სსიპ - ილიას სახელმწიფო უნივერსიტეტში
პერსონალურ მონაცემთა დაცვის წესი

ეს წესი შექმნილია ილიას სახელმწიფო უნივერსიტეტში პერსონალური მონაცემების დაცვის სტანდარტის ქართულ კანონმდებლობასა და ევროკავშირის რეგულაციებთან თანხვედრაში მოსაყვანად. ამ წესში გათვალისწინებულია ყველა ის პრინციპი და მიდგომა, რაც აუცილებელია ადამიანის პერსონალური მონაცემების ეფექტურად დაცვის უზრუნველსაყოფად.

თავი პირველი. ზოგადი დებულებები

მუხლი 1. სამართლებრივი საფუძვლები და მიზანი

1. საჯარო სამართლის იურიდიული პირის - ილიას სახელმწიფო უნივერსიტეტის (შემდგომში - უნივერსიტეტი) „პერსონალურ მონაცემთა დაცვის წესი“ შემუშავებულია პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის (შემდგომში „კანონი“), მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR), უნივერსიტეტის წესდებისა და შინაგანაწესის საფუძველზე.
2. წინამდებარე წესის მიზანია:
ა) მონაცემების დამუშავების და გაცემისას უზრუნველყოს უნივერსიტეტის ადმინისტრაციული, აკადემიური, დამხმარე, მოწვეული პერსონალის, სტუდენტების, ასევე იმ მესამე პირთა, რომლებიც უნივერსიტეტის სახელით ახორციელებენ თავიანთ უფლებამოსილებას, უფლებათა და თავისუფლებათა, მათ შორის პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვა;
ბ) უნივერსიტეტში ჩამოაყალიბოს პერსონალურ მონაცემთა დაცვის სტრატეგია, მონაცემთა დაცვის ძირითადი პრინციპები და მექანიზმები.
3. უნივერსიტეტში პერსონალურ მონაცემთა დამუშავების პრინციპებია:
ა) კანონიერება, სამართლიანობა და გამჭვირვალობა: პერსონალური მონაცემები მუშავდება კანონიერად, სამართლიანად და გამჭვირვალედ.
ბ) ლეგიტიმური მიზანი: მონაცემები მუშავდება განსაზღვრული და აშკარა ლეგიტიმური მიზნებიდან გამომდინარე, პროპორციული და აუცილებელი საშუალებების გამოყენებით. მონაცემების დამუშავება დაუშვებელია ლეგიტიმური მიზნის არსებობის გარეშე.
გ) მონაცემთა მინიმიზაცია: შეგროვებული მონაცემები უნდა იყოს ადეკვატური, შესაბამისი და განპირობებული აუცილებელი საჭიროებით.
დ) სიზუსტე: მონაცემები უნდა იყოს ზუსტი და განახლებული.
ე) შენახვის ვადის შეზღუდვა: მონაცემები უნდა ინახებოდეს ისეთი ფორმით და იმდენი ხნის განმავლობაში, რომ შესაძლებელი იყოს მონაცემთა სუბიექტების იდენტიფიცირება არა უმეტეს საჭიროზე მეტი ხნით.
ვ) მთლიანობა და კონფიდენციალურობა: პერსონალური მონაცემები უნდა დამუშავდეს ისე, რომ უზრუნველყოფილი იყოს უსაფრთხოება და კონფიდენციალურობა.
ზ) ანგარიშვალდებულება და პასუხისმგებლობა: უნივერსიტეტი პასუხისმგებელია პერსონალური მონაცემების დამუშავებაზე და ნებისმიერ შემთხვევასა თუ ინციდენტზე ანგარიშვალდებულია მონაცემთა სუბიექტის/სუბიექტების წინაშე.

მუხლი 2. ტერმინთა განმარტება

1. ამ წესში გამოყენებული ტერმინები განიმარტება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის შესაბამისად.

მუხლი 3. მონაცემთა დამუშავება

1. უნივერსიტეტი მონაცემებს ამუშავებს ავტომატური, ნახევრად ავტომატური და არაავტომატური საშუალებების გამოყენებით.
2. უნივერსიტეტი ამუშავებს სტუდენტის, აკადემიური, ადმინისტრაციული და დამხმარე პერსონალის, ასევე სხვა პირის/პირების პერსონალურ მონაცემებს, რომლებიც განსაზღვრულია კანონით, ხელშეკრულებებითა და უნივერსიტეტის შიდა რეგულაციებით.
3. უნივერსიტეტი საკუთარი კომპეტენციის ფარგლებში გამოსცემს ბრძანებებს, რისთვისაც ამუშავებს ისეთ პერსონალურ მონაცემებს, რომელიც დაკავშირებულია პირისთვის სტუდენტის სტატუსის მინიჭებასთან, შეწყვეტასთან, შეჩერებასთან, აღდგენასთან, ასევე მისთვის სოციალური შეღავათებისა და სტიპენდიების დანიშვნასა და სხვა კანონით გათვალისწინებული ქმედების განხორციელებასთან. უნივერსიტეტი უფლებამოსილია, ბრძანება გამოაქვეყნოს საჯარო გაცნობისათვის, თუ ეს განსაზღვრულია კანონით ან ეხება 50-ზე მეტ პირს.
4. უნივერსიტეტი, სტუდენტებისა და პერსონალის ინტერესებიდან გამომდინარე, ამუშავებს განსაკუთრებული კატეგორიის ისეთ მონაცემებს, როგორიცაა მონაცემები ჯანმრთელობის მდგომარეობასთან დაკავშირებით, მხოლოდ მონაცემთა სუბიექტის მიმართვის და მისი თანხმობის საფუძველზე. სუბიექტის თანხმობის ფორმა განსაზღვრულია შესაბამისი დოკუმენტაციით.
5. უნივერსიტეტს უფლება აქვს, დაამუშაოს მონაცემები პლაგიატის პრევენციისა და მისი გამოვლენის მიზნით.
6. უნივერსიტეტი უფლებამოსილია, დაამუშაოს პერსონალური მონაცემები დისციპლინური ღონისძიებების გატარების დროს.
7. უნივერსიტეტი ამუშავებს არასრულწლოვან პირთა მონაცემებს კანონიერი წარმომადგენლის თანხმობის საფუძველზე.
8. უნივერსიტეტი ამუშავებს უნივერსიტეტის აკადემიური და დამხმარე პერსონალის, ასევე წინასახელშეკრულებო ურთიერთობების პირობებში აპლიკანტების პერსონალურ მონაცემებს, ადამიანური რესურსების მართვისა და რეკრუტინგის პოლიტიკიდან და შესაბამისი ღონისძიებებიდან გამომდინარე.
9. უნივერსიტეტი უზრუნველყოფს პერსონალურ მონაცემთა დაცვის პროცესის მუდმივ მონიტორინგს.
10. უნივერსიტეტი უზრუნველყოფს პერსონალური მონაცემების დამუშავების შესახებ დასაქმებულისა და სტუდენტის ინფორმირებას ხელშეკრულების, წინამდებარე წესისა და სხვა ინფორმაციული ღონისძიებების მეშვეობით.

თავი მეორე. პერსონალურ მონაცემთა დამუშავებისა და დაცვის სტანდარტები

მუხლი 4. პერსონალურ მონაცემთა დამუშავების საფუძვლები

1. პერსონალურ მონაცემთა დამუშავება დასაშვებია, თუ:

ა) არსებობს მონაცემთა სუბიექტის თანხმობა;

ბ) მონაცემთა დამუშავება გათვალისწინებულია კანონით;

გ) მონაცემთა დამუშავება საჭიროა უნივერსიტეტის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობის შესასრულებლად;

დ) მონაცემთა დამუშავება საჭიროა მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად;

ე) მონაცემთა დამუშავება აუცილებელია მონაცემთა დამმუშავებლის (უნივერსიტეტის) ან მესამე პირის კანონიერი ინტერესის დასაცავად, გარდა იმ შემთხვევისა, როდესაც არსებობს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის აღმატებული ინტერესი;

ვ) კანონის თანახმად, მონაცემები საჯაროდ ხელმისაწვდომია ან მონაცემთა სუბიექტმა ისინი ხელმისაწვდომი გახადა;

ზ) მონაცემთა დამუშავება აუცილებელია კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესების დასაცავად;
თ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად (მისთვის მომსახურების გასაწევად);
2. იმისთვის, რომ პერსონალური მონაცემების დამუშავებას საფუძვლად დაედოს მონაცემთა სუბიექტის თანხმობა, აუცილებელია ეს თანხმობა:
ა) იყოს ნებაყოფლობითი;
ბ) გამოხატული იყოს წინასწარ, მონაცემთა დამუშავებამდე;
გ) გამოხატული იყოს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის მიღების შემდეგ;
დ) გამოხატული იყოს კონკრეტული, მკაფიოდ განსაზღვრული კანონიერი მიზანი მონაცემთა დამუშავებაზე;
ე) გამოხატვის საშუალება იყოს ნათელი, რომლითაც დგინდება მონაცემთა სუბიექტის ნება.

მუხლი 5. განსაკუთრებული კატეგორიის მონაცემთა დამუშავება
1. უნივერსიტეტი ამუშავებს განსაკუთრებული კატეგორიის მონაცემებს მხოლოდ მონაცემთა სუბიექტის წერილობითი თანხმობის არსებობის შემთხვევაში.
2. ნასამართლობასა და ჯანმრთელობის მდგომარეობასთან დაკავშირებული მონაცემების დამუშავება აუცილებელია შრომითი ვალდებულებების და ურთიერთობების ხასიათიდან გამომდინარე, მათ შორის დასაქმების თაობაზე გადაწყვეტილების მისაღებად.

მუხლი 6. პერსონალური მონაცემების მოპოვება მესამე პირებისგან
1. ილიას სახელმწიფო უნივერსიტეტმა მონაცემთა სუბიექტის პერსონალური მონაცემები შესაძლოა მესამე პირებისგან მოიპოვოს შემდეგი მიზნებისათვის: მონაცემთა სუბიექტის სრულყოფილი მომსახურებისთვის, საქართველოს კანონმდებლობით განსაზღვრულ შემთხვევებში, საქართველოს კანონმდებლობით უნივერსიტეტისთვის დაკისრებული მოვალეობების შესრულების მიზნით, ასევე მესამე პირებისგან, საჯარო სამართლის იურიდიული პირის სტატუსით მოქმედ ორგანიზაციებთან, პარტნიორ ორგანიზაციებთან გაფორმებული ხელშეკრულებებიდან გამომდინარე უნივერსიტეტის მიერ ნაკისრი ვალდებულებების შესრულების მიზნებისათვის.
2. მესამე პირს წარმოადგენს ფიზიკური და/ან იურიდიული პირი/პირები, საჯარო სამართლის იურიდიული პირის სტატუსით მოქმედი ორგანიზაციები.

მუხლი 7. ელექტრონული ფოსტისა და ტელეფონის ნომრის გამოყენება
1. ეფექტური და სწრაფი კომუნიკაციის მიზნით, უნივერსიტეტი ამუშავებს დასაქმებული პირების, ადმინისტრაციული პერსონალის, აკადემიური და მოწვეული პერსონალის, სტუდენტებისა და კურსდამთავრებულების ელფოსტებსა და ტელეფონის ნომრებს.

მუხლი 8. პერსონალური მონაცემების დაცვა
1. უნივერსიტეტი უზრუნველყოფს ელექტრონული ინფორმაციის დამმუშავებელი მოწყობილობის/მოწყობილობების დაცვას არაავტორიზებული წვდომისგან და განზრახ დაზიანებისაგან. ამასთანავე იღებს ზომებს, რათა მონაცემები დაცული იყოს უკანონო გამჟღავნებისგან, შეცვლისგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისგან.
2. უნივერსიტეტი იღებს ვალდებულებას, რომ საჭიროების შემთხვევაში განხორციელდეს შესაბამისი ტექნიკური და ორგანიზაციული ღონისძიებები რისკის შესაბამისი უსაფრთხოების დონის უზრუნველსაყოფად, მათ შორის:
ა) პერსონალური მონაცემების ფსევდონიმიზაცია და დაშიფვრა.

ბ) ზომები, რომლებიც უზრუნველყოფენ დამუშავების სისტემების მუდმივ კონფიდენციალურობას, მთლიანობას, არაავტორიზებული წვდომის შეზღუდვასა და მდგრადობას.
გ) ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში მონაცემების ხელმისაწვდომობისა და ხელმისაწვდომობის აღდგენის ღონისძიებები.
დ) უსაფრთხოების ზომების ეფექტურობის რეგულარული ტესტირება, შეფასება და განახლება.
3. უნივერსიტეტი უზრუნველყოფს მატერიალური სახით შენახული მონაცემების დაცვას გარეშე და არაავტორიზებულ პირთა წვდომისგან.
4. ილიას სახელმწიფო უნივერსიტეტის თითოეულ თანამშრომელს, საჭიროების შემთხვევაში, აქვს საკუთარი პერსონალური კომპიუტერი, რომელიც დაცულია შესაბამისი მომხმარებლითა და პაროლით, რომელზე წვდომაც აქვს მხოლოდ იმ თანამშრომელს, ვის მფლობელობაშიც არის პერსონალური კომპიუტერი. თანამშრომელს ეკრძალება ამ მომხმარებლისა და პაროლის შესახებ ინფორმაციის ნებისმიერი გზით გამჟღავნება.
5. უნივერსიტეტი უზრუნველყოფს მონაცემთა ბაზების იმგვარ ადმინისტრირებას, რომ საჭიროების შემთხვაში, ინფორმაცია ყველა სტუდენტს, აკადემიურ, ადმინისტრაციულ, დამხმარე და მოწვეულ პერსონალს, ასევე უნივერსიტეტთან დაკავშირებულ, ყველა შესაბამის პირს მიეწოდოს ინდივიდუალურად.
6. უნივერსიტეტში დასაქმებული ნებისმიერი პირი, რომელიც აღმოაჩენს დარღვევებს პერსონალურ მონაცემთა დამუშავებასთან მიმართებით, ვალდებულია ამის შესახებ ინფორმაცია დაუყოვნებლივ მიაწოდოს უნივერსიტეტის პერსონალურ მონაცემთა დაცვის ოფიცერს.
7. უნივერსიტეტი პერსონალური მონაცემების უკანონოდ დამუშავებას განიხილავს ადმინისტრაციულ სამართალდარღვევად და უზრუნველყოფს ინფორმაციის მიწოდებას შესაბამისი ორგანოებისთვის.

თავი მესამე. პერსონალურ მონაცემთა სუბიექტების და დამუშავებასთან დაკავშირებული პირების უფლებები და ვალდებულებები

მუხლი 9. მონაცემთა სუბიექტის უფლებები და ვალდებულებები

1. მონაცემთა სუბიექტს უფლება აქვს მოსთხოვოს უნივერსიტეტს ინფორმაცია მის შესახებ მონაცემთა დამუშავების თაობაზე. უნივერსიტეტი შეტყობინების მიღებიდან არაუგვიანეს 10 (ათი) კალენდარული დღისა უზრუნველყოფს მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდებას, თუ რომელი კატეგორიის ინფორმაცია მუშავდება, რა მიზნით და რა სამართლებრივი საფუძვლით, ასევე გაცემულია თუ არა მისი მონაცემები მესამე პირზე, ასეთის არსებობის შემთხვევაში ვისზე გაიცა ეს მონაცემი.
2. მონაცემთა სუბიექტს უფლება აქვს ნებისმიერ დროს, ყოველგვარი განმარტების ან დასაბუთების გარეშე გამოიხმოს მის მიერ გაცემული თანხმობა. ამ შემთხვევაში, მონაცემთა სუბიექტის მოთხოვნის საფუძველზე, მონაცემთა დამუშავება უნდა შეწყდეს ან/და დამუშავებული მონაცემები წაიშალოს ან განადგურდეს მოთხოვნიდან არაუგვიანეს 10 სამუშაო დღისა, თუ მონაცემთა დამუშავების სხვა საფუძველი არ არსებობს.
3. მონაცემთა სუბიექტს ასევე აქვს შემდეგი უფლებები:
ა) გასწორების უფლება: არაზუსტი პერსონალური მონაცემების შესწორების მოთხოვნის უფლება.
ბ) დამუშავების შეზღუდვის უფლება: დამუშავების შეზღუდვის უფლება გარკვეულ, კანონით განსაზღვრულ პირობებში.
გ) მონაცემთა პორტაბელურობის უფლება: მათი მონაცემების სტრუქტურირებულ, ჩვეულებრივ გამოყენებად ფორმატში მიღება და სხვა კონტროლერზე გადატანა.
დ) შეწინააღმდეგების უფლება: ლეგიტიმური ინტერესების ან პირდაპირი მარკეტინგის საფუძველზე მონაცემთა დამუშავების შემთხვევაში ან სხვა სამართლებრივი საფუძვლების არსებობისას ქმედების გასაჩივრების უფლება.

ე) გადაწყვეტილების ავტომატიზებულ მიღებასთან დაკავშირებული უფლებები: არ დაექვემდებაროს გადაწყვეტილებებს, რომლებიც დაფუძნებულია მხოლოდ ავტომატურ დამუშავებაზე, მათ შორის პროფილირებაზე.
ვ) კანონის მესამე თავით გათვალისწინებული სხვა უფლებები.
4. მონაცემთა სუბიექტის მიერ თანხმობის გამოხმობა არ იწვევს თანხმობის გამოხმობამდე და თანხმობის ფარგლებში წარმოშობილი სამართლებრივი შედეგების გაუქმებას.
5. მონაცემთა სუბიექტი ვალდებულია, უნივერსიტეტს მიაწოდოს ზუსტი და ჭეშმარიტი პერსონალური მონაცემი. განზრახ ან გაუფრთხილებლობით არაზუსტი პერსონალური ინფორმაციის მიწოდების შემთხვევაში პასუხისმგებლობა ეკისრება მონაცემთა სუბიექტს.

მუხლი 10. სტუდენტის უფლება-მოვალეობები
1. უნივერსიტეტი სტუდენტებს უნივერსიტეტთან მომსახურების ხელშეკრულების გაფორმებამდე აწვდის ინფორმაციას, რა სახის პერსონალურ მონაცემებს ამუშავებს მათ შესახებ უნივერსიტეტი.
2. სტუდენტები (მათი კანონიერი წარმომადგენლები, ასეთის არსებობის შემთხვევაში) ვალდებულნი არიან:
ა) დაიცვან წინამდებარე წესი, როდესაც ისინი წარმოადგენენ უნივერსიტეტს და უნივერსიტეტის სახელით მონაწილეობენ სხვადასხვა აქტივობაში.
ბ) დაიცვან წინამდებარე წესი, როდესაც იმყოფებიან უნივერსიტეტის ტერიტორიაზე, როგორც ამ უნივერსიტეტის სტუდენტები.
გ) შეატყობინონ უნივერსიტეტს თავისი პერსონალური მონაცემების ცვლილების შესახებ.
3. „ილიას სახელმწიფო უნივერსიტეტში პერსონალურ მონაცემთა დაცვის წესის“ დარღვევა არის სტუდენტის მიმართ დისციპლინური წარმოების დაწყების საფუძველი.
4. სტუდენტებისათვის პროგრამის ,,სახელმწიფო სტიპენდიები სტუდენტებს“ ფარგლებში სტიპენდიების (შემდგომში - ,,სტიპენდია“) დანიშვნის წარმოების პროცესში არსებული პერსონალური მონაცემების დამუშავება აუცილებელია აღნიშნული სტიპენდიის კონკრეტულ პირთა წრისათვის (სტუდენტებისათვის) სტიპენდიის დანიშვნის მიზნით, რაც ემსახურება მათი სწავლის უფლების რეალიზების დამატებით ხელშეწყობას.
5. 16 წელს მიღწეული არასრულწლოვანი სტუდენტის შესახებ მონაცემთა დამუშავება დასაშვებია მისი თანხმობის საფუძველზე, გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა, მათ შორის, როდესაც მონაცემთა დამუშავებისთვის აუცილებელია 16 წლიდან 18 წლამდე არასრულწლოვანისა და მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობა.
5.1. არასრულწლოვანის პერსონალური მონაცემების დამუშავებაზე თანხმობის მიღების შემთხვევაში გათვალისწინებული უნდა იქნეს შემდგომი გარემოებები:
ა) არასრულწლოვან პირებთან მიმართებით პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული მიზნები აღწერილი უნდა იყოს დეტალურად და მათ ასაკზე მორგებული ფორმით.
ბ) თანხმობა უნდა იყოს მკაფიო, გასაგები და მარტივად ხელმისაწვდომი.
გ) გათვალისწინებული უნდა იყოს არასრულწლოვანის/ბავშვების ასაკი და განვითარების დონე.
დ) დაუშვებელია კონფიდენციალურობის ვრცელი პოლიტიკის გამოყენება, რომლის გაგებაც რთულია ან რომელიც სამართლებრივი ტერმინებით არის დატვირთული.
ე) უნივერსიტეტი ვალდებულია, უზრუნველყოს თანხმობის გაცემა იმ ინფორმაციის საფუძველზე, რომელიც მონაცემთა სუბიექტს საშუალებას აძლევს, ადვილად მოახდინოს იდენტიფიცირება, ვინ არის დამუშავებისთვის პასუხისმგებელი პირი და გაიაზროს, თუ რას ეთანხმება იგი.
ვ) უნივერსიტეტი ვალდებულია, მკაფიოდ აღწეროს მონაცემთა შეგროვების მიზანი, რისთვისაც ითხოვს თანხმობას.
ზ) უნივერსიტეტი ვალდებულია, შეიმუშაოს მარტივი დოკუმენტი, რომელსაც გამოიყენებენ არასრულწლოვანები/ბავშვები და მათი მშობლები/კანონიერი წარმომადგენლები.

ამასთანავე აუცილებელია, რომ მშობლებმა/კანონიერმა წარმომადგენლებმა მიაწოდონ არასრულწლოვანებს/ბავშვებს მათი პერსონალური მონაცემების დამუშავების თაობაზე სრულყოფილი ინფორმაცია.
6. არასრულწლოვანის შესახებ განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია მხოლოდ მისი მშობლის ან სხვა კანონიერი წარმომადგენლის წერილობითი თანხმობის საფუძველზე, გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა.

მუხლი 11. უნივერსიტეტის პერსონალის უფლება-მოვალეობანი
1. უნივერსიტეტში დასაქმებული პირები ვალდებულნი არიან, დაიცვან წინამდებარე წესი.
2. უნივერსიტეტი უზრუნველყოფს პერსონალის ინფორმირებას, წინასახელშეკრულებო ურთიერთობის პერიოდში რა სახის და რა მოცულობის პერსონალურ მონაცემებს დაამუშავებს მათ შესახებ უნივერსიტეტი.
3. უნივერსიტეტში დასაქმებულ პირებს ეკისრებათ პასუხისმგებლობა, პერსონალური მონაცემების შემცველი დოკუმენტები და ფაილები არ დატოვონ ყურადღების გარეშე და მაქსიმალურად მიიღონ ყველა საჭირო ზომა, რათა არ მოხდეს პერსონალური მონაცემების უნებართვო გამჟღავნება.
4. უნივერსიტეტის პერსონალი ვალდებულია, არ გაამჟღავნოს და არ გადასცეს სამსახურებრივი მოვალეობის შესრულებისას მოპოვებული სხვისი პერსონალური მონაცემები მესამე პირებს. უნივერსიტეტში დასაქმებულ პირებს პერსონალური მონაცემების დაცვის ვალდებულება გააჩნიათ იმ შემთხვევაშიც, თუ ისინი აღარ იქნებიან დასაქმებულნი უნივერსიტეტში.
5. იმ შემთხვევაში, თუ პირები აღარ არიან დასაქმებულნი უნივერსიტეტში და დაარღვევენ წინამდებარე წესს, პასუხისმგებლობა დადგება მოქმედი კანონმდებლობის შესაბამისად.
6. პერსონალური მონაცემების დამუშავების შესახებ დადგენილი წესების დარღვევა არის უნივერსიტეტის პერსონალის მიმართ დისციპლინური წარმოების დაწყების საფუძველი.

თავი მეოთხე. ვიდეო და აუდიომონიტორინგი

მუხლი 12. უნივერსიტეტის შენობასა და ეზოში ვიდეომონიტორინგის განხორციელება
1. უნივერსიტეტის შენობაში ხორციელდება ვიდეომონიტორინგი, პირთა უსაფრთხოების, უნივერსიტეტის საკუთრების დაცვისა და გამოცდის/ტესტირების მონიტორინგის მიზნებისათვის.
2. უნივერსიტეტის შენობაში ვიდეომონიტორინგი მიმდინარეობს უწყვეტად, კვირაში 7 დღე, 24 საათის განმავლობაში.
3. უნივერსიტეტის ტერიტორიაზე დამონტაჟებულია ვიდეო-სამეთვალყურეო მოწყობილობები, რომელიც აღნიშნულია შესაბამისი საცნობი ნიშნით. უნივერსიტეტის შენობაში დამონტაჟებული ვიდეოსამეთვალყურეო მოწყობილობების დაფარვის არეალი მოიცავს უნივერსიტეტის დერეფნებს, საგამოცდო სივრცეებს, საპარკინგე ტერიტორიას და უნივერსიტეტის შიდა და გარე ეზოს.
4. უნივერსიტეტის ტერიტორიაზე განთავსებული ვიდეოსამეთვალყურეო მოწყობილობებიდან მიღებული ვიდეოჩანაწერები ინახება არა უმეტეს 40 (ორმოცი) დღისა. გარდა იმ შემთხვევისა, როდესაც კანონმდებლობით დადგენილი წესით რომელიმე უწყების მომართვის საფუძველზე საჭიროა ჩანაწერის შენახვა ამ პუნქტით დადგენილ ვადაზე მეტი ხნით.
5. ვიდეოჩანაწერებზე წვდომა დაშვებულია მხოლოდ ავტორიზებული პერსონალისთვის, როგორიცაა უნივერსიტეტის დაცვისა და უსაფრთხოების სამსახურის უფროსი და შესაბამისი თანამშრომლები, რომლებიც პასუხისმგებელნი არიან ვიდეომონიტორინგზე. ვიდეოჩანაწერებზე წვდომა ხორციელდება მხოლოდ ლეგიტიმური მიზნის არსებობის

შემთხვევაში, როგორიცაა: უნივერსიტეტში უსაფრთხოების უზრუნველყოფა, შესაძლო ინციდენტების გამოძიება, სამართლებრივი ვალდებულებების შესრულება ან/და სხვა შესაბამისი სამართლებრივი საფუძველი.
ვიდეოჩანაწერებზე წვდომა შესაძლებელია მხოლოდ დაცვისა და უსაფრთხოების სამსახურის უფროსის მიერ ან მისი მკაფიო თანხმობით, შესაბამისი მიზნისა და აუცილებლობის პრინციპების დაცვით.
6. ვიდეომონიტორინგის სისტემა და ვიდეოჩანაწერები დაცულია არამართლზომიერი ხელყოფისა და გამოყენებისგან, შესაბამისი ტექნიკური მექანიზმების მეშვეობით. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს ვიდეოჩანაწერებზე წვდომის თითოეული შემთხვევის აღრიცხვა, მათ შორის, მიმდინარეობს წვდომის დროისა და მომხმარებლის სახელის აღრიცხვა, რომელიც წვდომის განმახორციელებელი პირის იდენტიფიცირების შესაძლებლობას იძლევა.
7. ვიდეოსათვალთვალო სისტემაზე წვდომის უფლებამოსილების მქონე პირ(ებ)ის სამსახურიდან წასვლის ან/და მივლინების ან/და შვებულების დროს პერსონალურ მონაცემებზე წვდომის უფლებამოსილება გააჩნია უფლებამონაცვლე პირ(ებ)ს, რომელზეც/რომლებზეც გადადის იგივე უფლება-მოვალეობები.
8. ოპერატიულ-სამძებრო ღონისძიებებისა და დანაშაულის გამოძიების მიზნით, მოთხოვნის საფუძველზე, უნივერსიტეტი ვიდეოჩანაწერს გადასცეს შესაბამის უწყებებს, მხოლოდ მოსამართლის განჩინების ან გადაუდებელი აუცილებლობის შემთხვევაში პროკურორის მოტივირებული დადგენილების საფუძველზე.
9. ვიდეოჩანაწერები დაცულია დაშიფრული ციფრული შენახვის სისტემებში. შენახვის მოწყობილობებზე ფიზიკური წვდომა შეზღუდულია მხოლოდ ავტორიზებული პერსონალისთვის. ტარდება რეგულარული აუდიტი მონაცემთა მთლიანობისა და უსაფრთხოების უზრუნველსაყოფად.
10. მონაცემთა სუბიექტებს (სტუდენტებს, პერსონალს, სტუმრებს) უფლება აქვთ, ინფორმირებული იყვნენ ვიდეომონიტორინგის პრაქტიკის შესახებ, მიიღონ წვდომა მათთან დაკავშირებულ კადრებზე და კანონის შესაბამისად და გათვალისწინებულ შემთხვევებში მოითხოვონ მათი მონაცემების შესწორება ან წაშლა.
11. დაცვისა და უსაფრთხოების სამსახური საინფორმაციო ტექნოლოგიების სამსახურის დახმარებით უზრუნველყოფს ამ მუხლის მე-4 პუნქტით განსაზღვრული ვადის ამოწურვის შემდეგ ინფორმაციის წაშლასა და განადგურებას.

მუხლი 13. უნივერსიტეტის ცხელ ხაზზე შემოსული ზარების აუდიომონიტორინგი

1. უნივერსიტეტში სერვისის ეფექტურობისათვის ფუნქციონირებს სპეციალური ცხელი ხაზი, რომელზეც მიმდინარეობს შემოსული ზარების მონიტორინგი, ჩაწერა. წინამდებარე აუდიოჩანაწერები ინახება 1 (ერთი) თვის განმავლობაში.
2. საინფორმაციო ტექნოლოგიების სამსახური უზრუნველყოფს ამ მუხლის მე-10 პუნქტით განსაზღვრული ვადის ამოწურვის შემდეგ ინფორმაციის წაშლას და განადგურებას.

თავი მეხუთე. უნივერსიტეტის სტრუქტურული და დამხმარე ერთეულების მიერ პერსონალურ მონაცემთა დამუშავება

მუხლი 14. ილიას სახელმწიფო უნივერსიტეტის ადამიანური რესურსების სამსახურის მიერ უნივერსიტეტის თანამშრომლების პერსონალური მონაცემების დამუშავება

1. ილიას სახელმწიფო უნივერსიტეტის ადამიანური რესურსების მართვის სამსახური ამუშავებს და ინახავს უნივერსიტეტის თანამშრომლების პერსონალურ მონაცემებს, მათ შორის პირად საქმეებს, თანამშრომლებთან ხელშეკრულების გაფორმებისა და ადამიანური რესურსების ეფექტურად მართვის მიზნით. უნივერსიტეტის თანამშრომლების პირადი საქმე

მოიცავს შემდეგ პერსონალურ მონაცემებს: სახელი, გვარი, პირადი ნომერი, მისამართი, ტელეფონის ნომერი, აღნიშნული მონაცემები ასახულია შემდეგ დოკუმენტებში: პირადობის დამადასტურებელი დოკუმენტები, სახელის, გვარის შეცვლის შესახებ გადაწყვეტილება, ანგარიშის ნომერი, კვალიფიკაციის დამადასტურებელი დოკუმენტი/დოკუმენტები, შრომითი ხელშეკრულება, სხვადასხვა ბრძანება.

2. ილიას სახელმწიფო უნივერსიტეტის თანამშრომლების პირადი საქმეები ინახება მატერიალურად - ქაღალდმატარებლებზე და ელექტრონულად - Excel-ის სისტემაში, ასევე ნაწილობრივ ERP პროგრამაში;

3. ქაღალდმატარებლებზე არსებული პერსონალური მონაცემები ინახება უნივერსიტეტის ადამიანური რესურსების მართვის სამსახურისათვის განკუთვნილ ოთახში. ქაღალდმატარებლებზე არსებულ ინფორმაციაზე წვდომის უფლება აქვთ მხოლოდ ადამიანური რესურსების მართვის სამსახურის თანამშრომლებს;

4. ადამიანური რესურსების მართვის სამსახური უზრუნველყოფს ქაღალდმატარებლებზე შენახული პირადი საქმეების უსაფრთხოებას და გარეშე პირების წვდომისგან დაცვას. ამისათვის, იმ ოთახში, სადაც ინახება პირადი საქმეები, დაწესებულია მორიგეობა, სადაც სამუშაო დროის განმავლობაში მუდმივად იმყოფება სამსახურის მინიმუმ ერთი თანამშრომელი. სამუშაო დროის დასრულების შემდგომ, სამსახურის ოთახის კარი იკეტება, რომლის გასაღებზე წვდომა აქვთ მხოლოდ სამსახურის თანამშრომლებს, დაცვასა და დასუფთავების თანამშრომლებს. არასამუშაო საათებში ოთახის დაცვას უზრუნველყოფს ილიას სახელმწიფო უნივერსიტეტის დაცვისა და უსაფრთხოების სამსახური.

5. უნივერსიტეტის თანამშრომლების პერსონალური მონაცემები და პირადი ინფორმაცია ასევე ინახება Excel-ის სისტემაში, რომელზე წვდომაც აქვთ მხოლოდ ადამიანური რესურსების მართვის სამსახურის თანამშრომლებს სამსახურის ხელმძღვანელის (მისი არყოფნის შემთხვევაში, მისი მოვალეობის შემსრულებლის) თანხმობით. ის კომპიუტერული ტექნიკა, რისი მეშვეობითაც Excel-ის სისტემაში ინახება პერსონალური მონაცემები, დაცულია შესაბამისი მომხმარებლითა და პაროლით, რომელზე წვდომაც აქვთ მხოლოდ ადამიანური რესურსების მართვის სამსახურის თანამშრომლებს.

6. ილიას სახელმწიფო უნივერსიტეტში, თანამშრომლების პირადი საქმეები, თანამშრომელთან ხელშეკრულების შეწყვეტის შემდგომ ინახება 5 წლის განმავლობაში და ამის შემდეგ გადაეცემა უნივერსიტეტის არქივს.

მუხლი 15. ილიას სახელმწიფო უნივერსიტეტის ფაკულტეტების მიერ სტუდენტის პერსონალური მონაცემების შენახვა და დამუშავება

1. უნივერსიტეტს გააჩნია არქივი, რომელიც გამოიყენება პერსონალური მონაცემების დამუშავებისა და გრძელვადიანი შენახვის მიზნით. არქივში ინახება სტუდენტთა პირადი საქმეები, რომლებიც შეიცავს სხვადასხვა კატეგორიის პერსონალურ მონაცემებს (მათ შორის, იდენტიფიცირების შესაძლებლობის მქონე ინფორმაციას). აღნიშნული მონაცემები ექვემდებარება შენახვას კანონით დადგენილი ვადით — 75 წლის განმავლობაში, საქართველოს ეროვნული არქივის რეგულაციების შესაბამისად.

2. გარდა ამისა, უნივერსიტეტი ფლობს მუდმივად შესანახ დოკუმენტებსაც, რომლებიც ხშირად შეიცავს პერსონალურ მონაცემებს და უკავშირდება როგორც აკადემიურ და ადმინისტრაციულ, ასევე სამართლებრივ და შრომით ურთიერთობებს. ამ დოკუმენტებში თავმოყრილი პერსონალური მონაცემების შენახვა და დამუშავება ხორციელდება მკაცრად განსაზღვრული მიზნებისთვის, რაც ეფუძნება როგორც საქართველოს ,,პერსონალურ

მონაცემთა დაცვის შესახებ“ კანონის, ისე ევროკავშირის ზოგადი მონაცემთა დაცვის რეგულაციის (GDPR) ძირეულ პრინციპებს.

3. უნივერსიტეტი უფლებამოსილია, შეინახოს პერსონალური მონაცემები მხოლოდ იმ ვადით, რაც აუცილებელია დოკუმენტის სახეობიდან გამომდინარე, მისი მიზნის მიღწევისთვის ან სამართლებრივი ვალდებულებების შესასრულებლად. მონაცემების შენახვა არ სცილდება მკაფიოდ განსაზღვრულ და კანონიერ მიზნებს და ემყარება დაარქივების, საჯარო ინტერესის, აკადემიური ისტორიის შენარჩუნების ან სამართლებრივი ვალდებულებების შესრულების საჭიროებას.

4. უნივერსიტეტი იღებს შესაბამის ტექნიკურ და ორგანიზაციულ ზომებს, რათა დაცული იყოს მონაცემების უსაფრთხოება, კონფიდენციალურობა და მთლიანობა და არ მოხდეს მონაცემებზე უნებართვო წვდომა, განადგურება ან უკანონო დამუშავება.

მუხლი 16. უნივერსიტეტის საინფორმაციო ტექნოლოგიების (IT) სამსახურის ჩართულობა პერსონალურ მონაცემების დამუშავების პროცესში

1. ილიას სახელმწიფო უნივერსიტეტის საინფორმაციო ტექნოლოგიების სამსახური უზრუნველყოფს პერსონალური მონაცემების ელექტრონული წესით დამუშავების ტექნიკურ მხარდაჭერას.

2. IT სამსახურმა უნდა უზრუნველყოს საინფორმაციო ტექნოლოგიების გამართული ფუნქციონირება პერსონალურ მონაცემთა დაცვის სტანდარტების მიხედვით. გარდა ამისა, მან უნდა უზრუნველყოს ტექნიკური მხარდაჭერა სპეციალური საჭიროების მქონე სტუდენტებისა და მასწავლებლებისთვის საჭირო სამუშაო გარემოს შესაქმნელად.

3. ეს წესი განსაზღვრავს მონაცემთა უსაფრთხო შენახვის პოლიტიკას, სატელეკომუნიკაციო პოლიტიკას, ტექნიკური აღჭურვილობის კონფიგურაციის პოლიტიკას, სტუმრების/ვიზიტორების წვდომის და აღჭურვილობის გამოყენების პოლიტიკას, ინფორმაციის მგრძნობელობის პოლიტიკას, პაროლის პოლიტიკას, პერსონალური იდენტიფიკაციის პოლიტიკას და სხვა.

4. მონაცემები ავტომატურად შეინახება/რეზერვდება ყოველდღიურად.

მუხლი 17. ხარისხის უზრუნველყოფის სამსახურის მიერ პერსონალური მონაცემების დამუშავება

1. ილიას სახელმწიფო უნივერსიტეტის ხარისხის უზრუნველყოფის სამსახური პერსონალურ მონაცემებს ამუშავებს თავისი ფუნქციური მოვალეობების შესრულების ფარგლებში. აღნიშნული საქმიანობა მოიცავს როგორც სტუდენტების, ისე კურსდამთავრებულების, აკადემიური და მოწვეული თანამშრომლების პერსონალურ მონაცემებზე წვდომას და მათ დამუშავებას ხარისხის მონიტორინგისა და შეფასების მიზნით.

2. მონაცემთა დამუშავება ხორციელდება სამართლებრივი საფუძვლის შესაბამისად, მხოლოდ განსაზღვრული და ლეგიტიმური მიზნებისთვის და შეესაბამება საქართველოს კანონმდებლობასა და პერსონალური მონაცემების დაცვის შესახებ წესებს. პერსონალური მონაცემების ნებისმიერი დამუშავება ემყარება მინიმალიზაციის, სიზუსტისა და

კონფიდენციალურობის პრინციპებს და ხორციელდება სათანადო ტექნიკური და ორგანიზაციული უსაფრთხოების ზომების დაცვით.

3. ხარისხის მართვის სამსახურის მიერ საუნივერსიტეტო კვლევების ფარგლებში დამუშავებული პერსონალური მონაცემები იშლება და ნადგურდება კვლევის ანგარიშის დასრულებიდან 6 (ექვსი) თვის ვადაში.

თავი მეექვსე. პერსონალური მონაცემების დამუშავება ელექტრონული სისტემების მეშვეობით

მუხლი 18. საქმისწარმოების ელექტრონულ სისტემებში პერსონალური მონაცემების დამუშავება და ინფორმაციის უსაფრთხოების უზრუნველყოფა

1. სასწავლო-საგანმანათლებლო მიზნებიდან გამომდინარე, ილიას სახელმწიფო უნივერსიტეტში სტუდენტების პერსონალური მონაცემები მუშავდება და ინახება „სტუდენტთა სწავლის საფასურის და საფასურიდან მიღებული შემოსავლების აღრიცხვის ელექტრონულ სისტემაში“ („ბილინგის სისტემა“) და არჩევანის გარემოს უზრუნველყოფის სისტემაში (არგუსი). წინამდებარე სისტემებში პერსონალური მონაცემების შენახვა, დამუშავება და სხვა პროცედურები განსაზღვრულია შესაბამის წესში.

2. ილიას სახელმწიფო უნივერსიტეტში საქმისწარმოების ავტომატიზებულ სისტემა (e-doc) მეშვეობით ხდება კორესპონდენციის რეგისტრაცია და მოძრაობა რომელიც შეიცავს პერსონალურ მონაცემს. სისტემაში უნივერსიტეტის პერსონალს აქვს საკუთარი პროფილი, რომელიც დაცულია შესაბამისი მომხმარებლითა და პაროლით. წინამდებარე სისტემის მეშვეობით პერსონალური მონაცემების დამუშავებაზე მოქმედებს პერსონალური მონაცემების დაცვის შესაბამისი წესები, რაც განსაზღვრულია ამ წესითა და შესაბამისი საკანონმდებლო რეგულაციების მიხედვით.

3. ილიას სახელმწიფო უნივერსიტეტი აერთიანებს აკადემიურ, კვლევით, სასწავლო პროცესში ჩართულ და ადმინისტრაციულ-დამხმარე პერსონალს. სამუშაო პროცესში პერსონალი იყენებს სამსახურებრივ ელექტრონულ ფოსტას (@iliauni.edu.ge), რაც ასევე საქმისწარმოების პროცესითაა განსაზღვრული და ამარტივებს ინფორმაციის მიმოცვლას. - პერსონალურის ელექტრონული ფოსტა დაცულია შესაბამისი პაროლით, რომელზე წვდომაც აქვს მხოლოდ მის მფლობელს. პერსონალს ეკრძალება ელექტრონული ფოსტის პაროლის გამჟღავნება ან მისი უმეთვალყურეოდ დატოვება, მათ შორის სხვა მოწყობილობაში (არაპირად კომპიუტერში) დატოვება.

თავი მეშვიდე. ინციდენტი

მუხლი 19. ინციდენტის ცნება და შინაარსი

1. ინციდენტი განისაზღვრება, როგორც ნებისმიერი მოვლენა, რომელიც იწვევს უნივერსიტეტის მიერ გადაცემული, შენახული ან სხვაგვარად დამუშავებული პერსონალური მონაცემების შემთხვევით ან უკანონო განადგურებას, დაკარგვას, შეცვლას, უნებართვო გამჟღავნებას ან წვდომას.

2. უნივერსიტეტის ყველა თანამშრომელი, სტუდენტი და მესამე მხარე ვალდებულია, ინციდენტის არსებობის შემთხვევაში დაუყოვნებლივ შეატყობინონ პერსონალურ მონაცემთა დაცვის ოფიცერს.

3. ინციდენტის შესახებ შეტყობინება შეიძლება გაკეთდეს ელექტრონული ფოსტით, ცხელი ხაზის ან სხვა საკომუნიკაციო საშუალებების მეშვეობით.

4. ინციდენტის შესახებ შეტყობინების მიღებისთანავე, პერსონალურ მონაცემთა დაცვის ოფიცერი ატარებს პირველად შეფასებას ინციდენტის ხასიათისა და სიმძიმის დასადგენად.

4.1. ინციდენტის შეფასება მოიცავს შემდეგ კომპონენტებს:

ა) დაზარალებული მონაცემთა სუბიექტების იდენტიფიცირება.

ბ) პერსონალური მონაცემების ტიპისა და მოცულობის შეფასება.

გ) მონაცემთა სუბიექტებზე პოტენციური ზემოქმედების შეფასება.

დ) ინციდენტის მიზეზის იდენტიფიცირება.

ე) ინციდენტის მოგვარების გზების იდენტიფიცირება.

4.2. ინციდენტის შესაჩერებლად და მონაცემთა სუბიექტებისთვის შესაძლო ზიანის შესამცირებლად, საჭიროების შემთხვევაში მიიღება დაუყოვნებლივი ზომები, როგორიცაა:

ა) დაზარალებული სისტემების იზოლირება.

ბ) გატეხილი ანგარიშების შეჩერება.

გ) დროებითი უსაფრთხოების ზომების განხორციელება და სხვა.

4.3. უნივერსიტეტში ინციდენტების შესახებ ჩანაწერები ინახება მინიმუმ ხუთი წლის განმავლობაში და პერიოდულად განიხილება ტენდენციების გამოსავლენად და უნივერსიტეტის მონაცემთა დაცვის პრაქტიკის გასაუმჯობესებლად.

4.4. უნივერსიტეტი შეატყობინებს შესაბამის ზედამხედველ ორგანოს ინციდენტისა და პერსონალური მონაცემების ნებისმიერი დარღვევის შესახებ 72 საათის განმავლობაში.

4.5. შეტყობინება ზედამხედველობის ორგანოსთვის მოიცავს შემდეგ კომპონენტებს:

ა) პერსონალური მონაცემების დარღვევის ბუნება.

ბ) კატეგორიები და მონაცემთა სუბიექტების სავარაუდო რაოდენობა.

გ) პერსონალური მონაცემების ჩანაწერების კატეგორიები და სავარაუდო რაოდენობა.

დ) პერსონალურ მონაცემთა დაცვის ოფიცრის ან სხვა რელევანტური პირის ვინაობა და საკონტაქტო ინფორმაცია.

ე) დარღვევის სავარაუდო შედეგები.

ვ) მიღებული ან/და შემოთავაზებული ზომები დარღვევის აღმოსაფხვრელად.

4.6. ინციდენტებიდან მიღებული გამოცდილება გამოყენებული იქნება უნივერსიტეტის მონაცემთა დაცვის საერთო სტრატეგიისა და ინციდენტებზე რეაგირების შესაძლებლობების გასაუმჯობესებლად.

4.7. უნივერსიტეტი უზრუნველყოფს თანამშრომლებისა და სტუდენტებისთვის რეგულარულ ტრენინგებსა და საინფორმაციო პროგრამებს მონაცემთა დაცვისა და ინციდენტებზე რეაგირების პროცედურების შესახებ.

მუხლი 20. ინციდენტის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულება

1. ილიას სახელმწიფო უნივერსიტეტი ვალდებულია, აღრიცხოს ინციდენტი, დამდგარი შედეგი, მიღებული ზომები და ინციდენტის აღმოჩენიდან არაუგვიანეს 72 საათისა მის შესახებ წერილობით ან ელექტრონულად შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს, გარდა იმ შემთხვევისა, როდესაც ნაკლებად სავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

2. ინციდენტთან დაკავშირებული სხვა ქმედებები და სამართლებრივი პროცედურები ხორციელდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 29-ე მუხლის შესაბამისად.

მუხლი 21. ადამიანის უფლებებისა და თავისუფლებების შელახვის სიმძიმის განსაზღვრის კრიტერიუმები

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

ა) მონაცემთა სუბიექტის დისკრიმინაცია (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) მონაცემთა სუბიექტის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული 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 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) არასრულწლოვანების, შეზღუდული შესაძლებლობების მქონე პირებისა და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე მონაცემთა სუბიექტ(ებ)ის პერსონალური მონაცემების უკანონო დამუშავება.

2. ინციდენტით მონაცემთა სუბიექტების უფლებებისადმი გამოწვეული შესაძლო შედეგის სიმძიმის შეფასების შემდეგ საჭიროა სსიპ - ილიას სახელმწიფო უნივერსიტეტის მიერ ამ შედეგის დადგომის ალბათობის განსაზღვრა.

3. შედეგის დადგომის ალბათობა შეიძლება იყოს დაბალი, საშუალო ან მაღალი.

თავი მერვე. პერსონალურ მონაცემთა დაცვის ოფიცერი

მუხლი 22. პერსონალურ მონაცემთა დაცვის ოფიცრის ცნება და ფუნქცია-მოვალეობანი.

1. პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკითხების, მათ შორის — შესაბამისი მარეგულირებელი ნორმების მიღებისა და ცვლილებების, პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელი და უფლებამოსილი პირებისა და მათი თანამშრომლების ინფორმირების, ასევე კანონით გათვალისწინებული სხვა მოქმედებების უზრუნველსაყოფად, უნივერსიტეტი ნიშნავს პერსონალურ მონაცემთა დაცვის ოფიცერს.
2. პერსონალურ მონაცემთა დაცვის ოფიცერი ანგარიშვალდებულია უნივერსიტეტის რექტორისა და ადმინისტრაციის ხელმძღვანელის წინაშე.
3. პერსონალურ მონაცემთა დაცვის ოფიცრის ფუნქციები განისაზღვროს შემდეგნაირად:
ა) მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე, მათ შორის, უნივერსიტეტის შიდა მარეგულირებელი სამართლებრივი აქტების მიღების ან შეცვლის შესახებ, უნივერსიტეტისა და მისი თანამშრომლების ინფორმირება, მათთვის კონსულტაციებისა და მეთოდური დახმარების გაწევა თავისი უფლებამოსილების ფარგლებში.
ბ) მონაცემთა დამუშავებასთან დაკავშირებული შიდა რეგულაციებისა და მონაცემთა დაცვის ზეგავლენის შეფასების დოკუმენტის შემუშავებაში მონაწილეობა.
გ) უნივერსიტეტის მიერ საქართველოს კანონმდებლობისა და შიდა ორგანიზაციული დოკუმენტების შესრულების მონიტორინგი, მათ შორის, მონაცემთა აღრიცხვა, მონაცემების დამუშავების იდენტიფიცირება და დოკუმენტების მომზადება (პოლიტიკის დოკუმენტები და სხვა).
დ) მონაცემთა დამუშავებასთან დაკავშირებით განცხადებებისა და საჩივრების განხილვა და შესაბამისი რეკომენდაციების გაცემა.
ე) კონსულტაციების მიღება პერსონალურ მონაცემთა დაცვის სამსახურისგან, უნივერსიტეტის წარმომადგენლობა პერსონალურ მონაცემთა დაცვის სამსახურთან ურთიერთობაში, მისი მოთხოვნით ინფორმაციისა და დოკუმენტების წარდგენა და მისი დავალებებისა და რეკომენდაციების შესრულების კოორდინაცია და მონიტორინგი.
ვ) მონაცემთა სუბიექტის მიმართვის შემთხვევაში მისთვის მონაცემთა დამუშავების პროცესებისა და უფლებების შესახებ ინფორმაციის მიწოდება.
ზ) ინციდენტის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურის ინფორმირება.
თ) უნივერსიტეტის მიერ მონაცემთა დამუშავების სტანდარტების ამაღლების მიზნით სხვა ფუნქციების შესრულება.
4. უნივერსიტეტი იღებს ვალდებულებას უზრუნველყოს პერსონალურ მონაცემთა დაცვის ოფიცრის სათანადო ჩართულობა მონაცემთა დამუშავებასთან დაკავშირებით მნიშვნელოვანი გადაწყვეტილებების მიღების პროცესში, უზრუნველყოს ის შესაბამისი რესურსებით, აგრეთვე დამოუკიდებლობით საქმიანობის განხორციელებისას.

თავი მეცხრე. დასკვნითი დებულებები

მუხლი 23. დასკვნითი დებულებები

1. ამ წესში განსაზღვრულია უნივერსიტეტში პერსონალური მონაცემების დამუშავების წესები და პროცედურები. ნებისმიერი საკითხი, რაც ამ წესში არ არის გაწერილი, გადაწყდება

საქართველოს კანონმდებლობის შესაბამისად მათ შორის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის და უნივერსიტეტში არსებული სხვა რეგულაციებით.
2. ამ წესს ამტკიცებს უნივერსიტეტის რექტორი.

3. ამ წესის გაუქმება, მასში ცვლილებებისა და დამატებების შეტანა შესაძლებელია უნივერსიტეტში არსებული შესაბამისი რეგულაციის შესაბამისად.

4. ეს წესი ძალაშია მისი დამტკიცების მომენტიდან.