პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის

ბრძანება №19

2024 წლის 28 თებერვალი

ქ. თბილისი

ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 29-ე მუხლის მე-9 პუნქტის, 30-ე მუხლის მე-4 პუნქტისა და 88-ე მუხლის მე-4 პუნქტის „ა“ ქვეპუნქტის შესაბამისად, **ვბრძანებ:**

მუხლი 1

დამტკიცდეს ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმები და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების თანდართული წესი.

მუხლი 2

ეს ბრძანება ამოქმედდეს 2024 წლის 1 მარტიდან.

პერსონალურ მონაცემთა დაცვის
სამსახურის უფროსი **ლელა ჯანაშვილი**

ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმები და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესი

თავი I. ზოგადი დებულებები

მუხლი 1. მიზანი და რეგულირების სფერო

1. ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის (შემდგომ –– წესი) მიზანია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (შემდგომ – კანონი) 29-ე მუხლის პირველი პუნქტითა და 30-ე მუხლის მე-4 პუნქტით განსაზღვრული, ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის (შემდგომ – ინციდენტი) განსაზღვრის კრიტერიუმების დადგენა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის (შემდგომ – სამსახური) ინციდენტის შეტყობინების პროცედურების განსაზღვრა.

2. ეს წესი არ ვრცელდება კანონის მე-2 მუხლის მე-2 პუნქტის „ბ“ ქვეპუნქტით განსაზღვრული საქმიანობების მიზნებისთვის მონაცემთა დამუშავებასთან დაკავშირებულ ინციდენტებზე.

მუხლი 2. ტერმინთა განმარტება

ამ წესში გამოყენებულ ტერმინებს აქვთ კანონით განსაზღვრული მნიშვნელობა.

თავი II. ინციდენტის განსაზღვრის კრიტერიუმები

მუხლი 3. ინციდენტის ცნება და სახეები

1. ამ წესის მიზნებისთვის, ინციდენტი არის პერსონალურ მონაცემთა უსაფრთხოების დარღვევა (მათ შორის, ორგანიზაციული, ფიზიკური ან ტექნიკური), რომელიც იწვევს პერსონალური მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე, უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, წვდომას, შეგროვებას/მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას.

2. ინციდენტის სახეებია:

ა) კონფიდენციალურობის დარღვევა – პერსონალური მონაცემების უნებართვო გამჟღავნება ან წვდომა;

ბ) მთლიანობის დარღვევა – პერსონალური მონაცემების უნებართვო შეცვლა, აგრეთვე, არამართლზომიერი ან შემთხვევითი დაზიანება, დაკარგვა;

გ) ხელმისაწვდომობის დარღვევა – პერსონალურ მონაცემებზე წვდომის დაკარგვა, შეზღუდვა, მონაცემების განადგურება ან წაშლა.

მუხლი 4. ინციდენტის შეფასება

1. ინციდენტს შედეგად შესაძლოა მოჰყვეს ფიზიკური, ქონებრივი ან არაქონებრივი ღირებულების მატერიალური ან არამატერიალური ზიანი.

2. დამუშავებისთვის პასუხისმგებელმა პირმა ინციდენტის აღმოჩენისთანავე, ამ წესის მე-5 და მე-6 მუხლებით განსაზღვრული გარემოებებისა და კრიტერიუმების გათვალისწინებით, უნდა დაიწყოს ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობისა და სიმძიმის შეფასება.

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

4. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა ფასდება ხარისხობრივი ანალიზის საშუალებით, რა დროსაც ობიექტური გადაწყვეტილება მიიღება გამოცდილების, არსებული ინფორმაციის, ცოდნის, განსჯისა და ამ წესით განსაზღვრული კრიტერიუმების გათვალისწინებით.

მუხლი 5. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შექმნის სიმძიმის შეფასებისას გასათვალისწინებელი გარემოებები

ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი საფრთხის შექმნის სიმძიმის განსაზღვრის მიზნებისთვის, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს შემდეგი გარემოებები:

ა) რა სახის ინციდენტს აქვს ადგილი (პერსონალურ მონაცემთა კონფიდენციალურობის, მთლიანობის თუ ხელმისაწვდომობის დარღვევას);

ბ) იმ პერსონალური მონაცემების კატეგორია, რომლებზეც გავლენას ახდენს ინციდენტი;

გ) ეხება თუ არა ინციდენტი არასრულწლოვნის, შეზღუდული შესაძლებლობის მქონე პირისა ან სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე მონაცემთა სუბიექტის პერსონალურ მონაცემებს;

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

ე) დამუშავებისთვის პასუხისმგებელი პირის საქმიანობის განსაკუთრებული ხასიათი, რასაც შესაძლოა ახლდეს მომეტებული საფრთხე;

ვ) ინციდენტის მასშტაბი, მონაცემთა სუბიექტის ან/და პერსონალური მონაცემის რაოდენობის ან/და

მოცულობის თვალსაზრისით;

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

მუხლი 6. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის შეფასების კრიტერიუმები

ინციდენტი ადამიანის ძირითადი უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამომწვევად უნდა იქნეს მიჩნეული იმ შემთხვევებში, თუ მას მოჰყვა/შესაძლოა მოჰყვეს ერთ-ერთი შემდეგი შედეგი:

ა) მონაცემთა სუბიექტის დისკრიმინაცია, მისი ვინაობის მითვისება ან გაყალბება, ფინანსური ზიანი, მონაცემთა სუბიექტის რეპუტაციის შელახვა, პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალურობის დარღვევა, ან სხვა სახის მნიშვნელოვანი სოციალური ან/და ეკონომიკური ზიანი;

ბ) კანონით გათვალისწინებული მონაცემთა სუბიექტის უფლებების რეალიზებისათვის ხელის შეშლა, მათ შორის, მონაცემთა სუბიექტის უფლებების კანონით დადგენილ ვადებში რეალიზების შეზღუდვა;

გ) 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 ამ მუხლის „ა“, „ბ“, „დ“, „ე“ და „ვ“ ქვეპუნქტებით გათვალისწინებული ან სხვა მნიშვნელოვანი ზიანი არ ადგება;

დ) განსაკუთრებული კატეგორიის მონაცემების უკანონო გამჟღავნება;

ე) ფიზიკური ზიანი, მათ შორის, სამედიცინო მომსახურების მიღების შეზღუდვა, თუ აღნიშნული იწვევს სამედიცინო მანიპულაციის ან ოპერაციის გადადებას, რაც პაციენტის მკურნალობაზე ახდენს უარყოფით გავლენას;

ვ) არასრულწლოვნის, შეზღუდული შესაძლებლობების მქონე პირისა და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე მონაცემთა სუბიექტის პერსონალური მონაცემების უკანონო დამუშავება.

მუხლი 7. 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.

2. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა არის:

ა) დაბალი, თუ ნაკლებსავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს;

ბ) საშუალო, თუ ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნისა და ასეთი ზიანის/საფრთხის არარსებობის ალბათობა მეტნაკლებად თანაბარია;

გ) მაღალი, თუ – ინციდენტი დიდი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

თავი III. სამსახურისთვის ინციდენტის შეტყობინების წესი

მუხლი 8. ინციდენტის შეტყობინების ვალდებულება

1. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია ინციდენტის აღმოჩენიდან არაუგვიანეს 72 საათისა მის შესახებ შეატყობინოს სამსახურს კანონისა და ამ წესის შესაბამისად, თუ ინციდენტი საშუალო ან მაღალი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

2. 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, დამუშავებისთვის პასუხისმგებელი პირი არ უნდა დაელოდოს ინციდენტის შეფასების დასრულებას და ინციდენტის შესახებ უნდა შეატყობინოს სამსახურს. ასეთ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელი პირი ობიექტური მიზეზების გამო ვერ ახერხებს სამსახურისათვის ამ წესის მე-10 მუხლის მე-2 პუნქტით განსაზღვრული ინფორმაციის სრულად მიწოდებას, მისი წარდგენა შესაძლებელია განხორციელდეს ეტაპობრივად, გონივრულ ვადებში, გაუმართლებელი დაყოვნების გარეშე.

3. თუ დაბალია ალბათობა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, ინციდენტის სამსახურისთვის შეტყობინების ვალდებულება არ წარმოიშობა.

მუხლი 9. ინციდენტის შეტყობინება

1. დამუშავებისთვის პასუხისმგებელი პირი ინციდენტს სამსახურს ატყობინებს წერილობით ან ელექტრონულად.

2. თუ ინციდენტი შეეხება სახელმწიფო საიდუმლოების შემცველ ინფორმაციას, დამუშავებისთვის პასუხისმგებელი პირი ინციდენტს სამსახურს ატყობინებს საქართველოს კანონმდებლობით დადგენილი წესით.

3. ინციდენტის შეტყობინების მართვის ელექტრონული სისტემის ადმინისტრირებას ახორციელებს სამსახური.

4. ინციდენტის სამსახურისთვის შეტყობინების მიზნით, დამუშავებისთვის პასუხისმგებელი პირის მიერ მიწოდებული ინფორმაციის საფუძველზე, დამუშავებისთვის პასუხისმგებელი პირის მიერ განსაზღვრული, ინციდენტის შეტყობინებაზე პასუხისმგებელი პირი ავსებს ინციდენტის შეტყობინების ფორმას და წარუდგენს სამსახურს.

მუხლი 10. ინციდენტის ელექტრონულად შეტყობინება

1. ინციდენტის ელექტრონული ფორმით შეტყობინება ხორციელდება სამსახურის ოფიციალურ ვებგვერდზე განთავსებული, ინციდენტის შეტყობინების მართვის ელექტრონულ სისტემაში გენერირებული ფორმის მეშვეობით, რომელშიც მიეთითება:

ა) დამუშავებისთვის პასუხისმგებელი პირის სახელწოდება, სამართლებრივი ფორმა, საიდენტიფიკაციო ნომერი და მისამართი;

ბ) დამუშავებისთვის პასუხისმგებელი პირის საქმიანობის სფერო (საჯარო სექტორი, სამართალდამცავი ორგანო, კერძო სექტორი);

გ) ინციდენტის შეტყობინების ფორმის შევსებაზე პასუხისმგებელი პირის სახელი, გვარი, პოზიცია/თანამდებობა და საკონტაქტო მონაცემები (ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი);

დ) არსებობის შემთხვევაში, პერსონალურ მონაცემთა დაცვის ოფიცრის სახელი, გვარი და საკონტაქტო მონაცემები (ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი);

ე) არსებობის შემთხვევაში, სხვა საკონტაქტო პირის სახელი, გვარი, პოზიცია/თანამდებობა და საკონტაქტო მონაცემები (ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი);

ვ) ინციდენტის პირველადი შეტყობინება ხორციელდება, თუ დამატებითი ან განახლებული ინფორმაციის წარდგენა;

ზ) დამატებითი ან განახლებული ინფორმაციის წარდგენის შემთხვევაში, სამსახურის მიერ ინციდენტისთვის მინიჭებული საიდენტიფიკაციო ნომერი;

თ) ინციდენტის სტატუსი (მიმდინარე/დასრულებული/დაუდგენელი);

ი) ინციდენტის დაწყების დრო (თუ იგი ცნობილია) და დასრულების დრო (თუ ინციდენტი დასრულებულია);

კ) დამუშავებისთვის პასუხისმგებელი პირის მიერ ინციდენტის აღმოჩენის დრო;

ლ) იმ შემთხვევაში, თუ შეტყობინებით ინციდენტის შესახებ ინფორმაციის სამსახურისთვის სრულად მიწოდება ვერ ხორციელდება, განმარტება აღნიშნულის მიზეზის თაობაზე;

მ) ინციდენტის სახე:

მ.ა) კონფიდენციალურობის დარღვევა;

მ.ბ) მთლიანობის დარღვევა;

მ.გ) ხელმისაწვდომობის დარღვევა;

ნ) ინციდენტის შედეგები:

ნ.ა) მონაცემების შემთხვევით ან განზრახ განადგურება;

ნ.ბ) მონაცემების შემთხვევით ან განზრახ შეცვლა;

ნ.გ) დაშიფრული მოწყობილობის მოპარვა ან დაკარგვა;

ნ.დ) დაუშიფრავი მოწყობილობის მოპარვა ან დაკარგვა;

ნ.ე) მატერიალური დოკუმენტის მოპარვა, დაკარგვა ან მასზე უნებართვო წვდომა;

ნ.ვ) ელექტრონული ფორმით არსებულ მონაცემებზე უნებართვო წვდომა;

ნ.ზ) ელექტრონული ან/და მატერიალური ფორმით არსებულ მონაცემებზე წვდომის შესაძლებლობის შეზღუდვა;

ნ.თ) ვიდეომონიტორინგის ან/და აუდიომონიტორინგის სისტემის მეშვეობით დამუშავებულ მონაცემებზე უნებართვო წვდომა/მათი უკანონო გამჟღავნება;

ნ.ი) ელექტრონული ფოსტით განხორციელებულ მიმოწერაზე უნებართვო წვდომა/მისი უკანონო გამჟღავნება;

ნ.კ) ონლაინ პორტალზე არსებულ მომხმარებლის ანგარიშზე უნებართვო წვდომა/მასში არსებული მონაცემების უკანონო გამჟღავნება;

ნ.ლ) სოციალური მედიის ან/და მოკლე ტექსტური შეტყობინებების მიმოცვლის პლატფორმაზე

არსებულ მომხმარებლის ანგარიშზე უკანონო წვდომა/მასში არსებული მონაცემების უკანონო გამჟღავნება;

ნ.მ) საფოსტო კორესპონდენციაზე უკანონო წვდომა/მასში არსებული მონაცემების უკანონო გამჟღავნება;

ნ.ნ) ელექტრონულ მოწყობილობაში შენახულ მონაცემებზე უკანონო წვდომა;

ნ.ო) მონაცემების ზეპირსიტყვიერად გამჟღავნება;

ნ.პ) მონაცემებზე წვდომის მოპოვება მოტყუების ან შეცდომაში შეყვანის გზით;

ნ.ჟ) მონაცემების უკანონო გასაჯაროება;

ნ.რ) მონაცემთა დამუშავებისას დაშვებული შეცდომა;

ნ.ს) სისტემის ტექნიკური გამართულობის უზრუნველსაყოფად საჭირო სამუშაოები;

ნ.ტ) სხვა შედეგი;

ო) თუ ცნობილია ის მონაცემები, რომელზეც ინციდენტი გავლენას ახდენს:

ო.ა) სახელი, გვარი, დაბადების თარიღი;

ო.ბ) პირადი ან/და პასპორტის ნომერი;

ო.გ) საკონტაქტო მონაცემები;

ო.დ) საიდენტიფიკაციო ან წვდომის ინფორმაცია (მომხმარებლის სახელი, პაროლი);

ო.ე) სოციალური მედიის გვერდი (ე.წ. პროფილი);

ო.ვ) ეკონომიკური და ფინანსური მონაცემები;

ო.ზ) ოფიციალური დოკუმენტები ან მათი ასლები;

ო.თ) ადგილმდებარეობის მონაცემები (მათ შორის, გეოლოკაციის შესახებ ინფორმაცია);

ო.ი) პერსონალური მონაცემების შემცველი ფოტო, ვიდეო ან აუდიომასალა;

ო.კ) პირად საქმიანობასთან ან ოჯახურ ცხოვრებასთან დაკავშირებული ინფორმაცია;

ო.ლ) პროფესიულ საქმიანობასთან დაკავშირებული ინფორმაცია;

ო.მ) პირის მიერ განხორციელებული კომუნიკაციის ამსახველი მონაცემები;

ო.ნ) განსაკუთრებული კატეგორიის მონაცემები;

ო.ო) სხვა მონაცემი;

პ) თუ ცნობილია, იმ მონაცემთა სუბიექტების სავარაუდო ან ზუსტი რაოდენობა, რომლებზეც ინციდენტი გავლენას ახდენს;

ჟ) 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;

რ) საშუალო ან მაღალი ალბათობა იმისა, რომ ინციდენტი გამოიწვევს ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვან ზიანს/შექმნის მნიშვნელოვან საფრთხეს;

ს) 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;

ტ) 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;

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

ფ) შეუქმნის თუ არა ინციდენტის შესახებ ინფორმაციის გასაჯაროება საფრთხეს:

ფ.ა) სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოების და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესებს;

ფ.ბ) საზოგადოებრივი უსაფრთხოების ინტერესებს;

ფ.გ) დანაშაულის თავიდან აცილებას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას, მართლმსაჯულების განხორციელებას, პატიმრობისა და თავისუფლების აღკვეთის აღსრულებას, არასაპატიმრო სასჯელთა აღსრულებას და პრობაციას, ოპერატიულ-სამძებრო საქმიანობას;

ფ.დ) ქვეყნისთვის მნიშვნელოვან ფინანსურ ან ეკონომიკურ (მათ შორის, მონეტარულ, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესებს;

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

2. ამ წესის მე-9 მუხლის მე-4 პუნქტით განსაზღვრული პირის მიერ სამსახურისთვის მიწოდებული, ამ მუხლით გათვალისწინებული ინფორმაცია მყისიერად აისახება ინციდენტის შეტყობინების მართვის ელექტრონულ სისტემაში და ხელმისაწვდომი ხდება სამსახურის უფლებამოსილი პირისთვის.

მუხლი 11. ინციდენტის წერილობით შეტყობინება

ინციდენტის წერილობითი შეტყობინების შემთხვევაში შეტყობინება მოიცავს ამ წესის მე-10 მუხლის პირველი პუნქტით გათვალისწინებულ ინფორმაციას და სამსახურს წარედგინება „სახაზინო (საბიუჯეტო) დაწესებულებებში საქმისწარმოების ავტომატიზებული სისტემის მინიმალური სტანდარტის დამტკიცების შესახებ“ საქართველოს მთავრობის 2012 წლის 21 თებერვლის №64 დადგენილების მე-2 მუხლით გათვალისწინებული საქმისწარმოების ავტომატიზებული სისტემის მეშვეობით ან მატერიალური ფორმით.

მუხლი 12. ინციდენტის შესახებ შეტყობინების სამსახურში მიღებისა და რეგისტრაციის წესი

1. ინციდენტის შესახებ შეტყობინების ელექტრონული ფორმით მიღება და რეგისტრაცია ხორციელდება ავტომატურად, სამსახურის ინციდენტის შეტყობინების მართვის ელექტრონული სისტემის მეშვეობით.

2. ინციდენტის შესახებ წერილობითი შეტყობინების მიღებასა და რეგისტრაციას სამსახური

ახორციელებს სამსახურის საქმისწარმოების წესით გათვალისწინებული პროცედურით.