პერსონალურ მონაცემთა
დაცვის სამსახური

პერსონალურ მონაცემთა დაცვის სახელმძღვანელო რეკომენდაციები

მცირე და საშუალო ზომის მეწარმე სუბიექტებისათვის

მონაცემთა დაცვის რეკომენდაციები

ბიზნესისთვის

ნაწილი I. პერსონალურ მონაცემთა დაცვის ძირითადი საკითხები

ტერმინოლოგია

რა არის პერსონალური მონაცემი?

პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს უკავშირდება.

ფიზიკური პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, მათ შორის:

- სახელით, გვარით, ტელეფონის ნომრით;
- საიდენტიფიკაციო ნომრით;
- გეოლოკაციის მონაცემებით;
- ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემებით;
- ფიზიკური, ფიზიოლოგიური, ფსიქიკური, ფსიქოლოგიური, გენეტიკური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლით.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-3 მუხლის „ა“ პუნქტი.

რა არის განსაკუთრებული კატეგორიის მონაცემი?

ზოგიერთი პერსონალური მონაცემი, რომელსაც განსაკუთრებული კატეგორიის მონაცემებს საჭიროებენ დაცვის უფრო მაღალ სტანდარტს.

ამგვარ კატეგორიას მიეკუთვნება მონაცემი, რომელიც უკავშირდება ფიზიკური პირის:

- რასობრივ ან ეთნიკურ კუთვნილებას;
- პოლიტიკურ შეხედულებებს;
- რელიგიურ, ფილოსოფიურ ან სხვაგვარ მრწამსს;
- პროფესიული კავშირის წევრობას;
- ჯანმრთელობას, სქესობრივ ცხოვრებას;

- ბიომეტრიულ და გენეტიკურ მონაცემებს, რომლებიც ფიზიკური პირის უნიკალური იდენტიფიცირების მიზნით მუშავდება.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-3 მუხლის „ბ“ პუნქტი.

რას ნიშნავს პერსონალური მონაცემების დამუშავება?

მონაცემთა დამუშავება არის მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედება, მათ შორის, მათი შეგროვება, მოპოვება, მათზე წვდომა, მათი ფოტოგადაღება, ვიდეომონიტორინგი ან/და აუდიომონიტორინგი, ორგანიზება, დაჯგუფება, ურთიერთდაკავშირება, შენახვა, შეცვლა, აღდგენა, გამოთხოვა, გამოყენება, დაბლოკვა, წაშლა ან განადგურება, აგრეთვე მონაცემთა გამჟღავნება მათი გადაცემით, გასაჯაროებით, გავრცელებით ან სხვაგვარად ხელმისაწვდომად გახდომით;

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-3 მუხლი.

ვინ არიან მონაცემთა დამუშავების პროცესში ჩართული პირები?

დამუშავებისთვის პასუხისმგებელი პირი შესაძლოა იყოს ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, უშუალოდ ან დამუშავებაზე უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას;

მონაცემთა სუბიექტი – ნებისმიერი ფიზიკური პირი, რომლის შესახებ მონაცემი მუშავდება;

თანადამუშავებისთვის პასუხისმგებელი პირები – დამუშავებისთვის პასუხისმგებელი ორი ან ორზე მეტი პირი, რომლებიც ერთობლივად განსაზღვრავენ მონაცემთა დამუშავების მიზნებსა და საშუალებებს;

დამუშავებაზე უფლებამოსილი პირი – ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც მონაცემებს ამუშავებს დამუშავებისთვის პასუხისმგებელი

პირისთვის ან მისი სახელით. დამუშავებაზე უფლებამოსილ პირად არ მიიჩნევა დამუშავებისთვის პასუხისმგებელ პირთან შრომით ურთიერთობაში მყოფი ფიზიკური პირი.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-3 მუხლი.

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის გასათვალისწინებელი პუნქტები:

- ✓ დაფიქრდით, რამდენად შეესაბამება პერსონალური მონაცემების დამუშავების პროცესი განსაზღვრულ მიზანს;
- ✓ პერსონალური მონაცემები დაამუშავეთ მხოლოდ იმ მოცულობით, რაც საჭიროა განსაზღვრული მიზნის მისაღწევად;
- ✓ აცნობეთ მონაცემთა სუბიექტებს იმის შესახებ, თუ როგორ და რა მიზნებისთვის შეიძლება დამუშავდეს მათი პერსონალური მონაცემები;
- ✓ შეამოწმეთ, გაქვთ თუ არა შესაბამისი სამართლებრივი საფუძველი პერსონალური მონაცემების დამუშავებისთვის;
- ✓ დარწმუნდით, რომ თქვენს ხელთ არსებული პერსონალური მონაცემები დაცულია;
- ✓ შეინახეთ მონაცემთა სუბიექტის პერსონალური მონაცემები ზუსტი და განახლებული სახით;
- ✓ წაშალეთ ფიზიკური პირის პერსონალური მონაცემები, როდესაც მისი დამუშავება საჭირო აღარ არის.

„პერსონალურ მონაცემთა დაცვის“ შესახებ საქართველოს კანონის მოქმედების სფერო

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედება ვრცელდება:

- საქართველოს ტერიტორიაზე მონაცემთა ავტომატური საშუალებებით დამუშავებასა და ნახევრად ავტომატური საშუალებებით დამუშავებაზე;
- იმ მონაცემთა არაავტომატური საშუალებებით დამუშავებაზე, რომლებიც ფაილური სისტემის ნაწილია ან ფაილურ სისტემაში შესატანად მუშავდება;
- საქართველოს ფარგლების გარეთ რეგისტრირებული დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა საქართველოში არსებული ტექნიკური საშუალებების გამოყენებით დამუშავებაზე, გარდა იმ შემთხვევისა, როდესაც ტექნიკური საშუალებები მხოლოდ მონაცემთა ტრანზიტისთვის გამოიყენება.

მოქმედების სფეროსთან დაკავშირებით იხილეთ სრულად:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-2 მუხლი.

პერსონალურ მონაცემთა დამუშავების პრინციპები

პერსონალური მონაცემების დამუშავების კანონიერების მიზნით, დაცული უნდა იყოს პერსონალურ მონაცემთა დამუშავების პრინციპები. გარდა ამისა, მნიშვნელოვანია, რომ ორგანიზაციას აკისრია დამუშავების პრინციპებთან შესაბამისობის მტკიცების ტვირთი:

კანონიერება, სამართლიანობა, გამჭვირვალობა და მონაცემთა დამუშავება მონაცემთა სუბიექტის ღირსების შეულახავად:

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

პერსონალურ მონაცემთა კანონიერი დამუშავება გულისხმობს, რომ მონაცემები უნდა დამუშავდეს მხოლოდ მაშინ, როდესაც არსებობს შესაბამისი საფუძველი და დაცულია ყველა სამართლებრივი მოთხოვნა.

სამართლიანობა ყოვლისმომცველი პრინციპია, რომელიც მოითხოვს, რომ პერსონალური მონაცემები მონაცემთა სუბიექტის საზიანოდ, დისკრიმინაციულად არ

დამუშავდეს, არ აღმოჩნდეს მოულოდნელი ან შეცდომაში შემყვანი. ამ პრინციპის მიხედვით, მონაცემთა მოპოვება ან სხვაგვარად დამუშავება უსამართლო საშუალებებით, შეცდომაში შეყვანით ან მონაცემთა სუბიექტის ცოდნის გარეშე, დაუშვებელია.

გამჭვირვალობის პრინციპის მიხედვით, ფიზიკური პირებისთვის მათი მონაცემების დამუშავებამდე უნდა იყოს ნათელი, რომ მათთან დაკავშირებული პერსონალური მონაცემები შეგროვდება, გამოიყენება, ან სხვა სახით დამუშავდება. ამასთანავე, თუ პირებს ორგანიზაციის მიერ გარკვეული ინფორმაცია მიეწოდებათ მათი პერსონალური მონაცემების გამოყენებისა და საჭიროების შესახებ, აღნიშნული მათთვის გასაგები ენით უნდა განხორციელდეს.

მონაცემთა დამუშავების პროცესი უნდა წარიმართოს მონაცემთა სუბიექტის ღირსების შეულახავად და არ გამოიწვიოს ადამიანის უფლებებისა და თავისუფლებების შელახვის რისკი.

რეკომენდაციები:

- ✓ მონაცემთა დამუშავების დაწყებამდე უნდა განხორციელდეს დამუშავების კანონიერი საფუძვლის იდენტიფიცირება, მათ შორის, განსაკუთრებული კატეგორიის მონაცემების დამუშავების შემთხვევაში;
- ✓ დამუშავების შესახებ დეტალურ ინფორმაციას უნდა შეიცავდეს მონაცემთა დამუშავების პოლიტიკა, რომელიც დამუშავების ოპერაციების შესაბამისად პერიოდულად უნდა განახლდეს;
- ✓ უნდა შეფასდეს, რა გავლენა ექნება პერსონალურ მონაცემთა დამუშავებას მონაცემთა სუბიექტზე და უნდა დასაბუთდეს ყოველგვარი უარყოფითი ზემოქმედება მასზე;
- ✓ პერსონალური მონაცემები გამოყენებულ უნდა იქნეს მხოლოდ მონაცემთა სუბიექტის გონივრული მოლოდინის შესაბამისად ან განიმარტოს ნებისმიერი შემდგომი დამუშავების მიზანი;
- ✓ მონაცემთა შეგროვება არ უნდა განხორციელდეს მონაცემთა სუბიექტის მოტყუებით ან შეცდომაში შეყვანით;
- ✓ მონაცემთა სუბიექტებს ინფორმაცია უნდა მიეწოდოთ მათთვის გასაგები, მარტივად აღქმადი ფორმით, მკაფიო და მარტივი ენით;
- ✓ მონაცემთა დამუშავება არ უნდა ლახავდეს პირის ღირსებას.

კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზანი:

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

აღნიშნული პრინციპის თანახმად, დამუშავების ოპერაციის მიზნის განსაზღვრა მონაცემთა დაცვის კანონმდებლობის გამოყენებისა და მონაცემთა დაცვის სათანადო გარანტიების შემუშავებისთვის პირველი ეტაპია. ამასთანავე, მიზნის განსაზღვრა სხვა მოთხოვნების დაწესების წინაპირობას წარმოადგენს. მიზნის შეზღუდვის პრინციპი ადგენს საზღვრებს, რომლის ფარგლებშიც შესაძლებელია მოცემული მიზნისთვის შეგროვებული პერსონალური მონაცემების დამუშავება და შემდგომი გამოყენება.

რეკომენდაციები:

- ✓ წინასწარ უნდა განისაზღვროს პერსონალურ მონაცემთა დამუშავების მიზან(ებ)ი;
- ✓ სასურველია, განხორციელდეს, მონაცემთა დამუშავების მიზნ(ებ)ის დოკუმენტირება;
- ✓ დამუშავების მიზნ(ებ)ის შესახებ დეტალური ინფორმაცია მიაწოდოს მონაცემთა სუბიექტებს;
- ✓ რეგულარულად უნდა გადაიხედოს დამუშავების ოპერაციები და საჭიროების შემთხვევაში, განახლდეს შესაბამისი დოკუმენტაცია;
- ✓ თუ დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დამუშავება ხორციელდება თავდაპირველი მიზნისგან განსხვავებული მიზნით, უნდა შეფასდეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის მე-2 პუნქტით გათვალისწინებული შემთხვევები.

მონაცემთა მინიმიზაცია:

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

პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, როდესაც დამუშავების მიზნის მიღწევა, გონივრულობის ფარგლებში, შეუძლებელია სხვა საშუალებებით. დამუშავება არ უნდა იყოს არაპროპორციული ჩარევა მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებში და უნდა განხორციელდეს მხოლოდ იმ მოცულობით, რომელიც საჭიროა განსაზღვრული მიზნის მისაღწევად.

ამასთანავე, მონაცემთა მინიმიზაციის პრინციპი მჭიდრო კავშირშია მიზნის შეზღუდვის პრინციპთან და მისი დაცვა შესაძლებელია მხოლოდ იმ შემთხვევაში, როდესაც დამუშავებისთვის პასუხისმგებელი პირის მიერ კონკრეტული მიზნები მკაფიოდაა განსაზღვრული. მან მიზნის მიღწევის აუცილებლობის დასადგენად, უნდა გადახედოს დამუშავების ოპერაციის თითოეულ საფეხურს და მონაცემთა თითოეულ ელემენტს.

რეკომენდაციები:

- ✓ უნდა შეგროვდეს მხოლოდ იმ რაოდენობის პერსონალური მონაცემები, რაც საჭიროა კონკრეტული მიზნ(ებ)ის მისაღწევად;
- ✓ პერსონალურ მონაცემები არ უნდა შეგროვდეს იმ განზრახვით, რომ ისინი მომავალში ჰიპოთეტურად სასარგებლო აღმოჩნდება;
- ✓ შეგროვებული მონაცემები მიზნ(ებ)ის მიღწევისთვის საკმარისი რაოდენობის (და არა უფრო მეტი) უნდა იყოს;
- ✓ პერიოდულად უნდა გადაიხედოს, რა მონაცემებს ფლობს პასუხისმგებელი პირი და თუ მონაცემთა შენახვის საჭიროება აღარ არსებობს, იგი უნდა წაიშალოს.

მონაცემთა ნამდვილობა და სიზუსტე:

კანონის მე-4 მუხლის პირველი პუნქტის „დ“ ქვეპუნქტის მიხედვით, „მონაცემები უნდა იყოს ნამდვილი, ზუსტი და, საჭიროების შემთხვევაში, განახლებული. მონაცემთა დამუშავების მიზნების გათვალისწინებით, არაზუსტი მონაცემები უნდა გასწორდეს, წაიშალოს ან განადგურდეს გაუმართლებელი დაყოვნების გარეშე.“

საგულისხმოა, რომ მონაცემთა დამუშავების მიზნ(ებ)ის გათვალისწინებით, პასუხისმგებელი პირი ვალდებულია გაუმართლებელი დაყოვნების გარეშე უზრუნველყოს არაზუსტ მონაცემთა გასწორება, წაშლა ან განადგურება.

ხსენებული პრინციპის დაცვის მიზნისთვის პასუხისმგებელმა პირმა, კონტექსტიდან გამომდინარე, ფაქტებზე დაფუძნებული მონაცემები უნდა განასხვაოს იმ მონაცემებისგან, რომლებიც პირად შეფასებას ეფუძნება. პირად შეფასებაზე დაფუძნებულ მონაცემებთან მიმართებით კანონის მე-4 მუხლის პირველი პუნქტის „დ“ ქვეპუნქტით გათვალისწინებული მონაცემთა დამუშავების პრინციპის ზედმიწევნით დაცვა სავალდებულო არ არის.

რეკომენდაციები:

- ✓ სასურველია, დაინერგოს შესაბამისი მონაცემების სიზუსტის შემოწმების პროცედურა, ასევე, აღირიცხოს ინფორმაცია მონაცემთა მოპოვების წყაროს შესახებ.
- ✓ უნდა დაინერგოს პერსონალურ მონაცემთა განახლების პროცედურა და საჭიროების შემთხვევაში, განახლდეს არაზუსტი მონაცემები.
- ✓ მცდარი ჩანაწერების დამუშავების საჭიროების შემთხვევაში, ჩანაწერებში ნათლად უნდა იყოს მითითებული, რომ იგი წარმოადგენს შეცდომას.
- ✓ პასუხისმგებელმა პირმა პატივი უნდა სცეს მონაცემთა სუბიექტის უფლებას, მოითხოვოს მის შესახებ მონაცემთა გასწორება და ყურადღებით განიხილოს მონაცემთა სიზუსტესთან დაკავშირებული ნებისმიერი გამოწვევა.
- ✓ პასუხისმგებელმა პირმა, კონტექსტიდან გამომდინარე, ფაქტებზე დაფუძნებული მონაცემები უნდა განასხვაოს იმ მონაცემებისგან, რომლებიც პირად შეფასებას ეფუძნება. ფაქტებზე დაფუძნებული მონაცემების მიმართ კი ზედმიწევნით დაიცვას ნამდვილობისა და სიზუსტის პრინციპი.
- ✓ თუ სუბიექტისგან დამოუკიდებლად გამოავლენს პასუხისმგებელი პირი, რომ მის ხელთ არსებული მონაცემები მცდარია, გონივრულ ვადაში უნდა გაასწოროს, განაახლოს ან/და შეავსოს მონაცემები.

მონაცემთა შენახვის ვადის შეზღუდვა:

კანონის მე-4 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტის თანახმად, „მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად“.

შენახვის ვადის შეზღუდვის პრინციპში მოიაზრება, რომ მონაცემები უნდა წაიშალოს ან განხორციელდეს მათი ანონიმიზაცია, დამუშავების მიზნის მიღწევისთანავე. შენახვის ვადის შეზღუდვის პრინციპი გულისხმობს, რომ პასუხისმგებელმა პირმა წინასწარ უნდა აცნობოს მონაცემთა სუბიექტს შენახვის პერიოდის შესახებ, ასევე, უნდა უზრუნველყოს პრინციპთან შესაბამისობის დემონსტრირება. შესაბამისად, შენახვის ვადები უნდა განისაზღვროს ორგანიზაციის შიგნით, მონაცემთა დამუშავების დაწყებამდე.

რეკომენდაციები:

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

მონაცემთა უსაფრთხოება

კანონის მე-4 მუხლის პირველი პუნქტის „ვ“ ქვეპუნქტის თანახმად, „მონაცემების უსაფრთხოების დაცვის მიზნით მონაცემთა დამუშავებისას მიღებული უნდა იქნეს ისეთი ტექნიკური და ორგანიზაციული ზომები, რომლებიც სათანადოდ უზრუნველყოფს მონაცემთა დაცვას, მათ შორის, უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვისგან, განადგურებისგან ან/და დაზიანებისგან“.

პერსონალური მონაცემების უსაფრთხოების დაცვა მოითხოვს შესაბამისი ტექნიკური და ორგანიზაციული ზომების დანერგვას, რომელთა მიზანია: მონაცემთა

უსაფრთხოების დარღვევის (ინციდენტის) თავიდან აცილება და მართვა; მონაცემთა დამუშავების ამოცანების სწორად შესრულება და სხვა პრინციპებთან შესაბამისობის უზრუნველყოფა; და პირთა უფლებების ეფექტიანად განხორციელების ხელშეწყობა.

რეკომენდაციები:

- ✓ უნდა გაანალიზდეს, რა რისკები შეიძლება ახლდეს მონაცემთა სუბიექტის მონაცემების დამუშავებას და აღნიშნული გათვალისწინებულ იქნეს უსაფრთხოების ღონისძიებების დანერგვის პროცესში;
- ✓ შესაძლებლობის შემთხვევაში, უსაფრთხოების ზომებად გამოყენებულ უნდა იქნეს ფსევდონიმიზაციის მექანიზმი და ასევე, სხვა ტექნიკური და ორგანიზაციული ღონისძიებები;
- ✓ უსაფრთხოების ზომები პერიოდულად უნდა გადაიხედოს და საჭიროების შემთხვევაში, განახლდეს.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-4 მუხლი.

პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები პერსონალურ მონაცემთა დამუშავების პრინციპების შესახებ, 2024.

მონაცემთა დამუშავების საფუძვლები

მონაცემების დამუშავების საფუძველია:

- მონაცემთა სუბიექტის თანხმობა;
- კანონით განსაზღვრული შემთხვევა/კანონმდებლობით განსაზღვრული საჭიროება;
- საჭიროება განცხადების განსახილველად/მომსახურების გასაწევად;
- კანონის შესაბამისად მონაცემების საჯაროდ ხელმისაწვდომობა/მონაცემთა სუბიექტის მიერ პირადი ინფორმაციის საჯაროდ ხელმისაწვდომობა;
- მესამე პირის/დამუშავებისთვის პასუხისმგებელი პირის აღმატებული კანონიერი ინტერესი.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-5 მუხლი.

მონაცემთა დაცვის ევროპული საბჭოს რეკომენდაცია 05/2020 თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით, 2020.

ფიზიკური პირის განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია მხოლოდ იმ შემთხვევაში, თუ უზრუნველყოფილია მონაცემთა სუბიექტის უფლებებისა და ინტერესების დაცვის კანონით გათვალისწინებული გარანტიები და არსებობს შესაბამისი საფუძველი.

განსაკუთრებული კატეგორიის მონაცემების დამუშავების საფუძვლები იხილეთ:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-6 მუხლი.

რეკომენდაცია:

დამუშავებისთვის პასუხისმგებელმა პირმა წინასწარ უნდა განსაზღვროს, თუ რომელი სამართლებრივი საფუძველია რელევანტური კონკრეტული დამუშავების პროცესისთვის. მონაცემთა დამუშავების საფუძვლების განსაზღვრისას, გასათვალისწინებელია:

- ✓ მონაცემების კატეგორია;
- ✓ მონაცემთა სუბიექტების სპეციფიკური მახასიათებლები;
- ✓ მონაცემების დამუშავების კონტექსტი;
- ✓ მონაცემების დამუშავების პროცესი;
- ✓ მონაცემების დამუშავებისთვის პასუხისმგებელი პირის კომპეტენციის ფარგლები;
- ✓ მონაცემთა დამუშავებაში მონაწილის როლი.

მონაცემთა დამუშავების სპეციალურ წესებთან დაკავშირებით იხილეთ მეტი:

- პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაცია „რა უნდა ვიცოდეთ ბიომეტრიულ მონაცემთა დამუშავების შესახებ“, 2024.
- პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები ვიდეომონიტორინგის და აუდიომონიტორინგის განხორციელების თაობაზე, 2023.

ნაწილი II. მონაცემთა სუბიექტის უფლებები

რა უფლებები აქვს მონაცემთა სუბიექტს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიხედვით?

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიზანია პერსონალური მონაცემების დამუშავებისას, ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის, პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცვა.

კანონი განსაზღვრავს მონაცემთა სუბიექტის შემდეგ უფლებებს:

მონაცემთა სუბიექტის უფლების კატეგორია	ნორმატიული საფუძველი
მონაცემთა დამუშავების შესახებ ინფორმაციის მიღების უფლება	მე-13 მუხლი
მონაცემთა გაცნობისა და ასლის მიღების უფლება	მე-14 მუხლი
მონაცემთა გასწორების, განახლებისა და შევსების უფლება	მე-15 მუხლი
მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლება	მე-16 მუხლი
მონაცემთა დაბლოკვის უფლება	მე-17 მუხლი
მონაცემთა გადატანის (პორტირების) უფლება	მე-18 მუხლი
ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებასთან დაკავშირებული უფლებები	მე-19 მუხლი
თანხმობის გამოხმობის უფლება	მე-20 მუხლი
გასაჩივრების უფლება	22-ე მუხლი

მონაცემთა სუბიექტის მოთხოვნის შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, კანონით დადგენილი წესით უზრუნველყოს მონაცემთა სუბიექტის უფლებების განხორციელება, მათ შორის, მიიღოს ყველა ზომა ამავე კანონის მოთხოვნებთან შესაბამისობის და საჭიროების შემთხვევაში, მათი დემონსტრირების მიზნით.

მონაცემთა სუბიექტის უფლებების დაცვის ვალდებულება ვრცელდება აგრეთვე დამუშავებაზე უფლებამოსილ პირზე მასთან დაცულ/არსებულ მონაცემებთან მიმართებით.

იხილეთ მეტი:

- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-3 თავი.
- არასრულწლოვანთა პერსონალურ მონაცემთა დაცვა - თეორია და პრაქტიკა.

მონაცემთა სუბიექტის უფლებების შინაარსი და განხორციელების ზოგადი წესი

მონაცემთა დამუშავების შესახებ ინფორმაციის მიღების უფლება

მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს იმის დადასტურება, მუშავდება თუ არა მის შესახებ მონაცემები, დასაბუთებულია თუ არა მონაცემთა დამუშავება და მოთხოვნის შესაბამისად, უსასყიდლოდ მიიღოს შემდეგი ინფორმაცია:

- მონაცემის თაობაზე, რომელიც მუშავდება, აგრეთვე ამ მონაცემის დამუშავების საფუძვლისა და მიზნის შესახებ;
- მონაცემთა შეგროვების/მოპოვების წყაროს შესახებ;
- მონაცემთა შენახვის ვადის (დროის) შესახებ, ხოლო თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, ვადის განსაზღვრის კრიტერიუმების თაობაზე;
- მონაცემთა სუბიექტის კანონით გათვალისწინებული უფლებების შესახებ;
- მონაცემთა გადაცემის სამართლებრივი საფუძვლისა და მიზნების, აგრეთვე მონაცემთა დაცვის სათანადო გარანტიების შესახებ, თუ მონაცემები გადაეცემა სხვა სახელმწიფოს ან საერთაშორისო ორგანიზაციას;
- მონაცემთა მიმღების ვინაობის ან მონაცემთა მიმღებების კატეგორიების შესახებ, მათ შორის, ინფორმაცია მონაცემთა გადაცემის საფუძვლისა და მიზნის თაობაზე, თუ მონაცემები მესამე პირს გადაეცემა;
- ავტომატიზებული დამუშავების, მათ შორის, პროფაილინგის შედეგად მიღებული გადაწყვეტილების და იმ ლოგიკის შესახებ, რომელიც გამოიყენება ამგვარი გადაწყვეტილების მისაღებად, აგრეთვე მონაცემთა დამუშავებაზე მისი გავლენისა და დამუშავების მოსალოდნელი/სავარაუდო შედეგის თაობაზე.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-13 მუხლი.

მონაცემთა გაცნობისა და ასლის მიღების უფლება

მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირთან გაეცნოს მის შესახებ არსებულ პერსონალურ მონაცემებს და უსასყიდლოდ მიიღოს მათი ასლები.

თქვენ, როგორც დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოთ მონაცემთა სუბიექტის მოთხოვნის შესრულება, მათ შორის, განსაზღვროთ საფასური, თუ ეს საქართველოს კანონმდებლობით გათვალისწინებულია ან იგი მონაცემთა შენახვის ფორმისგან განსხვავებული ფორმით მათი გაცემისთვის დახარჯული რესურსის ან/და მოთხოვნის სიხშირიდან გამომდინარეობს.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-14 მუხლი.

მონაცემთა გასწორების, განახლებისა და შევსების უფლება

მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს მის შესახებ მცდარი, არაზუსტი ან/და არასრული მონაცემების გასწორება, განახლება ან/და შევსება.

თქვენ, როგორც დამუშავებისთვის პასუხისმგებელმა პირმა, უნდა უზრუნველყოთ მონაცემთა სუბიექტის მოთხოვნის შესრულება და მონაცემთა ყველა მიმღებს, აგრეთვე, ამავე მონაცემთა ყველა სხვა დამუშავებისთვის პასუხისმგებელ პირს და დამუშავებაზე უფლებამოსილ პირს, რომლებსაც თავად გადაეცით მონაცემები, შეატყობინოთ მონაცემთა განახლებისა და შევსების შესახებ, გარდა იმ შემთხვევისა, როდესაც ასეთი ინფორმაციის მიწოდება შეუძლებელია დამუშავებისთვის პასუხისმგებელი პირების/დამუშავებაზე უფლებამოსილი პირების ან მონაცემთა მიმღებების სიმრავლის ან/და არაპროპორციულად დიდი დანახარჯების გამო.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-15 მუხლი.

მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლება

მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს მის შესახებ მონაცემთა დამუშავების (მათ შორის, პროფაილინგის) შეწყვეტა, წაშლა ან განადგურება.

თქვენ, როგორც დამუშავებისთვის პასუხისმგებელმა პირმა, უნდა უზრუნველყოთ მონაცემთა სუბიექტის მოთხოვნის შესრულება, თუმცა უფლება გაქვთ, უარი განაცხადოთ აღნიშნული მოთხოვნის დაკმაყოფილებაზე, თუ:

- არსებობს მონაცემთა დამუშავების კანონით გათვალისწინებული რომელიმე საფუძველი;
- მონაცემები მუშავდება სამართლებრივი მოთხოვნის ან შესაგებლის დასაბუთების მიზნით;
- მონაცემთა დამუშავება აუცილებელია გამოხატვის ან ინფორმაციის თავისუფლების უფლების განსახორციელებლად;
- მონაცემები მუშავდება კანონით გათვალისწინებული საჯარო ინტერესებისთვის არქივირების მიზნით, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის და მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლების განხორციელება შეუძლებელს გახდის ან მნიშვნელოვნად დააზიანებს დამუშავების მიზნების მიღწევას.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-16 მუხლი.

მონაცემთა დაბლოკვის უფლება

მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს მონაცემთა დაბლოკვა, თუ არსებობს ერთ-ერთი შემდეგი გარემოება:

- მონაცემთა სუბიექტი სადავოს ხდის მონაცემების ნამდვილობას ან სიზუსტეს;

- მონაცემთა დამუშავება უკანონოა, თუმცა მონაცემთა სუბიექტი ეწინააღმდეგება მათ წაშლას და ითხოვს მონაცემთა დაბლოკვას;
- მონაცემები საჭირო აღარ არის მათი დამუშავების მიზნის მისაღწევად, თუმცა მონაცემთა სუბიექტს ისინი სჭირდება საჩივრის/სარჩელის წარსადგენად;
- მონაცემთა სუბიექტი მოითხოვს მონაცემთა დამუშავების შეწყვეტას, წაშლას ან განადგურებას და მიმდინარეობს ამ მოთხოვნის განხილვა;
- არსებობს მონაცემების მტკიცებულებად გამოყენების მიზნით შენახვის აუცილებლობა.

თქვენ, როგორც დამუშავებისთვის პასუხისმგებელმა პირმა, უნდა უზრუნველყოთ მონაცემთა სუბიექტის მოთხოვნის შესრულება, თუმცა უფლება გაქვთ, უარი თქვათ აღნიშნული მოთხოვნის დაკმაყოფილებაზე, როდესაც მონაცემთა დაბლოკვამ შეიძლება საფრთხე შეუქმნას:

- კანონით ან კანონქვემდებარე ნორმატიული აქტით თქვენთვის დაკისრებული მოვალეობების შესრულებას;
- კანონის შესაბამისად საჯარო ინტერესის სფეროსთვის მიკუთვნებული ამოცანების შესრულებას ან თქვენთვის მინიჭებული უფლებამოსილების განხორციელებას;
- თქვენი ან მესამე პირის ლეგიტიმურ ინტერესებს, გარდა იმ შემთხვევისა, როდესაც არსებობს მონაცემთა სუბიექტის, განსაკუთრებით არასრულწლოვანის, უფლებების დაცვის აღმატებული ინტერესი;
- მონაცემთა სუბიექტის ან მესამე პირის სასიცოცხლო ინტერესების დაცვას, აგრეთვე სახელმწიფო უსაფრთხოებისა და თავდაცვის მიზნებს.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-17 მუხლი.

მონაცემთა გადატანის (პორტირების) უფლება

კანონის მე-5 მუხლის პირველი პუნქტის „ა“ და „ბ“ ქვეპუნქტებითა და მე-6 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული საფუძვლებით მონაცემთა ავტომატური დამუშავების შემთხვევაში, თუ ეს ტექნიკურად შესაძლებელია, მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელი პირისგან სტრუქტურიზებული, საზოგადოდ გამოყენებადი და მანქანურად წაკითხვადი ფორმატით მიიღოს მის მიერ მიწოდებული მონაცემები ან მოითხოვოს ამ მონაცემთა სხვა დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემა.

იხილეთ მეტი:

- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ მე-18 მუხლი.
- რეკომენდაცია მონაცემთა გადატანის უფლების შესახებ https://pdps.ge/ka/content/984/rekomendaciebi?page=3
- სახელმძღვანელო რეკომენდაცია მონაცემთა პორტირების უფლების შესახებ https://pdps.ge/ka/content/984/rekomendaciebi?page=3

ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებასთან დაკავშირებული უფლებები

მონაცემთა სუბიექტს უფლება აქვს, არ დაექვემდებაროს მხოლოდ ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე, მიღებულ გადაწყვეტილებას, რომელიც მისთვის წარმოშობს სამართლებრივ ან სხვა სახის არსებითი მნიშვნელობის მქონე შედეგს, გარდა იმ შემთხვევისა, როდესაც პროფაილინგის საფუძველზე გადაწყვეტილების მიღება:

- ეფუძნება მონაცემთა სუბიექტის აშკარად გამოხატულ თანხმობას;
- აუცილებელია მონაცემთა სუბიექტსა და დამუშავებისთვის პასუხისმგებელ პირს შორის ხელშეკრულების დასადებად ან ხელშეკრულების შესასრულებლად;
- გათვალისწინებულია კანონით ან კანონის საფუძველზე დელეგირებული უფლებამოსილების ფარგლებში გამოცემული კანონქვემდებარე ნორმატიული აქტით.

თქვენ, როგორც დამუშავებისთვის პასუხისმგებელმა პირმა, უნდა უზრუნველყოთ მონაცემთა სუბიექტის მოთხოვნის შესრულება და უნდა მიიღოთ სათანადო ზომები მონაცემთა სუბიექტის უფლებების, თავისუფლებისა და ლეგიტიმური ინტერესების დასაცავად, მათ შორის, გადაწყვეტილების მიღების პროცესში ადამიანური რესურსის ჩართვის, მონაცემთა სუბიექტისთვის მისი მოსაზრების გამოთქმის და გადაწყვეტილების გასაჩივრების შესაძლებლობის მიცემის გზით.

იხილეთ მეტი:

- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ მე-19 მუხლი.
- რეკომენდაციები ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებასთან დაკავშირებული უფლებებისა და პროფაილინგის შესახებ, 2024.

- სახელმძღვანელო რეკომენდაცია ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებისა და პროფაილინგის შესახებ, 2016/679 რეგულაციის მიზნებისთვის, 2017.

თანხმობის გამოხმობის უფლება

მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, ყოველგვარი განმარტების ან დასაბუთების გარეშე, გამოიხმოს მის მიერ გაცემული თანხმობა. მონაცემთა სუბიექტის მოთხოვნის შესაბამისად, მონაცემთა დამუშავება უნდა შეწყდეს ან/და დამუშავებული მონაცემები წაიშალოს ან განადგურდეს, თუ მონაცემთა დამუშავების სხვა საფუძველი არ არსებობს.

მონაცემთა სუბიექტს უფლება აქვს, თანხმობა გამოიხმოს იმავე ფორმით, რომლითაც თანხმობა განაცხადა. მონაცემთა სუბიექტს თანხმობის გამოხმობამდე უფლება აქვს, თქვენგან მიიღოს ინფორმაცია თანხმობის გამოხმობის შესაძლო შედეგების შესახებ.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ მე-20 მუხლი.

გასაჩივრების უფლება

მონაცემთა სუბიექტს უფლება აქვს უფლებებისა და კანონით დადგენილი წესების დარღვევის შემთხვევაში, მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს, სასამართლოს ან/და ზემდგომ ადმინისტრაციულ ორგანოს.

იხილეთ მეტი:

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ 22-ე მუხლი.

როგორ უნდა დამუშავდეს მონაცემთა სუბიექტის უფლებებთან დაკავშირებული მოთხოვნები?

მონაცემთა დამუშავების პროცესი უნდა წარიმართოს კანონიერად, სამართლიანად, მონაცემთა სუბიექტისთვის გამჭვირვალედ და მისი ღირსების შეულახავად. მონაცემთა დამუშავების გამჭვირვალობის ვალდებულება არ ვრცელდება კანონით დადგენილ გამონაკლის შემთხვევებზე.

მნიშვნელოვანია მონაცემთა სუბიექტებთან კომუნიკაცია და მონაცემთა სუბიექტის უფლებების განხორციელების ხელშეწყობა. მაგალითად, ვებგვერდზე ელექტრონული ფორმის ინტეგრირებით, რომელიც მონაცემთა სუბიექტს შესაძლებლობას მისცემს, დაგიკავშირდეთ მარტივად.

საპასუხო შეტყობინება

ორგანიზაციამ უნდა უპასუხოს მონაცემთა სუბიექტის მოთხოვნას იმავე ფორმით, როგორც ეს მონაცემთა სუბიექტმა წარმოადგინა ან იმ ფორმით, რომლითაც მონაცემთა სუბიექტმა მოითხოვა პასუხის მიღება. სასურველია, წერილობით, მათ შორის, საჭიროების შემთხვევაში, ელექტრონული საშუალებით, ასევე, ზეპირი კონსულტაციით, მოთხოვნის და გარემოებების გათვალისწინებით.

საპასუხო ვადა

კანონი განსაზღვრავს მონაცემთა სუბიექტის მოთხოვნაზე საპასუხო 10 სამუშაო დღის ვადას, რომელიც შეიძლება გაგრძელდეს არაუმეტეს 10 სამუშაო დღით, შემდეგი უფლებების განხორციელებისას მიღებულ მოთხოვნათა საპასუხოდ:

- მონაცემთა დამუშავების შესახებ ინფორმაციის მიღების უფლება;
- მონაცემთა გაცნობისა და ასლის მიღების უფლება;
- მონაცემთა გასწორების, განახლებისა და შევსების უფლება;
- მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლება;
- თანხმობის გამოხმობის უფლება.

მონაცემთა სუბიექტს უნდა მიეწოდოს ინფორმაცია მონაცემთა დაბლოკვის თაობაზე მიღებული გადაწყვეტილების ან მონაცემთა დაბლოკვაზე უარის თქმის საფუძვლის შესახებ გადაწყვეტილების მიღებისთანავე, დაუყოვნებლივ, მაგრამ არაუგვიანეს მოთხოვნიდან 3 სამუშაო დღისა.

საფასური

კანონის მე-13, მე-14, მე-15, მე-16, მე-17, მე-18, მე-19, მე-20, 24-ე და 25-ე მუხლებით გათვალისწინებული მონაცემთა სუბიექტის უფლებების განხორციელება უზრუნველყოფილი უნდა იყოს უსასყიდლოდ, გარდა ამავე კანონით დადგენილი გამონაკლისებისა. მონაცემთა სუბიექტის მიერ მოთხოვნის არაგონივრული სიხშირით წარდგენის შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია, უარი განაცხადოს მის შესრულებაზე, რის შესახებაც ვალდებულია, დაუყოვნებლივ წერილობით აცნობოს მონაცემთა სუბიექტს და განუმარტოს გასაჩივრების უფლების შესახებ.

რეკომენდაციები:

როგორ უნდა იმოქმედოთ მონაცემთა სუბიექტის უფლებების განხორციელებასთან დაკავშირებულ მოთხოვნებთან მიმართებით?

- ✓ შეიმუშავეთ პროცედურა მონაცემთა სუბიექტის მოთხოვნებზე პასუხის გასაცემად და მოამზადეთ თქვენი გუნდი წარმოდგენილი განცხადებების შიდა სამუშაო პროცესებში ინტეგრირებისთვის;
- ✓ უფლებების განხორციელების ხელშეწყობის მიზნით, გაუადვილეთ მონაცემთა სუბიექტებს იმის ცოდნა, თუ რა უფლებები აქვთ თქვენი მომსახურების მიღებისას და როგორ დაგიკავშირდნენ ამ უფლებების განსახორციელებლად;
- ✓ მონაცემთა ეფექტიანი მართვის მიზნით, განაახლეთ თქვენი მომსახურების ელექტრონული სისტემა, რათა სწრაფად განსაზღვროთ დამუშავებული მონაცემები, ეფექტიანად იპოვოთ და მიიღოთ ინფორმაცია კონკრეტული პირის შესახებ;
- ✓ გამჭვირვალობის უზრუნველსაყოფად, ნათლად და გასაგებად აცნობეთ ინფორმაცია მონაცემთა სუბიექტებს თქვენ მიერ დამუშავებული პერსონალური მონაცემების შესახებ, როგორც დამუშავებამდე (მოსალოდნელი შედეგების შესახებ ინფორმაცია ასახეთ კონფიდენციალობის პოლიტიკაში), ასევე, დამუშავების პროცესში (მონაცემთა წვდომის უფლების დაცვისას);
- ✓ ყოველთვის უპასუხეთ მონაცემთა სუბიექტის მოთხოვნას კანონით დადგენილ ვადაში. თუ გჭირდებათ დამატებითი დრო პასუხისთვის ან თუ ვერ ასრულებთ მოთხოვნას, ამის შესახებ აცნობეთ მონაცემთა სუბიექტს ასევე, კანონით დადგენილ ვადაში;
- ✓ მონაცემთა სხვა პირებზე გადაცემის მოთხოვნის მიღების შემთხვევაში, არ დაგავიწყდეთ, გადაწყვეტილების მიღებამდე აცნობეთ მონაცემთა სუბიექტს

აღნიშნული მოთხოვნის შესახებ, ხოლო საჭიროებისამებრ, დაელოდოთ მის პასუხს;

- ✓ აღრიცხეთ მონაცემთა სუბიექტების მოთხოვნები და მიღებული თუ გაგზავნილი შეტყობინებები, და ასევე, მოთხოვნის შესრულებაზე თქვენს მიერ გაცემული უარის დასაბუთება.

ნაწილი III. კანონშესაბამისობის უზრუნველყოფა

მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას (“Privacy by Design and by Default”)

ახალი პროდუქტის ან მომსახურების შექმნის პროცესში, როგორც დამუშავებისთვის პასუხისმგებელ პირებს, გეკისრებათ ვალდებულება, გაითვალისწინოთ მონაცემთა დაცვის სტანდარტები და დანერგოთ მონაცემთა დამუშავების პრინციპები. დამატებით, მონაცემთა რაოდენობის, მონაცემთა დამუშავების მასშტაბის, შენახვის ვადებისა და მონაცემებზე წვდომის განსაზღვრისას უნდა უზრუნველყოთ ისეთი ტექნიკური და ორგანიზაციული ზომების მიღება, რომელთა საშუალებითაც ავტომატურად დამუშავდება მონაცემების მხოლოდ ის მოცულობა, რომელიც აუცილებელია დამუშავების კონკრეტული მიზნის მისაღწევად. აღნიშნული ზომების გამოყენება უნდა მოხდეს იმგვარად, რომ ნებადართული ალტერნატიული მიდგომის არჩევამდე, პირთა განუსაზღვრელი წრისთვის ავტომატურად უზრუნველყოფილი იყოს მონაცემთა მხოლოდ მინიმალურ მოცულობაზე წვდომა.

პერსონალურ მონაცემთა დაცვის სტანდარტების დანერგვისას უნდა გაითვალისწინოთ:

- მონაცემთა დამუშავების ხასიათი, კონტექსტი და ფარგლები;
- მონაცემთა დამუშავების თანმხლები რისკები, რომლებმაც, შესაძლოა, გავლენა იქონიოს მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებზე;
- ტექნიკური და ორგანიზაციული ზომების არსებობა მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებთან მიმართებით არსებული რისკების შესამცირებლად;
- იმგვარი ტექნიკური და ორგანიზაციული ზომების არსებობა, რომელთა საშუალებითაც დამუშავდება მონაცემების მხოლოდ ის მოცულობა, რომელიც აუცილებელია კონკრეტული მიზნის მისაღწევად.

მაგალითი:

წიგნების მაღაზიას შემოსავლების გაზრდის მიზნით სურს წიგნების ონლაინ გაყიდვა. მაღაზიის მეპატრონემ გადაწყვიტა, შექმნას სტანდარტული ფორმა ონლაინ შეკვეთებისთვის. იმისათვის, რომ მომხმარებლებმა მაღაზიას ყველა საჭირო ინფორმაცია მიაწოდონ, მეპატრონემ ონლაინ ფორმაში არსებული ყველა ველი სავალდებულო გახადა, მათ შორის, მომხმარებლის დაბადების თარიღი, ტელეფონის ნომერი და საცხოვრებელი მისამართი. თუმცა, მითითებული ველები არ არის აუცილებელი წიგნების გაყიდვისა და მიწოდებისთვის.

მაგალითად, როდესაც მომხმარებელს სურს ელექტრონული წიგნის შეკვეთა, მას შეუძლია პროდუქტის ჩამოტვირთვა პირდაპირ თავის მოწყობილობაზე. აღნიშნულის გათვალისწინებით, ინტერნეტ მაღაზიის მფლობელმა, გადაწყვიტა ორი ელექტრონული შესავსები ფორმის შექმნა: ერთი წიგნების შესაკვეთად, სადაც მომხმარებელი მისამართს მიუთითებს, ხოლო მეორე — ელექტრონული წიგნების გამოსაწერად. ეს უკანასკნელი არ შეიცავს მომხმარებლის მისამართის შესახებ ველს.

აღნიშნული ზომების დანერგვით, მაღაზიის მესაკუთრე დარწმუნდება, რომ გროვდება მხოლოდ იმ მოცულობის პერსონალური ინფორმაცია, რომელიც საჭიროა მონაცემთა დამუშავების მიზნის მისაღწევად.

<u>იხილეთ მეტი:</u>

- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ 26-ე მუხლი;
- მონაცემთა დაცვის ევროპული საბჭოს სახელმძღვანელო რეკომენდაცია: „მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას.

მონაცემთა დამუშავების აღრიცხვის ვალდებულება

თქვენი, როგორც ორგანიზაციის ვალდებულებაა, წერილობით, მათ შორის, ელექტრონული ფორმით აღრიცხოთ მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაცია. აღნიშნული ჩანაწერები ასახავს დამუშავების პროცესების შესახებ ზოგად მიმოხილვას, რომელიც ფარავს შემდეგ საკითხებს:

- დამუშავებისთვის პასუხისმგებელი პირის, სპეციალური წარმომადგენლის, პერსონალურ მონაცემთა დაცვის ოფიცრის, თანადამუშავებისთვის

პასუხისმგებელი პირების, დამუშავებაზე უფლებამოსილი პირის ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია;

- მონაცემთა დამუშავების მიზანი;
- მონაცემთა სუბიექტებისა და მონაცემთა კატეგორიები;
- მონაცემთა მიმღების (მათ შორის, სხვა სახელმწიფოში არსებული მონაცემთა მიმღების ან საერთაშორისო ორგანიზაციის) კატეგორიები;
- სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის მონაცემთა გადაცემის, აგრეთვე მონაცემთა დაცვის სათანადო გარანტიების თაობაზე, მათ შორის, პერსონალურ მონაცემთა დაცვის სამსახურის ნებართვა (ასეთის არსებობის შემთხვევაში;
- მონაცემთა შენახვის ვადები, ხოლო თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, მათი შენახვის ვადის განსაზღვრის კრიტერიუმები;
- მონაცემთა უსაფრთხოებისთვის მიღებული ორგანიზაციულ-ტექნიკური ზომების ზოგადი აღწერა;
- ინციდენტების შესახებ ინფორმაცია (ასეთის არსებობის შემთხვევაში).

თითოეული დამუშავებაზე უფლებამოსილი პირი და მის მიერ მონაცემთა დამუშავებაში კანონის 36-ე მუხლის მე-7 პუნქტით დადგენილი წესით ჩართული პირი ვალდებული არიან წერილობით ან ელექტრონულად უზრუნველყონ მონაცემთა დამუშავებასთან დაკავშირებული შემდეგი ინფორმაციის აღრიცხვა:

- დამუშავებაზე უფლებამოსილი პირის, პერსონალურ მონაცემთა დაცვის ოფიცრის, დამუშავებისთვის პასუხისმგებელი პირის, თანადამუშავებისთვის პასუხისმგებელი პირების, სპეციალური წარმომადგენლის ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია;
- დამუშავებისთვის პასუხისმგებელი პირისთვის ან მისი სახელით განხორციელებული მონაცემთა დამუშავების სახეების შესახებ;
- ამ მუხლის პირველი პუნქტის „ე“ ქვეპუნქტით გათვალისწინებული ინფორმაცია, თუ იგი მონაწილეობს სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის მონაცემთა გადაცემის პროცესში;
- მონაცემთა უსაფრთხოების უზრუნველსაყოფად მიღებული ორგანიზაციულ-ტექნიკური ზომების ზოგადი აღწერა;
- ინციდენტების შესახებ ინფორმაცია (ასეთის არსებობის შემთხვევაში).

თანადამუშავებისთვის პასუხისმგებელმა პირებმა, დამუშავებაზე უფლებამოსილმა პირმა და სპეციალურმა წარმომადგენელმა წარმოდგენილი ინფორმაცია შესაბამისი

მოთხოვნისთანავე, დაუყოვნებლივ, მაგრამ არაუგვიანეს 3 სამუშაო დღისა, უნდა მიაწოდოთ პერსონალურ მონაცემთა დაცვის სამსახურს.

იხილეთ მეტი:

- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 28-ე მუხლი;

მონაცემთა უსაფრთხოების დარღვევასთან (ინციდენტი) დაკავშირებული ვალდებულებები

რას გულისხმობს მონაცემთა უსაფრთხოების დარღვევა (ინციდენტი)?

ინციდენტი არის მონაცემთა უსაფრთხოების დარღვევა, რომელიც იწვევს მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას/მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას. ინციდენტის სახეებია:

- კონფიდენციალურობის დარღვევა – პერსონალური მონაცემების უნებართვო გამჟღავნება ან წვდომა;
- მთლიანობის დარღვევა – პერსონალური მონაცემების უნებართვო შეცვლა, აგრეთვე, არამართლზომიერი ან შემთხვევითი დაზიანება, დაკარგვა;
- ხელმისაწვდომობის დარღვევა – პერსონალურ მონაცემებზე წვდომის დაკარგვა, შეზღუდვა, მონაცემების განადგურება ან წაშლა.

ინციდენტს შედეგად შესაძლოა, მოჰყვეს ფიზიკური, ქონებრივი ან არაქონებრივი ღირებულების მატერიალური ან არამატერიალური ზიანი. ინციდენტის აღმოჩენისთანავე, გეკისრებათ ვალდებულება, შეაფასოთ ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა და სიმძიმე.

ინციდენტი აღმოჩენილად, შესაბამისად, თქვენ ინციდენტის შესახებ ინფორმირებულად მიიჩნევით იმ მომენტიდან, როდესაც მიიღეთ ინფორმაცია ინციდენტის არსებობის შესახებ.

კანონით განისაზღვრება კონკრეტული გარემოებები, რომელთა არსებობის დროსაც ინციდენტის თაობაზე გეკისრებათ პერსონალურ მონაცემთა დაცვის სამსახურის და, ასევე, რიგ შემთხვევებში, მონაცემთა სუბიექტის ინფორმირების ვალდებულება.

რა შემთხვევაში უნდა მიაწოდოთ ინფორმაცია პერსონალურ მონაცემთა დაცვის სამსახურს ინციდენტთან დაკავშირებით?

თქვენ გეკისრებათ ვალდებულება, ინციდენტის აღმოჩენიდან არაუგვიანეს 72 საათისა, მის შესახებ შეატყობინოთ სამსახურს, თუ ინციდენტი საშუალო ან მაღალი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

თუკი ინციდენტის სრულყოფილად შეფასება მისი აღმოჩენიდან 72 საათში ვერ ხერხდება, მაგრამ არსებობს გონივრული ეჭვის საფუძველი, რომ საშუალო ან მაღალი ალბათობით ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, თქვენ არ უნდა დაელოდოთ ინციდენტის შეფასების დასრულებას და ინციდენტის შესახებ უნდა შეატყობინოთ სამსახურს.

რა ფორმით უნდა მიეწოდოს ინფორმაცია პერსონალურ მონაცემთა დაცვის სამსახურს?

პერსონალურ მონაცემთა დაცვის სამსახურს ინციდენტის თაობაზე ინფორმაცია უნდა მიაწოდოთ წერილობით ან ელექტრონულად. თუ ინციდენტი შეეხება სახელმწიფო საიდუმლოების შემცველ ინფორმაციას, სამსახურს აღნიშნულის თაობაზე უნდა ეცნობოს კანონით დადგენილი წესით.

რა ინფორმაციას უნდა შეიცავდეს პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინება?

პერსონალურ მონაცემთა დაცვის სამსახურს ინციდენტის თაობაზე უნდა მიაწოდოთ ინფორმაცია:

- ინციდენტის გარემოებების, სახისა და დროის შესახებ;
- ინციდენტის შედეგად უნებართვოდ გამჟღავნებული, დაზიანებული, წაშლილი, განადგურებული, მოპოვებული, დაკარგული, შეცვლილი მონაცემების სავარაუდო კატეგორიებისა და რაოდენობის, აგრეთვე იმ მონაცემთა სუბიექტების სავარაუდო კატეგორიებისა და რაოდენობის შესახებ, რომლებსაც ინციდენტის შედეგად შეექმნათ საფრთხე;
- ინციდენტით გამოწვეული სავარაუდო ზიანის, მისი შემცირების ან აღმოფხვრის მიზნით დამუშავებისთვის პასუხისმგებელი პირის მიერ განხორციელებული ან დაგეგმილი ღონისძიებების შესახებ;

- იმის შესახებ, გეგმავს თუ არა დამუშავებისთვის პასუხისმგებელი პირი, ინციდენტის შესახებ შეატყობინოს მონაცემთა სუბიექტს (მონაცემთა სუბიექტებს) ამ კანონის 30-ე მუხლით დადგენილი წესით და რა ვადაში;
- პერსონალურ მონაცემთა დაცვის ოფიცრის ან სხვა საკონტაქტო პირის მონაცემების თაობაზე.

რა შემთხვევაში გეკისრებათ ინციდენტის თაობაზე მონაცემთა სუბიექტის ინფორმირების ვალდებულება?

თუ ინციდენტი მაღალი ალბათობით გამოიწვევს მნიშვნელოვან ზიანს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, თქვენ გეკისრებათ ვალდებულება ინციდენტის აღმოჩენიდან პირველი შესაძლებლობისთანავე, გაუმართლებელი დაყოვნების გარეშე, მის შესახებ აცნობოთ მონაცემთა სუბიექტს. გაითვალისწინეთ, რომ მონაცემთა უსაფრთხოების დარღვევის თაობაზე მონაცემთა სუბიექტისთვის მიწოდებული ინფორმაცია უნდა იყოს მარტივი და გასაგები.

მონაცემთა სუბიექტს უნდა მიეწოდოს შემდეგი ინფორმაცია:

- ინციდენტისა და მასთან დაკავშირებული გარემოებების ზოგადი აღწერა;
- ინციდენტით გამოწვეული სავარაუდო/დამდგარი ზიანის, მის შესამცირებლად ან აღმოსაფხვრელად განხორციელებული ან დაგეგმილი ღონისძიებების შესახებ;
- პერსონალურ მონაცემთა დაცვის ოფიცრის ან სხვა პირის საკონტაქტო მონაცემები.

თუ მონაცემთა სუბიექტის ინფორმირება არაპროპორციულად დიდ ხარჯებს ან ძალისხმევას მოითხოვს, აუცილებელია, ამ მუხლის პირველი პუნქტით გათვალისწინებული ინფორმაცია გაავრცელოთ საჯაროდ ან სხვა ისეთი ფორმით, რომელიც ჯეროვნად უზრუნველყოფს მონაცემთა სუბიექტის მიერ ინფორმაციის მიღების შესაძლებლობას.

იხილეთ მეტი:

- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 29-ე მუხლი;
- პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და პერსონალურ

მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ;

- პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები „ინციდენტთან დაკავშირებული ღონისძიებების განხორციელების თაობაზე“.

მონაცემთა დაცვაზე ზეგავლენის შეფასება

რას წარმოადგენს მონაცემთა დაცვაზე ზეგავლენის შეფასება?

როდესაც მონაცემთა დამუშავების შედეგად, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე, თქვენი, როგორც დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებაა, წინასწარ განახორციელოთ მონაცემთა დაცვაზე ზეგავლენის შეფასება. აღნიშნულის მიზანია რისკების შემცირება და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან შესაბამისობის უზრუნველყოფა.

როდის უნდა განხორციელდეს მონაცემთა დაცვაზე ზეგავლენის შეფასება?

თუ მონაცემთა დამუშავებისას ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე, გეკისრებათ მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების ვალდებულება. დამატებით, ზეგავლენის შეფასება აუცილებელია, თუ:

- მონაცემთა სუბიექტისთვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებთ სრულად ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე;
- ამუშავებთ დიდი რაოდენობით მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემებს;
- ახორციელებთ მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში.

რა ფორმით უნდა განხორციელდეს მონაცემთა დაცვაზე ზეგავლენის შეფასება და რა ინფორმაციას უნდა მოიცავდეს იგი?

მონაცემთა დაცვაზე ზეგავლენის შეფასებისას თქვენი ვალდებულებაა, შექმნათ წერილობითი დოკუმენტი, რომელიც შეიცავს:

- მონაცემთა კატეგორიის, მათი დამუშავების მიზნების, პროპორციულობის, პროცესისა და საფუძვლების აღწერას;
- ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეების შეფასებას და მონაცემთა უსაფრთხოების დაცვის მიზნით გათვალისწინებული ორგანიზაციულ-ტექნიკური ზომების აღწერას.

მონაცემთა დამუშავების პროცესის არსებითი ცვლილების შემთხვევაში, აუცილებელია, განაახლოთ მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი. ამასთან, აღნიშნული დოკუმენტის შენახვა სავალდებულოა მონაცემთა დამუშავების მთელი პერიოდის განმავლობაში, ხოლო მონაცემთა დამუშავების შეწყვეტის შემთხვევაში – არანაკლებ 1 წლის ვადით.

თუ მონაცემთა დაცვაზე ზეგავლენის შეფასების შედეგად გამოვლინდება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის მაღალი საფრთხე, აუცილებელია, მიიღოთ ყველა სათანადო ზომა საფრთხეების არსებითად შესამცირებლად და, საჭიროების შემთხვევაში, კონსულტაციის მიზნით მიმართოთ პერსონალურ მონაცემთა დაცვის სამსახურს. თუ დამატებითი ორგანიზაციულ-ტექნიკური ზომებით შეუძლებელია ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის არსებითად შემცირება, მონაცემთა დამუშავება არ უნდა განხორციელდეს.

<u>იხილეთ მეტი:</u>

- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 31-ე მუხლი;
- პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესის დამტკიცების შესახებ;
- პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები „მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) შესახებ“.

პერსონალურ მონაცემთა დაცვის ოფიცერი

რა შემთხვევაში გეკისრებათ პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულება?

თუ დამუშავებისთვის პასუხისმგებელი პირი წარმოადგენს სადაზღვევო ორგანიზაციას, კომერციულ ბანკს, მიკროსაფინანსო ორგანიზაციას, საკრედიტო ბიუროს, ელექტრონული კომუნიკაციის კომპანიას, ავიაკომპანიას, აეროპორტს, სამედიცინო დაწესებულებას, აგრეთვე, თუკი ამუშავებთ დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან ახორციელებთ მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს, ვალდებულნი ხართ დანიშნოთ ან განსაზღვროთ პერსონალურ მონაცემთა დაცვის ოფიცერი.

აუცილებელია, რომ პერსონალურ მონაცემთა დაცვის ოფიცერი:

- ჩართული იყოს მონაცემთა დამუშავებასთან დაკავშირებით მნიშვნელოვანი გადაწყვეტილების მიღების პროცესში;
- აღიჭურვოს სათანადო რესურსებით;
- იყოს დამოუკიდებელი საქმიანობის განხორციელებისას.

ვის არ ეკისრება პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ან განსაზღვრის ვალდებულება?

პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნა/განსაზღვრა არ ევალება იმ დამუშავებისთვის პასუხისმგებელ პირს/დამუშავებაზე უფლებამოსილ პირს, რომელიც ერთდროულად აკმაყოფილებს შემდეგ პირობებს:

- არ არის სადაზღვევო ორგანიზაცია, კომერციული ბანკი, მიკროსაფინანსო ორგანიზაცია, საკრედიტო ბიურო, ელექტრონული კომუნიკაციის კომპანია, ავიაკომპანია, აეროპორტი, სამედიცინო დაწესებულება;
- ამუშავებს შემდეგი რაოდენობის მონაცემთა სუბიექტის პერსონალურ მონაცემებს:
    - საქართველოს მოსახლეობის არაუმეტეს 3 პროცენტისა, რომელიც გამოითვლება მოსახლეობის საყოველთაო აღწერის ბოლო შედეგების მიხედვით;
    - საქართველოს მოსახლეობის არაუმეტეს 1 პროცენტის განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს, რომელიც გამოითვლება მოსახლეობის საყოველთაო აღწერის ბოლო შედეგების მიხედვით;
    - არ ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს.

ვალდებულების არარსებობის მიუხედავად, შესაძლებელია თუ არა პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნა?

თქვენ უფლებამოსილი ხართ, ვალდებულების არარსებობის მიუხედავად, დანიშნოთ პერსონალურ მონაცემთა დაცვის ოფიცერი. თუმცა, მისი ნებაყოფლობით დანიშვნის/განსაზღვრის შემთხვევაში, აუცილებელია, გაითვალისწინოთ პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნასთან/განსაზღვრასთან დაკავშირებით „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილ ყველა ვალდებულება.

იხილეთ მეტი:

- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 33-ე მუხლი;
- პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება დამუშავებისთვის პასუხისმგებელ პირთა და დამუშავებაზე უფლებამოსილ პირთა წრის განსაზღვრის შესახებ, რომლებსაც არ აქვთ ვალდებულება დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი;
- პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები „პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ“;
- პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შემუშავებული „მინიმალური სტანდარტი პერსონალურ მონაცემთა დაცვის ოფიცრებისთვის“.

მონაცემთა საერთაშორისო გადაცემასთან დაკავშირებული ვალდებულებები

კანონის თანახმად, მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვებია, თუ არსებობს მონაცემთა დამუშავების ამ კანონით გათვალისწინებული მოთხოვნები და შესაბამის სახელმწიფოში ან საერთაშორისო ორგანიზაციაში უზრუნველყოფილია მონაცემთა დაცვისა და მონაცემთა სუბიექტის უფლებების დაცვის სათანადო გარანტიები.

გარდა აღნიშნულისა, მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვებია, თუ:

- მონაცემთა გადაცემა გათვალისწინებულია საქართველოს საერთაშორისო ხელშეკრულებითა და შეთანხმებით;
- დამუშავებისთვის პასუხისმგებელი პირი უზრუნველყოფს მონაცემთა დაცვის სათანადო გარანტიებს დამუშავებისთვის პასუხისმგებელ პირსა და შესაბამის

სახელმწიფოს, ასეთი სახელმწიფოს სათანადო საჯარო დაწესებულებას, იურიდიულ პირს ან ფიზიკურ პირს ან საერთაშორისო ორგანიზაციას შორის დადებული ხელშეკრულებით (აღნიშნული საფუძვლით მონაცემთა გადაცემა შეიძლება მხოლოდ პერსონალურ მონაცემთა დაცვის სამსახურის ნებართვის მიღების შემდეგ);

- მონაცემთა გადაცემა გათვალისწინებულია საქართველოს სისხლის სამართლის საპროცესო კოდექსით (საგამოძიებო მოქმედების განხორციელების მიზნით), „უცხოელთა და მოქალაქეობის არმქონე პირთა სამართლებრივი მდგომარეობის შესახებ“ საქართველოს კანონით, „სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის შესახებ“ საქართველოს კანონით, „სამართალდაცვით სფეროში საერთაშორისო თანამშრომლობის შესახებ“ საქართველოს კანონით, „საქართველოს ეროვნული ბანკის შესახებ“ საქართველოს ორგანული კანონის ან „ფულის გათეთრებისა და ტერორიზმის დაფინანსების აღკვეთის ხელშეწყობის შესახებ“ საქართველოს კანონის საფუძველზე მიღებული ნორმატიული აქტით;
- შესაბამის სახელმწიფოში მონაცემთა დაცვის სათანადო გარანტიების არარსებობისა და შესაძლო საფრთხეების შესახებ ინფორმაციის მიღების შემდეგ მონაცემთა სუბიექტი განაცხადებს წერილობით თანხმობას;
- მონაცემთა გადაცემა აუცილებელია მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად და მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად უნარი არ აქვს, მონაცემთა დამუშავებაზე თანხმობა განაცხადოს;
- არსებობს კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესი (მათ შორის, დანაშაულის თავიდან აცილება, გამოძიება, გამოვლენა და სისხლისსამართლებრივი დევნა, სასჯელის აღსრულება და ოპერატიულ-სამძებრო ღონისძიებების განხორციელება) და მონაცემთა გადაცემა აუცილებელი და პროპორციული ზომაა დემოკრატიულ საზოგადოებაში.

თავის მხრივ, თქვენ გეკისრებათ ვალდებულება, მიიღოთ მონაცემთა უსაფრთხო გადაცემისთვის აუცილებელი ორგანიზაციული და ტექნიკური ზომები.

ამასთან, სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემული მონაცემების შემდგომი გადაცემა მესამე მხარისთვის დასაშვებია მხოლოდ იმ შემთხვევაში, თუ მონაცემთა შემდგომი გადაცემა ემსახურება თავდაპირველ მიზნებს და აკმაყოფილებს მონაცემთა გადაცემისთვის ამ მუხლით გათვალისწინებულ საფუძვლებსა და მონაცემთა დაცვის სათანადო გარანტიებს.

იხილეთ მეტი:

- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, V თავი;
- პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე ნებართვის გაცემის წესის და პერსონალურ მონაცემთა სხვა სახელმწიფოს ან/და საერთაშორისო ორგანიზაციისათვის გადაცემის თაობაზე განაცხადის ფორმის დამტკიცების შესახებ;
- პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე.

ნაწილი IV. პერსონალურ მონაცემთა უსაფრთხოების დაცვა

შესავალი მონაცემთა უსაფრთხოების ნაწილში

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი განსაზღვრავს წესებს მონაცემთა უსაფრთხოების შესახებ.

პერსონალურ მონაცემთა უსაფრთხოების დაცვის მიზნით, საჭიროა ისეთი ტექნიკური და ორგანიზაციული ზომების მიღება, რომლებიც სათანადოდ უზრუნველყოფენ მონაცემთა დაცვის, მათ შორის, უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვისგან, განადგურებისგან ან/და დაზიანებისგან. ტექნიკური და ორგანიზაციული ზომების შერჩევისა და გატარებისას, თვალყური უნდა ადევნოთ ტექნოლოგიების განვითარებას და მასთან დაკავშირებულ რისკებს.

გზამკვლევის აღნიშნულ ნაწილში არ არის განხილული მონაცემთა დაცვის ღონისძიებების სრული ჩამონათვალი. მონაცემთა დამუშავებისას და მონაცემთა დაცვის ღონისძიებების შერჩევისას, მხედველობაში უნდა მიიღოთ მონაცემთა დამუშავების კონტექსტი, მონაცემთა კატეგორიები და მონაცემთა უსაფრთხოების რისკები.

პერსონალურ მონაცემთა უსაფრთხოება და პოტენციური საფრთხეები

მონაცემთა უსაფრთხოების ზომების არასათანადოდ დაცვამ შესაძლოა, სერიოზული ნეგატიური შედეგები გამოიწვიოს, როგორიცაა, მაგალითად, რეპუტაციის შელახვა ან მომხმარებელთა მიერ ნდობის დაკარგვა. უსაფრთხოების ინციდენტმა, მაგალითად, მონაცემთა დაკარგვამ, შესაძლოა გამოიწვიოს ორგანიზაციის საქმიანობის შეჩერება და ფინანსური ზიანი. შესაბამისად, მონაცემთა უსაფრთხოების დაცვა წარმოადგენს როგორც მონაცემთა სუბიექტების, აგრეთვე ორგანიზაციების ინტერესის სფეროს.

იმის შესაფასებლად, თუ რამდენად დიდი რისკის შემცველია ყოველი მონაცემთა დამუშავების მოქმედება, პირველ რიგში, რეკომენდებულია დადგინდეს, რა გავლენას მოახდენს მონაცემთა სუბიექტების უფლებებზე და თავისუფლებებზე მონაცემთა დამუშავების აღნიშნული მოქმედება.

მონაცემთა სუბიექტების პერსონალური მონაცემების დასაცავად, უნდა გაითვალისწინოთ მონაცემთა უსაფრთხოების შედეგი სამი კომპონენტი:

მონაცემთა კონფიდენციალურობა, მთლიანობა, და ხელმისაწვდომობა. შესაბამისად, უნდა შეაფასოთ შემდეგი რისკები:

- პერსონალურ მონაცემებზე არაავტორიზებული ან შემთხვევითი წვდომა - მონაცემთა კონფიდენციალურობის დარღვევა (მაგალითად, კომპანიის ფინანსურ ან სახელფასო ინფორმაციაზე არაავტორიზებული წვდომა და მისი არამართლზომიერი გამოყენება);

- მონაცემთა არაავტორიზებული ან შემთხვევითი შეცვლა - მონაცემთა მთლიანობის დარღვევა (მაგალითად, წვდომის შესახებ ინფორმაციის შეცვლის ნიადაგზე, ცრუ ბრალდების წაყენება და განმახორციელებელი პირის წვდომაში დადანაშაულება);

- მონაცემთა დაკარგვა ან მონაცემებზე წვდომის დაკარგვა - ხელმისაწვდომობის დაკარგვა მონაცემებზე (მაგალითად, ნარკოტიკის მოხმარების შესახებ ინფორმაციის მიუღებლობა, პაციენტის ელექტრონულ მონაცემებზე წვდომის დაკარგვის გამო).

აგრეთვე, რეკომენდირებულია რისკების წყაროების იდენტიფიცირება — ვინ ან რა შეიძლება იყოს თითოეული უსაფრთხოების დარღვევის წარმოშობის მიზეზი, რომლის განსაზღვრის მიზნით, მნიშვნელოვანია როგორც შიდა, აგრეთვე გარე ადამიანური რესურსების გათვალისწინება (მაგალითად, ინფორმაციული ტექნოლოგიების ადმინისტრატორი, მომხმარებელი, გარე თავდამსხმელი, კონკურენტი), ასევე, შიდა ან გარე რესურსები (წყლის მიერ მიყენებული დაზიანება, სახიფათო ნივთიერებები, კომპიუტერული ვირუსები).

რისკების შეფასება მნიშვნელოვანია პოტენციური საფრთხეების იდენტიფიცირების მიზნით, მაგალითად, რა გარემოებებში იქნებოდა უსაფრთხოების ინციდენტის განხორციელება შესაძლებელი? (კომუნიკაციის არხებზე, ტექნოლოგიებზე, კომპიუტერულ სისტემებზე, ქაღალდზე არსებულ დოკუმენტებზე და სხვა).

უსაფრთხოების ინციდენტის შედეგად, პერსონალური მონაცემები შესაძლოა:

- იქნას გამოყენებული არასათანადოდ (უფლებების დარღვევით, დამუშავებისას შეცდომის გზით ან არასწორი დამუშავების გზით);
- იქნას შეცვლილი (მაგალითად, პროგრამული უზრუნველყოფის ან აპარატურის დაზიანების შედეგად, მავნე პროგრამის დაყენების გზით “software or hardware entrapment - keylogger, installation of malware”);
- დაიკარგოს (მაგალითად, პერსონალური კომპიუტერის მოპარვის ან მეხსიერების ბარათის დაკარგვის შედეგად);

- გახდეს დაკვირვების საგანი (მაგალითად, კომპიუტერის ეკრანზე დაკვირვება მატარებელში, გეოლოკაციის სერვისების გამოყენებით მოწყობილობებზე);
- მთლიანობის დარღვევა (მაგალითად, ვანდალიზმის, ბუნებრივი კატაკლიზმის შედეგად);
- გადაიტვირთოს (მაგალითად, მომსახურების გაწევის შეუძლებლობა თავდასხმიდან გამომდინარე გადატვირთულობის გამო "denial of service attack").
- გახდეს მიუწვდომელი (მაგალითად, კიბერთავდასხმის შედეგად, რომლის დროსაც კომპიუტერში არსებული ფაილები დაიშიფრება და მიუწვდომელი გახდება მფლობელისათვის).

რეკომენდაციები:

- ✓ ყოველი რისკის საპასუხოდ არსებული ან დაგეგმილი უსაფრთხოების ზომების განსაზღვრა (მაგალითად, წვდომის კონტროლი, მიკვლევადობა, შენობა-ნაგებობათა უსაფრთხოება, დაშიფვრა);
- ✓ რისკების ალბათობის და მასშტაბების გაზომვა (რისკის გასაზომად შესაძლოა გამოყენებული იქნას საზომი ერთეულის სისტემა, მაგალითად, რისკი შეიძლება შეფასდეს როგორც უმნიშვნელო, საშუალო სიმძიმის, მნიშვნელოვანი, მაქსიმალური სიმძიმის);
- ✓ ახალი ზომების იმპლემენტაცია და მონიტორინგი;
- ✓ მონაცემთა უსაფრთხოების აუდიტის ჩატარება. პერიოდულად, უნდა ჩატარდეს აუდიტი და ყოველი აუდიტის შედეგად უნდა შემუშავდეს სამოქმედო გეგმა, რომლის განხორციელებაც უნდა შემოწმდეს ორგანიზაციის მმართველი რგოლის მიერ.

უსაფრთხოების რისკების უფრო ნათლად აღსაქმელად რეკომენდირებულია რისკის მართვის დოკუმენტის შემუშავება, რომელიც ექვემდებარება პერიოდულ განახლებას. დოკუმენტში შესაძლოა გათვალისწინებული იქნას სერვერებთან დაკავშირებული მატერიალური და ადამიანური რისკები, აგრეთვე კომპიუტერებთან და ორგანიზაციების შენობა ნაგებობების უსაფრთხოებასთან დაკავშირებული რისკები. რისკების წინასწარი, სათანადოდ განსაზღვრა დაგეხმარებათ უსაფრთხოების დარღვევის დადგომისას ნეგატიური შედეგების აღმოფხვრაში.

პერსონალურ მონაცემთა დაცვის ორგანიზაციული ზომები

პერსონალურ მონაცემთა დაცვის ოფიცერი

პერსონალი მონაცემთა დაცვის ოფიცერი ზედამხედველობს ორგანიზაციაში პერსონალურ მონაცემთა უსაფრთხოების დაცვის სტანდარტს.

პერსონალურ მონაცემთა დაცვის ოფიცერი უზრუნველყოფს:

- ✓ მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე, მათ შორის, მარეგულირებელი სამართლებრივი ნორმების მიღების ან შეცვლის შესახებ, დამუშავებისთვის პასუხისმგებელი პირის, დამუშავებაზე უფლებამოსილი პირისა და მათი თანამშრომლების ინფორმირებას, მათთვის კონსულტაციისა და მეთოდური დახმარების გაწევას;
- ✓ მონაცემთა დამუშავებასთან დაკავშირებული შიდა რეგულაციებისა და მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის შემუშავებაში მონაწილეობას, აგრეთვე დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ საქართველოს კანონმდებლობისა და შიდა ორგანიზაციული დოკუმენტების შესრულების მონიტორინგს;
- ✓ მონაცემთა დამუშავებასთან დაკავშირებით შემოსული განცხადებებისა და საჩივრების ანალიზსა და შესაბამისი რეკომენდაციების გაცემას;
- ✓ პერსონალურ მონაცემთა დაცვის სამსახურისგან კონსულტაციების მიღებას, დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის წარმომადგენლობას პერსონალურ მონაცემთა დაცვის სამსახურთან ურთიერთობაში, მისი მოთხოვნით ინფორმაციისა და დოკუმენტების წარდგენას და მისი დავალებებისა და რეკომენდაციების შესრულების კოორდინაციასა და მონიტორინგს;
- ✓ მონაცემთა სუბიექტის მიმართვის შემთხვევაში მისთვის მონაცემთა დამუშავების პროცესებისა და მისი უფლებების შესახებ ინფორმაციის მიწოდებას;
- ✓ დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავების სტანდარტების ამაღლების მიზნით სხვა ფუნქციების შესრულებას.

ამავდროულად, მონაცემთა დაცვის ოფიცრის საქმიანობა ინციდენტების თავიდან აცილებაში საკვანძო როლს თამაშობს, რამდენადაც მას აკისრია ორგანიზაციის მრჩევლისა და კანონთან შესაბამისობის ზედამხედველობის ფუნქციები. პერსონალურ მონაცემებთან დაკავშირებული ინციდენტის დადგომის შემთხვევაში, მონაცემთა დაცვის ოფიცერი უნდა იყოს ინციდენტზე რეაგირებისთვის პასუხისმგებელ პირთა ჯგუფის წევრი. მონაცემთა დაცვის ოფიცერი ჩართული უნდა იყოს ისეთ ამოცანებში, როგორიცაა: ინციდენტზე

რეაგირების პროცედურებთან დაკავშირებული დოკუმენტაციისა და ინციდენტების შესახებ ინფორმაციის აღრიცხვის წარმოება, ასევე პერსონალურ მონაცემთა დაცვის სამსახურისთვის და მონაცემთა სუბიექტებისთვის შეტყობინებების მომზადება.

პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქცია შეიძლება, შეასრულოს დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის თანამშრომელმა ან სხვა პირმა მომსახურების ხელშეკრულების საფუძველზე. ამასთან, პერსონალურ მონაცემთა დაცვის ოფიცერს უფლება აქვს, შეასრულოს სხვა ფუნქციაც, თუ აღნიშნული არ წარმოშობს ინტერესთა კონფლიქტს.

გასათვალისწინებელია, რომ პერსონალურ მონაცემთა დაცვის ოფიცერს უნდა ჰქონდეს სათანადო ცოდნა მონაცემთა დაცვის სფეროში. ამასთან, იგი კონკრეტული ვითარების გათვალისწინებით ანგარიშვალდებული უნდა იყოს მაქსიმალურად მაღალი დონის მმართველობის სტრუქტურის წინაშე.

მომხმარებელთა ცნობიერების ამაღლება

აუცილებელია მონაცემთა დაცვის საკითხებზე თანამშრომლების და იმ პირთა ინფორმირება, ვინც პერსონალურ მონაცემებთან შემხებლობაშია. შესაბამის პირებს ინფორმაცია უნდა მიეწოდოთ კონფიდენციალურობის თემატიკაზე, აგრეთვე, რისკების საპასუხოდ მიღებული ზომების შესახებ.

აღნიშნული მიზნით, შესაძლებელია ცნობიერების ასამაღლებელი სემინარების გამართვა; მონაცემთა დაცვის თაობაზე, მარტივი და გასაგები ენით; თანამშრომლების და მონაცემებზე წვდომის მქონე პირებისთვის, მათი ფუნქცია-მოვალეობების შესაბამისი ინფორმაციის მიწოდება; პერსონალურ მონაცემთა დაცვის საკითხებზე შიდა საკომუნიკაციო არხის დანერგვა.

შიდა პოლიტიკის დოკუმენტის წარმოება

შესაძლებელია, კომპანიამ შეიმუშავოს შიდა გამოყენების პოლიტიკის დოკუმენტი, რომელშიც გაწერილი იქნება პერსონალური მონაცემების დაცვის და მონაცემთა უსაფრთხოების უზრუნველსაყოფად შესაბამისი წესები.

სხვა ორგანიზაციული ზომები

- ✓ მონაცემთა კლასიფიკაციის მიზნით, შესაბამისი წესის შემუშავება, რომელიც ინფორმაციის რამდენიმე დონეს გამოყოფს და სავალდებულოს გახდის

განსაკუთრებული კატეგორიის შემცველი მონაცემისა და დოკუმენტების „აღნიშვნას“.

- ✓ დოკუმენტების ყოველ გვერდზე (მათ შორის, ელექტრონულ დოკუმენტებშიც) განსაკუთრებული კატეგორიის მონაცემის შემცველობის შესახებ მითითება;
- ✓ ჩაატარეთ ტრენინგები ინფორმაციის უსაფრთხოების თემატიკაზე, ამავე თემაზე ცნობიერების ამაღლების მიზნით;
- ✓ კონტექსტიდან გამომდინარე, განიხილეთ კონფიდენციალურობის ხელშეკრულების დადების საკითხი პერსონალურ მონაცემებთან დაკავშირებით თანამშრომლებისათვის ან/და პერსონალური მონაცემების დამუშავების პროცესში ჩართულ/წინამდებარე საკითხებზე მომუშავე პირებისათვის.

პერსონალურ მონაცემთა დაცვის ტექნიკური ზომები

რეკომენდირებულია უსაფრთხოების გათვალისწინება შემდეგ საკითხებთან მიმართებით:

- ✓ აპარატურა (მაგალითად, სერვერები, სამუშაო მაგიდები, პერსონალური კომპიუტერი, მყარი დისკები);
- ✓ პროგრამული უზრუნველყოფა (მაგალითად, საოპერაციო სისტემა);
- ✓ კომუნიკაციის არხები (მაგალითად, ინტერნეტი);
- ✓ დოკუმენტები (ბეჭდური ფორმით არსებული დოკუმენტები და ასლები);
- ✓ ოფისის სივრცე.

მომხმარებელთა ავთენტიფიკაცია

იმისთვის, რომ მომხმარებლებმა (თანამშრომლებმა) მხოლოდ იმ ინფორმაციაზე განახორციელონ წვდომა, რაც მათ სჭირდებათ სამუშაოს შესასრულებლად, თანამშრომლებს უნდა მიენიჭოთ უნიკალური მაიდენტიფიცირებელი და გაიარონ ავთენტიფიკაცია კომპიუტერული მოწყობილობების გამოყენებამდე, შემდეგ მექანიზმებზე დაყრდნობით: ა) საშუალებები, რომლის შესახებ ინფორმირებულია ორგანიზაცია (მაგალითად, მომხმარებლის პაროლი); ბ) ფიზიკურად არსებული

საშუალებები (მაგალითად, საშვი); გ) პიროვნების ინდივიდუალური მახასიათებელი (მაგალითად, ხელმოწერა).

აღნიშნული მექანიზმის არჩევა დამოკიდებულია კონტექსტზე. ავთენტიფიკაცია შესაძლოა, სათანადოდ მივიჩნიოთ, როდესაც იგი სულ მცირე განხილულ ორ მექანიზმს ეყრდნობა.

ავტორიზაციის მართვა

მომხმარებლების ავტორიზაციის დიზაინი უნდა ეფუძნებოდეს მომხმარებელთა საჭიროებებს. მომხმარებლებს უნდა ჰქონდეთ წვდომა მხოლოდ იმ ინფორმაციაზე, რაც მათ სჭირდებათ საქმიანობის სფეროში დაკისრებული ვალდებულებების შესასრულებლად.

ავტორიზაციის მართვის კარგი პრაქტიკაა:

- ✓ პაროლების შესაქმნელად სხვადასხვა კრიტერიუმების განსაზღვრა (მაგალითად, სავალდებულო იყოს, რომ პაროლი შედგებოდეს სულ მცირე 8 სიმბოლოსგან და გამოყენებული იქნას სპეციალური სიმბოლოები);
- ✓ პაროლების უსაფრთხოდ შენახვა;
- ✓ ვადაგასული ნებართვების გაუქმება;
- ✓ პერიოდულად ნებართვების გადახედვა (მაგალითად, ყოველ 6 თვეში ერთხელ).

დაუშვებელია:

- ✓ ერთი ანგარიშის გაზიარება რამდენიმე მომხმარებლის მიერ;
- ✓ მომხმარებელთათვის ადმინისტრირების უფლების მინიჭება, რომელთაც არ ესაჭიროებათ წვდომა წინამდებარე ინფორმაციაზე თავისი მოვალეობის შესასრულებლად;
- ✓ მომხმარებლისათვის საჭიროზე მეტი უფლებების მინიჭება;
- ✓ დროებითი საჭიროებისას, გაცემული წვდომის უფლების შეზღუდვის დავიწყება, როდესაც წვდომა საჭირო აღარ არის მოვალეობების შესასრულებლად;
- ✓ მომხმარებლის ძველი ანგარიშის შენახვა, როდესაც მომხმარებელმა დატოვა ორგანიზაცია ან შეიცვალა თანამდებობა.

რეკომენდაცია

- ✓ კომპანიის ახალი თანამშრომლისთვის უნდა შეიქმნას ახალი, სპეციალური ანგარიში, რომელიც დაცულია რთული პაროლით.
- ✓ აუცილებელია თანამშრომელთა გაფრთხილება, რომ არ გაუზიარონ ერთმანეთს პირადი პაროლები, განსაკუთრებით მაშინ, თუ მათ არ აქვთ დაშვება ერთსა და იმავე ინფორმაციაზე და არ დატოვონ სამუშაო სივრცე მოწყობილობის პაროლით დაცვის გარეშე.
- ✓ თანამდებობის შეცვლასთან ერთად, აუცილებელია გადაიხედოს ინფორმაციაზე წვდომის დაშვებები.

პერსონალურ მონაცემთა დაცვა დეპერსონალიზაციის და ფსევდონიმიზაციის გზით

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი განმარტავს მონაცემთა დეპერსონალიზაციის ცნებას, რომლის მიხედვითაც დეპერსონალიზაცია მონაცემთა იმგვარი დამუშავებაა, როდესაც შეუძლებელია მონაცემთა სუბიექტთან მათი დაკავშირება ან ასეთი კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას, ხარჯებს ან/და დროს საჭიროებს. ევროპულ რეგულაციაში მსგავსი შინაარსით გამოიყენება ტერმინი ანომიმიზაცია.

კანონის თანახმად, მონაცემთა ფსევდონიმიზაცია არის მონაცემთა იმგვარი დამუშავება, როდესაც დამატებითი ინფორმაციის გამოყენების გარეშე, შეუძლებელია მონაცემების კონკრეტულ მონაცემთა სუბიექტთან დაკავშირება, აღნიშნული დამატებითი ინფორმაცია შენახულია ცალკე და ტექნიკური და ორგანიზაციული ზომების მეშვეობით მონაცემების იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირთან დაკავშირება არ ხდება.

პერსონალურ მონაცემთა დაცვის უზრუნველსაყოფად ტექნიკური ზომების დანერგვა ცალკეულ შემთხვევებში

ფიზიკური სამუშაო სივრცეების უსაფრთხოება

რეკომენდირებულია შემდეგი ზომების გატარება სამუშაო მაგიდების უსაფრთხოების უზრუნველსაყოფად:

- ✓ ავტომატურად ჩაკეტვის მექანიზმის გამოყენება, რომელიც შეზღუდავს პაროლის არმქონე პირის მიერ კომპიუტერის გამოყენებას;
- ✓ დააყენეთ პროგრამული უზრუნველყოფის დაცვის სისტემა (“*Firewall Software*”);

- ✓ გამოიყენეთ რეგულარულად განახლებული ვირუსების საწინააღმდეგო პროგრამული უზრუნველყოფის სისტემა;
- ✓ პროგრამული უზრუნველყოფის ავტომატური განახლებები, რომლებიც უსაფრთხოების სისტემის განახლებას უზრუნველყოფს;
- ✓ მომხმარებელთა ინფორმაციის განთავსება შესანახ სივრცეში, რომელიც რეგულარულად განახლებადია და ხელმისაწვდომია ორგანიზაციის ქსელით და არა სამუშაო მოწყობილობების საშუალებით.
- ✓ ისეთი მოწყობილობების გამოყენების შეზღუდვა, როგორიცაა მეხსიერების ბარათები, გარე მყარი დისკი და სხვა. აღნიშნული მოწყობილობების გამოყენება რეკომენდირებულია მხოლოდ აუცილებელი საჭიროების შემთხვევაში.

დაუშვებელია:

- ✓ მოძველებული ოპერაციული სისტემების გამოყენება;
- ✓ ადმინისტრირების უფლებების ისეთი მომხმარებლებისთვის მინიჭება, რომელთაც არ აქვთ კომპიუტერული უსაფრთხოების შესახებ შესაბამისი ცოდნა.

მნიშვნელოვანია თანამშრომლების ინფორმირება უსაფრთხოების დარღვევის დადგომის შემთხვევაში სამოქმედო გეგმის თაობაზე, მაგალითად, ვის აცნობონ, რა ვადაში და რა ფორმით.

დისტანციურად მუშაობა

დისტანციურად მუშაობისას, გასათვალისწინებელია შემდეგი რეკომენდაციები:

- ✓ დისტანციურად მუშაობის უსაფრთხოების პოლიტიკის დოკუმენტის შექმნა, რომელიც მოაწესრიგებს უსაფრთხოების შესახებ შესაბამის წესებს. აღნიშნული დოკუმენტი უნდა გახდეს ორგანიზაციის შიდა დოკუმენტაციის ნაწილი და მის შესახებ ეცნობოთ თანამშრომლებს;

- ✓ თუ საინფორმაციო სისტემის მიმართულებით დისტანციურად მუშაობისათვის აუცილებელი ხდება დამკვიდრებული წესების ცვლილება (მაგალითად, წვდომის კონტროლი), გაითვალისწინეთ რისკები და შეიმუშავეთ უსაფრთხოების უზრუნველსაყოფად შესაბამისი ღონისძიებები;

- ✓ დაბლოკეთ ვებსაიტებზე წვდომა, რომელიც შესაძლოა, საფრთხეს წარმოადგენდეს თქვენი კომპანიის სისტემების უსაფრთხოდ ფუნქციონირებისათვის;

- ✓ თუ თანამშრომლები პირად მოწყობილობებს იყენებენ სამსახურეობრივი მიზნებით, შეიმუშავეთ პირადი მოწყობილობების უსაფრთხოდ გამოყენების წესი და მიაწოდეთ მათ;
- ✓ განიხილეთ ვირტუალური კერძო ქსელის — “VPN”-ის გამოყენება, ორსაფეხურიანი ავთენტიფიკაციით;
- ✓ მონაცემთა უსაფრთხოდ გაცვლის მიზნით, აცნობეთ თანამშრომლებს, თუ რა საშუალებები, აპლიკაციები და კომუნიკაციის მეთოდები გამოიყენონ დისტანციური მუშაობისათვის.

მონაცემთა უსაფრთხოება პერსონალურ მონაცემთა საერთაშორისო გადაცემისას

მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვებია, თუ ამ სახელმწიფოში არსებობს მონაცემთა დამუშავების საქართველოს კანონით პერსონალურ მონაცემთა დაცვის შესახებ გათვალისწინებული მოთხოვნები და შესაბამის სახელმწიფოში ან საერთაშორისო ორგანიზაციაში უზრუნველყოფილია მონაცემთა დაცვისა და მონაცემთა სუბიექტის უფლებების დაცვის სათანადო გარანტიები.

იმ სახელმწიფოებისა და საერთაშორისო ორგანიზაციების ნუსხა, რომლებშიც უზრუნველყოფილია მონაცემთა დაცვის სათანადო გარანტიები, განისაზღვრება პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტით.

დამატებით იხილეთ:

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 29 თებერვლის ბრძანება „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“

პერსონალურ მონაცემთა უსაფრთხოების შესახებ გასათვალისწინებელი პუნქტების ჩამონათვალი
(სამაგალითო ნიმუში)

უსაფრთხოების ტექნიკურ-ორგანიზაციული ზომები	სტატუსი	პასუხისმგებელი პირი/გატარებული ღონისძიება	კომენტარი
მონაცემთა დამუშავების პროცესში ჩართული თანამშრომლების მუდმივი ინფორმირება და ცოდნის გაღრმავება მონაცემთა უსაფრთხოების თანამდევი რისკების თემატიკაზე			
მონაცემთა უსაფრთხოების შიდა პოლიტიკის დოკუმენტის წარმოება და მისთვის იურიდიული ძალის მინიჭება			
მონაცემთა უსაფრთხოების გათვალისწინება ახალი პროექტების დიზაინის ეტაპზევე			
მონაცემთა მინიმიზაციის პრინციპი - მონაცემთა			

დამუშავება საჭიროებასთან ადეკვატურობის დაცვით; მხოლოდ იმ მონაცემთა დამუშავება, რაც აუცილებელია დამუშავების მიზნის მისაღწევად			
განსაკუთრებული კატეგორიის მონაცემთათვის მონაცემთა კლასიფიკაციის პოლიტიკის დოკუმენტის შემუშავება			
იმ დოკუმენტებზე, რომლებიც შეიცავენ განსაკუთრებული კატეგორიის მონაცემებს შესაბამისი მინიშნებების დართვა			
მონაცემთა უსაფრთხოების თემატიკაზე ტრენინგების წარმოება; თანამშრომლების პერიოდულად ინფორმირება			

კონფიდენციალურობის ხელშეკრულების შემუშავება			
სისტემის უმოქმედობისას, გარკვეული დროის გასვლის შემდეგ, წვდომის შეზღუდვა ავტომატურ რეჟიმში; ანტივირუსული სისტემის განახლება და მონაცემთა ავტომატური შენახვის უზრუნველყოფა			
მეხსიერების ბარათების, გარე მყარი დისკების და სხვა მსგავსი მოწყობილობების გამოყენების შეზღუდვა, მათი გამოყენება მხოლოდ აუცილებელი საჭიროების შემთხვევაში			
ორგანიზაციის შენობა-ნაგებობების დაცვა (განგაშის სისტემა, კვამლის ამომცნობი სისტემა, ოთახების დაცვა, საშვის მოთხოვნა კონკრეტულ			

სივრცეში მოსახვედრად, ცეცხლმაქრი სისტემების არსებობა)			
მომხმარებელთათვის უნიკალური იდენტიფიკატორების მინიჭება			
კომპიუტერულ მოწყობილობებზე ავთენტიკაციის სავალდებულოობა			
დისტანციური მუშაობის უსაფრთხოების პოლიტიკის დოკუმენტის შემუშავება			
ვადაგასული საშვების მქონე პირებისათვის წვდომის შესაძლებლობის შეზღუდვა			
წვდომის უფლებამოსილებების პერიოდული გადახედვა			

განსაკუთრებული კატეგორიის მონაცემთა ფსევდონიმიზაცია ან დეპერსონალიზაცია			
მონაცემთა დეპერსონალიზაცია			
ვირტუალური კერძო ქსელი დისტანციურად მუშაობისათვის			
მოწყობილობების უსაფრთხოების უზრუნველყოფა დისტანციური მუშაობისას			

© პერსონალურ მონაცემთა დაცვის სამსახური, 2024

მის.: საქართველო, თბილისი, ნ. ვაჩნაძის N7, 0105
ბათუმი, ბაქოს N 48, 6010

ტელ.: (+995 32) 242 1000
E-mail: office@pdps.ge
www.pdps.ge