Innovations and reforms Center

ინოვაციებისა და რეფორმების ცენტრის შეფასება და რეკომენდაციები

„პერსონალურ მონაცემთა დაცვის შესახებ"

საქართველოს კანონის პროექტზე

ინოვაციებისა და რეფორმების ცენტრის შეფასება და რეკომენდაციები „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტზე

ინოვაციებისა და რეფორმების ცენტრმა, რომლის საქმიანობის ერთ-ერთ მიმართულებას წარმოადგენს საქართველოში პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა დაცვის ხელშეწყობა, საქართველოს პარლამენტში ინიცირებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტის სამართლებრივი ანალიზის საფუძველზე მოამზადა რეკომენდაციები, რომელთა მთავარი მიზანი ქართული კანონმდებლობის ევროსაბჭოს 108-ე მოდერნიზებულ კონვენციასა და მონაცემთა დაცვის ზოგად ევროპულ რეგულაციასთან (GDPR) კიდევ უფრო დაახლოებაა.

კანონპროექტი უდავოდ პროგრესულია, მასში ასახულია მონაცემთა დაცვის ახალი ევროპული სამართლებრივი ინსტრუმენტებით გათვალისწინებული ნოვაციები, მონაცემთა დასაცავად მისაღები აუცილებელი ტექნიკური თუ ორგანიზაციული ზომები, თუმცა პროექტის სიღრმისეული ანალიზი იძლევა კრიტიკული შენიშვნების გამოთქმის საფუძველს კანონპროექტის რამდენიმე მუხლთან მიმართებით, რომლებიც მონაცემთა დაცვის მნიშვნელოვან და ძირეულ ასპექტებს შეეხება.

ვიმედოვნებთ, კანონპროექტის არსებითი განხილვის პროცესში მოხდება რეკომენდაციების გათვალისწინება, რაც, თავის მხრივ, ხელს შეუწყობს ახალ ევროპულ სტანდარტებთან ქართული კანონმდებლობის სრული შესაბამისობის უზრუნველყოფას და ახლო პერსპექტივაში შესაძლებელს გახდის ევროკავშირის მიერ საქართველოსთან მონაცემთა თავისუფალი მიმოცვლის შესახებ გადაწყვეტილების მიღებას.

რეკომენდაცია მომზადდა პროექტის “მონაცემთა სუბიექტებისა და სხვა აქტორების გაძლიერება პირადი ცხოვრების ხელშეუხებლობის უფლების რეალიზაციისთვის” ფარგლებში, ნიდერლანდების საელჩოს მხარდაჭერით. დოკუმენტში მოცემული შეფასებები და რეკომენდაციები წარმოადგენს მხოლოდ ინოვაციებისა და რეფორმების ცენტრის პოზიციას და ის შეიძლება არ ასახავდეს ნიდერლანდების საელჩოს შეხედულებებს.

01 კანონის მოქმედების სფერო

კანონპროექტის მე-2 მუხლი განსაზღვრავს კანონის მოქმედების არეალს და გამონაკლისის სახით ითვალისწინებს კონკრეტულ სფეროებსა და საკითხებს (მაგალითად, სასამართლოს მიერ მართლმსაჯულებისა და საკონსტიტუციო კონტროლის განხორციელება, სახელმწიფო უსაფრთხოება და თავდაცვა), რომლებზეც კანონის მოქმედება საერთოდ არ ვრცელდება.

საქართველოსთვის, როგორც ხელშემკვრელი მხარისთვის, სავალდებულო ძალის მქონე ინსტრუმენტია ევროპის „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპული კონვენცია – ე.წ. 108-ე კონვენცია. 2018 წელს შესწორების ოქმის (CETS no.223) მიღებით კონვენციამ განიცადა მოდერნიზება (კონვენცია 108+).

მოდერნიზებული კონვენციის მე-3 მუხლი განსაზღვრავს კონვენციის მოქმედების მატერიალურ ფარგლებს. GDPR-ის მსგავსად, 108+ კონვენცია არ ვრცელდება ფიზიკური პირის მიერ პერსონალური მონაცემების ცალსახად პირადი ან ოჯახური საქმიანობის ფარგლებში დამუშავებაზე, თუმცა 108+ კონვენცია ზღუდავს ხელშემკვრელი სახელმწიფოების შესაძლებლობასა და უფლებას დაადგინონ მონაცემთა დამუშავების გარკვეულ კატეგორიებზე კონვენციის გავრცელების შემზღუდავი წესები, მათ შორის, ეროვნული უსაფრთხოებისა და თავდაცვის მიზნებისთვის.

108+ კონვენციის მე-11 მუხლის თანახმად, დაუშვებელია კონკრეტულ სფეროზე სრული გამონაკლისის დაშვება. წევრ სახელმწიფოებს გამონაკლისი შეუძლიათ დააწესონ მხოლოდ კონკრეტულ დებულებებთან დაკავშირებით, კერძოდ: მე-5 მუხლის მეოთხე პუნქტით (ლეგიტიმურობა და მონაცემთა ხარისხი), მე-7 მუხლის მეორე პუნქტით (მონაცემთა უსაფრთხოება), მე-8 მუხლის პირველი პუნქტით (დამუშავების გამჭვირვალობა) და მე-9 მუხლით (მონაცემთა სუბიექტის უფლებები) განსაზღვრულ დებულებებთან მიმართებით და ისიც მხოლოდ მაშინ, თუ ისინი გათვალისწინებულია წევრი სახელმწიფოს კანონმდებლობით, პატივს სცემს ფუნდამენტური უფლებებისა და თავისუფლებების არსს და წარმოადგენს საჭირო და პროპორციულ ღონისძიებას დემოკრატიულ საზოგადოებაში. ასეთი გამონაკლისის კანონმდებლობით დადგენის მიზანი შეიძლება იყოს ისეთი ლეგიტიმური და აღმატებული ინტერესები, როგორიცაა ეროვნული უსაფრთხოება, თავდაცვა, დანაშაულის პრევენცია, სასამართლოს მიუკერძოებლობა, მონაცემთა სუბიექტის ან სხვების უფლებებისა და ფუნდამენტური თავისუფლებების დაცვა, სამეცნიერო კვლევითი ან სტატისტიკური მიზნები და სხვა მკაფიოდ რეგლამენტირებული საზოგადოებრივი მნიშვნელობის ამოცანები.

კანონპროექტი

მუხლი 2. კანონის მოქმედების სფერო

1. ამ კანონის მოქმედება ვრცელდება საქართველოს ტერიტორიაზე ავტომატური, ნახევრად ავტომატური და არაავტომატური საშუალებებით მონაცემთა დამუშავებაზე, მათ შორის, დანაშაულის თავიდან აცილების, დანაშაულის გამოძიების, სისხლისსამართლებრივი დევნის, მართლმსაჯულების განხორციელების, პატიმრობისა და თავისუფლების აღკვეთის აღსრულების, ოპერატიულ-სამძებრო საქმიანობის, საზოგადოებრივი უსაფრთხოებისა და მართლწესრიგის დაცვის მიზნებისათვის მონაცემთა დამუშავებაზე (მიუხედავად იმისა, მიეკუთვნება თუ არა აღნიშნული სახელმწიფო საიდუმლოებას, გარდა ამავე მუხლის მე-2 პუნქტით გათვალისწინებული გამონაკლისებისა);

2. ამ კანონის მოქმედება არ ვრცელდება:
ა) ფიზიკური პირის მიერ მონაცემთა აშკარად პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში დამუშავებაზე, რომელიც დაკავშირებული არ არის მის სამეწარმეო, პროფესიულ საქმიანობასთან ან სამსახურებრივი მოვალეობის შესრულებასთან, ან ამ კანონის მე-10 მუხლით გათვალისწინებულ ვიდეოთვალთვალის განხორციელებასთან;
ბ) სახელმწიფო უსაფრთხოების (მათ შორის, ეკონომიკური უსაფრთხოების), თავდაცვის, სადაზვერვო და კონტრდაზვერვითი საქმიანობების მიზნებისათვის მონაცემთა დამუშავებაზე;
გ) სასამართლოს მიერ მართლმსაჯულებისა და საკონსტიტუციო კონტროლის განხორციელების მიზნებისთვის მონაცემთა დამუშავებაზე;
დ) მედიის მიერ საზოგადოების ინფორმირების მიზნით მონაცემთა დამუშავებაზე (გარდა 27-ე მუხლისა);
ე) მონაცემთა აკადემიური, სახელოვნებო და ლიტერატურული მიზნებისათვის დამუშავებაზე;

შეფასება/რეკომენდაცია

აღსანიშნავია, რომ კანონპროექტის მე-2 მუხლის პირველი პუნქტი და მეორე პუნქტის „ა“ ქვეპუნქტი შესაბამისობაშია, როგორც GDPR-თან და ე.წ პოლიციის დირექტივასთან, ასევე 108+კონვენციასთან.

რაც შეეხება პროექტის მე-2 პუნქტით შემოთავაზებულ გამონაკლის სფეროებს, კონვენციასთან შესაბამისობის უზრუნველყოფის მიზნით, მიზანშეწონილია, ისინი ნაწილობრივ მოექცნენ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედების სფეროში და გამონაკლისის სახით დათქმა გაკეთდეს კანონის კონკრეტულ მუხლებსა და დებულებებზე, რომელთა მოქმედებაც ამ სფეროებთან მიმართებით შეზღუდული იქნება. ასევე, სასურველია მიეთითოს აღნიშნულის გამომწვევი მიზეზები, კერძოდ, ის რომ: სფეროები, რომელთა მიმართებითაც კანონის მოქმედება ნაწილობრივ შეზღუდულია, რეგულირდება შესაბამისი კანონმდებლობით და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის სრულად გავრცელებამ შესაძლოა დააზიანოს ისეთი ლეგიტიმური ინტერესები, როგორიცაა ეროვნული უსაფრთხოების დაცვა, თავდაცვა, საზოგადოებრივი უსაფრთხოება, სახელმწიფოს მნიშვნელოვანი ეკონომიკური და ფინანსური ინტერესები, სასამართლოს მიუკერძოებლობისა და დამოუკიდებლობის უზრუნველყოფა, სხვათა უფლებები და თავისუფლებები, განსაკუთრებით სიტყვისა და გამოხატვის თავისუფლება.

02 ტერმინოლოგია

პერსონალურ მონაცემთა დაცვის სფეროში სპეციფიკური ტერმინოლოგია გამოიყენება, რომელიც შესაძლოა სხვა სამართლებრივ დარგებსა თუ დოკუმენტებში დამკვიდრებული ტერმინებისგან განსხვავებულ მნიშვნელობას ატარებდეს. აღნიშნული თავისებურებისა და ასევე ამ სფეროში არსებული ნოვაციების გათვალისწინებით, მნიშვნელოვნად მიგვაჩნია საერთაშორისოდ დამკვიდრებული ტერმინები შინაარსობრივი მნიშვნელობით ითარგმნოს და ადეკვატური ქართული შესატყვისები იქნას მოძიებული, რომლებიც თანხვედრაში იქნება საერთაშორისოდ აღიარებულ ტერმინებთან.

ტერმინოლოგიური თვალსაზრისით კანონპროექტთან არსებითი ხასიათის შენიშვნები არ გვაქვს. კანონპროექტით ქართულ სამართლებრივ სივრცეში შემოდის ისეთი ახალი ტერმინები, როგორებიცაა მონაცემთა პორტირება, პროფილირება და მისაღებად ვთვლით მათი ამ ფორმით დამკვიდრება ქართულ სამართლებრივ სივრცეში, თუმცა მიზანშეწონილად მიგვაჩნია ტერმინი დეპერსონალიზაციის შეცვლა ტერმინით ანონიმიზაცია, რომელიც უკეთ გამოხატავს თავად პროცესის შინაარსს და თანხვედრაში იქნება საერთაშორისოდ დამკვიდრებულ ტერმინთან.

ასევე, მნიშვნელოვნად მიგვაჩნია ქართულ კანონმდებლობაში დავამკვიდროთ ტერმინი – უფლება იყო დავიწყებული, რომლის შინაარსიც მოცემულია კანონპროექტის მე-18 მუხლში.

კანონპროექტი

მუხლი 3
წ) მონაცემთა დეპერსონალიზაცია - მონაცემთა იმგვარი დამუშავება, როდესაც შეუძლებელია მათი დაკავშირება მონაცემთა სუბიექტთან ან ასეთი კავშირის დადგენა არაპროპორციულად დიდი ძალისხმევას, ხარჯებს ან/და დროს საჭიროებს;

და შესაბამისი ჩანაწერი კანონპროექტის მე-4 მუხლში

მუხლი 18. მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლება

შეფასება/რეკომენდაცია

რამდენადაც ტერმინის „მონაცემთა დეპერსონალიზაცია“ შინაარსი და განმარტება შეესაბამება საერთაშორისოდ დამკვიდრებული ტერმინის „ანონიმიზაცია“ შინაარსს, ევროპულ კანონმდებლობასთან შესაბამისობისა და თარგმანისას ბუნდოვანების თავიდან აცილების მიზნით, მიზანშეწონილად მიგვაჩნია ტერმინი „დეპერსონალიზაცია“ ჩანაცვლდეს ტერმინით „ანონიმიზაცია“.

GDPR-მა მონაცემთა სუბიექტის მიერ მის შესახებ არსებული მონაცემების წაშლის მოთხოვნის უფლება კიდევ ერთხელ განამტკიცა და, ასევე, შემოიტანა ტერმინი - უფლება იყო დავიწყებული (right to be forgotten). თავად ტერმინი Google inc. და Google ესპანეთის წინააღმდეგ ევროპული სასამართლოს გადაწყვეტილებით დამკვიდრდა, რომლითაც Google-ს დაევალა მოსარჩელის შესახებ საძიებო სისტემის მეშვეობით ხელმისაწვდომი ინფორმაციის წაშლა, რადგანაც ეს ინფორმაცია, მიუხედავად იმისა, რომ შეესაბამებოდა სიმართლეს, აღარ იყო ადეკვატური, რელევანტური და განახლებული (up to date).

შესაბამისად, თავად ამ უფლების მნიშვნელობის ხაზგასასმელად, გარდა კანონპროექტში ამ იდეის ასახვისა, მნიშვნელოვანად მიგვაჩნია ის ტერმინის დონეზეც დამკვიდრდეს ქართულ კანონმდებლობაში და პროექტის მე-18 მუხლის სათაურს ფრჩხილებში დაემატოს ცნება - უფლება იყო დავიწყებული.

03 მონაცემთა დამუშავების საფუძველი – საჯარო ინტერესი

მონაცემთა დამუშავების ერთ-ერთი საფუძველია ე.წ „საჯარო ინტერესი“. ეს ცნება ხშირად საკამათოა, რამდენადაც თავისი არსით ისეთ საკითხებს ეხება, რაც შეუძლებელია ზუსტად და ამომწურავად იქნას განმარტებული, შესაბამისად, არსებობს რისკი, ეს ცნება მონაცემთა დამმუშავებლების მხრიდან არასწორად ან ვიწროდ იქნას ინტერპრეტირებული.

ამ საფუძვლის გამოყენება შესაძლებელია საჯარო უფლებამოსილებების, კანონით განსაზღვრული საჯარო ფუნქციების ან კანონით განსაზღვრულ საჯარო ინტერესებში შემავალი სპეციფიკური ამოცანების შესასრულებლად. ამ საფუძვლის გამოყენებისათვის აუცილებელი არ არის კანონმდებლობაში დამუშავების თაობაზე პირდაპირი ჩანაწერის არსებობა, მთავარია შესასრულებელ ფუნქციას ჰქონდეს მკაფიო სამართლებრივი საფუძველი, შესაბამისად ეს საფუძველი რელევანტურია როგორც საჯარო დაწესებულებებისთვის, ასევე იმ ორგანიზაციებისთვის, რომლებიც ასრულებენ/დაკისრებული აქვთ საჯარო სამართლებრივი უფლებამოსილებები. შესაბამისად, მნიშვნელოვანია „საჯარო ინტერესის“ ტერმინის საერთაშორისო სტანდარტებთან შესაბამისად ინტერპრეტაციის შესაძლებლობა შენარჩუნდეს.

კანონპროექტი

ე) მონაცემთა დამუშავება აუცილებელია საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად, მათ შორის, დანაშაულის თავიდან აცილების, დანაშაულის გამოძიების, სისხლისსამართლებრივი დევნის, მართლმსაჯულების განხორციელების, პატიმრობისა და თავისუფლების აღკვეთის აღსრულების, ოპერატიულ-სამძებრო საქმიანობის, საზოგადოებრივი უსაფრთხოებისა და მართლწესრიგის დაცვის მიზნებისათვის;

შეფასება/რეკომენდაცია

„საჯარო ინტერესის“ ტერმინის ინტერპრეტაცია ძალიან ფართოდ არის შესაძლებელი, შესაბამისად, ამ მუხლში მხოლოდ სამართალდამცავი ორგანოებისთვის რელევანტური მიზნების ჩამოთვლამ, შესაძლოა ამ ტერმინის ვიწრო და არასწორი გაგება/განმარტება გამოიწვიოს. მიზანშეწონილად მიგვაჩნია „ე“ პუნქტის ევროპული რეგულაციის მსგავსად ჩამოყალიბება შემდეგი რედაქციით – მონაცემთა დამუშავება აუცილებელია საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად ან მონაცემთა დამმუშავებლისთვის დაკისრებული საჯარო უფლებამოსილებების განსახორციელებლად.

ხოლო იმისათვის, რომ შემოთავაზებულ რედაქციაში ჩამოთვლილი ამოცანების (დანაშაულის თავიდან აცილება, გამოძიება და ა.შ.) განხორციელებისას მონაცემთა დამუშავება შესაბამისობაში იყოს ე.წ. პოლიციის დირექტივასთან, შესაძლებელია, ამავე მუხლის „გ“ ქვეპუნქტს დაემატოს აღნიშნული ჩამონათვალი და პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით „მონაცემთა დამუშავება საჭიროა მონაცემთა დამმუშავებლის მიერ მისთვის საქართველოს კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად, მათ შორის, დანაშაულის თავიდან აცილების, დანაშაულის გამოძიების, სისხლისსამართლებრივი დევნის, მართლმსაჯულების განხორციელების, პატიმრობისა და თავისუფლების აღკვეთის აღსრულების, ოპერატიულ-სამძებრო საქმიანობის, საზოგადოებრივი უსაფრთხოებისა და მართლწესრიგის დაცვის მიზნებისათვის“.

04 მონაცემთა პორტირება

მონაცემთა დაცვის კანონმდებლობის განახლების მიზანია მოქალაქეთა (მონაცემთა სუბიექტის) ისეთი ახალი უფლებებითა და გარანტიებით აღჭურვა, რომელიც მას მეტი კონტროლისა და საკუთარი მონაცემების დამუშავების პროცესში გარკვეული გადაწყვეტილებების მიღების შესაძლებლობას მისცემს. აღნიშნულის უზრუნველსაყოფად მოქმედი კანონი ითვალისწინებს მონაცემთა სუბიექტის მიერ ინფორმაციის მოთხოვნის/მონაცემებზე წვდომის უფლებას, ხოლო მონაცემთა სუბიექტის უფლებების უკეთ რეალიზაციისა და მისთვის მონაცემთა დამუშავების პროცესზე რეალური გავლენის მოხდენის ბერკეტის მისანიჭებლად, GDPR-ის მსგავსად, კანონპროექტი აღიარებს ახალ უფლებას - პორტირების (გადატანის) უფლებას. ეს უფლება გულისხმობს საკუთარ მონაცემების სტრუქტურირებული, გამოყენებადი და ელექტრონული ფორმით მიღების უფლებას ან ამ მონაცემების სხვა დამმუშავებლისთვის გადაცემის მოთხოვნის უფლებას, თუ ეს ტექნიკურად შესაძლებელია.

მნიშვნელოვანია, რომ მონაცემთა პორტირების უფლების განხორციელება ავტომატურად არ ნიშნავს მონაცემთა წაშლის მოთხოვნას. შესაბამისად, მონაცემთა გადამცემს სათანადო საფუძვლების არსებობისას კვლავ შეუძლია მონაცემების დამუშავება და მონაცემთა სუბიექტიც ინარჩუნებს რეგულაციით მინიჭებულ ყველა უფლებას, მათ შორის, მონაცემთა შესწორების, დაბლოკვისა და წაშლის მოთხოვნის უფლებებს.

პორტირების უფლების შესახებ აღსანიშნავია 29-ე მუხლის სამუშაო ჯგუფის სახელმძღვანელო პრინციპები, რომლებიც განმარტავს მონაცემთა პორტირების ძირითად ელემენტებს, ესენია:

- მონაცემთა სუბიექტის უფლება, მიიღოს საკუთარი მონაცემები, რომლებსაც დამმუშავებელი ამუშავებს სტრუქტურირებულ, გამოყენებად, წაკითხვად და თავსებად ფორმატში
- პერსონალური მონაცემების ერთი დამმუშავებლისგან მეორე დამმუშავებლისთვის გადაცემა, დაბრკოლების გარეშე, თუ ეს ტექნიკურად შესაძლებელია
- კონტროლის რეჟიმი - მონაცემთა სუბიექტი თავად წყვეტს, თუ ვის გადაეცემა მისი მონაცემები;

სახელმძღვანელო პრინციპებში მაგალითების სახით მოცემულია ერთ სოციალური ქსელში არსებული კონტაქტებისა და სხვა მონაცემების სხვა პროვაიდერთან და ჯანმრთელობის მდგომარეობასთან დაკავშირებული ჩანაწერების სხვა ჯანდაცვის პროვაიდერთან გადატანა, ვინაიდან პრაქტიკაში სწორედ ამ სფეროებშია პორტირების უფლება ყველაზე მოთხოვნადი და ტექნიკურად რეალიზებადი.

კანონპროექტი

მუხლი 20. მონაცემთა პორტირების (გადატანის) უფლება ამ კანონის მე-5 მუხლის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული საფუძვლით მონაცემთა ავტომატური დამუშავების შემთხვევაში, თუ ეს ტექნიკურად შესაძლებელია, მონაცემთა სუბიექტს უფლება აქვს, მონაცემთა დამმუშავებლისაგან სტუქტურიზებული, გამოყენებადი და ელექტრონული ფორმით მიიღოს მის მიერ მიწოდებული მონაცემები ან მოითხოვოს მათი სხვა დამმუშავებლისთვის გადაცემა.

შეფასება/რეკომენდაცია

გაურკვეველია, კანონპროექტი რატომ ავრცელებს პორტირების უფლებას მხოლოდ ჩვეულებრივი კატეგორიის მონაცემებზე და რატომ არის შეზღუდული თანხმობის საფუძველზე დამუშავებულ განსაკუთრებული კატეგორიის მონაცემების (განსაკუთრებით, ჯანმრთელობასთან დაკავშირებული მონაცემების) პორტირების უფლება, მაშინ, როდესაც ჯანდაცვის თანამედროვე სისტემებისა და ამ სფეროში გამოყენებული ელექტრონული ბაზების გათვალისწინებით, ეს ერთ-ერთი ყველაზე მოთხოვნადი და მარტივად რეალიზებადია. ასევე, მიზანშეწონილია, ევროპული რეგულაციის პრეამბულის 68-ე პუნქტის მსგავსად, კანონპროექტითაც ხაზი გაესვას იმ გარემოებას, რომ პორტირების უფლება არ გამორიცხავს მონაცემთა სუბიექტის მიერ პერსონალური მონაცემების წაშლის მოთხოვნას ან სუბიექტისთვის მინიჭებული სხვა უფლებებით სარგებლობას. ვფიქრობთ, აღნიშნულის ხაზგასმა მნიშვნელოვანია თავად პორტირების უფლების არსის უკეთ გადმოსაცემად.

05 თანხმობის გამოხმობა

მონაცემთა სუბიექტის უფლებების ჯეროვნად რეალიზების ერთ-ერთი მნიშვნელოვანი ასპექტია მონაცემთა დამუშავებისას სუბიექტის თანხმობის, როგორც მონაცემთა დამუშავების საფუძვლის, სწორად გამოყენება და მონაცემთა სუბიექტისთვის საკუთარ თანხმობაზე უარის თქმის უფლების მინიჭება.

GDPR მონაცემთა სუბიექტს ანიჭებს უფლებას ნებისმიერ დროს, დამატებითი ახსნა-განმარტებების გარეშე გამოითხოვოს მონაცემთა დამუშავებაზე გაცემული თანხმობა, თუმცა აღნიშნული უფლება ინკორპორირებულია რეგულაციის ცალკე მუხლით დარეგულირებულ თანხმობის კრიტერიუმებში (მუხლი 7.3).

გარდა იმისა, რომ რეგულაცია აქამდე მოქმედი დირექტივის მსგავსად მონაცემთა სუბიექტს ანიჭებს უფლებას, ნებისმიერ დროს უარი თქვას მის მიერ გაცემულ თანხმობაზე, ახალი ჩანაწერით ასევე ხაზი გაესვა ამ უფლების რეალიზების ფორმას. მონაცემთა სუბიექტს უნდა ჰქონდეს საშუალება ისეთივე მარტივი/იმავე ფორმით თქვას უარი მის მიერ გაცემულ თანხმობაზე, რა ფორმითაც გასცა თანხმობა. მაგ. თუ თანხმობა გაცემულია ონლაინ რამე ფორმის შევსებით, მონაცემთა სუბიექტს უნდა ჰქონდეს საშუალება იმავე ფორმით თქვას უარი თანხმობაზე.

კანონპროექტი

მუხლი 22. თანხმობის გამოხმობის უფლება

1. მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, ყოველგვარი განმარტების ან დასაბუთების გარეშე გამოიხმოს მის მიერ გაცემული თანხმობა. ამ შემთხვევაში, სუბიექტის მოთხოვნის შესაბამისად, მონაცემთა დამუშავება უნდა შეწყდეს ან/და დამუშავებული მონაცემები წაიშალოს ან განადგურდეს მოთხოვნიდან არაუგვიანეს 10 (ათი) სამუშაო დღისა, თუ არ არსებობს მონაცემთა დამუშავების სხვა საფუძველი.

2. მონაცემთა სუბიექტს უფლება აქვს თანხმობა გამოიხმოს იმავე ფორმით რა ფორმითაც განაცხადა თანხმობა.
3. მონაცემთა სუბიექტს თანხმობის გამოხმობამდე უფლება აქვს მონაცემთა დამმუშავებლისგან მოითხოვოს და მიიღოს ინფორმაცია თანხმობის გამოხმობის შესაძლო შედეგების შესახებ.

4. ამ მუხლის მოქმედება არ ვრცელდება მონაცემთა სუბიექტის მიერ ქონებრივი ან/და ფულადი ვალდებულებების შესრულების შესახებ მისივე თანხმობით დამუშავებულ მონაცემებზე.

შეფასება/რეკომენდაცია

კანონპროექტით გათვალისწინებული დათქმა, რომ მონაცემთა სუბიექტის მიერ თანხმობის გამოხმობის უფლება არ ვრცელდება ქონებრივი და/ან ფულადი ვალდებულებების შესრულების შესახებ დამუშავებულ მონაცემებზე (მუხლი 22.4), არსებითად არასწორად მიგვაჩნია. გასაგებია, რომ ამ ჩანაწერის პროექტში გაჩენის წინაპირობა ქართული კომპანიების მიერ თანხმობის, როგორც მონაცემთა დამუშავების საფუძვლის, ‚არასწორი გამოყენების პრაქტიკაა, როდესაც მსხვილი საფინანსო ინსტიტუტებიც კი ‘არ იწუხებდნენ’ თავს მონაცემთა დამუშავების ლეგიტიმური საფუძვლების იდენტიფიცირებით და მარტივ გზას – მონაცემთა სუბიექტის თანხმობის მოპოვებას ირჩევდნენ. სწორედ ამიტომ პრაქტიკაში ხშირად გამოითქმის კრიტიკული მოსაზრება ქცევის ამ მოდელის შესახებ.

მიუხედავად პრაგმატული მიზეზებისა (მათ შორის კომპანიებში არსებული ბიზნეს-პროცესები), 22-ე მუხლის მე-4 პუნქტის კანონპროექტში ამ სახით დატოვება არ ემსახურება თანხმობის ერთ-ერთი ძირეული ასპექტის (ნების თავისუფალი გამოვლენა) სწორად გაგებას. აქვე ხაზგასასმელია, რომ ამავე მუხლის პირველი პუნქტი ისედაც ითვალისწინებს, მონაცემთა შემდგომ დამუშავებას, თუ არ არსებობს მონაცემთა დამუშავების სხვა საფუძველი, მათ შორის მონაცემთა დამმუშავებლის ან მესამე პირის აღმატებული ინტერესი. შესაბამისად, არ არსებობს 22.4-ე მუხლის ამ ფორმულირებით დატოვების არც სამართლებრივი და არც პრაქტიკული მიზეზი.

დამატებით, გარდამავალი დებულებებით შესაძლებელია მონაცემთა დამმუშავებლებს მიეცეთ გონივრული ვადა „ქონებრივი ან/და ფულადი ვალდებულებების შესახებ“ მონაცემების დამუშავების რეალური საფუძვლების განსაზღვრისთვის.

06 მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში და მონაცემთა დაცვა პირველად პარამეტრად

მონაცემთა დაცვის მაღალი სტანდარტის უზრუნველსაყოფად რეგულაცია მონაცემთა დამმუშავებლებს ავალდებულებს რიგი ორგანიზაციულ-ტექნიკური ზომების მიღებას, მათ შორის ორი მნიშვნელოვანი პრინციპის დაცვას - მონაცემთა დაცვის სტანდარტების გათვალისწინებას ახალი პროდუქტის ან მომსახურების შექმნის პროცესში („Privacy by Design“) და მონაცემთა დაცვას პირველად პარამეტრად (Privacy by Default) .

ამ პრინციპების დაცვა მონაცემთა უსაფრთხოებასთან დაკავშირებული შემდგომი რისკების თავიდან აცილების მნიშვნელოვანი წინაპირობაა და უზრუნველყოფს მხოლოდ კანონიერი, კონკრეტული და მკაფიო მიზნის ადეკვატური მოცულობით მონაცემების დამუშავებას, მათ შორის მონაცემთა ბაზებისა და ონლაინ სერვისების შემუშავების საწყის ეტაპზევე. მნიშვნელოვანია, რომ პირადი ცხოვრებისადმი მეგობრული პირველადი პარამეტრები ნორმას წარმოადგენდეს - მათ შორის სოციალურ ქსელებსა ან მობილურ აპლიკაციებში. ასევე, მინიმუმამდე იქნას დაყვანილი მონაცემების პირთა განუსაზღვრელი წრისათვის ავტომატურად ხელმისაწვდომობა, გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა.

ამ პრინციპების დაცვა მონაცემთა დამმუშავებლისგან მოითხოვს გარკვეული ზომების მიღებას, რომელთა შორისაა:

- მონაცემთა სათანადო აღრიცხვა, კლასიფიცირება, განცალკევება;
- პროცესისა და სისტემის იმგვარი დაგეგმვა, რომ დამუშავების მიზნის მიღწევისა და შენახვის ვადის ამოწურვის შემდეგ შესაბამისი მონაცემები ავტომატურად წაიშალოს;
- მონაცემთა ანონიმიზაცია და ფსევდონომიზაცია;
- მონაცემთა იმგვარი ფორმით შენახვა (სტრუქტურიზებულ, გამოყენებად და ელექტრონულ ფორმატში), რომელიც გააადვილებს მონაცემთა პორტირების მოთხოვნებზე სათანადო რეაგირებას.

კანონპროექტი

მუხლი 26. მონაცემთა დამუშავების დაგეგმვის პროცესთან დაკავშირებული ვალდებულებები

1. მონაცემთა დამუშავების დაგეგმვისას მონაცემთა დამუშავების მიზნების, ფარგლების, მონაცემთა კატეგორიის, მოცულობის, მათზე წვდომის და მონაცემთა სუბიექტის უფლებების დარღვევის საფრთხის გათვალისწინებით, მონაცემთა დამმუშავებელმა უნდა მიიღოს ისეთი ორგანიზაციულ-ტექნიკური ზომები, რომელიც მაქსიმალურად უზრუნველყოფს მონაცემთა დამუშავების პრინციპებისა და ამ კანონით გათვალისწინებული სხვა ვალდებულებების ეფექტიან დაცვას.

2. მონაცემთა დამმუშავებელი ვალდებულია მონაცემთა ავტომატური დამუშავებისთვის მიიღოს ისეთი ორგანიზაციულ-ტექნიკური ზომები, რომლებიც მონაცემთა სუბიექტის მიერ განხორციელებული მოქმედების ან მონაცემთა დამმუშავებლის ადამიანური რესურსის ჩართულობის გარეშე, გამორიცხავს მონაცემების პირთა განუსაზღვრელი წრისათვის ავტომატურად ხელმისაწვდომობას, გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა.

შეფასება/რეკომენდაცია

შემოთავაზებულ რედაქციაში, კერძოდ, კანონპროექტის 26-ე მუხლში არასრულადაა წარმოდგენილი privacy by default პრინციპის კომპონენტები, დავიწროებულია ამ პრინციპის შინაარსი, კერძოდ:

- კანონპროექტით ეს პრინციპი ეხება მხოლოდ მონაცემთა ავტომატურ დამუშავებას;
- კანონპროექტით შემოთავაზებული რედაქცია მხოლოდ მონაცემთა ხელმისაწვდომობის საკითხს არეგულირებს, მაშინ, როცა რეგულაცია განსაზღვრავს კონკრეტულ ტექნიკურ და ორგანიზაციულ ზომებს, რათა თავისთავად/იმთავითვე თითოეული კონკრეტული მიზნისთვის მხოლოდ აუცილებელი მონაცემები დამუშავდეს.

მნიშვნელოვანია, ამ პრინციპებთან დაკავშირებით GDPR-ის მიდგომები სრულად იქნას ასახული ქართულ კანონმდებლობაში. შესაბამისად, მიზანშეწონილია კანონპროექტში, რეგულაციის პრემაბულის 78-ე პუნქტისა და 25-ე მუხლის მსგავსად დაკონკრეტდეს, რომ ამ პრინციპებთან შესაბამისობის დასადასტურებლად მონაცემთა დამმუშავებელმა უნდა შეიმუშაოს შიდა პოლიტიკა და გაატაროს ისეთი ღონისძიებები, როგორებიცაა მონაცემთა დამუშავების მინიმიზაცია, მონაცემების ფსევდონიმიზაცია შეძლებისდაგვარად მოკლე დროში, მონაცემთა დამუშავების გამჭვირვალობა და სხვა.

07 მონაცემთა დამუშავების ზეგავლენის შეფასება DPIA

GDPR-ი ამკვიდრებს მონაცემთა დამუშავების ზეგავლენის შეფასების კონცეფციას. ეს არის პროცესი, რომლის საშუალებითაც ორგანიზაციებს შეუძლიათ სისტემატურად შეაფასონ მათი ნებისმიერი პროდუქტისა თუ მომსახურების გავლენა ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვაზე. მონაცემთა დამუშავების ზეგავლენის შეფასება გულისხმობს მონაცემთა დამუშავების თითოეული სისტემისათვის მონაცემთა დაცვის რისკების სისტემური ანალიზის, გამოვლენისა და მინიმიზაციის პროცესს.

მონაცემთა დამუშავების ზეგავლენის შეფასება მონაცემთა დამმუშავებელს აძლევს პროცესებისა და პროდუქტების სისტემატური და სიღრმისეული ანალიზის, მონაცემთა დაცვასთან დაკავშირებული რისკების გამოვლენისა და აღმოფხვრის საშუალებას, რაც, თავის მხრივ, დადებით გავლენას ახდენს მომხმარებელთა ნდობის განმტკიცებაზეც. მონაცემთა დამუშავების ზეგავლენის შეფასება ასევე მნიშვნელოვანი ინსტრუმენტია ანგარიშვალდებულებისა და გამჭვირვალობის პრინციპების დაცვისა და მარეგულირებელ კანონმდებლობასთან შესაბამისობის დემონსტრირებისთვის.

კანონპროექტი

1. თუ მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნების და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებების შელახვის საფრთხე, მონაცემთა დამმუშავებელი ვალდებულია წინასწარ განახორციელოს მონაცემთა დამუშავების ზეგავლენის შეფასება.

2. გარდა პირველი პუნქტით გათვალისწინებული შემთხვევისა, მონაცემთა დამუშავების ზეგავლენის შეფასების განხორციელება სავალდებულოა თუ მონაცემთა დამმუშავებელი:

ა) მონაცემთა სუბიექტისათვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებს პროფილირების საფუძველზე;
ბ) ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემებს ან ახორციელებს მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში....

6. მონაცემთა სუბიექტების დიდ რაოდენობად მიიჩნევა საქართველოს მოსახლეობის არანაკლებ 3%-სა, რომელიც გამოითვლება მოსახლეობის საყოველთაო აღწერის ბოლო შედეგების მიხედვით.

შეფასება/რეკომენდაცია

მონაცემთა დამუშავების ზეგავლენის შეფასებასთან (DPIA) მიმართებით უნდა გამოიკვეთოს რამდენიმე პრობლემური საკითხი:

კანონპროექტის 31-ე მუხლის პირველი პუნქტი განსაზღვრავს მონაცემთა დამუშავების ზეგავლენის შეფასების ზოგად წესს და მონაცემთა დამმუშავებლებს ავალდებულებს წინასწარ განახორციელონ მონაცემთა დამუშავების ზეგავლენის შეფასება, თუ მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებების შელახვის საფრთხე. არსებული რედაქციით, შეფასების მიღმა შეიძლება დარჩეს კანონის ამოქმედებამდე დანერგილი მონაცემთა დამუშავების მოცულობითი და მნიშვნელოვანი პროცესები, რომლებიც ვერ დააკმაყოფილებენ ამავე მუხლის მე-2 პუნქტით გათვალისწინებულ კრიტერიუმებს, ვინაიდან კანონპროექტი ცალსახად ითვალისწინებს დათქმას ზეგავლენის შეფასების წინასწარ ჩატარების თაობაზე. შესაბამისად, მიზანშეწონილად მიგვაჩნია, გარდამავალი დებულებებით დადგინდეს გონივრული ვადა, რომლის განმავლობაშიც მონაცემთა დამუშავების ზეგავლენის შეფასების ვალდებულება გავრცელდება კანონის ამოქმედებამდე დაგეგმილ და მიმდინარე სისტემებთან მიმართებითაც, თუ მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნების და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებების შელახვის საფრთხე.

მონაცემთა სუბიექტების დიდ რაოდენობად მოსახლეობის არანაკლებ 3%-ის (წლევანდელი მონაცემებით დაახლოებით 110 000-ზე მეტი ადამიანის) მიჩნევა მნიშვნელოვნად ავიწროებს ამ მუხლის ან მთლიანად ამ ინსტრუმენტის (DPIA) მიზნებს, მიზანშეწონილად მიგვაჩნია 3%-ის მინიმუმ განახევრება და 1.5%-მდე შემცირება, რაც უზრუნველყოფს, მათ შორის, რიგი საჯარო დაწესებულებების, სადაზღვევო კომპანიებისა და ჯანდაცვის სექტორის პროვაიდერების მიერ მონაცემთა დამუშავების ზეგავლენის შეფასებას.

08 მონაცემთა უსაფრთხოება

პერსონალურ მონაცემთა დაცვის ერთ-ერთი ცენტრალური საკითხია მონაცემთა უსაფრთხოება.

სწორედ საკითხის მნიშვნელობის გამო GDPR-მა, გარდა კონკრეტული მუხლებისა და ვალდებულებების გათვალისწინებისა, მონაცემთა უსაფრთხოება პრინციპების დონეზეც განამტკიცა, როგორც მონაცემთა მთლიანობისა და კონფიდენციალურობის პრინციპი.

ეს პრინციპი გულისხმობს მონაცემთა იმგვარ დამუშავებას, რომ ორგანიზაციული და ტექნიკური საშუალებების გამოყენებით უზრუნველყოფილი იქნას მათი დაცვა, მათ შორის, არაავტორიზებული წვდომისგან, უკანონო დამუშავებისგან, შემთხვევითი დაკარგვისგან, განადგურების ან დაზიანებისგან. მონაცემთა მთლიანობასა და კონფიდენციალურობაზე ზრუნვის პრინციპის დონეზე განმტკიცება კიდევ უფრო უსვამს ხაზს მის მნიშვნელობას და რეგულაციასთან შესაბამისობის უზრუნველსაყოფად ორგანიზაციებს მოუწევთ ადეკვატური რესურსის გაღება.

მონაცემთა უსაფრთხოება რეგულაციაში განმტკიცებულია მონაცემთა დამმუშავებლების რიგი ვალდებულებებით, კონკრეტული ტექნიკური თუ ორგანიზაციული ზომებით. ერთ-ერთი ასეთი ვალდებულება მოცემულია რეგულაციის 32-ე მუხლში, რომელიც დამუშავების უსაფრთხოებას შეეხება და ადგენს უსაფრთხოების ისეთი ზომების მიღებას, როგორიცაა შიდა პოლიტიკის დოკუმენტების არსებობა, მონაცემთა დამუშავების მინიმიზაცია, დაუყოვნებელი ფსევდონიმიზაცია, მონაცემთა დამუშავების პროცესის გამჭვირვალობა, მონაცემთა სუბიექტების უფლებების ეფექტური რეალიზაცია და სხვა.

აღნიშნული ვალდებულების შესრულების დემონსტრირება ასევე შესაძლებელია ქცევის კოდექსის ან რეგულაციით გათვალისწინებული სერტიფიკაციის მოთხოვნის დაცვით.

კანონპროექტი

მუხლი 27. მონაცემთა უსაფრთხოება

1.მონაცემთა დამმუშავებელმა უნდა მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები მონაცემთა ამ კანონის შესაბამისად დამუშავების უზრუნველსაყოფად და უნდა შეძლოს მონაცემთა დამუშავების ამ კანონთან შესაბამისობის დადასტურება.

2.მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ვალდებულია, მიიღოს მონაცემთა დამუშავების შესაძლო და თანმდევი საფრთხეების შესაბამისი ორგანიზაციული და ტექნიკური ზომები (მათ შორის, მონაცემთა ფსევდონიმიზაცია, მონაცემებთან წვდომის აღრიცხვა, ინფორმაციული უსაფრთხოების მექანიზმები და სხვა), რომლებიც უზრუნველყოფენ მონაცემთა დაცვას უკანონო დამუშავების, შემთხვევითი დაკარგვის, განადგურების ან წაშლისგან.

3.მონაცემთა უსაფრთხოების უზრუნველსაყოფად აუცილებელი ორგანიზაციულ-ტექნიკური ზომების განსაზღვრისას დამმუშავებელმა და უფლებამოსილმა პირმა უნდა გაითვალისწინონ მონაცემთა კატეგორიები, მოცულობა, მონაცემთა დამუშავების მიზანი, ფორმა, საშუალებები და მონაცემთა სუბიექტის უფლებების დარღვევის შესაძლო საფრთხეები, ასევე, პერიოდულად შეაფასონ მონაცემთა უსაფრთხოების უზრუნველყოფის მიზნით მიღებული ტექნიკური და ორგანიზაციული ზომების ეფექტიანობა და საჭიროების შემთხვევაში, უზრუნველყონ მონაცემთა უსაფრთხოების დაცვისათვის ადეკვატური ზომების მიღება ან/და არსებულის განახლება.

შეფასება/რეკომენდაცია

მუხლის შინაარსი და შემოთავაზებული ფორმულირება ძირითადად შეესაბამება რეგულაციის ძირითად დებულებებს, თუმცა მიზანშეწონილია მუხლის სათაურის ცვლილება. მნიშვნელოვანია, კანონპროექტის 27-ე მუხლის სათაური შეესატყვისებოდეს რეგულაციის 32-ე მუხლის სათაურს – „მონაცემთა დამუშავების უსაფრთხოება“, რომელიც თავისთავად უფრო ფართოდ აწესრიგებს საკითხს, მონაცემთა დამუშავების მთლიან პროცესზე აკეთებს აქცენტს და არა მხოლოდ კონკრეტული მონაცემების უსაფრთხოებაზე.

ასევე, მნიშვნელოვანია რეგულაციის მიერ (მუხლის რედაქციით და შესაბამისი დეკლარაციული ნაწილით (recitles) იმ კონკრეტული ღონისძიებების უფრო დეტალურად ჩამოთვლა, რომლებიც შეიძლება იგულისხმებოდეს ორგანიზაციულ და/ან ტექნიკურ ზომებში და რომელთა არსებობაც უზრუნველყოფს მონაცემთა უსაფრთხოებას და აღნიშნულის დემონსტრირებას/დადასტურებას.

სასურველია, კანონის პროექტში უფრო დეტალურად გაიწეროს აღნიშნული ორგანიზაციული თუ ტექნიკური ზომები და განივრცოს და დაკონკრეტდეს მე-2 პუნქტში მოცემული ჩამონათვალი, კერძოდ: მე-2 მუხლში ფრჩხილებში არსებულ ჩანაწერს დაემატოს სერტიფიცირებული სისტემების გამოყენება, მონაცემთა დაცვის შიდა პოლიტიკის დოკუმენტების შემუშავება, დაშიფვრა, თაღლითობის პრევენციის სისტემები.

კანონპროექტი

4. მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ვალდებულია, უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების (მათ შორის, ინციდენტების შესახებ ინფორმაციის) აღრიცხვა. არაელექტრონული ფორმით არსებულ მონაცემთა დამუშავებისას მონაცემთა დამმუშავებელი ვალდებულია, უზრუნველყოს მონაცემთა გამჟღავნებასთან ან/და ცვლილებასთან დაკავშირებული ყველა მოქმედების აღრიცხვა.

5. მონაცემთა დამმუშავებელის და უფლებამოსილი პირის ნებისმიერი თანამშრომელი, რომელიც მონაწილეობს მონაცემთა დამუშავებაში ან აქვს წვდომა მონაცემებთან, ვალდებულია არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს, დაიცვას მონაცემთა საიდუმლოება და კონფიდენციალურობა, მათ შორის, სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგ.

6. მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ვალდებულია თანამშრომელთა უფლებამოსილებების შესაბამისად განსაზღვროს მათი მონაცემებზე წვდომის ფარგლები და გაატაროს ადეკვატური ღონისძიებები თანამშრომელთა მიერ მონაცემთა უკანონო დამუშავების ფაქტების თავიდან ასაცილებლად, გამოსავლენად და აღსაკვეთად, მათ შორის უზრუნველყოს თანამშრომელთა ინფორმირება მონაცემთა უსაფრთხოების დაცვის საკითხებზე.

შეფასება/რეკომენდაცია

09 მონაცემთა დაცვის ოფიცერი (DPO) – საკითხის მნიშვნელობა/ ევროპული მიდგომა

კანონპროექტი ითვალისწინებს ახალი ინსტიტუტის – მონაცემთა დაცვის ოფიცრის ამოქმედებას და გარკვეული კატეგორიის ორგანიზაციების მიერ ოფიცრების სავალდებულო წესით დანიშვნას. მონაცემთა დაცვის ოფიცრის სავალდებულო დანიშვნის წესი GDPR-მა დაამკვიდრა, თუმცა ეს ინსტიტუტი ევროკავშირის რამდენიმე წევრ ქვეყანაში მანამდეც არსებობდა, ბოლო წლებში კი ევროკავშირის სივრცეში მომუშავე კომპანიები და ინსტიტუტები პრაქტიკული საჭიროებიდან გამომდინარე ოფიცრებს ნებაყოფლობით ნიშნავდნენ. აღსანიშნავია, რომ ოფიცრის ინსტიტუტი უკვე გვხვდება ქართულ რეალობაშიც – ცალკეულ საჯარო დაწესებულებებსა და მსხვილ კერძო ორგანიზაციებს განსაზღვრული ჰყავთ ორგანიზაციის შიგნით მონაცემთა დაცვაზე პასუხისმგებელი პირები/სტრუქტურული ერთეულები.

მონაცემთა დაცვის ოფიცერი GDPR-ით გათვალისწინებული ახალი – ანგარიშვალდებულების პრინციპის უზრუნველყოფის ერთ-ერთ ქვაკუთხედად განიხილება. ანგარიშვალდებულების პრინციპი გულისხმობს GDPR-თან შესაბამისობის დემონსტრირებას. აღნიშნული კი სხვადასხვა ორგანიზაციულ-ტექნიკური ზომების გატარებითაა შესაძლებელი, მაგალითად: მონაცემთა დაცვის შიდა პოლიტიკებისა და პროცედურების დანერგვით, მონაცემთა დაცვის საკითხებზე ორგანიზაციის თანამშრომელთა ცნობიერების ამაღლებით, საზედამხედველო ორგანოსთან თანამშრომლობით და ა.შ. ამ პროცესების კოორდინაციასა და წარმართვაში მონაცემთა დაცვის ოფიცერს გადამწყვეტი როლი ენიჭება.

ანგარიშვალდებულების პრინციპისა და მონაცემთა დაცვის დამუშავების მასშტაბის გათვალისწინებით ევროპელმა კანონმდებლებმა განსაზღვრეს მონაცემთა დაცვის თვალსაზრისით შედარებით მაღალი რისკების შემცველი ორგანიზაციათა წრე (კრიტერიუმები) და მათთვის სავალდებულო გახადეს მონაცემთა დაცვის ოფიცრის დანიშვნა. ამასთან, დაადგინეს გარკვეული მოთხოვნები, მათ შორის ოფიცრის ფუნქციების, კვალიფიკაციის და ორგანიზაციის მმართველ რგოლთან ურთიერთობის კუთხითაც კი, რაც თავისთავად მიუთითებს ნებაზე, მონაცემთა დაცვის ოფიცრის ინსტიტუტი იყოს ეფექტიანი, ქმედითი და არა ფორმალური. მისასალმებელია შემოთავაზებული კანონპროექტით აღნიშნული ინსტიტუტის საქართველოში დანერგვა და მონაცემთა დამმუშავებლების იმ წრის განსაზღვრა, ვისთვისაც სავალდებულოა მონაცემთა დაცვის ოფიცრის დანიშვნა. აღნიშნული ინსტიტუტის ეფექტიან ფუნქციონირებას, მართლაც, შეუძლია არსებითი გავლენა მოახდინოს ქვეყანაში პერსონალური მონაცემების დაცვის სტანდარტების ამაღლებაზე და უზრუნველყოს ქართული კანონმდებლობისა და პრაქტიკის ევროკავშირის რეგულაციებთან და გამოცდილებასთან დაახლოება.

კანონპროექტი

მუხლი 33. პერსონალურ მონაცემთა დაცვის ოფიცერი

1. საჯარო დაწესებულება (გარდა რელიგიური და პოლიტიკური ორგანიზაციებისა), სადაზღვევო ორგანიზაცია, კომერციული ბანკი, მიკროსაფინანსო ორგანიზაცია, საკრედიტო ბიურო, ელექტრონული კომუნიკაციის კომპანია, ავიაკომპანია, აეროპორტი და ის სამედიცინო დაწესებულება, რომელიც მომსახურებას უწევს წელიწადში არანაკლებ 10000 მონაცემთა სუბიექტს, ასევე, ის მონაცემთა დამმუშავებელი/უფლებამოსილი პირი, რომელიც ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან ახორციელებს მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს, ვალდებულნი არიან დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი, რომელიც უზრუნველყოფს ... ...

4. პერსონალურ მონაცემთა დაცვის ოფიცერს უნდა ჰქონდეს სათანადო ცოდნა მონაცემთა დაცვის სფეროში. იგი ანგარიშვალდებულია მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის წინაშე.

5. მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა უნდა უზრუნველყოს პერსონალურ მონაცემთა დაცვის ოფიცრის სათანადო ჩართულობა მონაცემთა დამუშავებასთან დაკავშირებით მნიშვნელოვანი გადაწყვეტილების მიღების პროცესში და მისი დამოუკიდებლობა საქმიანობის განხორციელებისას.

შეფასება/რეკომენდაცია

პერსონალურ მონაცემთა დაცვის ოფიცრის ინსტიტუტის სავალდებულოდ შემოღებისა და მისი უფლება-მოვალეობების განსაზღვრის მიზანი მონაცემთა სუბიექტის უფლებების რეალიზაციისა და მონაცემთა დამუშავების კანონმდებლობასთან შესაბამისობის უზრუნველყოფისთვის ქმედითი და რეალური მექანიზმების შექმნაა. ამ თვალსაზრისით ძალიან მნიშვნელოვანია ისეთი საკანონმდებლო გარანტიების განსაზღვრა, რომელიც უზრუნველყოფს, ერთი მხრივ, მონაცემთა დაცვის ოფიცრის მიერ საკუთარი ფუნქციების ეფექტიან განხორციელებას, ხოლო, მეორე მხრივ, მისი საქმიანობის სათანადო პირობების შექმნას. ერთ-ერთი ასეთი გარანტია ევროპულ კანონმდებლობაში სწორედ მონაცემთა დაცვის ოფიცრის ანგარიშვალდებულებისა და როლის განსაზღვრაა – რეგულაციის 38-ე მუხლის მე-3 ნაწილით დადგენილია, რომ მონაცემთა დაცვის ოფიცერი უშუალოდ და პირდაპირ უმაღლეს მმართველ რგოლის წინაშეა ანგარიშვალდებული. შემოთავაზებულ კანონპროექტში ამგვარი მოთხოვნის არარსებობა ქმნის იმ საფრთხეს, რომ დაწესებულებებმა და კომპანიებმა მონაცემთა დაცვის პასუხისმგებლობა დააკისრონ საშუალო რგოლის რიგით თანამშრომელს, რომელსაც ბიუროკრატიული სისტემის გამო უშუალო კომუნიკაცია არ ექნება უმაღლეს მმართველობით რგოლთან, რაც მის დანიშვნას უბრალო ფორმალობად აქცევს და რეალურად ვერ უზრუნველყოფს მის ეფექტიან საქმიანობას. შესაბამისად, მიზანშეწონილია კანონპროექტის 33-ე მუხლის მე-4 პუნქტის ფორმულირება GDPR-ის მსგავსად, ჩამოყალიბდეს შემდეგი რედაქციით: „4. პერსონალურ მონაცემთა დაცვის ოფიცერს უნდა ჰქონდეს სათანადო ცოდნა მონაცემთა დაცვის სფეროში.

იგი ანგარიშვალდებულია მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის უმაღლესი მმართველობითი რგოლის წინაშე.

კანონპროექტი

6. მონაცემთა დამმუშავებელი/უფლებამოსილი პირი ვალდებულია, პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნიდან ან განსაზღვრიდან 10 (ათი) სამუშაო დღის ვადაში აცნობოს მისი ვინაობა და საკონტაქტო ინფორმაცია სახელმწიფო ინსპექტორის სამსახურს და ასევე გამოაქვეყნოს პროაქტიულად.

შეფასება/რეკომენდაცია

ასევე, სასურველია GDPR-ის 39.2 მუხლის მსგავსად, ქართულ კანონმდებლობაშიც აისახოს ოფიცრის ვალდებულება მონაცემთა დამუშავების რისკების გათვალისწინებასთან დაკავშირებით. ამ მიზნით, მიზანშეწონილია კანონპროექტის 33-ე მუხლის 1 პუნქტის „ვ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით „ვ) მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის მიერ მონაცემთა დამუშავების სტანდარტების ამაღლების მიზნით სხვა ფუნქციების შესრულებას, მათ შორის მონაცემთა დამუშავების მიზნების, ხასიათის, ფარგლების, ასევე მონაცემთა დამუშავებასთან დაკავშირებული რისკებისა და მონაცემთა შინაარსის გათვალისწინებით.“

10 ადმინისტრაციული ჯარიმები

პერსონალურ მონაცემთა დამუშავების წესების დარღვევისათვის როგორც ქართული, ისე სხვა ქვეყნების კანონმდებლობა, ითვალისწინებდა გარკვეულ ფინანსურ სანქციებს, თუმცა ფინანსური სანქციები ხშირად არ იყო/არ არის ეფექტიანი და ბიზნეს სუბიექტები ხშირად რამდენჯერმე ჯარიმის გადახდას ამჯობინებდნენ მონაცემთა დამუშავების პროცესის ცვლილებას და ამისთვის დამატებითი ხარჯის გაღებას.

რეგულაცია მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ვალდებულებებს ორ ჯგუფად ჰყოფს და ნაწილის დარღვევისათვის (მაგ. მონაცემთა დაცვა საფუძველში და თავისთავადი დაცულობა, მონაცემთა დაცვის ოფიცრის უფლებამოსილებები) ჯარიმის მაქსიმალურ შესაძლო ოდენობად განსაზღვრავს 10 მლნ ევროს ან საერთო წლიური ბრუნვის 2%, ხოლო სხვა ვალდებულებების დარღვევისათვის (მაგ. მონაცემთა დამუშავების პრინციპებისა და საფუძვლების დარღვევა, თანხმობის კრიტერიუმების დაუცველობა, განსაკუთრებული კატეგორიის მონაცემთა დამუშავების წესების დარღვევა, გადაწყვეტილებების ავტომატიზებულად მიღების წესების დარღვევა, მონაცემთა საერთაშორისო გადაცემა და სხვა) – 20 მლნ ევრო ან საერთო წლიური ბრუნვის 4% -ს.

კანონპროექტი

თავი VII, მუხლები – 47-65

ჯარიმის მინიმალური ოდენობა – 1000 ლარი, მაქსიმალური ოდენობა – 10 000 ლარი, ხოლო ერთი და იმავე დამმუშავებლის მიერ ჩადენილი რამდენიმე დარღვევის განხილვისას, ჯამურად – 20 000 ლარი.

შეფასება/რეკომენდაცია

მიუხედავად იმისა, რომ შემოთავაზებული კანონპროექტით მნიშვნელოვნად გაიზარდა ფინანსური ჯარიმების მინიმალური ოდენობა, ჯარიმის მაქსიმალური ოდენობა – 10 000 ლარი უცვლელი დარჩა.

ვფიქრობთ, არსებული მდგომარეობიდან და მონაცემთა დამუშავების წესების დარღვევების ხასიათიდან გამომდინარე (უკანონო ვიდეო-აუდიო თვალთვალი კერძო კომპანიების მხრიდანაც, დიდი მოცულობის ელექტრონული ბაზების არსებობა და მათთან მოპყრობის წესების არარსებობა, ორგანიზაციებში მონაცემთა დაცვის კულტურის არარსებობა და ა.შ), ასევე იმის გათვალისწინებით, რომ კანონპროექტი ასევე გვთავაზობს ადმინისტრაციული პასუხისმგებლობის შემამსუბუქებელ და დამამძიმებელ გარემოებებს და შემამსუბუქებელი გარემოებები იწვევს ჯარიმის ოდენობის შემცირებას, ქართული კომპანიებისათვის თუნდაც 10 000 ან 20 000 ლარიანი ჯარიმის დაკისრება ვერ იქნება იმ რეალური შედეგის მომტანი, რასაც შეიძლება მიზნად ისახავდეს ფინანსური სანქციები.

რა თქმა უნდა, ქართული რეალობიდან გამომდინარე ჯარიმების ოდენობა ვერ იქნება ევროპული რეგულაციის იდენტური და ქართულ კომპანიებს არ უნდა დაეკისროს რამდენიმე მილიონი ლარის გადახდა მონაცემთა დამუშავების წესების დარღვევისათვის, თუმცა მას მინიმუმ ე.წ „მსუსხავი ეფექტი“ მაინც უნდა ჰქონდეს კომპანიებისათვის, წინააღმდეგ შემთხვევაში, ასეთი მიდგომა და ჯარიმების აღნიშნული ოდენობა ეჭვქვეშ აყენებს სანქციების ეფექტიანობასა და პროპორციულობას.

ყოველივე აღნიშნულიდან გამომდინარე, მიზანშეწონილად მიგვაჩნია კანონპროექტის მე-7 თავით შემოთავაზებული ჯარიმების ოდენობის გაორმაგდება.