მონაცემთა ტრანსასაზღვრო გადაცემის შესაძლებლობას, და ასევე განამტკიცებს პერსონალურ მონაცემთა დამუშავების ძირითად პრინციპებს, ადგენს განსაკუთრებული კატეგორიის მონაცემების დამუშავების დაუშვებლობას სუბიექტის თანხმობის გარეშე.

2018 წლის 17-18 მაისს მოხდა კონვენციის მოდერნიზება[19], იგი ადგენს ახალ უფლებებს, და განამტკიცებს ძირითად პრინციპებს, ასევე მოდერნიზებული კონვენცია ითვალისწინებს საზედამხედველო ორგანოების დამოუკიდებლობის გარანტიებს, უფლებამოსილებათა განხორციელების დროს, იცავს დამუშავების სუბიექტის უფლებებს, მისი მოსაზრებების გათვალისწინების გზით. ასევე კონვენცია ზრდის დამმუშავებლის პასუხისმგებლობის და ანგარიშვალდებულობის გარანტიებს, მონაცემთა დამუშავებისას. ახალი დებულებები მოიცავს ზოგად, მარტივ და ლაკონურ პრინციპებს[20].

პირველად პერსონალური მონაცემების დაცვის უფლება დამოუკიდებელი სახით გაიწერა 2000 წელს, ევროკავშირის ფუნდამენტური უფლებების ქარტიის მე-8 მუხლით[23]. თანდათან ჩამოყალიბდა მოსაზრება, რომ არსებობდა ორი ცალკეული ცნება, ერთის მხრივ

---

[18] გლიგალიშვილი ნ., კუტალაძე მ., ევროკავშირის მიდგომა პერსონალური მონაცემების დაცვის სამართლებრივი რეგულირების საკითხისადმი, გამომცემლობა უნივერსალი., თბილისი 2018, 70.

[19] იხ. Modernised Convention For the Protection of Individuals with Regard to the Processinf of Personal Data, Consolidated text, 2018.

[20] იხ. < https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet> 20.05.2020.

[23] იხ. González Fuster G., The Emergence of Personal Data Protection as a Fundamental Right of the EU, London, 2014, 206.

კონფიდენციალურობა, სხვა სიტყვებით, პირადი ცხოვრებისადმი პატივისცემა, და მეორეს მხრივ პერსონალური მონაცემების დაცვა, რომელსაც ხშირად „მონაცემთა დაცვას“ უწოდებდნენ[21].

საქართველოში „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მიღებამდე, 2011 წლამდე, პერსონალური მონაცემების ცნება ზოგადი ადმინისტრაციული კოდექსით იყო მოწესრიგებული. კოდექსის (სსმ, 32(39) 15/07/1999 წლის რედაცია) 27-ე მუხლის „თ“ ნაწილის მიხედვით პერსონალური მონაცემი შემდეგი სახით იყო განმარტებული: „პერსონალური მონაცემები - საჯარო ინფორმაცია, რომელიც პირის იდენტიფიკაციის შესაძლებლობას იძლევა“[22]. ამრიგად ორ მნიშვნელოვან ტერმინს გამოკვეთდა კოდექსი, ეს იყო „საჯარო ინფორმაცია“ და „პირის იდენტიფიკაცია.“ კოდექსი ხაზს უსვამდა, რომ პერსონალური მონაცემები უნდა ყოფილიყო საჯარო და ამასთანავე საჯარო ინფორმაციის საფუძველზე უნდა მომხდარიყო პირის იდენტიფიკაცია.

დღეს პერსონალური მონაცემების დაცვის საკითხები საქართველოში საკანონმდებლო დონეზეა აყვანილი, 2011 წლის 28 დეკემბერს საქართველოს პარლამენტმა მიიღო კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, რომელიც დეტალურად განიხილავს პერსონალურ მონაცემების დაცვასთან დაკავშირებულ საკითხებს. 2013 წელს შეიქმნა პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი[23], ხოლო ევროპულ კავშირთან ასოცირების შეთანხმებას საქართველომ ხელი მოაწერა 2014 წლის 27 ივნისს, რომლის შემდეგ აუცილებელი გახდა ქმედითი

[21] იხ. იქვე 214.

[22] საქართველოს ზოგადი ადმინისტრაციული კოდექსის სსმ, 32 (39) 15/07/1999 წლის რედაქცია, მუხლი 27, „თ“ ნაწილი.

[23] იხ. საქართველოს მთავრობის დადგენილება N180 პერსონალურ მონაცემთა დაცვის ინსპექტორის საქმიანობისა და მის მიერ უფლებამოსილების განხორციელების წესის შესახებ დებულების დამტკიცების შესახებ, 2013, საქართველოს საკანონმდებლო მაცნე 19/07/2013, (ძალადაკარგულია 20/11/2019).

ღონისძიებების გატარება საქართველოს მხრიდან, და რა თქმა უნდა საკითხი პერსონალური მონაცემების დაცვასაც შეეხო[24].

საქართველოსა და ევროპულ კავშირს შორის ასოცირების ხელშეკრულების ხელმოწერის შემდეგ საქართველოში ქმედითი ღონისძიებების გატარება დაიგეგმა, რათა უკეთესად განხორციელებულიყო ევრორეგულაციებით გათვალისიწნებული წესები. ამის ერთ-ერთი შედეგია, სახელმწიფო ინსპექტორის სამსახურის ამოქმედება, რომელიც, აქამდე არსებული, პერსონალურ მონაცემთა დაცვის ინსპექტორის სამსახურის უფლებამონაცვლეს წარმოადგენს. აპარატის მოქმედების არეალი გაიზარდა (სახელმწიფო ინსპექტორის აპარატს დაემატა საგამოძიებო უფლებამოსილება) და ცალკე კანონით დარეგულირდა მისი უფლებამოსილებები[28]. ასევე აუცილებელი გახდა, რომ საკანონმდებლო ცვლილებებიც განხორციელებულიყო „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში, სწორედ ამიტომ საქართველოს პარლამენტში წარდგენილია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი, რომელზე მუშაობაც მიმდინარეობს, და რომელიც ასოცირების ხელშეკრულებით გათვალისწინებული მოთხოვნებს ითვალისწინებს. კანონის პროექტის დადებითი მხარე არის აგრეთვე ისიც, რომ დღეს მოქმედი კანონის მოქმედების სფერო გაფართოვდა, და იგი გავრცელდება არამარტო საჯარო სფეროზე, არამედ კერძო სფეროზეც, რადგან პერსონალური მონაცემების უდიდესი ნაწილი სწორედ კერძო სექტორის მიერ მუშავდება. ამას მოწმობს სტატისტიკური მონაცემებიც, რომლებიც მოცემულია ინსპექტორის ანგარიშებში[29].

დამატებით აღსანიშნავია, რომ 2018 წლის 25 მაისს ძალაში შევიდა ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაცია (General Data Protection Regulation), რომელიც მორგებულია თანამედროვეობას, რადგან თანამედროვე ტექნოლოგიების და ინტერნეტსივრცის განვითარებასთან ერთად აუცილებელი იყო დამატებით ისეთი რეგულაციების გატარება,

[24] წერეთელი მ., პერსონალურ მონაცმეების დაცვის სამართლებრივი მნიშვნელობა და დაცვის სტანდარტები ბიზნეს ურთიერთობებში,თბილისი, 2019, 8, იხ. ციტირება Karanja S.,

Transparency and Proportionality in the Schengen Information System and Border Control Cooperation, Netherlands, Martinus Nijhoff Publishers, 2008. გვ. 123.

[28] იხ. საქართველოს კანონი „სახელმწიფო ინსპექტორის შესახებ“ 2018.

[29] იხ. საქართველოს პერსონალურ მონაცემთა დაცვის ისნპექტორის ანგარიშები პეროსნალურ მონაცემთა დაცვის მდგომარეობა საქართველოში, თბილისი, 2013-2018.

რომელიც უზრუნველყოფდა პერსონალური მონაცემების უსაფრთხოდ დამუშავებას. აღნიშნული რეგულაციის ამოქმედებამდე, ევროპულ კავშირში მონაცემთა დაცვის საკითხები, ძირითადად, წესრიგდებოდა 1995 წლის დირექტივით 95/46/EC[25], რომელიც თითქმის 23 წელი მოქმედებდა.

დამატებით, ხაზგასასმელია თუ რა ძირითად საკითხებს ეხება, როგორც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, ისე საერთაშორისოდ აღიარებული სამართლებრივი აქტები, ესენია:

1. სფეროსთვის დამახასიათებელი ტერმინოლოგია და ცნებათა განმარტება;
2. სამართლებრივი აქტის მოქმედების ფარგლები;
3. მონაცემთა დაცვის პრინციპები და საფუძვლები, როგორც დამუშავების ზოგადი შემთხვევებისთვის, ისე სპეციალური წესები, დაკავშირებული, მაგალითად, ვიდეოკონტროლთან და პირდაპირ მარკეტინგთან;
4. მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ვალდებულებები მონაცემთა დამუშავებისას;
5. მონაცემთა სუბიექტის უფლებები და მათი შეზღუდვის ფარგლები;
6. მონაცემთა დაცვის საზედამხედველო სახელმწიფო ორგანო და მისი უფლებამოსილებები;
7. მონაცემთა დაცვის წესებთან დაკავშირებული დარღვევებისთვის გათვალისწინებული სანქციები.

[25] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი 2018, 34.

1.2 პერსონალურ მონაცემთა დამუშავების პრინციპების დანიშნულება და მიმართება დამუშავების წესებთან

„პერსონალური მონაცემების დამუშავების კანონიერება და მაღალ სტანდარტებთან შესაბამისობა არსებითადაა დამოკიდებული მონაცემთა დამუშავების პრინციპების დაცვაზე“[26]. მონაცემთა დამუშავების პრინციპები არის ის სახელმძღვანელო დებულებები, რომლის გამოყენება და დაცვა სავალდებულოა პერსონალურ მონაცემთა დამმუშავებლისათვის. მონაცემთა დამუშავების პრინციპებს გააჩნია კუმულაციური ხასიათი, რაც გულისხმობს, რომ მონაცემების დამუშავება მხოლოდ მაშინ მოექცევა კანონის მოქმედების სფეროში თუ ყველა პრინიციპის დაცვით დამუშავდება ისინი. დამატებით, აუცილებელია, როგორც კანონით გათვალისწინებული პრინციპების დაცვა, ასევე მონაცემთა დამუშავებისათვის შესაბამისი კანონიერი საფუძვლის არსებობა[27][28]. მონაცემთა დამუშავების პრინციპები არის შეზღუდვის ერთ-ერთი საშუალება, რომელიც მაქსიმალურად ბოჭავს მონაცემთა დამმუშავებელს, რათა მან რომელიმე პრინციპის გვერდის ავლით არ დაამუავოს მონაცემები. მონაცემთა დამუშავების პრინციპები თავისი ბუნებით აღმატებულია დამუშავების საფუძვლებზე, ეს ნიშნავს, რომ თუ მხარეებმა გაითვალისწინეს რაიმე და შეთანხმდნენ პირობაზე, რომელზეც თუნდაც ორივე მხარე თანახმაა, რომელიმე პრინციპთან წინააღმდეგობის შემთხვევაში, დამუშავების კანონიერება სადავო გახდება მონაცემთა დაცვის პერსპექტივიდან გამომდინარე.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ითვალისწინებს ხუთ პრინციპს, ესენია:

1. სამართლიანობა, კანონიერება და ღირსების დაცვა;
2. მიზნის შესაბამისი დამუშავება;

---

[26] პერსონალურ მონაცემთა დაცვის ისპექტორის ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში, თბილისი, 2013, 4.

[27] იხ.პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის ანგარიში „პერსონალურ მონაცემთა დაცვის მდგომარეობისა და ისნპექტორის საქმიანობის შესახებ“,თბილისი, 2016,

[28] .

3. პროპორციულობის;

4. მონაცემთა დამუშავების სისწორე/სიზუსტე;

5. შენახვის ვადის ლიმიტირება.[29]

აღნიშნულ ხუთ პრინციპს GDPR[30] უმატებს კიდევ ორ პრინციპს, კერძოდ, მონაცემთა უსაფრთხო დამუშავებისა და სუბიექტის წინაშე გამჭვირვალობის პრინციპებს[31]. მონაცემთა დამუშავების საფუძვლებთან ურთიერთმიმართების განმარტებისთვის, აუცილებელია თითოეული პრინციპის მოკლე აღწერა.

1. სამართლიანობის, კანონიერებისა და ღირსების დაცვის პრინციპი. მონაცემთა დამუშავება უნდა მოხდეს, როგორც კანონის სრული დაცვით, ასევე სამართლიანადაც, რათა მონაცემთა დამუშავებით სუბიექტს ღირსება არ შეელახოს[32]. „პერსონალური მონაცემები, რომლებიც ექვემდებარებიან ავტომატიზირებულ დამუშავებას, მიღებული და დამუშავებულ უნდა იყოს პირდაპირი და კნანონიერი გზით“ [33]. მონაცემთა დამუშავების სუბიექტისათვის ცნობილი უნდა იყოს, თუ რომელი მონაცემი გროვდება და მუშავდება, და შეგროვებული მონაცემებიდან რომელი მონაცემი არის გამოყენებადი.

სამართლიანობის პრონციპი გულისხმობს იმას, რომ თუ ერთი და იგივე სამართლებრივ მდგომარებაში არის რამოდენიმე პირი, რომელთა შესახებაც მუშავდება მონაცემები, ეს უნდა განხორციელდეს ერთი და იგივე საშუალებებით, ანუ ყველა სუბიექტის მიმართ გამოყენებულ უნდა იქნეს თანაბარი და სამართლიანი მიდგომა[34]. ამრიგად, სამართლიანობის და

[29] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მუხლი 4.

[30] General Data Protection Regulation - მონაცემთა დაცვის ძირითადი რეგულაცია.

[31] Guide to the General Data Protection Regulation (GDPR), Ico, 2019, 17.

[32] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მუხლი 4, ა ქვეპუნტი.

[33] კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“; ძალაშია 2006 წლის 1 აპრილიდან, მუხლი 5, ა ქვეპუნქტი.

[34] იხ. საქართველოს პერსონალურ მონაცემთა დაცვის ინპექტორის აპარატი, „რეკომედაციები შრომით ურთიერთობებში პერსონალური მონაცემების დაცვის შესახებ“, თბილისი, 2014, 2.

კანონიერების პრინციპში არ უნდა იგულისხმებოდეს მხოლოდ სუბიექტის ინფორმირებულობის საკითხის უპირატესობა მის შესახებ მონაცემთა დამუშავებაზე, სამართლიანობა და კანონიერება აქცენტს აკეთებს, იმაზე რომ პირის პერსონალური მონაცემები დამუშავდეს კანონის ფარგლებში, ანუ დამმუშავებელს ჰქონდეს ვალდებულება კანონის შესაბამისად დაამუშავოს ესა თუ ის მონაცემი (ნებისმიერ ეტაპზე უნდა მოხდეს სუბიექტის ინფორმირება, თუ რომელი მონაცემი მუშავდება და რისთვის, რა სახის მონაცემი მუშავდება, როგორ უნდა მოხდეს შემდეგ ამ მონაცემების გამოყენება და რომელი მონაცემი ექვემდებარება გამოყენებას, ხომ არ უნდა მოხდეს დამუშავებული მონაცემების მესამე პირებზე გადაცემა და ა.შ). აღნიშნული პრინციპის მიხედვით დამმუშავებელმა ისე უნდა დაამუშავოს მონაცემები, რომ დაცულ იქნეს დამუშავების სუბიექტებს შორის სამართლიანი ბალანსი, და გამოირიცხოს რომელიმე პირის მიმართ დისკრიმინაცია, და ღირსების შელახვა. „[...] ადამიანის ღირსება ყველა სხვა ძირითადი უფლების საფუძვლადაა მიჩნეული“[35]. დამმუშავებლები უნდა დარწმუნდნენ, რომ მათ მიერ მონაცემების შეგროვების და დამუშავების პრაქტიკა არ არღვევს კანონს და რომ ისინი ცნობილია დამუშავების სუბიექტისათვის[36].

2. მიზნობრიობის (მიზნის შესაბამისობისობის) პრინციპი - პერსონალური მონაცემები, რომლებიც მუშავდება მონაცემთა დამმუშავებლის მიერ შენახულ და დამუშავებულ უნდა იქნეს ზუსტად განსაზღვრული კანონიერი მიზნებისათვის და არ უნდა იყოს გამოყენებული მათთან შეუთავსებელი გზით. სწორედ ეს არის საფუძველი, დამმუშავებელმა მიიღოს ის შედეგი, რომელიც თავდაპირველად ჰქონდა განსაზღვრული. „პერსონალური მონაცემები უნდა დამუშავდეს კანონიერი

[35] გაგნიძე ე., საიქოძე ნ., პერსონალურ მონაცემთა დაცვასთან დაკავშირებული კერძო და საჯარო ინტერესის თანაფარდობა და უფლებაში ჩარევის საფუძვლიანობის კრიტერიუმები, სტუდენტური სამართლებრივი ჟურნალი, თბილისი, 2016, 66.

[36] <https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles> 02/03/2020.

და მკაფიოდ განსაზღვრული მიზნით, მონაცემთა დამუშავება თავად არ წარმოადგენს მიზანს, ისევე როგორც მიზანი არ შეიძლება იყოს აბსტრაქტული და ზოგადი ხასიათის, მიზანი უნდა იყოს კონკრეტული, მკაფიო და მარტივად გასაგები[37]. შესაბამისად, კონკრეტული მიზნები, რომლისთვისაც ხდება მონაცემთა დამუშავება უნდა იყოს მკაფიო და ლეგიტიმური, სწორედ ამიტომ ეს უნდა განისაზღვროს პერსონალურ მონაცემთა შეგროვების ეტაპზე. მონაცემთა მიზნობრიობის პრინციპი თავის მხრივ დაკავშირებულია მონაცემთა მინიმიზაციის პრინციპთან, რომელიც გულისხმობს მონაცემების დამუშავებას მინიმუმამდე დაყვანის გზით, ანუ მხოლოდ ის მონაცემები, რომელიც არის რელევანტური და დამუშავების მიზნების მიღწევისთვის საჭირო. „ამ პრინციპის თანახმად პერსონალური მონაცემები უნდა იყოს ადეკვატური, შესაბამისი და შემოიფარგლოს მხოლოდ დაზუსტებული, მკაფიო და ლეგიტიმური მიზნებისათვის“[42].

3. პროპორციულობის პრინციპი - მონაცემები, რომელიც მუშავდება უნდა იყოს იმ თავდაპირველი მიზნის შესაბამისი და პროპოციული, და უნდა დამუშავდეს მხოლოდ ის მონაცემი, რომელიც მიზნის მიღწევას შეუწყოფს ხელს[38]. მონაცემები უნდა დამუშავდეს იმ მოცულობით, რომელიც აუცილებელია კანონიერი მიზნის მისაღწევად, და ამასთანავე არ უნდა აღემატებოდეს თავდაპირველ მიზანს, უნდა იყოს ადეკვატური და პროპორციული. მონაცემები, რომელიც მუშავდება უნდა იყოს ადეკვატური, რელევანტური, და არა გადაჭარბებული იმ მიზნისთვის რისთვისაც ისინი ინახება[44].

---

[37] საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, „რეკომედაციები შრომით ურთიერთობებში პერსონალური მონაცემების დაცვის შესახებ“, თბილისი, 2014, 6.

[42] <https://www.futurelearn.com/courses/general-data-protection-regulation/0/steps/32412> 02/03/2020.

[38] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მუხლი 4, გ ქვეპუნქტი.

[44] Convention to the Protection Individual with regard to Aotomatic Processing of Personal Data., Strasburg.28.I.1981, Article 5/ c.

4. სიზუსტის პრინციპი - „მონაცემთა სიზუსტის უზრუნველყოფა უნდა აღვიქვათ მონაცემთა დამუშავების მიზნის კონტექსტში“[39]. ანუ ისეთი მონაცემი, რომელიც მიზნის შეუსაბამოდ იქნა დამუშავებული უნდა დაიბლოკოს, ან წაიშალოს, და ასევე საჭიროების შემთხვევაში უნდა განახლდეს. სწორედ აღნიშნულს მოიცავს პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი. ავტომატური დამუშავებისას პერსონალური მონაცემები უნდა იყოს ზუსტი და საჭიროების შემთხვევაში განახლებული[40].

5. შენახვის ვადის შეზღუდვის პრინციპი - „მონაცემები შესაძლოა შენახულ იქნეს, მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად. ამ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა დაიბლოკოს, წაიშალოს ან გადანდურდეს ან შენახულ უნდა იქნეს პირის იდენტიფიცირების გამომრიცხავი ფორმით“[41]. შესაბამისად, პერსონალური მონაცემები უნდა ინახებოდეს მხოლოდ იმ ფორმაში, რომელიც დამმუშავებელს საშუალებას მისცემს მონაცემთა სუბიექტის იდენტიფიცირების საშუალებას იქამდე, სანამ ამის საჭიროება იარსებებს. პერსონალური მონაცემების შენახვა უშუალო გავლენას ახდენს დაინტერესებული ინდივიდის პირადი ცხოვრების ინტერესზე, მიუხედავად იმისა შემდგომ გამოყენებულია თუ არა ეს მონაცემები[48]. ამიტომ დამმუშავებლის მიერ უნდა განისაზღვროს მონაცემთა შენახვის გარკვეული ვადა, რომლის გასვლის შემდეგ დამუშავებული მონაცემი უნდა განადგურდეს, დაიბლოკოს, წაიშალოს.

---

[39] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი, 2018, 145.

[40] Convention to the Protection Individual with regard to Aotomatic Processing of Personal Data., Strasburg.28.I.1981, Article 5/d.

[41] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მუხლი 4, ე ქვპუნქტი.

[48] ადამიანის უფლებათა ევროპული სასამართლოს 2008 წლის 4 დეკემბერი გადაწყვეტილება საქმეზე S. And Marper v. The United Kingdom, პარაგრაფი 121.

6. უსაფრთხოების პრინციპი - „პერსონალური მონაცემების უსაფრთხოებასა და კონფიდენციალობას უდიდესი მნიშვნელობა ენიჭება მონაცემთა სუბიექტებზე უარყოფითი გავლენისაგან თავიდან ასაცილებლად“ [42] . „მონაცემთა უსაფრთხოების პრინციპი მოითხოვს სათანადო ტექნიკური ან ორგანიზაციული ღონისძიებების გატარებას პერსონალური მონაცემების დამუშავების პროცესში“ [43] . მონაცემთა უსაფრთხოების ასეთი ზომები შეიძლება მოიცავდეს დაშიფვრის, ავთენტიფიკაციის და ავტორიზაციის მექანიზმების გამოყენებას [44] . უსაფრთხოების პრინციპის განხორციელება უმნიშვნელოვანესია, ვინაიდან მისი სწორად და კანონის შესაბამისად გამოყენება არის გარანტია როგორც დამმუშავებლის ასევე დამუშავების სუბიექტისათვის, რათა არ დაირღვეს მათი უფლებები.

უსაფთხოების პრინციპი დამმუშავებელს აარიდებს ზარალს მონაცემთა არასანქცირებული წვდომის შეცვლისა და გავრცელებისათვის.[45]

7. გამჭირვალობის პრინციპი - ევრორეგულაციის მიხედვით, აუცილებელია განისაზღვროს პასუხისმგებელი პირი, მონაცემთა უკანონო დამუშავების თავიდან ასაცილებლად. სწორედ ამიტომ რეგულაციას შემოაქვს ეს პრინციპი, რათა დარღვევის შემთხვევაში განსაზღვრული იყოს თუ ვის დაეკისრება შესაბამისი პასუხისმგებლობა. პასუხისმგებლობის განსაზღვრა ძალიან მნიშვნელოვანია, რადგან დამმუშავებელი მეტი ყურადღებით მოეკიდება მონაცემთა დამუშავებას. დამმუშავებელი პასუხისმგებელია და უნდა აჩვენოს მათი შესაბამისობა მონაცემთა დაცვის ყველა ზემოთ ჩამოთვლილ პრინციპთან, მან პასუხისმგებლობა უნდა აიღოს პერსონალური მონაცემების დამუშავებაზე, და იმაზე, თუ როგორ

[42] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი, 2018, 148.
[43] იხ. იქვე გვ. 149.
[44] <https://www.futurelearn.com/courses/general-data-protection-regulation/0/steps/32412> 02/03/2020.
[45] იხ. Convention to the Protection Individual with regard to Aotomatic Processing of Personal Data., Strasburg.28.I.1981, Article 7.

შეესაბამება ისინი GDPR-ს და მათ შეეძლებათ აჩვენონ (შესაბამისი ჩანაწერებითა და ზომებით) მათი შესაბამისობა[46]. ეს პრინციპი თავისი შინაარსით დაკავშირებულია, როგორც ანგარიშვალდებულების, ასევე, სამართლიანობის და კანონიერების პრინციპთან, რადგან ამ პრინციპის ძირითადი არსი არის ის, რომ მონაცემთა დამუშავების სუბიექტის ინფორმირებული იყოს მის შესახებ ნებისმიერი მონაცემის დამუშავების თაობაზე, და მისი მხრიდან მონაცემთა დამმუშავებელს ჰქონდეს მიღებული თანხმობა, წინააღმდეგ შემთხვევაში დამუშავება არ იქნება კანონიერი. დამმუშავებელი უნდა დარწმუნდეს, რომ მისი მუშაობის პრაქტიკა არ დაარღვევს არც კანონს, და არც სუბიექტის უფლებებს.

ისე არ უნდა იქნას გაგებული თითქოს პერსონალურ მონაცემთა დამუშავების პრინციპების არსებობა არის ერთადერთი წინაპირობა იმისა, რომ დამმუშავებელმა შეძლოს მონაცემთა დამუშავება. აუცილებელია, რომ პრინციპებთან ერთად დაცულ იქნეს დამუშავების წესებიც (საფუძვლები). მონაცემთა დამუშავებისთვის პრინციპებთან ერთად აუცილებელია მონაცემთა დამუშავების სუბიექტის თანხმობა ან თანხმობის ალტერნატივა[54]. აშკარა თანხმობა ნიშნავს წერილობით თანხმობას, თუ არ არსებობს წერილობითი თანხმობა, ეს უნდა იყოს გამართლებული (მაგ: არსებობს გარემოებები, როდესაც წერილობითი თანხმობა არ იქნება საკმარისი და მიზანშეწონილი, რადგან მუშაკი შესაძლოა იყოს განათლების არმქონე, ან არ ესმოდეს მოცემული ენა, ამ შემთხვევაში ინფორმაციის მიღება და თანხმობა შეიძლება საჭირო იყოს სიტყვიერად[47]). პერსონალური მონაცემების დამუშავება განსაკუთრებით მნიშვნელოვანია სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას[48]. საქართველოს კანონმდებლობა, ისევე როგორც GDPR ითვალისწინებს მონაცემთა

---

[46] <https://www.dataprotection.ie/en/individuals/principles-data-protection> 02,03.2020. ასევე <https://www.nibusinessinfo.co.uk/content/data-protection-principles-under-gdpr> 02/03/2020 [54] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მუხლი 5.

[47] Protection of worker's personal data, Internation Labour Office Geneva; ILO; 11

[48] არჩუაძე თ., პერსონალურ მონაცემთა დაცვის გარანტიები მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 2016, 6.

სუბიექტის თანხმობის ალტერნატივას. თანხმობა საჭირო არაა: ა) თუ დამუშავება გათვალისწინებულია კანონით; ბ) დამუშავება აუცილებელია დამმუშავებლის მიერ კანონმდებლობით გათალისწინებული ვალდებულებების შესასრულებლად; გ) დამუშავება აუცილებელია დამუშავების სუბიექტის სასიცოცხლო ინტერესების დასაცავად; დ) დამუშავება აუცილებელია მონაცემთა დამმუშავებლის ან მესამე პირის, კანონიერი ინტერესის დასაცავად, თუ არ არსებობს მონაცემთა სუბიექტის აღმატებული ინტერესი; ე) მონაცემები საჯაროდ ხელმისაწვდომია, ან საჯაროდ ხელმისაწვდომი გახადა სუბიექტმა; ვ) დამუშავება აუცილებელია მნიშვნელოვანი საჯარო ინტერესის დასაცავად; ზ) აუცილებელია დამუშავების სუბიექტის განცხადების განსახილველად (მომსახურების გასაწევად) [49] . მონაცემთა დამუშავებისას დამმუშავებლის მიერ უნდა იდენტიფიცირდეს შეგროვებული ინფორმაცია, კერძოდ, ხომ არ არის ის განსაკუთრებულად მგრძნობიარე, სენსიტიური მონაცემები, რადგან კანონი განსაკუთრებული მონაცემების დამუშავებისათვის განსხვავებული მიდგომაა ჩამოყალიბებული. სენსიტიური მონაცმეები განსაკუთრებულად დაცვის ქვეშ მყოფია და მისი დამუშავებისთვის, მაგალითად, აუცილებელია სუბიექტის წერილობითი თანხმობა[50].

შრომითი ურთიერთობებისათვის დამახასიათებელია განსაკუთრებული კატეგორიის მონაცემების დამუშავება, რაც გულისხმობს ნასამართლეობის, ნარკოლოგიური და ჯანმრთელობის ცნობის საფუძველზე მონაცემების დამუშავებას, შესაბამისად დამმუშავებელმა უნდა მიიღოს საკმარისი უსაფრთხოების ზომები, რათა განსაკუთრებული კატეგორიის მონაცემი არ დამუშავდეს სუბიექტის თანხმობის გარეშე. ადამიანის უფლებათა ევროპული სასამართლო მის ერთ-ერთ გადაწყვეტილებაში მიიჩნევს, რომ საკმარისი გარანტიები არ იყო შემქნილი მონაცემთა და პირადი ცხოვრების დასაცავად, ვინაიდან განსაკუთრებული კატეგორიის მონაცემის

[49] იხ. პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მუხლი 5, პუნქტი ბთ.
[50] არჩუაძე თ., პერსონალურ მონაცემთა დაცვის გარანტიები მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 2016, 12.

გამჟღავნებამ ხელი შეუშალა დასაქმების პროცესს, ვინაიდან მიუხედავად იმისა რომ მონაცემები უნდა შენახული მხოლოდ 5 წლის განმავლობაში, არ წაშლილა 5 წლის გასვლის შემდეგაც[51]. ამასთან, პერსონალურ მონაცემთა დაცვის ინსექტორმა სამართლადარმღვევად ცნო სამედიცინო ცენტრი, რომელმაც გასცა ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია მესამე პირზე[52]. იმ შემთხვევაშიც კი, როდესაც სახეზეა განსაკუთრებული კატეგორიის მონაცემთა დამუშავების სამართლებრივი საფუძველი, მონაცემთა სუბიექტის თანხმობის გარეშე დაუშვებელია მონაცემთა გასაჯაროება და მესამე პირისათვის გამჟღავნება [53] . საქართველოს სახელმწიფო ინსპექტორმა სამართალდამრღვევად ცნო კომპანია, რომელმაც მუდმივი მომხმარებლის ფოტოსურათები სუბიექტის თანხმობის გარეშე განათავსა Facebook-ზე, კომპანიამ ვერ დაასაბუთა როგორ მიიღწეოდა საფუძლის გარეშე საქმიანი რეპუტაციის დაცვის მიზანი, რაც კომპანიის მთავარი არგუმენტი იყო[54]. ევროკავშირის სამართალში, თანხმობა როგორც მონაცემთა დამუშავების საფუძველი, მკაცრად არის დადგენილი GDPR-ის მე-6 მუხლით[55]. მონაცემთა კანონიერად დამუშავება კომპლექსური თემაა და ხშირად ინდივიდუალურ მიდგომას და სამართლებრივ მსჯელობას მოითხოვს, თუმცა არსებობს ორი ძირითადი პირობა, რომელიც მონაცემთა კანონიერად დამუშავებისათვის ნებისმიერ შემთხვევაში აუცილებელია, ესენია, სამართლებრივი საფუძვლის არსებობა და კანონით დადგენილი

[51] იხ. ადამიანის უფლებათა ევროპული სასამართლოს 2012 წლის 13 ნოემბრის გადაწყვეტილება საქმეზე M.m v. The United Kingdom, პარაგრაფი 149, ასევე პარაგრაფი 207.
[52] საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 30 ივნისის გადაწყვეტილება, ი.ნ-ს განცხადებასთან დაკავშირებით განხილვის დასრულების შესახებ, საქმე N:გ-1/329/2017, 1.
[53] იქვე, გვ 6.
[54] საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 11 მაისის გადაწყვეტილება შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-1/262/2017, 2-4.
[55] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი 2018, 162.

პრინციპების დაცვა[56]. ასევე, იმისათვის, რათა მონაცემთა დამუშავებისას კანონი არ დაირღვეს უნდა არსებობდეს ერთი სამართლებრივი საფუძველი მაინც[57].

2. მონაცემთა დამუშავების პრინციპების მოქმედება მიმდინარე შრომით ურთიერთობებში

„მიუხედავად შრომის ხელშეკრულების მრავალი თავისებურებებისა, ის იურიდიული გაგებით, მაინც, კერძო სამართლებრივ ხელშეკრულებადაა მიჩნეული კონტინენტური ევროპის სამართალში“ [58], ხოლო კერძოსამართლებრივი ურიერთობებისათვის განსაზღვრულია ხელშეკრულების თავისუფლების პრინციპი. „კერძო სამართლის სუბიექტებს შეუძლიათ კანონის ფარგლებში თავისუფლად დადონ ხელშეკრულებები და განსაზღვრონ ამ ხელშეკრულებათა შინაარსი, მათ შეუძლიათ დადონ ისეთი ხელშეკრულებებიც, რომელიც კანონით გათვალისწინებული არ არის, მაგრამ არ ეწინააღმდეგება მას[59]“.

დასაქმებულთა პერსონალური მონაცემების დაცვის პრაქტიკის კოდექსში, რომელიც შრომის საერთაშორისო ორგანიზაციამ მიიღო, განისაზღვრა შრომის სამართალში არსებული ძირითადი ტერმინების დეფინიცია, რომლის მიხედვითაც „პერსონალური მონაცემი“ ნიშნავს, ნებისმიერ ინფორმაციას, რომელიც უკავშრდება, იდენთიფიცირებულ ან იდენტიფიცირებად დასაქმებულს, ხოლო დამუშავება მოიცავს, შეგროვებას, შენახვას, კომბინაციას [60]. „დამსაქმებლები და დასაქმებულები უნდა

[56] იხ. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაციები, პერსონალური მონაცემების დაცვა, გზამკვლევი დამწყები ბიზნესისათვის, გვ.6..
[57] იხ. იქვე გვ.7.
[58] ძამუკაშვილი დ,. შრომის სამართალი,თბილისი, 2013, 37.
[59] საქართველოს სამოქალაქო კოდექსის მუხლი 319, ნაწილი 1.
[60] იხ. Protection of worker's personal data, Internation Labour Office Geneva; ILO, 1.

აცნობიერებდნენ, რომ შრომით კონტექსტში განხორციელებული ბევრი ქმედება მოიცავს დასაქმებულთა პერსონალური მონაცემების, ზოგჯერ კი ძალზედ სენსიტიური ინფორმაციის დამუშავებას“ [61] . საქართველოს ორგანული კანონის საქართველოს შრომის კოდექსის მიხედვით „შრომითი ხელშეკრულება იდება წერილობითი ან ზეპირი ფორმით, განსაზღვრული ან განუსაზღვრელი ვადით“ [62] , შესაბამისად შრომითი ხელშეკრულების ვადის მოქმედების პერიოდში დამსაქმებელს, რომელიც არის ამ შემთხვევაში პერსონალურ მონაცემთა დამმუშავებელი, შეუძლია დაამუშავოს მოპოვებული ინფორმაცია დასაქმებულების შესახებ, ან მოიპოვოს დამატებით ინფორმაცია დასამუშავებლად. საკითხი მნიშვნელოვანია იმ მხრივაც, რომ კერძოსამართლებრივი ურთიერთობის ხასიათიდან გამომდინარე შესაძლოა ხელშეკრულებით განსხვავებული პირობები განისაზღვროს მხარეების მიერ. შრომით სამართალს გააჩნია სპეციალური მახასიათებლები, რომლებიც გასათვალისწინებელია დამსაქმებელსა და დასაქმებულს შორის არსებულ ურთიერთობაში, რადგან ეს ურთიერთობა არის სახელშეკრულებო, რომელიც ხასიათდება იურიდიული დაქვემდებარებით და რეგულირდება საკუთარი სამართლებრივი წესებით, ასევე, შრომის სამართალი ხელშეკრულების მხარეებს მოლაპარაკების საშუალებას აძლევს, რომ თავად ხელშეკრულების მხარეებმა დაარეგულირონ ურთიერთობის შინაარსის მნიშვნელოვანი ნაწილი [63] . სწორედ ამიტომ აუცილებელია შრომითსახელშრულებო ურთიერთობის დროს პერსონალური მონაცემები დამუშავდეს დამუშავების პრინციპების სრული დაცვით.

---

[61] გოშაძე კ., პერსონალურ მონაცმეთა დამუშავების პრინციპების იმპლემენტირება შრომით ურთიერთობებში., სოფიო ჩაჩავას და ვახტანგ ზაალიშვილის რედაქტორობით, თბილისი, 2014, 26, იხ, ციტირება Article 29 – Data Protection Working Party, Opinion 8/2001 on the Processing of Personal Data in the Employment Context (13.09.2001), 2.

[62] საქართველოს შრომის კოდექსი, მუხლი 6, ნაწილი 1.

[63] იხ. ადამიანის უფლებათა ევროპული სასამართლოს ადამიანის უფლებათა ევროპული სასამართლოს 2017 წლის 5 სექტემბრის გადაწყვეტილება საქმეზე Barbulescu v. Romania, პარაგრაფი N:117-118..

2.1 მონაცემთა დამუშავების პრინციპების ზოგადი რეალიზება დამმუშავებლის მიერ

შრომით სამართლებრივ ურთიერთობაში პერსონალურ მონაცემთა დამმუშავებელი არის დამსაქმებელი ან უფლებამოსილი პირი დამსაქმებელთან დადებული ხელშეკრულების შესაბამისად, რომელიც აგროვებს და ამუშავებს მონაცემებს. დამსაქმებლები აგროვებენ მონაცემებს დასაქმებულების შესახებ, სხვადასხვა მიზეზით: კანონის დაცვა, სამუშაო პირობების ხელშეწყობის, ტრენინგის და დაწინაურების მიზნით, პირადი უსაფხოების, ხარისხის კონტროლის გაუმჯობესების, საკუთრების დაცვის მიზნით და ა.შ. „პირადი მონაცემების“ დამუშავებისათვის უნდა არსებობდეს „იურიდიული საფუძველი“ [64]. ერთი შეხედვით მონაცემთა დამუშავების საფუძვლები, რომელსაც ითვალისწინებს საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ,“ არის მთავარი განმსაზღვრელი მონაცემთა დამუშავებისათვის, მაგრამ აქვე უნდა აღინიშნოს, რომ დამუშავების პრინციპები აღმატებულია დამუშავების საფუძვლებზე, ეს ნიშნავს, რომ თუ შრომით სახელშეკრულებო ურთიერთობაში მხარეები შეთანხმდნენ გარკვეულ საკითზე, რომელსაც შემხებლობა აქვს მონაცემთა გამოყენებასთან, დამუშავების პრინციპებიდან გამომდინარე ისინი სავალდებულოდ უნდა იქნეს გათალისწინებული, წინააღმდეგ შემთხვევაში დამუშავების კანონიერება შესაძლოა სადავო გახდეს დამუშავების პრინციპების კუმულაციური ხასიათიდან გამომდინარე. იმ შემთხვევაშიც კი, როდესაც სახეზეა კანონით გათვალისწინებული მონაცემთა დამუშავების რომელიმე საფუძველი, მხოლოდ ასეთი საფუძვლის და ლეგიტიმური მიზნის არსებობა არ არის პერსონალური მონაცემების დამუშავების კანონიერების საკმარისი პირობა[65].

[64] ადამიანის უფლებათა ევროპული სასამართლოს 2000 წლის 16 თებერვალი გადაწყვეტილება საქმეზე Aman v. Switzerland, პარაგრაფი 76.

[65] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის 20 მაისის გადაწყვეტილება შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმეზე N: 3-1/043/2015, გვ. 5.

2.1.1. დამუშავების პროცესის კანონიერების, სამართლიანობისა და ღირსების დაცვის უზრუნველყოფა

პერსონალური მონაცემები უნდა დამუშავდეს სამართლიანად და კანონიერად, სუბიექტის ღირსების შეულახავად, რათა თავიდან იქნეს აცილებული არასასურველი და მოულოდნელი ზიანი და ასევე შეცდომაში შეიყვანოს დაინტერესებული პირები. ასევე არ შეილახოს პირთა ღირსება[66]. GDPR ადგენს, რომ პერსონალური მონაცემები უნდა დამუშავდეს, კანონიერად, სამართლიანად და გამჭირვალე ფორმით სუბიექტთან მიმართებაში[75]. შესაბამისად, იმისათვის, რათა დამუშავება შრომით სახელშეკრულებო ურთიერთობებში იყოს კანონიერი საჭიროა განისაზღვროს დამუშავების კონკრეტული საფუძველი. აღნიშნულს GDPRის მიხედვით ეწოდა დამუშავების „კანონიერი საფუძველი“ [67] . საინტერესოა რა შეიძლება იგულისხმებოდეს მონაცემთა „კანონის შესაბამის“ დამუშავებაში, რადგან აღნიშნულ ფორმულირებას შესაძლოა მრავალი ინტერპერტაცია ჰქონდეს. „კანონის შესაბამისად“ დამუშავება მოითხვოს, რომ სადავო ნორმას რაიმე საფუძველი ჰქონდეს შიდა კანონმდებლობაში, ასევე უნდა ასახავდეს კანონის ხარისხს, ხემისაწვდომი და განჭვრეტადი იყოს დაინტერესებული პირთათვის[68]. ფორმულირებაში „კანონის შესაბამისი“ უნდა იგულისხმებოდეს მისი „არსებითი“ და არა „ოფიციალური“ გაგება [69] , ასევე დამატებით შეეძლოს კანონის

[66] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მუხლი 4, ა ქვეპუნქტი
[75] Regulation (EU) 2016/679 of the European Parlament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealond Directive 95/46/EC (General Data Protection Regulation) of 27 April 2016, 34., ასევე Code of practice on the protection of worker's personal data, Article 5.1.
[67] Guide to the General Data Protection Regulation (GDPR), ICO, 2019, 21.
[68] ადამიანის უფლებათა ევროპული სასამართლოს 2000 წლის 16 თებერვალი გადაწყვეტილება საქმეზე Aman v. Switzerland, პარაგრაფი 50.
[69] ადამიანის უფლებათა ევროპული სასამართლოს 1998 წლის 25 მარტის გადაწყვეტილება საქმეზე Kopp v. Switzerlad, პარაგრაფი 59.

უზენაესობიდან გამომდინარე შედეგების წინასწარ განსაზღვრა [70] . ინფორმაციის რაოდენობა და სახეობა, მოძიებული მასალები შეიძლება განსხვავდებოდეს, მაგრამ საბოლოოდ მონაცემები მუშავდება დასაქმებულების სამუშაოს შესაფასებლად. დამსაქმებელი და დასაქმებული, რომლებიც შრომითი ხელშეკრულებით არიან დაკავშირებულნი ერთმანეთთან, ერთი მხირვ დამსაქმებელს წარმოეშობა ნდობა დასაქმებულის მიმართ, რომ იგი თავის სამუშაოს შეასრულებს კეთილსინდისიერად, ხოლო მეორე მხრივ დასაქმებულს უჩნდება მოლოდინი, რომ დამსაქმებელი კეთილსინდისიერად მოეკიდება მის შრომას [71] . სწორედ კეთილსინდისიერების პრინციპია დაკავშირებული კანონიერად დამუშავების პრინციპთან, რადგან დამმუშავებელმა კეთილსინდისეირად უნდა მოიპოვოს მონაცემები და შემდეგ დაამუშავოს დასაქმებულის თანხმობის საფუძველზე.

პერსონალური მონაცემების დამუშავებისას სამართლიანი ბალანსი უნდა იქნეს დაცული მონაცემთა დამმუშავებლის კანონიერ ინტერესსა და მონაცემთა სუბიექტის პირადი ცხოვრების ხელშეუხებლობის და პერსონალური მონაცემების დაცვის უფლებას შორის [72] . მონაცემთა სუბიექტის (დასაქმებულის) თანხმობას მონაცემთა დამუშავებისას მხოლოდ მაშინ ექნება სათანადო საფუძველი, თუ სუბიექტს შეეძლება ზემოქმედების გარეშე მიიღოს გადაწყვეტილება თავისი პერსონალური მონაცემების დამუშავების შესახებ[73]. თუ მუშაკმა ვერ გაიაზრა სათანადოდ მონაცემთა დამუშავების შესახებ ინფორმაცია, ასეთი მონაცემი არ უნდა დამუშავდეს[74].

საქართველოს უზენაესმა სასამართლომ 2016 წლის 18 მარტის საქმეში (საქმე №ას-50-49-2016) გაიზიარა თბილისის სააპელაციო სასამართლოს

---

[70] იხ. იქვე პარაგრაფი 55.

[71] საქართველოს უზენაესი სასამართლოს სამოქალაქო საქმეთა პალატის 2015 წლის 22 მაისის გადაწყვეტილება საქმე №ას-243-230-2015.

[72] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის 20 მაისის გადაწყვეტილება შპს „ა“-ს შემოწმების დასრულების შესახებ, N:გ-1/043/2015, გვ. 5.

[73] იხ. პერსონალურ მონაცემთა დაცვის ინსპექტორის რეკომენდაციები შრომით ურთიერთობებში პერსონალური მონაცემების დაცვის შესახებ; 2014, 6.

[74] იხ. Protection of worker's personal data, Internation Labour Office Geneva; ILO; 3

მოსაზრება, რომ დასაქმებულმა დაარღვია შრომითი ხელშეკრულების პირობები, რაც გამოიხატა აბონენტთა სატელეფონო ცნობარის შედგენაში, და შემდეგ გავრცელებაში, რამაც დაარღვია დამსაქმებლის კომერციული საიდუმლოება, კონფიდენციალური მონაცემები, და მომხმარებელთა პირადი ინფორმაცია [75] . შესაბამისად, შრომითსამართლებრივ ურთიერთობაში მნიშვნელოვანია არ დაირღვეს მონაცემთა დამუშავების სამართლიანობის პრინციპი, როგორც დამსაქმებლის ასევე დასაქმებულის მხრიდან, რადგან ამ კონკრეტული საქმიდან გამომდინარე დასაქმებული არის მონაცემთა დამმუშავებელი და შესაბამისი პასუხისმგებლობა ეკისრება მონაცემთა სამართლიანი და კანონიერი დამუშავებისათვის. მონაცემთა დამმუშავებლის მხრიდან მხოლოდ ისეთი მონაცემები უნდა დამუშავდეს, რომელიც ეხება მონაცემთა სუბიექტის სამუშაოს [76] . ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) მიხედვით, დასაქმებულთა თანხმობა ხელშეკრულებაში უნდა იყოს განცალკევებული, ან თუ ეს გათვალისწინებულია სამუშაო ხელშეკრულებაში უნდა იყოს აშკარად განსხვავებული ფორმით და დოკუმენტის სახით, (თუ არ არსებობს ალტერნატიული თანხმობის მიღების საფუძველი) თანხმობის მიცემამდე თანამშრომლებს ინფორმირებულნი უნდა იყვნენ საკუთარი უფლებების შესახებ[77].

საქართველოს საკონსტიტუციო სასამართლოს განმარტებით, თუ სუბიექტს აქვს სურვილი, საზოგადოება გაეცნოს მის შესახებ შეგროვებულ მონაცემებს, თანხმობა უნდა გაიცეს ინდივიდუალურად [78] , რაც გულისხმობს, რომ დამსაქმებელმა მონაცემთა დამუშავების დაწყებამდე უნდა მიაწოდოს დასაქმებულს ინფორმაცია თუ რომელი მონაცემი

[75] საქართველოს უზენაესი სასამართლოს სამოქალაქო საქმეთა პალატის 2016 წლის 18 მარტის განჩინება საქმე N:ას-50-49-2016, პარაგრაფი 13.

[76] ადამიანის უფლებათა ევროპული სასამართლოს 2017 წლის 5 სექტემბრის გადაწყვეტილება საქმეზე Barbulescu v. Romania, პარაგრაფი N38.

[77] იხ. A&L Goodbody, GDPR for Employers, გვ. 1.

[78] საკონსტიტუციო სასამართლოს 2019 წლის 7 ივნისის გადაწყვეტილება №1/4/693,857 საქმეზე „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ“, პარ N32.

მუშავდება, დამუშავების მიზანი და იურიდიული საფუძველი, მონაცემთა შენარჩუნების პერიოდი ან კრიტერიუმები, პერსონალური მონაცემების მიმღების კატეგორიები, ინდივიდის უფლებები, მათ შორის კორექტირების, წაშლის უფლება, საჩივრის უფლება, უნდა გადეცეს თუ არა მესამე პირს ეს მონაცემები და ამ დროს დაცვის გარანტიები და ა.შ[79]. ზემოაღნიშნულ გადაწყვეტილებაში სატელეფონო ცნობარის შედგენასთან დაკავშირებით არცერთი სატელეფონო ცნობარის სუბიექტის ინფორმირება არ მომხდარა, შესაბამისად დარღვეულია სამართლიანად და კანონიერად დამუშავების პრინციპი, რასაც შესაძლოა შედეგად მოჰყოლოდა სუბიექტის ღირსების შელახვა, რეაგირება დროული რომ არ ყოფილიყო დამსაქმებლის მხრიდან. სწორედ ამიტომ კანონიერების და სამართლიანობის პრინციპი პირდაპირ კავშირშია გამჭირვალობის პრინციპთან.

დასაქმებულთა შესახებ ინფორმაცია ხელმისაწვდომი უნდა იყოს უშუალოდ დაინტერესებული თანამშრომისთვის. ყველა მონაცემი ინდივიდუალურად უნდა იყოს მოპოვებული თანამშრომლისგან[80]. CJEU ერთ-ერთ გადაწყვეტილებაში მსჯელობს უნდა მომხდარიყო თუ არა თვითდასაქმებული პირების ინფორმირების გარეშე, შემოსავალთან დაკავშირებული საგადასახადო მონაცემების გადაცემა, საგადასახადო ადმინისტრირების ეროვნული სააგენტოდან, ჯანმრთელობის დაზღვევის ეროვნულ ფონდში (რუმინეთში)[81], CJEU დაადგინა, რომ მონაცემთა გადაცემისას, ვინაიდან გადასაცემი ორგანოც ამუშავებს მონაცემებს უნდა ეცნობოს მონაცემთა სუბიექტების გადაცემის ან დამუშავების შესახებ, სხვა შემთხვევაში მონაცემთა დამუშავება დაუშვებელია[82]. იმის შეფასება თუ რამდენად მართებულად მუშავდება ინფორმაცია დამსაქმებლის მხრიდან,

[79] იხ. A&L Goodbody, GDPR for Employers, გვ. 4.

[80] Code of practice on the protection of worker's personal data, article 6.1.

[81] CJEU, In Case c-201/14 Smaranda Bara and Others V. Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF), 1 Octomber 2015, პარაგრაფი 14-17.

[82] CJEU, In Case c-201/14 Smaranda Bara and Others V. Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF), 1 Octomber 2015, პარაგრაფი 47.

ნაწილობრივ დამოკიდებულია იმაზე, თუ როგორ მოიპოვებს იგი ამ მონაცემებს. აუცილებლად გასათვალისწინებელია თუ რა გავლენას ახდენს დაინტერესებული პირების ინტერესზე, როგორც ჯგუფურად, ასევე ინდივიდუალურად, რადგან თუ ერთი პირის მიმართ მაინც მოხდება არასამართლიანი და უკანონო დამუშავება, მაშინ აღნიშნული პრინციპის დარღვევა მაინც მოხდება[83].

ამრიგად, სამართლიანობის, კანონიერებისა და ღირსების დაცვის პრინციპი უპირველესად არეგულირებს ურთიერთობას დამმუშავებელსა და მონაცემთა დამუშავების სუბიექტს შორის. დამუშავების პროცესი დამმუშავებლის მიერ არ უნდა იქნეს საიდუმლოდ წარმოებული, ამით დამმუშავებელს ექნება გარანტია ის უარყოფითი შედეგები აიცილოს თავიდან, რაც შესაძლოა დამუშავების პროცესს მოყვეს. სწორედ ამიტომ, დამუშავების კანონიერიერება დამუშავების დაწყების ეტაპიდანვე უნდა უზრუნველყოს დამმუშავებელმა. იგი ასევე უნდა დარწმუნდეს, რომ დამუშავების სუბიექტი ინფორმირებულია დამუშავებაზე და მის შედეგს აცნობიერებს. აღნიშნული პრინციპის შესაბამისად დამმუშავებელს უფლება აქვს სუბიექტის ლეგიტიმური ინტერესის შესაბამისად იმოქმედოს, და უფრო მეტიც, თუ საჭიროა შესაძლოა გასცდეს მისი უფლებამოსილების ფარგლებს.

2.1.2. მიზნის მკაფიოდ განსაზღვრა, როგორც პროპორციული დამუშავების უზრუნველყოფის წინაპირობა

მონაცემები უნდა შეგროვდეს დაზუსტებული, მკაფიო, რელევანტური, აშკარა და ლეგიტიმური მიზნით, და არ უნდა დამუშავდეს შემდგომ თავდაპირველ მიზანთან შეუთავსებელად. (მაგ: სახელფასო მიზნით შეგროვებული მუშაკთა პირადი მონაცემები არ შეიძლება შემდგომ

[83] Guide to the General Data Protection Regulation (GDPR), Ico,2019,22.

გამოყენებული იყოს პირდაპირი მარკეტინგის მიზნით[84], ასევე არ უნდა იქნეს გამოყენებული სიმართლის დადგენის მიზნით პოლიგრაფია (სიმართლის გადამოწმების მოწყობილობა), ან სხვა მსგავსი ტესტირების პროცედურები თანამშრომლებზე [85] . დამსაქმებლები აკონტროლებენ დასაქმებულებს, გარკვეულ შემთვევაში დამსაქმებელს შეიძლება მოეთხოვებოდეს კიდეც თანამშრომლის მონიტორინგი, რომელსაც საფუძველი შეიძლება სხვადასხვა იყოს. ეს შეიძლება იყოს, როგორც სამსახურებრივი მოვალეობის სრულყოფილად შესრულების, ასევე მომსახურების გაუმჯობესების მიზნით, სამართალდამცავი ორგანოებისათვის გადასაცემად, დანაშაულის დაფარვის და თავიდან აცილების მიზნით. დამსაქმებელმა უნდა განასხვავოს ნებადართული და აკრძალული მონიტორინგის მიზენები, რომელიც შეიძლება იყოს: ა) სისტემის სტაბილურად ფუქნციონირების უზრუნველყოფა; ბ) უზრუნველყოს მონაცემთა კანონიერი დამუშავება; დ) თანამშრომლების ეფექტური მუშაობის უზრუნველსაყოფა [86] . კონტროლი შესაძლოა განხორციელდეს სხვადასხვა გზებით, ეს შეიძლება იყოს სპეციალური პროგრამების შექმა, რომელიც აკონტროლებს დასაქმებული პირების კომპიუტერებს, პირად ტელეფონებს, პირადი ელექტრონული ფოსტის კონტროლი, ვიდეო თვალთვალის სისტემის განხროციელებით სამუშაოს მიმდინარეობის მეთვალყურეობა. მაგალითად სამხეთ

დოკოტაში დასაქმებული პირები სპეციალური ტექნოლოგიის გამოყენებით შესაბამის ორგანოებს ინფორმაციას აწვდიან ისეთი კომპიუტერების შესახებ, სადაც ბავშვთა პორნოგრაფიის ფაქტებია

მოძიებული[87]. მონიტორინგი დამსაქმებლის მხრიდან შესაძლოა

[84] Article 29- Data Protection Working Party, opinion 8/2001 on the processing of personal data in the employment context, Adopted on 13 seqtember 2001, 20.

[85] Protection of worker's personal data, Internation Labour Office Geneva; ILO; 4.

[86] Paul p. K and Reiner. S "Manual on Data Protection in Employment Context", Ludwig Boltzmann Institute of Human Rights, Vienna Mandated Body, November 2006, 35.

[87] V. John Ella, J.D., CIPP, Jackson Lewis P.C. "Employee monitoring and workpace Privacy Law", Washington, D.C. April 6, 7, and 8, 2016, 3.

განხორციელდეს როგორც სამუშაო საათების დროს, ასევე სამუშაო საათების დასრულების შემდეგ, თუ კონტროლის განსახორციელებლად გამოიყენება გარე კონტროლის მექანიზმები, (მაგ: პირად ტელეფონში პროგრამის ჩაწერით, რომელიც ადგილმდებარეობას განსაზღვრავს) რათა დამსაქმებელმა გაიგოს თანამშრომლის ადგილსამყოფელი.

დამსაქმებლების მხრიდან თანამშრომლების მონიტორინგი შესაძლოა გამოხატულ იქნეს არამარტო დამსაქმებლის სუბიექტური ნებით, არამედ აუცილებელიც კი იყოს გარკვეული სამუშაოს სპეციფიკიდან გამომდინარე. აუცილებლობა გულისხმობს, რომ ჩარევა მნიშნველოვანი სოციალური საჭიროებებიდან გამომდინარე უნდა იყოს პროპორციული ლეგიტიმური მიზნის მისაღწევად [88]. ჩრდილოეთ დაკოტასა და ვისკონსის შტატში დამსაქმებლებს აეკრძალათ დასაქმებულის სხეულში მიკრო ჩიპების (RFID) ჩაყენება, რომელიც მათ ადგილმდებარეობას განსაზღვრავდა [89]. ცნობილი ფაქტია სუპერმარკეტი „ფრესკოს“ მიერ განხორციელებული მონიტორინგი გასახდელ ოთახებში[90], რომლის მიზანი თითქოსდა მომსახურების გაუმჯობესება იყო, მაგრამ რეალურად დარღვეულია მიზნის პროპორციულობის პრინციპი, რადგან მომსახურების გაუმჯობესების მიზანი არ შეიძლება იყოს გასახდელი და ჰიგიენისთვის განკუთვნილი ოთახების ვიდეოკონტროლი. უსაფთხოების და საკუთრების დაცვის მიზნით დაუშვებელია საპირფარეშოების და თანამშრომელთა გამოსაცვლელი ოთახების ვიდეოკონტროლი [91]. ფარული მონიტორინგი დაიშვება მხოლოდ მაშინ, როდესაც ის შესაბამისობაშია ეროვნულ

---

[88] ადამიანის უფლებათა ევროპული სასამართლოს 1987 წლის 26 მარტის გადაწყვეტილება, საქმეზე Leander v. Sweden, პარაგრაფი 58.

[89] V. John Ella, J.D., CIPP, Jackson Lewis P.C. “Employee monitoring and workpace Privacy Law”, Washington, D.C. April 6, 7, and 8, 2016, 9.

[90] < https://netgazeti.ge/news/186433/> 30.04.2020.

[91] საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 25 მაისის გადაწყვეტილება, შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-1/286/2017, გვ. 5-6, ასევე საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 16 ივნისის გადაწყვეტილება, შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-1/314/2017 გვ.1, იქვე გვ.11.

კანონმდებლობასთან[92], ასევე მონიტორგინგით შეგროვებული მონაცემები არ უნდა იყოს ერთადერთი რომელიც შეაფასებს დასაქმებულების მუშაობას[93].

მონიტორინგიც მონაცემთა დამუშავებაა, რადგან გროვდება ინფორმაცია დასაქმებულ პირებზე. მონიტორინგს რომელსაც განახორციელებს დამსაქმებელი ამ შემთხვევაში აუცილებელია, იყოს მიზნობრივი მოსალოდნელი შედეგთან, რასაც დამუშავებით მიიღებს. ჩნდება კითხვა, რატომ არის აუცილებელი მიზნის დაზუსტება? ეს მოთხოვნა მიზნად ისახავს, რომ ნათლად და მკაფიოდ იყოს მოპოვებული მონაცემები და შესაბამისობაში იყოს დაინტერესებული პირების გონივრულ მოლოდინთან[94].

ავსტრია, ფინეთი, ლუქსემბურგი, პორტუგალია, სლოვაკეთი და გერთიანებული სამეფო არიან ის სახელმწიფოები, რომლებმაც დაარეგულირეს სამუშაო ადგილის კონფიდენციალურობის საკითხი როგორც შრომითი კანონებით ასევე სპეციალური კანონმდებლობით [95], ავსტიაში, ესტონეთში, ფინეთში, საბერძნეთში, ლიტვაში, ლუქსემბურგში, ნორვეგიაში, პოლონეთში, სლოვაკეთსა და მაკედონიის ყოფილი იუგოსლავიის რესპუბკილაში, დამსაქმებლებს ევალებათ უშუალოდ აცნობონ დასაქმებულებს მონიტორინგის დაწყებამდე[105], ავსტრიაში, დანიაში, ფინეთში, საფრანგეთში, გერმანიაში, საბერძნეთში, იტალიაში, პორტუგალიასა და შვედეთში შეუძლიათ ელექტრონული ფოსტის მონიტორინგი, ლუქსემბურგში დამსაქმებლებს არ შეუძლიათ გახსნან ელ. წერილი რომელიც აშკარა „კერძო“ და პირადი ხასიათისაა, ჩეხეთის რესპუბლიკა, იტალია და სლოვენია ისევე, როგორც მოლდოვას რესპუბლიკა, გარკვეულწილად ზღუდავს თუ რამდენად შეუძლია დამსაქმებელს გააკონტროლოს თავისი თანამშრომლის კომუნიკაცია,

[92] Protection of worker's personal data, Internation Labour Office Geneva; ILO; 4.

[93] იხ. იქვე გვ. 2.

[94] Guide to the General Data Protection RegulaTion (GDPR), Ico, 2019, 25.

[95] ადმიანის უფლებათა ევროპული სასამართლოს 2017 წლის 5 სექტემბრის გადაწყვეტილება საქმეზე Barbulescu v. Romania, პარაგრაფი N52. [105] იქვე, პარაგრაფი N53.

იმისდა მიხედვით ეს კომუნიკაცია, პროფესიულია თუ პერსონალური, ხოლო გერმანიასა და პორტუგალიაში მას შემდეგ რაც დამსაქმებელი მიხვდება რომ კომუნიკაცია არის პირადი, უნდა შეწყვიტოს მისი კითხვა[96]. დასაქმებულების ინფორმირება, რა მიზნით ხდება მათი მონიტორინგი აუცილებელი კომპონენტია მიზნობრიობის პრინციპის სწორად განხორციელებისათვის. დამსაქმებელმა შრომით ურთიერთობის პროცესში უნდა დაამუშავოს მხოლოდ ის პერსონალური მონაცემი, რომელიც აუცილებელია აღნიშნული მიზნის მისაღწევად[97].

„გარდა, იმისა რომ დამუშავების მიზანი მკაფიო უნდა იყოს პროცესში მონაწილე პირებისათვის, იგი ასევე უნდა იყოს კანონით ნებადართულის საქმიანობის ნაწილი“ [98] [99] . მიზნობრიობის პრინციპი კავშირშია გამჭირვალობის, სამართლიანობის, თანასწორობის პრინციპებთან და ასევე მონაცემების პროპორციულად დამუშავების საფუძველის უზრუნველყოფის საშუალებაა. თანაზომიერების ასევე მოითხოვს რომ დაცული იყოს პროპორციულობა ვიწრო გაგებით, აუცილებელია დადგინდეს სამართლიანი ბალანსი იმგვარად, რომ დაცული სიკეთე და მისი დაცვის ინტერესი აღემატებოდეს შეზღუდული უფლების დაცვის ინტერესს [100] . პერსონალურ მონაცემთა დაცვის ინსპექტორი უთითებს დამსაქმებელი კომპანიის მიერ მონაცემების არაპროპორციულ და დიდი მოცულობით დამუშავებაზე, მომხმარებლის შესახებ ინფორმაციის დედისთვის და სავარაუდო მეგობრებისთვის (სოციალური ქსელიდან) გადაცემის გამო და ავალებს კომპანიას, რომ პერსონალური მონაცემების დამუშავების მარეგულირებელი სახელშეკრულებო პირობებში მკაფიოდ და

---

[96] იქვე, პარაგრაფი N54.

[97] პერსონალურ მონაცემთა დაცვის ინსპექტორის რეკომენდაციები შრომით ურთიერთობებში პერსონალური მონაცემების დაცვის შესახებ, თბილისი, 2014, 3.

[98] გოშაძე კ., პერსონალურ მონაცემთა დამუშავების პრინციპების იმპლემენტირება შრომით ურთიერთობებში., სოფიო ჩაჩავას და ვახტანგ ზაალიშვილის რედაქტორობით, თბილისი

[99] , 36.

[100] საკონსტიტუციო სასამართლოს 2019 წლის 7 ივნისის გადაწყვეტილება №1/4/693,857 საქმეზე „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ“, პარაგრაფი N: 36.

კონკრეტულად ჩამოაყალიბოს მონაცემთა დამუშავების მიზნები, და განსაზღვრულიყო დასამუშავებელ მონაცემთა მოცულობა[101].

საქმეზე Barbulescu v. Romania[102] ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, ადამიანის უფლებათა ევროპული კონვენციის მე8 მუხლის დარღვევა, რადგან დამსაქმებლის მხრიდან ადგილი ჰქონდა ელექტრონული ფოსტის კონტროლს, რომლის შესახებ დასაქმებული პირები ინფორმირებულები არ ყოფილან. ელექტრონული ფოსტის კონტროლის მიზანი იყო, ის რომ დასაქმებულებს არ გამოეყენებინათ სამსახურებრივი ინტერნეტი არასამუშაო მიზნებისათვის. შესაბამისად, აუცილებელი იყო დასაქმებულების ინფორმირება კონტროლის მიზანთან დაკავშირებით, ვინაიდან ინფორმირება არ მოხდა შესაბამისად დამუშავება იყო მიზნის შეუსაბამო და დარღვეულია მიზნობრიობის პრინციპი.

მიზნის სწორად განსაზღვრის პრინციპი პირდაპირ კავშირშია პროპორციულობის პრინციპთან, რადგან აუცილებელია, რომ მონაცემები დამუშავდეს მინიმალურ ოდენობამდე დაყვანით (მინიმიზაციის პრინციპი) მხოლოდ იმ მოცულობით და მხოლოდ ის მონაცემები, რომელიც აუციელებელია მიზნის მისაღწევად. დამსაქმებლებმა პატივი უნდა სცენ დასამების მიზნებისათვის მონაცემთა დამუშავებათან დაკავშირებულ პრინციპებს[103]. იმ პრინციპების ჩამოთვალში, რომელიც დამსაქმებელმა უნდა გაითვალისწინოს მონაცემთა დამუშავებისთვის, სწორედ პროპორციულობის პრინციპია ერთ-ერთი, რადგან მისი სწორად განხორციელება აუცილებელია მონაცემთა სწორად დამუშავებისთვის. პერსონალურ მონაცემთა დაცვის ინსპექტორმა ერთ-ერთ გადაწყვეტილებაში აღნიშნა - „მიუხედავად იმისა, რომ სააფთიაქო ქსელში

[101] საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 28 მარტის გადაწყვეტილება ლ.ა-ს განცხადებასთან დაკავშირებული განხილვის დასრულების შესახებ, საქმეN:გ-1/165/2017, გვ. 10, ასევე საქართველოს პერსონალურ მონაცემთა დაცვის ისნპექტორის 2017 წლის 21 აპრილის გადაწყვეტილება მ.ა-ს განცხადებასთან დაკავშირებული განხილვის დასრულების შესახებ, საქმე N:გ-1/210/2017, გვ 7-8.

[102] ადამიანის უფლებათა ევროპული სასამართლოს 2017 წლის 5 სექტემბრის გადაწყვეტილება საქმეზე Barbulescu v. Romania.

[103] Top 10 principles for worker's Data Privacy and Protection, the future word od work.

აუდიოვიდეომონიტორინგზე თანხმობა გაცხადებული იყო დასაქმებული პირების მხრიდან, მის შედეგად დამუშავებული მონაცემები ვერ ჩაითვლება კანონიერი მიზნის ადეკვატურ და პროპორციულ საშუალებად[104]“ რადგან თუმცა კანონიერი მიზნით ხდება დამუშავება, ამ მიზნის მიღწევა შეიძლება ნაკლები მოცულობით და პირად ცხოვრებაში ნაკლები ჩარევით[105]. ვინაიდან სააფთიაქო ქსელში აუდიოვიდეომონიტორნგი ხორციელდებოდა არამარტო დასაქმებული პირების, არამედ მომხამრებლების მიმართაც. გაერთიანებულ საქმეში C 293/12 და C 594/12, სასამართლომ იმსჯელა, რომ მიუხედავად დიდი საჯარო ინტერესისა (დანაშაულის თავიდან აცილება) ელექტრონული საკომუნიკაციო საშულებებით და საჯარო წყაროებიდან მოპოვებული მონაცმეების გადაცემა სახელწიფო ორგანოსთვის იყო არაპროპორციული[106], რადგან სუბიექტების წრე გასაზღვრული არ ყოფილა კანონმდებლობით, ვინაიდან ელექტრონული საკომუნიკაციო საშულებით მონიტორინგი ხორციელდებოდა არამხოლოდ სავარუდო დამნაშავეების, არამედ ისეთი სუბიექტებისაც, რომელთა მიმართ დანაშაულის ფატი არ არსებობდა[107].

ზემოთ არაერთხელ აღინიშნა, რომ მიმდინარე შრომით ურთიერთობებში დამსაქმებლების მხრიდან ხდება საკმაო მოცულობის მონაცემების დამუშავება, რომელიც შესაძლოა თავდაპირველი დამუშავების მიზნისგან განსხვავდებოდეს. მონაცემთა ყოველი ახალი მიზნით დამუშავება დაკავშირებული უნდა იყოს კონკრეტულ სამართლებრივ საფუძველთან, თუნდაც მონაცემები თავდაპირველად დამუშავებული იყოს კონკრეტული, ლეგიტიმური მიზნით. ყოველი ახალი მიზნით დამუშავებას კი აუცილებლად სჭირდება დამოუკიდებელი სამართლებრივი საფუძველი.

---

[104] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის 20 მაისის გადაწყვეტილება შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-1/043/2015, გვ 6.

[105] იქვე, გვ. 5.

[106] CJEU, In Joined Cases C 293/12 and C 594/12, Digital Rights Ireland Ltd (C 293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, 8 April, 2014, პარაგრაფი 68.

[107] იხ. იქვე, პარაგრაფი 61.

დამსაქმებელი, რომელიც არის შრომითსამართლებრივ ურთიერთობებში ძირითადი დამმუშავებელი, მინიმიზაციის პრინციპის გათვალისწინებით უნდა შეამციროს დასამუშავებელი მონაცემები იმ ინფორმაციამდე, რომელიც შესაბამისი იქნება დამუშავების კონკრეტული მიზნისათვის.

2.1.3. მონაცემთა მიზნობრივი განახლება და სისწორის დაცვა

შეგროვებული ინფორმაციის დამუშავებისას დამსაქმებელმა, რომელიც არის მონაცემთა ძირითადი დამმუშავებლი შრომით სახელშეკრულებო ურთიერთობებში, უნდა დაამუშავოს მხოლოდ ის მონაცემები, რომელიც არის ნამდვილი. თუ დამუშავებული მონაცემები არ შეესაბამება რეალობას ექვემდებარება განადგურებას, წაშლას და დაბლოკვას[108]. დამსაქმებლები, როგორც კერძოსამართლებრივი ურთიერთობის მონაწილე სუბიექტები სამუშაოს სპეციფიკიდან გამომდინარე სარგებლობენ სხვადასხვა ბაზებით, სადაც შესაძლოა ინახებოდეს არამარტო თანამშრომლების შესახებ მონაცემები, არამედ მომხმარებელთა მონაცემები. ასეთი პროგრამები, ბაზები იქმნება მომსახურების გაუმჯობესების მიზნით. აუცილებელია ასეთი ბაზების მიზნობრივი განახლება გარკვეული პერიოდის გასვლის შემდეგ, ასევე არაზუსტი მონაცემების გასწორება, რადგან ინფორმაციები იცვლება, შეიძლება საჭიროც აღარ იყოს კონკრეტული მონაცემების შენახვა, ამიტომ თუ მონაცემები არ იქნება ნამდვილი, პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მოქმედების სფეროც ვერ გავრცელდება მათზე. თბილისის საქალაქო სასამართლო, ოფიციალური ვებ გვერდიდან მონაცემების განუახლებლობის და მონაცემების შენახვის ვადის პრინციპის დარღვევის გამო სამართალდამრღვევად ცნო პერსონალურ

[108] იხ. პერსონალურ მონაცემთა დაცის შესახებ საქართველოს კანონი, მუხლი 4, პუნქტი დ.

მონაცემთა დაცვის ინსპექტორმა და მიუთითა შესაბამისი ვერბგვერდზე მონაცემების განახლების და სიზუსტის დაცვაზე[109].

„მონაცემთა სიზუსტის უზრუნველყოფის მოვალეობა უნდა აღვიქვათ მონაცემთა დამუშავების მიზნის კონტექტში“[11101119]. პერსონალურ მონაცემთა დაცვის ინსპექტორთან ერთ-ერთი პირის განცხადებით მიმართვის საფუძველი გახდა სწორედ ის, რომ იგი დამსაქმებლისგან ვერ იღებდა ინფორმაციას მისი პერსონალური მონაცემების დამუშავების შესახებ და ასევე მიუთითებდა, რომ მის შესახებ მონაცემების დამუშავება დაიწყო უცხო კონტრაქტორი კომპანიის მიერ მიწოდებული ინფორმაციის საფუძველზე და დამსაქმებელს არ გადაუმოწმებია მონაცემთა სისწორე[112]. აღნიშნულ გადაწყვეტილებაში დამსაქმებლის ბრალეულობა ვერ დადგინდა, ვინაიდან უცხო კონტრაქტორის მიერ მიწოდებული მონაცემების გამოყენება და დამუშავება საჭირო აღარ გახდა, მაგრამ რა იქნებოდა თუ მონაცემების გადამოწმების გარეშე დაიწყებდა მონაცემთა დამმუშავებელი, ამ შემთხვევაში დამსაქმებელი კომპანია? საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ ითვალისწინებს რომ, მხოლოდ ნამდვილი და ზუსტი მონაცემები უნდა დამუშავდეს, ხოლო თუ მონაცემები არ არის რეალური ექვემდებარება წაშლას, განადგურებას, დაბლოკვას, ამასთანავე არაზუსტი მონაცემების დამუშავება ვერ მოექცევა კანონის მოქმედების სფეროში[12113114]. პერსონალური მონაცემების მოპოვება რა თქმა უნდა არ გულისხმობს ინფორმაციის მიღებას არაპირდაპირი გზით, მაგალითად ყოფილ დამსაქმებელთან კონსულტაციას[115], უნდა აღინიშნოს ისიც, რომ სიზუსტის პრინციპიდან გამომდინარე ის მონაცემები, რომელიც

---

[109] საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 28 თებერვლის გადაწყვეტილება, მ.დ-ს განცხასების განხილვის დასრულების შესახებ, საქმე N:გ-
[110] /103/2017, გვ. 3, გვ.6.
[111] მონაცემთა დაცვის ევროპილი სახელმძღანელო, ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი 2018, 145.
[112] საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის 7 სექტემბრის გადაწყვეტილება, გ.ნ-ს განცხადების განხილვის დასრულების შესახებ, საქმე N:გ-
[113] /507/2018, გვ. 3.
[114] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მუხლი 4, პუნქტი დ.
[115] Protection of worker’s personal data, Internation Labour Office Geneva; ILO; 15.

საჭირო აღარ არის თავდაპირველი მიზნის მისაღწევად უნდა დაუბრუნდეს სუბიექტს. დამსაქმებელმა უნდა გადადგას ყველა გონივრული ნაბიჯი, რომ მონაცემები არ იყოს არასრული ან არაზუსტი, საჭირო მიზნისთვის დამუშავებული მონაცემები უნდა იყოს დაცული, არაუმეტეს იმ ვადით რაც საჭიროა მუშაკთა იდენთიფიკაციისთვის[116]. ამრიგად, სიზუსტის პრინციპის შინაარსიდან გამომდინარე იმისათვის, რათა მონაცემები იყოს ზუსტი აუცილებელია, როგორც დამსაქმებლის, ასევე დასაქმებულის მოქმედება არსებობდეს, მაგრამ სიზუსტის დაცვა დამსაქმებლის ვალდებულებაა. დასაქმებულს შეუძლია მოითხოვოს მის შესახებ მონაცემების შესწორება, რაზეც დამსაქმებელმა შესაბამისი მოქმედებები უნდა განახორციელოს, დამსაქმებელი კი საკუთარი ინციატივით კანონით დადგენილი იმპერატიული დათქმით ვალდებულია არაზუსტი მონაცემები შეასწოროს და მიიღოს მათი განადგურების/წაშლის/დაბლოკვის გადაწყვეტილება. პერსონალური მონაცემების წაშლის ან გასწორების შემთხვევაში, დამსაქმებელმა უნდა აცნობოს ყველა მხარეს, რომელთაც ადრე მიეწოდათ არასწორი ან არაზუსტი მონაცემები[117]. მონაცემთა სიზუსტის პრინციპიდან გამომომდინარე CJEU ერთ-ერთ გადაწყვეტილებაში მსჯელობს, აგრეთვე კონფიდენციალობის დაცვის ვალდებულებაზეც, ის აღნიშნავს, რომ მონაცემთა დაცვის სუბიექტმა უნდა იცოდეს, რომ პერსონალური მონაცემები დამუშავებულია სწორი და კანონიერი გზით, ასევე მონაცემები ზუსტია და მისი გამჟღავნების აუცილებლობის შემთხვევაში მოხდება მისი ინფორმირება [118] . თითოეულ თანამშრომელს აქვს უფლება მოითხოვოს მონაცემებზე წვდომა და საჭიროების შემთხვევაში მათი შესწორება და წაშლა[119].

[116] Article 29 – Data Protection working party, Opinion 8/2001 on the processing data in the employment context, Adopted on 13 seqtember 2001, 21.

[117] იხ. Protection of worker's personal data, Internation Labour Office Geneva; ILO; 7.

[118] იხ. CJEU, In case C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, 7 May 2009. პარაგრაფი 71.

[119] Council of future committe of ministers of the comitte recommendation No. R (89) 2, of ministers to member State on the Protection of Personal Data used for employment purposes;

პერსონალური მონაცემების მიზნობრივი განახლების და სიზუსტის პრინციპთან პირდაპირ კავშირშია შენახვის ვადის პრინციპი, რადგან მიზნობრივი განახლებისათვის აუცილებელია, რომ დამსაქმებლის მიერ განისაზღვროს გარკვეული ვადა, რა ვადის განმავლობაშიც მონაცემები ეტაპობრივად აუცილებლად გადამოწმდება, ხოლო გადამოწმების შემდეგ შესაძლოა განახლდეს/წაიშალოს/განადგურედეს/დაიბლოკოს. სახელმწიფო ინსპექტორმა სამართალდარღვევად ცნო სასტუმროს და მაღაზიათა ქსელის მიერ ვიდეოჩანაწერების განუსაზღვრელი ვადით შენახვა[120], რადგან აღარ არსებობდა ვიდეოჩანაწერების შენახვის მიზანი, რომელიც თავდაპირველად იყო განსაზღრული კომპანიის და მაღაზიათა ქსელის მიერ. შენახვის ვადას უკავშირდებოდა ასევე თბილისის საქალაქო სასამართლოს მხრიდან სამართალდარღვევა, რამდენადაც მის ოფიციალურ ვებგვერდზე მონაცემების განუსაზღვრელი ვადით შენახვისა [121] და სასტუმრო ქსელის მხრიდან მომხმარებლების მონაცემების უვადოდ შენახვისთვის [122] [123] არ არსებობდა რეგულაცია. CJEU ერთ-ერთ გადაწყვეტილებაში მსჯელობს, რამდენად არის შესაძლებელი მონაცემებზე წვდომა 1 წლის განმავლობაში, თუ მონაცემები გაცილებით დიდხანს ინახება, (ამ შემთხვევაში კოლეჯის მიერ) სასამართლო აღნიშნავს, რომ როდესაც იზღუდება ასეთ მონაცემებზე წვდომა ეს არ წამოადგენს სამართლიან ბალანსს[124], ვიანიდან პერსონალურ მონაცემთა მიმღებ პირებს

(Adopted by the Committee of Ministers on 18 January 1989 at the 423rd meeting of the Ministers' Deputies), 12, 12.1 .

[120] საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის გადაწყვეტილება, შპს „ა“ს შემოწმების დასრულების შესახებ, საქმე N: გ-1/286/2017, გვ.4, გვ.8, ასევე საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 16 ივნისის გადაწყვეტილება შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N: გ-1/314/2017, გვ.9.

[121] იხ. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 28 თებერვლის გადაწყვეტილება, მ.დ-ს განცხადების განხილვის დასრულების შესახებ, საქმე
N: გ-1/103/2017, გვ. 6.

[122] იხ. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის 26 დეკემბრის გადაწყვეტილება, სს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-

[123] /701/2018, გვ. 3.

[124] იხ. CJEU, In case C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, 7 May 2009, პარაგრაფი 70.

უნდა ჰქონდეთ მონაცემებზე დაშვების უფლება, არამხოლოდ ახალდენლი, არამედ წარსული დროის მიმართ[125]. შესაბამისად სიზუსტის და შენახვის ვადის პრინციპიდან გამომდინარე დამსაქმებელმა უნდა განსაზღვროს: ა) ინფორმაციის შეგროვების ეტაპზე მონაცემთა დამუშავების ვადა; ბ) მონაცემთა შეგროვების წყარო და ინფორმაციის პერიოდულად გადახედვის სავარაუდო დრო; გ) განსაზღვროს დამუშავებული მონაცემების მოცულობა, მიზნის პროპორციულად დამუშავებასთან მიმართებაში; დ) დამუშავების სავარაუდო შედეგიანობა, რადგან თუ კონკრეტული ინფორმაციის დამუშავებით არ მიიღწევა შედეგი, ასეთი მონაცემი უპირველესად არასაჭიროა და არამიზნობრივი.

2.1.4. დამუშავების მთელი პროცესის უსაფრთხოდ უზრუველყოფა

GDPR-ის მე-5 მუხლის პირველი პუნქტის "f" ქვეპუნტით გათვალისწინებულია, რომ მონაცემთა დამუშავებისას უზრუნველყოფილ იქნეს მონაცემთა სათანადო უსაფრთხოება, მათ შორის უკანონო და უნებართვო დამუშავების, შემთხვევითი განადგურების და ზარალის თავიდან ასაცილებლად[126]. მონაცემთა უსაფრთხოდ დამუშავებისათვის და შენახვისათვის დამმუშავებელი ვალდებულია მიიღოს ყველა საჭირო ტექნიკური და ორგანიზაციული ზომები, ელექტრონულად შეგროვებული მონაცემები უნდა აღრიცხოს, რათა თავიდან იქნეს აცილებული მონაცემების შემთხვევითი ან უკანონო განადგურება, შეცვლა, გამჟღავნება, მოპოვება, უკანონო დაკარგვა, ასევე უსაფრთხოების ზომები უნდა იყოს რისკების ადეკვატური [127] . უსაფრთხოების პრინციპი მოითხოვს, რომ

[125] იხ. იქვე. პარაგრაფი 71.
[126] იხ. Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), of 27 April 2016, 36.
[127] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მუხლი 17.
[134]<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/security/> 07.05.2020.

გათვალისწინებულ იქნეს რისკის ანალიზი, ორგანიზაციული პოლიტიკა და ფიზიკური და ტექნიკური ზომები[134]. GDPR არ განსზღვრავს უსაფრთხოების ზომებს, რომელიც უნდა ჰქონდეს დამმუშავებელს, ის მოითხოვს უსაფრთხოების ისეთ დონეს, რომელიც შესაბამისია დამუშავების რისკებთან. უსაფრთხოებისთვის დამმუშავებელმა აუცილებლად უნდა გაითვალისწინოს, პერსონლურ მონაცემებზე წვდომის მოცულობა და სუბიექტი, რომელიც გამოიყენებს დამუშავებულ მონაცემებს (დასაქმებული პირი/თანამშრომელი).

GDPR-ის მიხედვით მონაცემების უსაფრთხოებისათვის გამოიყენება მონაცემთა ფსევდონიმიზაცია და ანონიმიზაცია[128]. ფსევდონიმიზაცია ეს არის მონაცემთა დაშტრიხვას და ჩანაცვლებას ფსევდონიმებით[129], ხოლო ანონიმიზაცია გულისხმობს დამუშავების შემდეგ მონაცემების შენახვას ანონიმური სახით, ისე რომ დამუშავების თავდაპირველი მიზანს აღარ ემსახურებოდეს, საბოლოოდ ანონიმიზაციით მონაცემებიდან ამოიღება ისეთი მონაცემები რომლებითაც პირის იდენტიფიცირება ხდებოდა[137]. მონაცემთა უსაფრთხოდ დამუშავება ქმნის კონფიდენციალურობის წინაპირობას. სწორედ კონფიდენციალურობის და პერსონალური მონაცემების დაცვის მიზნით გაამართლა მოპასუხე მხარემ ექსპერტის ვინაობის (სახელის და გვარის) გასაიდუმლოება[130]. უსაფრთხოების დარღვევაზე მიუთითებს პერსონალურ მონაცემთა დაცვის ინსპექტორი, როდესაც დამსაქმებლები სამართალდამცავ ორგანოებს, პროკურორის დადგენილების და სასამართლოს განჩინების გარეშე გადასცემენ მონაცემებს, და ასევე არ აღრიცხავენ ტექნიკური საშუალებებით, ამ

[128] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი 2018, 148, ასევე გვ.108.
[129] იხ. იქვე გვ, 148.
[137] იხ, იქვე გვ. 108.
[130] საკონსტიტუციო სასამართლოს 2017 წლის 27 მარტის გადაწყვეტილება N:1/4/757 საქმეზე „საქართველოს მოქალაქე გიორგი კრავეიშვილი საქართველოს მთავრობის წინააღმდეგ“, პარაგრაფი N: 10.

შემთხვევაში აუდიოვიდეო ჩანაწერებით მოპოვებულ მონაცემებს[131], ასევე ხაზგასასმელია, რომ მონაცემთა უსაფრთხოების დაცვასთან დაკავშირებით მოთხოვნების შეუსრულებლობის დადგენისათვის აუცილებელი არ არის სამართლებრივი შედეგის - მონაცემთა უკანონო დამუშავების ფაქტის დადგომა, საკმარისია მონაცემთა დამმუშავებელმა არ გაითვალისწინოს მონაცემთა დამუშავებასთან დაკავშირებული რისკები და თავის ქმედებით ან უმოქმედობით შექმნას მონაცემთა უკანონო დამუშავების საფრთხე[132]. უსაფრთხოების პრინციპისთვის დამახასიათებელია: ა) ქმნის თავდაცვის გარანტიებს დამუშავების სუბიექტებისთვის; ბ) დადებით გავლენას ახდენს დამმუშავებელზე, რადგან ახალი კანონის პეროექტის მიხედვით სწორედ დამმუშვებელი არის ანგარიშვალდებული და პასუხისმგებელი მონაცემების დამუშავებაზე; გ) ქმნის უსაფრთხოების ზომებისთვის საჭირო საშულებებს, იქნება ეს ტექნიკური თუ ორგანიზაციული; დ) დამუშავების დაწყებისას წინასწარ ავალდებულებს დამმუშავებელს გაითვალისწინოს უსაფრთხოების რისკები, რომელიც ადეკვატური უნდა იყოს, რაც შემდგომ დაეხმარება მას მონაცემთა კანონის შესაბამისად დამუშავებაში; ე) აღნიშნული პრინციპიდან გამომდინარე დამმუშავებელმა უნდა შეზღუდოს მონაცემებეზე წვდომა; ვ) დამმუშავებელმა მონაცემთა უსაფრთხოებისათვის გათვალისწინებული საშუალებების გამოყენებისას უნდა გაითავლისწინოს მონაცემების მოცულობა და, ასევე, მოსალოდნელი შედეგი. დამსაქმებელთან უსაფრთხოების ზომის მისაღებად აუცილებელია არსებობდეს ერთი ადამიანი, რომელიც სრულად იქნება პასუხისმგებელი მონაცემთა უსაფრთხო დამუშავებაზე[141].

---

[131] საქართველოს პერსონალურ მონაცემთა დაცვის ისნპექტორის 2017 წლის 25 მაისის გადაწყვეტილება, შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N: გ-1/286/2017, გვ.8, ასევე საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის გადაწყვეტილება შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N: გ-1/314/2017, გვ.9.

[132] საქართველოს პერსონალურ მონაცმეთა დაცვის ინსპექტორის 2018 წლის 26 დეკემბრის გადაწყვეტილება სს „ა“-ს შემოქმების დასრულების შესახებ, საქმე N: გ-1/701/2018, გვ. 9.

[141] <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-..regulation-gdpr/security/> 07.05.2020.

უსაფრთხოების პრინციპი შრომითი ურთიერთობებისთვის აუცილებელი და საჭიროდ განსახორციელებელია დამმუშავებლის მიერ, ვინაიდან თუ მონაცემთა დამუშავების, დამუშავებული მონაცემების შენახვის და შემდეგ მისი განადურებისას, უსაფრთხოების სათანადო ზომები იქნება დაცული, მონაცემთა კანონიერად და სამართლიანად დამუშავების გარანტია უფრო მეტად გაიზრდება, შესაბამისად დამმუშავებელს აარიდებს არასასურველ და უარყოფით შედეგებს, რომელიც შესაძლოა მონაცემთა დამუშავების პროცესს მოყვეს.

2.1.5. მონაცემთა დამმუშავებლის მიერ ანგარიშვალდებულებისა და გამჭვირვალობის დემონსტრირება

ნაშრომის დასაწყისში აღინიშნა, რომ GDPR-ით გათვალისწინებული მოთხოვნების შესაბამისობაში მოყვანის მიზნით საქართველოს პარლამენტში წარდგენილია კანონის პროექტი, რომელიც მნიშვნელოვანია არა მხოლოდ იმიტომ, რომ ის პასუხობს საერთაშორისო გამოწვევებს, არამედ იმიტომაც, რომ კანონის პროექტთ განისაზღვრა მონაცემთა დამმუშავებელთა წრე. მოქმედი კანონმდებლობის მიხედვით მონაცემთა დამმუშავების მარეგულირებელი ნორმები მხოლოდ საჯარო პირებზე ვრცელდებოდა, ხოლო კანონის პროექტის მიხედვით დაემატა კერძო პირების მიერ მონაცემთა დამუშავებაც. ასევე მნიშვნებლოვანია ისიც, რომ კანონის პროექტით განისაზღვრა მონაცემთა დამუშავების კანონიერების უზრუნველყოფის მიზნით დამმუშავებლის ანგარიშვალდებულობის და გამჭირვალობის პრინციპის დემონსტრირების აუცილებლობა. „მონაცემთა დამმუშავებელი პასუხისმგებელია მონაცემთა დამუშავების ამ მუხლით განსაზღვრული პრინციპების დაცვაზე და უნდა შეეძლოს მათთან

შესაბამისობის დემონსტრირება“ [133] . „ანგარიშვალებულება მოითხოვს მონაცემთა დამუშავებლისა და უფლებამოსილი პირის მიერ იმ ზომების აქტიურად და მუდმივად გატარებას, რომლებიც ხელს შეუყოფს და განამტკიცებს მონაცემთა დაცვას დამუშავების პროცესში“ [134] . ანგარიშვალებლობის პრინციპი გულისხმობს, რომ მონაცემთა დამმუშავებელს და უფლებამოსილ პირს უნდა ჰქონდეთ სათანადო პასუხისმგებლობა აღებული დამუშავების პრინციპების დაცვასთან და დამუშავების წესებთან დაკავშირებით, რათა ნებისმიერ დროს უნდა შეძლონ მონაცემთა დაცვასთან შესაბამისობის დემონსტრირება. რა არის საჭირო იმისათვის, რომ შრომით სახელშეკრულებო ურთიერთობების დროს დამსაქმებელმა გააკეთოს ანგარიშვალებულობის დემონსტრირებისთვის? ეს შეიძლება გამოიხატოს სხვადასხვა ქმედებაში: ა) დამუშავებული მონაცემების აღრიცვხაში, მიზნის შესაბამისობასთან მიმართებაში (თანამშრომლების დაწინაურება, სერთიფიცირება, ტესტირება, ჯანმრთელობის დაცვა, მონიტორინგი, ტრენინგები და ა.შ); ბ) ყველა მონაცემები უნდა იყოს სათანადო წესით შენახული, ისე რომ მასზე წვდომა შეიძლებოდეს მხოლოდ დამსაქმებლის, ან მის მიერ არჩეული ნდობით აღჭურვილი პირის მიერ (ხელშეკრულების საფუძვლით); გ) მიღებულ უნდა იქნეს უსაფრთხოების ზომები მონაცემთა გამჟღავნების თავიდან ასაცილებლად (მაგალითად შესაბამისი ბაზებზე წვდომა უნდა შეიძლებოდეს კოდური სიტყვებით, ან ციფრების კომბინაციით, ხელშეკრულებაში უნდა ჩაიწეროს, თუ როდის დაიშვება მონაცემთა გაცემა, და რის საფუძველზე); დ) წინასწარ გათვალისწინებულ უნდა იქნეს რისკები, რაც შესაძლოა მოჰყვეს დამუშავებას, ე) მუდმივი კონტაქტი უნდა იქონიოს სახელწიფო ინსპექტორის აპარატთან; ვ) ყველა ზემოთ აღნიშნული მოქმედება შესაბამისი ფორმით და დოკუმენტურად უნდა ჰქონდეს

[133] პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის პროექტი, მუხლი 4, პუნქტი 3.

[134] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი, 2018, 152.

გაფორმებული. დამმუშავებელი არ უნდა დაელოდოს ხარვეზზე მითითებას, საზედამხედველო ორგანოსგან ან სუბიექტისგან [135] , გამჭირვალობის პრინციპი მოითხოვს, რომ ნებისმიერი ინფორმაცია და კომუნიკაცია რომელიც დაკავშირებულია მონაცემთა დამუშავებასთან მარტივად ხელმისაწვდომი და გასაგები იყოს დამუშავების სუბიქტისათვის[136].

2.2. მონაცემთა დამუშავების აუთსორსის ურთიერთმიმართება დამუშავების პრინციპებთან

მონაცემთა დამუშავების ძირითადი სუბიექტები არიან, დამმუშავებელი (შრომით ურთიერთობებში ეს არის დამსაქმებელი), მონაცემთა დამუშავების სუბიექტი (შრომით ურთიერთობებში დასაქმებული) და უფლებამოსილი პირი, რომელიც დამმუშავებელთან დადებული ხელშეკრულების საფუძველზე მოქმედებს და ამუშავებს მონაცემებს.

უფლებამოსილი პირის ჩართვა დამუშავების პროცესში აუცილებელი არაა, თუმცა, ზოგიერთ შემთხვევაში, იგი „ეხმარება“ დამმუშავებელს მონაცემთა დამუშავებაში. ხშირია შემთხვევები, როდესაც ორგანიზაცია საკუთარი დასაქმებულების შესახებ მონაცემებს ამუშავებს აუთსორსის (გარე-წყაროს) დახმარებით, რამდენადაც ეს უკანასკნელი მეტად კომპეტენტურია პირადი საქმეების მართვის მიმართულებით. ასეთი შემთხვევები, ძირითადად, ხშირია მცირე და საშუალო ბიზნესის წარმომადგენლებთან, თუმცა არ არის გამორიცხული სხვა, მეტად მსხვილ კომპანიებთან.

ამდენად, შრომითი ურთიერთობებისთვის ხშირია უფლებამოსილი პირის მიერ მონაცემთა დამუშავების შემთხვევები. უფლებამოსილი პირი მონაცემთა დამუშავების დაწყების მომენტიდან სარგებლობს

[135] იხ. იქვე 155.

[136] <https://www.dataprotection.ie/en/individuals/principles-data-protection> 02.03.2020.

დამმუშავებლის მიერ მინიჭებული უფლებამოსილებით და დადგენილ ფარგლებში. ამდენად, შრომითსამართლებრივ ურთიერთობებში უფლებამოსილი პირის ჩართვა კარგი გზაა, რათა დამმუშავებელმა დაზოგოს რესურსი და მეტად ეფექტურად უზრუნველყოს საკუთარი მიზნების მიღწევა, მაგრამ დადებითთან ერთად უარყოფითი შედეგიც შეიძლება დადგეს, თუ დამსაქმებლის მხრიდან ხელშეკრულებით ზუსტად არ იქნება უფლებამოსილი პირის უფლება-მოვალეობები განსაზღვრული. პერსონალურ მონაცემთა დაცვის ინსპექტორმა სამართალდარღვევად გამოაცხადა დამსაქმებლის ქმედება, როდესაც დავალების ხელშეკრულება არ მოიცავდა ნათელ და მკაფიო მითითებებს უფლებამოსილი პირის მიერ მონაცემთა დამუშავების სპეციალურ წესებზე და აკრძალვებზე[146], ასევე მომსახურების ხელშეკრულება, რომელიც არ ითვალისწინებდა უფლებამოსილი პირის მხრიდან პერსონალური მონაცემების უსაფრთხოების დაცვის ვალდებულებებს და გარანტიებს[147].

შრომით სამართლებრივი ურთიერთობებში ხშირია ასევე შემთხვევები, როდესაც დამუშავების სუბიექტს გონია, რომ მის პერსონალურ მონაცემებს ამუშავებს დამსაქმებელი, მაგრამ რეალურად მისთვის ცნობილი არაა მონაცემთა დამუშავების აუთსორსთან დაკავშირებით. როდესაც დამუშავების პროცესში ერთვება აუთსორსი კომპანია დამმუშავებელთან დადებული ხელშეკრულების საფუძველზე, ხდება მონაცემთა ძირითადი დამმუშავებელი, შესაბამისად ყველა უფლება-მოვალეობით სარგებლობს რომლითაც დამმუშავებელი, და მონაცემთა დამუშავების ყველა პრინციპის დაცვით უნდა დაამუშავოს მონაცემები.

[146] იხ. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 21 აპრილის გადაწყვეტილება, მ.ა-ს განცხადების განხილვის დასრულების შესახებ, საქმე N: გ-1/210/2017, გვ.8.

[147] იხ. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის 26 დეკემბრის გადაწყვეტილება სს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-1/701/2018, გვ.4.

2.2.1. დამმუშავებლის ვალდებულებები აუთსორსის წინარე პერიოდსა და მიმდინარე პროცესში

დამმუშავებელსა და უფლებამოსილ პირს შორის ურთიერთობა იწყება სამართლებრივი აქტის ან ხელშეკრულების საფუძველზე [137] . რომელი საფუძვლითაც არ უნდა დაიწყოს სამართლებრივი ურთიერთობა, აუცილებელია წინასწარ დეტალურად გაიწეროს უფლება-მოვალეობები დამმუშავებლის მიერ. უფლებამოსილი პირი მოქმედებს მხოლოდ დავალების/მომსახურების ხელშეკრულების საფუძველზე, ამიტომ მონაცემთა კანონიერი და უსაფრთხო დამუშავებისთვის აუცილებელია აგრეთვე ხელშეკრულების პირობები იყოს კონკრეტული და დეტალური. აუცილებელია: ა) არსებობდეს მონაცემთა დამუშავების მიზანი; ბ) დამუშავების ფარგლები; გ) დამმუშავებლის თანხმობის გარეშე მონაცემების გადაცემის აკრძალვის დაუშვებლობა; დ) დავის შემთხვევაში დამუშავებული მონაცემების დამმუშავებლისთვის გადაცემა; ე) საქმიანობის გაუქმების ან საქმიანობის შეწყვეტისას, გაუქმებამდე ან შეწყვეტამდე ყველა მონაცემის გადაცემის ვალდებულება დამმუშავებლისთვის [138] [139] [49]. „უფლებამოსილ პირთან დადებული ხელშეკრულება მკაფიოდ და ნათლად უნდა ადგენდეს უფლებამოსილი პირის, მათ შორის მონაცემთა დამმუშავებლის ვალდებულებებს, პერსონალური მონაცემების დამუშავებასთან დაკავშირებით“[140]. საქართველოს უზენაესმა სასამართლომ ერთ-ერთ გადაწყვეტილებაში აღნიშნა, რომ მოპასუხეს, როგორც უფლებამოსილ პირს, რამდენადაც იგი მოქმედებდა დამსაქმებლის მიერ მინიჭებული უფლებამოსილების ფარგლებში (ხელშეკრულების

[137] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მუხლი 16, პუნქტი [138] .

[139] იხ, იქვე მუხლი 16, პუნქტი 1-7.

[140] საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 21 აპრილის გადაწყვეტილება, მ.ა-ს განცხადებასთან დაკავშირებული განხრილვის დასრულების შესახებ, საქმე N: გ-1/210/2017, გვ. 9.

შესაბამისად) ევალებოდა ხელშეკრულების შესაბამისად უფლებამოსილ პირსა და დამმუშავებელს შორის კონფიდენციალობის ვალდებულება, უფლებამოსილ პირს არ უნდა ემოქმედა კონკრეტული სახელშეკრულებო ვალდებულების ფარგლებს გარეთ, მონაცემთა დამუშავების შემთხვევაში, წინასწარ უნდა მოეპოვებინა თანხმობა დამმუშავებლისგან ,რადგან ეს სცილდება დამმუშავებლის (დამსაქმებლის) მანდატს, ანუ დასაქმებულის პერსონალური მონაცემების გამჟღავნებისთვის წინასწარ წერილობითი თანხმობა უნდა მოეპოვებინა, როგორც დამსაქმებლისგან, ასევე მონაცემთა სუბიექტისგან
(დასაქმებულისგან)[141].

ვინაიდან შრომითი ურთიერთობები სპეციფიკურია თავისი ბუნებიდან გამომდინარე, და მონაცემთა დიდი რაოდენობა მუშავდება დამსაქმებლის მხრიდან, აუცილებელია უფლებამოსილი პირის საქმიანობის კონტროლი, შემოწმება განხორციელდეს გარკვეული ინტენსივობით, რომელიც დამსაქმებელმა უნდა განსაზღვროს. უსაფრთხოების სტანდარტები დამმუშავებლის მხრიდან წინასწარ უნდა განისაზღვროს წერილობითი ფორმით, იქნება ეს აუდიტის ჩატარების უფლება, თუ დამუშავების შემოწმების საჭიროება[142].

მომსახურების/დავალების ხელშეკრულება აუცილებელია იყოს დეტალური, მასში აუცილებლად უნდა ჩაიწეროს: ა) დამუშავების საფუძველი; ბ) დამუშავების მიზნები; გ) დამუშავების მოცულობა და ფარგლები; დ) დამუშავების ვადა; ე) ახალი მიზნით დამუშავებაზე დამუშავების სუბიექტის ინფორმირება კანონის შესაბამისად; ვ) დამმუშავებლისათვის ინფორმაციის მიწოდების ვალდებულება, როგორც დამუშავების დაწყების და მიმდინარეობის დროს, ასევე დასრულების შემდეგ; ზ) მითითება ანგარიშვალდებულობაზე მონაცემთა დამუშავებისას; თ) დამუშავების შეწყვეტისას მონაცემების გადაცემის ვალდებულება

[141] საქართველოს უზენაესი სასამართლოს 2015 წლის 22 მაისის გადაწყვეტილება საქმე N: ას-243-230-2015.

[142] იხ. Rosemary J., Clarke J., Data Protection Compliance in the UK, United Kingdom, 2010, 32.

დამმუშავებლისთვის; ი) დამმუშავებლის პასუხისმგებლობის ფარგლები უფლებამოსილი პირის მიერ ვალდებულების დარღვევისას; კ) უფლებამოსილი პირის პასუხისმგებლობის ზომები ხელშეკრულებით დადგენილი პირობების დარღვევისას.

დამმუშავებელსა და აუთსორს კომპანიას შორის დადებული ხელშეკრულება არის კერძო სამართლებრივი ხასიათის, რომელიც სამართლის სუბიექტებს შორის თანასწორუფლებიანობის საფუძველს ქმნის [143] , ხოლო ასეთი ურთიერთობისთვის დამახასიათებელია კეთილსინდისიერების პრინციპი, და დაუშვებელია არა მხოლოდ ის, რომ ვალდებულების შესრულება ხდება მიუღებელი ქმედებით, არამედ იგი იცავს სამართლებრივი ურთიერთობის მონაწილეების ნდობას სამოქალაქო ბრუნვის შესახებ, რომ არ მოხდეს სამართლებრივი უფლებების ბოროტად გამოყენება[144]. უფლებამოსილი პირი და მასთან მომუშავე თანამშრომელი, ვალდებულია არ გასცდეს მისთვის მინიჭებულ უფლებამოსილებას, და დაიცვას მოპოვებული მონაცემების საიდუმლოება, საქმიანობის შეწყვეტის შემდეგაც[145][146].

2.2.2. მონაცემთა აუთსორსი მონაცემთა საერთაშორისო გადაცემის კონტექსტში

მონაცემთა ტრანს საზღვრო გადაცემა, ანუ სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისათვის გადაცემად ითვლება მონაცემთა გადაცემა ისეთი მიმღებისათვის, რომელზეც არ ვრცელდება საქართველოს იურისდიქცია [147] . მიმდინარე შრომითი ურთიერთობებიც არ არის გამონაკლისი, რადგან ისეთი უცხოური კომპანიები რომელთა იურიდიული

[143] თოლთლაძე ლ., გაბრიძიძე გ., თუმანიშვილი გ., ტურავა პ., ჩაჩანიძე ე., განმარტებითი იურიდიული ლექსიკონი, თბილისი 2012, 253.
[144] იქვე გვ.252.
[145] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მუხლი 17, პუნქტი [146] .
[147] < https://personaldata.ge/ka/orginnerpage8> 02.05.2020.

მისამართი არ არის საქართველოში ხშირად ითხოვენ მათ კომპანიაში დასაქმებულ პირთა შესახებ მონაცემების მიწოდებას. აღნიშნულს მოწმობს ისიც, რომ სახელმწიფო ინსპექტორის სამსახურმა 2019 წელს მონაცემთა გადაცემის შესახებ 14 განაცხადი განიხილა, 11 შემთხვევაში სახელმწიფო ინსპექტორის სამსახურს მიმართა კერძო ორგანიზაციაამ, 1 შემთხვევა იყო საჯარო დაწესებულება, ხოლო 2 შემთხვევა უცხოური არასამეწამეო იურიდიული პირის ფილიალი, ძირითადი მოთხოვნა კი იყო დასაქმებული პირების ან/და კლიენტების პერსონალური მონაცემების გადაცემა [148] . გადაცემის დროს, ის სახელმწიფოები, ორგანიზაციები თუ კერძო კომპანიები, რომლებსაც გადაეცემა დასაქმებულ პირთა მონაცემები ირიბად გულისხმობს უფლებამოსილი პირის მიერ მონაცემთა დამუშავებას, ვინაიდან ინფორმაციის გადაცემის დროს ისინი ამუშავებენ შესაბამისი მიზნით მონაცემებს. მონაცემთა საერთაშორისო გადაცემის დროს გადამცემი და გადასაცემი სახელმწიფოს ეროვნული კანონების მიახლოებამ არ უნდა გამოიწვიოს სუბიექტთა დაცული უფლებების შემცირება, არამედ პირიქით უნდა შეეცადოს ეს უფლებები დაიცვას[158].

სახელმწიფო ინსპექტორის სამსახურის მიერ გამოცემულია სახელმძღვანელო, რომელიც დეტალურად განიხილავს ხელშეკრულებით გათვალისწინებული საერთაშორისო გადაცემის დროს განცხადების შევსების, მისი განხილვის და გასაჩივრების წესს [149] . სახელმწიფო ინსპექტორის მიერ ასევე მიღებულია პერსონალურ მონაცემთა სათანადო გარანტიების მქონე ქვეყნების ნუსხა[150].

---

[148] სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში, თბილისი, 2019, 81. [158] CEJU, Joined cases C-468/10 and C-469/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) And Federación de Comercio Electrónico y Marketing Directo (FECEMD) V Administración del Estado, 24 Noember, 2011, Article 28.

[149] იხ. სახელმწიფო ინსპექტორის სამსახურის სახელმძღვანელო სხვა სახელმწიფოსათვის ან სახელმწიფო იურისდიქციის ქვეშ მყოფი იურიდიული ან ფიზიკური პირისათვის ან საერთაშორისო ორგანიზაციისთვის პერსონალურ მონაცემთა გადაცემის შესახებ პერსონალურ მონაცემთა დაცვის ინსპექტორის ნებართვის მისაღებად წარსადგენი განცხადების შევსების, განცხადების განხილვის ვადების და შედეგის გასაჩვრების წესის შესახებ, თბილისი, 2019 .

[150] იხ. <http://newadmin.personaldata.ge/wp-content/uploads/2018/09/white-list_final-1.pdf> 02.05.2020.

აღნიშნულ დოკუმენტში ჩამოთვლილი ქვეყნების ზოგიერთი ნაწილი არ შედის ევროკავშირის შემადგენლობაში, მაგრამ სახელმწიფო ინსპექტორის სამსახური მიიჩნევს, რომ ეს იმ ქვეყნების ძირითადი ჩამონათვალია, რომელთა მხრიდან მონაცემთა გადაცემისას იქნება სათანადო უსაფრთხოების ზომები მიღებული. მიუხედავად ამისა, მიმდინარე შრომითი ურთიერთობების დროს დამმუშავებელმა უნდა გაითვალისწინოს და შეაფასოს მონაცემთა დამუშავების რისკების ადეკვატურობა. დამმუშავებელმა განსაკუთრებით უნდა გაითვალისწინოს: ა) გადასაცემ მონაცემთა დამუშავების მიზნები; ბ) გადასაცემ მონაცემთა მოცულობა; გ) მიმღები სუბიექტის მიერ მიღებული უსაფრთხოების ზომები დ) მიმღები სუბიექტის კანონმდებლობა და შესაბამისი პრაქტიკა მონაცემთა გადაცემის დროს; ე) დარღვევის შემთხვევაში აღსრულების წესი. აღნიშნულთან ერთად აუცილებელია განისაზღვროს თუ რა სახის პერსონალური მონაცემი უნდა გადაეცეს სუბიექტს, და არსებობს თუ არა ამ გადაცემის საფუძველი.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიხედვით, მონაცემთა გადაცემის დროს აუცილებელია არსებობდეს გადაცემის საფუძველი, მონაცემთა დაცვის გარანტიები იყოს უზრუნველყოფილი მიმღები და გადამცემი სუბიექტის მხრიდან, ასევე შესაძლებელია თუ საერთაშორისო შეთანხმებით ან ხელშეკრულებით არის გათვალისწინებული გადაცემა, და ასევე დამმუშავებელი თუ შექმნის მონაცემთა დაცის სათანადო გარანტიებს[151].

მონაცემთა დაცვის ძირითადი რეგულიაცია (GDPR) იცავს პირადი მონაცემების გადაცემას, რაც ნიშნავს, რომ ორგანიზაციებს არ შეუძლიათ პირადი მონაცემების გადაცემა ევროპული ეკონომიკური ზონის გარეთ[162]. პირველი, რაც მიმდინარე შრომითი ურთიერთობის დროს დამმუშავებელმა უნდა გაითვალისწინოს მესამე ქვეყანაში პერსონალური მონაცემების გადაცემისას არის თუ რამდენად ადეკვატურია მესამე ქვეყანა ან

[151] იხ. პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მუხლი 41.
[162] <https://www.lexology.com/library/detail.aspx?g=8aa887fd-1103-4a98-aa13-0137215b2b19> 03.05.2020.

საერთაშორისო ორგანიზაცია (უზრუნველყფილ იქნება თუ არა მონაცემთა დაცვის ადეკვატურობა) [152] . დაცვის ადეკვატურობისთვის ევროკომისია ითვალისწინებს ისეთ ელემენტებს, როგორიც არის კანონი, ადამიანის უფლებების და თავისუფლებების პატივისცემა, ეროვნული უსაფრთხოება, მონაცემთა დაცვის წესები, მონაცემთა დაცვის ორგანოს არსებობის სავალდებულოობა [153] . თუ მონაცემები გადაიცემა ადეკვატურ ქვეყანაში, მაშინ გადაცემა შესაძლებელია გარანტიების დაწესების გარეშე, ამჟამად სიაში შედის კანადა, ისრაელი, ახალი ზელანდია და შვეიცარია, სია მუდმივ განახლებს განიცდის ევროკომიის მხრიდან[154].

მიმდინარე შრომით ურთიერთობებში, როდესაც დამსაქმებლის მხრიდან ხდება დასაქმებული პირების შესახებ მონაცემების საერთაშორისო გადაცემა აუცილებელია განცხადებით მიმართოს სახელწიფო ისნპექტორს, და თანხმობა მიიღოს. დამსაქმებელმა უნდა დაასაბუთოს მონაცემების გადაცემის აუცილებლობა და ასევე წინასწარ უნდა შეფასდეს მისი მხრიდან დაცვის ადეკვატურობა. „პერსონალურ მონაცემთა დაცვის არსი სწორედ იმაში მდგომარეობს, რომ კანონმდებლობამ შექმნას რეალური შესაძლებლობა, პრევენცია იმიას, რომ უკანონო საშუალებების გამოყენებით პირმა არ განიცადოს ზიანი“ [155] . „ევროკავშირის რეგულაცია წევრი ქვეყნებისთვის არ არის ერთმნიშვნელოვნად ამკრძალავი სამართლებრივი აქტი, მონაცემთა გადაცემის კუთხით მესამე ქვეყანასთან მიმართებაში, მაშინაც კი, როდესაც ეს სახელმწიფოები ვერ უზრუნველყოფენ მონაცემთა სათანადო დაცვას“[156].

---

[152] <https://www.dataprotection.ie/en/organisations/international-transfers> 03.05.2020.

[153] <https://www.dataprotection.ie/en/organisations/international-transfers> 03.05.2020, ასევე Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), of 27 April 2016, Article 45.

[154] <https://www.lexology.com/library/detail.aspx?g=8aa887fd-1103-4a98-aa13-0137215b2b19> 03.05.2020.

[155] ლაფარაშვილი ი., პერსონალურ მოაცემთა საერთაშორისო გადაცემის სამართლებრივი მოწესრიგება ქართული და ევროპული სტანდარტების მიხედვით, თბილისი, 2018, 17.

[156] იქვე, გვ 35.

3. მონაცემთა დაცვის ოფიცერი, როგორც დამუშავების ანგარიშვალდებულების პრინციპის რეალიზების ეფექტური გზა

მას შემდეგ რაც დამსაქმებელსა და დასაქმებულს შორის იდება შრომითი ხელშეკრულება, დამსაქმებელს აქვს უფლება დაამუშავოს დასაქმებულის პირადი მონაცემები საჭირო მიზნებიდან გამომდინარე. სასამართლო გადაწყვეტილებებით, სახელწიფო ინსპექტორის ყოველწლიური ანგარიშებით და მის მიერ გამოტანილი გადაწყვეტილებების ანალიზი ცხადყოფს, რომ მიუხედავად კანონის არაერთი ჩანაწერისა, რომ მონაცემები უნდა დამუშავდეს კანონიერი და უსაფრთხო გზით არაერთი დარღვევა იკვეთება დამსაქმებლების მხრიდან. უსაფრთხოების და ანგარიშვალდებულობის, გამჭირვალობის პრინციპის რეალიზება შრომით სახელშეკრულებო ურთიერთობებისთვის ძალიან მნიშვნელოვანია. მონაცემთა უსაფრთხო და კანონიერი გზით დამუშავება დადებითი აღმოჩნდება, როგორც დამსაქმებლის ასევე ნებისმიერი სხვა პირისათვის, რომელიც დამუშავების პროცესში იქნებიან ჩართულები. ზემოთ არაერთხელ აღინიშნა, რომ საქართველოს პარლამენტში წარდგენილია „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის პროექტი, რომელის საფუძველზეც არაერთი ცვლილება იგეგმება კანონში. კანონის პროექტი მონაცემთა დაცვის კანონიერების უზრუნველყოფის მიზნით, შედარებით მსხვილ ორგანიზაციებში ითვალისწინებს პერსონალურ მონაცემთა დაცვის ოფიცრის პოზიციის განსაზღვრას. კანონის პროექტით, პერსონალურ მონაცემთა დაცვის ოფიცერი არის მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის მიერ განსაზღვრული/დანიშნული პირი, რომელიც ახორციელებს შესაბამის უფლებამოსილებებს [157] . ის ორგანიზაციები, რომლებსაც ევალებათ განსაზღვრონ ოფიცერი არის: საჯარო დაწესებულება, (გარდა რელიგიური და პოლიტიკური ორგანიზაციებისა),

[157] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი მუხლი 3, პუნქტი ღ.

სადაზღვეო ორგანიზაცია, კომერციული ბანკი, მიკროსაფინანსო ორგანიზაცია საკრედიტო ბიურო, ელექტრონული კომუნიკაციის კომპანია, ავიაკომპანია, აეროპორტი, და ის სამედიცინო დაწესებულება რომელიც მომსახურებას უწევს წელიწადში 10000 მონაცემთა სუბიექტს, ასევე ის დამმუშავებელი/უფლებამოსილი პირი, რომელიც ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან ახორციელებს მათი ქცევის სისტემურ და მასშტაბურ მონიტორინგს[158]. ამდენად, პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულება გაიწერება კანონმდებლობით, რაც გავრცელდება როგორც საჯარო, ასევე კერძო სექტორზე, სადაც დიდი რაოდენობით მონაცემები მუშავდება. მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულება გავრცელდება, აგრეთვე უფლებამოსილი პირის მიერ მონაცემთა დამუშავებაზე, რაც უმნიშვნელოვანესია შრომითი ურთიერთობებისთვის, სადაც ხშირია შემთხვევები უფლებამოსილი პირების მიერ მონაცემთა დამუშავებისა. დამსაქმებლები, რომლებიც დიდი რაოდენობით მონაცემებს ამუშავებენ ვალდებულნი იქნებიან მონაცემთა დაცვის ოფიცერს მიაწოდონ მონაცემთა დამუშავების ყველა ეტაპის შესახებ ინფორმაცია, რაც დამუშავების ეტაპს მეტად ეფექტურს და უსაფრთხოს გახდის.

„მონაცემთა დაცვის ოფიცერი (DPO) არის პირი, რომელიც დამმუშავებელ ორგანიზაცის აწვდის რჩევებს, მონაცემთა დაცვის წესებთან შესაბამისობაზე, ის „ანგარიშვალებულობის ქვაკუთხედია“, ვინაიდან ხელს უწყობს შესაბამისობას, და, ამავდროულად, მოქმედებს, როგორც შუამავალი საზედამხედველო ორგანოებს, მონაცემთა სუბიექტებს, და დამნიშნავ ორგანიზაციას შორის, ხოლო ანგარიშვალდებულობის პრინციპი განსაკუთრებით მნიშვნელოვანია, ევროკავშირის მონაცემთა წესების აღსრულებისათვის [159] . უფლებამოსილების განხორციელებისას აუცილებელი არ არის მონაცემთა დაცვის ოფიცერი მხოლოდ იურიდიული

[158] იქვე მუხლი 33, პუნქტი 1.

[159] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი 2018, 198.

პრაქტიკის შესაბამისად ასრულებდეს უფლებამოსილებას, ეს პოზიცია მოითხოვს შერეული, მათ შორის ექსპერტის ცოდნის აუცილებლობასაც[160], ასევე მან უნდა იცოდეს მონაცემთა დამუშავების ყველა მეთოდი, როგორებიც არის ავტომატური, ნახევრად ავტომატური და არაავტომატური მეთოდები[161].

მნიშვნელოვანია, აგრეთვე მონაცემთა დამუშავების მოცულობის განსაზღვრის საკითხიც. მაგალითად ჰოლანდიაში საავადმყოფოების და აფთიაქების მიერ მონაცემთა დამუშავება ყოველთვის განიხილება „ფართომასტაბიან“ დამუშავებად, თუ მონაცემთა დამუშავება მოიცავს 10000 რეგისტრირებული პაციენტის მონაცემებს, რომელიც ერთ სისტემაში იყრის თავს, ხოლო ჩეხეთის მონაცემთა დაცვის ორგანოს მიღებული გადაწყვეტილების შესაბამისად, „დიდი მასშტაბის“ დასადგენად აუცილებელია დამუშავებაში ჩართული იყოს 10000 მონაცემთა დამუშავების სუბიექტი, და მონაცემებს ამუშავებდეს 20-ზე მეტი ფილიალი.[162]

მონაცემთა დაცვის ოფიცრის დანიშვნას ითვალისწინებს GDPR-ის 37-39 მუხლები[163]. კანონის პროექტის მიხედვით მონაცემთა დაცვის ოფიცრის უფლებამოსილებებია: ა) დამმუშავებლის და უფლებამოსილი პირის მონიტორინგი; ბ) დოკუმენტების სისწორეზე და შესაბამისობაზე მონიტორინგი; გ) დამმუშავებლის და უფლებამოსილი პირის ინფორმირება, დ) კონსულტაციების მიღება და შესრულების კონტროლი (სახელმწიფო

[160] იხ. Goshadze k., The Data Protection Officer (DPO)- ensuring greater Data Protection compliance, იოსებ კელენჯერიძის, ზურაბ ჭყონიას, ნათია გაბედავას, ნატო გიგაურის, მარიამ ბობოხიძის და თამარ ქავჭარაძის რედაქტორობით, თბილისი., 2020, 43.

[161] იხ. იქვე გვ.44

[162] იხ. Goshadze k., The Data Protection Officer (DPO)- ensuring greater Data Protection compliance, იოსებ კელენჯერიძის, ზურაბ ჭყონიას, ნათია გაბედავას, ნატო გიგაურის, მარიამ ბობოხიძის და თამარ ქავჭარაძის რედაქტორობით, თბილისი., 2020, 43, იხ. ციტირება Breitbarth, P. (2018). On lang Scale Data Processing and GDPR Comlpiance [https://iapp. org/news/a/on-large-scale-data-processing-andgdpr-compliance/].

[163] იხ. Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), of 27 April 2016, Article 37-39.

ინსპექტორის სამსახურისგან); ე) წარმომადგენლობითი უფლებამოსილება სახელმწიფო ინსპექტორის აპარატთან; ვ) მითითებების და რეკომენდაციების შესრულებაზე მონიტორინგი; ზ) მონაცემთა დამუშავების სუბიექტისთვის ინფორმაციის მიწოდება; თ) ანაგრიშვალებულობა დამმუშავებლის და უფლებამოსილ პირთან[164].

მონაცემთა დაცვის ოფიცრის დანიშვნა დამსაქმებელს გარანტიას მისცემს, დამუშავება განხორციელდეს კანონის ფარგლებში, ასევე დამსაქმებელი ნებისმიერ დროს, დროის მცირე მონაკვეთში მიიღებს მონაცემთა დაცვის ოფიცრისგან რეკომენდაციებს, რჩევებს, უახლეს ინფორმაციაზე დაყრდნობით მონაცემთა კანონის შესაბამის დამუშავებაზე. მონაცემთა დაცვის ოფიცრის ხელშეკრულებაში დამსაქმებლის მხრიდან აუცილებელია განისაზღვროს: ა) ხელშეკრულების საგანი, ბ) ხელშეკრულების საფუძველი, გ) ხელშეკრულების მოქმედების ვადა, დ) მონაცემთა დაცვის ოფიცრის ფუნქციები, ე) მონაცემთა დაცვის ოფიცრის ვალდებულებები, ვ) ოფიცრის პასუხისმგებლობის მოცულობა, ზ) დავის წარმოშობის შემთხვევაში მისი გადაწყვეტის გზები.

[164] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი, მუხლი 33 მუხლი 1.

დასკვნა

პერსონალურ მონაცემთა დაცვის პრინციპები არის ის ძირითადი სახელმძღვანელო დებულებები, რომლის შესრულების ვალდებულებაც გათვალისწინებულია კანონით, მაგრამ ნაშრომის ანალიზი ცხადყოფს, რომ მიუხედავად კანონის არაერთი ჩანაწერისა, რეკომენდაციებისა, პერსონალურ მონაცემთა დაცვის პრინციპები სათანადოდ ვერ რეალიზდება მიმდინარე შრომით ურთიერთობებში. განსაკუთრებით მაშინ, როდესაც პერსონალურ მონაცემთა დაცვის პრინციპების დაცვისკენ არის მიმართული, როგორც საქართველოს კანონმდებლობა, ასევე საერთაშორისო რეგულაციები. მიმდინარე შრომით ურთიერთობებში ხელშეკრულების თავისუფლების პრინციპს უფრო მეტი ყურადღება ეთმობა, ვიდრე დამუშავების პრინციპების სწორად გატარებას. საჯარო სფეროს კონტროლი პრინციპების იმლემენტირების კუთხით ბევრად მარტივია, ვინაიდან მოქმედი კანონის მოქმედების სფერო მხოლოდ საჯარო სფეროზე ვრცელდება, სწორედ ამიტომ კერძო სექტორის მონიტორინგი ამ მხრივ ნაკლებად ხდება. უნდა აღინიშნოს, რომ მიმდინარე შრომით ურთიერთობებში მონაცემთა დამუშავების პრინციპებს განსაკუთრებული მნიშვნელობა აქვს, ვინაიდან დამსაქმებელების/უფლებამოსილი პირების მხრიდან საკმაო მოცულობის მონაცემები მუშავდება.

პერსონალურ მონაცემთა დაცვის პრინციპების იმპლემენტირებისათვის აუცილებელია უპირველეს ყოვლისა დაინეგროს და გატარდეს კანონმდებლობაში საერთაშორისო რეგულაციები, დოკუმენტურად და დეტალურად გაიწეროს მონაცემთა დამუშავების წესები და პრინციპები ხელშეკრულებებით ან შინაგანაწესებით, რა დროსაც მხოლოდ დამსაქმებლის და უფლებამოსილი პირის ნება არ არის საკმარისი, აუცილებელია დასაქმებულ პირების ინფორმირება მოხდეს, იქნება ეს ტრენინგები, სემინარები თუ ტესტირებები. აუცილებელია თითოეული თანამშრომელი იყოს ჩართული დამუშავების კანონიერების პროცესში.

პრინციპების იმპლემენტირებისათვის აუცილებელია თითოეული პრინციპისთვის დამახასიათებელი ნიშნები წინასწარ იქნეს განსაზღვრული დამმუშავებლის მიერ.

სამართლიანობის, კანონიერებისა და ღირსების დაცვის პრინციპი:

1. დამუშავების დაწყებისას უნდა იქნეს განსაზღვრული დამუშავების მიზანი;
2. აუცილებლად უნდა მოხდეს დამუშავების სუბიექტთა ინფორმირება დამუშავების ნებისმიერი ეტაპის დროს, (რომელი მონაცემი მუშავდება, რა მოცულობის, გადაეცემა თუ არა ეს მონაცმეები მესამე პირებს (უფლებამოსილი პირი) და ა.შ);
3. წინასწარ უნდა განისაზღვროს დასამუშავებელ მონაცემთა მოცულობა, და დამუშავების ფარგლები;
4. აუცილებელია მონაცემთა სუბიექტის თანხმობა დამუშავებაზე;
5. ერთსა და იმავე სამართლებრივ მდგომარეობაში მყოფი სუბიექტის მონაცემები ერთნაირად უნდა დამუშავდეს, დისკრიმინაციის თავიდან ასაცილებლად;

მიზნის მკაფიოდ განსაზღვრის (პროპორციულობის) პრინციპი:

1. დამუშავების მიზანი უნდა იყოს ლეგიტიმური და მკაფიო (თუნდაც დამატებით მონაცემთა დამუშავებისას);
2. დამუშავება უნდა შეესაბამებოდეს საბოლოო მიზანს, რისთვისაც მონაცემები მუშავდება;
3. დამუშავების მიზანი არ უნდა იყოს გადაჭარბებული, და დაცულ უნდა იქნეს პროპორციულობის პრინციპი;
4. ხელშეკრულებით უნდა განისაზღვროს დასამუშავებელი მონაცემების მოცულობა და ფარგლები.

მონაცემთა მიზნობრივი განახლება, სისწორის დაცვის და შენახვის ვადის

პრინციპი:

1. ინფორმაციის შეგროვების ეტაპზე უნდა განისაზღვროს მონაცემთა დამუშავების ვადა;
2. დამუშავების ეტაპზე უნდა დადგინდეს მონაცემთა შეგროვების წყარო და ინფორმაციის პერიოდულად გადახედვის სავარაუდო დრო/ინტერვალობა;
3. განსაზღვროს დამუშავებული მონაცემების მოცულობა, მიზნის პროპორციულად დამუშავებასთან მიმართებაში;
4. უნდა განისაზღვროს დამუშავების მოცულობა, და მისი დამუშავების მიზანთან შესაბამისობა (ამ ეტაპზე უნდა დადგინდეს ხომ არ ექვემდებარება დამუშავებული მონაცემები განადგურებას/წაშლას/დაბლოკვას, ან შეიძლება გათვალისწინებულ იქნეს ხელშეკრულებით ასეთი მონაცემების დამუშავების სუბიექტისთვის გადაცემა);
5. დამუშავების დაწყებისთანავე უნდა დადგინდეს დამუშავების სავარაუდო შედეგიანობა, რადგან თუ კონკრეტული ინფორმაციის დამუშავებით არ მიიღწევა შედეგი, ასეთი მონაცემი უპირველესად არასაჭიროა და არამიზნობრივი.

უსაფრთხოების პრინციპი:

1. უნდა შეიქმნას თავდაცვის გარანტიები დამუშავების სუბიექტებისთვის;
2. ტექნიკური და ორგანიზაციული ზომების გამოყენებით დამმუშავებლის უნდა შეიქმნას უსაფრთხოების ზომები (იქნება ეს სხვადასხვა ბაზები, მონიტორინგი სამსახური, თუ მონაცემთა დაცვის ოფიცრის დანიშვნა);
3. დამუშავების დაწყებისას წინასწარ უნდა იქნეს გათვალისწინებული უსაფრთხოების რისკები;

4. შესაძლებელია უსაფრთხოების პრინციპის უკეთ რეალიზებისათვის გარკვეულ მონაცემებზე წვდომა იქნეს შეზღუდული;

5. თუ დამუშავება დაკავშირებულია მონაცემთა ბაზებთან, ან სხვა ტექნიკურ საშუალებების გამოყენებასთან, აუცილებელია ბაზებზე წვდომა შეიძლებოდეს კოდური სიტყვებით, ან ციფრთა კომბინაციით. და ამისათვის წინასწარ განსაზღვრული უნდა იყოს ერთი ან რამდენიმე პირი, რომლებსაც ექნებათ ხელშეკრულებით გათვალისწინებული დაშვება მონაცემებზე;

6. დამმუშავებელმა მონაცემთა უსაფრთხოებისათვის გათვალისწინებული საშუალებების გამოყენებისას უნდა გაითვალისწინოს მონაცემების მოცულობა და, ასევე, მოსალოდნელი შედეგი.

ანგარიშ ვალდებულობის, გამჭირვალობის პრინციპი;

1. დამმუშავებლის მიერ სისტემატიურად უნდა ხდებოდეს დამუშავებული მონაცემების აღრიცხვა დამუშავების მიზანთან შესაბამისობაში;

2. დამუშავების რისკები უნდა იქნეს განსაზღვრული

დამუშავების დაწყების ეტაპიდანვე;

3. დამმუშავებელმა ინფორმაცია მარტივად ხელმისაწვდომი უნდა გახადოს დამუშავების სუბიექტისთვის და დაინტერესებული პირისთვის;

4. ხელშეკრულებით უნდა განისაზღვროს მონაცემთა გამჟღავნების და გაცემის შესაძლებლობები, და ასევე დარღვევის შემთხვევაში პასუხისმგებლობის ზომა და სახე;

5. ხარვეზის აღმოჩენისას მაქსიმალურად დროის მცირე მონაკვეთში უნდა მოხდეს მისი აღმოფხვრა (ეს ვადა შესაძლოა ხელშეკრულებით განისაზღვროს);

6. საზედამხელდველო ორგანოსთან მუდმივი კონტაქტი უნდა ხორციელდებოდეს, მისგან რჩევების/რეკომენდაციების და შენიშვნების მისაღებად;

7. ხელშეკრულებით უნდა განისაზღვროს აღნიშნული პრინციპის დარღვევისას პასუხისმგებელი პირი, და შესაბამისი პასუხისმგებლობის სახე.

უნდა აღინიშნოს აგრეთვე, რომ შრომითი ხელშეკრულების თავისუფლების პრინციპი ისე არ უნდა იყოს გაგებული, თითქოს მხარეებს მაქსიმალურ თავისუფლებას ანიჭებს კანონმდებლობა. არ შეიძლება სახელშეკრულებო ურთიერთობებში ისეთი პირობების დადგენა, რომელიც კანონს ეწინააღმდეგება, მხარეები მხოლოდ კანონის ფარგლებში მინიჭებული უფლებამოსილებით უნდა სარგებლობდნენ.

შრომით ხელშეკრულებაში, ასევე ულფებამოსილ პირთან და მონაცემთა დაცვის ოფიცერთან დადებულ ხელშეკრულებაში უნდა განისაზღროს დეტალურად პერსონალურ მონაცემთა დამუშავების წესები. ეს პირობები შესაძლოა იყოს, როგორც ძირითადი ხელშეკრულების ნაწილი, ასევე დამმუშავებელს შეუძლია ცალკე ხელშეკრულებით დაარეგულიროს პერსონალურ მონაცემთა დამუშავების საკითხები, შესაბამისად, ყველა სუბიექტისგან ინდივიდუალური და ინფორმირებული თანხმობა იქნება მიღებული მონაცემთა დამუშავებაზე. ასევე აუცილებელია, რომ ჩამოყალიბდეს ერთგვაროვანი პრაქტიკა პრინციპების დაცვასთან დაკავშირებით.

შრომით ხელშეკრულებაში (ან დამოუკიდებელ ხელშეკრულებაში) აუცილებელია მითითებული იყოს:

- მონაცემთა დამუშავების პრინციპების რეალიზებისთვის შექმნილი გარანტიები;
- თუ მონაცემთა დამუშავება უნდა განხორციელდეს უფლებამოსილი პირის მიერ, მის შესახებ დეტალურად უნდა იყოს მითითებული მისი უფლებამოსილების ფარგლები (უფლებამოსილი პირის დასახელება, იურიდიული მისამართი, საქმიანობის განხორციელების ფარგლები, დამუშავებულ მონაცემთა მოცულობა, მონაცემთა დამუშავების ვადა და ა.შ);
- დამმუშავებლის უფლებამოსილებები (უფლებები და ვალდებულებები უნდა გაიწეროს დეტალურად);
- დამუშავების სუბიექტის უფლებები და ვალდებულებები დეტალურად;
- თუ დამსაქმებელი არის უცხოური კომპანიის ფილიალი რომლის იურიდიული მისამართი სხვა ქვეყანაშია და აუცილებელია საერთაშორისო გადაცემა, დეტალურად უნდა გაიწეროს ასეთი დამუშავების საფუძველი და მოცულობა;
- დამმუშავებლის მხრიდან მონიტორინგი განხორციელების სახე და საფუძველი (1. ვიდეო კონტროლი; 2. აუდიო კონტროლი; 3. აუდიო-ვიდეო კონტროლი; 4. ელექტრონული ფოსტის კონტროლი; 5. საიტების და ვებგვერდებზე წვდომის კონტროლი; 6. ჰიგიენის და გამოსაცვლელი ოთახების კონტროლი; 7. ინფორმაციის სამართალდამცავი ორგანოებზე ან სასამართლოსთვის გადაცემის კონტროლი და ა.შ);
- დავის გადაწყვეტის გზები;
- მხარეების მიერ გამოხატული თანხმობა უნდა დადასტურდეს ხელმოწერით.

თუ აუცილებელია შრომითი სახელშეკრულებო ურთიერთობიდან გამომდინარე დამატებით მონაცემთა დამუშავება, აუცილებლად უნდა განხორციელდეს ინფორმირება და ყოველ კონკრეტულ შემთხვევაში უნდა

მოხდეს თანხმობის მიღება, იგივე გზით რაც ზემოთ არის მითითებული. დამსაქმებელსა (მონაცემთა დამმუშავებელი) და სხვა პირს (უფლებამოსილ პირი) შორის დადებული მომსახურების/დავალების ხელშეკრულებაში აუცილებლად უნდა იყოს მითითებული:

- ხელშეკრულების საგანი;
- მხარეები დეტალურად;
- ხელშეკრულების საფუძველი;
- ხელშეკრულების მიზანი;
- ხელშეკრულების მოქმედების ვადა;
- უფლებამოსილი პირის უფლებამოსილების ფარგლები;
- დასამუშავებელი მონაცემების მოცულობა;
- უფლებამოსილი პირის პასუხისმგებლობა დამმუშავებლის წინაშე;
- უფლებამოსილი პირის ინდივიდუალური პასუხისმგებლობა ხელშეკრულების პირობების დარღვევისას;
- უსაფრთხოების ზომები დეტალურად;
- დამუშავებული მონაცემების დაბრუნების ვალდებულება

(საქმიანობის შეჩერების, დამუშავების შეწყვეტის ან დავის არსებობის შემთხვევაში);

დამსაქმებელსა და მონაცემთა დაცვის ოფიცერს შორის დადებული ხელშეკრულება უნდა შეიცავდეს:

- ხელშეკრულების საგანს;
- ხელშეკრულების საფუძველს;
- ხელშეკრულების ვადას;
- მონაცემთა დაცვის ოფიცრის ფუნქციებს;

- მონაცემთა დაცვის ოფიცრის უფლებებს და ვალდებულებებს; მონაცემთა დაცვის ოფიცრის პასუხისმგებლობის მოცულობას; დავის წარმოშობის შემთხვევაში დავის გადაწყვეტის გზას. თუ თითოეული ხელშეკრულებაში, რომელიც დამსაქმებლის მიერ გაფორმდება, დეტალურად გაიწერება ზემოთ აღნიშნული რეკომენდაციები მონაცემთა დამუშავების ეტაპი იქნება კანონის შესაბამისი, ასევე პრინციპების იმპლემენტირებაც სწორად მოხდება მიმდინარე შრომით ურთიერთობებში.

ბიბლიოგრაფია:

1. არჩუაძე თ., პერსონალურ მონაცემთა დაცვის გარანტიები მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 2016;
2. გოშაძე კ., პერსონალურ მონაცემთა დამუშავების პრინციპების იმპლემენტირება შრომით ურთიერთობებში., სოფიო ჩაჩავას და ვახტანგ ზაალიშვილის რედაქტორობით, თბილისი 2014;
3. გაგნიძე ე., საიქოძე ნ., პერსონალურ მონაცემთა დაცვასთან დაკავშირებული კერძო და საჯარო ინტერესის თანაფარდრობა და უფლებაში ჩარევის საფუძვლიანობის კრიტერიუმები.,სტუდენტური სამართლებრივი ჟურნალი, თბილისი, 2016;
4. გლიგალიშვილი ნ., კუტალაძე მ., ევროკავშირის მიდგომა პერსონალური მონაცემების დაცვის სამართლებრივი რეგულირების საკითხისადმი, გამომცემლობა უნივერსალი., თბილისი 2018;
5. თოლთლაძე ლ., გაბრიჩიძე გ., თუმანიშვილი გ., ტურავა პ., ჩაჩანიძე ე., განმარტებითი იურიდიული ლექსიკონი, თბილისი, 2012;
6. ლაფარაშვილი ი., პერსონალურ მოაცემთა საერთაშორისო გადაცემის სამართლებრივი მოწესრიგება ქართული და ევროპული სტანდარტების მიხედვით, თბილისი, 2018;
7. მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი 2018;
8. პერსონალურ მონაცემთა დაცვის ინსპექტორის რეკომენდაციები შრომით ურთიერთობებში პერსონალური მონაცემების დაცვის შესახებ, თბილისი, 2014;
9. პირადი და ოჯახური ცხოვრების პატივისცემის უფლება და სახელმწიფოს ვალდებულებები, ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკისა და საქართველოს საკონსტიტუციო სასამართლოს პრაქტიკის მიმოხილვა., ოქტომბერი, 2017;

10. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაციები, პერსონალური მონაცემების დაცვა, გზამკვლევი დამწყები ბიზნესისათვის;
11. სახელმწიფო ინსპექტორის სამსახურის სახელმძღვანელო სხვა სახელმწიფოსათვის ან სახელმწიფო იურისდიქციის ქვეშ მყოფი იურიდიული ან ფიზიკური პირისათვის ან საერთაშორისო ორგანიზაციისთვის პერსონალურ მონაცემთა გადაცემის შესახებ პერსონალურ მონაცემთა დაცვის ინსპექტორის ნებართვის მისაღებად წარსადგენი განცხადების შევსების, განცხადების განხილვის ვადების და შედეგის გასაჩვრების წესის შესახებ, თბილისი, 2019;
12. ძამუკაშვილი დ,. შრომის სამართალი,თბილისი, 2013;
13. წერეთელი მ., პერსონალურ მონაცემების დაცვის სამართლებრივი მნიშვნელობა და დაცვის სტანდარტები ბიზნეს ურთიერთობებში, თბილისი, 2019;
14. Article 29 - Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, Adopted on 13 September2001;
15. A&L Goodbody, GDPR for Employers;
16. Council of Europe Committee of Ministers of the Committee recomenadtion No. R (89) 2, of Ministers to member States on the Protection of Personal Data used for employment purposes; (Adopted by the Committee of Ministers on 18 January 1989 at the 423rd meeting of the Ministers' Deputies);
17. González Fuster G., The Emergence of Personal Data Protection as a Fundamental Right of the EU, London, 2014;
18. Guide to the General Data Protection Regulation (GDPR), Ico; 2019;
19. Goshadze k., The Data Protection Officer (DPO)- ensuring greater Data Protection compliance, იოსებ კელენჯერიძის, ზურაბ ჭყონიას, ნათია გაბედავას, ნატო გიგაურის, მარიამ ბობოხიძის და თამარ ქავჟარაძის რედაქტორობით, თბილისი., 2020.
20. Paul p. K and Reiner. S “Manual on Data Protection in Employment Context”, Ludwig Boltzmann Institute of Human Rights, Vienna Mandated Body, November

2006;

21. Protection of worker's personal data, Internation Labour Office Geneva; ILO;
22. Rosemary J., Clarke J., Data Protection Compliance in the UK, United Kingdom, 2010;
23. Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), of 27 April 2016;
24. Top 10 principles for Worker's Data Privacy and Protection, the future word of work;
25. V. John Ella, J.D., CIPP, Jackson Lewis P.C "Employee monitoring and workpace Privacy Law", Washington, D.C. April 6, 7, and 8, 2016;

სამართლებრივი აქტები:

1. საქართველოს სამოქალაქო კოდექსი, თბილისი 1997;
2. საქართველოს შრომის კოდექსი, თბილისი 2010;
3. საქართველოს ზოგადი ადმინისტრაციული კოდექსი, თბილისი 1999;
4. საქართველოს ზოგადი ადმინისტრაციული კოდექსის სსმ, 32(39) 15/07/1999 წლის რედაცია. <https://matsne.gov.ge/ka/document/view/16270?publication=0>
5. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", თბილისი 2011;
6. „სახელმწიფო ინსპექტორის შესახებ" საქართველოს კანონი, 2018
7. საქართველოს კანონის პროექტი „პერსონალურ მონაცემთა დაცვის შესახებ";
8. საქართველოს მთავრობის დადგენილება N180 პერსონალურ მონაცემთა დაცვის ინსპექტორის საქმიანობისა და მის მიერ უფლებამოსილების განხორციელების წესის შესახებ დებულების დამტკიცების შესახებ, 2013, საქართველოს საკანონმდებლო მაცნე 19/07/2013, (ძალადაკარგულია 20/11/2019);
9. ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია,

1950;

10. Convention to the Protection Individual with regard to Aotomatic Processing of Personal Data., Strasburg.28.I.1981;
11. კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“; ძალაშია 2006 წლის 1 აპრილიდან.
12. Modernised Convention For the Protection of Individuals with Regard to the Processinf of Personal Data, Consolidated text, 2018;
13. Code of practice on the protection of worker's personal data.

სასამართლოს გადაწყვეტილებები:

1. საკონსტიტუციო სასამართლოს 2017 წლის 27 მარტის გადაწყვეტილება N:1/4/757 საქმეზე „საქართველოს მოქალაქე გიორგი კრავეიშვილი საქართველოს მთავრობის წინააღმდეგ“;
2. საკონსტიტუციო სასამართლოს 2019 წლის 7 ივნისის გადაწყვეტილება №1/4/693,857 საქმეზე „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ“.
3. საქართველოს უზენაესი სასამართლოს 2015 წლის 22 მაისის გადაწყვეტილება საქმე N: ას-243-230-2015;
4. საქართველოს უზენაესი სასამართლოს სამოქალაქო საქმეთა პალატის 2016 წლის 18 მარტის განჩინება საქმე N:ას-50-49-2016;
5. თბილისის სააპელაციო სასამართლოს ადმინისტრაციულ საქმეთა პალატის 2016 წლის 26 აპრილის გადაწყვეტილება N3ბ/1059-15;
6. ადამიანის უფლებათა ევროპული სასამართლოს 1987 წლის 26 მარტის გადაწყვეტილება, საქმეზე Leander v. Sweden;
7. ადამიანის უფლებათა ევროპული სასამართლოს 1998 წლის 25 მარტის გადაწყვეტილება საქმეზე Kopp v. Switzerlad;
8. ადამიანის უფლებათა ევროპული სასამართლოს 2000 წლის 16 თებერვალი გადაწყვეტილება საქმეზე Aman v. Switzerland;

9. ადამიანის უფლებათა ევროპული სასამართლოს 2008 წლის 4 დეკემბრის გადაწყვეტილება საქმეზე S. And Marper v. The United Kingdom;
10. ადამიანის უფლებათა ევროპული სასამართლოს 2012 წლის 13 ნოემბრის გადაწყვეტილება საქმეზე M.M. v. The United Kingdom;
11. ადამიანის უფლებათა ევროპული სასამართლოს 2017 წლის 5 სექტემბრის გადაწყვეტილება საქმეზე Barbulescu v. Romania;
12. ადამიანის უფლებათა ევროპული სასამართლოს 2017 წლის 27 ივნისის გადაწყვეტილება საქმეზე Satakunnan Markkinaporssi oy and Satamedia oy v. Finald;
13. CJEU, In case C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, 7 May 2009;
14. CJEU Joined cases C-468/10 and C-469/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) And Federación de Comercio Electrónico y Marketing Directo (FECEMD) V Administración del Estado, 24 Noember, 2011;
15. CJEU, Joined cases C 293/12 and C 594/12, Digital Rights Ireland Ltd (C 293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, 8 April, 2014;
16. CJEU, In Case c-201/14 Smaranda Bara and Others V. Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF), 1 Octomber 2015;

სახელმწიფო ინსპექტორის გადაწყვეტილებები:

1. პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის 20 მაისის გადაწყვეტილება შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-1/043/2015.

2. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 28 თებერვლის გადაწყვეტილება, მ.დ-ს განცხადების განხილვის დასრულების შესახებ, საქმე N:გ-1/103/2017
3. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 28 მარტის გადაწყვეტილება ლ.ა-ს განცხადებასთან დაკავშირებული განხილვის დასრულების შესახებ, საქმე N:გ-1/165/2017
4. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 21 აპრილის გადაწყვეტილება მ.ა-ს განცხადებასთან დაკავშირებული განხილვის დასრულების შესახებ, საქმე N:გ-1/210/2017
5. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 11 მაისის გადაწყვეტილება შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-1/262/2017
6. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 25 მაისის გადაწყვეტილება, შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-1/286/2017
7. საქართველოს პერსონალურ მონაცმეთა დაცვის ინსპექტორის 2017 წლის 16 ივნისის გადაწყვეტილება, შპს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-1/314/2017;
8. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 30 ივნისის გადაწყვეტილება, ი.ნ-ს განცხადებასთან დაკავშირებით განხილვის დასრულების შესახებ, საქმე N:გ-1/329/2017;
9. საქართველოს ინსპექტორის 2018 წლის 7 სექტემბრის გადაწყვეტილება, გ.ნ-ს განცხადების განხილვის დასრულების შესახებ, საქმე N:გ-1/507/2018
10. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის 26 დეკემბრის გადაწყვეტილება, სს „ა“-ს შემოწმების დასრულების შესახებ, საქმე N:გ-1/701/2018.

ანგარიშები:

1. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის ანგარიში

„პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში“ თბილისი 2013-2014 წ;

2. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის ანგარიში

„პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში“ თბილისი, 2014 ;

3. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის ანგარიში „პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ“ თბილისი 2015 ;
4. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის ანგარიში „პერსონალურ მონაცემთა დაცვის მდგომარეობისა და ინსპექტორის საქმიანობის შესახებ“ თბილისი, 2016 ;
5. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის ანგარიში „პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ“ თბილისი, 2017;
6. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის ანგარიში „პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ“ თბილისი, 2018;
7. სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში, თბილისი 2019.

ელექტრონული რესურსი:

1. [https://www.dataprotection.ie/en/individuals/principles-data-protection] 02.03.2020
2. [https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protectionprinciples] 02/03/2020
3. [https://www.futurelearn.com/courses/general-data-protection-regulation/0/steps/32412] 02/03/2020

4. [https://www.nibusinessinfo.co.uk/content/data-protection-principles-under-gdpr] 02/03/2020
5. [https://netgazeti.ge/news/186433/] 30.04.2020
6. [https://personaldata.ge/ka/orginnerpage8] 02.05.2020
7. [http://newadmin.personaldata.ge/wp-content/uploads/2018/09/white-list_final-1.pdf] 02.05.2020
8. [https://www.lexology.com/library/detail.aspx?g=8aa887fd-1103-4a98-aa13-0137215b2b19] 03.05.2020
9. [https://www.dataprotection.ie/en/organisations/international-transfers] 03.05.2020
10. [https://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN%20%2021] 03.05.2020
11. [https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/security/] 07.05.2020
12. [https://personaldata.ge/ka/recommendations] 07.05.2020
13. [https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet] 20.05.2020
14. [https://z-lib.org/]
15. [https://www.ssrn.com/index.cfm/en/]
16. [https://hudoc.echr.coe.int/]
17. [https://curia.europa.eu/]
18. [https://eur-lex.europa.eu/]
19. [https://personaldata.ge/ka/about-us]
20. [https://ico.org.uk/]
21. [https://matsne.gov.ge/]
22. [https://personaldata.ge/ka/decisions]
23. [https://elibrary.sou.edu.ge/]
24. [http://ecd.court.ge/Decision]