შპს ქართულ-ამერიკული უნივერსიტეტის

ინციდენტის იდენტიფიცირებისა და მასზე რეაგირების პოლიტიკა

შინაარსი

მუხლი 1. ზოგადი ინფორმაცია მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის შესახებ

1. შპს ქართულ-ამერიკული უნივერსიტეტის (შემდგომში - უნივერსიტეტი) უზრუნველყოფს ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის პირადი ცხოვრებისა და პერსონალური მონაცემების დაცვას. უნივერსიტეტი განსაკუთრებულ ყურადღებას ანიჭებს მისი დასაქმებულების, ასევე სხვა პირების პერსონალურ მონაცემთა დაცვას. შესაბამისად, იგი პერსონალურ მონაცემებს ამუშავებს საქართველოს კანონმდებლობის, მათ შორის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის, სხვა ნორმატიული აქტებისა და უნივერსიტეტის მიერ ამ სფეროში დამტკიცებული პოლიტიკების შესაბამისად.

მუხლი 2. პოლიტიკის მიზანი

1. წინამდებარე პოლიტიკის მიზანია უნივერსიტეტის, როგორც პერსონალურ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის, მიერ ინციდენტის იდენტიფიცირების მექანიზმის დანერგვა, მასზე დროული რეაგირება და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული ვალდებულებების შესრულება.
2. უნივერსიტეტი ინციდენტთან დაკავშირებით მოქმედებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონისა და სხვა ნორმატიული აქტების შესაბამისად.

მუხლი 3. ტერმინთა განმარტებები

წინამდებარე პოლიტიკაში გამოყენებულ ტერმინებს აქვთ შემდეგი მნიშვნელობა:

ა) **პერსონალური მონაცემი** (შემდგომ – მონაცემი) – ნებისმიერი ინფორმაცია, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს უკავშირდება. ფიზიკური პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, მათ შორის, სახელით, გვარით, საიდენტიფიკაციო ნომრით, გეოლოკაციის მონაცემებით, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემებით, ფიზიკური, ფიზიოლოგიური, ფსიქიკური, ფსიქოლოგიური, გენეტიკური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლით;

ბ) **განსაკუთრებული კატეგორიის მონაცემი** – მონაცემი, რომელიც უკავშირდება ფიზიკური პირის რასობრივ ან ეთნიკურ კუთვნილებას, პოლიტიკურ შეხედულებებს, რელიგიურ, ფილოსოფიურ ან სხვაგვარ მრწამსს, პროფესიული კავშირის წევრობას, ჯანმრთელობას, სქესობრივ ცხოვრებას, ბრალდებულის,

მსჯავრდებულის, გამართლებულის ან დაზარალებულის სტატუსს სისხლის სამართლის პროცესში, მსჯავრდებას, ნასამართლობას, განრიდებას, ადამიანით ვაჭრობის (ტრეფიკინგის) ან „ქალთა მიმართ ძალადობის ან/და ოჯახში ძალადობის აღკვეთის, ძალადობის მსხვერპლთა დაცვისა და დახმარების შესახებ“ საქართველოს კანონის შესაბამისად დანაშაულის მსხვერპლად ცნობას, პატიმრობას და მის მიმართ სასჯელის აღსრულებას, აგრეთვე ბიომეტრიულ და გენეტიკურ მონაცემებს, რომლებიც ფიზიკური პირის უნიკალური იდენტიფიცირების მიზნით მუშავდება;

გ) **ჯანმრთელობასთან დაკავშირებული მონაცემი** – მონაცემთა სუბიექტის ფიზიკური ან ფსიქიკური ჯანმრთელობის შესახებ, აგრეთვე მისთვის სამედიცინო მომსახურების გაწევის თაობაზე ინფორმაცია, თუ იგი მონაცემთა სუბიექტის ფიზიკური ან ფსიქიკური ჯანმრთელობის შესახებ ინფორმაციას იძლევა;

დ) **დამუშავებისთვის პასუხისმგებელი პირი** – ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, უშუალოდ ან დამუშავებაზე უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას;

ე) **მონაცემთა დამუშავება** – მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედება, მათ შორის, მათი შეგროვება, მოპოვება, მათზე წვდომა, მათი ფოტოგადაღება, ვიდეომონიტორინგი ან/და აუდიომონიტორინგი, ორგანიზება, დაჯგუფება, ურთიერთდაკავშირება, შენახვა, შეცვლა, აღდგენა, გამოთხოვა, გამოყენება, დაბლოკვა, წაშლა ან განადგურება, აგრეთვე მონაცემთა გამჟღავნება მათი გადაცემით, გასაჯაროებით, გავრცელებით ან სხვაგვარად ხელმისაწვდომად გახდომით;

ვ) **მონაცემთა სუბიექტი** – ნებისმიერი ფიზიკური პირი, რომლის შესახებ მონაცემიც მუშავდება;

მუხლი 4. ინციდენტის ცნება და სახეები

1. 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 5. ინციდენტის იდენტიფიცირების პროცედურა

1. იმ შემთხვევაში, თუ უნივერსიტეტში პერსონალური მონაცემების დამმუშავებელი პირ(ებ)ი/დასაქმებული, ან დამუშავებაზე უფლებამოსილი პირი (ასეთის არსებობის შემთხვევაში) აღმოაჩენს, რომ ადგილი აქვს პერსონალურ მონაცემთა უსაფრთხოების ნებისმიერი სახის დარღვევას, მათ შორის, მათ არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას/მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას, იგი ვალდებულია, დაუყოვნებლივ, მაგრამ არაუგვიანეს 24 საათისა, აღნიშნულის შესახებ შეატყობინოს უნივერსიტეტის პერსონალურ მონაცემთა დაცვის ოფიცერს ნებისმიერი შესაძლო საშუალებით (სატელეფონო კომუნიკაცია, ელექტრონული ფოსტა, მოკლე ტექსტური შეტყობინება ან სხვა მისთვის ხელმისაწვდომი საკომუნიკაციო საშუალება);
2. ამ მუხლის პირველი პუნქტით გათვალისწინებული ვალდებულების დარღვევა შესაძლოა გახდეს უნივერსიტეტის უფლებამოსილი თანამშრომლისთვის ან სხვა უფლებამოსილი პირისთვის (ასეთის არსებობის შემთხვევაში) შრომითი ხელშეკრულებიდან, შინაგანაწესიდან ან უნივერსიტეტის სხვა შიდაუწყებრივი დანაწესიდან გამომდინარე დისციპლინური წარმოების დაწყების, ხოლო გადაცდომის დადასტურების შემთხვევაში კი შესაბამისი დისციპლინური პასუხისმგებლობის დაკისრების ან სხვა სამართლებრივი სახის ღონისძიებების გატარების საფუძველი.
3. ამ მუხლის პირველი პუნქტით გათვალისწინებული შეტყობინება უნდა შეიცავდეს შემდეგ ინფორმაციას:
    - ინციდენტის თარიღი;
    - ინციდენტის სახე (მოკლე აღწერა);
    - დარღვევის აღწერა/შინაარსი;
    - იმ მონაცემების აღწერა, რომელთა მიმართაც დაფიქსირდა ინციდენტი;
    - ინციდენტის შედეგები;
    - დაზარალებულთა სავარაუდო რაოდენობა;
    - ინციდენტით გამოწვეული სავარაუდო ზიანი, მისი მოცულობა.
4. უნივერსიტეტის პერსონალურ მონაცემთა დაცვის ოფიცერი, ზემოთ აღნიშნული შეტყობინების საფუძველზე, დაუყოვნებლივ იწყებს ინციდენტის და მასთან დაკავშირებული ყველა ფაქტობრივი გარემოების მოკვლევას და უზრუნველყოფს მისი შედეგების, დამდგარი/მოსალოდნელი ზიანის ხარისხისა და საფრთხის შეფასებას.

5. ინციდენტი ადამიანის ძირითადი უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამომწვევად იქნება 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 პუნქტის „ა“, „ბ“, „დ“, „დ“ და „ე“ ქვეპუნქტებით გათვალისწინებული ან სხვა მნიშვნელოვანი ზიანი არ ადგება;
   დ) განსაკუთრებული კატეგორიის მონაცემების უკანონო გამჟღავნება;
   ე) არასრულწლოვნის, შეზღუდული შესაძლებლობების მქონე პირისა და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე მონაცემთა სუბიექტის პერსონალური მონაცემების უკანონო დამუშავება.
6. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა არის:
   ა) დაბალი, თუ ნაკლებად სავარაუდოა, 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 მეტ-ნაკლებად თანაბარია;
   გ) მაღალი, თუ – ინციდენტი დიდი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

მუხლი 6. ინციდენტის შედეგად დამდგარი/მოსალოდნელი მნიშვნელოვანი საფრთხის ხარისხის დასადგენად გასათვალისწინებელი გარემოებები

ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი საფრთხის შექმნის სიმძიმის განსაზღვრის მიზნებისთვის, უნივერსიტეტი ითვალისწინებს და აფასებს შემდეგ გარემოებებს:

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 7. ინციდენტზე რეაგირების პროცესი

1. უნივერსიტეტი, პერსონალურ მონაცემთა დაცვის ოფიცრის აქტიური ჩართულობით, უზრუნველყოფს ინციდენტების, დამდგარი შედეგისა და მიღებული ზომების აღრიცხვას, წინამდებარე პოლიტიკის №1 დანართით (ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტების რეესტრი) განსაზღვრული ფორმით;
2. ინციდენტი აღმოჩენილად, ხოლო უნივერსიტეტი ინციდენტის შესახებ ინფორმირებულად ითვლება იმ მომენტიდან, როდესაც მან შეიტყო ინციდენტის შესახებ.
3. უნივერსიტეტი, ინციდენტის აღმოჩენიდან/გამოვლენიდან ან აღნიშნულის თაობაზე მისთვის შეტყობინებიდან, დაუყოვნებლივ, ყოველგვარი გაუმართლებელი დაყოვნების გარეშე, პერსონალურ მონაცემთა დაცვის ოფიცრისა და საჭიროების შემთხვევაში, შესაბამისი სტრუქტურული ერთეულების, მათ შორის ინფორმაციული ტექნოლოგიების სამსახურის აქტიური ჩართულობით, უზრუნველყოფს მის ხელთ არსებული სათანადო ტექნიკური და ორგანიზაციული ზომების მიღებას ინციდენტის ზუსტი

დაიდენტიფიცირების, მისგან მომდინარე საზიანო შედეგების გამოვლენისა და ეფექტიანი აღმოფხვრის მიზნით.

4. უნივერსიტეტის პერსონალურ მონაცემთა დაცვის ოფიცერი უზრუნველყოფს ინციდენტის აღმოჩენიდან, არაუგვიანეს 72 საათისა, მის შესახებ წერილობითი ან ელექტრონული ფორმით პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინებას, თუ ინციდენტი საშუალო ან მაღალი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.
5. პერსონალურ მონაცემთა დაცვის სამსახურისათვის გაგზავნილი შეტყობინება უნდა შეიცავდეს შემდეგ ინფორმაციას:
    - ინციდენტის გარემოებების, სახისა და დროის შესახებ;
    - ინციდენტის შედეგად უნებართვოდ გამჟღავნებული, დაზიანებული, წაშლილი, განადგურებული, მოპოვებული, დაკარგული, შეცვლილი მონაცემების სავარაუდო კატეგორიებისა და რაოდენობის, აგრეთვე იმ მონაცემთა სუბიექტების სავარაუდო კატეგორიებისა და რაოდენობის შესახებ, რომლებსაც ინციდენტის შედეგად შეექმნათ საფრთხე;
    - ინციდენტით გამოწვეული სავარაუდო ზიანის, მისი შემცირების ან აღმოფხვრის მიზნით უნივერსიტეტის მიერ განხორციელებული ან დაგეგმილი ღონისძიებების შესახებ;
    - იმის შესახებ, გეგმავს თუ არა უნივერსიტეტი ინციდენტის შესახებ შეატყობინოს მონაცემთა სუბიექტს (მონაცემთა სუბიექტებს) და რა ვადაში;
    - პერსონალურ მონაცემთა დაცვის ოფიცრის ან სხვა საკონტაქტო პირის მონაცემების შესახებ.
6. აღნიშნული მუხლის მე-5 პუნქტით გათვალისწინებული ინფორმაციის გარდა, პერსონალურ მონაცემთა დაცვის სამსახურს ასევე უნდა მიეწოდოს „ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმებისა და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ინციდენტის შეტყობინების წესის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2024 წლის 28 თებერვლის №19 ბრძანების მე-10 მუხლით გათვალისწინებული ინფორმაცია.
7. 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, უნივერსიტეტი არ დაელოდება ინციდენტის შეფასების დასრულებას და ინციდენტის შესახებ შეატყობინებს პერსონალურ მონაცემთა დაცვის სამსახურს. ასეთ შემთხვევაში, თუ უნივერსიტეტი ობიექტური მიზეზების გამო ვერ ახერხებს ინფორმაციის სრულად მიწოდებას, მისი

წარდგენა განხორციელდება ეტაპობრივად, გონივრულ ვადებში, გაუმართლებელი დაყოვნების გარეშე.

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

მუხლი 8. ინციდენტის შესახებ მონაცემთა სუბიექტის ინფორმირების ვალდებულება

1. თუ ინციდენტი მაღალი ალბათობით გამოიწვევს მნიშვნელოვან ზიანს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, უნივერსიტეტი ვალდებულია ინციდენტის აღმოჩენიდან პირველი შესაძლებლობისთანავე, გაუმართლებელი დაყოვნების გარეშე, აცნობოს მონაცემთა სუბიექტს ინციდენტის შესახებ და მარტივ და მისთვის გასაგებ ენაზე მიაწოდოს შემდეგი ინფორმაცია:
   ა) ინციდენტისა და მასთან დაკავშირებული გარემოებების ზოგადი აღწერა;
   ბ) ინციდენტით გამოწვეული სავარაუდო/დამდგარი ზიანის, მის შესამცირებლად ან აღმოსაფხვრელად განხორციელებული ან დაგეგმილი ღონისძიებების შესახებ;
   გ) პერსონალურ მონაცემთა დაცვის ოფიცრის ან სხვა პირის საკონტაქტო მონაცემები.
2. თუ მონაცემთა სუბიექტის ინფორმირება არაპროპორციულად დიდ ხარჯებს ან ძალისხმევას მოითხოვს, უნივერსიტეტი ამ მუხლის პირველი პუნქტით გათვალისწინებულ ინფორმაციას გაავრცელებს საჯაროდ ან სხვა ისეთი ფორმით, რომელიც ჯეროვნად უზრუნველყოფს მონაცემთა სუბიექტის მიერ ინფორმაციის მიღების შესაძლებლობას.
3. ამ მუხლის პირველი და მე-2 პუნქტებით გათვალისწინებული ვალდებულება არ წარმოიშობა ერთ-ერთი შემდეგი გარემოების არსებობისას:
   ა) ინციდენტის შესახებ მონაცემთა სუბიექტის ინფორმირება 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.

ბ) უნივერსიტეტმა მიიღო შესაბამისი უსაფრთხოების ზომები, რის შედეგადაც თავიდან იქნა აცილებული ადამიანის ძირითადი უფლებებისა და თავისუფლებების დარღვევის მნიშვნელოვანი საფრთხე.

მუხლი 9. ინციდენტის პრევენციის მიზნით ზომების მიღება

1. უნივერსიტეტში მიღებულია მონაცემთა დაცვისათვის საჭირო ყველა ის ორგანიზაციული და ტექნიკური ზომა, რომელიც, თავის მხრივ, მიმართულია ინციდენტების მაქსიმალურად თავიდან არიდების, მისი დროული აღმოჩენის/გამოვლენის და ინციდენტის შედეგების ეფექტიანი აღმოფხვრისათვის.
2. უნივერსიტეტი პერმანენტულად უზრუნველყოფს მისი თანამშრომლებისთვის პერსონალური მონაცემების არსის, ასევე მათი დაცვის მნიშვნელობისა და აუცილებლობის საკითხებზე ინფორმაციის მიწოდებას, შესაბამისი საინფორმაციო ხასიათის შეხვედრების, სწავლებების, ტრენინგების, სასწავლო პრაქტიკული სახის კურსების ჩატარების ფორმით, ინციდენტის იდენტიფიცირებისა და მასზე ეფექტური რეაგირების მიმართულებით.
3. უნივერსიტეტი უზრუნველყოფს მონაცემთა დამუშავებაში ჩართულ თანამშრომლებთან, ასევე დამუშავებაზე უფლებამოსილ პირებთან (ასეთის არსებობის შემთხვევაში) შესაბამისი სამართლებრივი მექანიზმის გათვალისწინებასა და მათთვის ვალდებულების დაკისრებას, რათა უზრუნველყოფილი იყოს ინციდენტის იდენტიფიცირება მაქსიმალურად მოკლე ვადაში და მასზე რეაგირება კანონმდებლობით დადგენილი წესით.

მუხლი 10. მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმები

1. უნივერსიტეტი უზრუნველყოფს მონაცემთა სუბიექტის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის III თავით გათვალისწინებული უფლებების დაცვას.
2. მონაცემთა დამუშავებასთან დაკავშირებულ ნებისმიერ საკითხზე, მონაცემთა სუბიექტი უფლებამოსილია, მიმართოს უნივერსიტეტის ადამიანური რესურსების მართვის სამსახურის უფროსს ან/და პერსონალურ მონაცემთა დაცვის ოფიცერს.
3. პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე დავის შემთხვევაში მონაცემთა სუბიექტს უფლება აქვს, კანონმდებლობით დადგენილი წესით, მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს ან/და სასამართლოს.