პერსონალურ მონაცემთა
დაცვის სამსახური

რეკომენდაციები ინციდენტთან დაკავშირებული ღონისძიებების განხორციელების თაობაზე

www.pdps.ge

რეკომენდაციები ემსახურება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ნორმათა განმარტებას, საუკეთესო პრაქტიკის დამკვიდრების ხელშეწყობას, ის არ წარმოადგენს სამართლებრივ აქტს, არის სარეკომენდაციო ხასიათის და არ წარმოშობს დამატებით უფლებებსა და ვალდებულებებს.

შინაარსი

შესავალი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, ევროპის სახელმწიფოებში მოქმედი რეგულაციების მსგავსად, ითვალისწინებს პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული ინციდენტის ცნებას[1]. ამასთანავე, კანონი განსაზღვრავს ინციდენტთან დაკავშირებული ინფორმაციის აღრიცხვის, ხოლო ზოგიერთ შემთხვევაში, ინციდენტის ირგვლივ არსებული გარემოებებისა და მის შედეგად წარმოქმნილი რისკების შესახებ ინფორმაციის პერსონალურ მონაცემთა დაცვის სამსახურისთვის და მონაცემთა სუბიექტებისთვის მიწოდების ვალდებულებას. ინციდენტების შესახებ ინფორმაციის სისტემატიზების და მათ შესახებ ინფორმირების ამგვარი მექანიზმი მონაცემთა დაცვის ქართულ კანონმდებლობაში სიახლეს წარმოადგენს და მისი მიზანია, ხელი შეუწყოს პერსონალური მონაცემების უკანონო დამუშავების შედეგად მონაცემთა სუბიექტების უფლებებისადმი მოსალოდნელი უარყოფითი შედეგების თავიდან არიდებას.

წინამდებარე რეკომენდაციები მიზნად ისახავს, მათ შორის, კონკრეტულ პრაქტიკულ მაგალითებზე მითითებით, გაანალიზოს კანონმდებლობის ზემოაღნიშნული დანაწესი, რათა შესაბამისმა პასუხისმგებელმა სუბიექტებმა სრულყოფილად აღიქვან მათთვის დაკისრებული ვალდებულებების არსი და ფარგლები.

რეკომენდაციები მომზადებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) ნორმატიული შინაარსისა და მონაცემთა დაცვის ევროპული საბჭოს (EDPB) სახელმძღვანელო რეკომენდაციების[2] ანალიზის საფუძველზე.

[1] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) მე-3 მუხლის „წ“ ქვეპუნქტი.

[2] EDPB, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, 2023.

1. ინციდენტის ცნება

იმისთვის, რომ პასუხისმგებელმა სუბიექტებმა ჯეროვნად შეძლონ ინციდენტებთან დაკავშირებული ვალდებულების შესრულება, აუცილებელია, მათ სათანადოდ ესმოდეთ, თუ რას წარმოადგენს ინციდენტი.

ინციდენტის ცნებას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის „წ“ ქვეპუნქტი განსაზღვრავს, რომლის თანახმად, 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.

ზემოაღნიშნული ცნების შესაბამისად, განსაკუთრებით საყურადღებოა, რომ ინციდენტის არსებობის განსაზღვრის მიზნებისთვის:

- მონაცემთა განადგურებად მიჩნეულ უნდა იქნეს შემთხვევა, რომლის შედეგად მონაცემები საერთოდ აღარ არსებობს, ან აღარ არსებობს რაიმე გამოყენებადი ფორმით;
- მონაცემთა დაზიანება სახეზეა მაშინ, როდესაც მონაცემები შეიცვალა, გახდა არაზუსტი ან არასრული;
- მონაცემთა დაკარგვად უნდა ჩაითვალოს, როდესაც მონაცემები შესაძლოა კვლავ არსებობდეს, თუმცა ისინი აღარ არის დამუშავებისთვის პასუხისმგებელი პირის მფლობელობაში, ან როდესაც მონაცემები კვლავ დამუშავებისთვის პასუხისმგებელ პირთან ინახება, მაგრამ მას აღარ აქვს მათზე კონტროლი ან/და სათანადო წვდომა.

თითოეული ინციდენტი, თავისი არსით, ინფორმაციული უსაფრთხოების პრინციპების დარღვევაა, თუმცა ინფორმაციული უსაფრთხოების დარღვევის ყველა შემთხვევა არ წარმოადგენს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრულ ინციდენტს. აღნიშნული კანონის მიზნებისთვის, ინციდენტად ინფორმაციული უსაფრთხოების დარღვევის მხოლოდ ის შემთხვევები მიიჩნევა, რომლებიც პერსონალურ მონაცემებს შეეხება. ***მაგალითად, თუ ადგილი ჰქონდა კიბერშეტევას, რომლის შედეგად, კომპანიის მონაცემთა ბაზაში განადგურდა ინფორმაცია კომპანიის ბალანსზე არსებული ავტომობილების შესახებ (რაც არ მოიცავდა მონაცემთა სუბიექტის პერსონალურ მონაცემებს), ასეთი შემთხვევა არ ჩაითვლება ინციდენტად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიზნებისთვის, რადგან ინციდენტს გავლენა არ მოუხდენია პერსონალურ მონაცემებზე.***

იმის მიხედვით, თუ მათ შედეგად ინფორმაციული უსაფრთხოების რომელი პრინციპი დაირღვა, ინციდენტების დაჯგუფება შესაძლებელია შემდეგ სახეებად:

ა) კონფიდენციალურობის დარღვევა - როდესაც ხდება პერსონალური მონაცემების უნებართვო ან შემთხვევითი გამჟღავნება ან მათზე ამგვარი წვდომა. ***კონფიდენციალურობის დარღვევის ერთ-ერთ მაგალითად შეიძლება ჩაითვალოს შემთხვევა, როდესაც, ინციდენტის შედეგად, მონაცემთა ბაზაზე წვდომა მიეცა არაუფლებამოსილ პირს;***

ბ) მთლიანობის დარღვევა - როდესაც ხდება პერსონალური მონაცემების უნებართვო ან შემთხვევითი შეცვლა. ***მთლიანობის დარღვევის ერთ-ერთ მაგალითად შეიძლება ჩაითვალოს შემთხვევა, როდესაც სამედიცინო დაწესებულების თანამშრომელმა მონაცემთა ბაზაში შემთხვევით გადაანაცვლა მონაცემები პაციენტების სისხლის ჯგუფის შესახებ;***

გ) ხელმისაწვდომობის დარღვევა - როდესაც დამუშავებისთვის პასუხისმგებელი პირი კარგავს პერსონალურ მონაცემებზე წვდომას, ან ხდება წვდომის უნებართვო შეზღუდვა ან დაზიანება, ასევე, მონაცემების ამგვარი განადგურება ან წაშლა. ***ხელმისაწვდომობის დარღვევის ერთ-ერთ მაგალითად შეიძლება ჩაითვალოს შემთხვევა, როდესაც საფინანსო დაწესებულების საინფორმაციო სისტემაზე განხორციელდა კიბერთავდასხმა, რომლის შედეგად პერსონალური მონაცემები დაიშიფრა თავდამსხმელის მიერ, თუმცა არ მომხდარა მონაცემთა გადინება. შესაბამისად, ადგილი აქვს მხოლოდ ხელმისაწვდომობის დარღვევას, რომლის საფუძველზეც დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ პირს ეზღუდება წვდომა პერსონალურ მონაცემებზე.***

ზოგიერთი ინციდენტი შესაძლოა ერთდროულად არღვევდეს როგორც მონაცემთა კონფიდენციალურობის, ისე მთლიანობის ან/და ხელმისაწვდომობის პრინციპს.

2. ინციდენტის აღმოჩენა

იმისთვის, რომ შესაძლებელი გახდეს ინციდენტებთან დაკავშირებული ვალდებულებების შესრულება და მონაცემთა სუბიექტების უფლებებისადმი მოსალოდნელი უარყოფითი შედეგების თავიდან აცილებისთვის საჭირო ღონისძიებების დროულად გატარება, პირველ რიგში, აუცილებელია, ინციდენტი დროულად იქნეს აღმოჩენილი.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლი მონაცემთა დამუშავებაში ჩართულ სუბიექტებს ავალდებულებს, მიიღონ მონაცემთა დამუშავების თანამდევი რისკების ადეკვატური ტექნიკური და ორგანიზაციული ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას დაკარგვისგან, უკანონო დამუშავებისგან, მათ შორის, განადგურებისგან, წაშლისგან, შეცვლისგან, გამჟღავნებისგან ან გამოყენებისგან. აღნიშნული გულისხმობს, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა და დამუშავებაზე უფლებამოსილმა პირებმა უნდა იზრუნონ იმგვარი უსაფრთხოების ზომების შემოღებაზე, რომლებითაც შესაძლებელი იქნება ინციდენტების ეფექტური პრევენცია, ხოლო მათი მოხდენის შემთხვევაში, დროული გამოვლენა და აღკვეთა.

მაგალითისთვის, ინციდენტების გამოსავლენად ეფექტიანი ზომების მიღება შესაძლოა გულისხმობდეს მონაცემთა დამუშავების პროცესში უჩვეულო აქტივობების აღმოსაჩენად ისეთი ტექნიკური მექანიზმების გამოყენებას, როგორიცაა მონაცემთა ნაკადის და „ლოგების“ ანალიტიკა ან/და სხვა. ავრეთვე მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელ პირს გააჩნდეს ინციდენტის აღმოჩენის შემდეგ მასზე შემდგომი რეაგირების შიდა წესი და განსაზღვრული ჰყავდეს რეაგირების პროცესზე პასუხისმგებელი კონკრეტული პირები. მნიშვნელოვანია, შიდა წესი უზრუნველყოფდეს ინციდენტის შესახებ ინფორმაციის დროულ

და ეფექტურ მიწოდებას შესაბამისი პასუხისმგებელი პირებისთვის, მათ შორის, საჭიროების შემთხვევაში, დაწესებულების მაღალი მმართველობითი რგოლის წარმომადგენლებისთვის.

გარდა ამისა, დამუშავებისთვის პასუხისმგებელ პირს თითოეულ დამუშავებაზე უფლებამოსილ პირთან შეთანხმებული უნდა ჰქონდეს კონკრეტული პროცედურა, რომლითაც იგი დროულად მიიღებს მათ მიერ დაფიქსირებული ინციდენტების შესახებ ინფორმაციას. თავის მხრივ, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 29-ე მუხლი დამუშავებაზე უფლებამოსილ პირს ავალდებულებს, ინციდენტის შესახებ დაუყოვნებლივ აცნობოს დამუშავებისთვის პასუხისმგებელ პირს.

ინციდენტი აღმოჩენილად, ხოლო დამუშავებისთვის პასუხისმგებელი პირი ინციდენტის შესახებ ინფორმირებულად იმ მომენტიდან ითვლება, როდესაც მან შეიტყო ან უნდა შეეტყო ინციდენტის შესახებ.

ზოგიერთი ტიპის ინციდენტის არსებობის ცალსახად გამოვლენა, მისი ხასიათიდან გამომდინარე, ნაკლებ სირთულეს უკავშირდება და მათთან მიმართებით, დამუშავებისთვის პასუხისმგებელი პირის სათანადო დონეზე ინფორმირებულობის მომენტის განსაზღვრაც შედარებით მარტივია. ზოგჯერ კი, იმის სათანადოდ დადგენას, შეიძლება თუ არა უსაფრთხოების დარღვევამ პერსონალური მონაცემების არამართლზომიერი დამუშავება გამოიწვიოს, გარკვეული დამატებითი ღონისძიებების გატარება და დრო სჭირდება. შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირის მიერ ამგვარი ინციდენტის აღმოჩენის ზუსტი დროის განსაზღვრა, შესაძლოა, გარკვეულ შეფასებას მოითხოვდეს. ***მაგალითად, ისეთ შემთხვევებში, როდესაც შესაძლო ინციდენტის შესახებ ინფორმაციას დამუშავებისთვის პასუხისმგებელი პირი რომელიმე მედიასაშუალებისგან ან სხვა მესამე პირისგან მიიღებს, იმთავითვე არ უნდა ჩაითვალოს, რომ იგი ინციდენტის შესახებ სათანადოდ ინფორმირებულია. ამგვარი ინფორმაციის მიღების შემდეგ, დამუშავებისთვის პასუხისმგებელ პირს ინციდენტის არსებობის ვარაუდის სარწმუნოობის დასადგენად შესაძლოა დასჭირდეს გარკვეული გონივრული პერიოდი.*** შესაბამისად, ინციდენტის აღმოჩენის მომენტად ის დრო უნდა იქნეს მიჩნეული, როდესაც პირველადი მოკვლევისა და შეფასების საფუძველზე, დამუშავებისთვის პასუხისმგებელმა პირმა შეიტყო ან უნდა შეეტყო ინციდენტის შესახებ. თავის მხრივ, ინციდენტის აღმოჩენისა და მისი შესაძლო შედეგების პირველადი შეფასებისთვის საჭირო ღონისძიებები დამუშავებისთვის პასუხისმგებელმა პირმა მყისიერად, ყოველგვარი არასათანადო დაყოვნების გარეშე უნდა გაატაროს.

3. აღმოჩენილ ინციდენტთან დაკავშირებული ვალდებულებები

3.1. ინციდენტის აღრიცხვა

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს და მის სპეციალურ წარმომადგენელს (ასეთის არსებობის შემთხვევაში), ისევე, როგორც დამუშავებაზე უფლებამოსილ პირს, ევალებათ,

აღრიცხონ მონაცემთა დამუშავებასთან დაკავშირებული, მათ შორის, ინციდენტების შესახებ ინფორმაცია. აღსანიშნავია, რომ ეს ვალდებულება ყველა აღმოჩენილ ინციდენტზე ვრცელდება, მიუხედავად იმისა, ექვემდებარება თუ არა ინციდენტი პერსონალურ მონაცემთა დაცვის სამსახურისთვის ან/და მონაცემთა სუბიექტებისთვის შეტყობინებას.

პერსონალურ მონაცემთა დაცვის სამსახურის მოთხოვნის შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირები, დამუშავებაზე უფლებამოსილი პირები და სპეციალური წარმომადგენლები ვალდებულნი არიან, ნებისმიერ ინციდენტთან დაკავშირებით მათ ხელთ არსებული ინფორმაცია დაუყოვნებლივ, მაგრამ არაუგვიანეს 3 სამუშაო დღისა წარუდგინონ სამსახურს.

რაც შეეხება ინციდენტის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისთვის და მონაცემთა სუბიექტებისთვის, მოთხოვნის გარეშე, საკუთარი ინიციატივით შეტყობინებას, ამის ვალდებულება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 29-ე და 30-ე მუხლით არის განსაზღვრული და დამუშავებისთვის პასუხისმგებელ პირს ეკისრება. ნიშანდობლივია, რომ ამგვარი შეტყობინების ვალდებულება, ინციდენტის აღრიცხვის საჭიროებისგან განსხვავებით, ყველა ინციდენტზე არ ვრცელდება და იგი თითოეულ შემთხვევაში კონკრეტულ შეფასებას საჭიროებს, რა დროსაც მხედველობაში უნდა იქნეს მიღებული ინციდენტისგან მონაცემთა სუბიექტების უფლებების მიმართ დამდგარი ან მოსალოდნელი შედეგები.

3.2. ინციდენტის შეფასება

იმის მიხედვით, თუ რა შესაძლო შედეგებს იწვევს ინციდენტი ადამიანის ძირითადი უფლებებისა და თავისუფლებების მიმართ, იგი შეიძლება პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულებას დაექვემდებაროს. ამასთანავე, ზოგიერთ შემთხვევაში, მოსალოდნელი შედეგებიდან გამომდინარე, შესაძლოა, ასევე საჭირო იყოს, რომ ინციდენტის შესახებ გარკვეული ინფორმაცია მონაცემთა სუბიექტებსაც ეცნობოთ. ნიშანდობლივია, რომ ამ ღონისძიებების განხორციელების ვალდებულება, ინციდენტების შესახებ ინფორმაციის აღრიცხვის ვალდებულებისგან განსხვავებით, ყველა ინციდენტზე არ ვრცელდება და მისი არსებობა თითოეულ შემთხვევაში შეფასებას საჭიროებს. შეფასებისას კი მხედველობაში უნდა იქნეს მიღებული ინციდენტისგან მონაცემთა სუბიექტების უფლებების მიმართ მოსალოდნელი შედეგები და ამ შედეგის დადგომის ალბათობის ხარისხი.

ასევე, აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული ინციდენტის ხასიათიდან გამომდინარე, ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებების შელახვის ალბათობა და სიმძიმე ფასდება ხარისხობრივი ანალიზის შედეგად, ვინაიდან ინციდენტით გამოწვეული/მოსალოდნელი ზიანის რაოდენობრივი სახით გამოსახვა შესაძლოა შეუძლებელიც კი იყოს. ამგვარი ანალიზის ფარგლებში, ობიექტური გადაწყვეტილება მიიღება გამოცდილების, არსებული ინფორმაციის, ცოდნის, განსჯის და პერსონალურ მონაცემთა დაცვის სამსახურის მიერ დამტკიცებული

წესით დადგენილი კრიტერიუმების გათვალისწინებით. ანალიზის ეს ტიპი სიტყვიერად აღწერს ადამიანის უფლებებისა და თავისუფლებების შელახვის ალბათობას და ინციდენტის გავლენის მასშტაბს. შესაბამისად, მნიშვნელოვანია ანალიზის პროცესში პერსონალურ მონაცემთა დაცვის ოფიცრის მონაწილეობა, ასეთის არსებობის შემთხვევაში.

ინციდენტის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების და მონაცემთა სუბიექტების ინფორმირების ვალდებულება მხოლოდ უშუალოდ დამუშავებისთვის პასუხისმგებელ პირს ეკისრება. ამდენად, იმის გამოსარკვევად, ექვემდებარება თუ არა ესა თუ ის ინციდენტი პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების და მონაცემთა სუბიექტების ინფორმირების ვალდებულებებს, დამუშავებისთვის პასუხისმგებელმა პირმა ინციდენტის აღმოჩენისთანავე უნდა დაიწყოს მისი შეფასება. შეფასების ფარგლებში უნდა განისაზღვროს როგორც ინციდენტით მონაცემთა სუბიექტების უფლებებისადმი გამოწვეული შესაძლო შედეგის სიმძიმე, ისე ამ შედეგის დადგომის ალბათობა. გარკვეული სახის მონაცემების უკანონო დამუშავების შედეგად არსებული სავარაუდო რისკების შეფასება დამუშავებისთვის პასუხისმგებელ პირს, შესაძლოა, მონაცემთა დაცვაზე ზეგავლენის შეფასების ფარგლებშიც ჰქონდეს განხორციელებული, თუმცა ამგვარი შეფასება ჰიპოთეტური და გარკვეულწილად ზოგადია. შესაბამისად, აუცილებელია, ინციდენტის შედეგად მოსალოდნელი შედეგები უკვე დამდგარი, კონკრეტული გარემოებების გათვალისწინებით შეფასდეს.

3.2.1. ადამიანის უფლებებისა და თავისუფლებების შელახვის სიმძიმის შეფასების კრიტერიუმები

ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებების შელახვის სიმძიმე დამუშავებისთვის პასუხისმგებელი პირის მიერ უნდა შეფასდეს, მათ შორის, შემდეგი კრიტერიუმების გათვალისწინებით:

- **ინციდენტის სახე**

როგორც აღინიშნა, ინციდენტი ყოველთვის უკავშირდება პერსონალურ მონაცემებს და ინფორმაციული უსაფრთხოების საყოველთაოდ აღიარებული პრინციპების შესაბამისად, იყოფა შემდეგ სახეებად:

- კონფიდენციალურობის დარღვევა;
- მთლიანობის დარღვევა;
- ხელმისაწვდომობის დარღვევა.

ინციდენტის სახე, ზოგიერთ შემთხვევაში, შესაძლოა, იმთავითვე მიანიშნებდეს მის საფუძველზე მონაცემთა სუბიექტების უფლებრივი მდგომარეობისკენ მიმართული შესაძლო შედეგების მომეტებულ სიმძიმეზე. ***მაგალითად, მონაცემების კონფიდენციალურობის დარღვევა, კერძოდ, მათი არაუფლებამოსილი პირის ხელში მოხვედრა, ხშირ შემთხვევაში,***

მონაცემთა სუბიექტების უფლებებისადმი უფრო მძიმე შედეგების გამომწვევად შეიძლება ჩაითვალოს, ვიდრე იმავე მონაცემების მთლიანობის ან ხელმისაწვდომობის დარღვევა.

- **იმ პერსონალური მონაცემების კატეგორია, რომლებზეც ინციდენტი გავლენას ახდენს**

ინციდენტის შესაძლო შედეგების სიმძიმის შეფასებისას, ბუნებრივია, ყურადღება უნდა მიექცეს იმ პერსონალური მონაცემების კატეგორიას, რომლებზეც ინციდენტი გავლენას ახდენს.

აღნიშნული არ მოიცავს მხოლოდ იმის განსაზღვრას, მიემართება თუ არა ინციდენტი განსაკუთრებული კატეგორიის მონაცემებს. ამგვარი შეფასებისას ყურადღება უნდა გამახვილდეს თითოეული მონაცემის შინაარსის სენსიტიურობაზე, რაც შესაძლოა არამხოლოდ განსაკუთრებული კატეგორიის მონაცემებს ახასიათებდეთ. რაც უფრო სენსიტიურია მონაცემები, მით უფრო მძიმე შეიძლება იყოს ინციდენტის შედეგად მათი უკანონო დამუშავებით გამოწვეული შედეგი.

მონაცემების კატეგორიის შეფასებისას მნიშვნელოვანია, რომ მონაცემები შეფასდეს როგორც ცალ-ცალკე, ისე ერთობლიობაში. ზოგიერთ შემთხვევაში, ინციდენტის შედეგად უკანონოდ დამუშავებული, განყენებული სახით აღებული რომელიმე მონაცემი შესაძლოა არ ატარებდეს განსაკუთრებით სენსიტიურ ხასიათს, თუმცა არაუფლებამოსილი პირის მიერ ყველა მათგანზე წვდომის ერთდროულად მოპოვების შეთხვევაში იქმნებოდეს მონაცემთა სუბიექტის უფლებების შელახვის უფრო მაღალი ხარისხი.

შეფასებისას ასევე გასათვალისწინებელია, თუ რა ხასიათს იძენს მონაცემები ინციდენტის შედეგად მათზე არაუფლებამოსილი წვდომის მქონე პირების ვინაობის და მათი მონაცემთა სუბიექტთან კავშირის გათვალისწინებით. *მაგალითად, მშვილებლების ვინაობისა და მისამართის ბიოლოგიური მშობლებისთვის გამჟღავნების შემთხვევა უფრო სენსიტიური ინფორმაციის კატეგორიად უნდა ჩაითვალოს, ვიდრე ეს სხვა პირების მიერ მათზე წვდომის შემთხვევაში იქნებოდა.*

- **განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე პირები, როგორც მონაცემთა სუბიექტები**

ინციდენტის შედეგად ადიამანის უფლებებისა თავისუფლებების შელახვის სიმძიმის განსაზღვრისას დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეაფასოს, ეხება თუ არა ინციდენტი არასრულწლოვნების, შეზღუდული შესაძლებლობის მქონე პირებისა და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე მონაცემთა სუბიექტ(ებ)ის პერსონალურ მონაცემებს.

იმ შემთხვევაში, თუ ინციდენტი ეხება ზემოაღნიშნულ პირებს, რომლებიც ამა თუ იმ ფაქტობრივი ან სამართლებრივი გარემოების გამო უფლებების შელახვის მომეტებული საფრთხის წინაშე არიან, ინციდენტის სავარაუდო შედეგი შეიძლება უფრო მძიმედ შეფასდეს, ვიდრე ეს სხვა მონაცემთა სუბიექტების შემთხვევაში იქნებოდა.

- **მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობის ხარისხი**

შეფასებისთვის ასევე მნიშვნელოვანია, რამდენად მარტივად არის შესაძლებელი ინციდენტის შედეგად არამართლზომიერად დამუშავებული მონაცემებით კონკრეტული პირების იდენტიფიცირება ან იდენტიფიცირებულ პირებთან ამ მონაცემების დაკავშირება. ზოგიერთი მონაცემი, მისი შინაარსის გათვალისწინებით, შესაძლოა, პირდაპირ ახდენდეს პირის იდენტიფიცირებას ან მარტივად იყოს დაკავშირებადი ამა თუ იმ კონკრეტულ სუბიექტთან. ზოგჯერ კი, ინფორმაციის ამა თუ იმ კონკრეტულ პირთან დაკავშირება რთულია, თუმცა მაინც შესაძლებელი. ***მაგალითად, მონაცემების ფსევდონიმიზაცია საგრძნობლად ამცირებს ასეთ მონაცემებზე უკანონო წვდომის შემთხვევაში კონკრეტული პირების იდენტიფიცირების რისკს, თუმცა მხოლოდ ფსევდონიმიზაციით ამ რისკების სრულად აღმოფხვრა არ ხდება.***

- **მონაცემთა სუბიექტ(ებ)ის უფლებებისა და ინტერესების მიმართ დამდგარი შედეგი**

შეფასების ფარგლებში, ყურადღება უნდა გამახვილდეს, რამდენად მძიმე შეიძლება იყოს ინციდენტით გამოწვეული შედეგი მონაცემთა სუბიექტებისათვის. შესაბამისად, მოცემული კრიტერიუმის ფარგლებში უნდა შეფასდეს, ხომ არ გამოიწვევს ინციდენტი სუბიექტის უფლებებისათვის ისეთ მძიმე შედეგებს, როგორიცაა ვინაობის მითვისება (ე.წ. "Identity theft"), მონაცემთა სუბიექტისთვის ფიზიკური, ფსიქოლოგიური ან ფინანსურ ზიანი, რეპუტაციის შელახვა და სხვა.

- **დამუშავებისთვის პასუხისმგებელი პირის საქმიანობის განსაკუთრებული ხასიათი**

ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისადმი მოსალოდნელი ზიანის სიმძიმის შეფასებისას მხედველობაში მიიღება დამუშავებისთვის პასუხისმგებელი პირის საქმიანობის ხასიათიც, რასაც შესაძლოა ახლდეს მომეტებული საფრთხე. ***მაგალითად, თუ ინციდენტი სამედიცინო დაწესებულების მიერ მონაცემთა დამუშავებას ეხება, რომელიც, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებს ამუშავებს, იარსებებს სავარაუდო ზიანის მომეტებული სიმძიმის პრეზუმფცია. ასევე, საქმიანობის ხასიათიდან გამომდინარე, ზიანის მომეტებული სიმძიმის პრეზუმფცია იარსებებს, მაგალითად, სამართლდამცავ ორგანოებთან, ან ფინანსურ დაწესებულებთან დაკავშირებულ შემთხვევებში.***

- **ინციდენტის მასშტაბი, მონაცემთა სუბიექტის ან/და პერსონალური მონაცემის რაოდენობის ან/და მოცულობის თვალსაზრისით;**

ზოგიერთ შემთხვევაში, შესაძლოა, ინციდენტი ერთი ან რამდენიმე პირის მონაცემებს შეეხოს, ზოგჯერ კი შეიძლება ინციდენტის შედეგად ათასობით პირის მონაცემების უსაფრთხოება დაირღვეს. როგორც წესი, დაზარალებულ მონაცემთა სუბიექტების დიდი რაოდენობა მოსალოდნელი ზიანის სიმძიმის პრეზუმფციას განაპირობებს. მიუხედავად ამისა, დაზარალებული მონაცემთა სუბიექტების მცირე რაოდენობა ყოველთვის არ ნიშნავს ინციდენტის შედეგად მოსალოდნელი ზიანის სიმცირეს. მონაცემთა სუბიექტების რაოდენობასთან ერთად, თითოეულ შემთხვევაში ყურადღება უნდა მიექცეს იმ მონაცემების რაოდენობასა და მოცულობას, რომლებსაც ინციდენტი შეეხო. ადამიანის უფლებებისა და თავისუფლებებისადმი მნიშვნელოვანი ზიანი, შესაძლოა, ერთი ან რამდენიმე მონაცემთა

სუბიექტის არსებობის შემთხვევაშიც გამოიკვეთოს, ინციდენტის შედეგად უკანონოდ დამუშავებული მონაცემების მოცულობისა და ხასიათიდან გამომდინარე.

- **სხვა გარემოებები**

აღსანიშნავია, რომ ზემოაღნიშნული კრიტერიუმები არ არის ამომწურავი და ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისადმი მოსალოდნელი ზიანის სიმძიმის განსაზღვრისას, თითოეულ შემთხვევაში უნდა შეფასდეს სხვა არსებითი მნიშვნელობის მქონე გარემოებებიც.

3.2.2. ადამიანის უფლებებისა და თავისუფლებების შელახვის სიმძიმის განსაზღვრის კრიტერიუმები

ინციდენტი, ადამიანის უფლებებისა და თავისუფლებების შელახვის სიმძიმის თვალსაზრისით, მნიშვნელოვანი ზიანის გამომწვევად უნდა იქნეს მიჩნეული, მათ შორის, იმ შემთხვევებში, თუ მას მოჰყვა/შესაძლოა მოჰყვეს ერთ-ერთი შემდეგი შედეგი:

- მონაცემთა სუბიექტის დისკრიმინაცია (მათ შორის უკანონოდ მოპოვებული მონაცემების გამოყენებით პროფაილინგის შედეგად), ვინაობის მითვისება (ე.წ. Identity Theft) ან გაყალბება, ფინანსური ზიანი (მაგ. საკრედიტო ბარათის მონაცემების მოპარვა), მონაცემთა სუბიექტის რეპუტაციის შელახვა, პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალობის დარღვევა, ან სხვა სახის მნიშვნელოვანი სოციალური ან/და ეკონომიკური ზიანი;
- მონაცემთა სუბიექტის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული უფლებების რეალიზებისათვის ხელის შეშლა, მათ შორის, მონაცემთა სუბიექტის უფლებების კანონით დადგენილ ვადებში რეალიზების შეზღუდვა;
- პერსონალური მონაცემების იმგვარი წაშლა/განადგურება, რომელიც არ ექვემდებარება აღდგენას, ან მისი აღდგენა არაპროპორციულად დიდ დროსა და ძალისხმევას საჭიროებს, გარდა იმ შემთხვევისა, როდესაც პერსონალური მონაცემების (გარდა განსაკუთრებული კატეგორიის პერსონალური მონაცემისა) დამუშავების მიზნიდან გამომდინარე, მათი წაშლის/განადგურების შედეგად, მონაცემთა სუბიექტს მნიშვნელოვანი ზიანი არ ადგება;
- განსაკუთრებული კატეგორიის მონაცემების უკანონო გამჟღავნება;
- ფიზიკური ზიანი, მათ შორის, სამედიცინო მომსახურების მიღების შეზღუდვა, თუ აღნიშნული იწვევს სამედიცინო მანიპულაციის ან ოპერაციის გადადებას, რაც პაციენტის მკურნალობაზე ახდენს უარყოფით გავლენას;
- არასრულწლოვნების, შეზღუდული შესაძლებლობების მქონე პირებისა და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე მონაცემთა სუბიექტ(ებ)ის პერსონალური მონაცემების უკანონო დამუშავება.

როგორც აღინიშნა, ზემოთ მოცემული ჩამონათვალი არ არის ამომწურავი. შესაბამისად, კონკრეტული ფაქტობრივი გარემოებების გათვალისწინებით, ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვან ზიანად ინციდენტით გამოწვეული სხვა სახის შედეგებიც შეიძლება იქნეს მიჩნეული.

3.2.3. შედეგის დადგომის ალბათობა

ინციდენტით მონაცემთა სუბიექტების უფლებებისადმი გამოწვეული შესაძლო შედეგის სიმძიმის შეფასების შემდეგ საჭიროა ამ შედეგის დადგომის ალბათობის განსაზღვრა. ამა თუ იმ შესაძლო შედეგის დადგომის ალბათობა შეიძლება იყოს, დაბალი, საშუალო ან მაღალი.

ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებების შელახვის ალბათობა:

- **დაბალია,** თუ ნაკლებსავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს;
- **საშუალოა,** თუ ინციდენტის შედეგად ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნისა და ასეთი ზიანის/საფრთხის არარსებობის ალბათობა მეტნაკლებად თანაბარია. აღნიშნული მოიცავს შემთხვევას, როდესაც დამუშავებისთვის პასუხისმგებელი პირის მხრიდან შეუძლებელია ინციდენტის შედეგად ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის მაღალი ან დაბალი ალბათობის მტკიცება.
- **მაღალია,** თუ ინციდენტი დიდი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

3.3. პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინება

3.3.1. შეტყობინების ვალდებულება

ინციდენტი პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულებას ექვემდებარება, თუ მისი შეფასების შედეგად იკვეთება, რომ:

- არსებობს გარკვეული ალბათობა, რომ ინციდენტი გამოიწვევეს იმგვარ შედეგს, რომელიც, ზემოაღნიშნული კრიტერიუმების შესაბამისად, ადამიანის ძირითად უფლებებისა და თავისუფლებებისადმი მნიშვნელოვანი ზიანის გამომწვევად/მნიშვნელოვანი საფრთხის შემცველად მოიაზრება;
- აღნიშნული ალბათობა არის საშუალო ან მაღალი, ან ასეთი შედეგი უკვე დამდგარია.

თუ ინციდენტის შედეგად ადამიანის ძირითადი უფლებებისა და თავისუფლებებისადმი მნიშვნელოვანი ზიანის გამოწვევის/მნიშვნელოვანი საფრთხის შექმნის ალბათობა დაბალია (ამგვარი შედეგი ნაკლებსავარაუდოა), ინციდენტის პერსონალურ მონაცემთა დაცვის

სამსახურისთვის შეტყობინება სავალდებულო არ არის, თუმცა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია აღრიცხოს ინციდენტი „პერსონალურ მონაცემთა დაცვის შეახებ“ საქართველოს კანონის 28-ე მუხლის შესაბამისად.

დაბალი ალბათობის მტკიცების ტვირთი დამუშავებისთვის პასუხისმგებელ პირს ეკისრება.

3.3.2. შეტყობინების ვადა

დამუშავებისთვის პასუხისმგებელმა პირმა პერსონალურ მონაცემთა დაცვის სამსახურს ინციდენტის შესახებ შეტყობინება მისი აღმოჩენიდან არაუგვიანეს 72 საათის ვადაში უნდა მიაწოდოს. მიუხედავად აღნიშნული ზღვრული ვადის არსებობისა, დამუშავებისთვის პასუხისმგებელი პირი არ უნდა დაელოდოს მის ამოწურვას და თითოეულ შემთხვევაში, შეტყობინება უნდა განახორციელოს ინციდენტის აღმოჩენიდან შეძლებისდაგვარად უმოკლეს დროში, გაუმართლებელი დაყოვნების გარეშე. თითოეული შეტყობინების დროულობის შეფასებისას მხედველობაში უნდა იქნეს მიღებული ინციდენტის ხასიათი, მასშტაბი და მონაცემთა სუბიექტების უფლებებისადმი მოსალოდნელი შედეგების სიმძიმე.

ზოგიერთ შემთხვევაში, ინციდენტის კომპლექსურობის, მიმდინარე ხასიათის, ან/და სხვა ობიექტური გარემოების გათვალისწინებით, მისი სრულყოფილად შეფასება აღმოჩენიდან 72 საათის ვადაში, შესაძლოა, ვერ მოხერხდეს. ასეთ დროს, თუ დამუშავებისთვის პასუხისმგებელი პირის ხელთ არსებული ინფორმაციის საფუძველზე უკვე იკვეთება გონივრული ეჭვის საფუძველი, რომ საშუალო ან მაღალი ალბათობით ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, დამუშავებისთვის პასუხისმგებელი პირი არ უნდა დაელოდოს შეფასების დასრულებას, შეტყობინებით უნდა მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს და წარუდგინოს მას იმ დროისთვის არსებული ინფორმაცია. ამგვარ შემთხევაში, ინციდენტთან დაკავშირებული ინფორმაციის პერსონალურ მონაცემთა დაცვის სამსახურისთვის წარდგენა შესაძლებელია განხორციელდეს ეტაპობრივად, გონივრულ ვადებში, გაუმართლებელი დაყოვნების გარეშე.

3.3.3. შეტყობინების ფორმა და წესი

პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინება შეიძლება განხორციელდეს როგორც წერილობით, ისე ელექტრონულად, სამსახურის მიერ სპეციალურად ამ მიზნით შექმნილი ინციდენტის შეტყობინებების მართვის ელექტრონული სისტემის მეშვეობით. გასათვალისწინებელია, რომ თუ ინციდენტი სახელმწიფო საიდუმლოების შემცველ ინფორმაციას შეეხება, პერსონალურ მონაცემთა დაცვის სამსახურისთვის მის შესახებ შეტყობინება საქართველოს კანონმდებლობით დადგენილი წესით უნდა მოხდეს.

შეტყობინების ფორმის შევსება და მისი წარდგენა უნდა განახორციელოს პერსონალურ მონაცემთა დაცვის ოფიცერმა, ხოლო მისი არყოფნის შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირის მიერ განსაზღვრულმა სხვა პირმა.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 29-ე მუხლის მე-3 პუნქტის თანახმად, ინციდენტის შესახებ შეტყობინება შემდეგ ინფორმაციას უნდა მოიცავდეს:

- ინციდენტის გარემოებები, სახე და დრო;
- ინციდენტის შედეგად უნებართვოდ გამჟღავნებული, დაზიანებული, წაშლილი, განადგურებული, მოპოვებული, დაკარგული, შეცვლილი მონაცემების სავარაუდო კატეგორიები და რაოდენობა, აგრეთვე, იმ მონაცემთა სუბიექტების სავარაუდო კატეგორიები და რაოდენობა, რომლებსაც ინციდენტის შედეგად შეექმნათ საფრთხე;
- ინციდენტით გამოწვეული სავარაუდო ზიანი, მისი შემცირების ან აღმოფხვრის მიზნით დამუშავებისთვის პასუხისმგებელი პირის მიერ განხორციელებული ან დაგეგმილი ღონისძიებები;
- გეგმავს თუ არა დამუშავებისთვის პასუხისმგებელი პირი, ინციდენტის შესახებ შეატყობინოს მონაცემთა სუბიექტ(ებ)ს, კანონის 30-ე მუხლით დადგენილი წესით და რა ვადაში;
- პერსონალურ მონაცემთა დაცვის ოფიცრის ან სხვა საკონტაქტო პირის მონაცემები.

ინციდენტის შეტყობინების ფორმის შინაარსს და მასში მისათითებელი ინფორმაციის დეტალურ ჩამონათვალს კი პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტი განსაზღვრავს, რომლის თანახმად, სამსახურისთვის წარსადგენი ინციდენტის შეტყობინების ფორმა მოიცავს როგორც სავალდებულოდ შესავსებ, ისე არასავალდებულო ველებს. კერძოდ, შეტყობინების ფორმაში მიეთითება:

- დამუშავებისთვის პასუხისმგებელი პირის სახელწოდება, სამართლებრივი ფორმა, საიდენტიფიკაციო ნომერი და მისამართი;
- დამუშავებისთვის პასუხისმგებელი პირის საქმიანობის სფერო (საჯარო სექტორი, სამართალდამცავი ორგანო ან კერძო სექტორი);
- ინციდენტის შეტყობინების ფორმის შევსებაზე პასუხისმგებელი პირის სახელი, გვარი, პოზიცია/თანამდებობა და საკონტაქტო მონაცემები (ტელეფონის ნომერი და ელექტრონული ფოსტის მისამართი);
- არსებობის შემთხვევაში, პერსონალურ მონაცემთა დაცვის ოფიცრის სახელი, გვარი და საკონტაქტო მონაცემები (ტელეფონის ნომერი და ელექტრონული ფოსტის მისამართი);
- არსებობის შემთხვევაში, სხვა საკონტაქტო პირის სახელი, გვარი, პოზიცია/თანამდებობა და საკონტაქტო მონაცემები (ტელეფონის ნომერი და ელექტრონული ფოსტის მისამართი);
- ხორციელდება ინციდენტის პირველადი შეტყობინება, თუ დამატებითი ან განახლებული ინფორმაციის წარდგენა;
- დამატებითი ან განახლებული ინფორმაციის წარდგენის შემთხვევაში, პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ინციდენტისთვის მინიჭებული საიდენტიფიკაციო ნომერი;
- ინციდენტის სტატუსი (მიმდინარეა თუ დასრულებული);
- ინციდენტის დაწყების დრო (თუ იგი ცნობილია) და დასრულების დრო (თუ ინციდენტი დასრულებულია);
- დამუშავებისთვის პასუხისმგებელი პირის მიერ ინციდენტის გამოვლენის დრო;

- ინციდენტის გამოვლენის წყარო (მონაცემთა სუბიექტის შეტყობინება, მესამე პირის შეტყობინება, სისტემის აუდიტი, სისტემის ტესტირება, დამუშავებაზე უფლებამოსილი პირის შეტყობინება, დასაქმებულის შეტყობინება და სხვა);
- იმ შემთხვევაში, თუ შეტყობინებით ინციდენტის შესახებ ინფორმაციის სამსახურისთვის სრულად მიწოდება ვერ ხორციელდება, განმარტება აღნიშნულის მიზეზის შესახებ;
- ინციდენტის სახე (კონფიდენციალურობის დარღვევა; მთლიანობის დარღვევა; ხელმისაწვდომობის დარღვევა);
- ინციდენტის შედეგები (მონაცემების შემთხვევით ან განზრახ განადგურება; მონაცემების შემთხვევით ან განზრახ შეცვლა; დაშიფრული მოწყობილობის მოპარვა ან დაკარგვა; დაუშიფრავი მოწყობილობის მოპარვა ან დაკარგვა; მატერიალური დოკუმენტის მოპარვა, დაკარგვა ან მასზე უნებართვო წვდომა; ელექტრონული ფორმით არსებულ მონაცემებზე უნებართვო წვდომა; ელექტრონული ან/და მატერიალური ფორმით არსებულ მონაცემებზე წვდომის შესაძლებლობის შეზღუდვა; ვიდეო ან/და აუდიო მონიტორინგის სისტემის მეშვეობით დამუშავებულ მონაცემებზე უნებართვო წვდომა/მათი უკანონო გამჟღავნება; ელექტრონული ფოსტით განხორციელებულ მიმოწერაზე უნებართვო წვდომა/მისი უკანონო გამჟღავნება; ონლაინ პორტალზე არსებულ მომხმარებლის ანგარიშზე უნებართვო წვდომა/მასში არსებული მონაცემების უკანონო გამჟღავნება; სოციალური მედიის ან/და მოკლე ტექსტური შეტყობინებების მიმოცვლის პლატფორმაზე არსებულ მომხმარებლის ანგარიშზე უკანონო წვდომა/მასში არსებული მონაცემების უკანონო გამჟღავნება; საფოსტო კორესპონდენციაზე უკანონო წვდომა/მასში არსებული მონაცემების უკანონო გამჟღავნება; ელექტრონულ მოწყობილობაში შენახულ მონაცემებზე უკანონო წვდომა; მონაცემების ზეპირსიტყვიერად გამჟღავნება; ელექტრონულ სისტემაში უნებართვო შეჭრა/შეღწევა (**ჰაკერული თავდასხმა *(მაგ.: credential stuffing, malware, DDoS, ransomware, სხვა)); მონაცემებზე წვდომის მოპოვება მოტყუების ან შეცდომაში შეყვანის გზით (phishing, spear phishing, smishing, vishing)***; მონაცემების შემთხვევით ან განზრახ გასაჯაროება; დამუშავებისას დაშვებული შეცდომა; სისტემის ტექნიკური გამართულობის უზრუნველსაყოფად საჭირო სამუშაოები ***(ე.წ. „მეინთენენსი“)*** და სხვა);
- ინციდენტის გამომწვევი სავარაუდო მიზეზი, თუ იგი ცნობილია (დასაქმებული პირის/ყოფილი დასაქმებულის შეცდომა ან გაუფრთხილებლობა; დასაქმებული პირის/ყოფილი დასაქმებულის განზრახი ქმედება; დამუშავებისთვის უფლებამოსილი პირის შეცდომა ან გაუფრთხილებლობა; დამუშავებისთვის უფლებამოსილი პირის განზრახი ქმედება; მესამე პირის შეცდომა ან გაუფრთხილებლობა; მესამე პირის განზრახი ქმედება და სხვა);
- იმ მონაცემების ტიპი, რომლებზეც ინციდენტი გავლენას ახდენს (სახელი, გვარი, დაბადების თარიღი; პირადი ან/და პასპორტის ნომერი; საკონტაქტო მონაცემები; საიდენტიფიკაციო ან წვდომის ინფორმაცია (მომხმარებლის სახელი, პაროლი); სოციალური მედიის გვერდი (ე.წ. პროფილი); ეკონომიკური და ფინანსური მონაცემები; ოფიციალური დოკუმენტები ან მათი ასლები; ადგილმდებარეობის მონაცემები ***(მაგ.: გეოლოკაციის შესახებ ინფორმაცია)***; პერსონალური მონაცემების შემცველი ფოტო, ვიდეო ან აუდიო მასალა; პირად საქმიანობასთან ან ოჯახურ ცხოვრებასთან დაკავშირებული ინფორმაცია; პროფესიულ საქმიანობასთან დაკავშირებული ინფორმაცია; პირის მიერ

განხორციელებული კომუნიკაციის ამსახველი მონაცემები; განსაკუთრებული კატეგორიის მონაცემები და სხვა);

- იმ მონაცემთა სუბიექტების სავარაუდო ან ზუსტი რაოდენობა, რომლებზეც ინციდენტი გავლენას ახდენს;
- არიან თუ არა ინციდენტის შედეგად დაზარალებული მონაცემთა სუბიექტები არასრულწლოვნები, შეზღუდული შესაძლებლობების მქონე პირები ან/და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე პირები.
- ინციდენტის ზოგადი აღწერა;
- ალბათობა იმისა, რომ ინციდენტი გამოიწვევს ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვან ზიანს/მნიშვნელოვან საფრთხეს (საშუალო/მაღალი);
- ინფორმაცია მონაცემთა უსაფრთხოების დამცავი და ინციდენტის ხელშემშლელი იმ ტექნიკური ან/და ორგანიზაციული ზომების შესახებ, რომლებიც ინციდენტის დროს უკვე იყო გატარებული;
- ინფორმაცია მონაცემთა უსაფრთხოების და ინციდენტის შედეგად მოსალოდნელი ზიანის შემცირების უშუალოდ ხელშემწყობი იმ ტექნიკური ან/და ორგანიზაციული ზომების შესახებ, რომლებიც ინციდენტის მოხდენის შემდეგ გატარდა;
- ინფორმაცია მონაცემთა უსაფრთხოების და ინციდენტის შედეგად მოსალოდნელი ზიანის შემცირების უშუალოდ ხელშემწყობი იმ ტექნიკური ან/და ორგანიზაციული ზომების შესახებ, რომელთა გატარებაც სამომავლოდ იგეგმება;
- განხორციელდა თუ არა, როდის და რა ფორმით, ინციდენტის შესახებ მონაცემთა სუბიექტ(ებ)ის ინფორმირება;
- იმ შემთხვევაში, თუ მონაცემთა სუბიექტ(ებ)ის ინფორმირება არ განხორციელებულა, იგეგმება თუ არა, როდის და რა ფორმით;
- მიეცათ/მიეცემათ თუ არა მონაცემთა სუბიექტ(ებ)ს რაიმე მითითება/რეკომენდაცია ინციდენტის შედეგად მოსალოდნელი ზიანის თავიდან ასაცილებლად;
- შეუქმნის თუ არა ინციდენტის შესახებ ინფორმაციის გასაჯაროება საფრთხეს: სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოების და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესებს; საზოგადოებრივი უსაფრთხოების ინტერესებს; დანაშაულის თავიდან აცილებას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას, მართლმსაჯულების განხორციელებას, პატიმრობისა და თავისუფლების აღკვეთის აღსრულებას, არასაპატიმრო სასჯელთა აღსრულებას და პრობაციას, ოპერატიულ-სამძებრო საქმიანობას; ქვეყნისთვის მნიშვნელოვან ფინანსურ ან ეკონომიკურ (მათ შორის, მონეტარულ, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესებს;
- კანონის 29-ე მუხლის მე-11 პუნქტით გათვალისწინებულ შემთხვევაში, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების სფეროში შესაბამის კომპეტენტურ უწყებასთან შეთანხმების თაობაზე ინფორმაცია;
- საჭიროების შემთხვევაში, სხვა დამატებითი ინფორმაცია.

3.4. მონაცემთა სუბიექტ(ებ)ის ინფორმირება

3.4.1. ინფორმირების ვალდებულება

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტს აცნობოს ინციდენტის შესახებ, თუ ინციდენტის შეფასების შედეგად იკვეთება, რომ:

- არსებობს გარკვეული ალბათობა, რომ ინციდენტი გამოიწვევეს იმგვარ შედეგს, რომელიც, ზემოაღნიშნული კრიტერიუმების შესაბამისად, ადამიანის ძირითად უფლებებისა და თავისუფლებებისადმი მნიშვნელოვანი ზიანის გამომწვევად/მნიშვნელოვანი საფრთხის შემცველად მოიაზრება;
- აღნიშნული ალბათობა არის მაღალი, ან ასეთი შედეგი უკვე დამდგარია.

არ არსებობს ისეთი ინციდენტების შესახებ მონაცემთა სუბიექტების ინფორმირების ვალდებულება, რომლებიც პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინებას არ ექვემდებარებიან.

3.4.2. ინფორმირების ვადა და წესი

დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს ინციდენტის შესახებ უნდა აცნობოს მისი აღმოჩენიდან პირველი შესაძლებლობისთანავე, გაუმართლებელი დაყოვნების გარეშე. ინციდენტის შესახებ ინფორმირებისას მონაცემთა სუბიექტებს უნდა მიეწოდოთ 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.

ინციდენტის შესახებ ინფორმირებისას, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტებს ნებისმიერი ინფორმაცია უნდა მიაწოდოს მარტივ, გასაგებ ენაზე. მთავარი მიზანი უნდა იყოს მონაცემთა სუბიექტებისთვის ისეთი ინფორმაციის მიწოდება, რომელიც მათ დაეხმარება საკუთარ უფლებათა დაცვის რეალიზაციასა და მოსალოდნელი უარყოფითი შედეგების თავიდან აცილებაში.

ინციდენტის შესახებ თითოეულ მონაცემთა სუბიექტს უნდა ეცნობოს უშუალოდ. ***მაგალითისთვის, აღნიშნული შეიძლება განხორციელდეს ინდივიდუალური საფოსტო გზავნილების, ელექტრონული ფოსტის ან მოკლე ტექსტური შეტყობინებების გაგზავნით.*** თუ თითოეული მონაცემთა სუბიექტის ინდივიდუალურად ინფორმირება არაპროპორციულად დიდ ხარჯებს ან ძალისხმევას მოითხოვს, ინფორმირება შეიძლება განხორციელდეს ინფორმაციის საჯაროდ გავრცელებით, ან სხვა ისეთი ფორმით, რომელიც მონაცემთა სუბიექტის მიერ ინფორმაციის მიღების შესაძლებლობას ჯეროვნად უზრუნველყოფს. დამუშავებისთვის პასუხისმგებელმა პირმა შეტყობინების გასავრცელებლად ისეთი არხი

უნდა შეარჩიოს, რომ ინფორმაცია ინციდენტის შედეგად დაზარალებული რაც შეიძლება მეტი მონაცემთა სუბიექტისთვის გახდეს ხელმისაწვდომი.

იმისთვის, რომ ინციდენტის შესახებ მონაცემთა სუბიექტებისთვის მიწოდებული შეტყობინება სათანადოდ აღქმადი იყოს, იგი მხოლოდ ამ საკითხს უნდა ეთმობოდეს. ინციდენტის შესახებ ინფორმაცია მონაცემთა სუბიექტს არ უნდა გაეგზავნოს რაიმე სხვა შინაარსის შემცველ ინფორმაციასთან ერთად.

3.4.3. ინფორმირების ვალდებულების გამომრიცხავი გარემოებები

ინციდენტის შესახებ მონაცემთა სუბიექტები ინფორმირების ვალდებულება არ წარმოიშობა, თუ ეს საფრთხეს შეუქმნის:

- სახელმწიფო საიდუმლოების დაცვის ინტერესებს;
- სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესებს;
- საზოგადოებრივი უსაფრთხოების ინტერესებს;
- დანაშაულის თავიდან აცილებას, ოპერატიულ-სამძებრო საქმიანობას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას;
- მართლმსაჯულების განხორციელებას;
- პატიმრობისა და თავისუფლების აღკვეთის აღსრულებას, არასაპატიმრო სასჯელთა აღსრულებას და პრობაციას;
- ქვეყნისთვის მნიშვნელოვან ფინანსურ ან ეკონომიკურ (მათ შორის, მონეტარულ, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესებს.

მონაცემთა სუბიექტების ინფორმირების ვალდებულება ასევე არ წარმოიშობა იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელმა პირმა მიიღო შესაბამისი უსაფრთხოების ზომები, რის შედეგადაც თავიდან იქნა აცილებული ადამიანის ძირითადი უფლებებისა და თავისუფლებების დარღვევის მნიშვნელოვანი საფრთხე.

რომელიმე ზემოაღნიშნული გარემოების არსებობის საფუძვლით მონაცემთა სუბიექტებისთვის ინფორმაციის მიუწოდებლობის შემთხვევაში, შესაბამისი გარემოების არსებობის მტკიცების ტვირთი დამუშავებისთვის პასუხისმგებელ პირს ეკისრება.

3.5. ზიანის შემცირება/აღმოფხვრა

პერსონალურ მონაცემთა დაცვის სამსახურისთვის და მონაცემთა სუბიექტებისთვის ინფორმაციის შესაბამის ვადებსა და ფორმით მიწოდებასთან ერთად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ინციდენტის აღმოჩენისთანავე დააიდენტიფიციროს მისგან მომდინარე შესაძლო ზიანის თავიდან აცილების ან/და შემცირების თვალსაზრისით სხვა ეფექტური ღონისძიებები და მყისიერად დაიწყოს მათი გატარება. ამ თვალსაზრისით, მიზანშეწონილია, რომ დამუშავებისთვის პასუხისმგებელ/დამუშავებაზე უფლებამოსილ

პირებს გაწერილი ჰქონდეთ პროცედურა, რომელიც განსაზღვრავს დარღვევის აღმოჩენის შემდგომ გასატარებელი ზოგადი ღონისძიებების პროცესს, მათ შორის, როგორ მართონ და აღმოფხვრან ამა თუ იმ სახის დარღვევა, რა კრიტერიუმებით შეაფასონ რისკები და გადასცენ შეტყობინება. ასევე მიზანშეწონილია, რომ დამუშავებისთვის პასუხისმგებელი/დამუშავებაზე უფლებამოსილი პირების თანამშრომლები ზედმიწევნით იყვნენ ინფორმირებულნი ასეთი პროცედურების, მექანიზმების არსებობისა და გასატარებელ ღონისძიებათა თანმიმდევრობისა და განხორციელების აუცილებლობის შესახებ.

3.6. დამუშავებაზე უფლებამოსილი პირის როლი

როგორც აღინიშნა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 29-ე მუხლის თანახმად, ინციდენტის შესახებ შეტყობინების პერსონალურ მონაცემთა დაცვის სამსახურისთვის წარდგენის ვალდებულება მხოლოდ დამუშავებისთვის პასუხისმგებელ პირს ეკისრება. თავის მხრივ, დამუშავებაზე უფლებამოსილი პირი ვალდებულია, ინციდენტის შესახებ დაუყოვნებლივ აცნობოს დამუშავებისთვის პასუხისმგებელ პირს. ამასთან, ამავე კანონის 36-ე მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს შორის დადებული წერილობითი შეთანხმება, სხვა სავალდებულო პირობებთან ერთად, უნდა ითვალისწინებდეს დამუშავებაზე უფლებამოსილი პირის ვალდებულებას, კანონით დადგენილ ვალდებულებებთან შესაბამისობის უზრუნველსაყოფად დამუშავებისთვის პასუხისმგებელ პირს მიაწოდოს სათანადო ინფორმაცია და ხელი შეუწყოს მის მიერ მონაცემთა დამუშავების მონიტორინგის განხორციელებას. ამდენად, ინციდენტის შესახებ ინფორმაციის საზედამხედველო ორგანოსთვის მიწოდება დამუშავებისთვის პასუხისმგებელმა პირმა უნდა განახორციელოს, თუმცა მის მიერ აღნიშნული ვალდებულების ჯეროვნად შესრულებისთვის აუცილებელია დამუშავებაზე უფლებამოსილი პირის სათანადო ჩართულობა.

აღსანიშნავია, რომ დამუშავებაზე უფლებამოსილი პირი არ არის ვალდებული, დამუშავებისთვის პასუხისმგებელი პირის ინფორმირებამდე შეაფასოს ინციდენტის შესაძლო შედეგები და განსაზღვროს შესაძლო უარყოფითი შედეგების პრევენციისთვის გასატარებელი ღონისძიებები. მისი ვალდებულებაა, დამუშავებისთვის პასუხისმგებელ პირს ინციდენტის შესახებ დაუყოვნებლივ აცნობოს. აღნიშნულის განხორციელება კი დამუშავებაზე უფლებამოსილი პირის მიერ ინციდენტის აღმოჩენის მომენტიდანვე არის შესაძლებელი. რაც შეეხება ინციდენტის შედეგად მონაცემთა სუბიექტების უფლებებისადმი წარმოშობილი რისკების შეფასებას და იმის განსაზღვრას, ექვემდებარება თუ არა ინციდენტი პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინებას, აღნიშნული დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებაა.

3.7. თანადამუშავებისთვის პასუხისმგებელი პირები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 35-ე მუხლის პირველი პუნქტის თანახმად, თუ მონაცემთა დამუშავებაში ჩართული არიან თანადამუშავებისთვის პასუხისმგებელი პირები, ისინი ვალდებულნი არიან წინასწარ, წერილობით განსაზღვრონ კანონის მოთხოვნების შესრულებასთან დაკავშირებით, თითოეულის ვალდებულებები და პასუხისმგებლობა. შესაბამისად, ინციდენტის აღრიცხვისა და შეტყობინების, როგორც კანონით გათვალისწინებული მოთხოვნის მიმართ თითოეული თანადამმუშავებლის ვალდებულებების და პასუხისმგებლობების წინასწარ, წერილობით განსაზღვრა თავად მათ ევალებათ.

4. პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ინციდენტის შესახებ ინფორმაციის გამოქვეყნება

დამუშავებისთვის პასუხისმგებელი პირისგან ინციდენტის შესახებ შეტყობინების მიღების შემდეგ პერსონალურ მონაცემთა დაცვის სამსახური შეისწავლის მიღებულ ინფორმაციას და განსაზღვრავს შემდგომი ღონისძიებების გატარების მიზანშეწონილობას.

თუ პერსონალურ მონაცემთა დაცვის სამსახურისთვის წარდგენილი შეტყობინების თანახმად, დამუშავებისთვის პასუხისმგებელი პირი არ ან ვერ უზრუნველყოფს ინციდენტის თაობაზე მონაცემთა სუბიექტ(ებ)ის ინფორმირებას, ინციდენტის გარემოებების, სავარაუდო ზიანის ან/და მონაცემთა სუბიექტების რაოდენობის გათვალისწინებით, პერსონალურ მონაცემთა დაცვის სამსახური უფლებამოსილია, მიიღოს გადაწყვეტილება ინციდენტის შესახებ მის ხელთ არსებული ინფორმაციის გასაჯაროების თაობაზე. პერსონალურ მონაცემთა დაცვის სამსახური ინციდენტის შესახებ ინფორმაციას არ გაასაჯაროებს, თუ ეს საფრთხეს შეუქმნის:

- სახელმწიფო საიდუმლოების დაცვის ინტერესებს;
- სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესებს;
- საზოგადოებრივი უსაფრთხოების ინტერესებს;
- დანაშაულის თავიდან აცილებას, ოპერატიულ-სამძებრო საქმიანობას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას;
- მართლმსაჯულების განხორციელებას;
- პატიმრობისა და თავისუფლების აღკვეთის აღსრულებას, არასაპატიმრო სასჯელთა აღსრულებას და პრობაციას;
- ქვეყნისთვის მნიშვნელოვან ფინანსურ ან ეკონომიკურ (მათ შორის, მონეტარულ, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესებს.

ინციდენტის შესახებ ინფორმაცია ასევე არ გასაჯაროვდება მაშინ, თუ პერსონალურ მონაცემთა დაცვის სამსახურში ინციდენტის შესახებ წარმოდგენილ შეტყობინებას თან ახლავს მონაცემთა დამუშავებისთვის პასუხისმგებელი საჯარო ან კერძო დაწესებულების მითითება, რომ ინფორმაციის გასაჯაროება საფრთხეს შეუქმნის:

- სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოების და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესებს;
- საზოგადოებრივი უსაფრთხოების ინტერესებს;
- დანაშაულის თავიდან აცილებას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას;
- მართლმსაჯულების განხორციელებას;
- პატიმრობისა და თავისუფლების აღკვეთის აღსრულებას, არასაპატიმრო სასჯელთა აღსრულებას და პრობაციას, ოპერატიულ-სამძებრო საქმიანობას;
- ქვეყნისთვის მნიშვნელოვან ფინანსურ ან ეკონომიკურ (მათ შორის, მონეტარულ, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესებს.

5. ინციდენტის შეუტყობინებლობის სამართლებრივი შედეგები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 78-ე და 79-ე მუხლების თანახმად, ინციდენტის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულების, ისევე, როგორც ინციდენტის შესახებ მონაცემთა სუბიექტისთვის შეტყობინების ვალდებულების არაჯეროვანი შესრულება, ადმინისტრაციულ სამართალდარღვევას წარმოადგენს. შესაბამისად, ამგვარი გარემოებების გამოვლენის შემთხვევაში, პერსონალურ მონაცემთა დაცვის სამსახური განახორციელებს ადმინისტრაციული სამართალდარღვევის საქმისწარმოებას და უზრუნველყოფს დამრღვევთათვის ზემოაღნიშნული მუხლებით გათვალისწინებული პასუხისმგებლობის დაკისრებას.

ნატო ვაჩნაძის ქუჩა N° 7, თბილისი

ბაქოს ქუჩა N° 48, ბათუმი

(+995 32) 242 1000

office@pdps.ge