პერსონალურ მონაცემთა
დაცვის ინსპექტორის აპარატი

რეკომენდაციები

ინტერნეტ სივრცეში პერსონალურ მონაცემთა დაცვის შესახებ

ინტერნეტ მომსახურების გამწევთათვის

დოკუმენტი შემუშავებულია პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის, მონაცემთა დაცვის ევროპული სტანდარტებისა და საერთაშორისო პრაქტიკის ანალიზის საფუძველზე. დოკუმენტი სარეკომენდაციო ხასიათისაა. მისი მიზანია, მონაცემთა დამმუშავებელ ორგანიზაციებს განუმარტოს უფლება-მოვალეობები და ინტერნეტ სივრცეში პერსონალური მონაცემების შემცველი ინფორმაციის გამოყენებისას გასათვალისწინებელი მნიშვნელოვანი გარემოებები.

შესავალი

თანამედროვე ეპოქაში ინტერნეტი გლობალურ საკომუნიკაციო და საინფორმაციო საშუალებად იქცა. მისი საშუალებით უამრავი ადამიანი ახორციელებს კომუნიკაციას, ელექტრონულ შესყიდვებს, იღებს სხვადასხვა სახის მომსახურებას, იხდის გადასახადებს, აწარმოებს ოფიციალურ თუ არაოფიციალურ კორესპონდენციას. ელექტრონული კომუნიკაციის საშუალებების განვითარება, სახელმწიფო და საბანკო სერვისების ელექტრონულ სივრცეში გადატანა, ასევე, სოციალური ქსელების პოპულარობა განაპირობებს პერსონალური მონაცემების დიდი მოცულობით დაგროვებას ინტერნეტში.

აღნიშნულ პროცესებში, პერსონალურ მონაცემთა არასათანადო დაცვა ზრდის მონაცემთა დანაშაულებრივი მიზნებისათვის გამოყენების რისკებს და საფრთხის ქვეშ აყენებს ინტერნეტის მომხმარებელთა პირადი ცხოვრების ხელშეუხებლობას. ამიტომ, მნიშვნელოვანია, რომ ინტერნეტ მომსახურების გამწევ ორგანიზაციებს კარგად ჰქონდეთ გაცნობიერებული კანონმდებლობით მათზე დაკისრებული ვალდებულებები.

წინამდებარე რეკომენდაცია განკუთვნილია ინტერნეტ მომსახურების გამწევთათვის და ითვალისწინებს სახელმძღვანელო წესებს ინტერნეტში პირადი ინფორმაციის დაცვის, უსაფრთხოების ზომების და პერსონალურ მონაცემთა დაცვის კუთხით კანონმდებლობით განსაზღვრული უფლებებისა და ვალდებულებების შესახებ.

სახელმძღვანელო წესები ინტერნეტ მომსახურების გამწევებისათვის

*რეკომენდაციის მიზნებისთვის ტერმინი **„ინტერნეტ მომსახურების გამწევი“** მოიცავს როგორც ინტერნეტის მიმწოდებელს, ასევე ინტერნეტ მომსახურების (მათ შორის, ვებჰოსტინგი, ელექტრონული ფოსტა, სოციალური ქსელები, აუდიო-ვიდეო კომუნიკაციის სერვისები, საძიებო სისტემები, ონლაინ მაღაზიები) მიმწოდებელს. თითოეულ მათგანზე, მათი კომპეტენციისა და საქმიანობის სპეციფიკის გათვალისწინებით, ვრცელდება ამ რეკომენდაციაში მოცემული წესები.*

ინტერნეტ სივრცეში ინტერნეტ მომსახურების გამწევის ხელში ხვდება დიდი მოცულობით პერსონალური მონაცემების შემცველი ინფორმაცია, *მაგალითად, მომხმარებლის მიერ შევსებული ანკეტა, IP (ინტერნეტ ოქმის) მისამართი, მომხმარებლის საბანკო გარათის მონაცემები, პირადი ნომერი, ტელეფონის ნომერი, ადგილმდებარეობის მონაცემები, მისამართი და სხვა.* მნიშვნელოვანია, ინტერნეტ მომსახურების გამწევის მიერ მონაცემთა შეგროვება და შემდგომი დამუშავება მოხდეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნების შესაბამისად და ამ პროცესში გათვალისწინებული იყოს ქვემოთ მოცემული სახელმძღვანელო წესები.

1.1. ზოგადი პრინციპები

ინტერნეტ სივრცეში პერსონალურ მონაცემთა შეგროვების, შენახვის ან სხვაგვარი დამუშავების პროცესში დაუშვებელია:

- ინტერნეტ მომსახურების გამწევის ანონიმურობა;
- მონაცემების დამუშავება კანონიერი მიზნისა და შესაბამისი სამართლებრივი საფუძვლის არსებობის გარეშე;
- კანონიერი მიზნის შეუსაბამო და ამ მიზნის მიღწევისთვის არაპროპორციული მოცულობით მონაცემთა დამუშავება;
- მონაცემების შენახვა იმაზე მეტი ვადით, რაც აუცილებელია მათი დამუშავების მიზნის მისაღწევად;
- მონაცემთა დამუშავება ადამიანის უფლებებისა და თავისუფლებების, კერძოდ ადამიანის ღირსებისათვის შემლახავი ფორმით.

1.2. პერსონალურ მონაცემთა დაცვის შიდა სტანდარტი და კონფიდენციალურობის განაცხადი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ადგენს პერსონალურ მონაცემთა დაცვის ზოგად წესებსა და მოთხოვნებს. მიზანშეწონილია, ინტერნეტ მომსახურების გამწევს ჰქონდეს პერსონალურ მონაცემთა დაცვის მკაფიო და დეტალური შიდა სტანდარტი, რომელიც ასახავს მისი საქმიანობის სპეციფიკას და დაარეგულირებს პეროსონალური მონაცემების შეგროვების, მონაცემებზე წვდომის, შენახვის, განადგურების და მესამე პირებისათვის გადაცემის წესებს.

მომსახურების გამწევის შიდა სტანდარტის შესახებ ინფორმაცია მომხმარებლისთვის ხელმისაწვდომი უნდა იყოს ე.წ კონფიდენციალურობის განაცხადის (ე.წ. Privacy policy) საშუალებით, რომელშიც მარტივად და მომხმარებლისათვის გასაგებად იქნება გადმოცემული დეტალური ინფორმაცია ვებგვერდით სარგებლობისას მომხმარებლის პერსონალური მონაცემების დამუშავების პროცესზე, მონაცემთა შენახვის ვადაზე, მონაცემების მესამე მხარისთვის გამჟღავნებაზე, მომსახურების შეწყვეტის შემთხვევაში მონაცემთა შემდგომ გამოყენებაზე და მომხმარებლის მიერ საკუთარი უფლებების განხორციელების საშუალებებზე.

მომხმარებელს საშუალება უნდა ჰქონდეს, გაეცნოს კონფიდენციალურობის განაცხადს ინტერნეტ მომსახურების მიღებამდე და თანხმობა გამოხატოს მისი პერსონალური მონაცემების განაცხადში მოცემული წესების შესაბამისად დამუშავებაზე.

ვებგვერდის არარეგისტრირებული მომხმარებლებიც ინფორმირებულნი უნდა იყვნენ კონფიდენციალურობის განაცხადის თაობაზე, რისი უზრუნველყოფაც შესაძლებელია განაცხადის მთავარ გვერდზე თვალსაჩინო ადგილას განთავსებით.

1.3. მონაცემთა უსაფრთხოება

მონაცემთა უსაფრთხოება მოიცავს ოპერაციული, ფუნქციური და სტრატეგიული კონტროლის მექანიზმების ერთობლიობას, რომელიც ემსახურება მონაცემთა სიზუსტისა და კონფიდენციალურობის უზრუნველყოფას. ინტერნეტ მომსახურების მიმწოდებელი ვალდებულია, მიიღოს მონაცემთა შემთხვევითი ან უკანონო განადგურებისაგან, შეცვლისაგან, გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისგან დაცვის ორგანიზაციული და ტექნიკური ზომები.

მიზანშეწონილია, ორგანიზაციამ ცალკე დოკუმენტად ან პერსონალურ მონაცემთა დაცვის შიდა სტანდარტის ფარგლებში დაადგინოს პერსონალურ მონაცემთა უსაფრთხოების სტანდარტი, რომელიც უნდა მოიცავდეს:

- მონაცემთა დამუშავებასთან დაკავშირებული რისკების შეფასებას;
- ფიზიკური, ტექნიკური და ინფორმაციული უსაფრთხოების ზომებს;
- პერსონალური მონაცემების შემცველ ბაზებზე დაშვების დონეებს;
- კონტროლის მექანიზმებს;
- პასუხისმგებლობას უსაფრთხოების ზომების უგულებელყოფისთვის.

ორგანიზაციის მიერ გატარებული უსაფრთხოების ზომები უნდა იყოს მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური. სასურველია, ყველა შესაძლო რისკი წინასწარ შეფასდეს და შესაბამისად განისაზღვროს მათი მართვის კონკრეტული გეგმა, რომელიც უსაფრთხოების პრობლემის წარმოშობის შემთხვევაში, დროის მცირე მონაკვეთში შეამცირებს/აღკვეთს პერსონალურ მონაცემთა გამჟღავნების საფრთხეს და უზრუნველყოფს ეფექტური ზომების მიღებას.

მნიშვნელოვანია, რომ მომხმარებელთა პერსონალური მონაცემები ინახებოდეს დაცულ კომპიუტერში/სისტემაში და მათზე წვდომა იყოს მკაცრად განსაზღვრული. ინფორმაციაზე წვდომა უნდა ჰქონდეთ მხოლოდ იმ პირებს, ვისაც ეს ესაჭიროებათ მათი საქმიანობიდან და მონაცემთა დამუშავების მიზნებიდან გამომდინარე.

მონაცემთა უსაფრთხოების უზრუნველყოფის მიზნით ინტერნეტ მომსახურების გამწევმა უნდა გამოიყენოს უსაფრთხოების საუკეთესო პრაქტიკა და სერტიფიცირებული ტექნოლოგიები. დაცული უნდა იყოს მონაცემთა მთლიანობა და კონფიდენციალურობა ისევე, როგორც ქსელის და შესაბამისი სერვისების ფიზიკური და ლოგიკური უსაფრთხოება.

1.4. მონაცემთა სუბიექტის უფლებების დაცვა

ინტერნეტ მომსახურების გამწევი ვალდებულია, დაიცვას მომხმარებელთა პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა დაცვის უფლებები.

მომხმარებელს უფლება აქვს იცოდეს რა ტიპის პერსონალურ მონაცემები მუშავდება მის შესახებ, რა მიზნით და რა სამართლებრივი საფუძვლით, ხდება თუ არა მონაცემთა მესამე პირებისთვის გადაცემა, რა საფუძვლით და რა მიზნით.

ინტერნეტ მომსახურების გამოყენების შემთხვევაში, მომხმარებელი ინფორმირებული უნდა იყოს მის მონაცემებთან დაკავშირებული რისკებისა და მათ შესამცირებლად არსებული

ტექნიკურ/პროგრამული საშუალებების შესახებ. მომხმარებლისთვის მიწოდებული ინფორმაცია უნდა იყოს ზუსტი და განახლებული.

მომხმარებელი ინფორმირებული უნდა იყოს ინტერნეტით ანონიმური სარგებლობის ან კონკრეტული ტრანზაქციების ანონიმურად განხორციელების საშუალების შესახებ, თუ კი ეს შესაძლებელია კონკრეტული მომსახურების სპეციფიკიდან გამომდინარე.

მომხმარებელს უფლება აქვს, ნებისმიერ დროს, განმარტების გარეშე უარი განაცხადოს მის მიერვე გაცემულ თანხმობაზე და მოითხოვოს მონაცემთა დამუშავების შეწყვეტა ან/და დამუშავებულ მონაცემთა წაშლა/განადგურება. მომსახურების გამწევს უნდა ჰქონდეს მოქნილი სისტემა, რომელიც უზრუნველყოფს მომხმარებლის მხრიდან მისი პერსონალური მონაცემების დამუშავების შეწყვეტის შესახებ მოთხოვნაზე სწრაფ რეაგირებას.

ინტერნეტ მომსახურების გამწევმა უნდა შეატყობინოს მონაცემთა სუბიექტს მათ/მის შესახებ არსებული ინფორმაციის გამჟღავნების ან უკანონო გამოყენების საფრთხის შესახებ. *მაგალითად, ვებგვერდზე კიბერ თავდასხმის დროს, ვებგვერდის ადმინისტრაციამ უნდა მოახდინოს მომხმარებელთა გაფრთხილება აღნიშნული ფაქტის შესახებ.*