სსიპ ბათუმის შოთა რუსთაველის
სახელმწიფო უნივერსიტეტი

05 ივნისი, 2024 წელი

ბრძანება №01-02/ 75

ბსუ-ში პერსონალურ მონაცემთა დაცვის პოლიტიკის დამტკიცების თაობაზე

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის, „უმაღლესი განათლების შესახებ“ საქართველოს კანონის 22-ე მუხლის, ბსუ-ს წესდების მე-13 მუხლის, ,,ბსუ-ს ელექტრონული სერვისების ადმინისტრირების წესის დამტკიცების შესახებ“ ბსუ-ს რექტორის 2021 წლის 07 სექტემბრის N01-02/154 ბრძანების საფუძველზე

ვბრძანებ:

1. დამტკიცდეს წინამდებარე ბრძანების N1 **დანართის** შესაბამისად **ბსუ-ში პერსონალურ მონაცემთა დაცვის პოლიტიკა.**
2. ბრძანება გამოქვეყნდეს ბსუ-ს ვებგვერდზე (,,ველებში: ,,საუნივერსიტეტო ნორმატიული აქტები“; ,,რექტორის ბრძანებები“).
3. წინამდებარე ბრძანებით დამტკიცებული პოლიტიკა განთავსდეს ბსუ-ს სტუდენტურ პორტალზე და სტუდენტის გზამკვლევში (იურიდიულმა დეპარტამენტმა უზრუნველყოს შესაბამის თავში ამ პოლიტიკის დამატება).
4. ბრძანება დაეგზავნოს ბსუ-ს რექტორის მოადგილეებს, ადმინისტრაციის ხელმძღვანელს, ბსუ-ს ხარისხის უზრუნველყოფის სამსახურს, ბსუ-ს დამოუკიდებელ სამეცნიერო-კვლევით ინსტიტუტებს, ფაკულტეტებს, საქმისწარმოების სამსახურს (კანცელარია), საინფორმაციო ტექნოლოგიების სამსახურს, იურიდიულ დეპარტამენტს, სასწავლო პროცესის დეპარტამენტს, საზოგადოებასთან ურთიერთობის სამსახურს და ყველა სტრუქტურულ ერთეულს.
5. ბრძანება ძალაშია ხელმოწერისთანავე.
6. ბრძანება შეიძლება გასაჩივრდეს კანონმდებლობით დადგენილ ვადაში და წესით ბათუმის საქალაქო სასამართლოში (ქ. ბათუმი, სტეფანე ზუბალაშვილის №30).

რექტორი, პროფესორი **მერაბ ხალვაში**

ბსუ-ს რექტორის 2024 წლის
05 ივნისის N01-02/75 ბრძანების
N1 დანართი

ბსუ-ში პერსონალურ მონაცემთა დაცვის პოლიტიკა

მუხლი 1. ზოგადი დებულებანი

1. საჯარო სამართლის იურიდიული პირი - ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტში (შემდგომში - „უნივერსიტეტი“ ან „ბსუ“ ან „დამსაქმებელი“) პერსონალურ მონაცემთა დაცვის პოლიტიკა (შემდგომში - „პოლიტიკა“ ან „წესი“) შემუშავებულია საქართველოს კანონმდებლობის, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის, „უმაღლესი განათლების შესახებ“ საქართველოს კანონის, ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის, ბსუ-ს წესდების, ეთიკის კოდექსისა და სხვა სამართლებრივი აქტების მოთხოვნათა დაცვით.
2. წინამდებარე წესის მიზანია პერსონალური მონაცემების (შემდგომში - „მონაცემი“) დამუშავებისას უზრუნველყოს უნივერსიტეტის პერსონალის (აკადემიური, სამეცნიერო, ადმინისტრაციული, დამხმარე, მოწვეული მასწავლებელთა პერსონალი, პროფესიული განათლების მასწავლებელთა პერსონალი, შრომითი ხელშეკრულებით დასაქმებული სხვა პირები), სტაჟიორების, სტუდენტების/მასწავლებლის მომზადების საგანმანათლებლო პროგრამაზე ჩარიცხული პირების (შემდეგში - სტუდენტები), პროფესიული სტუდენტების, მსმენელების უფლებათა და თავისუფლებათა დაცვა.
3. ბსუ-ში პერსონალურ მონაცემთა დამუშავების პრინციპებია: სამართლიანობა, კანონიერება, კონკრეტული კანონიერი მიზნის არსებობის აუცილებლობა, ადეკვატურობა, პროპორციულობა, ნამდვილობა, სიზუსტე, მონაცემების შენახვის ვადა.

მუხლი 2. ტერმინთა განმარტება

1. წინამდებარე წესის მიზნებისთვის მასში გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:
ა) პერსონალური მონაცემი - ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. ფიზიკური პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, მათ შორის, სახელით, გვარით, საიდენტიფიკაციო ნომრით, გეოლოკაციის მონაცემებით, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემებით, ფიზიკური, ფიზიოლოგიური, ფსიქიკური, ფსიქოლოგიური, გენეტიკური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლით;
ბ) განსაკუთრებული კატეგორიის მონაცემი - მონაცემები დაკავშირებული პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიულ კავშირში გაწევრიანებასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლობასთან,

ადმინისტრაციულ პატიმრობასთან, პირისთვის აღკვეთის ღონისძიების შეფარდებასთან, პირთან საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან, აგრეთვე ბიომეტრიული და გენეტიკური მონაცემები, რომლებიც ზემოაღნიშნული ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა;

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

დ) მონაცემთა ავტომატური საშუალებებით დამუშავება – მონაცემთა დამუშავება ინფორმაციული ტექნოლოგიების გამოყენებით;

ე) მონაცემთა არაავტომატური საშუალებებით დამუშავება – მონაცემთა დამუშავება ინფორმაციული ტექნოლოგიების გამოყენების გარეშე;

ვ) მონაცემთა ნახევრად ავტომატური საშუალებებით დამუშავება – მონაცემთა დამუშავება ავტომატური საშუალებებისა და არაავტომატური საშუალებების ერთობლივი გამოყენებით;

ზ) ფაილური სისტემა – მონაცემთა სტრუქტურიზებული წყება, რომელშიც ისინი დალაგებული და ხელმისაწვდომია კონკრეტული კრიტერიუმის მიხედვით;

თ) მონაცემთა სუბიექტი - ნებისმიერი ფიზიკური პირი, რომლის მონაცემებიც მუშავდება უნივერსიტეტის მიერ;

ი) მონაცემთა სუბიექტის თანხმობა – მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე აქტიური მოქმედებით, წერილობით (მათ შორის, ელექტრონულად) ან ზეპირად, თავისუფლად და მკაფიოდ გამოხატული ნება;

კ) მონაცემთა სუბიექტის წერილობითი თანხმობა – თანხმობა, რომელსაც მონაცემთა სუბიექტმა ხელი მოაწერა ან რომელიც მან სხვაგვარად გამოხატა წერილობით (მათ შორის, ელექტრონულად) მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე შესაბამისი ინფორმაციის მიღების შემდეგ;

ლ) დამუშავებისთვის პასუხისმგებელი პირი - ბსუ, რომელიც თავისი კომპეტენციის ფარგლებში განსაზღვრავს პერსონალურ მონაცემთა დამუშავების მიზნებსა და საშუალებებს და მონაცემების დამუშავებას ახდენს უშუალოდ ან უფლებამოსილი პირის მეშვეობით;

მ) უფლებამოსილი პირი - ნებისმიერი ფიზიკური ან იურიდიული პირი, რომელიც ამუშავებს მონაცემებს უნივერსიტეტისთვის ან მისი სახელით;

ნ) მონაცემთა მიმღები - ნებისმიერი დაწესებულება, ფიზიკური ან იურიდიული პირი, კერძო ან საჯარო სექტორის თანამშრომელი, რომელსაც უნივერსიტეტი გადასცემს მონაცემებს, გარდა პერსონალურ მონაცემთა დაცვის სამსახურისა;

ო) ვიდეომონიტორინგი – ბსუ-ში განთავსებული/დამონტაჟებული ტექნიკური საშუალებების გამოყენებით ვიზუალური გამოსახულების მონაცემთა დამუშავება, კერძოდ, ვიდეოკონტროლი ან/და ვიდეოჩაწერა (გარდა ფარული საგამოძიებო მოქმედებისა);

პ) ინციდენტი - მონაცემთა უსაფრთხოების დარღვევა, რომელიც იწვევს მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე უნებართვო

გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას ან სხვაგვარ უნებართვო დამუშავებას;

ჟ) პერსონალურ მონაცემთა დაცვის ოფიცერი - ბსუ-ს მიერ განსაზღვრული/ დანიშნული პირი, რომელიც ასრულებს ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონითა და წინამდებარე წესით განსაზღვრულ ფუნქციებს.

2. წინამდებარე წესში გამოყენებული სხვა ტერმინები განიმარტება ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის (შემდეგში - კანონის) შესაბამისად.

მუხლი 3. მონაცემთა დამუშავება

1. ბსუ-ში მონაცემებს დამუშავება ხორციელდება ავტომატური, ნახევრად ავტომატური და არაავტომატური საშუალებების გამოყენებით.

2. უნივერსიტეტი ამუშავებს პერსონალის (აკადემიური, სამეცნიერო, ადმინისტრაციული, დამხმარე, მოწვეული მასწავლებელთა პერსონალი, პროფესიული განათლების მასწავლებელთა პერსონალი, შრომითი ხელშეკრულებით დასაქმებული სხვა პირები), სტაჟიორების, სტუდენტების, პროფესიული სტუდენტების, მსმენელებისა და სხვა პირების (სახელშეკრულებო ურთიერთობებიდან გამომდინარე) პერსონალურ მონაცემებს.

3. უნივერსიტეტი უზრუნველყოფს პერსონალური მონაცემების დამუშავების შესახებ მონაცემთა სუბიექტების ინფორმირებას, მათთან გაფორმებული ხელშეკრულებისა და წინამდებარე წესის მეშვეობით.

4. არასრულწლოვნის შესახებ მონაცემთა დამუშავებისას გათვალისწინებული უნდა იქნას მისი საუკეთესო ინტერესები. არასრულწლოვანის შესახებ მონაცემთა დამუშავება მისი თანხმობის საფუძველზე დასაშვებია, თუ მან 16 წლის ასაკს მიაღწია, ხოლო 16 წლამდე არასრულწლოვანის შესახებ მონაცემთა დამუშავება – მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობით.

5. ბსუ ძირითადად ამუშავებს ისეთ მონაცემთა კატეგორიას, როგორიცაა: პერსონალისა და სტუდენტის/პროფესიული სტუდენტის/ მსმენელის სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი, მოქალაქეობა, ტელეფონის ნომერი, ელექტრონული ფოსტა, ფაქტობრივი/იურიდიული მისამართი, საბანკო რეკვიზიტები, სამუშაო გამოცდილება, სამეცნიერო საქმიანობა, უნივერსიტეტში სტუდენტის, პროფესიული სტუდენტის სასაწავლო პროცესთან, ასევე პერსონალის შრომითი ურთიერთობიდან და საუნივერსიტეტო აქტივობებიდან/საქმიანობიდან გამომდინარე სხვა მონაცემები.

6. ბსუ-ს მიერ დამუშავებული მონაცემები აისახება:

ა) საქმისწარმოების ელექტრონულ სისტემაში (e-FLOW), რომელზეც თითოეულ მომხმარებელს წვდომა აქვს, მისი სახელი და გვარის (მომხმარებელი) და უნიკალური/ინდივიდუალური პაროლის მეშვეობით;

ბ) ბსუ-ს ოფიციალურ ვებგვერდზე - www.bsu.edu.ge (ადმინისტრირება ხორციელდება და სხვა სტრუქტურულ ერთეულებს/მართვის ორგანოებს წვდომა აქვს ბსუ-ს რეგულაციების შესაბამისად; ძირითადი ადმინისტრატორია ბსუ-ს საინფორმაციო ტექნოლოგიების სამსახური და საზოგადოებასთან ურთიერთობის სამსახური);

გ) სასწავლო პროცესის მართვის ელექტრონულ სისტემასა (spm.bsu.edu.ge) და ბსუ-ს ელექტრონულ პორტალზე (portal.bsu.edu.ge), ბსუ-ს ელექტრონული სერვისების

ადმინისტრირების წესის შესაბამისად (ადმინისტრატორია ბსუ-ს სასწავლო პროცესის დეპარტამენტი);
დ) უმაღლესი განათლების მართვის საინფორმაციო სისტემაში (ბსუ-ს, როგორც ავტორიზებული მომხმარებლის, მიერ აისახება კანონმდებლობით გათვალისწინებული ინფორმაცია; წვდომა აქვს ბსუ-ს ხარისხის უზრუნველყოფის სამსახურს და სასწავლო პროცესის დეპარტამენტს);
ე) პროფესიული განათლების მართვის საინფორმაციო სისტემაში (ბსუ-ს, როგორც ავტორიზებული მომხმარებლის, მიერ აისახება კანონმდებლობით გათვალისწინებული ინფორმაცია; წვდომა აქვს ბსუ-ს პროფესიული პროგრამების მართვისა და უწყვეტი განათლების ცენტრის უფლებამოსილ პერსონალს);
ვ) საქართველოს სახელმწიფო ხაზინის ელექტრონული მომსახურების სისტემაში (წვდომა აქვს ბსუ-ს საფინანსო-ეკონომიკურ დეპარტამენტს და ადმინისტრაციის ხელმძღვანელს);
ზ) სწავლის საფასურის/ფინანსური დავალიანების მქონე სტუდენტების/პირების შესახებ მონაცემთა ბაზაში (აწარმოებს ბსუ-ს ბუღალტერია);
თ) სახელმწიფო შესყიდვების ერთიანი ელექტრონულ სისტემაში (აწარმოებს ბსუ-ს შესყიდვების სამსახური).

7. ბსუ-ში დამუშავებული მონაცემების შენახვის ვადები განსაზღვრულია საქართველოს კანონმდებლობისა და ბსუ-ს საქმეთა ნომენკლატურის, შესაბამისი სასწავლო პროცესის მარეგულირებელი სამართლებრივი აქტების მიხედვით. პერსონალური ინფორმაციის განსაზღვრული მიზნებით დამუშავება გაგრძელდება იმ ვადით, რომელიც შეესაბამება უნივერსიტეტის მიერ გასაწევი მომსახურების/საქმიანობის მიზნებს ან/და გათვალისწინებულია კანონმდებლობით.

მუხლი 4. მონაცემთა დამუშავების მიზანი

1. ბსუ მონაცემებს ამუშვებს მხოლოდ კანონიერი მიზნებისთვის და შესაბამისი მოცულობით.
2. ბსუ-ს მიერ მონაცემების დამუშავების მიზანია:
ა) სტუდენტის/პროფესიული სტუდენტის, მსმენელის სტატუსთან, სასწავლო პროცესთან, საუნივერსიტეტო აქტივობებთან და სხვადასხვა შეღავათებთან დაკავშირებით სამართლებრივი აქტების გამოცემა (სტატუსის მინიჭება/შეწყვეტა/შეჩერება/მობილობა/ კრედიტების აღიარება/სასწავლო პროცესში დაბრუნება/დაჯილდოება/შეღავათის მინიჭება სწავლის საფასურში/განთავისუფლება/სტიპენდიის დანიშვნა/პრაქტიკაზე დაშვება და სხვა);
ბ) პლაგიატის პრევენცია და მისი გამოვლენა;
გ) დასაქმებულთან შრომითი ხელშეკრულების გაფორმება, მივლინების და პროფესიული განვითარების ღონისძიებაში მონაწილეობის ხარჯების ანაზღაურება;
დ) დასაქმებულის შეფასების პროცესის წარმართვა, წახალისებისა და დისციპლინური ღონისძიებების გატარება;
ე) პერსონალის ჯანმრთელობის დაზღვევა;
ვ) განცხადების/საჩივრის განხილვა;
ზ) მონაცემთა სუბიექტთან დადებული ხელშეკრულებით ნაკისრი ვალდებულების შესრულება;

თ) მომსახურების ან საქონლის მოწოდებისათვის ფიზიკურ პირებთან ანგარიშსწორება;
ი) სახელმწიფო შესყიდვების განხორციელება;
კ) სხვადასხვა ანგარიშების, სტატისტიკური მონაცემების და კვლევების/პროექტების განხორციელება;
ლ) მონაცემთა უსაფრთხოების უზრუნველყოფა;
მ) ბსუ-ს ან სხვა პირების უსაფრთხოებისა და საკუთრების დაცვა;
ნ) მონაცემთა სუბიექტისათვის შესაბამისი კორესპონდენციის/შეტყობინების გაგზავნა/ჩაბარება;
ო) თანამშრომლობის ხელშეკრულების/მემორანდუმის/შეთანხმების გაფორმება ან/და ცვლილებების/დამატებების შეტანა;
პ) საქართველოს კანონმდებლობით, ბსუ-ს წესდებით, შინაგანაწესითა და სხვა შიდა სამართლებრივი აქტებით განსაზღვრული უფლებამოსილებების განხორციელება.
3. უნივერსიტეტი უფლებამოსილია პერსონალურ მონაცემთა შემცველი დოკუმენტი/სამართლებრივი აქტი გამოაქვეყნოს საჯარო გაცნობისათვის, თუ ეს განსაზღვრულია კანონით ან ეხება 50-ზე მეტ პირს.

მუხლი 5. მონაცემთა დამუშავების საფუძვლები

1. მონაცემთა დამუშავება დასაშვებია, თუ:

ა) მონაცემთა დამუშავება გათვალისწინებულია კანონით;
ბ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტთან დადებული გარიგებით ნაკისრი ვალდებულების შესასრულებლად ან მონაცემთა სუბიექტის მოთხოვნით გარიგების დასადებად;
გ) მონაცემთა სუბიექტმა განაცხადა თანხმობა მის შესახებ მონაცემთა დამუშავებაზე, ერთი ან რამდენიმე კონკრეტული მიზნით;
დ) მონაცემთა დამუშავება საჭიროა დამუშავებისთვის პასუხისმგებელი პირის მიერ საქართველოს კანონმდებლობით მისთვის დაკისრებული მოვალეობების შესასრულებლად;
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, მათ შორის, ეპიდემიის მონიტორინგის ან/და მისი გავრცელების აღკვეთის, ჰუმანიტარული კრიზისების, ბუნებრივი და ადამიანის მოქმედებით გამოწვეული კატასტროფების სამართავად;
ზ) მონაცემთა დამუშავება აუცილებელია მნიშვნელოვანი საჯარო ინტერესის დასაცავად;
თ) 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;
ი) 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 6. პერსონალური მონაცემების დაცვა

1. ბსუ-ს საქმიანობის სპეციფიკიდან გამომდინარე მონაცემები ინახება, როგორც ელექტრონული სახით, ასევე მატერიალური სახით.

2.უნივერსიტეტი უზრუნველყოფს ელექტრონული ინფორმაციის დამმუშავებელი მოწყობილობის დაცვას არაავტორიზებული წვდომისგან.

3. **ბსუ** <u>ელექტრონული სახით არსებულ პერსონალურ მონაცემთა დაცვის მიზნით</u> **უზრუნველყოფს:**

ა) კომპიუტერული ქსელის გამართულად ფუნქციონირებას, ქსელის უსაფრთხოებისთვის გამოიყენება პროგრამული უზრუნველყოფის საშუალებები და ანტივირუსული პროგრამები;

ბ) თითოეულ კომპიუტერთან ინდივიდუალური მომხმარებლის წვდომას;

გ) საქმისწარმოების ელექტრონულ სისტემაში (**eFlow**) წვდომას მხოლოდ უფლებამოსილი პირის მიერ მისთვის მინიჭებული მომხმარებლის სახელითა და პაროლით. დასაქმებულებს წვდომა აქვთ მხოლოდ იმ კორესპონდენციაზე და შესაბამისად, იმ პერსონალურ მონაცემებზე, რომელთა განხილვა/დამუშავება მათ ფუნქცია-მოვალეობას/უფლებამოსილებას წარმოადგენს. სისტემაში სრული ხედვის რეჟიმი (წვდომა ყველა კორესპონდენციაზე) სამსახურებრივი უფლებამოსილებიდან გამომდინარე, აქვს საქმისწარმოების სამსახურს (კანცელარია).

4. უნივერსიტეტი უზრუნველყოფს მონაცემთა ბაზების იმგვარ ადმინისტრირებას, რომ ინფორმაცია ყველა სტუდენტს და დასაქმებულს მიეწოდოს ინდივიდუალურად.

5. ბსუ-ში მატერიალური სახით არსებული მონაცემები შესანახად გადაეცემა საქმისწარმოებაზე (დოკუმენტაციის შენახვაზე) პასუხისმგებელ სტრუქტურულ ერთეულს და მათზე წვდომა აქვთ მხოლოდ შესაბამისი ფუნქცია-მოვალეობის/უფლებამოსილების მქონე პირებს.

6. დასაქმებულის მიერ ინფორმაციის გავრცელება დაიშვება მხოლოდ შესაბამისი სამართლებრივი საფუძვლის არსებობისას.

7. ნებისმიერი პირი, რომელიც აღმოაჩენს დარღვევებს პერსონალურ მონაცემთა დამუშავებასთან მიმართებით, ვალდებულია ამის შესახებ ინფორმაცია დაუყოვნებლივ მიაწოდოს უნივერსიტეტის ადმინისტრაციას (რექტორს/ადმინისტრაციის ხელმძღვანელს).

8. ბსუ უზრუნველყოფს ინფორმაციის მიწოდებას შესაბამისი სამართლადამცავი ორგანოებისთვის, თუ მონაცემების უკანონოდ მოპოვებამ, დამუშავებამ, შენახვამ, გამოყენებამ ან/და გავრცელებამ გამოიწვია <u>მნიშვნელოვანი</u> ზიანი.

მუხლი 7. პერსონალური მონაცემების მოპოვება მესამე პირებისგან

1. 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 პირებთან, სახელმწიფო სექტორში მოქმედ ორგანიზაციებთან, პარტნიორ ორგანიზაციებთან გაფორმებული ხელშეკრულებებიდან გამომდინარე უნივერსიტეტის მიერ ნაკისრი ვალდებულებების შესრულების მიზნებისათვის.
2. მესამე პირს წარმოადგენს ფიზიკური და/ან იურიდიული პირი, სახელმწიფო სექტორში მოქმედი ორგანიზაციები.

მუხლი 8. განსაკუთრებული კატეგორიის მონაცემთა დამუშავება
1.უნივერსიტეტში აკრძალულია განსაკუთრებული კატეგორიის მონაცემთა დამუშავება, გარდა იმ შემთხვევისა, როცა არსებობს სუბიექტის წერილობითი თანხმობა.
2. ბსუ ,,უმაღლესი განათლების შესახებ" საქართველოს კანონის და ,,პროფესიული განათლების შესახებ" საქართველოს კანონის საფუძველზე ამუშავებს განსაკუთრებული კატეგორიის მონაცემებს (პერსონალის ნასამართლობასთან დაკავშირებით).

მუხლი 9. გარდაცვლილი პირის შესახებ მონაცემთა დაცვა
1. მონაცემთა სუბიექტის გარდაცვალების შემდეგ მის შესახებ მონაცემთა დამუშავება დასაშვებია:
ა) წინამდებარე წესის მე-5 მუხლით (,,**მონაცემთა დამუშავების საფუძვლები**") განსაზღვრული საფუძლებით;
ბ) თუ ამ მონაცემთა დამუშავება აკრძალული არ არის მონაცემთა სუბიექტის მშობლის, შვილის, შვილიშვილის ან მეუღლის მიერ (გარდა იმ შემთხვევისა, როდესაც მონაცემთა სუბიექტმა გარდაცვალებამდე წერილობით აკრძალა მისი გარდაცვალების შემდეგ მის შესახებ მონაცემთა დამუშავება).

მუხლი 10. ვიდეო/აუდიო მონიტორინგის განხორციელება
ბსუ-ში ვიდეო/აუდიო მონიტორინგი ხორციელდება ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონისა და ბსუ-ში ვიდეომონიტორინგის განხორციელების რეგულაციის შესაბამისად.

მუხლი 11. პერსონალის უფლება-მოვალეობანი
1. უნივერსიტეტი წინასახელშეკრულებო ურთიერთობის პერიოდში უზრუნველყოფს დასაქმებულის ინფორმირებას, თუ რა სახის პერსონალური მონაცემების დაამუშავება ხორციელდება ბსუ-ში.
2. ბსუ-ს დასაქმებულს უფლება აქვს მოსთხოვოს უნივერსიტეტს ინფორმაცია მის შესახებ მონაცემთა დამუშავების თაობაზე.
3. ბსუ-ში დასაქმებულებს ეკრძალებათ პერსონალური მონაცემების შემცველი დოკუმენტებისა და ფაილების უყურადღებოდ დატოვება.

4. უნივერსიტეტის დასაქმებული ვალდებულია არ გაამჟღავნოს და არ გადასცეს ბსუ-ში არსებული სხვისი პერსონალური მონაცემები სხვა პირებს. აღნიშნული ვალდებულება ვრცელდება ამ დასაქმებულთან შრომითი ურთიერთობის შეწყვეტის შემდეგ პერიოდზეც.
5. პერსონალური მონაცემების დამუშავების შესახებ დადგენილი რეგულაციის დარღვევა გახდება უნივერსიტეტის დასაქმებულის მიმართ დისციპლინური წარმოების დაწყების საფუძველი.

მუხლი 12. მონაცემთა სუბიექტის უფლებები და ვალდებულებები

1. მონაცემთა სუბიექტს უფლება აქვს დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს იმის დადასტურება, მუშავდება თუ არა მის შესახებ მონაცემები, დასაბუთებულია თუ არა მონაცემთა დამუშავება და მოთხოვნის შესაბამისად უსასყიდლოდ მიიღოს შემდეგი ინფორმაცია:
ა) მის შესახებ იმ მონაცემის თაობაზე, რომელიც მუშავდება, აგრეთვე ამ მონაცემის დამუშავების საფუძვლისა და მიზნის შესახებ;
ბ) მონაცემთა შეგროვების/მოპოვების წყაროს შესახებ;
გ) მონაცემთა შენახვის ვადის (დროის) შესახებ, ხოლო თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, ვადის განსაზღვრის კრიტერიუმების თაობაზე;
დ) მონაცემთა სუბიექტის უფლებების შესახებ;
ე) მონაცემთა გადაცემის სამართლებრივი საფუძვლისა და მიზნების, აგრეთვე მონაცემთა დაცვის სათანადო გარანტიების შესახებ, თუ მონაცემები გადაეცემა სხვა სახელმწიფოს ან საერთაშორისო ორგანიზაციას;
ვ) მონაცემთა მიმღების ვინაობის ან მონაცემთა მიმღებების კატეგორიების შესახებ, მათ შორის, ინფორმაცია მონაცემთა გადაცემის საფუძვლისა და მიზნის თაობაზე, თუ მონაცემები მესამე პირს გადაეცემა;
2.უნივერსიტეტი შეტყობინების მიღებიდან არაუგვიანეს 10 (ათი) კალენდარული დღისა უზრუნველყოფს მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდებას. ეს ვადა განსაკუთრებულ შემთხვევებში და სათანადო დასაბუთებით შეიძლება გაგრძელდეს არაუმეტეს 10 სამუშაო დღით, რის შესახებაც მონაცემთა სუბიექტს დაუყოვნებლივ უნდა ეცნობოს.
3. თუ საქართველოს კანონმდებლობით სხვა რამ არ არის გათვალისწინებული, მონაცემთა სუბიექტს უფლება აქვს, თავად აირჩიოს ამ მუხლის პირველი პუნქტით გათვალისწინებული ინფორმაციის მიწოდების ფორმა. ამასთანავე, თუ მონაცემთა სუბიექტი სხვა ფორმით არ მოითხოვს ინფორმაციის მიწოდებას, მას ინფორმაცია მიეწოდება იმავე ფორმით, რომლითაც მოხდა ინფორმაციის მოთხოვნა.
4. მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს მის შესახებ მცდარი, არაზუსტი ან/და არასრული მონაცემების გასწორება, განახლება ან/და შევსება. მოთხოვნის წარდგენიდან არაუგვიანეს 10 სამუშაო დღისა (თუ საქართველოს კანონმდებლობით სხვა ვადა არ არის დადგენილი) მონაცემები უნდა გასწორდეს, განახლდეს ან/და შეივსოს ან მონაცემთა სუბიექტს ეცნობოს მოთხოვნაზე უარის თქმის საფუძველი და განემარტოს უარის გასაჩივრების წესი.
5. მონაცემთა სუბიექტს უფლება აქვს მოითხოვოს მის შესახებ მონაცემთა დამუშავების შეწყვეტა, წაშლა ან განადგურება. ამ შემთხვევაში, მოთხოვნიდან არაუგვიანეს 10 სამუშაო დღისა (თუ საქართველოს კანონმდებლობით სხვა რამ არ არის დადგენილი) უნდა შეწყდეს მონაცემთა დამუშავება ან/და მონაცემები უნდა წაიშალოს ან

განადგურდეს. მონაცემთა სუბიექტს უნდა ეცნობოს მოთხოვნაზე უარის თქმის საფუძველი და განემარტოს უარის გასაჩივრების წესი.
6. მონაცემთა სუბიექტს უფლება აქვს მოითხოვოს **მონაცემთა დაბლოკვა,** თუ არსებობს ერთ-ერთი შემდეგი გარემოება:
ა) მონაცემთა სუბიექტი სადაოდ ხდის მონაცემების ნამდვილობას ან სიზუსტეს;
ბ) მონაცემთა დამუშავება უკანონოა, თუმცა მონაცემთა სუბიექტი ეწინააღმდეგება მათ წაშლას და ითხოვს მონაცემთა დაბლოკვას;
გ) მონაცემები საჭირო აღარ არის მათი დამუშავების მიზნის მისაღწევად, თუმცა მონაცემთა სუბიექტს ისინი სჭირდება საჩივრის/სარჩელის წარსადგენად;
დ) მონაცემთა სუბიექტი მოითხოვს მონაცემთა დამუშავების შეწყვეტას, წაშლას ან განადგურებას და მიმდინარეობს ამ მოთხოვნის განხილვა;
ე) არსებობს მონაცემების მტკიცებულებად გამოყენების მიზნით შენახვის აუცილებლობა.
7. მონაცემთა სუბიექტს უფლება აქვს მიიღოს ინფორმაცია მონაცემთა დაბლოკვის თაობაზე მიღებული გადაწყვეტილების ან მონაცემთა დაბლოკვაზე უარის თქმის საფუძვლის შესახებ გადაწყვეტილების მიღებისთანავე, დაუყოვნებლივ, მაგრამ არაუგვიანეს მოთხოვნიდან 3 სამუშაო დღისა.

მუხლი 13. თანხმობის გამოხმობის უფლება

1. მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, ყოველგვარი განმარტების ან დასაბუთების გარეშე გამოიხმოს მის მიერ გაცემული თანხმობა. ამ შემთხვევაში, მონაცემთა სუბიექტის მოთხოვნის შესაბამისად, მონაცემთა დამუშავება უნდა შეწყდეს ან/და დამუშავებული მონაცემები წაიშალოს ან განადგურდეს მოთხოვნიდან არაუგვიანეს 10 სამუშაო დღისა, თუ მონაცემთა დამუშავების სხვა საფუძველი არ არსებობს.
2. მონაცემთა სუბიექტს უფლება აქვს, თანხმობა გამოიხმოს იმავე ფორმით, რომლითაც თანხმობა განაცხადა.
3. მონაცემთა სუბიექტს თანხმობის გამოხმობამდე უფლება აქვს, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს და მიიღოს ინფორმაცია თანხმობის გამოხმობის შესაძლო შედეგების შესახებ.

მუხლი 14. სტუდენტის/პროფესიული სტუდენტის/მსმენელის უფლება-მოვალეობები

1. უნივერსიტეტი სტუდენტს/პროფესიულ სტუდენტს/მსმენელს მომსახურების ხელშეკრულების გაფორმებამდე აწვდის ინფორმაციას თუ რა სახის პერსონალურ მონაცემების დამუშავება ხორციელდება მის მიმართ ბსუ-ში.
2. სტუდენტები/პროფესიული სტუდენტები/მსმენელები ვალდებულნი არიან:
ა) დაიცვან წინამდებარე წესი, როდესაც ისინი წარმოადგენენ უნივერსიტეტს და უნივერსიტეტის სახელით მონაწილეობენ სხვადასხვა აქტივობაში;
ბ) შეატყობინონ უნივერსიტეტს მათი პერსონალური მონაცემების ცვლილების შესახებ.
3. წინამდებარე წესის დარღვევა არის დისციპლინური წარმოების დაწყების საფუძველი.

მუხლი 15. გაასაჩივრების უფლება

მონაცემთა სუბიექტს უფლება აქვს, წინამდებარე წესით გათვალისწინებული უფლებებისა და დადგენილი ვალდებულებების დარღვევის შემთხვევაში მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს ან სასამართლოს.

მუხლი 16. ელექტრონული ფოსტისა და ტელეფონის ნომრის გამოყენება

ეფექტური და სწრაფი კომუნიკაციის მიზნით, უნივერსიტეტი ამუშავებს ბსუ-ს პერსონალის, სტუდენტების/პროფესიული სტუდენტების/მსმენელებისა და კურსდამთავრებულების ელ-ფოსტებსა და ტელეფონის ნომრებს.

მუხლი 17. დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის ვალდებულებები

1. მონაცემთა სუბიექტის მოთხოვნის შესაბამისად, ბსუ ვალდებულია დადგენილი წესით უზრუნველყოს მონაცემთა სუბიექტის უფლებების განხორციელება, მათ შორის, მიიღოს ყველა ზომა ამავე კანონის მოთხოვნებთან შესაბამისობის და, საჭიროების შემთხვევაში, მათი დემონსტრირების მიზნით.
2. მონაცემების უშუალოდ მონაცემთა სუბიექტისგან შეგროვებისას ბსუ ვალდებულია მონაცემთა შეგროვებამდე ან შეგროვების დაწყებისთანავე მონაცემთა სუბიექტს მიაწოდოს სულ მცირე შემდეგი ინფორმაცია:

ა) დამუშავებისთვის პასუხისმგებელი პირის, მისი წარმომადგენლის ან/და დამუშავებაზე უფლებამოსილი პირის (ასეთის არსებობის შემთხვევაში) ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია;

ბ) მონაცემთა დამუშავების მიზნებისა და სამართლებრივი საფუძვლის შესახებ;

გ) მონაცემთა მიწოდების სავალდებულოობის შესახებ, ხოლო თუ მონაცემთა მიწოდება სავალდებულოა – მონაცემთა მიწოდებაზე უარის თქმის სამართლებრივი შედეგების თაობაზე, აგრეთვე ინფორმაცია იმის შესახებ, რომ მონაცემთა შეგროვება/მოპოვება გათვალისწინებულია საქართველოს კანონმდებლობით ან აუცილებელი პირობაა ხელშეკრულების დასადებად (ასეთი ინფორმაციის არსებობის შემთხვევაში);

დ) დამუშავებისთვის პასუხისმგებელი პირის ან მესამე პირის მნიშვნელოვანი ლეგიტიმური ინტერესების შესახებ;

ე) პერსონალურ მონაცემთა დაცვის ოფიცრის ვინაობა და საკონტაქტო ინფორმაცია;

ვ) მონაცემთა მიმღების ვინაობა ან მონაცემთა მიმღებების კატეგორიები (ასეთის არსებობის შემთხვევაში);

ზ) მონაცემთა დაგეგმილი გადაცემისა და მონაცემთა დაცვის სათანადო გარანტიების არსებობის შესახებ, მათ შორის, მონაცემთა გადაცემაზე ნებართვის თაობაზე (ასეთის არსებობის შემთხვევაში), თუ დამუშავებისთვის პასუხისმგებელი პირი გეგმავს

თ) მონაცემთა შენახვის ვადის შესახებ, ხოლო თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, ვადის განსაზღვრის კრიტერიუმების თაობაზე;

ი) მონაცემთა სუბიექტის უფლებების შესახებ.

3. თუ მონაცემების შეგროვება უშუალოდ მონაცემთა სუბიექტისგან არ ხდება, ბსუ ვალდებულია მონაცემთა სუბიექტს მიაწოდოს ამ მუხლის მე-2 პუნქტით ქვეპუნქტებით გათვალისწინებული ინფორმაცია, აგრეთვე აცნობოს, მის შესახებ რომელი მონაცემები მუშავდება და ამ მონაცემთა მოპოვების წყარო, მათ შორის, მოპოვებულ იქნა თუ არა მონაცემები საჯაროდ ხელმისაწვდომი წყაროდან.

მუხლი 18. მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა

1. ბსუ წერილობით ან ელექტრონულად უზრუნველყოფს მონაცემთა დამუშავებასთან დაკავშირებული შემდეგი **ინფორმაციის აღრიცხვას:**
ა) დამუშავებისთვის პასუხისმგებელი პირის, სპეციალური წარმომადგენლის, პერსონალურ მონაცემთა დაცვის ოფიცრის, თანადამუშავებისთვის პასუხისმგებელი პირების, დამუშავებაზე უფლებამოსილი პირის ვინაობა/სახელწოდება და საკონტაქტო ინფორმაცია;
ბ) მონაცემთა დამუშავების მიზნების შესახებ;
გ) მონაცემთა სუბიექტებისა და მონაცემთა კატეგორიების შესახებ;
დ) მონაცემთა მიმღების (მათ შორის, სხვა სახელმწიფოში არსებული მონაცემთა მიმღების ან საერთაშორისო ორგანიზაციის) კატეგორიების შესახებ;
ე) სხვა სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის მონაცემთა გადაცემის, აგრეთვე მონაცემთა დაცვის სათანადო გარანტიების თაობაზე, მათ შორის, პერსონალურ მონაცემთა დაცვის სამსახურის ნებართვის შესახებ (ასეთის არსებობის შემთხვევაში);
ვ) მონაცემთა შენახვის ვადების შესახებ, ხოლო თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, მათი შენახვის ვადის განსაზღვრის კრიტერიუმების თაობაზე;
ზ) მონაცემთა უსაფრთხოებისთვის მიღებული ორგანიზაციულ-ტექნიკური ზომების ზოგადი აღწერა;
თ) ინციდენტების შესახებ ინფორმაცია (ასეთის არსებობის შემთხვევაში).

მუხლი 19. ინციდენტი

1. ბსუ ვალდებულია აღრიცხოს ინციდენტი, დამდგარი შედეგი, მიღებული ზომები, ინციდენტის აღმოჩენიდან არაუგვიანეს 72 საათისა, მის შესახებ წერილობით ან ელექტრონულად შეატყობინოს/წარუდგინოს პერსონალურ მონაცემთა დაცვის სამსახურს, გარდა იმ შემთხვევისა, როდესაც ნაკლებსავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.
2. დამუშავებაზე უფლებამოსილი პირი ვალდებულია აღრიცხოს მონაცემთა დამუშავებასთან დაკავშირებული, მათ შორის ინციდენტის შესახებ ინფორმაცია. აღნიშნული ვალდებულება ყველა აღმოჩენილ ინციდენტზე ვლინდება, მიუხედავად იმისა, ექვემდებარება თუ არა ინციდენტი პერსონალურ მონაცემთა დაცვის სამსახურისთვის ან/და მონაცემთა სუბიექტისთვის შეტყობინებას.

მუხლი 20. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შექმნის სიმძიმის შეფასებისას გასათვალისწინებელი გარემოებები

1. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებების შელახვის სიმძიმის შეფასებისას გათვალისწინებული უნდა იქნეს შემდეგი გარემოებები:
1.1. <u>ინციდენტის სახე</u> :
ა) კონფიდენციალურობის დარღვევა – პერსონალური მონაცემების უნებართვო გამჟღავნება ან წვდომა;

ბ) მთლიანობის დარღვევა – პერსონალური მონაცემების უნებართვო შეცვლა, აგრეთვე, არამართლზომიერი ან შემთხვევითი დაზიანება, დაკარგვა;
გ) ხელმისაწვდომობის დარღვევა – პერსონალურ მონაცემებზე წვდომის დაკარგვა, შეზღუდვა, მონაცემების განადგურება ან წაშლა.

1.2. იმ პერსონალური მონაცემების კატეგორია, რომლებზეც გავლენას ახდენს ინციდენტი;
1.3. ეხება თუ არა ინციდენტი არასრულწლოვნის, შეზღუდული შესაძლებლობის მქონე პირისა ან სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე მონაცემთა სუბიექტის პერსონალურ მონაცემებს;
1.4. ინციდენტის შედეგად მონაცემთა სუბიექტის მესამე პირთა მიერ იდენტიფიცირების შესაძლებლობის ხარისხი;
1.5. დამუშავებისთვის პასუხისმგებელი პირის საქმიანობის განსაკუთრებული ხასიათი, რასაც შესაძლოა ახლდეს მომეტებული საფრთხე;
1.6. ინციდენტის მასშტაბი, მონაცემთა სუბიექტის ან/და პერსონალური მონაცემის რაოდენობის ან/და მოცულობის თვალსაზრისით;
1.7. სხვა ისეთი გარემოება, რამაც შესაძლოა არსებითი გავლენა მოახდინოს ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შექმნის ალბათობის სიმძიმეზე.

მუხლი 21. ადამიანის უფლებებისა და თავისუფლებების შელახვის სიმძიმის განსაზღვრის კრიტერიუმები

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

ა) მონაცემთა სუბიექტის დისკრიმინაცია, მისი ვინაობის მითვისება ან გაყალბება, ფინანსური ზიანი, მონაცემთა სუბიექტის რეპუტაციის შელახვა, პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალურობის დარღვევა, ან სხვა სახის მნიშვნელოვანი სოციალური ან/და ეკონომიკური ზიანი;
ბ) მონაცემთა სუბიექტის უფლებების რეალიზებისათვის ხელის შეშლა, მათ შორის, მონაცემთა სუბიექტის უფლებების კანონით დადგენილ ვადებში რეალიზების შეზღუდვა;
გ) პერსონალური მონაცემების იმგვარი წაშლა/განადგურება, რომელიც არ ექვემდებარება აღდგენას, ან მისი აღდგენა არაპროპორციულად დიდ დროსა და ძალისხმევას საჭიროებს, გარდა იმ შემთხვევისა, როდესაც პერსონალური მონაცემების (გარდა განსაკუთრებული კატეგორიის პერსონალური მონაცემისა) დამუშავების მიზნიდან გამომდინარე, მათი წაშლის/განადგურების შედეგად, მონაცემთა სუბიექტს 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) არასრულწლოვნების, შეზღუდული შესაძლებლობების მქონე პირებისა და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე მონაცემთა სუბიექტ(ებ)ის პერსონალური მონაცემების უკანონო დამუშავება.

მუხლი 22. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობის განსაზღვრა

1. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა შესაძლოა იყოს დაბალი, საშუალო ან მაღალი.

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

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

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

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

მუხლი 23. პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულება

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

2. თუკი ინციდენტის სრულყოფილად შეფასება მისი აღმოჩენიდან 72 საათში ვერ ხერხდება, მაგრამ არსებობს გონივრული ეჭვის საფუძველი, რომ საშუალო ან მაღალი ალბათობით ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, ბსუ არ უნდა დაელოდოს ინციდენტის შეფასების დასრულებას და ინციდენტის შესახებ უნდა შეატყობინოს სამსახურს.

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

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

5. ინციდენტის სამსახურისთვის შეტყობინების მიზნით, დამუშავებისთვის პასუხისმგებელი პირის მიერ მიწოდებული ინფორმაციის საფუძველზე, პერსონალურ მონაცემთა დაცვის ოფიცერი ავსებს ინციდენტის შეტყობინების ფორმას და წარუდგენს სამსახურს.

6. ინციდენტის შესახებ შეტყობინება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) ინციდენტის გარემოებების, სახისა და დროის შესახებ;

ბ) ინციდენტის შედეგად უნებართვოდ გამჟღავნებული, დაზიანებული, წაშლილი, განადგურებული, მოპოვებული, დაკარგული, შეცვლილი მონაცემების სავარაუდო

კატეგორიებისა და რაოდენობის, აგრეთვე იმ მონაცემთა სუბიექტების სავარაუდო კატეგორიებისა და რაოდენობის შესახებ, რომლებსაც ინციდენტის შედეგად შეექმნათ საფრთხე;

გ) ინციდენტით გამოწვეული სავარაუდო ზიანის, მისი შემცირების ან აღმოფხვრის მიზნით დამუშავებისთვის პასუხისმგებელი პირის მიერ განხორციელებული ან დაგეგმილი ღონისძიებების შესახებ;

დ) იმის შესახებ, გეგმავს თუ არა დამუშავებისთვის პასუხისმგებელი პირი, ინციდენტის შესახებ შეატყობინოს მონაცემთა სუბიექტს და რა ვადაში.

ე) პერსონალურ მონაცემთა დაცვის ოფიცრის ან სხვა საკონტაქტო პირის მონაცემებს.

7. ინციდენტის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულების, ისევე, როგორც ინციდენტის შესახებ მონაცემთა სუბიექტისთვის შეტყობინების ვალდებულების არაჯეროვანი შესრულება წარმოადგენს ადმინისტრაციულ სამართალდარღვევას.

მუხლი 24. მონაცემთა სუბიექტის ინფორმირების ვალდებულების გამომრიცხავი გარემოებები

1. ინციდენტის შესახებ მონაცემთა სუბიექტების ინფორმირების ვალდებულება არ წარმოიშობა, თუ ეს საფრთხეს შეუქმნის:

ა) საზოგადოებრივი უსაფრთხოების ინტერესებს;

ბ) დანაშაულის თავიდან აცილებას, ოპერატიულ-სამძებრო საქმიანობას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას;

გ) მართლმსაჯულების განხორციელებას;

2. მონაცემთა სუბიექტების ინფორმირების ვალდებულება ასევე არ წარმოიშობა იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელმა პირმა მიიღო შესაბამისი უსაფრთხოების ზომები, რის შედეგადაც თავიდან იქნა აცილებული ადამიანის ძირითადი უფლებებისა და თავისუფლებების დარღვევის მნიშვნელოვანი საფრთხე.

მუხლი 25. ინციდენტის შესახებ მონაცემთა სუბიექტის ინფორმირების ვალდებულება

1. თუ ინციდენტი მაღალი ალბათობით გამოიწვევს მნიშვნელოვან ზიანს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, ბსუ ვალდებულია ინციდენტის აღმოჩენიდან პირველი შესაძლებლობისთანავე, გაუმართლებელი დაყოვნების გარეშე აცნობოს მონაცემთა სუბიექტს ინციდენტის შესახებ და მარტივ და მისთვის გასაგებ ენაზე მიაწოდოს შემდეგი ინფორმაცია:

ა) ინციდენტისა და მასთან დაკავშირებული გარემოებების ზოგადი აღწერა;

ბ) ინციდენტით გამოწვეული სავარაუდო/დამდგარი ზიანის, მის შესამცირებლად ან აღმოსაფხვრელად განხორციელებული ან დაგეგმილი ღონისძიებების შესახებ;

გ) პერსონალურ მონაცემთა დაცვის ოფიცრის ან სხვა პირის საკონტაქტო მონაცემები.

მუხლი 26 . პერსონალურ მონაცემთა დაცვის ოფიცერი

1. ბსუ-ში პერსონალურ მონაცემთა დამუშავების პროცესების პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის უზრუნველყოფას შრომითი

ხელშეკრულების საფუძველზე ახორციელებს პერსონალურ მონაცემთა დაცვის ოფიცერი.

2. **პერსონალურ მონაცემთა დაცვის ოფიცერი:**

ა) აკონტროლებს უნივერსიტეტში პერსონალურ მონაცემთა დამუშავების პროცესს;

ბ) საჭიროების შემთხვევაში მონაწილეობს მონაცემთა დამუშავების რისკების შეფასების პროცესში;

გ) საჭიროების შემთხვევაში თანამშრომლობს პერსონალურ მონაცემთა დაცვის სამსახურთან;

დ) უზრუნველყოფს თანამშრომელთა ინფორმირებასა და გადამზადებას პერსონალურ მონაცემთა დაცვის საკითხებზე;

ე) განიხილავს მონაცემთა სუბიექტის განცხადებებს, საჩივრებს და/ან მომართვებს;

ვ) პერსონალურ მონაცემთა დაცვის საკითხზე კონსულტაციას უწევს ბსუ-ს პერსონალს/სტუდენტებს/პროფესიულ სტუდენტებს/მსმენელებსა და კურსდამთავრებულებს;

ზ) აწარმოებს და პერსონალურ მონაცემთა დაცვის სამსახურს წარუდგენს ფაილური სისტემების კატალოგებს;

თ) გამოავლენს, შეისწავლის და სათანადო რეაგირებას ახდენს პერსონალურ მონაცემთა დარღვევის ფაქტებზე;

ი) ახდენს მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე, მათ შორის, მარეგულირებელი სამართლებრივი ნორმების მიღების ან შეცვლის შესახებ, დამუშავებისთვის პასუხისმგებელი პირის, დამუშავებაზე უფლებამოსილი პირისა და მათი თანამშრომლების ინფორმირებას, მათთვის კონსულტაციისა და მეთოდური დახმარების გაწევას;

კ) მონაწილეობს მონაცემთა დამუშავებასთან დაკავშირებული შიდა რეგულაციებისა და მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის შემუშავებაში, აგრეთვე ახდენს დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ საქართველოს კანონმდებლობისა და შიდა ორგანიზაციული დოკუმენტების შესრულების მონიტორინგს;

ლ) ახდენს მონაცემთა დამუშავებასთან დაკავშირებით შემოსული განცხადებებისა და საჩივრების ანალიზსა და შესაბამისი რეკომენდაციების გაცემას;

მ) ახდენს პერსონალურ მონაცემთა დაცვის სამსახურისგან კონსულტაციების მიღებას, დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის წარმომადგენლობას პერსონალურ მონაცემთა დაცვის სამსახურთან ურთიერთობაში, მისი მოთხოვნით ინფორმაციისა და დოკუმენტების წარდგენას და მისი დავალებებისა და რეკომენდაციების შესრულების კოორდინაციასა და მონიტორინგს;

ნ) მონაცემთა სუბიექტის მიმართვის შემთხვევაში ახდენს მისთვის მონაცემთა დამუშავების პროცესებისა და მისი უფლებების შესახებ ინფორმაციის მიწოდებას;

ო) დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავების სტანდარტების ამაღლების მიზნით ასრულებს სხვა ფუნქციებს.

2. პერსონალურ მონაცემთა დაცვის ოფიცერს უნდა ჰქონდეს სათანადო ცოდნა მონაცემთა დაცვის სფეროში.

3. პერსონალურ მონაცემთა დაცვის ოფიცერი კონკრეტული ვითარების გათვალისწინებით ანგარიშვალდებულია ბსუ-ს რექტორისა და ადმინისტრაციის ხელმძღვანელის (კანცლერის) წინაშე.

5. დამუშავებისთვის პასუხისმგებელმა პირმა და დამუშავებაზე უფლებამოსილმა პირმა უნდა უზრუნველყონ პერსონალურ მონაცემთა დაცვის ოფიცრის სათანადო ჩართულობა მონაცემთა დამუშავებასთან დაკავშირებით მნიშვნელოვანი გადაწყვეტილების მიღების პროცესში, უზრუნველყონ იგი შესაბამისი რესურსებით, აგრეთვე უზრუნველყონ მისი დამოუკიდებლობა საქმიანობის განხორციელებისას.
6. ბსუ ვალდებულია პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნიდან ან მისი შეცვლიდან მისი ვინაობა და საკონტაქტო ინფორმაცია **არაუგვიანეს 10 სამუშაო დღის ვადაში** აცნობოს პერსონალურ მონაცემთა დაცვის სამსახურს, რომელიც აქვეყნებს აღნიშნულ ინფორმაციას.
7. ბსუ ვალდებულია პერსონალურ მონაცემთა დაცვის ოფიცრის ვინაობა და საკონტაქტო ინფორმაცია პროაქტიულად გამოაქვეყნოს უნივერსიტეტის ოფიციალურ ვებგვერდზე.
8. პერსონალურ მონაცემთა დაცვის ოფიცრის დროებითი არყოფნის ან მისი უფლებამოსილების შეწყვეტის შემთხვევაში ბსუ ვალდებულია გაუმართლებელი დაყოვნების გარეშე პერსონალურ მონაცემთა დაცვის ოფიცრის უფლებამოსილებით აღჭურვოს სხვა პირი.

მუხლი 27. დასკვნითი დებულებები

1. პერსონალურ მონაცემთა დაცვის მიზნით ბსუ-ს შესაბამისმა სტრუქტურულმა ერთეულებმა უზრუნველყონ მომსახურებისა და შრომით ხელშეკრულებებში, ასევე ბსუ-ს სამართლებრივ აქტებში ცვლილებების განხორციელება (ასეთის საჭიროებისას).
2. პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკითხები, რომელიც არ არის გათვალისწინებული წინამდებარე წესით, რეგულირდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით.
3. წინამდებარე წესი შეთანხმებულია (ვიზირებულია) ბსუ-ს ადმინისტრაციის ხელმძღვანელთან და დამტკიცებულია ბსუ-ს რექტორის ბრძანებით. წესში ცვლილებებისა და დამატებების შეტანა შესაძლებელია მისი მიღებისათვის დადგენილი წესით.