



შპს საზოგადოებრივი კოლეჯი ამაგის
დირექტორის ბრძანება



№ 00009885



06/08/2024

შპს საზოგადოებრივი კოლეჯი ამაგის პერსონალურ მონაცემთა დაცვის პოლიტიკის დამტკიცების შესახებ

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის და შპს საზოგადოებრივი კოლეჯი ამაგის წესდების შესაბამისად,

ვ ბ რ ძ ა ნ ე ბ :

1. დამტკიცდეს შპს საზოგადოებრივი კოლეჯი ამაგის პერსონალურ მონაცემთა დაცვის პოლიტიკა დანართის შესაბამისად.
2. ეს ბრძანება ძალაშია ხელმოწერისთანავე.

კერძო კოლეჯების ასოციაცია
შპს საზოგადოებრივი კოლეჯი ამაგი
დირექტორი
სუხიშვილი სოფიო

პერსონალურ მონაცემთა დაცვის პოლიტიკა

მუხლი 1. ზოგადი დებულებები

1. პერსონალურ მონაცემთა დაცვის პოლიტიკა (ტექსტში შემდგომში პოლიტიკა) განსაზღვრავს შპს საზოგადოებრივი კოლეჯი ამაგის (ტექსტში შემდგომში კოლეჯი) პერსონალური მონაცემის დამუშავებისას ადამიანის (მომხმარებლების) უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის დაცვის საშუალებებს, ასევე პერსონალური მონაცემების უსაფრთხოებას და კონფიდენციალობას.

2. ამ პოლიტიკაში მოცემულ ტერმინებს აქვს ისეთივე განმარტება როგორც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში.

3. ამ პოლიტიკის მოქმედება ვრცელდება კოლეჯში მონაცემთა ავტომატური საშუალებებით დამუშავებასა და ნახევრად ავტომატური საშუალებებით დამუშავებაზე, იმ მონაცემთა არაავტომატური საშუალებებით დამუშავებაზე, რომლებიც ფაილური სისტემის ნაწილია ან ფაილურ სისტემაში შესატანად მუშავდება.

მუხლი 2. მონაცემთა დამუშავების პრინციპები

1. პერსონალური მონაცემების დამუშავების დროს აუცილებელია მონაცემთა დამუშავების პრინციპების დაცვა.

2. მონაცემთა დამუშავებისას დაცული უნდა იქნეს შემდეგი პრინციპები:

ა) მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად, მონაცემთა სუბიექტისთვის გამჭვირვალედ და მისი ღირსების შეუღახავად. მონაცემთა დამუშავების გამჭვირვალობის ვალდებულება არ ვრცელდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილ გამონაკლის შემთხვევებზე;

ბ) მონაცემები უნდა შეგროვდეს/მოპოვებული უნდა იქნეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზნებისთვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებელი მიზნით;

გ) მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად. მონაცემები იმ მიზნის თანაზომიერი უნდა იყოს, რომლის მისაღწევაც ისინი მუშავდება;

დ) მონაცემები უნდა იყოს ნამდვილი, ზუსტი და, საჭიროების შემთხვევაში, განახლებული. მონაცემთა დამუშავების მიზნების გათვალისწინებით, არაზუსტი მონაცემები უნდა გასწორდეს, წაიშალოს ან განადგურდეს გაუმართლებელი დაყოვნების გარეშე;

ე) მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა წაიშალოს, განადგურდეს ან შენახული უნდა იქნეს დეპერსონალიზებული ფორმით, გარდა იმ შემთხვევისა, თუ მონაცემთა დამუშავება განსაზღვრულია კანონით ან/და კანონის შესაბამისად გამოცემული კანონქვემდებარე ნორმატიული აქტით და მონაცემთა შენახვა აუცილებელი და პროპორციული ზომია დემოკრატიულ საზოგადოებაში აღმატებული ინტერესების დასაცავად;

ვ) მონაცემების უსაფრთხოების დაცვის მიზნით მონაცემთა დამუშავებისას მიღებული უნდა იქნეს ისეთი ტექნიკური და ორგანიზაციული ზომები, რომლებიც სათანადოდ უზრუნველყოფს მონაცემთა დაცვას, მათ შორის, უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვისგან, განადგურებისგან ან/და დაზიანებისგან.

მუხლი 3. მონაცემთა დამუშავების საფუძვლები

მონაცემთა დამუშავება დასაშვებია, თუ არსებობს ერთ-ერთი შემდეგი საფუძველი:

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 დასადავად;

გ) მონაცემთა დამუშავება გათვალისწინებულია კანონით;

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 საქართველოს კანონმდებლობით განსაზღვრული საჯარო ინტერესის სფეროსთვის მიკუთვნებული ამოცანების შესასრულებლად, მათ შორის, დანაშაულის თავიდან აცილების, დანაშაულის გამოძიების, სისხლისსამართლებრივი დევნის, მართლმსაჯულების განხორციელების, პატიმრობისა და თავისუფლების აღკვეთის აღსრულების, არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის, ოპერატიულ-სამძებრო საქმიანობის, საზოგადოებრივი უსაფრთხოების, მართლწესრიგის დაცვის, მათ შორის, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების უზრუნველყოფის, მიზნებისთვის;

ი) 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;

კ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად (მისთვის მომსახურების გასაწევად).

მუხლი 4. განსაკუთრებული კატეგორიის მონაცემთა დამუშავება

1. განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია მხოლოდ იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელი პირის მიერ უზრუნველყოფილია მონაცემთა სუბიექტის უფლებებისა და ინტერესების დაცვის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული გარანტიები და არსებობს ერთ-ერთი შემდეგი საფუძველი:

ა) მონაცემთა სუბიექტმა განაცხადა წერილობითი თანხმობა ერთი ან რამდენიმე კონკრეტული მიზნით განსაკუთრებული კატეგორიის მონაცემთა დამუშავებაზე;

ბ) განსაკუთრებული კატეგორიის მონაცემთა დამუშავება პირდაპირ და სპეციალურად რეგულირდება კანონით და მათი დამუშავება აუცილებელი და პროპორციული ზომის დემოკრატიულ საზოგადოებაში;

გ) განსაკუთრებული კატეგორიის მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დასაცავად და მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად უნარი არ აქვს, განსაკუთრებული კატეგორიის მონაცემთა დამუშავებაზე განაცხადოს თანხმობა;

დ) განსაკუთრებული კატეგორიის მონაცემთა დამუშავება აუცილებელია ჯანმრთელობის დაცვის სფეროში პრევენციული, პროფილაქტიკური, დიაგნოსტიკური, სამკურნალო, სარეაბილიტაციო და პალიატიური მზრუნველობის, მომსახურების, სამედიცინო მოწყობილობების და პროდუქტების ხარისხისა და უსაფრთხოების, საზოგადოებრივი ჯანმრთელობის და ჯანმრთელობის დაცვის სისტემის მართვის მიზნებით საქართველოს კანონმდებლობის ან ჯანმრთელობის დაცვის სპეციალისტთან დადებული ხელშეკრულების (თუ ამ მონაცემებს ამუშავებს პირი, რომელსაც პროფესიული საიდუმლოების დაცვის ვალდებულება ეკისრება) შესაბამისად;

ე) განსაკუთრებული კატეგორიის მონაცემთა დამუშავება აუცილებელია სოციალური უზრუნველყოფისა და სოციალური დაცვის სფეროში, მათ შორის, სოციალური უზრუნველყოფის სისტემისა და მომსახურების მართვისთვის საქართველოს კანონმდებლობით დამუშავებისთვის პასუხისმგებელი პირისთვის დაკისრებული მოვალეობის შესასრულებლად ან მონაცემთა სუბიექტის კონკრეტული უფლებების განსახორციელებლად;

ვ) განსაკუთრებული კატეგორიის მონაცემთა დამუშავება საჭიროა დანაშაულის თავიდან აცილების (მათ შორის, სათანადო ანალიტიკური კვლევის), დანაშაულის გამოძიების, სისხლისსამართლებრივი დევნის, მართლმსაჯულების განხორციელების, პატიმრობისა და თავისუფლების აღკვეთის აღსრულების, არასაკატიმრო სასჯელთა აღსრულებისა და პრობაციის, დროებითი მოთავსების იზოლატორში პირის განთავსების უზრუნველყოფის, უკანონო მიგრაციის წინააღმდეგ ბრძოლის, საერთაშორისო დაცვის განხორციელების, ადმინისტრაციულ სამართალდარღვევებზე რეაგირების, სამოქალაქო და სახანძრო უსაფრთხოების უზრუნველყოფის, ოპერატიულ-სამძებრო საქმიანობის, საზოგადოებრივი უსაფრთხოების ან/და მართლწესრიგის დაცვის (მათ შორის, შესაბამისი სამართალდამცავი ორგანოს ან სასამართლოს მიერ კრიმინოლოგიური კვლევის ჩატარების) მიზნებისთვის და ამ მონაცემთა დამუშავება გათვალისწინებულია შესაბამისი კანონით ან კანონითა და მის საფუძველზე გამოცემული კანონქვემდებარე ნორმატიული აქტით;

ზ) განსაკუთრებული კატეგორიის მონაცემები მუშავდება ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების უზრუნველსაყოფად;

თ) განსაკუთრებული კატეგორიის მონაცემების დამუშავება აუცილებელია შრომითი ვალდებულებებისა და ურთიერთობის ხასიათიდან გამომდინარე, მათ შორის, დასაქმების შესახებ გადაწყვეტილების მისაღებად ან დასაქმებულის შრომითი უნარების შესაფასებლად;

ი) მონაცემთა სუბიექტმა გამოყენების აშკარა აკრძალვის დათქმის გარეშე საჯარო გახადა თავისი მონაცემები;

კ) განსაკუთრებული კატეგორიის მონაცემთა დამუშავება აუცილებელია მნიშვნელოვანი საჯარო ინტერესის დასაცავად;

ლ) განსაკუთრებული კატეგორიის მონაცემები მუშავდება პოლიტიკური, პროფესიული გაერთიანების, რელიგიური ან არარელიგიური ფილოსოფიური რწმენის ორგანიზაციის მიერ იმავე საქმიანობის მიზნებისთვის. ამ შემთხვევაში აღნიშნულ მონაცემთა დამუშავება შეიძლება დაკავშირებული იყოს მხოლოდ ამ გაერთიანების/ორგანიზაციის მოქმედ ან ყოფილ წევრებთან ან პირებთან, რომლებსაც მუდმივი კავშირი აქვთ ამ გაერთიანებასთან/ორგანიზაციასთან მისი მიზნებიდან გამომდინარე, იმ პირობით, რომ მონაცემთა სუბიექტის თანხმობის გარეშე აღნიშნული მონაცემების მესამე პირისთვის გაცემა არ მოხდება;

მ) განსაკუთრებული კატეგორიის მონაცემთა დამუშავება აუცილებელია კანონის შესაბამისად საჯარო ინტერესებისთვის არქივირების, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის, თუ კანონი ითვალისწინებს სათანადო და კონკრეტული ღონისძიებების განხორციელებას მონაცემთა სუბიექტის უფლებებისა და ინტერესების დასაცავად. განსაკუთრებული კატეგორიის მონაცემთა დამუშავების ეს საფუძველი არ გამოიყენება, თუკი

სპეციალური კანონით პირდაპირ გათვალისწინებულია ამ მონაცემთა დამუშავების შეზღუდვა დამატებითი და განსხვავებული პირობებით;

ნ) განსაკუთრებული კატეგორიის მონაცემები მუშავდება მიგრაციის მონაცემთა ერთიანი ანალიტიკური სისტემის ფუნქციონირების მიზნით;

ო) განსაკუთრებული კატეგორიის მონაცემები მუშავდება შეზღუდული შესაძლებლობის მქონე პირთა და სპეციალური საგანმანათლებლო საჭიროების მქონე პირთა განათლების უფლების განხორციელების მიზნით;

პ) განსაკუთრებული კატეგორიის მონაცემები მუშავდება „ქალთა მიმართ ძალადობის ან/და ოჯახში ძალადობის აღკვეთის, ძალადობის მსხვერპლთა დაცვისა და დახმარების შესახებ“ საქართველოს კანონის მე-11 მუხლის მე-2 პუნქტით გათვალისწინებული საკითხის განხილვის მიზნით;

ჟ) განსაკუთრებული კატეგორიის მონაცემები მუშავდება მსჯავრდებულთა და ყოფილ პატიმართა რესოციალიზაციისა და რეაბილიტაციის, აგრეთვე არასრულწლოვანთა რეფერირების პროცესის კოორდინაციის მიზნით;

რ) განსაკუთრებული კატეგორიის მონაცემები მუშავდება ღია სასამართლო სხდომის შედეგად მიღებული სასამართლო აქტის „საერთო სასამართლოების შესახებ“ საქართველოს ორგანული კანონის შესაბამისად საჯარო ინფორმაციის სახით გაცემის ან გამოქვეყნების მიზნით;

ს) განსაკუთრებული კატეგორიის მონაცემები მუშავდება „საჯარო შესყიდვების შესახებ“ საქართველოს კანონით პირდაპირ გათვალისწინებულ შემთხვევებში;

ტ) განსაკუთრებული კატეგორიის მონაცემები მუშავდება უწყებათაშორისი კოორდინაციის ინსტიტუციური მექანიზმის ფუნქციონირებისთვის – ბავშვის სიცოცხლისთვის, ჯანმრთელობისთვის ან უსაფრთხოებისთვის ან/და ბავშვის საუკეთესო ინტერესებისთვის ან მისი უფლებისთვის მიყენებული ზიანის ან მოსალოდნელი რისკების შემცველი შემთხვევის გამოვლენის ან/და მართვის მიზნებისთვის და ამ მიზნების ფარგლებში, საქართველოს მთავრობის მიერ განსაზღვრულ კომპეტენტურ ორგანოებს (უწყებებს) შორის კოორდინაციის უზრუნველსაყოფად, ბავშვის უფლებათა კოდექსის 83-ე მუხლის მე-3 ნაწილითა და 84-ე მუხლის 2¹ ნაწილით გათვალისწინებულ შემთხვევებში.

2. ამ მუხლის პირველი პუნქტის „რ“ ქვეპუნქტით გათვალისწინებული მონაცემების დამუშავების შემთხვევაში მათი საჯარო ინფორმაციის სახით გაცემა და გამოქვეყნება დასაშვებია „საერთო სასამართლოების შესახებ“ საქართველოს ორგანული კანონის შესაბამისად.

მუხლი 5. მონაცემების შეგროვება

მონაცემები განსხვავდება საქმიანობის ტიპისა და მიზნების მიხედვით. ის შეიძლება იყოს შემდეგი:

ა) იდენტიფიკაციის მონაცემები:

ა.ა) სახელი, გვარი;

ა.ბ) მისამართი (ფიზიკური და ელექტრონული);

ა.გ) ტელეფონის ნომერი;

ა.დ) პირადი ნომერი ან სხვა საიდენტიფიკაციო ნომერი.

ბ) კონტაქტის მონაცემები:

ბ.ა) ელექტრონული ფოსტის მისამართი;

ბ.ბ) ტელეფონის ნომერი;

ბ.გ) ფიზიკური მისამართი.

გ) დემოგრაფიული მონაცემები:

გ.ა) დაბადების თარიღი;

გ.ბ) სქესი;

- გ.გ) ენა;
- გ.დ) ეროვნება.
- დ) ფინანსური მონაცემები:
 - დ.ა) საბანკო ანგარიშის ინფორმაცია;
 - დ.ბ) საკრედიტო ან სადებეტო ბარათის ინფორმაცია;
 - დ.გ) საგადასახადო ინფორმაცია.
- ე) დასაქმების მონაცემები:
 - ე.ა) სამუშაო გამოცდილება;
 - ე.ბ) განათლება;
 - ე.გ) სამუშაო სტატუსი;
 - ე.დ) შემოსავლები.
- ვ) მომხმარებლის აქტივობის მონაცემები:
 - ვ.ა) შესყიდვების ისტორია;
 - ვ.ბ) ვებ-გვერდზე ან აპლიკაციაში აქტივობა;
 - ვ.გ) გადახდის მეთოდები და ტრანზაქციები.
- ზ) ტექნიკური მონაცემები:
 - ზ.ა) IP მისამართი;
 - ზ.ბ) ბრაუზერის ტიპი და ვერსია;
 - ზ.გ) ოპერაციული სისტემა;
 - ზ.დ) ლოგ ფაილები და კუკები.
- თ) მდებარეობის მონაცემები:
 - თ.ა) GPS მონაცემები;
 - თ.ბ) ადგილმდებარეობის ისტორია.
- ი) პრეფერენციები და ჩვევები:
 - ი.ა) მარკეტინგული პრეფერენციები;
 - ი.ბ) პროდუქტებისა და მომსახურების პრეფერენციები;
 - ი.გ) სოციალური ქსელის აქტივობა.
- კ) სამედიცინო და ჯანმრთელობის მონაცემები:
 - კ.ა) ჯანმრთელობის ისტორია;
 - კ.ბ) დაზღვევის ინფორმაცია;
 - კ.გ) სამედიცინო კვლევების შედეგები.

მუხლი 6. მონაცემების შეგროვების მეთოდები

მონაცემების შეგროვების მეთოდებია:

- ა) ონლაინ ფორმები:
 - ა.ა) ვებ-გვერდზე ან აპლიკაციაში მომხმარებლის მიერ შევსებული სარეგისტრაციო ფორმები, უკუკავშირის ფორმები, შეკვეთის ფორმები და სხვა;
 - ა.ბ) პირადი და კონტაქტური ინფორმაციის შეგროვება (მაგ.: სახელი, ელ. ფოსტა, ტელეფონის ნომერი).
- ბ) კუკები (Cookies) და სხვა ტრეკინგ ტექნოლოგიები:
 - ბ.ა) ვებ-გვერდების ან აპლიკაციების გამოყენების დროს ავტომატურად შეგროვება ქცევის მონაცემების (მაგ.: ვიზიტების ისტორია, ნავიგაცია, კლიკები);
 - ბ.ბ) ტექნიკური და ანალიტიკური მონაცემების შეგროვება.
- გ) ელექტრონული ფოსტის კამპანიები:
 - გ.ა) მომხმარებლის პასუხები ელ. ფოსტაზე;
 - გ.ბ) ელ. ფოსტის მისამართების შეგროვება.

დ) მომხმარებლის მიერ გენერირებული კონტენტი:

დ.ა) სოციალურ ქსელებში, ფორუმებზე ან მიმოხილვებში მომხმარებლის მიერ განთავსებული ინფორმაცია;

დ.ბ) კომენტარები, პოსტები, მიმოხილვები.

ე) გამოძიებები და გამოკითხვები:

ე.ა) მომხმარებლის მიერ შევსებული გამოკითხვები, კითხვარები და კვლევები;

ე.ბ) მოსაზრებები, პრეფერენციები, შეფასებები.

ვ) მობილური აპლიკაციები:

ვ.ა) აპლიკაციის გამოყენების მონაცემები, მომხმარებლის მიერ გაწეული აქტივობები, აპლიკაციაში შესული ინფორმაცია;

ვ.ბ) GPS და ადგილმდებარეობის მონაცემები.

ზ) ტრანზაქციები და ფინანსური ოპერაციები:

ზ.ა) გაყიდვების სისტემები, ფინანსური პლატფორმები;

ზ.ბ) გადახდის მეთოდები, ტრანზაქციების ისტორია.

თ) მომხმარებელთა მომსახურება:

თ.ა) მომხმარებლის ზარები, ჩატში ან ელ. ფოსტით გადამუშავებული მოთხოვნები;

თ.ბ) მომსახურების სერვისებთან დაკავშირებული ინფორმაციები.

ი) ფიზიკური ღონისძიებები:

ი.ა) კონფერენციები, გამოფენები, სემინარები;

ი.ბ) სარეგისტრაციო ფორმები, შეხვედრების ჩანაწერები.

კ) პარტნიორები და მესამე მხარეები:

კ.ა) პარტნიორული პროგრამები და მესამე მხარეების მეშვეობით მიღებული მონაცემები;

კ.ბ) სხვა კომპანიების და ორგანიზაციების მონაცემთა ბაზები.

მუხლი 7. შეგროვილი მონაცემების გამოყენების მიზნები

კოლეჯი მონაცემებს იყენებს შემდეგი ძირითადი მიზნებისთვის:

ა) მომსახურების მიწოდება და გაუმჯობესება:

ა.ა) მომხმარებლის საჭიროებების ანალიზი: მომხმარებლის პრეფერენციებისა და ქცევის ანალიზი, რათა შესთავაზონ უფრო პერსონალიზებული და შესაბამისი მომსახურებები;

ა.ბ) მომსახურების გაუმჯობესება: მომხმარებლის უკუკავშირის და გამოყენების მონაცემების საფუძველზე მომსახურების გაუმჯობესება.

ბ) მომხმარებელთან ურთიერთობა და მხარდაჭერა:

ბ.ა) მომხმარებლის მომსახურება: მომხმარებლის კითხვებზე პასუხის გაცემა, პრობლემების გადაჭრა და მომსახურების მხარდაჭერა;

ბ.ბ) კომუნიკაცია: მომხმარებელთან კომუნიკაცია ელ. ფოსტით, სატელეფონო ზარებით ან სხვა არხებით.

გ) უსაფრთხოება და თაღლითობის პრევენცია:

გ.ა) უსაფრთხოების ზომები: მონაცემების უსაფრთხოების უზრუნველყოფა და მომხმარებლის ანგარიშების დაცვა;

გ.ბ) თაღლითობის აღმოჩენა: თაღლითობის პრევენციის და აღმოჩენის სისტემების მართვა.

დ) იურიდიული ვალდებულებების შესრულება:

დ.ა) კანონმდებლობის დაცვა: იურიდიული მოთხოვნების და რეგულაციების დაცვა, როგორცაა მონაცემთა დაცვის კანონმდებლობა;

დ.ბ) ანგარიშგება და აუდიტი: კოლეჯის საქმიანობის შესაბამისობა და აუდიტის პროცესების მართვა.

მუხლი 8. მონაცემთა დამუშავება

1. მონაცემების დამუშავება მოიცავს მონაცემების შეგროვებას, შენახვას, გამოყენებას, გაზიარებას და განადგურებას.

2. მონაცემთა დამუშავებისათვის აუცილებელია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული რომელიმე საფუძვლის არსებობა და მონაცემთა დამუშავების პრინციპების დაცვა.

3. კოლეჯმა მონაცემთა დამუშავების თითოეულ შემთხვევაში თავად უნდა უზრუნველყოს მონაცემთა დამუშავების საფუძვლის განსაზღვრა.

4. იმისათვის, რომ პერსონალური მონაცემების დამუშავებას საფუძვლად დაედოს მონაცემთა სუბიექტის თანხმობა, აუცილებელია რომ 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 მიზნით მონაცემთა დამუშავებაზე;

ე) გამოხატოს ისეთი საშუალებით, რომლითაც ნათლად დგინდება მონაცემთა სუბიექტის ნება.

5. მონაცემთა სუბიექტის თანხმობით მონაცემთა დამუშავებამდე, კოლეჯი უნდა დარწმუნდეს, რომ სახეზეა თანხმობის კანონიერებისთვის განსაზღვრული ყველა ზემოაღნიშნული კომპონენტი და ამასთანავე, დაცულია თანხმობის კანონით გათვალისწინებული ფორმა - წერილობითი (მათ შორის, ელექტრონულად) ან ზეპირი.

6. თუ მონაცემთა დამუშავება გათვალისწინებულია კანონით, ასეთ შემთხვევაში პერსონალური მონაცემების დამუშავება ხდება მონაცემთა სუბიექტის თანხმობის გარეშე.

7. თუ მონაცემთა დამუშავება საჭიროა მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად - ამ შემთხვევაში, მონაცემთა დამუშავების მიერ მონაცემების დამუშავება აუცილებელი უნდა იყოს მონაცემთა სუბიექტის სასიცოცხლო ინტერესის დასაცავად და სასიცოცხლო ინტერესის დაცვის აუცილებლობა, უნდა შეფასდეს ყოველ კონკრეტულ შემთხვევაში ინდივიდუალური გარემოებების გათვალისწინებით.

8. თუ მონაცემთა დამუშავება აუცილებელია მონაცემთა დამუშავების, ან მესამე პირის კანონიერი ინტერესების დასაცავად - ამ შემთხვევაში უნდა არსებობდეს დამუშავების, ან მესამე პირის კანონით დაცული ინტერესი და ის უნდა აღემატებოდეს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის ინტერესს.

9. მონაცემთა სუბიექტის თანხმობის გარეშე შესაძლებელია მონაცემების დამუშავება ასევე:

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

ბ) მონაცემთა დამუშავება აუცილებელია კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესის დასაცავად;

გ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად (მისთვის მომსახურების გასაწევად).

10. განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია მონაცემთა სუბიექტის წერილობითი თანხმობით, ან თუკი ჯანმრთელობის მდგომარეობასთან დაკავშირებული მონაცემების დამუშავება აუცილებელია შრომითი ვალდებულებების და ურთიერთობის ხასიათიდან გამომდინარე, მათ შორის, დასაქმების თაობაზე გადაწყვეტილების მისაღებად და ა.შ.

11. 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, გარდა

კანონით პირდაპირ გათვალისწინებული შემთხვევებისა, მათ შორის, როდესაც მონაცემთა დამუშავებისთვის აუცილებელია 16 წლიდან 18 წლამდე არასრულწლოვანისა და მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობა.

12. არასრულწლოვანის შესახებ განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია მხოლოდ მისი მშობლის ან სხვა კანონიერი წარმომადგენლის წერილობითი თანხმობის საფუძველზე, გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა.

13. თუ პერსონალი ავადმყოფობის გამო ვერ გამოცხადდება კოლეჯში და საჭიროა საპატიო მიზეზის დადგენა და წარმოადგენს საავადმყოფო ფურცლს (ე.წ. „ბიულეტენი“), ასეთ შემთხვევაში მნიშვნელოვანია, კოლეჯმა წინასწარ განუმარტოს მონაცემთა სუბიექტს მისი ჯანმრთელობის მდგომარეობასთან დაკავშირებული ინფორმაციის დამუშავების მიზანი და მან გამოხატოს ნება მისი განსაკუთრებული კატეგორიის მონაცემის დამუშავების თაობაზე.

მუხლი 9. ბიომეტრიული მონაცემების დამუშავება

1. ბიომეტრიული მონაცემი არის პირის ფიზიკური, ფსიქიკური, ან ქცევის მახასიათებელი, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისთვის და იძლევა ამ პირის იდენტიფიცირების შესაძლებლობას. მაგალითად, ბიომეტრიული მონაცემებია თითის ანაბეჭდი, ტერფის ანაბეჭდი, თვალის ფერადი გარსი, სახის მახასიათებლები.

2. დაუშვებელია კოლეჯში პერსონალის შესვლა-გასვლის კონტროლი თითის ანაბეჭდის საშუალებით.

მუხლი 10. მონაცემთა დამუშავება კოლეჯის შენობაში შესვლისა და შენობიდან გასვლის აღრიცხვის მიზნით

1. კოლეჯის შენობაში შესვლისა და შენობიდან გასვლის აღრიცხვის მიზნით კოლეჯის შეუძლია შეაგროვოს შემდეგი მონაცემები: სახელი, გვარი, საიდენტიფიკაციო დოკუმენტის ნომერი და სახე, მისამართი, შესვლისა და გასვლის თარიღები და დრო, ასევე შენობაში შესვლისა და შენობიდან გასვლის მიზეზები.

2. ამ მუხლის პირველი პუნქტით გათვალისწინებულ მონაცემთა შენახვის ვადა არ უნდა აღემატებოდეს მათი ჩაწერის დღიდან სამ წელს, თუ კანონით სხვა რამ არ არის დადგენილი. სამწლიანი ვადის გასვლის შემდეგ ისინი უნდა წაიშალოს ან განადგურდეს.

მუხლი 11. მონაცემთა დამუშავებაზე პასუხისმგებელი პირები

მონაცემთა დამუშავებაზე პასუხისმგებელი პირები არიან კოლეჯის თანამშრომლები საკუთარი კომპეტენციის ფარგლებში დამუშავებული მონაცემების თაობაზე.

მუხლი 12. წვდომა პერსონალურ მონაცემებზე

1. მონაცემთა სუბიექტს უფლება აქვს, მიიღოს ინფორმაცია მისი პერსონალური მონაცემების დამუშავებასთან დაკავშირებით, კერძოდ, ინფორმაცია მონაცემთა დამუშავების მიზანზე და სამართლებრივ საფუძველზე, მონაცემთა შეგროვების გზებზე, ასევე, იმაზე, თუ ვის გადაეცა მისი მონაცემები, რა მიზნითა და რა საფუძველით.

2. ამ მუხლის 1-ლი პუნქტით გათვალისწინებული ინფორმაციის მიწოდების ფორმას ირჩევს თავად მონაცემთა სუბიექტი.

3. მონაცემთა სუბიექტს მოთხოვნილი ინფორმაცია უნდა მიეწოდოს დაუყოვნებლივ, ან მოთხოვნიდან არაუგვიანეს 10 (ათი) დღისა, თუ აუცილებელია მოთხოვნილი ინფორმაციის სხვა დაწესებულებაში მოძიება, დაწესებულებასთან კონსულტაცია, მოსაძიებელია დიდი მოცულობით ინფორმაცია და სხვა.

4. სავალდებულოა მესამე პირებისთვის პერსონალური მონაცემების გამჟღავნებისას მოხდეს ინფორმაციის გაცემის ფაქტების აღრიცხვა, რაც უნდა მოიცავდეს შემდგომ ინფორმაციას:

- ა) რა მონაცემი იქნა გაცემული,
- ბ) ვისთვის, როდის და რა სამართლებრივი საფუძვლით.

მუხლი 13. მონაცემების შენახვა და დაცვა

1. მონაცემების უსაფრთხო და ეფექტური შენახვა არის კრიტიკულად მნიშვნელოვანი კოლეჯისთვის.

2. მონაცემების უსაფრთხო და ეფექტური შენახვის ძირითადი მეთოდები და ზომებია: ფიზიკური სერვერები, ლოკალური სერვერები, დაცული მონაცემთა ცენტრები, ღრუბლოვანი სერვისები, ღრუბლოვანი პლატფორმები, რეზერვული ასლები, მონაცემთა ბაზები, ინედქსაციის და ოპტიმიზაციის ტექნიკა, შიფრაცია, დასვენებულ მდგომარეობაში მყოფი მონაცემების შიფრაცია, ავტორიზაცია და ავთენტიფიკაცია, წვდომის კონტროლი, უსაფრთხოების პროტოკოლები და პროცედურები, ნაკადების მონიტორინგი, რეგულარული აუდიტები და ტესტირება, შემთხვევების ტესტირება, მონაცემთა დაცვა რეზერვების მეშვეობით, დაცული რეზერვული საცავები, ინფორმაციის უსაფრთხოების პოლიტიკა, საერთო პოლიტიკის შემუშავება და თანამშრომლების სწავლება.

მუხლი 14. მონაცემთა უსაფრთხოება

1. მონაცემთა დამმუშავებელი ვალდებულია მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისაგან, შეცვლისაგან, გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან.

2. მონაცემთა დამმუშავებელი ვალდებულია უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა. არაელექტრონული ფორმით არსებულ მონაცემთა დამუშავებისას მონაცემთა დამმუშავებელი ვალდებულია უზრუნველყოს მონაცემთა გამჟღავნებასთან ან/და ცვლილებასთან დაკავშირებული ყველა მოქმედების აღრიცხვა.

3. მონაცემთა უსაფრთხოებისათვის მიღებული ზომები მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური უნდა იყოს.

4. მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ნებისმიერი თანამშრომელი, რომელიც მონაწილეობს მონაცემთა დამუშავებაში, ვალდებულია არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს. ამასთანავე, მას ეკისრება ვალდებულება, დაიცვას მონაცემთა საიდუმლოება, მათ შორის, მისი სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგ.

5. მონაცემთა უსაფრთხოების დაცვის ზომები განისაზღვრება საქართველოს კანონმდებლობით.

მუხლი 15. მონაცემების შენახვის ვადები

1. სხვადასხვა ტიპის მონაცემებს შეიძლება ჰქონდეთ სხვადასხვა შენახვის ვადები, რომლებიც განისაზღვრება მონაცემების ტიპის, მათი გამოყენების მიზნისა და კანონმდებლობის მოთხოვნების მიხედვით.

2. კოლეჯში მოქმედებს მონაცემების შენახვის შემდეგი ვადები:

ა) პირადი მონაცემები ინახება მანამდე, სანამ მომხმარებელი თანხმდება კომუნიკაციაზე ან თავისი მონაცემების გამოყენებაზე;

ბ) ფინანსური მონაცემები ინახება არაუმეტეს 7 წელი ბუღალტრული და იურიდიული მოთხოვნების შესაბამისად;

გ) მომსახურების მონაცემები ინახება არაუმეტეს 5 წელი;

დ) იურიდიული დოკუმენტები ინახება კონტრაქტის ვადის ამოწურვის შემდეგ 6 წელი იურიდიული დაცვის უზრუნველყოფის მიზნით, ხოლო სასამართლო დოკუმენტები ინახება 10 წელი ან მეტი, იურიდიული მოთხოვნების შესაბამისად;

ე) სხვა მასალები საჭიროებისამებრ, მაგრამ არაუმეტეს 10 წლისა.

მუხლი 16. მონაცემების წაშლის პროცესი

1. მონაცემების წაშლის პროცესი მოიცავს ნაბიჯებს და ტექნიკას, რომლებიც საჭიროა იმის უზრუნველსაყოფად, რომ მონაცემები სრულად და უსაფრთხოდ წაიშალოს. კოლეჯმა უნდა განახორციელონ ისეთი პროცედურები, რომელიც უზრუნველყოფს, რომ წაშლილი მონაცემები აღარ იყოს აღდგენილი და ხელმისაწვდომი არასასურველი პირებისთვის.

2. მონაცემების წაშლის პროცესი მოიცავს მონაცემების იდენტიფიკაციას და კატეგორიზაციას. მონაცემთა ინვენტარიზაცია მოიცავს მონაცემების ტიპების, შენახვის ლოკაციების და ვადების იდენტიფიცირებას, ხოლო პრიორიტეტიზაცია არის იდენტიფიცირება, რომელიც მონაცემები უნდა წაიშალოს პირველ რიგში, მათი სენსიტიურობისა და იურიდიული ვალდებულებების გათვალისწინებით.

3. მონაცემების წაშლის პროცედურა მოიცავს დეტალურ ნაბიჯებს და პასუხისმგებლობებს, პასუხისმგებელი პირების განსაზღვრას, უსაფრთხო წაშლის ტექნიკების მობილიზებას.

მუხლი 17. ელექტრონული მონაცემების წაშლა

ელექტრონული მონაცემების წაშლა მოიცავს:

ა) საოპერაციო სისტემის ფუნქციებს - ფაილების წაშლა ოპერაციული სისტემის ფუნქციების გამოყენებით (მაგ., Windows-ის recycle bin, Linux-ის rm ბრძანება);

ბ) მონაცემთა ბაზების წაშლას - მონაცემების წაშლა მონაცემთა ბაზიდან SQL ბრძანებების გამოყენებით (მაგ., DELETE, DROP);

გ) სპეციალიზებული პროგრამების გამოყენება - სპეციალური პროგრამების გამოყენება მონაცემთა უსაფრთხო წაშლისთვის (მაგ., DBAN, Eraser).

მუხლი 18. ფიზიკური მონაცემების წაშლა

ფიზიკური მონაცემების წაშლა მოიცავს:

ა) დოკუმენტების დაფშვნას - ფიზიკური დოკუმენტების დაფშვნა სპეციალური მოწყობილობების გამოყენებით;

ბ) დახრევა ან დაწვას - ფიზიკური დოკუმენტების დახრა ან დაწვა მათი განადგურებისთვის;

გ) მყარი დისკების განადგურებას - მყარი დისკების განადგურება სპეციალური მოწყობილობების ან პროცედურების გამოყენებით.

მუხლი 19. წაშლის დოკუმენტირება

წაშლის დოკუმენტირება მოიცავს მონაცემების წაშლის პროცესის დოკუმენტაციას, რომელიც მოიცავს წაშლის თარიღს, მეთოდებს და პასუხისმგებელ პირებს.

მუხლი 20. მონაცემების გაზიარება

1. მონაცემების გაზიარება მოიცავს კონკრეტული პირობების და ნებართვების გათვალისწინებას, რათა უზრუნველყოფს მონაცემების უსაფრთხოება და კონფიდენციალობა. მონაცემები შეიძლება გაზიარებული იყოს შიდა თანამშრომლებთან, თუმცა მხოლოდ იმ თანამშრომლებთან, ვისაც სჭირდება ეს ინფორმაცია სამუშაო მოვალეობების შესრულებისთვის და ვისაც აქვს შესაბამისი უფლებები და პარტნიორებთან, თუმცა ეს საჭიროა უნდა იყოს თანამშრომლობისა და საერთო პროექტების მიზნებისათვის. მონაცემები შეიძლება გაზიარებული იყოს ასევე მომხმარებლებთან მხოლოდ იმ შემთხვევაში, თუ ისინი თანხმდებიან და ამისთვის არსებობს ნათელი მიზანი და სამართალდამცავ ორგანოებთან, თუმცა ეს საჭიროა უნდა იყოს სამართლებრივი მოთხოვნების ან გამოძიების ფარგლებში.

მუხლი 21. მონაცემთა სუბიექტის უფლებები

1. მონაცემთა სუბიექტის უფლებები მოიცავს უფლებებს, რომლებიც იცავენ პირადი მონაცემების უსაფრთხოებას და კონფიდენციალობას.

2. მონაცემთა სუბიექტის ძირითადი უფლებებია: ინფორმაციის მიღების უფლება, მონაცემებზე წვდომის უფლება, მონაცემების კორექტირებისა და განახლების უფლება, მონაცემების წაშლის უფლება, მონაცემების გადატანის უფლება, პროტესტის უფლება.

მუხლი 22. ვიდეოთვალთვალი

1. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად ვიდეოთვალთვალის განხორციელება დასაშვებია დანაშაულის თავიდან აცილების, მისი გამოვლენის, საზოგადოებრივი უსაფრთხოების, პირის უსაფრთხოებისა და საკუთრების დაცვის, არასრულწლოვანის დაცვის (მათ შორის, მავნე ზეგავლენისგან დაცვის), საიდუმლო ინფორმაციის დაცვის, გამოცდის/ტესტირების მიზნებისთვის, აგრეთვე სხვა საჯარო ან/და სხვა ლეგიტიმური ინტერესის სფეროსთვის მიკუთვნებული ამოცანების შესასრულებლად, თუ ვიდეომონიტორინგის განხორციელება მონაცემთა დამუშავების მიზნის ადეკვატური და პროპორციული საშუალებაა.

2. დაუშვებელია ვიდეოთვალთვალის განხორციელება კოლეჯში დასაქმებული პირების ქცევის მონიტორინგის ან/და შინაგანაწესის დაცვის კონტროლის მიზნით.

3. ვიდეოთვალთვალი უნდა განხორციელდეს მხოლოდ შესასვლელის (შენობის შესასვლელი, დერეფანი, კიბის უჯრედი) და გარე პერიმეტრის გასაკონტროლებლად.

4. სამუშაო ადგილზე ვიდეოთვალთვალი დასაშვებია მხოლოდ გამონაკლის შემთხვევებში, თუ ეს აუცილებელია პირის უსაფრთხოების, საკუთრების დაცვისა და საიდუმლო ინფორმაციის დაცვის მიზნით და თუ ამ მიზნების მიღწევა სხვა საშუალებით შეუძლებელია.

5. იმ სივრცეში, სადაც ხორციელდება ვიდეოთვალთვალი, თვალსაჩინო ადგილას უნდა იყოს განთავსებული გამაფრთხილებელი ნიშანი ვიდეოთვალთვალის მიმდინარეობის შესახებ.

6. სამუშაო ადგილზე ვიდეოთვალთვალის სისტემის გამოყენებისას კოლეჯში დასაქმებული ყველა პირი წერილობითი ფორმით უნდა იყოს ინფორმირებული ვიდეოთვალთვალის განხორციელებისა და მისი უფლებების შესახებ.

7. ვიდეოსათვალთვალო სისტემის მეშვეობით მომზადებული ჩანაწერების მესამე პირებისთვის გადაცემა დაუშვებელია გარდა გამონაკლისისა. თუ კოლეჯის მიმართავს სამართალდამცავი ორგანო და მოითხოვს ვიდეოჩანაწერს, კოლეჯმა ჩანაწერის გადაცემის საკითხი უნდა შეაფასოს ინდივიდუალურად, საქართველოს მოქმედი კანონმდებლობის მოთხოვნების გათვალისწინებით (შესაბამისი ოპერატიულ-სამძებრო ღონისძიებებისა და დანაშაულის გამოძიების მიზნით ვიდეოჩანაწერის გადაცემისთვის, შესაძლოა, აუცილებელი იყოს მოსამართლის განჩინება, ან გადაუდებელი აუცილებლობის შემთხვევაში პროკურორის მოტივირებული დადგენილება).

8. მონაცემთა უკანონო, ან შემთხვევითი გამჟღავნების, ან ნებისმიერი სხვა ფორმით გამოყენების თავიდან აცილების მიზნით, ასევე, მონაცემებზე არავტორიზებული წვდომის პრევენციისთვის კოლეჯის დირექტორის ბრძანებით განისაზღვრება ვიდეოსათვალთვალო სისტემის წვდომაზე უფლებამოსილების მქონე პირ(ებ)ი და მისი სამსახურიდან წასვლის ან/და მივლინების ან/და შვებულების პერიოდში შემცველი პირ(ებ)ი.

9. მონაცემთა დამუშავებელმა უნდა შექმნას ვიდეოჩანაწერების შენახვისათვის განკუთვნილი ფაილური სისტემა (მონაცემთა ბაზა, სადაც პერსონალური მონაცემები დალაგებული და ხელმისაწვდომია კონკრეტული კრიტერიუმის მიხედვით) და შეინახოს ჩანაწერები ავტომატური შენახვის დროის გასვლიდან ერთი თვის განმავლობაში. სისტემა ჩანაწერების (სურათები/ხმა) გარდა უნდა შეიცავდეს ინფორმაციას მონაცემთა დამუშავების თარიღის, ადგილისა და დროის შესახებ.

10. მონაცემთა ყველა დამმუშავებელი ვალდებულია თითოეულ ფაილურ სისტემასთან დაკავშირებით აწარმოოს ფაილური სისტემის კატალოგი, რომელიც მოიცავს ფაილური სისტემის სტრუქტურისა და შინაარსის დეტალურ აღწერილობას.