მონაცემთა უსაფრთხოების დარღვევის (ინციდენტი) მართვის პროცედურა

თავი I. ზოგადი დებულებები, მიზანი და ტერმინთა განმარტება

მუხლი 1. რეგულირების სფერო და მიზანი

1. წინამდებარე პროცედურა წარმოადგენს ა(ა)იპ - „ქონებრივი უფლებების კოლექტიურ საფუძველზე მმართველი ორგანიზაცია - ინტელექტუალური საკუთრების მფლობელთა ასოციაციის“ (შემდგომში - ასოციაცია) (ს/ნ: 404574475) შიდა სახელმძღვანელო დოკუმენტს. იგი აწესრიგებს იმპორტიორების მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) მართვის, ლოკალიზაციის, სამართლებრივი შეფასებისა და შეტყობინების წესს.

2. პროცედურის მიზანია ორგანიზაციაში მონაცემთა უსაფრთხოების შესაძლო დარღვევისას მყისიერი და კოორდინირებული რეაგირების უზრუნველყოფა, საინფორმაციო ნაკადებზე მიყენებული ზიანის მინიმიზაცია, რისკების სწორი სამართლებრივი შეფასება და საქართველოს მოქმედი კანონმდებლობით დადგენილი მოთხოვნების შესრულება.

მუხლი 2. ტერმინთა განმარტება

ინციდენტის მართვის წინამდებარე პროცედურაში გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:

ა) მონაცემთა უსაფრთხოების დარღვევა (ინციდენტი) - 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;

ბ) კონფიდენციალურობის დარღვევა - პერსონალური მონაცემების უნებართვო გამჟღავნება ან წვდომა;

გ) მთლიანობის დარღვევა - პერსონალური მონაცემების უნებართვო შეცვლა, აგრეთვე არამართლზომიერი ან შემთხვევითი დაზიანება, დაკარგვა;

დ) ხელმისაწვდომობის დარღვევა - პერსონალურ მონაცემებზე წვდომის დაკარგვა, შეზღუდვა, მონაცემების განადგურება ან წაშლა;

ე) პერსონალურ მონაცემთა დაცვის ოფიცერი - ასოციაციის მიერ დანიშნული უფლებამოსილი პირი, რომელიც დამოუკიდებლად ზედამხედველობს

ორგანიზაციაში მონაცემთა დამუშავების პროცესების კანონმდებლობასთან შესაბამისობას და უშუალოდ მართავს ინციდენტების მართვის პროცესს;

ვ) სახელმწიფო აუდიტის სამსახური - „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული მონაცემთა დაცვის საზედამხედველო ორგანო;

ზ) მონაცემთა სუბიექტი - ნებისმიერი ფიზიკური პირი, რომლის შესახებ მონაცემიც მუშავდება.

თავი II. ინციდენტის აღმოჩენა და შიდა შეტყობინების პროცედურა

მუხლი 3. თანამშრომელთა ვალდებულებები და პირველადი რეაგირება

1. დეპარტამენტის ნებისმიერი თანამშრომელი, რომელიც სამსახურებრივი მოვალეობის შესრულებისას დააფიქსირებს, ეჭვს მიიტანს ან მესამე პირისგან მიიღებს ინფორმაციას მონაცემთა უსაფრთხოების შესაძლო დარღვევის, ტექნიკური ხარვეზის, ფიზიკური გასაღების დაკარგვის, სამუშაო სივრცეში უცხო პირის უნებართვო შეღწევის ან მატერიალური დოკუმენტების სეიფის გარეთ არასანქცირებული გადაადგილების შესახებ, ვალდებულია დაუყოვნებლივ, აღმოჩენისთანავე, უზრუნველყოს სათანადო რეაგირება.
2. დაუშვებელია თანამშრომლის მიერ ინციდენტის ფაქტის დამალვა ან ინფორმაციის მიწოდების დროში გაჭიანურება.

მუხლი 4. შიდა შეტყობინების უზრუნველყოფა

1. ინციდენტის ან მისი საფრთხის იდენტიფიცირების შემთხვევაში, კერძო კოპირების დეპარტამენტის და იურიდიული დეპარტამენტის ნებისმიერი თანამშრომელი, აგრეთვე, ინფორმაციული ტექნოლოგიების სპეციალისტი ვალდებულნი არიან მყისიერად, ზეპირი ან წერილობითი ფორმით (შიდა ელექტრონული კომუნიკაციის არხებით) ინფორმაცია მიაწოდონ ასოციაციის პერსონალურ მონაცემთა დაცვის ოფიცერს.
2. თუ ინციდენტი გამოვლენილია ავტომატიზებული უსაფრთხოების სისტემების დამცავი მექანიზმების მიერ, ინფორმაცია ავტომატურად ეგზავნება ინფორმაციული ტექნოლოგიების სპეციალისტს, რომელსაც, თავის მხრივ, ეკისრება პერსონალურ მონაცემთა დაცვის ოფიცრისთვის შეტყობინების ვალდებულება.
3. პირველადი შეტყობინების მიღებისთანავე, ინფორმაციული ტექნოლოგიების სპეციალისტი, კერძო კოპირების დეპარტამენტის უფროსი და პერსონალურ მონაცემთა დაცვის ოფიცერი ერთობლივად ახორციელებენ ინციდენტის პირველად შეფასებას და იღებენ შესაბამის გამოსასწორებელ ზომებს.

თავი III. ინციდენტის სიმძიმის შეფასება

მუხლი 5. ინციდენტის შესწავლისა და შეფასების წესი

1. ინციდენტის აღმოფხვრის პარალელურად, პერსონალურ მონაცემთა დაცვის ოფიცერი კერძო კოპირების დეპარტამენტის უფროსთან, ინფორმაციული ტექნოლოგიების სპეციალისტთან და, საჭიროების შემთხვევაში, სხვა ინციდენტთან შემხებლობაში მყოფ პირთან/პირებთან ერთად იწყებს ფაქტის სიღრმისეულ სამართლებრივ და ტექნიკურ მოკვლევას.

2. ასოციაცია კერძო კოპირების დეპარტამენტის საქმიანობის ფარგლებში ინციდენტს აფასებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონისა და „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და სახელმწიფო აუდიტის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ“ სახელმწიფო აუდიტის სამსახურის გენერალური აუდიტორის №008 ბრძანების შესაბამისად.

3. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შექმნის სიმძიმის შეფასებისას გასათვალისწინებელი გარემოებებია:

    ა) ინციდენტის სახე; იმ პერსონალური მონაცემების კატეგორია, რომლებზეც გავლენას ახდენს ინციდენტი;

    ბ) ინციდენტის შედეგად მონაცემთა სუბიექტის მესამე პირთა მიერ იდენტიფიცირების შესაძლებლობის ხარისხი;

    გ) ინციდენტის მასშტაბი, მონაცემთა სუბიექტის ან/და პერსონალური მონაცემის რაოდენობის ან/და მოცულობის თვალსაზრისით;

    დ) სხვა ისეთი გარემოება, რამაც შესაძლოა არსებითი გავლენა იქონიოს ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შექმნის ალბათობის სიმძიმეზე.

მუხლი 6. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობის განსაზღვრა

1. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა შესაძლოა იყოს დაბალი, საშუალო ან მაღალი:

ა) დაბალი რისკი - ინციდენტი სრულად აღმოფხვრილია ორგანიზაციის შიდა პერიმეტრზე, მონაცემები არ გამჟღავნებულა არაუფლებამოსილ პირებზე, არ მომხდარა მათი გაჟონვა და გამორიცხულია ნებისმიერი უარყოფითი ზეგავლენა პირთა უფლებებსა თუ კომერციულ ინტერესებზე.

ბ) საშუალო რისკი - ადგილი აქვს მონაცემებზე წვდომის დროებით შეზღუდვას ან შიდა არასანქცირებულ წვდომას, ზიანი ლოკალიზებულია, თუმცა არსებობს მცირე ალბათობა, რომ ინციდენტმა ირიბი გავლენა იქონიოს მონაცემთა სუბიექტებზე.

გ) მაღალი რისკი - სახეზეა მონაცემთა ბაზების უნებართვო გამჟღავნება, კომერციული საიდუმლოების ან პერსონალური მონაცემების ორგანიზაციის გარეთ, არაუფლებამოსილი პირების ხელში ჩავარდნა, რამაც შესაძლოა გამოიწვიოს ადამიანის ძირითადი უფლებებისა და თავისუფლებების ხელყოფის ან იმპორტიორთა ინტერესების დაზიანების მომეტებული საფრთხე.

თავი IV. ინციდენტის შესახებ სახელმწიფო აუდიტის სამსახურისა და მონაცემთა სუბიექტის შეტყობინების წესი

მუხლი 7. სახელმწიფო აუდიტის სამსახურის ინფორმირება

1. თუ წინამდებარე პროცედურის მე-5 და მე-6 მუხლების საფუძველზე ჩატარებული სამართლებრივი შეფასებით დადგინდება, რომ მონაცემთა ინციდენტი საშუალო ან მაღალი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, ასოციაცია ვალდებულია ინციდენტის შესახებ შეტყობინების მიღებიდან გონივრულ ვადაში, მაგრამ არაუგვიანეს 72 საათისა, აცნობოს სახელმწიფო აუდიტის სამსახურს.

2. ასოციაცია სახელმწიფო აუდიტის სამსახურისთვის წარსადგენ ოფიციალურ დოკუმენტს ამზადებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონისა და „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და სახელმწიფო აუდიტის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ“ სახელმწიფო აუდიტის სამსახურის გენერალური აუდიტორის №008 ბრძანების შესაბამისად.

3. თუკი 72-საათიან ვადაში შეუძლებელია სრული ინფორმაციის მოპოვება, სახელმწიფო აუდიტის სამსახურს ასოციაცია აწვდის პირველად მონაცემებს

განსაზღვრულ ვადაში, ხოლო დანარჩენ ინფორმაციას წარადგენს ეტაპობრივად, ყოველგვარი დაუსაბუთებელი დაყოვნების გარეშე.

მუხლი 8. მონაცემთა სუბიექტის ინფორმირების წესი

1. თუ ინციდენტი მაღალი ალბათობით გამოიწვევს მნიშვნელოვან ზიანს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, ასოციაცია ვალდებულია ინციდენტის აღმოჩენიდან პირველი შესაძლებლობისთანავე, გაუმართლებელი დაყოვნების გარეშე აცნობოს მონაცემთა სუბიექტს ინციდენტის შესახებ და მარტივ და მისთვის გასაგებ ენაზე მიაწოდოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 30-ე მუხლის პირველი პუნქტით გათვალისწინებული ინფორმაცია.

2. სუბიექტისთვის გაგზავნილი შეტყობინება უნდა იყოს შედგენილი მკაფიო, მარტივი და გასაგები ენით.

3. სუბიექტის ინფორმირების ვალდებულება არ წარმოიშობა, თუ სახეზეა ერთ-ერთი შემდეგი წინაპირობა:

    ა) ასოციაციამ ინციდენტის დადგომამდე უზრუნველყო მონაცემთა სათანადო ტექნიკური დაცვა;

    ბ) ინციდენტის დაფიქსირებისთანავე გატარდა მყისიერი და ეფექტიანი ზომები, რის შედეგადაც სრულად გამოირიცხა მომეტებული საფრთხის რეალურად დადგომის ალბათობა;

    გ) სუბიექტთა ინდივიდუალური ინფორმირება მოითხოვს არაპროპორციულად დიდ ძალისხმევას. ასეთ შემთხვევაში, ასოციაცია ახორციელებს საჯარო შეტყობინებას (განცხადებას) ან იყენებს სხვა იდენტურად ეფექტიან ალტერნატიულ საშუალებას, რომლითაც უზრუნველყოფილი იქნება პირთა თანაბარი საინფორმაციო ხელმისაწვდომობა.

თავი V. ინციდენტების რეგისტრაცია, სისტემური ანალიზი და პრევენცია

მუხლი 9. ინციდენტების შიდა აღრიცხვის ჟურნალის წარმოება

1. დეპარტამენტში დაფიქსირებული ნებისმიერი უსაფრთხოების დარღვევა, მიუხედავად მისი მასშტაბისა, სპეციფიკისა და რისკის ხარისხისა (მათ შორის დაბალი რისკის მქონე შიდა ხარვეზებიც), ექვემდებარება სავალდებულო შიდა რეგისტრაციას.

2. პერსონალურ მონაცემთა დაცვის ოფიცერი აწარმოებს „მონაცემთა უსაფრთხოების ინციდენტების შიდა აღრიცხვის სპეციალურ ჟურნალს“ (ელექტრონული ფორმით), სადაც ფიქსირდება:

   ა) ინციდენტის აღმოჩენის ზუსტი თარიღი, დრო და გარემოებები;

   ბ) ფაქტობრივი გარემოებების მოკლე აღწერა და დარღვეული მონაცემების კატეგორიები;

   გ) ინციდენტის კლასიფიკაცია (რისკის დონის მითითება);

   დ) ზიანის აღმოსაფხვრელად და საინფორმაციო ნაკადების დასაცავად გატარებული ორგანიზაციული და ტექნიკური ზომები;

   ე) პერსონალურ მონაცემთა დაცვის სამსახურისა თუ მონაცემთა სუბიექტების ინფორმირების ფაქტი, თარიღი და ფორმა (ან ინფორმაციის მიუწოდებლობის სამართლებრივი საფუძველი).

მუხლი 10. სისტემური ხარვეზების აღმოფხვრა და პრევენციული ღონისძიებები

1. ინციდენტის სრულად აღმოფხვრის, სისტემების სტაბილურ რეჟიმში დაბრუნებისა და ზიანის ლოკალიზაციის შემდგომ, პერსონალურ მონაცემთა დაცვის ოფიცერი, კერძო კოპირების დეპარტამენტის უფროსი და ინფორმაციული ტექნოლოგიების სპეციალისტი ახდენენ მომხდარი ფაქტის სიღრმისეულ ანალიზს.

2. მოკვლევის შედეგად იდენტიფიცირდება პროგრამული უზრუნველყოფის ან შიდა ორგანიზაციული მართვის სისტემების გამოწვევები/ნაკლოვანებები, რის საფუძველზეც მონაცემთა დაცვის ოფიცერი შეიმუშავებს რეკომენდაციებს, მომავალში ანალოგიური ხასიათის ინციდენტების განმეორების თავიდან აცილების მიზნით.

თავი VI. დასკვნითი დებულებები

მუხლი 11. პროცედურის გადახედვა, განახლება და თანამშრომელთა ინფორმირება

1. წინამდებარე პროცედურის ეფექტიანობა ექვემდებარება მუდმივ მონიტორინგს პერსონალურ მონაცემთა დაცვის ოფიცრის მიერ.

2. დოკუმენტის გეგმური გადახედვა და აუდიტი ხორციელდება 6 (ექვსი) თვეში ერთხელ მაინც, ხოლო არაგეგმური გადახედვა და მასში ცვლილებების/დამატებების შეტანა ხდება მოქმედ პერსონალურ მონაცემთა დაცვის კანონმდებლობაში ცვლილების შეტანისას, დეპარტამენტის ტექნოლოგიური ინფრასტრუქტურის, საინფორმაციო ქსელების ან

პროგრამული უზრუნველყოფის მოდიფიცირებისას, არსებული მონაცემთა უსაფრთხოების დარღვევის ანალიზის საფუძველზე, თუ გამოვლინდა დამატებითი ორგანიზაციულ-ტექნიკური დამცავი ზომების დანერგვის აუცილებლობა.

3. ნებისმიერი ცვლილება მტკიცდება ასოციაციის გენერალური დირექტორის ბრძანებით პერსონალურ მონაცემთა დაცვის ოფიცერთან წინასწარი შეთანხმების საფუძველზე.

4. წინამდებარე პროცედურის, აგრეთვე მასში განხორციელებული ნებისმიერი ცვლილების გაცნობა დეპარტამენტის არსებული და ახალი თანამშრომლებისთვის არის სავალდებულო. გაცნობის ფაქტი დასტურდება თანამშრომლის პირადი ხელმოწერით სპეციალურ საინფორმაციო ფურცელზე.