შპს ქართულ-ამერიკული უნივერსიტეტის

მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი

შინაარსი

მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი 1

პრეამბულა 3

სამართლებრივი და რეგულატორული კონტექსტი 3

დოკუმენტის მნიშვნელობა მონაცემთა დამუშავების პროცესში 4

დოკუმენტში განხილული ძირითადი სფეროები მოიცავს: 4

ზოგადი ინფორმაცია მონაცემთა დამუშავებაზე პასუხისმგებელი პირის შესახებ 4

ზოგადი ინფორმაცია მონაცემთა დამუშავებაზე უფლებამოსილი პირებისა და თანანდამმუშავებლების შესახებ 5

სერვისის პროვაიდერები: 6

მონაცემთა სუბიექტები 6

შიდა დაინტერესებული მხარეები: 6

მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების მიზნები 7

მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების საფუძვლები 7

მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების დრო 7

მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის შენახვის ვადა 7

მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის გამოქვეყნება 8

ნაწილი I - მონაცემთა დამუშავების პროცესი **9**

მონაცემთა დამუშავების პროცესის აღწერა 9

მონაცემთა დამუშავების მასშტაბთან დაკავშირებული სხვა დამატებითი ინფორმაცია 15

მონაცემთა დამუშავების მასშტაბთან დაკავშირებული სხვა დამატებითი ინფორმაცია 18

მონაცემთა დამუშავების მიზანი და პრინციპები 19

ნაწილი II - ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეები და მათი ხარისხობრივი ანალიზი 21

მონაცემთა დამუშავების სახე: 21

მონაცემთა დამუშავების შესაძლო შედეგები 23

საფრთხეების შეფასება და მათზე რეაგირება 26

ნაწილი III - ინფორმაცია ზეგავლენის შეფასების პროცესში გამოყენებული მეთოდოლოგიის შესახებ 30

ზეგავლენის შეფასებისას გამოყენებული მეთოდოლოგია 30

პრეამბულა

შპს ქართულ-ამერიკული უნივერსიტეტის (შემდგომ - უნივერსიტეტი) მიერ პერსონალურ მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი შემუშავებულია „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის, პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის №21 ბრძანებით დამტკიცებული „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმები და შეფასების წესის" და კანონმდებლობით დადგენილი სხვა მოთხოვნების საფუძველზე. უნივერსიტეტის მიერ პერსონალურ მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი (შემდგომ - „დოკუმენტი") გამოიყენება უნივერსიტეტის მიერ სტუდენტების, აკადემიური პერსონალის, მოწვეული პერსონალის, კონტრაქტორებისა და სხვა თანამშრომლების პერსონალურ მონაცემთა დამუშავების პროცესში და ვრცელდება უნივერსიტეტის მიერ მონაცემების ნებისმიერი ფორმით დამუშავებაზე.

მონაცემთა დაცვაზე ზემოქმედების შეფასება (DPIA) ჩატარდა მონაცემთა სუბიექტების კონფიდენციალურობისთვის პოტენციური რისკების შესაფასებლად უნივერსიტეტში მონაცემთა დამუშავებასთან დაკავშირებით. დოკუმენტი მიზნად ისახავს მონაცემთა დაცვის ზოგად რეგულაციებთან (GDPR) და „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონთან შესაბამისობის უზრუნველყოფას და გამოვლენილი რისკის შესამცირებლად საჭირო ზომების მიღებას.

დოკუმენტი წარმოადგენს მონაცემთა დაცვისა და კონფიდენციალურობის უფრო ფართო ჩარჩოს ძირითად ელემენტს. იგი ხელს უწყობს კონკრეტული რისკების იდენტიფიცირებას ორგანიზაციის საქმიანობის სპეციფიკის გათვალისწინებით, ასევე, აღნიშნული რისკების პოტენციური გავლენის შეფასებას და მათ შესამცირებლად შესაბამისი პრევენციული ღონისძიებების გატარებას.

სამართლებრივი და რეგულატორული კონტექსტი

დოკუმენტი შემუშავებულია შემდეგი სამართლებრივი ჩარჩოების შესაბამისად:

ა) GDPR-ის 35-ე მუხლი, რომელიც ავალდებულებს ორგანიზაციას დოკუმენტის შემუშავებას, მაშინ როდესაც მონაცემთა დამუშავება, თავისი არსით, სავარაუდოა, რომ გამოიწვევს მონაცემთა სუბიექტების პერსონალური მონაცემების რაიმე სახით ხელყოფას და შესაბამისად, მათი ძირითადი უფლებებისა და თავისუფლებების შელახვას;

ბ) საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", რომელიც აწესებს მსგავს მოთხოვნებს პერსონალური მონაცემების დასაცავად, მათ შორის რისკების შეფასების და კონფიდენციალურობის პრინციპების უზრუნველყოფის ვალდებულებების ჩათვლით.

დოკუმენტის შემუშავების აუცილებლობა განსაკუთრებით მნიშვნელოვანია მაშინ, როდესაც მონაცემთა დამუშავება მოიცავს:

პირთა სისტემატურ მონიტორინგს (მაგ. ვიდეო მონიტორინგის საშუალებით).
განსაკუთრებული კატეგორიის მონაცემების ფართომასშტაბიან დამუშავებას, როგორიცაა ჯანმრთელობის ან ბიომეტრიული მონაცემები.
ტექნოლოგიის ინოვაციური გამოყენება, რამაც შეიძლება გავლენა მოახდინოს მონაცემთა კონფიდენციალურობაზე (მაგ., გადაწყვეტილების ავტომატური მიღება ან ხელოვნური ინტელექტის საფუძველზე დამუშავება).

დოკუმენტის მნიშვნელობა მონაცემთა დამუშავების პროცესში

დოკუმენტის შემუშავება აუცილებელია არა მხოლოდ ორგანიზაციის მიერ კანონთან შესაბამისობის უზრუნველსაყოფად, არამედ მონაცემთა სუბიექტებისა და დაინტერესებული მხარეების ნდობის გასამყარებლად. დოკუმენტის მიღებით, უნივერსიტეტი გამოხატავს მზაობას მონაცემთა დამუშავების გამჭვირვალობისა და ანგარიშვალდებულების მიმართ, ამცირებს მონაცემთა დარღვევის ან არასწორად გამოყენების რისკს და ორგანიზაციულ დონეზე ქმნის სამართლებრივ ჩარჩოს სუბიექტთა პერსონალურ მონაცემთა დასაცავად.

დოკუმენტი უზრუნველყოფს მონაცემთა დამუშავების თანმხლები და პოტენციური შედეგების ყოვლისმომცველ ანალიზს და ეხმარება ორგანიზაციას, ჩამოაყალიბოს და გამართოს ისეთი სამუშაო პროცესები, ტექნიკური სისტემები და პოლიტიკა, რომელიც იცავს პერსონალურ მონაცემებს. აღნიშნული პროაქტიული მიდგომა არა მხოლოდ აზღვევს ორგანიზაციას მარეგულირებელი სანქციებისგან, არამედ არეგულირებს ურთიერთობას კლიენტებთან, მომხმარებლებსა და თანამშრომლებთან მათი კონფიდენციალურობის დაცვის უზრუნველყოფის გზით.

დოკუმენტში განხილული ძირითადი სფეროები მოიცავს:

- მონაცემთა დამუშავების კანონიერებას;
- უნივერსიტეტის მიერ სუბიექტების შესახებ მოპოვებული ინფორმაციის დამუშავების აუცილებლობასა და პროპორციულობას;
- პოტენციური რისკების შეფასებას პირთა ძირითადი უფლებებისა და თავისუფლებების დასაცავად;
- ქმედით მექანიზმებს გამოვლენილი რისკების პრევენციისათვის;
- უნივერსიტეტის მიერ მონაცემთა დაცვის უზრუნველსაყოფად განხორციელებულ ღონისძიებებსა და ტექნიკურ გარანტიებს;
- მონაცემთა სუბიექტების და მონაცემთა დამუშავებაზე პასუხისმგებელი/უფლებამოსილი პირების უფლებებსა და ვალდებულებებს.

ზოგადი ინფორმაცია მონაცემთა დამუშავებაზე პასუხისმგებელი პირის შესახებ

შპს ქართულ-ამერიკული უნივერსიტეტი წარმოადგენს უმაღლეს საგანმანათლებლო დაწესებულებას, რომელიც საკუთარი ფუნქციების შესრულებისათვის ამუშავებს სტუდენტების, აკადემიური პერსონალის, მოწვეული პერსონალის, კონტრაქტორებისა და სხვა თანამშრომლების მონაცემებს, მათ შორის არასრულწლოვნის მონაცემებსაც. საკუთარი უფლებამოსილებისა და მოვალეობების სრულფასოვნად შესრულებისათვის უნივერსიტეტს ესაჭიროება პერსონალურ მონაცემთა სუბიექტების პერსონალურ მონაცემთა დამუშავება. აღნიშნული პროცესი იწყება აბიტურიენტთა უნივერსიტეტში რეგისტრაციის დღიდან და გრძელდება მთელი სასწავლო პროცესის მანძილზე, ასევე, შესაბამისი ხელშეკრულებების ვადით, დასაქმებულების/სხვა ფიზიკური პირების შემთხვევაში. სუბიექტთა შესახებ დამუშავებული მონაცემები მოიცავს სტუდენტების, ლექტორებისა და სხვა თანამშრომლების პირადი მონაცემების, სტუდენტის უნივერსიტეტში სწავლის განმავლობაში მისი შეფასებისა და აქტიურობის შესახებ ინფორმაციებს.
უმაღლესი განათლების უზრუნველყოფის მიზნებისათვის მონაცემთა დამუშავების პროცესში უნივერსიტეტი ერთიანი სისტემის ნაწილია, რომელშიც ჩართულია საქართველოს განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტრო და მის დაქვემდებარებაში არსებული საჯარო სამართლის იურიდიული პირები, რომლებიც საკუთარი უფლებამოსილებების ფარგლებში განსაზღვრავენ მონაცემთა

დამუშავების ფორმასა და მიზნებს. ამრიგად, უნივერსიტეტში მონაცემები მუშავდება როგორც ელექტრონული პლატფორმების, ასევე - ქაღალდურ მატარებლებზეც. პერსონალური მონაცემების დაცვა საუნივერსიტეტო საზოგადოების ყველა წევრის უფლებაა, შესაბამისად მონაცემთა დამუშავება მკაფიოდ რეგლამენტირებული პროცესია და უნივერსიტეტი უზრუნველყოფს ყველა წევრის პერსონალური მონაცემების დაცვას, რისთვისაც მას შემუშავებული აქვს პერსონალურ მონაცემთა დამუშავების წესი და განსაზღვრული ჰყავს პერსონალურ მონაცემთა დაცვის ოფიცერი.

ზოგადი ინფორმაცია მონაცემთა დამუშავებაზე უფლებამოსილი პირებისა და თანანდამმუშავებლების შესახებ

უნივერსიტეტს ჰყავს მონაცემთა დამუშავებაზე უფლებამოსილი პირები, რომლებიც პერსონალურ მონაცემებს ამუშავებენ მხოლოდ უნივერსიტეტის მიზნების განსახორციელებლად. უნივერსიტეტს და მონაცემთა დამუშავებაზე უფლებამოსილ პირებს შორის გაფორმებულია ხელშეკრულებები, რომლებიც მოიცავს პერსონალურ მონაცემთა დაცვის საკითხების დეტალურ მოწესრიგებას და დამუშავებაზე უფლებამოსილ პირებს ავალდებულებს იმოქმედონ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან სრული შესაბამისობით. წერილობითი შეთანხმება ასევე მოიცავს იმ საკითხებს, რომლებიც გათვალისწინებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 36-ე მუხლის მე-2-3 პუნქტებით.

უნივერსიტეტი ახორციელებს დამუშავებაზე უფლებამოსილი პირების მიერ მისი ფუნქცია-მოვალეობების შესრულებისას ტექნოლოგიურ-ორგანიზაციული ზომებისა და მონაცემების დამუშავების მონიტორინგს. მოთხოვნის შემთხვევაში, უნივერსიტეტი უზრუნველყოფს მონაცემთა სუბიექტებისთვის დამუშავებაზე უფლებამოსილი პირების შესახებ ინფორმაციის მიწოდებას.

უფლებამოსილი პირები თავად არ წარმოადგენენ მონაცემთა დამუშავებისათვის პასუხისმგებელ პირებს, რადგან მათ მიერ მონაცემების დამუშავება ემსახურება სხვა კლიენტი ორგანიზაციების მიზნებს და მონაცემთა დამუშავების კონკრეტული საშუალებები განისაზღვრება კლიენტი ორგანიზაციის მითითების შესაბამისად. აქედან გამომდინარე, მონაცემთა დამუშავების კონტექსტში უფლებამოსილი პირები მონაცემებს ამუშავებენ დამუშავებისთვის პასუხისმგებელი პირისთვის ან მისი სახელით.

მონაცემთა დამუშავებაზე უფლებამოსილი პირები პასუხისმგებლები არიან მხოლოდ იმ მონაცემთა უსაფრთხოებაზე, რასაც ის ამუშავებენ და იმ ვადით, რა ვადითაც აღნიშნული მონაცემები მუშავდება.

უნივერსიტეტს ჰყავს მონაცემთა თანადამმუშავებელი პირებიც. შპს ფიტპასს ჯორჯია, შპს სადაზღვევო კომპანია „ევროინსი“ და სს საქართველოს ბანკი უზრუნველყოფენ უნივერსიტეტს შესაბამისი მომსახურებით. კერძოდ, კომპანია „ფიტპასს“ უნივერსიტეტს სთავაზობს კორპორატიულ მომსახურებას, რომლის ფარგლებშიც უნივერსიტეტის თანამშრომლებს შეუძლიათ დაკავდნენ 40-ზე მეტი სპორტული აქტივობით, 150-ზე მეტ ობიექტში, ყოველღიურად, თვეში ერთი სააბონენტო გადასახადით. უნივერსიტეტი უზრუნველყყოფს ასეთ დროს სუბიექტებისგან პერსონალური მონაცემების გადაცემასა და დამუშავებაზე თანხმობის მიღებას მათ მიერ ელექტრონული კითხვარის შევსების მეშვეობით. სადაზღვევო კომპანია „ევროინსს“ კი უზრუნველყოფს უნივერსიტეტის თანამშრომლებს შესაბამისი სადაზღვევო მომსახურებით. რაც შეეხება სს საქართველოს ბანკს, უნივერსიტეტი თნამშრომლობს მასთან სახელფასო ბარათის შეკვეთის მიზნებისთვის.
შპს ფიტპასს ჯორჯია, შპს სადაზღვევო კომპანია „ევროინსი“ და სს საქართველოს ბანკი წარმოადგენენ მონაცემთა თანადამმუშავებელ პირებს, რადგან მათ მიერ მონაცემების დამუშავება ემსახურება საკუთარ ორგანიზაციულ მიზნებს და მონაცემთა დამუშავების კონკრეტული საშუალებები განისაზღვრება მათი მითითების შესაბამისად.

აქედან გამომდინარე, მონაცემთა დამუშავების კონტექსტში ზემოაღნიშნული კომპანიები გამოდიან, როგორც თანადამმუშავებელი პირები, რომლებიც მონაცემებს ამუშავებენ საკუთარი ორგანიზაციისთვის და საკუთარი სახელით. კომპანიებს, როგორც თანადამმუშავებელ პირებსა და დამუშავებისათვის პასუხისმგებელ პირს შორის ფორმდება შესაბამისი ხელშეკრულება (წერილობითი შეთანხმება), რომლითაც განისაზღვრება მონაცემთა დამუშავების საფუძვლები და მიზნები, დასამუშავებელ მონაცემთა კატეგორიები, მონაცემთა დამუშავების ვადა და დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის უფლებები და ვალდებულებები. წერილობითი შეთანხმება ასევე მოიცავს იმ საკითხებს, რომლებიც გათვალისწინებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 36-ე მუხლის მე-2-3 პუნქტებით.
შპს ფიტპასს ჯორჯია, შპს სადაზღვევო კომპანია „ევროინსი“ და სს საქართველოს ბანკი, როგორც თანადამმუშავებელი პირები, პასუხისმგებლები არიან მხოლოდ იმ მონაცემთა უსაფრთხოებაზე, რასაც ისინი ამუშავებენ და იმ ვადით, რა ვადითაც აღნიშნული მონაცემები მუშავდება.

სერვისის პროვაიდერები:

ორგანიზაციები, რომლებიც დაამუშავებენ პერსონალურ მონაცემებს უნივერსიტეტის სახელით, როგორიცაა ღრუბლოვანი საცავის პროვაიდერები, IT მხარდაჭერის მომწოდებლები ან მარკეტინგული სააგენტოები, ვალდებულნი არიან მონაცემთა დამუშავების ხელშეკრულებებით (DPA) უზრუნველყონ მონაცემთა დაცვის მოთხოვნების დაცვა.
საზედამხედველო ორგანოები: შესაბამისობის კონტექსტში, მონაცემთა დაცვის შესაბამის სამეთვალყურეო ორგანოს (მაგ., საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორს ან ეკვივალენტურ GDPR ორგანოებს) შეუძლია ზედამხედველობა გაუწიოს დამუშავების აქტივობების კანონიერებას, განსაკუთრებით იმ შემთხვევებში, როდესაც საქმე ეხება მაღალი რისკის დამუშავებას.

მონაცემთა სუბიექტები

უნივერსიტეტი ამუშავებს შემდეგი ფიზიკური პირების პერსონალურ მონაცემებს:
ა) მოქმედი და ყოფილი თანამშრომლები, მათ შორის, შრომითი ხელშეკრულებით დასაქმებული პირები;
ბ) ვაკანტური პოზიციების დასაკავებლად გამოცხადებულ კონკურსში მონაწილე კანდიდატები;
გ) სტაჟიორები;
დ) სტუდენტები, ადმინისტრაციული და აკადემიური პერსონალი;
ე) მოწვეული პერსონალი;
ვ) ვიზიტორები;
ზ) არასრულწლოვნები;
თ) ვიდეომონიტორინგის არეალში მოხვედრილი სხვა პირები;
ი) კონტრაქტორები (როგორც კერძო სამართლის იურდიული პირი, ასევე საჯარო სამართლის და ფიზიკური პირი);
კ) პროექტების ფარგლებში საინფორმაციო სესიებზე მოსული პირები.

შიდა დაინტერესებული მხარეები:

მონაცემთა დაცვის ოფიცერი (DPO): პასუხისმგებელია უნივერსიტეტის მონაცემთა დაცვის სტრატეგიის ზედამხედველობაზე და კონფიდენციალურობის კანონებთან შესაბამისობის უზრუნველყოფაზე.
ადამიანური რესურსები (HR): ჩართულია თანამშრომელთა მონაცემების დამუშავებაში დაქირავების, მუშაობის მენეჯმენტისა და სახელფასო ჩამონათვალისთვის.
მარკეტინგის გუნდი: პასუხისმგებელია მომხმარებელთა მონაცემების დამუშავებაზე ქცევის გასაანალიზებლად, კამპანიების დასაწყებად და კომუნიკაციის შესანარჩუნებლად.

IT დეპარტამენტი: მართავს ტექნიკურ ინფრასტრუქტურას, რომელიც მხარს უჭერს პერსონალური მონაცემების შეგროვებას, შენახვას და უსაფრთხოებას.
იურიდიული დეპარტამენტი: უზრუნველყოფს მითითებებს მონაცემთა დაცვის რეგულაციებთან შესაბამისობაში, აკონტროლებს მონაცემთა დამუშავების ხელშეკრულებებს და მართავს მონაცემთა სუბიექტის უფლებებს.

მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების მიზნები

მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი ხელს უწყობს დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა დამუშავებისას უზრუნველყოს:

1. მონაცემთა დამუშავების საწყის ეტაპზე მონაცემთა მიმართ არსებული საფრთხეების პროაქტიულად გათვალისწინება;
2. მონაცემთა დამუშავების შედეგად, ადამიანის ძირითადი უფლებებისა და თავისუფლებების მიმართ წარმოშობილი საფრთხეების იდენტიფიცირება, შეფასება და არსებითად შემცირება;
3. კანონიერი და სამართლიანი გადაწყვეტილების მიღება მონაცემთა დამუშავების პროცესის დაწყების თაობაზე;
4. ყველა დაინტერესებული პირის ჩართვა მონაცემთა დამუშავების პროცესში და მათი ინფორმირება აღნიშნულ საკითხებზე;
5. მონაცემთა დამუშავების გამჭვირვალობა;
6. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონითა და საერთაშორისო რეგულაციებით გათვალისწინებულ ვალდებულებებთან შესაბამისობა.

მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების საფუძვლები

მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელება სავალდებულოა, თუ:
1. მონაცემთა დამუშავებისას ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე;
2. დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტისთვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებს სრულად ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე;
3. დამუშავებისთვის პასუხისმგებელი პირი ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემებს;
4. დამუშავებისთვის პასუხისმგებელი პირი ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში.

მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების დრო

ზეგავლენის შეფასება ხორციელდება მონაცემთა დამუშავების პროცესის დაწყებამდე ან მისი ცვლილების/განახლების შემთხვევაში.

მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის შენახვის ვადა

უნივერსიტეტი ვალდებულია ზეგავლენის შეფასების დოკუმენტი შეინახოს მონაცემთა დამუშავების მთელი პერიოდის განმავლობაში, ხოლო მონაცემთა დამუშავების შეწყვეტის შემთხვევაში – არანაკლებ 1 წლის ვადით.

მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის გამოქვეყნება

საზოგადოებაში მაღალი ნდობის მქონე დაწესებულების რეპუტაციის მოპოვების, კანონმდებლობასთან შესაბამისობის, ანგარიშვალდებულებისა და გამჭვირვალობის პრინციპების დაცვის დემონსტრირების ინტერესიდან გამომდინარე, მონაცემთა დაცვის ზეგავლენის დოკუმენტი ექვემდებარება გასაჯაროებას, გარდა იმ შემთხვევებისა თუ ამით შეიძლება საფრთხე შეექმნას:
ა) სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესებს;
ბ) საზოგადოებრივი უსაფრთხოების ინტერესებს;
გ) დანაშაულის თავიდან აცილებას;
დ) ოპერატიულ-სამძებრო საქმიანობას;
ე) დანაშაულის გამოძიებას;
ვ) სისხლისსამართლებრივ დევნას;
ზ) მართლმსაჯულების განხორციელებას;
თ) პატიმრობისა და თავისუფლების აღკვეთის აღსრულებას;
ი) არასაპატიმრო სასჯელთა აღსრულებას და პრობაციას;
კ) ქვეყნისთვის მნიშვნელოვან ფინანსურ ან ეკონომიკურ (მათ შორის, მონეტარულ, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესებს;
ლ) დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის აღმატებულ ლეგიტიმურ ინტერესებს.

დამუშავებისთვის პასუხისმგებელი პირი	
სახელწოდება	ქართულ-ამერიკული უნივერსიტეტი
სამართლებრივი ფორმა	შპს
მონაცემთა დაცვის ოფიცერი	შპს „სეიფთი ქორფ“
საკონტაქტო პირი	(+995 32) 220 65 20; tamarrobakidze@gau.edu.ge; info@gau.edu.ge

ნაწილი I - მონაცემთა დამუშავების პროცესი

მონაცემთა დამუშავების პროცესის აღწერა
მონაცემთა მიღების წყაროები: უნივერსიტეტისთვის პერსონალურ მონაცემთა მიღების წყაროებია: უნივერსიტეტისთვის პერსონალურ მონაცემთა მიღების წყაროებია: ა) მონაცემთა სუბიექტის აშკარა, აქტიურად გამოვლენილი თანხმობის (ასევე, რეკრუტინგის, გარიგების, სტუდენტის რეგისტრაციის) საფუძველზე მონაცემების მიწოდება; ბ) ვიდეომონიტორინგის განხორციელების გზით მოპოვებული მონაცემები; გ) უნივერსიტეტის ვებ-საიტიდან მიღებული მონაცემები, რომელშიც სუბიექტი ავსებს სახელს გვარს, ტელეფონის ნომერს, ელექტრონული ფოსტის მისამართს; დ) უცხოელი სტუდენტების აგენტებისაგან, რომლებიც ახდენენ სტუდენტების ჩარიცხვასთან დაკავშირებული პროცედურების წარმოებას ჩარიცხვის მსურველი პირების ნების შესაბამისად; ე) უმაღლესი განათლების მართვის საინფორმაციო სისტემიდან მონაცემების მიღება; ვ) სასწავლო პროცესის მიმდინარეობისას მონაცემთა შექმნა (პირადი საქმის, სასწავლო პროცესის მართვის ელექტრონული სისტემის („გონი“), დისტანციური სწავლების მოდულის და სხვა საშუალებებით); ზ) Google-ის სააპლიკაციო ფორმის მეშვეობით მონაცემების მიღება; თ) უცხოელი აპლიკანტების სარეგისტრაციო ფორმებიდან მონაცემების მიღება (https://docs.google.com/forms/d/e/1FAIpQLSeObaFFOVE635-U-nJL6GoRdTl0EobWsuvrV24h7Qo8TkBpGA/viewform); ი) საკონსულტაციო სააგენტოების ელ. ფოსტა, რომლის მეშვეობითაც იგზავნება admissions.gau.edu.ge-ს მეილ-ჯგუფთან სტუდენტის პასპორტისა და საგანმანათლებლო დოკუმენტების სკანირებული ვერსიები; კ) შპს ჯეოლაბის ვებგვერდის საშუალებით რეგისტრაცია - სარეგისტრაციო ფორმის შევსების შედეგად მონაცემების მიღება; ლ) უნივერსიტეტის „პერსონალურ მონაცემთა დამუშავების პოლიტიკის“ ან/და კანონით განსაზღვრული მიზნებით ნებისმიერი კანონიერი წყაროდან ინფორმაციის მოპოვება. **მონაცემთა შენახვა და მისი ვადები:** 1. უნივერსიტეტი ინახავს მხოლოდ იმ მონაცემებს, რომლებიც აუცილებელია მონაცემთა დამუშავების კონკრეტული, კანონიერი მიზნის მისაღწევად. 2. პერსონალური მონაცემები ინახება ფაილურ სისტემაში იმ ვადით, რომლითაც მიიღწევა ლეგიტიმური მიზანი პერსონალურ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისა და მონაცემთა სუბიექტებისთვის გათვალისწინებული საფუძვლით. 2. განსაკუთრებული კატეგორიის მონაცემები ინახება ავტომატური და არაავტომატური საშუალებებით იმ ვადით, რომლითაც მიიღწევა ლეგიტიმური მიზანი პერსონალურ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისა და მონაცემთა სუბიექტებისთვის გათვალისწინებული საფუძვლით. 3. მონაცემები ინახება კანონმდებლობით განსაზღვრული ვადების შესაბამისად. მონაცემთა შენახვის ვადებისა და წესის განსაზღვრის საჭიროების შემთხვევაში, უნივერსიტეტი ითვალისწინებს პერსონალურ მონაცემთა დამუშავების პრინციპებს. 4. უნივერსიტეტში მონაცემთა მატერიალური ფორმით შენახვისათვის დადგენილია შემდეგი ვადები: ა) სტუდენტის პირადი საქმეები ინახება 75 წლის ვადით; ბ) თანამშრომელთა პირადი საქმეები ინახება 75 წლის ვადით;

გ) სტუდენტთა საბაკალავრო, სამაგისტრო და სადოქტორო ნაშრომები ინახება 75 წლის ვადით;
დ) თანამშრომელთა სამუშაო დროის აღრიცხვის დოკუმენტები ინახება 3 წლის ვადით, ხოლო სამუშაო დროის სააღრიცხვო ტაბელები (გრაფიკები), ჟურნალები 1 წლის ვადით;
ე) სტუდენტების საგამოცდო ნაშრომები ინახება 3 წლის ვადით;
ვ) სტუდენტთა განცხადებები ინახება 3 წლის ვადით;
ზ) კოლეგიური ორგანოებს - აკადემიური საბჭოს და ადმინისტრაციული საბჭოს გადაწყვეტილებები ინახება მუდმივად;
თ) კოლეგიური ორგანოების - აკადემიური საბჭოს და ადმინისტრაციული საბჭოს სხდომის ოქმები ინახება 3 წლის ვადით;
ი) ბრძანებები ძირითადი საქმიანობის ინახება მუდმივად;
ი.1) პირადი შემადგენლობის ბრძანებები ინახება 75 (სამოცდათხუთმეტი) წლის ვადით;
ი.2) ადმინისტრაციულ სამეურნეო საკითხების ბრძანებები ინახება 5 (ხუთი) წლის ვადით;
კ) ხელშეკრულებები ინახება 5 (ხუთი) წლის ვადით;
კ.1) შრომითი ხელშეკრულებები (კონტრაქტები) – 75 წლის ვადით;
კ.2) ხელშეკრულებები, შეთანხმებები, კონტრაქტები - მომარაგება-გასაღებაზე, ყიდვა-გაყიდვაზე - 6 წლის ვადით;
კ.3) მომსახურების ხელშეკრულებები 6 წლის ვადით;
ლ) გასული წერილები ინახება 5 (ხუთი) წლის ვადით;
მ) მიღება-ჩაბარების აქტები ინახება 6 (ექვსი) წლის ვადით;
ნ) თანამშრომელთა განცხადებები ინახება 75 (სამოცდათხუთმეტი) წლის ვადით;
ნ.1) თანამშრომელთა პირად საქმეში არ შესული განცხადებები ინახება 5 (ხუთი) წლის ვადით;
ო) განცხადებები ვაკანტური თანამდებობების დასაკავებლად კონკურსში მონაწილეობის შესახებ 3 (სამი) წლის ვადით;
პ) ბრძანებები ვაკანსიის გამოცხადების თაობაზე ინახება 3 (სამი) წლის ვადით;
ჟ) ფინანსური ანგარიშგებები ინახება 5 (ხუთი) წლის ვადით.
5. შენახვის ვადის გასვლის შემდეგ მატერიალური ფორმით არსებული დოკუმენტები ნადგურდება, რის შესახებაც დგება შესაბამისი აქტი - განადგურების ოქმი.

მონაცემებზე წვდომა:
1. თანამშრომლებს წვდომა აქვთ მხოლოდ იმ მონაცემებზე და იმ ფარგლებში, რაც აუცილებელია მათი მოვალეობების შესასრულებლად. თანამშრომლის შვებულების ან სხვა მიზეზით მოვალეობის შესრულების შემთხვევაში მოვალეობის შემსრულებელს აქვს წვდომა ასევე იმ პირის წვდომის ფარგლებში, ვის მოვალეობასაც ასრულებს, მოვალეობის შესრულების ბრძანებაში განსაზღვრულ ფარგლებში და წესით.
2. უნივერსიტეტის სასწავლო პროცესის მართვის ელექტრონულ სისტემაზე წვდომა აქვს:
ა) დეკანატის თანამშრომლებს;
ბ) აკადემიური პროცესის მართვის სამსახურს;
გ) იურიდიულ სამსახურს (შეზღუდული წვდომა);
დ) საფინანსო სამსახურს (შეზღუდული წვდომა);
ე) ადამიანური რესურსების მართვის სამსახურს (შეზღუდული წვდომა);
ვ) საქმისწარმოების სამსახურს (შეზღუდული წვდომა);
ზ) მარკეტინგისა და კომუნიკაციის სამსახურს (შეზღუდული წვდომა);
თ) სტრატეგიული განვითარების სამსახურს (შეზღუდული წვდომა).
3. უნივერსიტეტის საფინანსო აღრიცხვის სისტემაზე წვდომა აქვს ფინანსურ სამსახურს, რომელსაც წვდომა ადამიანური რესურსების მართვის სამსახურის უფროსის ნებართვით, ასევე, შესაძლოა ჰქონდეთ დასაქმებულთა იმ მონაცემების შესახებ, რომლებიც საჭიროა ანაზღაურების გასაცემად.
4. უნივერსიტეტში სტუდენტებისთვის განკუთვნილ საბარათე სისტემაზე წვდომა აქვს შესაბამისი სკოლის დეკანსა და ადმინისტრაციას, IT სამსახურს, მარკეტინგის სამსახურს და საგამოცდო ცენტრის თანამშრომლებს.

5. admissions.gau.edu.ge-ს მეილ-ჯგუფზე წვდომა აქვთ მხოლოდ სტუდენტთა მიღების ოფისის მენეჯერებს.
6. უნივერსიტეტის სასწავლო ცენტრის - შპს ჯეოლაბის მონაცემები ინახება უნივერსიტეტის Google Drive-ზე, რომელზე წვდომაც უნივერსიტეტის თანამშრომლებს აქვთ.
7. Google Meet-ზე წვდომა დისტანციური შეხვედრებისას აქვთ სტუდენტებს, ლექტორებს და ნებისმიერ სხვა პირს, რომელიც სარგებლობს უნივერსიტეტის კორპორატიული მეილით.
8. თანამშრომლის პირად საქმეებზე (მატერიალური დოკუმენტები) ან/და პირად საქმეში არსებულ საქმის მასალებზე წვდომის უფლება აქვს პერსონალის მართვის სამსახურს, პირადი საქმის წარმოებისა და მასში შესაბამისი ინფორმაციის შეტანის მიზნით.
9. კოლეგიური ორგანოების სხდომის ოქმებზე წვდომის უფლება აქვს კანცელარიას მათი აღრიცხვისა და შენახვის მიზნით.
10. დოკუმენტბრუნვის სისტემაზე და მასში არსებულ ინფორმაციაზე:
ა) სრული წვდომის უფლება აქვს - კანცელარიასა და იურიდიულ სამსახურს შემოსული კორესპონდენციის განაწილებისა და სათანადო რეაგირების უზრუნველყოფის მიზნით;
ბ) შეზღუდული წვდომის უფლება აქვთ - პერსონალის მართვის სამსახურსა და საფინანსო სამსახურს მათზე განაწილებული კორესპონდენციის განხილვისა და შესაბამისი პასუხების მომზადების მიზნით.

მონაცემთა გადაცემა/გამჟღავნება:
1. უნივერსიტეტის მიერ დამუშავებული მონაცემები სამართლებრივი საფუძვლის არსებობის შემთხვევაში კანონმდებლობით დადგენილი წესითა და მოცულობით შეიძლება გადაეცეს შემდეგ მესამე პირებს:
ა) სამართალდამცავ ორგანოებს;
ბ) სასამართლოს;
გ) პერსონალურ მონაცემთა დაცვის სამსახურს;
დ) კანონმდებლობით დადგენილ სხვა გათვალისწინებულ ორგანოებს.
2. მონაცემი შესაძლოა ასევე გადაცეს:
ა) განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტროს;
ბ) იუსტიციის სამინისტროს;
გ) თავდაცვის სამინისტროს;
დ) სამართალდამცავ სტრუქტურებს;
ე) სამთავრობო ან/და ადგილობრივი თვითმმართველობის ორგანოებს კანონით განსაზღვრულ შემთხვევებში;
ვ) საერთაშორისო ორგანიზაციას, როცა ეს აუცილებელია აკადემიური, ადმინისტრაციული მიზნებისთვის სტუდენტებისა და დასაქმებულების საუკეთესო ინტერესებიდან გამომდინარე;
ზ) უმაღლესი საგანმანათლებლო აქტივობების ორგანიზატორებს;
თ) საქართველოს განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტროს სისტემაში არსებულ სსიპ - განათლების ხარისხის განვითარების ეროვნულ ცენტრს;
ი) სსიპ - განათლების მართვის საინფორმაციო სისტემას;
კ) სსიპ - შემოსავლების სამსახურს;
ლ) აუდიტორულ კომპანიებს;
მ) კომპანია „ფიტპასს“ (უნივერსიტეტი უზრუნველყყოფს ასეთ დროს სუბიექტებისგან პერსონალური მონაცემების გადაცემასა და დამუშავებაზე თანხმობის მიღებას მათ მიერ ელექტრონული კითხვარის შევსების მეშვეობით);
ნ) სადაზღვევო კომპანია „ევროინსს“ (სუბიექტის თანხმობა ვლინდება ხელშეკრულებაზე ხელმოწერით);
ო) ადამიანური რესურსების მართვის ციფრული პორტალი HR Digital Co.;
პ) ბანკს სახელფასო ბარათის შეკვეთის მიზნით;
ჟ) სსიპ - შეფასებისა და გამოცდების ეროვნულ ცენტრს;
რ) სხვა უმაღლესი საგანმანათლებლო დაწესეულებას მობილობის მიზნებისთვის.
2[1]. უნივერსიტეტის კვლევის განვითარების და ხელშეწყობის სამსახური უნივერსიტეტის მიერ

ორგანიზებულ ღონისძიებებზე და კურსებზე დამსწრეთა რეგისტრაციებსა და ფოტოებს აწვდის დონორს პროექტის ფარგლებში.
2^2. უნივერსიტეტი მონაცემებს ამუშავებს სტატისტიკის მიზნითაც: სტრატეგიული განვითარების სამსახური წლის განმავლობაში ახორციელებს რამდენიმე ტიპის კვლევას. ხორციელდება სემესტრული გამოკითხვა სტუდენტებისთვის და მუშავდება თვითადმინისტრირებადი კითხვარი, რომელიც მიბმულია სტუდენტთა პორტალზე. ანალიზისითვის მიზნებისთვის მონაცემთა დაჯგუფება ხდება მოქალაქეობის, საფეხურის, პროგრამის, კურსის და ჯგუფის მიხედვით. ყოველწიური გამოკითხვისას გამოიყენება თვითადმინისტრირებადი კითხვარი google form-ის პლატფორმაზე, რომელიც სტუდენტებს ეგზავნებათ იმეილების მეშვეობით. მონაცემების სტატისტიკური დამუშავების შემდეგ უნივერსიტეტი აკეთებს რაპორტს და ელ. ფოსტის მეშვეობით უგზავნის შესაბამის დონორებს, სკოლებს/დეპარტამენტებს/სამსახურებს.
2^3. უნივერსიტეტის უცხოელ სტუდენტთა მიღების ოფისი მარკეტინგულ მასალებზე წვდომის უფლებას ანიჭებს საკონსულტაციო კომპანიებს. წვდომის დონე განისაზღვრება ხელმძღვანელობის მიერ და ექვემდებარება ადმინისტრატორის მონიტორინგს.
3. უნივერსიტეტი იყენებს მესამე პირს მომსახურების გაწევის პროცესში დახმარების, შიდა ინფორმაციული ტექნოლოგიების სისტემების გამართული მუშაობისა და მართვისათვის;
4. ამ მუხლის 1-2^3 პუნქტებით გათვალისწინებულ შემთხვევებში ინფორმაციის გამჟღავნებისას უნივერსიტეტი ახდენს სუბიექტთა ინფორმირებას. ამასთან, აღრიცხავს, თუ რომელი მონაცემი იქნა გამჟღავნებული, ვისთვის, როდის და რა სამართლებრივი საფუძვლით. აღნიშნული ინფორმაცია ინახება სუბიექტის შესახებ მონაცემებთან ერთად მათი შენახვის ვადის განმავლობაში.
5. უნივერსიტეტი სარგებლობს პორტალით - DHR.ge, რომელიც უნივერსიტეტს უზრუნველყოფს შესაბამისი ელექტორნული ბაზით, რომელშიც ხდება ადამიანური რესურსების მართვისთვის აუცილებელი ინფორმაციების (მათ შორის, პირადი და საკონტაქტო ინფორმაციის, ანაზღაურების, სამუშაო განაკვეთის, დასწრების აღრიცხვისა და შვებულებების) გაზიარება.

ვიდეო მონიტორინგი:
1. უნივერსიტეტი ვიდეომონიტორინგის სისტემას იყენებს კანონით დაკისრებული ვალდებულებების შესასრულებლად - პირის უსაფრთხოებისა და საკუთრების დაცვის, აგრეთვე, არასრულწლოვანთა მავნე ზეგავლენისაგან დაცვის მიზნებისთვის.
2. მონაცემთა დამუშავების შესახებ მონაცემთა სუბიექტების ინფორმირების მიზნით შენობაში თვალსაჩინო ადგილებში განთავსებულია შესაბამისი გამაფრთხილებელი ნიშნები და პერსონალური მონაცემების დამუშავებაზე პასუხისმგებელი პირის საკონტაქტო ინფორმაცია.
3. უნივერსიტეტი უზრუნველყოფს იმ თანამშრომელთა სათანადო წესით ინფორმირებას, რომელთა სამუშაო სივრცეც ექცევა ვიდეომონიტორინგის სისტემის ხედვის არეალში.
4. ვიდეო მონიტორინგის სისტემა და ჩანაწერები დაცულია არამართლზომიერი წვდომისა და გამოყენებისაგან. წვდომაზე უფლებამოსილი პირია დაცვის სამსახურის უფროსი. მასზე წვდომა დაცულია მომხმარებლის სახელითა და პაროლით. უნივერსიტეტი უზრუნველყოფს ვიდეოჩანაწერებზე წვდომის თითოეული შემთხვევის აღრიცხვას, მათ შორის, წვდომის დროისა და მომხმარებლის სახელის აღრიცხვას, რომელიც წვდომის განმახორციელებელი პირის იდენტიფიცირების შესაძლებლობას იძლევა.
5. ვიდეო მონიტორინგის სისტემა დაცულია შიფრაციის ფუნქციით და აღჭურვილია შესაბამისი თვითგანადგურების მექანიზმით. კამერის მონიტორები განთავსებულია დაცვის ოთახში, რომელიც იკეტება გასაღებით. შემუშავებულია გასაღებსა და ვიდეო მონიტორინგით მოპოვებულ მონაცემებზე წვდომის ავტორიზაციის მქონე პირთა წრე, რომელსაც წარმოადგენს დაცვის თანამშრომელი. ამას გარდა, საგამოცდო პერიოდში გამოცდის მიმდინარეობისას საგამოცდო აუდიტორიას ვიდეომონიტორინგის მეშვეობით. აკვირდება საგამოცდო სამსახურის წარმომადგენელი.
6. ვიდეო მონიტორინგით მოპოვებული მონაცემების შენახვის ვადაა 30 კალენდარული დღე, რის შემდეგაც, მონაცემები სისტემის მიერ ავტომატურად ნადგურდება. არ ნადგურდება მხოლოდ ისეთი ვიდეოჩანაწერი, რომელიც ერთვის დისციპლინური წარმოების ფარგლებში მოპოვებულ

დოკუმენტაციას.
7. ვიდეო მონიტორინგის არეალი მოიცავს:
ა) უნივერსიტეტის საერთო არეალს;
ბ) დერეფნებს;
გ) შენობების შესასვლელებს;
დ) რამდენიმე აუდიტორიას, რომლებიც აღჭურვილია ძვირადღირებული ტექნიკით;
ე) საგამოცდო აუდიტორიებს;
ვ) კიბის უჯრედებს;
ზ) კაფეტერიას;
თ) უნივერსიტეტის გარე პერიმეტრს, რომელშიც შედის - უნივერსიტეტის გარე სივრცე, ჭიშკრები, ღობეები, შემოსასვლელი, ავტოსადგომი;
ი) კორპუსებს შორის გადასასვლელებს;
კ) ბიბლიოთეკას.
8. ვიდეო მონიტორინგი არ ხორციელდება გამოსაცვლელ ოთახებში, ჰიგიენისთვის განკუთვნილ ადგილებში ან ისეთ სივრცეში, სადაც სუბიექტს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს ან/და ვიდეო მონიტორინგის განხორციელება საყოველთაოდ აღიარებულ ზნეობრივ ნორმებს ეწინააღმდეგება.

ვიდეომონიტორინგის სისტემაზე წვდომის კონტროლი:
უნივერსიტეტის საკუთრებაში არსებული ვიდეო მონიტორინგის სისტემის ფარგლებში განსაზღვრულია შემდეგი ტიპის წვდომები:
ა) ვიდეო კამერების მონიტორინგი რეალურ (online) რეჟიმში - აღნიშნული წვდომის მქონე მომხმარებელს შეუძლია მხოლოდ თვალყური ადევნოს მიმდინარე კადრებს. შეზღუდული აქვს ჩანაწერის გადახვევის და გადმოწერის (კომპიუტერზე ან ინფორმაციის სხვა მედია მატარებელზე) უფლება;
ბ) ვიდეო კამერების ჩანაწერების გადახვევის და თვალყურის დევნების უფლება - აღნიშნული წვდომის მქონე მომხმარებელს შეუძლია როგორც კამერების რეალურ რეჟიმში მონიტორინგი, ასევე, ჩანაწერების გადახვევა და თვალყურის დევნება, მაგრამ შეზღუდული აქვს ჩანაწერის გადმოწერის (კომპიუტერზე ან ინფორმაციის სხვა მედია მატარებელზე) უფლება;
გ) ვიდეო კამერების ჩანაწერების გადმოწერა - აღნიშნული წვდომის მქონე მომხმარებელს შეუძლია კამერების რეალურ რეჟიმში მონიტორინგი, ჩანაწერების გადახვევა და თვალყურის დევნება, ჩანაწერების გადმოწერა ლოკალურ ქსელში და შესაბამისი დასტურის შემთხვევაში უფლებამოსილი პირისთვის მიწოდება;
დ) ტექნიკური მხარდაჭერის უფლება - აღნიშნული წვდომის მქონე მომხმარებელს აქვს ვიდეო მონიტორინგის სისტემაში ახალი მომხმარებლების შექმნის, არსებული მომხმარებლების გაუქმების, ვიდეო მონიტორინგის სისტემაში არსებული ელექტრონულად შესრულებული მოქმედებების (ლოგების) მონიტორინგის, ტექნიკური პრობლემების შემთხვევაში ხარვეზის აღმოსაფხვრელად სხვადასხვა ქმედებების განხორციელების, ასევე კონფიგურაციების ცვლილებების განხორციელების უფლება.
შენიშვნა: მომხმარებელი არის ნებისმიერი პირი რომელსაც აქვს წვდომა ვიდეო მონიტორინგის სისტემაზე. ვიდეო მონიტორინგის სისტემაზე წვდომა წარმოებს მხოლოდ ინდივიდუალური მომხმარებლის სახელისა და პაროლის საშუალებით.

პირდაპირი მარკეტინგი
1. მონაცემთა დამუშავებაზე პასუხისმგებელი პირი პირდაპირ მარკეტინგს ეწევა რეგიონებში დამამთავრებელი კლასის მოსწავლეებთან სარეკლამო შეხვედრებისას მათთან შემდგომში მარკეტინგული კამპანიის მიზნით ინფორმაციის გასაზიარებლად. ინფორმაცია იგზავნება ელექტრონულ ფოსტაზე და SMS-ის სახით.
1[1]. უნივერსიტეტი პირდაპირ მარკეტინგს ახორციელებს სმს კომუნიკაციის სახით. კერძოდ, სწავლის

მანძილზე სტუდენტს იღებს პერიოდულად სხვადასხვა სახის საინფორმაციო ტიპის შეტყობინებებს სმს-ის სახით. აღნიშნული ინფორმაციის მიღება გათვალისწინებულია ხელშეკრულების პირობებით.
2. უნივერსიტეტის მიერ ჩატარებულ ღია კარის დღეებსა და მოდელირებულ ლექციებზე დასასწრებად აბიტურიენტები და მოსაწვლეები უნივერსიტეტს აწვდიან პირად ინფორმაციას, რომელსაც შემდეგ უნივერსიტეტი მათთან კომუნიკაციისთვის და მათთვის სხვა ღონისძიებების შეთავაზებისთვის იყენებს.
3. უნივერსიტეტი პირდაპი მარკეტინგს ახორციელებს სკოლებში, ტრენინგ-ცენტრეში, სოციალურ ქსელებში, საკუთარ ღონისძიებებში.
4. შპს ჯეოლაბი, როგორც უნივერსიტეტის სასწავლო ცენტრი, პირდაპირ მარკეტინგს ახორციელებს ვაკანსიების, სტაჟირების პროგრამების და სხვადასხვა უფასო პროგრამებისა თუ აქტივობების შესახებ ინფორმაციების ან ელ. ფოსტის საშუალებით დაგზავნისას.
5. უნივერსიტეტი უზრუნველყოფს მონაცემთა სუბიექტ(ებ)ისგან თანხმობის მიღებას მათი მონაცემების შემდგომში დამუშავებისთვის პირდაპირი მარკეტინგის გზით საქართველოს კანონმდებლობის შესაბამისად.
6. მონაცემთა სუბიექტის სახელის, გვარის, მისამართის, ტელეფონის ნომრისა და ელექტრონული ფოსტის მისამართის გარდა, პირდაპირი მარკეტინგის მიზნით, სხვა მონაცემთა დამუშავების საჭიროების შემთხვევაში, უნივერსიტეტი უზრუნველყოფს მიიღოს წერილობითი თანხმობა მონაცემთა სუბიექტისგან.
7. მონაცემთა სუბიექტის თანხმობის მიღებამდე და პირდაპირი მარკეტინგის განხორციელებისას მონაცემთა სუბიექტ(ებ)ს ნათლად, მარტივ და მისთვის გასაგებ ენაზე განემარტება მის მიერ თანხმობის ნებისმიერ დროს გამოხმობის უფლება და ამ უფლების განხორციელების მექანიზმი/წესი.
8. პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავებისას, უნივერსიტეტი აღრიცხავს მონაცემთა სუბიექტის მიერ მის შესახებ მონაცემთა დამუშავებაზე თანხმობის მიცემისა და თანხმობის გამოხმობის დროსა და ფაქტს, რის შესახებ ინფორმაციასაც ინახავს პირდაპირი მარკეტინგის განხორციელების ვადით და პირდაპირი მარკეტინგის განხორციელების შეწყვეტიდან 1 (ერთი) წლის განმავლობაში.
9. პირდაპირი მარკეტინგის განხორციელების მიზნით თანხმობისა და ტელეფონის დაფიქსირების შემდეგ, ტელეფონის ნომრის ცვლილების შემთხვევაში, მონაცემთა სუბიექტი უფლებამოსილია დამუშავებისთვის უფლებამოსილ პირს დაუკავშირდეს საკონტაქტო მონაცემებზე და შეატყობინოს ცვლილების შესახებ, რათა უზრუნველყოფილი იქნეს ზუსტი და სწორი მონაცემების აღრიცხვა.

მონაცემთა სუბიექტის უფლებები:
1. მონაცემთა სუბიექტი უფლებამოსილია:
ა) მიიღოს ინფორმაცია მისი მონაცემების დამუშავების შესახებ;
ბ) მიიღოს ინფორმაცია მონაცემების თანადამმუშავებლის ან/და უფლებამოსილი პირის შესახებ;
გ) მიიღოს ინფორმაცია მონაცემთა დამუშავების მიზნებზე, საფუძვლებსა და კატეგორიებზე;
დ) მიიღოს ინფორმაცია მონაცემთა იმ მიმღების ვინაობასა ან კატეგორიაზე, რომელსაც გადაეცა ან მომავალში გადაეცემა მონაცემები;
ე) მიიღოს ინფორმაცია მონაცემთა შენახვის ვადაზე, ან თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, ვადის განსაზღვრის კრიტერიუმებზე;
ვ) მიიღოს ნებისმიერი ხელმისაწვდომი ინფორმაცია მონაცემთა შეგროვების წყაროს შესახებ, თუ მონაცემთა შეგროვება არ ხდება უშუალოდ მონაცემთა სუბიექტისაგან;
ზ) მოითხოვოს მონაცემთა გაცნობა და ასლის მიღება;
თ) მოითხოვოს მის შესახებ დამუშავებული მცდარი/არაზუსტი მონაცემების დაუყოვნებლივ გასწორება, განახლება, გადატანა ან მონაცემთა დამუშავების მიზნების გათვალისწინებით, არასრული მონაცემების შევსება, მათ შორის, დამატებითი ცნობის/დოკუმენტის წარდგენის გზით;
ი) მოითხოვოს მონაცემთა დამუშავების შეწყვეტა, მონაცემთა წაშლა ან მონაცემტა განადგურება თანხმობის გამოთხოვით;
კ) მოითხოვოს მონაცემთა დაბლოკვა.

ზეგავლენის დოკუმენტის განახლება და დამატებითი ინფორმაცია:
მონაცემთა დამუშავებასთან დაკავშირებული ცალკეული საკითხების ან/და პროცესის არსებითი ცვლილების შემთხვევაში დამუშავებისთვის პასუხისმგებელი პირი პერსონალურ მონაცემთა დაცვის ოფიცერის აქტიური ჩართულობით ვალდებულია განაახლოს ზეგავლენის დოკუმენტი.

პროცესში მონაწილე და ჩართული პირები და მათ მიერ გამოთქმული მოსაზრებები:
უნივერსიტეტი ზეგავლენის შეფასების პროცესში უზრუნველყოფს შემდეგი პირების **მონაწილეობას:**
ა) შესაბამისი სტრუქტურული ერთეული ან პირი, რომელიც პასუხისმგებელია კონკრეტული პროდუქტის ან მომსახურების შექმნასა თუ განახლებაზე, რომლის ფარგლებშიც ხორციელდება მონაცემთა დამუშავება;
ბ) პერსონალურ მონაცემთა დაცვის ოფიცერი;
გ) საინფორმაციო ტექნოლოგიებზე პასუხისმგებელი სტრუქტურული ერთეული/პირი.
უნივერსიტეტი ზეგავლენის შეფასების პროცესში უზრუნველყოფს შემდეგი პირების **ჩართულობას:**
ა) ექსპერტი, რომელიც ფლობს კონკრეტული პროცესების შესახებ სპეციალურ ცოდნას;
ბ) მონაცემთა სუბიექტები ან მათი წარმომადგენლები;
გ) სხვა პირი, რომლის მონაწილეობა მნიშვნელოვანია ზეგავლენის შეფასების პროცესში.

მონაცემთა დამუშავების მასშტაბთან დაკავშირებული სხვა დამატებითი ინფორმაცია

მონაცემთა კატეგორია

მონაცემთა სუბიექტთან ურთიერთობის ხასიათიდან და მონაცემთა დამუშავების მიზნიდან გამომდინარე, საჭიროებისამებრ, შეიძლება დამუშავდეს შემდეგი პერსონალური მონაცემები:
ა) საიდენტიფიკაციო მონაცემები - სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი, სქესი;
ბ) საკონტაქტო მონაცემები - იურიდიული და ფაქტობრივი მისამართები, ტელეფონი, ელ. ფოსტა;
გ) განსაკუთრებული კატეგორიის მონაცემები - ინფორმაცია მოქალაქეობის შესახებ, სტუდენტის/თანამშრომლების ჯანმრთელობის შესახებ, ნასამართლობის, სქესობრივი თავისუფლებისა და ხელშეუხებლობის წინააღმდეგ მიმართული დანაშაულის ჩადენისთვის ნასამართლობის შესახებ;
დ) დიპლომების დამოწმებული ასლები;
ე) დასაქმების სტატუსი;
ვ) განათლება;
ზ) ნებისმიერი სხვა ინფორმაცია, რომელიც გათვალისწინებულია შესაბამისი სერვისის, აგრეთვე, უნივერსიტეტის უფლებამოსილების მარეგულირებელი აქტებით.
თ) ცხელი ხაზების მოსარგებლეთა პერსონალური მონაცემები, ამასთან, მონაცემები მუშავდება მხოლოდ აბონენტის (ბენეფიციარის) ინფორმირებით;
ი) სამუშაო გამოცდილება - პოზიცია, თანამდებობა, თანამდებობრივი სარგო, კვალიფიკაცია, ანაზღაურება;
კ) განცხადება ან/და დოკუმენტი, რითაც დასტურდება დასაქმებულის ნება შრომითი ურთიერთობის წარმოშობასთან დაკავშირებით;
ლ) პირადობის დამადასტურებელი დოკუმენტის/პასპორტის ასლი;
მ) განათლების ან შესაბამისი კვალიფიკაციის დამადასტურებელი დოკუმენტის ასლი;
ნ) სტუდენტის სკოლის ატესტატი;

ო) ავტობიოგრაფია - Curriculum Vitae (CV);
პ) 1 ფოტოსურათი ციფრული სახით;
ჟ) მოქმედი საბანკო ანგარიშის ოფიციალური რეკვიზიტი;
რ) დაგროვებითი საპენსიო რეფორმის ფარგლებში, საპენსიო სქემიდან გასვლის დამადასტურებელი დოკუმენტი, ასეთის არსებობის შემთხვევაში;
ს) საშემოსავლო გადასახადის შეღავათით სარგებლობის შემთხვევაში, აღნიშნულის დამადასტურებელი დოკუმენტი - ცნობა შემოსავლების სამსახურიდან;
ტ) 17 წელს მიღწეული პირის (გარდა იმ პირისა, რომელიც წვევამდელთა სამხედრო აღრიცხვას არ ექვემდებარება) წვევამდელის სამხედრო აღრიცხვაზე ყოფნის ან წვევამდელის სამხედრო აღრიცხვიდან მოხსნის დამადასტურებელი დოკუმენტი;
უ) არასრულწლოვანთა ფოტოსურათები, ღონისძიებებზე და სასწავლო კურსებზე რეგისტრაციის მონაცემები დონორთან გადაგზავნის მიზნით;
ფ) სოციალური ქსელის ბმული;
ქ) ვიდეომონიტორინგის არეალში მოხვედრილი სხვა პირების გამოსახულება;
ღ) სამხედრო აღრიცხვის მოწმობა (მამაკაცი თანამშრომლების/სტუდენტების შემთხვევაში);
ყ) ნიშნების ფურცელი წინა სასწავლებლიდან;
შ) საკომუნიკაციო ინფორმაცია სტუდენტის მშობლების ან იმ პირების შესახებ, რომლებთან დაკავშირებაც შესაძლებელია აუცილებლობის შემთხვევაში;
შ) ინფორმაცია სტუდენტის აკადემიური მოსწრების შესახებ;
ც) ინფორმაცია სტუდენტის ყოფილი უნივერსიტეტ(ებ)ის შესახებ;
ძ) სტუდენტის სტატუსის განმსაზღვრელი სამართლებრივი აქტები;
წ) გარდაცვლილთა საიდენტიფიკაციო მონაცემები - გარდაცვლილი სტუდენტის სტატუსის შეწყვეტის, შრომითი ურთიერთობების შეწყვეტის შესახებ ბრძანების გამოცემის და განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტროს ბაზაში ასახვის მიზნით.

მონაცემთა დამუშავების საფუძველი

1. პერსონალურ მონაცემთა დამუშავება ხდება შემდეგი საფუძვლებით:
ა) მონაცემთა სუბიექტმა განაცხადა თანხმობა მის შესახებ მონაცემთა ერთი ან რამდენიმე კონკრეტული მიზნით დამუშავებაზე;
ბ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტთან დადებული გარიგებით ნაკისრი ვალდებულების შესასრულებლად ან მონაცემთა სუბიექტის მოთხოვნით გარიგების დასადებად;
გ) მონაცემთა დამუშავება აუცილებელია უნივერსიტეტისთვის კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად;
დ) მონაცემთა დამუშავება გათვალისწინებულია კანონით;
ე) კანონის თანახმად, მონაცემი საჯაროდ ხელმისაწვდომია ან მონაცემთა სუბიექტმა იგი საჯაროდ ხელმისაწვდომი გახადა;
ვ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დასაცავად;
ზ) მონაცემთა დამუშავება აუცილებელია დამუშავებისთვის პასუხისმგებელი პირის ან მესამე პირის მნიშვნელოვანი ლეგიტიმური ინტერესების დასაცავად, გარდა იმ შემთხვევისა, თუ არსებობს მონაცემთა სუბიექტის (მათ შორის, არასრულწლოვანის) უფლებების დაცვის აღმატებული ინტერესი;
თ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად (მისთვის მომსახურების გასაწევად).
2. განსაკუთრებული კატეგორიის მონაცემებს უნივერსიტეტი ამუშავებს მხოლოდ იმ შემთხვევაში თუ:
ა) ჯანმრთელობასთან დაკავშირებული მონაცემები მუშავდება სპეციალური საგანმანათლებლო საჭიროების მქონე პირთა განათლების უფლების რეალიზების მიზნით. ასევე, საბიულეტინო სისტემის უზრუნველყოფისთვის. უნივერსიტეტი ამუშავებს სტუდენტებისა და პერსონალის მოქალაქეობის

შესახებ ინფორმაციას განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტროს მოთხოვნების შესაბამისად, რადგან სამინისტროს ბაზაში - სტუდენტის და პერსონალის მონაცემებში სავალდებულო წესით უნდა იყოს აღნიშნული ინფორმაცია. ამასთან, მოქალაქეობის შესახებ ინფორმაცია მუშავდება მათი საიმიგრაციო და განათლების აღიარების მიზნებისათვის. ასევე, მუდმივად ხდება უცხოელი სტუდენტების შესახებ სტატისტიკის გამოთხოვა სხვადასხვა ქვეყნების საელჩოებიდან მათი ქვეყნის მოქალაქეების შესახებ. უნივერსიტეტი უცხო ქვეყნის მოქალაქეობის შესახებ ინფორმაციას, ასევე, გასცემს საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროზე. ამასთან, საქსტატი ყოველწლიურად ითხოვს დასაქმებულთა რაოდენობებს მოქალაქეობისა ჭრილში. დამატებით, კვლევის განვითარების და ხელშეწობის ოფისი პასუხისმგებელია მოქალაქეობასთან დაკავშირებული ინფორმაციის დამუშავებაზე, დონორის მოთხოვნის შემთხვევაში. მოქალაქეობის შესახებ ინფორმაციის დახმარებით, უნივერსიტეტი აპლიკანტს აწვდის ამომწურავ ინფორმაციას სავიზო პროცედურების შესახებ, რომელიც საქართველოში მოსახვედრად უნდა გაიაროს. უნივერსიტეტი რიგ შემთხვევებში საკონსულტაციო კომპანიებს ექსკლუზიური პირობებით უფორმებს ხელშეკრულებებს განსაზღვრულ ქვეყნებზე. თუკი, აპლიკანტი დამოუკიდებლად უკავშირდება უნივერსიტეტს და ექსკლუზიური ქვეყნის მოქალაქეა, უნივერსიტეტი აპლიკანტს აწვდის საკონსულტაციო კომპანიის საკონტაქტო ინფორმაციას და სთხოვს მათთან დაკავშირებას;

ბ) ნასამართლობის, სქესობრივი თავისუფლებისა და ხელშეუხებლობის წინააღმდეგ მიმართული დანაშაულის ჩადენისთვის ნასამართლობისა და ჯანმრთელობის მდგომარეობასთან დაკავშირებული მონაცემების დამუშავება აუცილებელია შრომითი ვალდებულებისა და ურთიერთობის ხასიათიდან გამომდინარე, მათ შორის დასაქმების თაობაზე გადაწყვეტილების მისაღებად. უმაღლესი გაანთლების შესახებ საქართველის კანონის 32-ე მუხლის მე-2 პუნქტის თანახმად, უმაღლეს საგანმანათლებლო დაწესებულებაში არ შეიძლება დასაქმდეს „სქესობრივი თავისუფლებისა დახელშეუხებლობის წინააღმდეგ მიმართულ დანაშაულთან ბრძოლის შესახებ“ საქართველოს კანონით გათვალისწინებული სქესობრივი თავისუფლებისა დახელშეუხებლობის წინააღმდეგ მიმართული დანაშაულის ჩადენისთვის ნასამართლევიპირი ან/და პირი, რომელსაც იმავე კანონის საფუძველზე სასამართლომ ჩამოართვა საგანმანათლებლო დაწესებულებაში საქმიანობის უფლება.

3. იმ შემთხვევაში, თუ უნივერსიტეტი მონაცემებს დაამუშავებს მონაცემთა სუბიექტის თანხმობით, თანხმობა მხოლოდ იმ შემთხვევაში ჩაითვლება ნამდვილად, თუ ის გაცემულია შესაბამისი ინფორმაციის მიღების შემდეგ, ნებაყოფლობით, მონაცემთა განსაზღვრული და კონკრეტული მიზნით დამუშავებაზე. თანხმობა გაიცემა ნებაყოფლობით და მონაცემთა სუბიექტის აქტიური მოქმედებით.

მონაცემთა დამუშავების აუცილებლობის, თანაზომიერებისა და პროპორციულობის შეფასება

სტუდენტები უნივერსიტეტში და საგამოცდო ცენტრში შესასვლელად ტესტირების მიზნებისთვის იყენებენ უნივერსიტეტის მიერ მიწოდებულ კუთვნილ ბარათებს, რომლებზეც დატანილია მათი სახელი, გვარი, ფოტოსურათი და პირადი ნომერი. აღნიშნული საბარათე სისტემის მიზანია საგამოცდო ცენტრში გამოცდის საწერად შემსვლელ სტუდენტთა იდენტიფიცირება და საგამოცდო რეგისტრაციისას იმგვარი რისკების პრევენცია, როგორიც შეიძლება იყოს სტუდენტის მიერ სხვა ფაკულტეტის საგნის გამოცდის წერა, სტუდენტის სტატუსის არ მქონე პირის მიერ გამოცდის წერა და სხვა. პირადი ნომრის ბარათზე დატანის აუცილებლობა განპირობებულია იმ ფაქტით, რომ სტუდენტები საგამაოცდო ცენტრში საკუთარ ნაშრომებს აწერენ ინდივიდუალურ საიდენტიფიკაციო ნომრებს, რომელთა მეშვეობითაც ხდება ნაშრომების იდენტიფიცირება და შესაბამისად, ინდივიდუალური შეფასება.

უნივერსიტეტის მიერ მონაცემთა უსაფრთხოებისთვის მიღებული ტექნიკური და ორგანიზაციული ზომები წარმოადგენს ამავე დოკუმენტით განსაზღვრული მონაცემთა დამუშავების მიზნების მიღწევის აუცილებელ, ნაკლებად მზღუდავ და პროპორციულ მექანიზმებს.

მიუხედავად კანონმდებლობით დადგენილი ვალდებულებებისა, უნივერსიტეტი უზრუნველყოფს ნებისმიერი მონაცემთა სუბიექტის უფლებების დაცვას, კერძოდ, ვიდეო ჩანაწერების მოთხოვნის შემთხვევაში, იგი ახორციელებს ყველა იმ პირის დეპერსონალიზაციას, რომელიც არ არის დაკავშირებული ჩანაწერის მოთხოვნის მიზანთან.

უნივერსიტეტი მონაცემთა დამუშავების პროცესში ხელმძღვანელობს მონაცემთა და ვადის მინიმიზაციის პრინციპებით და აღნიშნულისა და შიდა რეგულატორული მოთხოვნების შესაბამისად ადგენს ყოველი კონკრეტული ინფორმაციისათვის შენახვის ვადას. (დეტალური ინფორმაცია იხილეთ უნივერსიტეტის პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტში)

მონაცემთა დამუშავების მასშტაბთან დაკავშირებული სხვა დამატებითი ინფორმაცია

მუშავდება თუ არა არასრულწლოვანთა ან სხვა მოწყვლადი ჯგუფის მონაცემები? რა სიხშირით ხდება მონაცემთა დამუშავება? მონაცემთა დამუშავების გეოგრაფიული არეალი. სხვა მნიშვნელოვანი ინფორმაცია მონაცემთა დამუშავების მასშტაბების განსასაზღვრად.

უნივერსიტეტი გამონაკლის შემთხვევებში ამუშავებს არასრულწლოვანთა პერსონალურ მონაცემებს. კერძოდ, მაშინ, როცა სტუდენტი აბარებს პირველ კურსზე და მას ჯერ არ აქვს შესრულებული 18 წელი. ასეთ შემთხვევაში, როგორც ყველა სტუდენტი, არასრულწლოვანიც წარმოადგენს ყველა საჭირო დოკუმენტს კანონიერ წარმომადგენელთან ერთად.
ამასთან, უნივერსიტეტი ამუშავებს სპეციალური საგანმანათლებლო საჭიროების მქონე სტუდენტების შესახებ ინფორმაციას (მათ შორის, ჯანმრთელობასთან დაკავშირებულ ინფორმაციას) მათთვის განათლების უფლების რეალიზების მიზნით.
უნივერსიტეტში მონაცემთა დამუშავების პროცესი არ შემოიფარგლება მხოლოდ საქართველოს ტერიტორიით. კერძოდ, მუდმივად ხდება უცხოელი სტუდენტების შესახებ სტატისტიკის გამოთხოვა სხვადასხვა ქვეყნების საელჩოებიდან მათი ქვეყნის მოქალაქეების შესახებ. უნივერსიტეტი უცხო ქვეყნის მოქალაქეობის შესახებ ინფორმაციას, ასევე, გასცემს საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროზე. ამასთან, საქსტატი ყოველწლიურად ითხოვს დასაქმებულთა რაოდენობებს მოქალაქეობისა ჭრილში. დამატებით, კვლევის განვითარების და ხელშეწობის ოფისი პასუხისმგებელია მოქალაქეობასთან დაკავშირებული ინფორმაციის დამუშავებაზე, დონორის მოთხოვნის შემთხვევაში. მოქალაქეობის შესახებ ინფორმაციის დახმარებით, უნივერსიტეტი აპლიკანტს აწვდის ამომწურავ ინფორმაციას სავიზო პროცედურების შესახებ, რომელიც საქართველოში მოსახვედრად უნდა გაიაროს. უნივერსიტეტი რიგ შემთხვევებში საკონსულტაციო კომპანიებს ექსკლუზიური პირობებით უფორმებს ხელშეკრულებებს განსაზღვრულ ქვეყნებზე. თუკი, აპლიკანტი დამოუკიდებლად უკავშირდება უნივერსიტეტს და ექსკლუზიური ქვეყნის მოქალაქეა, უნივერსიტეტი აპლიკანტს აწვდის საკონსულტაციო კომპანიის საკონტაქტო ინფორმაციას და სთხოვს მათთან დაკავშირებას. ამასთან, უნივერსიტეტისთვის პერსონალურ

მონაცემთა მიღების წყაროა უცხოელი სტუდენტების აგენტები, რომლებიც ახდენენ სტუდენტების ჩარიცხვასთან დაკავშირებული პროცედურების წარმოებას ჩარიცხვის მსურველი პირების ნების შესაბამისად.
უნივერსიტეტი, ასევე, მონაცემებს გადასცემს საერთაშორისო ორგანიზაციას, როცა ეს აუცილებელია აკადემიური, ადმინისტრაციული მიზნებისთვის სტუდენტებისა და დასაქმებულების საუკეთესო ინტერესებიდან გამომდინარე.

მონაცემთა დამუშავების მიზანი და პრინციპები

მონაცემთა დამუშავების მიზნები:
1. უნივერსიტეტის მიერ პერსონალურ მონაცემთა დამუშავების მიზნებია:
ა) უმაღლესი საგანმანათლებლო საქმიანობის განხორციელება;
ბ) სამსახურეობრივი საქმიანობის განხორციელება;
გ) სასწავლო პროცესის მათ შორის დისტანციური სწავლების შეუფერხებელი მიმდინარეობის უზრუნველყოფა;
დ) სამუშაო პროცესის შეუფერხებელი მიმდინარეობის უზრუნველყოფა;
ე) სტუდენტთა რეგისტრაცია;
ვ) უმაღლეს საგანმანათლებლო დაწესებულებაში ჩარიცხვის პროცესის უზრუნველყოფა, რაც მოიცავს პირობითი და უპირობო მოწვევის წერილების გამზადებას, სსიპ - განათლების ხარისხის განვითარების ეროვნულ ცენტრში უცხოეთში მიღებული განათლების აღიარების პროცედურების გავლას;
ზ) სტუდენტებისა და მთლიანი პერსონალის პირადი საქმეების წარმოება;
თ) სტუდენტთა აღრიცხვის, შეფასების, მათი მობილობის უზრუნველყოფა;
ი) სპეციალური საგანმანათლებლო საჭიროების მქონე სტუდენტთათვის განათლების უფლების რეალიზება;
კ) უნივერსიტეტში დასაქმების მსურველი კვალიფიციური კადრების რეკრუტირება;
ლ) ელექტრონული შეფასების სისტემის წარმოების მიზნით, მონაცემთა ბაზების სრულყოფა;
მ) დოკუმენტბრუნვის ორგანიზება და კონტროლი;
ნ) უმაღლესი განათლების დამადასტურებელი დოკუმენტის გაცემა;
ო) უნივერსიტეტის საკუთრების, ქონების დაცვის, სტუდენტთა, თანამშრომელთა ან/და სტუმართა/მესამე პირთა ფიზიკური უსაფრთხოების უზრუნველყოფა;
პ) უნივერსიტეტის მხრიდან გაწეული მომსახურების ხარისხის გაუმჯობესება;
ჟ) ზემდგომი ორგანოებისთვის მოთხოვნილი ინფორმაციის მიწოდება;
რ) სტუდენტთა აკადემიური მიღწევის მაჩვენებლების შეგროვება;
ს) სტუდენტთა და დასაქმებულთა სხვადასხვა აქტივობებში ჩართვის უზრუნვლყოფა;
ტ) სსიპ - განათლების მართვის საინფორმაციო სისტემისთვის მოთხოვნილი ინფორმაციის მიწოდება, მათ ბაზაში მონაცემების ატვირთვა;
უ) უმაღლეს საგანმანათლებლო დაწესებულებაში სტუდენტის ჩარიცხვის, სტატუსის აღდგენის/შეჩერების/შეწყვეტის პროცესების შეუფერხებლად წარმართვა;
ფ) კვლევის განვითარების და ხელშეწობის მიზნით კონტრაქტების მომზადება და ფინანსურ და იურიდიულ სამსახურთან, ასევე, დონორ ორგანიზაციასთან გადაგზავნა;
ქ) ომბუდსმენის მიერ საკუთარი მოვალეობების შესრულება;

ღ) შრომითი ურთიერთობების ადმინისტრირება რეკრუტინგის მიზნით;
ყ) დონორის მოთხოვნის საფუძველზე რეპორტინგის პროცესის წარმოება;
შ) სავიზო მიმართულებით პროცესის წარმართვა და ფასილიტირება;
ჩ) კანონმდებლობით დაკისრებული სხვა უფლებამოსილებების განხორციელება.

2. უნივერსიტეტის მიერ პერსონალურ მონაცემთა ვიდეომონიტორინგის გზით დამუშავების მიზნებია:
ა) კანონით დაკისრებული ვალდებულებების შესრულება;
ბ) უსაფრთხოებისა და საკუთრების დაცვა (მათ შორის შიდა სივრცის ეფექტური ლოჯისტიკა ან ტექნიკური ოპერაციების ეფექტიანობა, რაც უნივერსიტეტის ხელმძღვანელობას აძლევს იმ ტიპის მონაცემებს, რომლებიც საჭიროა ყოველდღიური მუშაობის ოპტიმიზაციისთვის);
გ) არასრულწლოვანთა მავნე ზეგავლენისაგან დაცვა;
დ) დანაშაულის თავიდან აცილება:
ე) დანაშაულის გამოვლენა;
ვ) პროფესიული ზედამხედველობა და ხარისხის უზრუნველყოფა;
ზ) უნივერსიტეტში მყოფი სტუდენტებისთვის შეთავაზებული სერვისების ხარისხის მუდმივი გაუმჯობესება;
თ) სამართლებრივი დავების გადაწყვეტა (ვიდეოჩანაწერები ემსახურება ყველა ჩართული მხარის, სტუდენტების, მათ შორის არასრულწლოვნებისა და უნივერსიტეტის თანამშრომლების დაცვა - დავის ან ნებისმიერი სახის ბრალდებების შემთხვევაში, ვიდეო ჩანაწერები წარმოადგენს ფაქტობრივ მტკიცებულებებს დავისა თუ გაუგებრობის სამართლიანი და ზუსტი გადაწყვეტისთვის);
ი) საგამოცდო/ტესტირების მიზნებისთვის.

პერსონალურ მონაცემთა დამუშავება ხორციელდება საქართველოსა და საერთაშორისო კანონმდებლობით გათვალისწინებული შემდეგი პრინციპებით:

- სამართლიანობის პრინციპი;
- გამჭვირვალობა;
- მიზნის შეზღუდვის პრინციპი;
- მონაცემთა მინიმიზაციის პრინციპი;
- ვადის მინიმიზაციის პრინციპი;
- მონაცემთა სიზუსტის პრინციპი;
- უსაფრთხოების პრინციპი.

ნაწილი II - ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეები და მათი ხარისხობრივი ანალიზი

რისკის დონე	რისკის კატეგორია	აღწერა და საჭირო ღონისძიებები
I	არაარსებითი	უმნიშვნელო ინციდენტი, რომელიც განიხილება, როგორც მცირე გავლენის მქონე ლოკალური შემთხვევა, რომელიც გავლენას არ ახდენს უნივერსიტეტის ფუნქციონირებაზე. არ საჭიროებს კონკრეტული პროცედურების განხორციელებას, საჭიროა სამუშაოს შესრულების მონიტორინგი
II	არსებითი	სერიოზული შემთხვევა, რომელიც აფერხებს უნივერსიტეტის ერთ ან მეტ პროცესს. საჭიროა შემუშავდეს რისკის შემცირების პროცედურები, შეფასდეს პრიორიტეტები და დაიგეგმოს რისკის შემცირების საკონტროლო ღონისძიებები.
III	კრიტიკული	კრიტიკული ინციდენტი, რომელიც სრულად აფერხებს ან აჩერებს უნივერსიტეტის მუშაობას. საჭიროა შეჩერდეს სამუშაო/სასწავლო პროცესი, დაუყოვნებლივ უნდა იქნას მიღებული ზომები რისკის შესამცირებლად

მონაცემთა დამუშავების სახე:	
❖ დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტისთვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებს სრულად ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე;	+
❖ დამუშავებისთვის პასუხისმგებელი პირი ამუშავებს დიდი რაოდენობით (საქართველოს მოსახლეობის არანაკლებ 3 პროცენტისა, რომელიც გამოითვლება მოსახლეობის აღწერის ბოლო შედეგების მიხედვით) მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემებს;	+
❖ დამუშავებისთვის პასუხისმგებელი პირი ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში;	+
❖ მონაცემთა სუბიექტების ქცევის ან მდგომარეობის (მათ შორის, ფიზიკური/ჯანმრთელობის) სისტემატური და მასშტაბური მონიტორინგი გარკვეული ელექტრონული სისტემის/ტექნოლოგიის მეშვეობით, ან ასეთი მონიტორინგი მიმდინარეობს დასაქმებულთა მიმართ;	+
❖ ახალი ტექნოლოგიის დანერგვა ან ინოვაციური გამოყენება;	+

❖ მონაცემთა ბაზების შედარება ან გაერთიანება, რომელიც წარმოიქმნება ორი ან მეტი სხვადასხვა მონაცემთა დამუშავების პროცესიდან, სხვადასხვა მიზნებისთვის ან/და სხვადასხვა დამუშავებისთვის პასუხიმგებელი პირის მიერ;	
❖ მონაცემთა დამუშავებას შედეგად შესაძლოა, მოჰყვეს მონაცემთა სუბიექტისდისკრიმინაცია;	+
❖ მონაცემთა სუბიექტები არიან მოწყვლადი პირები, მათ შორის, დამუშავებისათვის პასუხისმგებელი პირის თანამშრომლები, სამედიცინო დაწესებულების პაციენტები, არასრულწლოვნები, შეზღუდული შესაძლებლობის მქონე პირები დასხვა.	+
❖ უნივერსიტეტი ამუშავებს განსაკუთრებული კატეგორიის მონაცემებს, რისი გათვალისწინებითაც საგანმანათლებლო და ადმინისტრაციული საქმიანობის პროცესში შესაძლოა შეიქმნას ამ მონაცემების გამჟღავნების საფრთხე, მათ შორის, უნივერსიტეტის დასაქმებულის დაუდევარი ქმედებიდან გამომდინარე, მატერიალურად არსებული დოკუმენტების შენახვის ორგანიზაციული წესების დარღვევიდან გამომდინარე ან/და მესამე პირზე ინფორმაციის გადაცემის საფუძვლის სამართლებრივად არასწორად შეფასებიდან გამომდინარე.	+
❖ საარქივო მასალის და სხვადასხვა დოკუმენტაციის განადგურება	+
❖ ინტერნეტის, პროგრამული უზრუნველყოფის, ტექნიკის პრობლემები	+
❖ კიბერდანაშაული	+

.

მონაცემთა დამუშავების შესაძლო შედეგები		რისკის დონე
❖ ვინაობის მითვისება (ე.წ. Identity Theft) ან გაყალბება	უნივერსიტეტი აქტიურად ამუშავებს იმგვარ პერსონალურ მონაცემებს, როგორიცაა პირადობის მოწმობები, მათი ნომრები, ფინანსურ ინფორმაცია და სხვა, რაც განაპირობებს მათ სამიზნედ ქცევას ჰაკერებისა და ფიშინგის სქემების.	II
❖ ფინანსური დანაკარგი	ფიზიკური პირებისთვის პირდაპირი ფინანსური ზიანის მიყენების ფაქტი ნაკლებად ხშირია, მაგრამ მაინც შესაძლებელია კიბერ თავდასხმების გამო, რომელიც მათ შორის მიემართება საბანკო ანგარიშებს.	II
❖ მონაცემთა სუბიექტის რეპუტაციის შელახვა, აკადემიურ ან პროფესიულ შესაძლებლობებზე მავნე ზემოქმედება	პერსონალური ან აკადემიური მონაცემების ბოროტად გამოყენებამ შეიძლება ზიანი მიაყენოს სტუდენტების ან პერსონალის რეპუტაციას, თუმცა ეს ხშირად მოითხოვს მიზანმიმართულ ან განზრახ ქმედებებს.	II
❖ პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალობის დარღვევა	განსაკუთრებული კატეგორიის ინფორმაცია, მათ შორის, ჯანმრთელობასთან დაკავშირებული მონაცემები, შეიძლება ადვილად ხელმისაწვდომი იყოს არაავტორიზებული წვდომის შემთხვევებში.	II
❖ ფსევდონიმიზებული პერსონალური მონაცემების უკანონო გამჟღავნება	მიუხედავად იმისა, რომ ფსევდონიმიზაცია მონაცემთა დაცვის დამატებითი მექანიზმია, შესაძლებელია საფრთხე შეექმნათ ამ მონაცემების უსაფრთხოებას ხელახალი იდენტიფიკაციის მიზნით, განსაკუთრებით, მონაცემთა გაფართოებული ანალიტიკის ან მონაცემთა დაუდევრად დამუშავების გზით.	II
❖ სხვა სახის მნიშვნელოვანი სოციალური ან/და ეკონომიკურიზიანი	ზიანი, როგორიცაა სტიგმატიზაცია ან დისკრიმინაცია, შეიძლება დადგეს მონაცემების	II

	გამჟღავნების შედეგად, მაგრამ, როგორც წესი, აღნიშნული საჭიროებს მიზანმიმართულ, განზრახ უფლების ბოროტად გამოყენების შემთხვევის არსებობას.	
❖ ჯანმრთელობის მდგომარეობის გაუარესება	ნაკლებად სავარაუდოა, თუ დარღვევა არ მიემართება განსაკუთრებული კატეგორიის სამედიცინო ან ფსიქოლოგიურ მონაცემებს.	I
❖ სასიცოცხლო მნიშვნელობის ინფრასტრუქტურაზე წვდომის შეზღუდვა	უნივერსიტეტი იშვიათად დგას ინფრასტრუქტურის გაუმართაობის პრობლემის წინაშე, თუმცა სისტემების შეფერხებამ შეიძლება დროებით სწავლის მიმდინარეობის შეფერხებაც გამოიწვიოს.	I
❖ სამართლებრივი ქმედებები და დავა დაზარალებული პირების ან მარეგულირებელი ორგანოების მხრიდან	სავარაუდოა, რომ მოხდეს მძიმე და განსაკუთრებულ მონაცემებთან დაკავშირებული დარღვევების შემთხვევაში, თუმცა მარეგულირებლის მხრიდან დავის ალბათობა დაბალია უნივერსიტეტის მიერ კანონით დადგენილი მოთხოვნების სათანადოდ შესრულების გამო.	I
❖ მონაცემთა აღდგენის მცდელობის გამო სისტემის ფუნქციონირების შეფერხება	დამოკიდებულია სარეზერვო (back up) და ინციდენტზე რეაგირების პროტოკოლების სათანადოდ არსებობაზე.	II
❖ არაავტორიზებული წვდომა, რომელიც შესაძლოა განხორციელდეს კიბერ თავდასხმით (დაჰაკვით), ფიშინგით, სუსტი საპაროლე სისტემით	უნივერსიტეტში პერსონალური მონაცემების (მათ შორის განსაკუთრებული და ფინანსური ინფორმაციის) მოცულობის გამო.	II
❖ მონაცემთა დაკარგვა, რომელიც შესაძლოა განხორციელდეს ტექნიკის (ჰარდვეარის) გაუმართაობის, დასაქმებულის დაუდევრობით ან განზრახ ქმედებების გამო	არასაკმარისი სარეზერვო ასლების ან განზრახი კიბერ შეტევების შემთხვევაში სავარაუდოა.	II
❖ მონაცემთა უკანონო გამჟღავნება, სენსიტიური ინფორმაციის გავრცელება არაავტორიზებული მხარეებისთვის რომელიც შესაძლოა განხორციელდეს ინფორმაციის გაჟონვით, სისტემის დაუცველობით ან მოწყობილობების მოპარვით	უნივერსიტეტში აქტიურად მუშავდება სენსიტიური მონაცემები, რაც მათ წვდომის სამიზნედ გახდმას განაპირობებს.	II
❖ მონაცემთა მოდიფიკაცია, მონაცემების არაავტორიზებული ან შემთხვევითი შეცვლა, რომელიც შესაძლოა განხორციელდეს სტუდენტის ქულების, კვლევის შედეგად მიღებული მონაცემების ან ფინანსური ჩანაწერების ხელყოფით	რადგან საჭიროა ინსაიდერის წვდომა ან კონკრეტული სისტემის დაუცველობა.	I

❖ მონაცემთა არაპროპორციულად, საჭიროზე მეტ ხანს შენახვა და სათანადო წესის დაუცველად განადგურება, რომელიც შესაძლოა განხორციელდეს კანონით დადგენილ ვადაზე მეტხანს მონაცემების შენახვის ან დაუშრედერებელი ფაილების შენახვის გზით	რადგან ხდება მაშინ, როდესაც არ არსებობს მონაცემთა დამუშავების ყოვლისმომცველი პოლიტიკა.	II
❖ კანონით დადგენილი მოთხოვნების შეუსრულებლობა შიდაორგანიზაციული დოკუმენტაციის გაუმართაობის გამო, მათ შორის, ინფორმირებული თანხმობების ფორმების და გაფრთხილებების არ არსებობის გამო	რადგან ამ საფრთხეს განაპირობებს ცნობიერების და კადრების გადამზადების შემთხვევების ნაკლებობა არსებული რეგულაციების შესახებ.	II
❖ საარქივო მასალის და სხვადასხვა დოკუმენტაციის განადგურებას თან შეიძლება მოჰყვეს საგადასახადოს/აუდიტის შემოწმების პროცესის შესაძლო შეფერხება, საქმისწარმოების პროცესის შეფერხება, სტუდენტებთან, აკადემიურ და ადმინისტრაციულ პერსონალთან, მომწოდებლებთან და პარტნიორებთან კონტრაქტების და მემორანდუმების არ არსებობა განახლებამდე	რადგან არსებობს ელექტრონული ასლების, საარქივო მასალა და სხვა დოკუმენტაცია სპეციალურად განკუთვნილ დაცულ სივრცეებშია შენახული, ხორციელდება განადგურებული დოკუმენტაციის აღწერა და პრიორიტეტების განსაზღვრა ეტაპობრივი აღდგენისთვის. ასევე, ხდება ელექტრონული ასლების მეშვეობით დოკუმენტაციის აღდგენა შესაბამისი სამსახურის მიერ და უზრუნველყოფილია კონტრაქტების და მემორანდუმების ხელახლა გაფორმების პროცესი	I
❖ ინტერნეტის, პროგრამული უზრუნველყოფის, ტექნიკის პრობლემებს თან შეიძლება მოჰყვეს კონკრეტული ან მთლიანი სასწავლო / სამუშაო პროცესის მცირე შეფერხება, ხანგრძლივი გათიშვის შემთხვევაში სასწავლო / სამუშაო პროცესის შეჩერება, უნივერსიტეტის ძირითადი პროცესების უწყვეტად გაგრძელება თუ დიდი რაოდენობით ტექნიკის დაზიანებასთან არ გვაქვს საქმე.	რადგან არსებობს ალტერნატიული ხაზი, ასევე, ოფიციალური პარტნიორები Microsoft-ის, Google-ის და სხვა, რაც პროგრამულ უზრუნველყოფასთან დაკავშირებულ რისკებს ამცირებს. არსებობს Firewall-ის, ანტივირუსული აპლიკაციების, LAN შეზღუდვა, ასლები ინახება პერიოდულად, ტექნიკია პერიოდულად მოწმდება, ხდება მოძველებული ტექნიკის ახლით ჩანაცვლება. ასევე, ასრებობს სარეზერვო კომპიუტერული მარაგი. სერიოზული პრობლემის შემთხვევაში ხდება IT დახმარების გაწევა ხარვეზის აღმოსაფხვრელად, საჭიროების შემთხვევაში ხორციელდება ოფიციალურ მომწოდებლებთან დაკონტაქტება. ამ პროცესებში ჩართულია საინფორმაციო ტექნოლოგიების სამსახური	I
❖ კიბერდანაშაულს თან ახლავს მონაცემების დაკარგვის საშიშროება, რაც იწვევს სასწავლო/სამუშაო პროცესის შესაძლო შეფერხებას.	რადგან ხორციელდება მნიშვნელოვანი ინფორმაციის გარე დაცულ სერვერებზე შენახვა, პერიოდულად იქმნება ინფორმაციის სარეზერვო ასლები და ინახება (კვირაში ერთხელ). სერიოზული პრობლემის შემთხვევაში ხდება IT დახმარების გაწევა ხარვეზის აღმოსაფხვრელად, საჭიროების შემთხვევაში ხორციელდება ოფიციალურ მომწოდებლებთან დაკონტაქტება. ამ პროცესებში ჩართულია საინფორმაციო ტექნოლოგიების სამსახური და იურიდიული სამსახური	II

საფრთხეების შეფასება და მათზე რეაგირება

მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დასაცავად განსაზღვრული უსაფრთხოების ზომები და ორგანიზაციულ-ტექნიკური ზომების აღწერა

1. უნივერსიტეტი სათანადო ზომების მიღებით უზრუნველყოფს მონაცემთა უსაფრთხოებას, მათ დაცვას შემთხვევითი ან უკანონო განადგურებისგან, შეცვლისაგან, გამჟღავნებისგან, მოპოვებისგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან.

2. მონაცემებზე წვდომა აქვთ მხოლოდ იმ თანამშრომლებს და იმ მოცულობით, რომელთაც მონაცემები სჭირდებათ საკუთარი ფუნქცია-მოვალეობების შესასრულებლად.

3. უნივერსიტეტის პერსონალისა და სტუდენტების პირადი მონაცემების შენახვა ხდება როგორც მატერიალური, ისე ელექტროუნლი ფორმით, კერძოდ, კომპიუტერებში, დრაივზე, სასწავლო პროცესის მართვის ელექტრონულ სისტემაში და მეხსიერების ბარათებზე.

4. უნივერსიტეტი ელეტრონული სახით ინფორმაციის შესანახად და გადასაგზავნად იყენებს Microsoft-ის და Google-ის ღრუბლოვან სისტემებს.

5. სასწავლო პროცესის მართვის ელექტრონულ სისტემაში არსებული მონაცემები ინახება Microsoft Azure ღრუბლის სისტემაში. მონაცემები ინახება Google sheet-შიც. Google Drive-ზე ინახება პირადობის მოწმობა, უნივერსიტეტის მიერ გაფორმებული ხელშრეკრულებები, რომლებიც, თავის მხრივ, მატერიალურადაც ინახება ფიზიკურ სივრცეში - უნივერსიტეტის მიერ ცალკე გამოყოფილ ოთახში, ბაინდერებში.

6. შპს ჯეოლაბის მიერ დამუშავებული მონაცემები ინახება ორგანიზაციის Google Drive-ზე, რომელზე წვდომაც აქვთ მენეჯერებს, რომლებიც უშუალოდ არიან ჩართულები პროცესებში.

7. უნივერსიტეტში ყველა კორპორატიულ იმეილს აქვს საკუთარი დრაივი და თითოეული მფლობელი უფლებამოსილია, ატვირთოს მასალები. საზიარო დრაივის შემთხვევაში თავად თანამშრომლები წყვეტენ ვის გაუზიარონ კონკრეტული ფაილი, რისი აღრიცხვაც ხდება. დრაივზე არსებული გასაზიარებელი მასალების სუბიექტთა წრე მოიცავს უნივერსიტეტში დასაქმებულ პირებს, რომლებიც სარგებლობენ კორპორატიული მეილით.

8. უნივერსიტეტი მონაცემებს ინახავს უნივერსიტეტის კუთვნილ კომპიუტერებში. სასწავლო პორტალის გახსნა უნივერსიტეტის ან კორპორატიული ელ. ფოსტის მეშვეობით შესაძლებელია არასერვერულ მოწყობილობებში სამუშაო და საგანმანათლებლო პროცესის შეუფერხებლად წარმართვის მიზნით.

9. უნივერსიტეტი უზრუნველყოფს განსაკუთრებული კატეგორიის მონაცემების ცალკე შენახვას როგორც ელექტრონული, ისე მტერიალური ფაილინგის სისტემით. აღნიშნულ ფაილებზე წვდომა აქვს მხოლოდ უნივერსიტეტის ომბუდსმენს.

10. უცხოელ სტუდენტთა მიღებისას მონაცემებზე წვდომა აქვთ მხოლოდ შესაბამის პოზიციაზე მომუშავე პირებს. აღნიშნულზე მონიტორინგს უზრუნველყოფს ადმინისტრატორი.

11. უნივერსიტეტი სარგებლობს სასწავლო პრცესის მართვის ელექტრონული სისტემით, რომელშიც უსაფრთხოების მიზნით, განსაზღვრულია მომხმარებლის სახელით და პაროლით ავტენთიფიკაციის მექნიზმი. პროგრამულად განისაზღვრება ავტენთიფიცირებული მომხმარებლის ავტორიზაციის დონეები და როლები. სისტემა ინტეგრირებულია Google პლატფორმასთან, შესაბამისად, სტუდენტი პორტალზე ავტორიზაციას გადის უნივერსიტეტის მიერ შექმნილი პირადი ელ-ფოსტით და მასზე არსებული პაროლით. აკადემიური და ადმინისტრაციული პერსონალის მომხმარებლის დამატება

ხდება სისტემის ადმინისტრატორის მიერ, ხოლო მათი სისტემაში ავტორიზაცია ხორციელდება ან ინდივიდუალური მომხმარებლის სახელითა და პაროლით, ან უნივერსიტეტის მიერ შექმნილი ელ-ფოსტით. აკრძალულია მომხმარებლის სახელისა და პაროლის მესამე პირისთვის გამჟღავნება/სარგებლობაში გადაცემა.

12. ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული მოქმედებები აღირიცხება/ლოგირდება შესაბამის სისტემაში. არაელექტრონული ფორმით არსებულ მონაცემთა დამუშავებისას უნივერსიტეტის დასაქმებული შესაბამისი პირ(ებ)ი ვალდებული არიან უზრუნველყონ მონაცემთა გამჟღავნებასთან ან/და ცვლილებასთან დაკავშირებული ყველა მოქმედების (მათ შორის, ინციდენტების შესახებ ინფორმაციის) აღრიცხვა.

13. ელექტრონული ფორმით არსებული მონაცემები განთავსებულია საერთო წვდომის ფაილებში, რომლებზე წვდომაც აქვს უნივერსიტეტში დასაქმებულ პირებს მხოლოდ სამსახურეობრივი მოვალეობის შესასრულებლად საჭირო ინფორმაციის ფარგლებში და მხოლოდ კორპორატიული ელ.ფოსტის მეშვეობით.

14. უნივერსიტეტი სარგებლობს ვებგვერდით - www.gau.edu.ge, რომელიც ინფორმაციული ხასიათისაა, ვინაიდან ვებგვერდზე არ ხდება სხვა პირის მიერ მონაცემების ატვირთვა. ვებგვერდზე ხორციელდება უნივერსიტეტში მიმდინარე ღონისძიებების, ფოტომასალების ასახვა. ასევე, გარკვეული სახის დოკუმენტაციის, კერძოდ, წესდების, შინაგანაწესისა, დებულების, აკადემიურ და ადმინისტრაციულ პერსონალის შესახებ ინფორმაციის, მათ შორის საკონტაქტო ინფორმაციის ატვირთა. როგორც საიდენტიფიკაციო, ისე ბიომეტრიული მონაცემების ვებ-საიტზე გამოქვეყნებასთან დაკავშირებით უნივერსიტეტი უზრუნველყოფს მონაცემთა სუბიექტებისგან ექსპლიციტური თანხმობის მიღებას შესაბამის თანხმობის ფურცელზე ხელმოწერით.

15. უნივერსიტეტი ინფორმაციას იღებს შპს ჯეოლაბის ვებ-გვერდიდან - https://geolab.edu.ge. შპს ჯეოლაბი უნივერსიტეტის ადმინისტრაციულ-ფინანსურ სამსახურს აწვდის მხოლოდ სტუდენტების შესაბამის მონაცემებს (ადმინისტრაციის ნაწილში). ასევე, ცნობებს სასწავლო დაწესებულებიდან, რათა სტუდენტებმა ისარგებლონ ფასდაკლებით. შპს ჯეოლაბის ვებ-გვერდზე რეგისტრირდებიან კურსის გავლის მსურველები და ავსებენ ისეთ მონაცემებს, როგორებიცაა: სასურველი კურსი; სახელი და გვარი; ელფოსტა; პირადი ნომერი; ტელეფონის ნომერი; საცხოვრებელი ქალაქი; საცხოვრებელ მისამართი; დაბადების ადგილი; დაბადების თარიღი; სამუშაო ადგილი/საწავლებელი; სოციალური ქსელის ბმული და სხვა. ჯეოლაბის ვებგვერდზე ინახება სტანდარტული მონაცემი, როგორიცაა არის IP მისამართი.

16. უნივერსიტეტი სარგებლობს COOKIES სისტემით და იყენებს შემდეგ COOKIES:

ა) october_session : გამოიყენება მომხმარებლის სესიის იდენტიფიკაციისთვის უნიკალური ID-ის მინიჭებით;

ბ) _ga: დაინსტალირებულია Google Analytics-ის მიერ, ითვლის ვიზიტორებს, სესიას და თვალყურს ადევნებს საიტის გამოყენებას საიტის ანალიტიკური ანგარიშისთვის. ქუქი-ფაილი ინახავს ინფორმაციას ანონიმურად და ანიჭებს შემთხვევით გენერირებულ ნომერს უნიკალური ვიზიტორების ამოსაცნობად;

გ) _gid: დაინსტალირებულია Google Analytics-ის მიერ და ინახავს ინფორმაციას იმის შესახებ, თუ როგორ იყენებენ ვიზიტორები ვებსაიტს და ასევე ქმნის ანალიტიკურ ანგარიშს ვებსაიტის მუშაობის შესახებ. შეგროვებული ზოგიერთი მონაცემი მოიცავს ვიზიტორთა რაოდენობას, მათ წყაროს და გვერდებს, რომლებსაც ისინი ანონიმურად სტუმრობენ;

დ) _gat_gtag_UA_*: Google Analytics იყენებს აღნიშნულ ქუქი-ფაილს მომხმარებლის უნიკალური ID-ის შესანახად;

ე) _ga_*: Google Analytics იყენებს აღნიშნულ ქუქი-ჩანაწერს გვერდების ნახვების შესანახად და დასათვლელად;

ვ) YSC: გამოიყენება Youtube გვერდებზე ჩაშენებული ვიდეოების ნახვებისთვის თვალყურის დევნის მიზნით;

ზ) VISITOR_INFO1_LIVE: გამოიყენება YouTube-ის მიერ გამტარუნარიანობის გასაზომად;

თ) VISITOR_PRIVACY_METADATA: YouTube იყენებს აღნიშნულ ქუქი ფაილს მომხმარებლის ქუქიების თანხმობის მდგომარეობის შესანახად მიმდინარე დომენზე;

ი) guest_id: Twitter იყენებს აღნიშნულ ქუქი-ფაილს, ვებსაიტის ვიზიტორის იდენტიფიცირებისა და თვალყურის დევნისათვის. თუ მომხმარებელი შესულია Twitter-ის პლატფორმაზე არეგისტრირებს და აგროვებს ინფორმაციას რეკლამის პრეფერენციების შესახებ.

17. უნივერსიტეტის ვებგვერდში ჩაშენებულია google analitics, რომელიც იძლევა ზოგად ინფორმაციას იმის თაობაზე, თუ რომელი ქყვეყნიდან და რამდენი მომხმარებელი ესტუმრა საიტს, პირდაპირ საიტზე შემოვიდა თუ სხვა სოციალური ქსელიდან გადმოვიდა და რომელი მოწყობილობით შემოვიდა.

18. დასაქმებულთა მატერიალური ფორმით არსებული დოკუმენტაცია (მიმდინარე დოკუმენტები, აქტიური პირადი საქმეები) ინახება პერსონალის მართვის სამსახურში ბაინდერებში აკინძული ფორმით, შესაბამის კარადაში, რომელიც იკეტება გასაღებით. დასკანერებულია ყველა დასაქმებულის დოკუმენტები. სტუდენტების პირადი საქმეები დასკანერებულია და მათზე წვდომა აქვთ შესაბამისი ფაკულტეტის დეკანატის თანამშრომლებს. სტუდენტების მატერიალური ფორმით არსებული დოკუმენტაცია (მიმდინარე დოკუმენტები, აქტიური პირადი საქმეები), ასევე, ინახება შესაბამისი ფაკულტეტის დეკანატებში ბაინდერებში აკინძული ფორმით. დოკუმენტებზე ან/და მათში დაცულ ინფორმაციაზე წვდომა შესაძლებელია მხოლოდ პერსონალის მართვის სამსახურისგან აღნიშნული დოკუმენტაციის მიღების და შესაბამისი აღრიცხვის გზით.

19. უნივერსიტეტში სტუდენტებისა და დასაქმებულების პირადი საქმეები არქივდება როგორც ფიზიკური, ისე ელექტრონული სახით. აღნიშნული მონაცემები ფიზიკურად დასაარქივებლად გადაეცემა სტუდენტთა მომსახურების სამსახურს. კანცელარია აარქივებს კანცელარიაში დაცულ ინფორმაციას, ხოლო პერსონალის მართვის სამსახური აარქივებს პერსონალთან დაკავშირებულ არააქტიურ ფაილებს. უნივერსიტეტის მიერ გამოყოფილია ცალკე ოთახი საცავში, რომელშიც ინახება დაარქივებული სახით მონაცემები. აღნიშნულ საცავში შესვლა შეუძლია პერსონალის მართვის სამსახურის სტუდენტთა მომსახურების სამსახურის და კანცელარიის თანამშრომლებს თავისი დაშვების დონის შესაბამისად. არქივის ოთახში შესვლა აღირიცხება. უნივერსიტეტში, ასევე, IT სამსახური ახორციელებს მონაცემების ელექტრონულად დაარქივებას მყარ დისკებზე.

20. განსაკუთრებული კატეგორიის მონაცემებიდან, როგორიცაა ჯანმრთელობაზე ინფორმაცია, ინახება პირად საქმეებში და ელექტრონულ სისტემაში და მათზე წვდომა ხდება მხოლოდ ავტორიზებული პირების მიერ. გათვალისწინებულია უსაფრთხოებისა და წვდომაზე აღრიცხვის სისტემა.

დამუშავებისთვის პასუხისმგებელი პირის მიერ განხორციელებული/დაგეგმილი კონკრეტული ღონისძიებები, რომლებიც აღმოფხვრის ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეებს ან/და ამცირებს მათი დადგომის მაღალ ალბათობას

უნივერსიტეტი ვალდებულია მონაცემთა სუბიექტს დეტალურად აცნობოს ინფორმაცია იმის შესახებ, თუ რა მონაცემებს აგროვებს, როგორ იყენებს მათ, ვის გადასცემს და როგორ იცავს მონაცემთა უსაფრთხოებას.

უნივერსიტეტში დასაქმებული ნებისმიერი პირი, რომელიც მონაწილეობს მონაცემთა დამუშავებაში ან რომელსაც აქვს მონაცემებზე წვდომა, ვალდებულია:

ა) არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს;

ბ) დაიცვას მონაცემთა საიდუმლოება და კონფიდენციალურობა, მათ შორის, სამსახურებრივი

უფლებამოსილების შეწყვეტის შემდეგ;

გ) არ გამოიყენოს მონაცემები პირადი, არასამსახურებრივი მიზნებისთვის;

დ) არ გახადოს მონაცემები ხელმისაწვდომი არაუფლებამოსილი პირებისათვის, მათ შორის მონაცემთა უყურადღებოდ დატოვების და/ან არაუფლებამოსილი პირების თანდასწრებით განხილვის გზით.

წინამდებარე დოკუმენტით დადგენილი წესების დარღვევა წარმოადგენს უნივერსიტეტის შინაგანაწესისა, პერსონალთან დადებული ხელშეკრულებებისა და სამედიცინო კვლევებისა და პროექტების ჩატარების პროცესში უნივერსიტეტის კვლევის კეთილსინდისიერების კომიტეტის მიერ შემუშავებული დებულების დარღვევას და ითვალისწინებს შესაბამის დისციპლინურ ზომას. კონფიდენციალური ინფორმაციის დაცვის ვალდებულება თანამშრომლის სამუშაოდან წასვლის შემდგომაც არსებობს.

მონაცემთა უსაფრთხოება უზრუნველყოფილია უნივერსიტეტის ინფორმაციული უსაფრთხოების პოლიტიკის შესაბამისად. ვებგვერდზე მონაცემთა უსაფრთხოების უზრუნველსაყოფად მიღებულია შესაბამისი ორგანიზაციულ-ტექნიკური ზომები (მათ შორის, შეღწევადობის ტესტირებები, მონაცემებზე წვდომის შეზღუდვა იმ მომხმარებლებით, რომელთა უშუალო ფუნქცია-მოვალეობებში შედის მონაცემთა დამუშავება).

უნივერსიტეტში მონაცემთა დამუშავება ხორციელდება ციფრული ფაილებისთვის მონაცემთა წაშლის უსაფრთხო პროტოკოლებით (სერთიფიცირებული წაშლის ხელსაწყოების გამოყენებით), ხოლო ფიზიკური დოკუმენტები შრედერდება ან იწვება.

ამასთან, მონაცემთა გადაცემის ყველა აქტივობა აღრიცხულია და შემოწმებულია. მონაცემთა გადაცემის შემთხვევაში უნივერსიტეტი უზრუნველყოფს შესაბამისი ინფორმირებული თანხმობების მოპოვებას მონაცემთა სუბიექტებისგან.

ამასთან, პერსონალურ მონაცემთა დაცვა ხორციელდება უნივერსიტეტის პერსონალის ტრენინგის სესიებით, შესაბამისი დოკუმენტაციის დანერგვით, როგორებიცაა პერსონალურ მონაცემთა დაცვის პოლიტიკა, ინციდენტზე რეაგირების გეგმა, ვიდეო-მონიტორინგის დებულება და სხვა. ამათან უნივერსიტეტი ახორციელებს მონაცემთა დამუშავების რეგულარულ აუდიტს პერსონალურ მონაცემთა დაცვის ოფიცრის მეშვეობით, ასევე რევიზიას დანერგილი დოკუმენტაციის, მათში საჭიროების შემთხვევაში ცვლილებების განხორციელების და შესაბამისად, კანონთან შესაბამისობის მიზნით.

ნაწილი III - ინფორმაცია ზეგავლენის შეფასების პროცესში გამოყენებული მეთოდოლოგიის შესახებ

ზეგავლენის შეფასებისას გამოყენებული მეთოდოლოგია
კანონმდებლობა ითვალისწინებს ზეგავლენის შეფასების სხვადასხვა ეტაპზე გამოსაყენებელ მეთოდებსა და ინსტრუმენტებს: ა) „SWOT“ ანალიზი - სტრატეგიული დაგეგმარების მეთოდი, რომელიც აფასებს დამუშავებისთვის პასუხისმგებელი პირის მდგომარეობას, მის შესაძლებლობებს და შეისწავლის საქმიან გარემოს, მათ შორის, ახდენს დაინტერესებული მხარეების მოლოდინების, ასევე მონაცემთა დამუშავების პროცესის ძლიერი და სუსტი მხარეების, შესაძლებლობებისა და საფრთხეების ანალიზს, ადგენს დამუშავებისთვის პასუხისმგებელი პირის წინაშე არსებულ მოთხოვნებსა და მონაცემთა დამუშავების პროცესის მონაწილეების უნარებს. ბ) ინდივიდუალური და ჯგუფური დისკუსიები - იგეგმება საჭიროებიდან გამომდინარე, ნებისმიერი რელევანტური ინფორმაციის გადაცემის/გაზიარების მიზნით; გ) სამუშაო შეხვედრები/სემინარები - მიზნად ისახავს მონაცემთა დამუშავების პროცესის მონაწილეებისთვის საფრთხის შესახებ ინფორმაციის გაზიარებას.
პერსონალურ მონაცემთა დაცვის ოფიცერთან კონსულტირების მექანიზმის გამოყენება: თუ ზეგავლენის შეფასების შედეგად გამოვლინდება საფრთხე, უნივერსიტეტი იღებს ყველა აუცილებელ ზომას საფრთხეების არსებითად შესამცირებლად და კონსულტაციის მიზნით მიმართავს პერსონალურ მონაცემთა დაცვის ოფიცერს წინასწარი კონსულტაციის მიღების მიზნით.