ინციდენტზე რეაგირების პოლიტიკა

2024 წელი

1. სკოლის შესახებ

შპს „თბილისის ზოგადსაგანმანათლებლო სკოლა-ლიცეუმი მწიგნობართუხუცესი“ (შემდგომში - სკოლა):
საიდენტიფიკაციო ნომერი: 211360141;
იურიდიული მისამართი: საქართველო, თბილისი, ლეო კვაჭაძის ქუჩა #12
რეგისტრაციის თარიღი: 17 იანვარი, 1996 წელი.

2. ინციდენტზე რეაგირების პოლიტიკის მიზანი

შპს „თბილისის ზოგადსაგანმანათლებლო სკოლა-ლიცეუმი მწიგნობართუხუცესის“, როგორც პასუხისმგებლიანი დაწესებულებისთვის, მნიშვნელოვანია პერსონალურ მონაცემთა მაღალი ხარისხით დაცვა და უსაფრთხოების უზრუნველყოფა, ასევე მონაცემთა უსაფრთხოების დარღვევის ეფექტურად აღმოჩენა და სათანადო წესით რეაგირება.

წინამდებარე დოკუმენტის მიზანია განსაზღვროს რეაგირების წესი იმ მონაცემთა უსაფრთხოების დარღვევის შემთხვევებზე, რომელიც კვალიფიცირდება ინციდენტად და განსაზღვროს პასუხისმგებელი პირები აღნიშნულ პროცესში.

3. პირთა წრე, ვისზეც ვრცელდება ინციდენტზე რეაგირების პოლიტიკის დოკუმენტი

აღნიშნული პოლიტიკის დოკუმენტით განსაზღვრული წესი სრულად ვრცელდება სკოლაზე, დირექტორზე, მოადგილეებზე, სკოლაში დასაქმებულ ნებისმიერ პირზე და ყველა იმ მესამე პირზე, ვისაც რაიმე ფორმით შეიძლება ჰქონდეს შეხება იმ პერსონალურ მონაცემებთან, რომელსაც სკოლა ამუშავებს მისი საქმიანობის პროცესში.

4. ტერმინთა განმარტება

მონაცემთა განადგურება - შემთხვევა, როდესაც მონაცემები საერთოდ აღარ არსებობს, ან აღარ არსებობს რაიმე გამოყენებადი ფორმით.

მონაცემთა დაზიანება - შემთხვევა, როდესაც მონაცემები შეიცვალა, გახდა არაზუსტი ან არასრული.

მონაცემთა დაკარგვა - შემთხვევა, როდესაც მონაცემები შესაძლოა კვლავ არსებობდეს, თუმცა ისინი აღარ არის სკოლის მფლობელობაში, ან როდესაც მონაცემები კვლავ სკოლაში ინახება, მაგრამ სკოლას აღარ აქვს მათზე კონტროლი ან/და სათანადო წვდომა.

წინამდებარე პოლიტიკის დოკუმენტში გამოყენებულ სხვა ტერმინებს აქვთ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრული მნიშვნელობა.

5. სახელმძღვანელო ნორმატიული აქტები

ინციდენტის დადგომის შემთხვევაში, შესაბამისმა პირებმა უნდა იხელმძღვანელონ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონითა (შემდგომში **„კანონი“)** და პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის N19 ბრძანებით „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ“ (შემდგომში **„ბრძანება“)** .

წინამდებარე პოლიტიკის დოკუმენტი, თავის მხრივ, აწესრიგებს დამატებით შიდა პროცედურულ საკითხებს ინციდენტის დადგომის შემთხვევაში, კანონთან და კანონქვემდებარე ნორმატიულ აქტთან სკოლის საქმიანობის შესაბამისობის მიზნით.

6. ინციდენტის სახეები

- **კონფიდენციალურობის დარღვევა** – პერსონალური მონაცემების უნებართვო ან შემთხვევითი გამჟღავნება ან მათზე ამგვარი წვდომა.

- **მთლიანობის დარღვევა** – პერსონალური მონაცემების უნებართვო შეცვლა, აგრეთვე, არამართლზომიერი ან შემთხვევითი დაზიანება, დაკარგვა.

- **ხელმისაწვდომობის დარღვევა** – პერსონალურ მონაცემებზე წვდომის დაკარგვა, ან წვდომის უნებართვო შეზღუდვა ან დაზიანება, ასევე მონაცემების ამგვარი განადგურება ან წაშლა.

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

7. როგორ ხდება პერსონალურ მონაცემებთან დაკავშირებული ინციდენტები

ქვევით მოცემულია გავრცელებული შემთხვევები, რა დროსაც ადგილი აქვს პერსონალურ მონაცემებთან დაკავშირებულ ინციდენტს:

- ადამიანური შეცდომა;
- მატერიალური ფორმით არსებული დოკუმენტების დაკარგვა ან მოპარვა;
- იმ ტექნიკის დაკარგვა ან მოპარვა, სადაც შენახულია პერსონალური მონაცემები;
- კონფიდენციალური მონაცემების განზრახ ან უნებლიე გამჟღავნება არაუფლებამოსილი მესამე მხარისთვის;
- კონფიდენციალურ ინფორმაციაზე არაავტორიზებული/არაუფლებამოსილი წვდომა;
- კიბერშეტევასთან (Hacking) დაკავშირებული ინციდენტი;
- პერსონალური მონაცემების, მათ შორის, განსაკუთრებული კატეგორიის მონაცემების შემცველი ელექტრონული ფოსტის გაგზავნა სხვა ადრესატ(ებ)ისთვის/მესამე პირ(ებ)ისთვის;

- პერსონალური მონაცემების უყურადღებოდ დატოვება მარტივად ხელმისაწვდომ ადგილზე;
- შენობის დაყაჩაღება, გაქურდვა, დატბორვა, ხანძარი, ნგრევა და ა.შ.
- პერსონალური მონაცემების არასათანადო განკარგვა.

იმ ფაქტის გათვალისწინებით, რომ ადამიანური შეცდომა ინციდენტის გამომწვევი მნიშვნელოვანი მიზეზი შეიძლება იყოს, სკოლის თითოეული თანამშრომელი ვალდებულია პერსონალურ მონაცემებთან დაკავშირებით სათანადო სიფრთხილე გამოიჩინოს.

8. ინციდენტის აღმოჩენა

8.1. ინციდენტის აღმოჩენის წესი

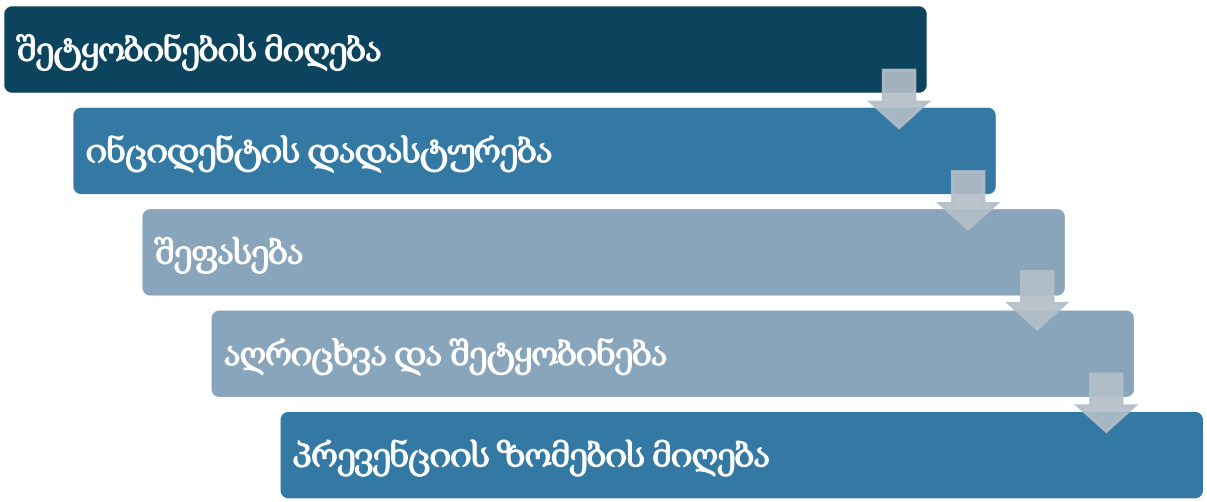
ელექტრონული ფორმით არსებულ პერსონალურ მონაცემებთან დაკავშირებული ინციდენტის აღმოჩენის მიზნით სკოლაში არსებული სისტემა დაფუძნებულია ლოგირების მეთოდზე. აღნიშნული გულისხმობს, რომ სისტემურად აღირიცხება მონაცემების მიმართ განხორციელებული ნებისმიერი მოქმედება და შესაძლებელია იმის იდენტიფიცირება, თუ ვინ, როდის და რა ქმედება განახორციელა კონკრეტული მონაცემის მიმართ.

სკოლა ასევე ახორციელებს მისი ელექტრონული სისტემის მუდმივ მონიტორინგს. სისტემა დაცულია ვირუსებისგან და სხვა საფრთხისგან. უსაფრთხოების სისტემა მუშაობს იმ ფორმით, რომ სისტემაში უნებართვო წვდომის შემთხვევაში IT სამსახური დაუყონებლივ იღებს შეტყობინებას მსგავსი შეღწევის შესახებ.

მატერიალური ფორმით არსებულ პერსონალურ მონაცემებთან დაკავშირებით, კი, სკოლაში მოქმედებს დაცვის ადეკვატური ზომები.

9. ინციდენტზე რეაგირების პროცესი და პასუხისმგებელი პირები.

ქვემოთ მოცემული ცხრილი, აღნიშნავს სკოლაში არსებულ პროცედურას ინციდენტის მართვასთან დაკავშირებით:



ეტაპი 1: შეტყობინების მიღება

ნებისმიერი პირი, ვისთვისაც ცნობილი გახდა ინციდენტის თაობაზე, ინციდენტის აღმოჩენისთანავე ან ასეთი ალბათობის შემთხვევაში, ინციდენტზე რეაგირების გუნდს უნდა აცნობოს. ასევე შეტყობინების ასლი (CC) გაუგზავნოს/მიაწოდოს პერსონალურ მონაცემთა დაცვის ოფიცერს ან/და დირექტორს და შეატყობინოს მის ხელთ არსებული შემდეგი ინფორმაცია:

1) ინციდენტის შესახებ ინფორმაციის წარმდგენი პირის ვინაობა და საკონტაქტო მონაცემები;
2) ინციდენტის აღწერა;
3) მონაცემთა კატეგორია, რომელსაც ეხება ინციდენტი;
4) მონაცემთა სავარაუდო ოდენობა, რომელსაც ეხება ინციდენტი;
5) ინციდენტის მდებარეობა;
6) ინციდენტის დრო და ადგილი;
7) სხვა დეტალები ინციდენტთან დაკავშირებით.

მნიშვნელოვანია, რომ ინციდენტის აღმომჩენმა პირმა ზემოაღნიშნული ინფორმაცია მიაწოდოს ინციდენტზე რეაგირების გუნდს მაშინვე, როდესაც მისთვის ცნობილი გახდება ინციდენტის შესახებ და არ დაელოდოს დამატებითი/კონკრეტული დეტალების მოძიებას/მოკვლევას ინციდენტთან დაკავშირებით.

იმ შემთხვევაში, თუ ინციდენტი აღმოჩენილია სკოლის IT სამსახურის/თანამშრომლის მიერ, შესაბამისი პირი ვალდებულია დაუყონებლივ განახორციელოს ქმედებები, რათა აღმოფხვრას სისტემური ხარვეზი და შეამციროს შესაძლო საფრთხე. აღნიშნული ქმედებები შესაძლოა მოიცავდეს:

- აპლიკაციების გათიშვას;
- ანგარიშების დახურვას;
- პაროლების შეცვლას;
- დაკარგული ინფორმაციის/დოკუმენტაციის მოძიებას;
- წვდომების შეზღუდვა/გაუქმებას და სხვა.

ეტაპი 2: ინციდენტის დადასტურება

ინციდენტთან დაკავშირებით შეტყობინების მიღებისთანავე ინციდენტზე რეაგირების გუნდი ახორციელებს სწრაფ მოკვლევას ინციდენტთან დაკავშირებით, მათ შორის, როდის მოხდა ინციდენტი და როდის მოხდა მისი აღმოჩენა, როგორ მოხდა, რომელ მონაცემებზე რა სახის გავლენა მოახდინა.

აღსანიშნავია, რომ ინციდენტზე რეაგირების გუნდი იქმნება დირექტორის ბრძანებით, რომელიც წარმოადგენს აღნიშნული პოლიტიკის დანართს.

ინციდენტზე რეაგირების გუნდი დაკომპლექტებულია ისეთი პირებისგან, ვისაც გააჩნია ინციდენტის შეფასების კომპეტენცია. გუნდის სავალდებულო წევრს წარმოადგენს პერსონალურ მონაცემთა დაცვის ოფიცერი.

ეტაპი 3: შეფასება

ინციდენტზე რეაგირების გუნდი ვალდებულია განახორციელოს ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობისა და სიმძიმის შეფასება.

აღნიშნული შეფასება უნდა განხორციელდეს ფაქტობრივი გარემოებების შეფასებით, ბრძანებით განსაზღვრული კრიტერიუმების შესაბამისად.

ეტაპი 4: აღრიცხვა და შეტყობინება

თუ ინციდენტზე რეაგირების გუნდი მიიჩნევს, რომ ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა საშუალო ან მაღალია, სკოლა ვალდებულია აღრიცხვოს იგი ინციდენტების რეესტრში და დაუყონებლივ, მაგრამ არაუგვიანეს ინციდენტის აღმოჩენიდან 72 საათისა, მის შესახებ შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს (შემდგომში - სამსახური) კანონისა და ბრძანებით განსაზღვრული წესის შესაბამისად.

სკოლა ინციდენტის შესახებ შეტყობინებას სამსახურს წარუდგენს ელექტრონული ან წერილობით ფორმით. ელექტრონული ფორმით შეტყობინებას სკოლა წარადგენს სამსახურის შეტყობინების მართვის ელექტრონული სისტემის საშუალებით. წერილობითი ფორმით შეტყობინება სამსახურს წარედგინება სკოლის მიერ დამტკიცებული ფორმის მიხედვით, რომელიც თან ერთვის წინამდებარე პოლიტიკის დოკუმენტს დანართი N1-ის სახით.

თუ ინციდენტზე რეაგირების გუნდი მიიჩნევს, რომ ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა მაღალია, სკოლა ასევე ვალდებულია პირველი შესაძლებლობისთანავე, გაუმართლებელი დაყოვნების გარეშე აცნობოს მონაცემთა სუბიექტს ინციდენტის შესახებ და მარტივ და გასაგებ ენაზე მიაწოდოს შემდეგი ინფორმაცია:

- ინციდენტისა და მასთან დაკავშირებული გარემოებების ზოგადი აღწერა;

- ინციდენტით გამოწვეული სავარაუდო/დამდგარი ზიანი, მის შესამცირებლად ან აღმოსაფხვრელად განხორციელებული ან დაგეგმილი ღონისძიებების შესახებ;
- პერსონალურ მონაცემთა დაცვის ოფიცრის ან სხვა პირის საკონტაქტო მონაცემები.

მონაცემთა სუბიექტის ინფორმირება უნდა განხორციელდეს ინდივიდუალურად თითოეული სუბიექტისათვის ელექტრონულ ფოსტაზე გაგზავნილი წერილობითი შეტყობინების გზით.

თუ მონაცემთა სუბიექტის ინფორმირება არაპროპორციულად დიდ ხარჯებს ან ძალისხმევას მოითხოვს (მაგალითად, თუ მონაცემთა სუბიექტების წრე ფართოა და ა.შ), სკოლა ინციდენტთან დაკავშირებულ ინფორმაციას გამოაქვეყნებს მის ვებსაიტზე საჯაროდ ხელმისაწვდომი ფორმით, ისე რომ ჯეროვნად იქნეს უზრუნველყოფილი მონაცემთა სუბიექტის მიერ ინფორმაციის მიღების შესაძლებლობა.

თუ ინციდენტზე რეაგირების გუნდი მიიჩნევს, რომ ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა დაბალია, ასეთი ინციდენტი ექვდემდებარება მხოლოდ ინციდენტების რეესტრში აღრიცხვას და სკოლას არ ეკისრება შეტყობინების ვალდებულება სამსახურისათვის ან/და მონაცემთა სუბიექტისათვის.

ეტაპი 5: პრევენციის ზომების მიღება

ზემოაღნიშნული ღონისძიებების გატარებისა და ინციდენტთან დაკავშირებით აუცილებელი ზომების მიღების შემდგომ, ინციდენტზე რეაგირების გუნდმა უნდა მოიკვლიოს და გაანალიზოს ის პროცესები/მიზეზები, რამაც ინციდენტი გამოიწვია.

აღნიშნული შესაძლოა გულისხმობდეს შემდეგ ქმედებებს:

- შიდა პოლიტიკის დოკუმენტების გადახედვა და ცვლილება;
- ახალი პოლიტიკის დოკუმენტების შემუშავება;
- თანამშრომელთა გადამზადება და ტრენინგი;
- სათანადო ხელშეკრულებებში ვალდებულებების განსაზღვრა;
- სისტემის ტექნიკური აუდიტი და ხარვეზების აღმოფხვრა;
- ანტივირუსული სისტემის განახლება და სხვა.

10. ინციდენტის რეესტრში აღრიცხვა

თითოეული ინციდენტი უნდა აღირიცხოს ინციდენტების რეესტრში, რომლის ფორმაც დამტკიცებულია სკოლის დირექტორის მიერ და ერთვის წინამდებარე პოლიტიკის დოკუმენტს დანართი N2-ის სახით.

დირექტორის ბრძანებით განისაზღვრება ინციდენტის რეესტრში აღრიცხვაზე პასუხისმგებელი პირი.

ინციდენტის რეესტრში აღირიცხება შემდეგი ინფორმაცია:

1. ინციდენტის აღწერა;
2. ინციდენტის დაწყებისა და დასრულების თარიღი;

3. პერსონალური მონაცემების კატეგორია, რომელზეც გავლენა მოახდინა ინციდენტმა;
4. პერსონალური მონაცემების ოდენობა, რომელზეც გავლენა მოახდინა ინციდენტმა;
5. ინციდენტის ხარისხი (მაღალი/საშუალო/დაბალი);
6. განხორციელდა თუ არა სამსახურისთვის შეტყობინება;
7. განხორციელდა თუ არა მონაცემთა სუბიექტების შეტყობინება.

ინციდენტის რეესტრში ინფორმაცია ინციდენტის შესახებ ინახება 1 წლის ვადით, რის შემდეგაც იგი ნადგურდება/იშლება პასუხისმგებელი პირის მიერ.

11. პერსონალურ მონაცემთა დაცვის ოფიცრის როლი

პერსონალურ მონაცემთა დაცვის ოფიცერი წარმოადგენს ინციდენტზე რეაგირების გუნდის წევრს, რომელიც აქტიურად არის ჩართული ინციდენტის მართვის პროცესში.

პერსონალურ მონაცემთა დაცვის ოფიცერი გასცემს რჩევებსა და რეკომენდაციებს, მონაწილეობს რისკების შეფასების პროცესში და მეთოდურ დახმარებას უწევს სკოლას.

12. პოლიტიკის დოკუმენტის ცვლილება

წინამდებარე დოკუმენტი პერიოდულად განახლებადია სკოლის მიერ. ცვლილებების შესახებ სათანადო პირებს ეცნობებათ ელექტრონული ფოსტის საშუალებით.

13. საკონტაქტო ინფორმაცია

პერსონალურ მონაცემთა დაცვის ოფიცერი - შპს „პიელსი ქონსალთინგი“ (საკონტაქტო ელექტრონული ფოსტა: info@plcconsulting.ge , საკონტაქტო ნომერი: 505 05 46 99).

თარიღი: 01 აგვისტო, 2024 წელი

ინციდენტზე რეაგირების პოლიტიკის

დანართი N1

ინციდენტის შეტყობინების ფორმა

1. დამუშავებისთვის პასუხისმგებელი პირის საიდენტიფიკაციო მონაცემები *

სახელმწოდება:

სამართლებრივი ფორმა:

საიდენტიფიკაციო ნომერი:

მისამართი:

2. დამუშავებისთვის პასუხისმგებელი პირის საქმიანობის სფერო *

☐ კერძო სექტორი
☐ საჯარო სექტორი
☐ სამართალდამცავი ორგანო

3. ინციდენტის შეტყობინების ფორმის შევსებაზე პასუხისმგებელი პირის მონაცემები *

სახელი:

გვარი:

პოზიცია/თანამდებობა:

ტელეფონის ნომერი:

ელექტრონული ფოსტის მისამართი:

4. არსებობის შემთხვევაში, ინფორმაცია პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ

სახელი:

გვარი:

ტელეფონის ნომერი:

ელექტრონული ფოსტის მისამართი:

5. არსებობის შემთხვევაში, სხვა საკონტაქტო პირის მონაცემები

სახელი:

გვარი:

პოზიცია/თანამდებობა:

ტელეფონის ნომერი:

ელექტრონული ფოსტის მისამართი:

6. ინციდენტის სტატუსი *

☐ მიმდინარე
☐ დასრულებული

☐ დაუდგენელია

7. ინციდენტის დაწყების დრო
(დღე/თვე/წელი)

8. ინდიცენტის დასრულების დრო
(დღე/თვე/წელი)

9. დამუშავებისთვის პასუხისმგებელი პირის მიერ ინციდენტის აღმოჩენის დრო
(დღე/თვე/წელი)

10. იმ შემთხვევაში, თუ შეტყობინებით ინციდენტის შესახებ ინფორმაციის სამსახურისთვის სრულად მიწოდება ვერ ხორციელდება, განმარტება აღნიშნულის მიზეზის თაობაზე

11. ინციდენტის სახე

☐ კონფიდენციალურობის დარღვევა
☐ ხელმისაწვდომობის დარღვევა
☐ მთლიანობის დარღვევა

12. 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

☐ ვიდეომონიტორინგის ან/და აუდიომონიტორინგის 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 მოკლეტექსტური 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

☐ მონაცემებზე წვდომის მოპოვება მოტყუების ან შეცდომაში შეყვანის გზით

☐ მონაცემების უკანონო გასაჯაროება

☐ დამუშავებისას დაშვებული შეცდომა

☐ სისტემის ტექნიკური გამართულობის უზრუნველსაყოფად საჭირო სამუშაოები

☐ სხვა (მიუთითეთ)

13. თუ ცნობილია ის მონაცემები, რომელზეც 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

☐ სხვა (მიუთითეთ)

14. თუ ცნობილია, იმ მონაცემთა სუბიექტების სავარაუდო ან ზუსტი რაოდენობა, რომლებზეც ინციდენტი გავლენას ახდენს

რაოდენობა -

15. უკავშირდება თუ არა ინციდენტის შედეგი არასრულწლოვანს, შეზღუდული შესაძლებლობების მქონე პირს ან/და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე პირს, თუ აღნიშნულის შესახებ ცნობილია

☐ დიახ
☐ არა

16. საშუალო ან მაღალი ალბათობა იმისა, რომ ინციდენტი გამოიწვევს ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვან ზიანს/მნიშვნელოვან საფრთხეს

☐ საშუალო
☐ მაღალი

17. ინფორმაცია მონაცემთა უსაფრთხოების და ინციდენტის შედეგად მოსალოდნელი ზიანის შემცირების უშუალოდ ხელშემწყობი იმ ტექნიკური ან/და ორგანიზაციული ზომების (მონაცემთა უსაფრთხოების უზრუნველმყოფი ტექნიკური, პროგრამული და ფიზიკური უსაფრთხოების გადაწყვეტები/მექანიზმები, ორგანიზაციული ფორმალიზებული პოლიტიკები და არაფორმალიზებული წესები) შესახებ, რომლებიც ინციდენტის შემდეგ გატარდა

18. ინფორმაცია მონაცემთა უსაფრთხოების და ინციდენტის შედეგად მოსალოდნელი ზიანის შემცირების უშუალოდ ხელშემწყობი იმ ტექნიკური ან/და ორგანიზაციული ზომების (მონაცემთა უსაფრთხოების უზრუნველმყოფი ტექნიკური, პროგრამული და ფიზიკური უსაფრთხოების გადაწყვეტები/მექანიზმები, ორგანიზაციული ფორმალიზებული პოლიტიკები და არაფორმალიზებული წესები) შესახებ, რომელთა გატარებაც სამომავლოდ იგეგმება

19. გეგმავს თუ არა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ინციდენტის შესახებ მონაცემთა სუბიექტ(ებ)ის ინფორმირებას, რა ვადაში და რა ფორმით

20. შეუქმნის თუ არა ინციდენტის შესახებ ინფორმაციის გასაჯაროება საფრთხეს (მონიშნეთ შესაბამისი საფრთხის არსებობის შემთხვევაში)

☐ 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

21. კანონის 29-ე მუხლის მე-11 პუნქტით გათვალისწინებულ შემთხვევაში, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების სფეროში შესაბამის კომპეტენტურ უწყებასთან შეთანხმების თაობაზე ინფორმაცია

ინციდენტზე რეაგირების პოლიტიკის
დანართი N2

ინციდენტის რეესტრი

(შაბლონური ფორმა)

1.	ინციდენტის აღწერა	
2.	ინციდენტის დაწყების თარიღი	
3.	ინციდენტის დასრულების თარიღი	
4.	პერსონალური მონაცემების კატეგორია, რომელზეც გავლენა მოახდინა ინციდენტმა	
5.	პერსონალური მონაცემების ოდენობა, რომელზეც გავლენა მოახდინა ინციდენტმა	
6.	ინციდენტის ხარისხი (მაღალი/საშუალო/დაბალი)	
7.	განხორციელდა თუ არა სამსახურისთვის შეტყობინება	
8.	განხორციელდა თუ არა მონაცემთა სუბიექტების ინფორმირება	