დამტკიცებულია კოლეჯის დირექტორის
2026 წლის 16 ივნისის N 60 „ო“ ბრძანებით

მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი

პრეამბულა

სსიპ კოლეჯი „ერქვანი“ -ს (შემდგომში - ორგანიზაცია) 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. ორგანიზაციის მიერ პერსონალურ მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი (შემდგომ - „დოკუმენტი”) გამოიყენება დაწესებულების მიერ სუბიექტების (ჩამონათვალი) მონაცემთა დამუშავების პროცესში და ვრცელდება დაწესებულების მიერ მონაცემების ნებისმიერი ფორმით დამუშავებაზე.

მონაცემთა დაცვაზე ზემოქმედების შეფასება (DPIA) ჩატარდა მონაცემთა სუბიექტების კონფიდენციალურობისთვის პოტენციური რისკების შესაფასებლად ორგანიზაციის მონაცემთა დამუშავებასთან დაკავშირებით. დოკუმენტი მიზნად ისახავს მონაცემთა დაცვის „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) 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 ისეთი კატეგორიის მონაცემების დიდი რაოდენობით დამუშავებას, როგორიცაა განათლებასთან და ჯანმრთელობასთან დაკავშირებული მონაცემები.

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, ორგანიზაცია 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;
- ორგანიზაციას მიერ სუბიექტების შესახებ მოპოვებული ინფორმაციის დამუშავების აუცილებლობასა და პროპორციულობას;
- პოტენციური რისკების შეფასებას პირთა ძირითადი უფლებებისა და თავისუფლებების დასაცავად;
- ქმედით მექანიზმებს გამოვლენილი რისკების პრევენციისათვის;
- ორგანიზაციის 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

1. ორგანიზაციას წარმოადგენს სსიპ კოლეჯი „ერქვანი“, რომელიც ახორციელებს შესაბამის საგანმანათლებლო მომსახურებას.

2. ორგანიზაციაში მონაცემები მუშავდება როგორც ელექტრონული პლატფორმების, ასევე დოკუმენტური (მატერიალური ფორმით).

3. მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მონაცემები:

სსიპ კოლეჯი „ერქვანი“

საიდენტიფიკაციო კოდი: 222934671

მისამართი: ქ. ამბროლაური ვაჟა - ფშაველას ქ. N10

ტელეფონის ნომერი: (+995) 595 06 86 40

ელექტრონული ფოსტა: koleji.erqvani@gmail.com

პერსონალურ მონაცემთა დამუშავებაზე უფლებამოსილი პირი

1. ორგანიზაციას ჰყავს მონაცემთა დამუშავებაზე უფლებამოსილი პირები, რომლებიც მონაცემებს ამუშავებენ მხოლოდ ორგანიზაციის ლეგიტიმური მიზნების განსახორციელებლად.

2. ორგანიზაციას და უფლებამოსილ პირებს შორის გაფორმებულია შესაბამისი ხელშეკრულებები, რომლებიც, მათ შორის მოიცავს პერსონალურ მონაცემთა დაცვის საკითხების მოწესრიგებას და უფლებამოსილ პირ(ებ)ს ეკისრებათ სამართლებრივი ურთიერთობების ფარგლებში მათ მიერ დამუშავებული მონაცემების კონფიდენციალურობის უზრუნველყოფის ვალდებულება.

3. ორგანიზაცია ახორციელებს უფლებამოსილი პირების მიერ მათი ფუნქცია - მოვალეობების შესრულებისას ტექნიკურ - ორგანიზაციული ზომებისა და მონაცემების დამუშავების მონიტორინგს.

4. მოთხოვნის შემთხვევაში, ორგანიზაცია უზრუნველყოფს მონაცემთა სუბიექტ(ებ)ისთვის უფლებამოსილი პირ(ებ)ის შესახებ ინფორმაციის მიწოდებას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონითა და ამ პოლიტიკით დადგენილი წესით.

მონაცემთა სუბიექტები

ორგანიზაცია 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) რეგისტრირებული პირები ანუ აპლიკანტები (სწავლის მსურველები);

დ) პროფესიული სტუდენტები;

ე) მსმენელები;

ვ) არასრულწლოვანთა/ქმედუუნარო სსსმ პირთა მშობლები/კანონიერი წარმომადგენლები;

ზ) მომწოდებლები;

თ) პროფორიენტაციაზე მოსული პირები;

ი) დამსაქმებლები;

კ) ვიზიტორები;

ლ) აპლიკანტი;

მ) კურსდამთავრებული;

ნ) პარტნიორთა ორგანიზაციის წარმომადგენლები;

ო) ვიდეოთვალთვალის არეალში მოხვედრილი სხვა პირები.

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 დოკუმენტის შენახვის ვადა

ორგანიზაცია 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.

მონაცემთა დამუშავების პროცესი

მონაცემთა დამუშავების პროცესის აღწერა

მონაცემთა მიღების წყაროები:

ორგანიზაციისთვის პერსონალურ მონაცემთა მიღების წყაროებია:

ა) მონაცემთა სუბიექტ(ებ)ის: დასაქმებულის, დასაქმების კანდიდატის, მომსახურების ხელშეკრულების ან სხვა სახის იურიდიული ურთიერთობის საფუძველზე ორგანიზაციასთან სამართლებრივ კავშირში მყოფი პირის მიერ ნებაყოფლობით, ინფორმირებული და მკაფიოდ გამოხატული ნებით მიწოდებული პერსონალური მონაცემები;

ბ) საგანმანათლებლო მომსახურების განხორციელების ფარგლებში დაკავშირებული ინფორმაცია.

გ) ვიდეომონიტორინგის განხორციელების გზით მოპოვებული მონაცემები;

დ) საქართველოს კანონმდებლობით დაკისრებული მოვალეობების ეფექტიანად განსახორციელების მიზნით ორგანიზაციის მიერ პერსონალურ მონაცემების მოპოვება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი წესით.

პერსონალურ მონაცემთა შენახვის წესი, ვადები და მათი განადგურების პროცედურა

1. ორგანიზაციაში მონაცემთა შენახვისათვის დადგენილია ინფორმაციის დამუშავების ვადები, რომელიც განსაზღვრულია ორგანიზაციის პერსონალურ მონაცემთა დაცვის პოლიტიკით:

ა) თანამშრომელთა პირადი საქმეები ინახება 5 წლის ვადით, **შემდეგ გადაეცემა ცენტრალურ არქივს;**

ბ) სტუდენტთა პირადი საქმეები ინახება 5 წლის ვადით, **შემდეგ გადაეცემა ცენტრალურ არქივს;**

გ) გაცემული განათლების დამადასტურებელი დოკუმენტის (დიპლომი, სერტიფიკატი) რეგისტრაციის წიგნი ინახება 5 წლის ვადით;

დ) სტუდენტების პორტფოლიოები, შეფასების უწყისები და სასწავლო მასალების ხარჯვის აქტები ინახება 5 წლის ვადით, **შემდეგ გადაეცემა ცენტრალურ არქივს.**

მატერიალური ფორმით არსებული დოკუმენტაცია (აქტიური პირადი საქმეები) ინახება კანცელარიაში, ხოლო დიპლომები, სერტიფიკატები და რეგისტრაციის ჟურნალები ინახება დირექტორის მოადგილესთან.

მატერიალური ფორმით არსებული დოკუმენტაცია, რომელიც არ არის აქტიურ მოხმარებაში, არქივდება და ინახება სპეციალურად გამოყოფილ ოთახში. ოთახი იკეტება გასაღებით, რომელიც ინახება ბიბლიოთეკართან. დაარქივებულ დოკუმენტებზე წვდომა შესაძლებელია დირექტორის ნებართვით, შესაბამისი წერილობითი საფუძვლის არსებობისას.

შენახვის ვადის გასვლის შემდეგ მატერიალური ფორმით არსებული დოკუმენტები, თუკი ისინი არ გადაეცემა ცენტრალურ არქივს, ნადგურდება, რის შესახებაც დგება შესაბამისი აქტი.

ზემოთ აღნიშნული ვად(ებ)ის გასვლის შემდეგ დოკუმენტები უნდა განადგურდეს იმ ფორმით, რომ შეუძლებელი იყოს მასზე არსებული ინფორმაციის აღდგენა (მაგალითად, აღნიშნული დოკუმენტების ფიზიკური განადგურება) ან მოითხოვდეს შეუსაბამოდ დიდ ძალისხმევას (მაგალითად, დაშრედერება).

2. ვიდეომონიტორინგის მეშვეობით დამუშავებული მონაცემების შენახვის ვადა არის 30 (ოცდაათი) დღე (თუ საქართველოს კანონმდებლობით სხვა ვადა არ არის განსაზღვრული), აღნიშნული ვადის გასვლის შემდეგ ვიდეოჩანაწერები იშლება პროგრამულად, ავტომატური გზით.

4. ვიდეომონიტორინგის მეშვეობით დამუშავებული მონაცემების შენახვის ზემოთ აღნიშნული ვადების ხანგრძლივობა პროპორციული და ადეკვატურია ლეგიტიმური

მიზნების მისაღწევად, პრაქტიკაში მათი ეფექტიანი რეალიზების უზრუნველსაყოფად. ვიდეოჩანაწერების შენახვის ვადები წარმოადგენს გონივრულ პერიოდს, რა დროსაც შესაძლებელია საჭირო გახდეს კონკრეტული ვიდეოჩანაწერის მოძიება და მისი დანიშნულებისამებრ გამოყენება, ორგანიზაციის განსაზღვრული ლეგიტიმური მიზნების მისაღწევად და აღნიშნული მიზნებიდან გამომდინარე კანონიერი ინტერესების სფეროს მიკუთვნებული ამოცანების ეფექტიანად განსახორციელებლად.

5. წინამდებარე მუხლით განსაზღვრული ვადების ხანგრძლივობით ორგანიზაციაში მატერიალური სახით არსებული პერსონალური მონაცემების შემცველი ინფორმაცია ინახება ორგანიზაციის მიერ სპეციალურად გამოყოფილ საკეტით დაცულ ოთახებში, რომელზეც გარეშე, არაუფლებამოსილ პირთა ფიზიკური წვდომა შეზღუდულია. აღნიშნულ ინფორმაციაზე წვდომა გააჩნია მხოლოდ ორგანიზაციის შესაბამის თანამშრომელს.

6. პერსონალური მონაცემების შემცველი ინფორმაციის შენახვის შესაბამისი ვადის გასვლის შემდეგ, აღნიშნული ინფორმაციის შემცველი დოკუმენტები უნდა განადგურდეს დაუყოვნებლივ, ყოველგვარი გაუმართლებელი დაყოვნების გარეშე. განადგურების პასუხისმგებლობა ეკისრება აღნიშნულ ინფორმაციის შენახვასა და დაცვაზე პასუხისმგებელ შესაბამისი სტრუქტურული ერთეულის უფლებამოსილ თანამშრომლებს. პერსონალური მონაცემების შემცველი ინფორმაციის განადგურების თაობაზე უნდა შედგეს აღნიშნული პროცედურის განხორციელების დამადასტურებელი ოქმი, რომელშიც აღინიშნება განადგურებული პერსონალური მონაცემების შემცველი დოკუმენტების კატეგორია/ჩამონათვალი, ასევე განადგურების თარიღი. ზემოთ აღნიშნულ ოქმს ხელს აწერენ შემდეგი პირები: ორგანიზაციის დირექტორი ასევე, აღნიშნული ინფორმაციის შენახვასა და დაცვაზე პასუხისმგებელი შესაბამისი უფლებამოსილების მქონე დასაქმებულები.

პერსონალურ მონაცემებზე წვდომა, მონაცემთა უსაფრთხოება და დასაქმებულთა ვალდებულებები მონაცემთა უსაფრთხოების უზრუნველყოფის ასპექტში

1. ორგანიზაციის დირექტორის ან მის მიერ საამისოდ განსაზღვრული უფლებამოსილი პირის, ბრძანებებით განსაზღვრულია პერსონალურ მონაცემებზე წვდომის მქონე სათანადო უფლებამოსილების მქონე პირები, რომლებიც შესაძლოა იყვნენ ორგანიზაციის დასაქმებულები, მომსახურების ხელშეკრულების ან სხვა სახის იურიდიული ურთიერთობის საფუძველზე ორგანიზაციასთან სამართლებრივ კავშირში მყოფი პირები, რომელთაც წვდომა გააჩნიათ მხოლოდ იმ კონკრეტულ მონაცემ(ებ)ზე და იმ მოცულობით, რომელიც აუცილებელია მათზე შრომითი ხელშეკრულებით, ბრძანებით, ორგანიზაციის შიდაუწყებრივი აქტების საფუძველზე ან/და სხვა სამართლებრივი ურთიერთობიდან გამომდინარე დაკისრებული/განსაზღვრული ფუნქცია-მოვალეობების ეფექტიანად განსახორციელებლად.

1.1. პერსონალურ მონაცემებზე წვდომის მქონე სათანადო უფლებამოსილების მქონე პირები:

ა) ორგანიზაციის დირექტორი, ასევე მის მიერ ბრძანებით განსაზღვრული სხვა უფლებამოსილი პირები, მათ მიერ შესასრულებელი ფუნქცია - მოვალეობების ფარგლებში;

ბ) ორგანიზაციის დირექტორის მოადგილე(ებ)ი;

გ) ორგანიზაციის სამსახურების/მიმართულებების ხელმძღვანელები.

დ) ორგანიზაციის პროფესიული თანამშრომელი.

ე) ორგანიზაციის უსაფრთხოების/დაცვის სამსახურის/მონიტორინგის სამსახურში დასაქმებული პირები.

ვ) ორგანიზაციის ადამიანური რესურსების მართვისა და საქმისწარმოების სამსახური და მასში დასაქმებული პირები.

ზ) ორგანიზაციის ინფორმაციული ტექნოლოგიების სამსახურის სპეციალისტი;

თ) ორგანიზაციის იურისტი;

ი) ორგანიზაციის საფინანსო ეკონომიკური დეპარტამენტის ბუღალტრული აღრიცხვის სამსახური და მათში დასაქმებული პირები;

2. ორგანიზაციის მიერ დამუშავებული პერსონალური მონაცემების დაკარგვის, მათზე უკანონო წვდომის, მათ შორის, უკანონო დამუშავების, განადგურების, წაშლის, შეცვლის, გამჟღავნების, არადანიშნულებისამებრ/არამიზნობრივი გამოყენების პრევენციის მიზნით ორგანიზაციაში მიღებულია მონაცემთა დაცვის სათანადო ორგანიზაციულ-ტექნიკური ზომები.

2.1. ორგანიზაციაში ქაღალდის მატარებელზე არსებულ, მატერიალური სახით მოცემულ, პერსონალურ მონაცემებზე წვდომა აქვთ მხოლოდ ორგანიზაციის იმ შესაბამისი სამსახურ(ებ)ის თანამშრომლებს, რომლებსაც აღნიშნული ინფორმაციის დამუშავება ესაჭიროებათ თავიანთი სამსახურებრივი მოვალეობ(ებ)ის შესასრულებლად, მათზე დაკისრებული ფუნქცია-მოვალეობების განხორციელების ფარგლებში. აღნიშნულიდან გამომდინარე, მატერიალური სახით არსებული პერსონალური მონაცემების შემცველ დოკუმენტებზე შეზღუდულია გარეშე, მესამე პირთა ფიზიკური წვდომა, ისინი განთავსებულია ცალკე, საკეტით დაცულ ოთახებში იმდაგვარად, რომ მათზე წვდომა გააჩნდეს მხოლოდ საამისოდ უფლებამოსილ სამსახურებს და მათ თანამშრომლებს, მხოლოდ იმ მოცულობით რაც აუცილებელია სამსახურებრივი უფლება-მოვალეობების განსახორციელებლად.

2.1. ორგანიზაციაში არსებული ელექტრონული მოწყობილობები (კომპიუტერული საშუალებები, პროგრამები, ქსელები), რომელთა მეშვეობითაც ავტომატური ფორმით მუშავდება მონაცემები, დაცულია ლიცენზირებული ანტივირუსით. პერსონალურ მონაცემებზე წვდომის მქონე უფლებამოსილ პირებს, შესაბამის კომპიუტერულ მოწყობილობაში, პროგრამაში, ქსელში შესასვლელად განსაზღვრული აქვთ

ინდივიდუალური მომხმარებლის სახელები და საერთაშორისო სტანდარტით დადგენილი კომბინაციის შემცველი პაროლები, რომლებიც პერიოდულად ახლდება. აღნიშნულ ელექტრონულ საშუალებებს გააჩნია მონაცემთა მიმართ განხორციელებულ ქმედებათა აღმრიცხველი ელექტრონული ჟურნალი, ესე იგი აღნიშნულ პროგრამებში განთავსებულ მონაცემთა მიმართ განხორციელებული ნებისმიერი ქმედება (მათ შორის პროგრამაში შესვლა, პროგრამიდან გამოსვლა, მონაცემების დამატება, დათვალიერება, გადმოწერა, წაშლა, განადგურება) აღირიცხება პროგრამულად (ე.წ. ლოგირების სისტემა).

3. ორგანიზაციის ნებისმიერი დასაქმებული, რომელიც მონაწილეობს მონაცემთა დამუშავებაში ან რომელსაც სამსახურებრივი უფლება-მოვალეობების ფარგლებში აქვს მონაცემებზე წვდომა, ვალდებულია არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს, დაიცვას მონაცემთა საიდუმლოება და კონფიდენციალურობა, მათ შორის, სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგ. ზემოთ აღნიშნულ პირებს ეკრძალებათ, პირადი ან/და სხვა არალეგიტიმური მიზნით, სამსახურებრივად მათ გამგებლობაში/მფლობელობაში არსებული პერსონალური მონაცემების ნებისმიერი ფორმით დამუშავება, მათ შორის მათი ნახვა, დათვალიერება, მოსმენა, გადახვევა, გადმოწერა, გამჟღავნება, წაშლა ან/და განადგურება. ხსენებულ პირებს ეკისრებათ, მათ ხელთ არსებული გონივრული შესაძლებლობის ფარგლებში, აღნიშნული პერსონალური მონაცემების დაცვის ვალდებულება. პერსონალურ მონაცემებზე უკანონო წვდომის, ინციდენტის ან სხვა პერსონალური მონაცემების ხელყოფისკენ მიმართული ნებისმიერი ქმედების გამოვლენის ან/და დაფიქსირების შემთხვევაში ორგანიზაციის თანამშრომელი ვალდებულია აღნიშნული გარემოების თაობაზე დაუყოვნებლივ, ყოველგვარი გაუმართლებელი დაყოვნების გარეშე, შეატყობინოს ორგანიზაციის დირექტორს ან/და პერსონალურ მონაცემთა დაცვის ოფიცერს.

მესამე პუნქტით გათვალისწინებული ვალდებულებების დარღვევა შესაძლოა გახდეს ორგანიზაციის დასაქმებულისთვის მასთან დადებული შრომითი ხელშეკრულებიდან, ორგანიზაციის შინაგანაწესიდან ან სხვა შიდაუწყებრივი დანაწესიდან გამომდინარე დისციპლინური წარმოების დაწყების, ხოლო სამსახურებრივი ვალდებულების დარღვევის/გადაცდომის დადასტურების შემთხვევაში კი, შესაბამისი დისციპლინური პასუხისმგებლობის დაკისრების საფუძველი.

მონაცემთა გადაცემა/გამჟღავნება:

1. ორგანიზაციის მიერ დამუშავებული მონაცემები სამართლებრივი საფუძვლის არსებობის შემთხვევაში კანონმდებლობით დადგენილი წესითა და მოცულობით შეიძლება გადაეცეს შემდეგ მესამე პირებს:

ა) სამართალდამცავ ორგანოებს;

ბ) სასამართლოს;

გ) სახელმწიფო აუდიტის სამსახურს;

დ) კანონმდებლობით დადგენილ სხვა გათვალისწინებულ ორგანოებს.

2. ამ მუხლის პირველი პუნქტით გათვალისწინებულ შემთხვევებში ინფორმაციის გამჟღავნებისას ორგანიზაცია აღრიცხავს, თუ რომელი მონაცემი იქნა გამჟღავნებული, ვისთვის, როდის და რა სამართლებრივი საფუძვლით. აღნიშნული ინფორმაცია ინახება სუბიექტის შესახებ მონაცემებთან ერთად მათი შენახვის ვადის განმავლობაში.

ვიდეომონიტორინგის საშუალებით პერსონალურ მონაცემთა დამუშავება

1. ორგანიზაციაში მიმდინარეობს ვიდეომონიტორინგი კანონმდებლობით განსაზღვრული სამართლებრივი საფუძვლებიდან გამომდინარე, შემდეგი ლეგიტიმური მიზნების, კერძოდ, დანაშაულის გამოვლენის, პირის უსაფრთხოებისა და საკუთრების დაცვის, არასრულწლოვნის მავნე ზეგავლენისგან დაცვის, კონფიდენციალური ინფორმაციის დაცვის, ასევე ორგანიზაციისთვის მნიშვნელოვანი ლეგიტიმური მიზნების ეფექტიანად მიღწევის უზრუნველსაყოფად.

2. ვიდეომონიტორინგის ხედვის არეალში მოქცეულ სივრცეებში თვალსაჩინო ადგილას განთავსებულია გამაფრთხილებელი ნიშნები ვიდეომონიტორინგის მიმდინარეობის თაობაზე, რომლის საშუალებითაც მონაცემთა სუბიექტები ინფორმირებულნი არიან ვიდეო კამერების მეშვეობით მათი პერსონალური მონაცემების დამუშავებასთან დაკავშირებით.

3. დასაქმებულები, რომელთა სამუშაო ადგილზეც მიმდინარეობს ვიდეომონიტორინგი, კანონმდებლობით განსაზღვრული წესით, წერილობითი ფორმით გაფრთხილებულნი არიან ვიდეომონიტორინგის განხორციელების მიზნების, უფლებებისა და მათი პრაქტიკაში რეალიზების პროცედურების თაობაზე.

4. ორგანიზაციის მიერ ვიდეომონიტორინგი ხორციელდება მუდმივად, კერძოდ, 24/7 რეჟიმში.

5. ვიდეოჩანაწერის შენახვის ვადა არის 30 (ოცდაათი) დღე (თუ საქართველოს კანონმდებლობით სხვა ვადა არ არის განსაზღვრული), აღნიშნული ვადის გასვლის შემდეგ ვიდეოჩანაწერები იშლება პროგრამულად, ავტომატური გზით.

6. ვიდეომონიტორინგის მეშვეობით დამუშავებული ვიდეოჩანაწერები განთავსებულია დამოუკიდებელ პროგრამულ ქსელში, რომელიც მარშუტიზატორის მეშვეობით დაკავშირებულია ვიდეოჩამწერ მოწყობილობებთან. ვიდეოჩამწერ მოწყობილობებზე გარეშე პირ(ებ)ის ფიზიკური წვდომა შეზღუდულია, კერძოდ, ისინი განთავსებულია ცალკე გამოყოფილ, შესაბამისი საკეტით დაცულ ოთახებში, რომლებზეც წვდომა გააჩნიათ ორგანიზაციის ინფორმაციული ტექნოლოგიების სამსახურის თანამშრომლებს.

7. ვიდეომონიტორინგის მეშვეობით დამუშავებულ ვიდეოჩანაწერებზე წვდომა აქვთ მხოლოდ ორგანიზაციის უფლებამოსილ წარმომადგენლებს/თანამშრომლებს, კერძოდ, ორგანიზაციის ინფორმაციული ტექნოლოგიების სამსახურისა და დაცვის სამსახურის თანამშრომელს. თითოეულ ასეთ პირს ვიდეომონიტორინგის სისტემაზე წვდომისთვის/სისტემაში შესასვლელად განსაზღვრული აქვს ინდივიდუალური მომხმარებლის სახელი და პაროლი.

მონაცემთა სუბიექტის უფლებები:

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 მონაცემთა განადგურება (გარდა საქართველოს კანონით განსაზღვრული მკაცრი აღრიცხვის დოკუმენტებში ასახული მონაცემებისა, რომლებზეც ვრცელდება საქართველოს კანონი მკაცრი აღრისცხვის დოკუმენტების შესახებ, სხვა ნორმატიული აქტები და შიდა მარეგულირებელი დოკუმენტები) თანხმობის გამოთხოვით;

კ) მოითხოვოს მონაცემთა დაბლოკვა.

2. აღნიშნული უფლებებით სარგებლობისათვის მონაცემთა სუბიექტი უნდა დაუკავშირდეს დამუშავებაზე უფლებამოსილ პირს ან დამუშავებისათვის პასუხისმგებელ პირს, იმ შემთხვევაში, თუ მონაცემები მასთან ინახება.

3. იმის შესახებ, თუ ვინ ახორციელებს მონაცემების შენახვასა და მონაცემთა სუბიექტის ზემოაღნიშნული უფლებების ფარგლებში განხორციელებულ მომართვაზე რეაგირებას, ორგანიზაციასა და კონკრეტულ კლიენტ ორგანიზაციას შორის ურთიერთობის ფარგლებში, მონაცემთა სუბიექტი ინფორმირებულია პოლიტიკის შესაბამისად.

4. მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში ორგანიზაცია ვალდებულია მოთხოვნის თაობაზე შეტყობინების მიღებიდან არაუგვიანეს 10 (ათი) სამუშაო დღისა უზრუნველყოს მონაცემთა სუბიექტისათვის შესაბამისი ინფორმაციის მიწოდება. ეს ვადა განსაკუთრებულ შემთხვევებში და სათანადო დასაბუთებით შეიძლება გაგრძელდეს არაუმეტეს 10 (ათი) სამუშაო დღით, რის შესახებაც მონაცემთა სუბიექტს დაუყოვნებლივ უნდა ეცნობოს.

5. მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, ყოველგვარი განმარტების ან დასაბუთების გარეშე გამოიხმოს მის მიერ გაცემული თანხმობა. თანხმობის გამოხმობა შესაძლებელია იმავე ფორმით, როგორც მისი გაცემა, გარდა იმ შემთხვევებისა, როდესაც ინფორმაციის შენახვა/არქივირება სავალდებულოა საქართველოს კანონმდებლობით დადგენილი წესის შესაბამისად.

6. მონაცემთა სუბიექტის უფლებები შეიძლება შეიზღუდოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებულ შემთხვევებში და წესით. კერძოდ, მონაცემთა სუბიექტის ზემოთ აღნიშნული უფლებები შეიძლება შეიზღუდოს, თუ ეს პირდაპირ არის გათვალისწინებული საქართველოს კანონმდებლობით (მათ შორის „დაწესებულებების საქმიანობის პროცესში შექმნილი ტიპობრივი მმართველობითი დოკუმენტების ნუსხის (მათი შენახვის ვადების მითითებით)“ დამტკიცების შესახებ საქართველოს იუსტიციის მინისტრის N 72 ბრძანება) ამით არ ირღვევა ადამიანის ძირითადი უფლებები და თავისუფლებები, ეს არის აუცილებელი და პროპორციული ზომა დემოკრატიულ საზოგადოებაში და ამ უფლებების განხორციელებამ შეიძლება საფრთხე შეუქმნას:

ა) სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესებს;

ბ) საზოგადოებრივი უსაფრთხოების ინტერესებს;

გ) დანაშაულის თავიდან აცილებას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას, მართლმსაჯულების განხორციელებას, პატიმრობისა და თავისუფლების აღკვეთის აღსრულებას, არასაპატიმრო სასჯელთა აღსრულებას და პრობაციას, ოპერატიულ-სამძებრო საქმიანობას;

დ) ქვეყნისთვის მნიშვნელოვან ფინანსურ ან ეკონომიკურ (მათ შორის, მონეტარულ, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესებს;

ე) მონაცემთა სუბიექტის მიერ პროფესიული, მათ შორის, რეგულირებადი პროფესიის, ეთიკის ნორმების დარღვევის გამოვლენას და მისთვის პასუხისმგებლობის დაკისრებას;

ვ) ამ მუხლის პირველი პუნქტის „ა“, „ბ“, „გ“, „დ“, „ე“, „ზ“ ან „ი“ ქვეპუნქტით განსაზღვრულ სფეროებში მარეგულირებელი ან/და ზედამხედველობის განმახორციელებელი ორგანოების ფუნქციებისა და უფლებამოსილებების განხორციელებას;

ზ) მონაცემთა სუბიექტის ან/და სხვა პირების უფლებებსა და თავისუფლებებს, მათ შორის, გამოხატვის თავისუფლებას;

თ) სახელმწიფო, კომერციული, პროფესიული და კანონით გათვალისწინებული სხვა სახის საიდუმლოებების დაცვას;

ი) სამართლებრივი მოთხოვნის ან შესაგებლის დასაბუთებას.

7. ამ მუხლის პირველი პუნქტით გათვალისწინებული ზომა შეიძლება გამოყენებულ იქნეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შეზღუდვის მიზნის მისაღწევად.

8. იმ შემთხვევაში, როდესაც მონაცემთა სუბიექტის უფლებების რეალიზებისათვის განსახორციელებელი ქმედებები მონაცემთა დამუშავების პროცესში ჩართული სხვა უწყებების (საქართველოს განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტრო, სსიპ განათლების ხარისხის განვითარების ეროვნული ცენტრი, სსიპ - განათლების მართვის საინფორმაციო სისტემა, სსიპ - შემოსავლების სამსახური, იუსტიციის სამინისტრო, თავდაცვის სამინისტრო, სამართალდამცავი სტრუქტურები, სამთავრობო/ადგილობრივი თვითმმართველობის ორგანოები კანონით განსაზღვრულ შემთხვევებში) უფლებამოსილებებს განეკუთვნება, ორგანიზაცია უფლებამოსილია აღნიშნული წერილობით განუმარტოს მონაცემთა სუბიექტს.

9. მონაცემთა სუბიექტი სარგებლობს „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით გათვალისწინებული სუბიექტის ყველა სხვა უფლებით.

ზეგავლენის დოკუმენტის განახლება და დამატებითი ინფორმაცია:

1. დოკუმენტში ცვლილებების შეტანის ინიცირებას ახდენს პერსონალურ მონაცემთა დაცვის ოფიცერი ან/და ოფიცერთან შეთანხმებით ორგანიზაციის იურისტი ან სხვა შესაბამისი უფლებამოსილი პირი.

2. დოკუმენტს მიიღებს ან/და მასში შესულ ცვლილებებს ამტკიცებს ორგანიზაციის დირექტორი შესაბამისის ადმინისტრაციულ სამართლებრივი აქტით - ბრძანებით.

მონაცემთა დამუშავების მასშტაბთან დაკავშირებული სხვა დამატებითი ინფორმაცია

მონაცემთა კატეგორია

ორგანიზაციაში დამუშავებული პერსონალური მონაცემების კატეგორია

ორგანიზაციამ მასზე დაკისრებული ფუნქცია-მოვალეობების ეფექტიანად განსახორციელებლად შესაძლებელია დაამუშავოს შემდეგი სახის პერსონალური მონაცემები:

დასაქმებულები - სახელი, გვარი, ფოტოსურათი, დაბადების თარიღი, ასაკი, სქესი, მისამართი, პირადი ნომერი, პირადობის დამადასტურებელი დოკუმენტის სერია და ნომერი, პირადობის დამადასტურებელი დოკუმენტის გაცემის ვადა, ავტობიოგრაფია, რეზიუმე (CV), განათლების შესახებ ინფორმაცია, უცხო ენის ცოდნის შესახებ ინფორმაცია, დიპლომის ასლი ან განათლების დამადასტურებელი მოწმობა, კომპიუტერული პროგრამების ცოდნის შესახებ ინფორმაცია, სამუშაო გამოცდილების შესახებ ინფორმაცია, გავლილი ტრენინგებისა და გადამზადებების შესახებ ინფორმაცია, შენობაში შესვლისა და შენობიდან გასვლის დრო, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, საბანკო ანგარიშის ნომერი, საპენსიო სქემაში ჩართვასთან დაკავშირებული ინფორმაცია, საშემოსავლო შეღავათით სარგებლობის საფუძველთან დაკავშირებული ინფორმაცია, დაკავებული პოზიცია (თანამდებობა), ანაზღაურების შესახებ ინფორმაცია, ინფორმაცია ნასამართლობის და უფლების ჩამორთმევის შესახებ, სახელის ანდა გვარის შეცვლის შემთხვევაში შესაბამისი ცვლილების დამდგენი დოკუმენტი, ინფორმაცია ჯანმრთელობის მდგომარეობის შესახებ, ვიდეო ჩანაწერი;

პროფესიული სტუდენტისა და მსმენელები - სახელი, გვარი, პირადი ნომერი, პირადობის დამადასტურებელი დოკუმენტის სერია, ნომერი და გაცემის ვადა, დაბადების მოწმობის სერია, ნომერი და გაცემის ვადა, ფოტოსურათი, მისამართი, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, დაბადების თარიღი, სქესი, სახელის ანდა გვარის შეცვლის შემთხვევაში შესაბამისი ცვლილების დამდგენი დოკუმენტი, სოციალური მახასიათებელი, სხვა დაწესებულებაში მიღებული განათლების შესახებ ინფორმაცია, უცხოეთში მიღებული განათლების შესახებ ინფორმაცია, მოქალაქეობა, სამხედრო ვალდებულების შესახებ ინფორმაცია, აკადემიური მოსწრებისა და გაცდენების შესახებ ინფორმაცია, სტატუსის განმსაზღვრელი ყველა სამართლებრივი აქტის/აქტები (ჩარიცხვის, სტატუსის შეჩერების, სტატუსის შეწყვეტის, სტატუსის აღდგენის, მობილობის, კვალიფიკაციის მინიჭების ბრძანებები), საჭიროების შემთხვევაში, ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია (სსსმ მოსწავლის შემთხვევაში), სსსმ მოსწავლის შემთხვევაში სტატუსის მინიჭების დოკუმენტაცია და ინდივიდუალური სასწავლო გეგმები, ფორმალური და არაფორმალური განათლების აღიარებასთან დაკავშირებული დოკუმენტაცია.

მშობელი/კანონიერი წარმომადგენელი - სახელი, გვარი, პირადი ნომერი, პირადობის დამადასტურებელი დოკუმენტის სერია, ნომერი და გაცემის ვადა, მისამართი, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, დაბადების თარიღი, სქესი, მოქალაქეობა, ვიდეო ჩანაწერი, წარმომადგენლობის მტკიცებულება.

ვიზიტორები - სახელი, გვარი, ვიდეო ჩანაწერი, ტელეფონის ნომერი.

ვაკანტური პოზიციების დასაკავებლად გამოცხადებულ კონკურსში მონაწილე კანდიდატები - სახელი, გვარი, დაბადების თარიღი, ასაკი, სქესი, მისამართი, პირადი ნომერი, პირადობის დამადასტურებელი დოკუმენტის სერია და ნომერი, პირადობის დამადასტურებელი დოკუმენტის გაცემის ვადა, რეზიუმე (CV), განათლების შესახებ ინფორმაცია, უცხო ენის ცოდნის შესახებ ინფორმაცია, დიპლომის ასლი ან განათლების დამადასტურებელი მოწმობა, კომპიუტერული პროგრამების ცოდნის შესახებ ინფორმაცია, სამუშაო გამოცდილების შესახებ ინფორმაცია, გავლილი ტრენინგებისა და გადამზადებების შესახებ ინფორმაცია, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი.

აპლიკანტი - სახელი, გვარი, პირადი ნომერი, პირადობის ნომერი, მისამართი, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, დაბადების თარიღი, სქესი, სოციალური მახასიათებელი, სხვა დაწესებულებაში მიღებული განათლების შესახებ ინფორმაცია, უცხოეთში მიღებული განათლების შესახებ ინფორმაცია, მოქალაქეობა, სამხედრო ვალდებულების შესახებ ინფორმაცია, საჭიროების შემთხვევაში, ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია (სსსმ პირის შემთხვევაში).

კურსდამთავრებულები - სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი, განათლება, სამუშაო ადგილი, ხელფასი, კარიერულ წინსვლასთან დაკავშირებული საკითხები.

პარტნიორი ორგანიზაციების წარმომადგენლები - სახელი, გვარი, დაბადების თარიღი, ასაკი, სქესი, მისამართი, პირადი ნომერი, პირადობის დამადასტურებელი დოკუმენტის სერია და ნომერი, პირადობის დამადასტურებელი დოკუმენტის გაცემის ვადა, რეზიუმე (CV), განათლების შესახებ ინფორმაცია, უცხო ენის ცოდნის შესახებ ინფორმაცია, დიპლომის ასლი ან განათლების დამადასტურებელი მოწმობა, კომპიუტერული პროგრამების ცოდნის შესახებ ინფორმაცია, სამუშაო გამოცდილების შესახებ ინფორმაცია, გავლილი ტრენინგებისა და გადამზადებების შესახებ ინფორმაცია, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, საბანკო ანგარიშის ნომერი, საპენსიო სქემაში ჩართვასთან დაკავშირებული ინფორმაცია, საშემოსავლო შეღავათით სარგებლობის საფუძველთან დაკავშირებული ინფორმაცია, დაკავებული პოზიცია (თანამდებობა), ანაზღაურების შესახებ ინფორმაცია, ინფორმაცია ნასამართლობის და უფლების ჩამორთმევის შესახებ, სახელის ანდა გვარის შეცვლის შემთხვევაში შესაბამისი ცვლილების დამდგენი დოკუმენტი, ინფორმაცია ჯანმრთელობის მდგომარეობის შესახებ, ვიდეო ჩანაწერი.

დამსაქმებლები - სახელი, გვარი, მისამართი, ტელეფონის ნომერი, ელექტრონული ფოსტა, მომწოდებელთა/ სავარაუდო მომწოდებელთა ფიზიკურ პირთა მონაცემები სახელი, გვარი, დაბადების თარიღი, ასაკი, სქესი, მისამართი, პირადი ნომერი, პირადობის დამადასტურებელი დოკუმენტის სერია და ნომერი, პირადობის დამადასტურებელი დოკუმენტის გაცემის ვადა, განათლების შესახებ ინფორმაცია, უცხო ენის ცოდნის შესახებ ინფორმაცია, დიპლომის ასლი ან განათლების დამადასტურებელი მოწმობა, მართვის მოწმობა, ავტოსატრანსპოტო საშუალების ფლობის/ სარგებლობის

მტკიცებულება, ტექ დათვალიერების დოკუმენტი, კომპიუტერული პროგრამების ცოდნის შესახებ ინფორმაცია, სამუშაო გამოცდილების შესახებ ინფორმაცია, გავლილი ტრენინგებისა და გადამზადებების შესახებ ინფორმაცია, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, საბანკო ანგარიშის ნომერი, საპენსიო სქემაში ჩართვასთან დაკავშირებული ინფორმაცია, ვიდეო ჩანაწერი

პროფორიენტაციაზე მოსულ პირთა მონაცემები - სახელი გვარი, სკოლის დასახელება, ტელეფონის ნომერი, ელექტრონული ფოსტა, ფოტო - ვიდეო მასალა.

ვიდეომონიტორინგის ხედვის არეალში მოხვედრილი პირების ვიზუალური გამოსახულება;

მონაცემთა დამუშავების საფუძველი

პერსონალურ მონაცემთა, მათ შორის განსაკუთრებული კატეგორიის მონაცემების, დამუშავების სამართლებრივი საფუძვლები

1) ორგანიზაციაში მონაცემები მუშავდება შემდეგი საფუძვლ(ებ)ის არსებობის შემთხვევაში:

ა) მონაცემთა სუბიექტმა განაცხადა/გამოხატა თანხმობა ერთი ან რამდენიმე კონკრეტული მიზნით მონაცემთა დამუშავებაზე;

ბ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტთან დადებული გარიგებით ნაკისრი ვალდებულების შესასრულებლად ან მონაცემთა სუბიექტის მოთხოვნით გარიგების დასადებად;

გ) მონაცემთა დამუშავება გათვალისწინებულია კანონით;

დ) მონაცემთა დამუშავება საჭიროა ორგანიზაციის მიერ საქართველოს კანონმდებლობით მისთვის დაკისრებული მოვალეობების შესასრულებლად;

ე) მონაცემთა დამუშავება აუცილებელია ორგანიზაციის ან მესამე პირის მნიშვნელოვანი ლეგიტიმური ინტერესების დასაცავად, გარდა იმ შემთხვევისა, თუ არსებობს მონაცემთა სუბიექტის (მათ შორის, არასრულწლოვნის) უფლებების დაცვის აღმატებული ინტერესი.

ორგანიზაციის მიერ მონაცემების დამუშავებასთან დაკავშირებული შესაძლო/არსებული

საფრთხეების შეფასების პროცესი

საფრთხეებისა და მათი წყაროების იდენტიფიცირება

ორგანიზაციაში მუშავდება სრულწლოვანი და არასრულწლოვანი პირების პერსონალური მონაცემები დიდი ოდენობით. აღნიშნული მონაცემები მუშავდება სრულყოფილი და ეფექტიანი საგანმანათლებლო მომსახურების გაწევისათვის აუცილებელი განსახორციელებელი პროცედურების ფარგლებში. შესაბამისად, აღნიშნულ პროცესში შესაძლებელია ჩართული იყოს ორგანიზაციის სხვადასხვა სამსახურის დასაქმებულები მათი კომპეტენციების შესაბამისად. საგანმანათლებლო მომსახურების გაწევის სპეციფიკის და პროცესში ჩართული პერსონალის ოდენობის, ასევე სხვა გარეშე, მესამე პირების (სახელმწიფო დაწესებულებები, მაგალითად, გამოძიების ორგანოები, სადაზღვევო კომპანიები და ა.შ.) ჩართულობის ფაქტორმა შესაძლებელია შექმნას განსაკუთრებული კატეგორიის მონაცემთა მესამე პირებისთვის, სამართლებრივი საფუძვლის გარეშე, გამჟღავნების საფრთხე. აღნიშნული შედეგ(ებ)ის გამომწვევი მიზეზები/ფაქტორები შესაძლებელია იყოს განსაკუთრებული კატეგორიის მონაცემების დამუშავების პროცესთან შეუსაბამო დაცვითი ღონისძიებები, კერძოდ, არასათანადოდ განხორციელებული ორგანიზაციული ან/და ტექნიკური ზომები, პერსონალის მიერ დაუდევარი დამოკიდებულებიდან გამომდინარე განსაკუთრებული კატეგორიის მონაცემების დამუშავების პროცესში დადგენილი უსაფრთხოების ზომების დარღვევა, მონაცემთა გამჟღავნების სამართლებრივი საფუძვლების არასწორი შეფასების საფუძველზე გარეშე პირებისათვის განსაკუთრებული კატეგორიის მონაცემთა გამჟღავნება, უფლებამოსილი თანამშრომლის მიერ დამუშავებულ მონაცემთა მიმართ დადგენილი შენახვის პროცედურის დარღვევა. ზემოთ აღნიშნულ პროცესს, მისი სენსიტიურობისა და განხორციელების სპეციფიკურობის გათვალისწინებით, ზოგადად, თან სდევს ხსენებული აბსტრაქტული საფრთხეების წარმოქმნისა და პრაქტიკაში მათი განვითარების შესაძლებლობა.

მონაცემთა დამუშავების შესაძლო შედეგები და პოტენციური (აბსტრაქტული) საფრთხეების ხარისხობრივი ანალიზი.

საქმიანობის პროცესში მონაცემთა დამუშავებასთან დაკავშირებული თანმდევი დაიდენტიფიცირებული სავარაუდო (აბსტრაქტული) საფრთხეების პრაქტიკულ რეალიზებას, ზოგადად, შესაძლოა მოჰყვეს ადამიანის უფლებებისა და თავისუფლებების შემლახავი/შემზღუდავი შემდეგი შედეგები:

ა) პერსონალური მონაცემების კონფიდენციალობის დარღვევა. პერსონალურ მონაცემთა დამუშავების პროცესში, დასაქმებულები, მათი სამსახურებრივი ფუნქცია - მოვალეობების ფარგლებში, უშუალოდ არიან ჩართულები, შესაბამისად, მათ ეკისრებათ მათ მიერ სამსახურებრივ ფარგლებში მიღებული ინფორმაციის კონფიდენციალურობის უპირობო დაცვის უზრუნველყოფა, აღნიშნული ვალდებულების არაჯეროვანმა

შესრულებამ კი შესაძლოა გამოიწვიოს მონაცემთა უსაფრთხოების, მათი შინაარსის, ინფორმაციის მთლიანობის დარღვევა. თუმცა, იმის გათვალისწინებით, რომ ორგანიზაციის დასაქმებულები მაღალი პასუხისმგებლობით ეკიდებიან მათზე დაკისრებულ ვალდებულებებს, რაც მათ შორის გამოიხატება, ორგანიზაციაში დანერგილი მონაცემთა უსაფრთხოების ორგანიზაციულ - ტექნიკური ზომების ზედმიწევნით დაცვაში, ზემოთ აღნიშნული საფრთხის დადგომის ალბათობა არის დაბალი.

ბ) მონაცემთა სუბიექტის რეპუტაციის შელახვა - აღნიშნული საფრთხე, ზოგადად, თან სდევს მონაცემთა დამუშავების პროცესს, მით უფრო იმ ფონზე, როდესაც ორგანიზაცია ამუშავებს მომხმარებლების კატეგორიის მონაცემებს, ასევე პერსონალის მიერ დაწესებულებაში მყოფი მომხმარებლის ინდივიდუალური ქცევების, ხასიათის, ფიზიკური, ფსიქიკური მდგომარეობისა და მათი პიროვნებისათვის დამახასიათებელი სხვა უნიკალური ნიშან-თვისებების შესახებ ინფორმაციას. შესაბამისად, აღნიშნული ინფორმაციის არასათანადო დაცვას და მის უკანონო გამჟღავნებას, შესაძლოა შედეგად მოჰყვეს მომხმარებლის რეპუტაციისათვის დამაზიანებელი შედეგები. თუმცა, იმის გათვალისწინებით, რომ ორგანიზაციაში მონაცემთა დაცვის უსაფრთხოების მიმართულებით, გატარებულია ეფექტიანი დაცვითი ღონისძიებები, მიღებულია ორგანიზაციულ - ტექნიკური ზომები, აღნიშნული საფრთხის პრაქტიკაში რეალიზების ალბათობა, არის დაბალი.

გ) სხვა სახის მნიშვნელოვანი ფიზიკური, ქონებრივი ან არაქონებრივი ღირებულების მატერიალური ან არამატერიალური ზიანი - ზოგადად, პერსონალურ მონაცემთა კანონმდებლობით დადგენილი მოთხოვნების დარღვევით დამუშავებას შესაძლოა მოჰყვეს სხვა ისეთი სახის საზიანო შედეგი, რომელიც მნიშვნელოვნად (საგრძნობლად და არსებითად) გააუარესებს მონაცემთა სუბიექტის ფიზიკურ, ქონებრივ ან არაქონებრივ მდგომარეობას, რომელიც შესაძლოა გამოიხატოს როგორც მატერიალური, ასევე არამატერიალური ზარალის სახით. თუმცა, იმის გათვალისწინებით, რომ ორგანიზაციაში, მონაცემთა დაცვის უსაფრთხოების მიმართულებით, გატარებულია ეფექტიანი დაცვითი ღონისძიებები, მიღებულია სათანადო ორგანიზაციულ - ტექნიკური ზომები, აღნიშნული აბსტრაქტული საფრთხის პრაქტიკული რეალიზების ალბათობა არის საშუალო.

საფრთხეებზე რეაგირება

ხაზგასმით უნდა აღინიშნოს, რომ მოცემულ ეტაპზე ორგანიზაციაში მონაცემთა დაცვის უსაფრთხოების მიმართულებით გატარებული ეფექტიანი დაცვითი ღონისძიებების, მიღებული ორგანიზაციულ-ტექნიკური ზომების, გათვალისწინებით, ზემოთ აღნიშნული საფრთხეების არსებობისა და მათი პრაქტიკაში განხორციელების ალბათობის მაჩვენებელი არის დაბალი. თუმცა, ზემოთ განხილული და, ზოგადად, არსებული აბსტრაქტული (სავარაუდო) საფრთხეების შემცირების და მაქსიმალურად განეიტრალების, მათი პრაქტიკაში განხორციელების ყველა შესაძლო წინაპირობის აღმოფხვრის მიზნით, ორგანიზაცია მუდმივად ზრუნავს მონაცემთა ეფექტიანი

დაცვისაკენ მიმართული მთელი რიგი ორგანიზაციული და ტექნიკური ზომების ხარისხის გაუმჯობესებაზე. აღნიშნულიდან გამომდინარე, პერიოდულად მოწმდება ორგანიზაციაში მონაცემთა დამუშავებისას მიღებული უსაფრთხოების სტანდარტების/პროცედურის კანონმდებლობის მოთხოვნებთან შესაბამისობა. ორგანიზაცია პერმანენტულად უზრუნველყოფს მისი თანამშრომლებისთვის პერსონალური მონაცემების არსის, ასევე დამუშავებისას მათი უსაფრთხოების დაცვის მნიშვნელობისა და პრაქტიკაში ეფექტიანი რეალიზებისაკენ მიმართულ საკითხებზე ინფორმაციის მიწოდებას, შესაბამისი საინფორმაციო ხასიათის შეხვედრების, სწავლებების, ტრენინგების, სასწავლო პრაქტიკული სახის კურსების ჩატარების ფორმით.

საფრთხეების შეფასება და მათზე რეაგირება

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

1. ორგანიზაცია სათანადო ზომების მიღებით უზრუნველყოფს მონაცემთა უსაფრთხოებას, მათ დაცვას მონაცემთა დაკარგვისგან, უკანონო დამუშავებისგან, მათ შორის, განადგურებისგან, წაშლისგან, შეცვლისგან, გამჟღავნებისგან ან გამოყენებისგან.

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

3. ორგანიზაცია 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.

4. წინამდებარე დოკუმენტით დადგენილი წესების დარღვევა წარმოადგენს ორგანიზაციის შინაგანაწესისა და დასაქმებულთან დადებული შრომითი ხელშეკრულებების დარღვევას და ითვალისწინებს შესაბამისი პასუხისმგებლობის დაკისრებას დისციპლინური პასუხისმგებლობის შესახებ დებულებით დადგენილი წესის საფუძველზე. კონფიდენციალური ინფორმაციის დაცვის ვალდებულება დასაქმებულის შრომითი ურთიერთობის შეწყვეტის შემდგომაც არსებობს.

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

6. ორგანიზაციის დასაქმებულებისა და მომხმარებლის პირადი მონაცემების შენახვა ხდება როგორც მატერიალური, ისე ელექტრონული ფორმით.

7. დასაქმებულთა მატერიალური ფორმით არსებული დოკუმენტაცია (მიმდინარე დოკუმენტები, აქტიური პირადი საქმეები) ინახება საქმისწარმოების სამსახურში ბაინდერებში.

8. ელექტრონული მოწყობილობების მეშვეობით დამუშავებული მონაცემები ინახება ორგანიზაციის დაცულ შიდა სერვერებზე, რომელიც განთავსებულია ცალკე ოთახში, დაცულ ადგილას.

9. განსაკუთრებული კატეგორიის მონაცემებიდან, როგორიცაა ჯანმრთელობასთან დაკავშირებული ინფორმაცია, ინახება დოკუმენტებში 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

ხაზგასმით უნდა აღინიშნოს, რომ მოცემულ ეტაპზე ორგანიზაციაში მონაცემთა დაცვის უსაფრთხოების მიმართულებით გატარებული ეფექტიანი დაცვითი ღონისძიებების, მიღებული ორგანიზაციულ-ტექნიკური ზომების, გათვალისწინებით, ზემოთ აღნიშნული საფრთხეების არსებობისა და მათი პრაქტიკაში განხორციელების ალბათობის მაჩვენებელი არის დაბალი. თუმცა, ზემოთ განხილული და, ზოგადად, არსებული აბსტრაქტული (სავარაუდო) საფრთხეების შემცირების და მაქსიმალურად განეიტრალების, მათი პრაქტიკაში განხორციელების ყველა შესაძლო წინაპირობის აღმოფხვრის მიზნით, ორგანიზაცია მუდმივად ზრუნავს განსაკუთრებული კატეგორიის მონაცემთა ეფექტიანი დაცვისაკენ მიმართული მთელი რიგი ორგანიზაციული და ტექნიკური ზომების ხარისხის გაუმჯობესებაზე. აღნიშნულიდან გამომდინარე, პერიოდულად მოწმდება ორგანიზაციაში მონაცემთა დამუშავებისას მიღებული უსაფრთხოების სტანდარტების/პროცედურის კანონმდებლობის მოთხოვნებთან შესაბამისობა. ორგანიზაცია პერმანენტულად უზრუნველყოფს მისი თანამშრომლებისთვის პერსონალური მონაცემების არსის, ასევე დამუშავებისას მათი უსაფრთხოების დაცვის მნიშვნელობისა და პრაქტიკაში ეფექტიანი რეალიზებისაკენ მიმართულ საკითხებზე ინფორმაციის მიწოდებას, შესაბამისი საინფორმაციო ხასიათის შეხვედრების, სწავლებების, ტრენინგების, სასწავლო პრაქტიკული სახის კურსების ჩატარების ფორმით.

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 ოფიცერი

1. ორგანიზაციას ჰყავს პერსონალურ მონაცემთა დაცვის ოფიცერი - შპს ,,ჯეო სეიფთი“ (ს/ნ: 405321637), საკონტაქტო მონაცემები: ტელეფონის ნომერი - 577 543 021; ელფოსტა: amiran.japaridze@geosafety.ge

2. პერსონალურ მონაცემთა დაცვის ოფიცრის ვინაობა და მისი საკონტაქტო მონაცემები პროაქტიულად გამოქვეყნებულია ორგანიზაციის ოფიციალურ ვებგვერდზე.

3. პერსონალურ მონაცემთა დაცვის ოფიცერი:

ა) აკონტროლებს ორგანიზაციაში პერსონალურ მონაცემთა დამუშავების პროცესებს;

ბ) მონაწილეობს მონაცემთა დამუშავებისას წარმოშობილი/სამომავლო რისკების შეფასების პროცესში;

გ) განიხილავს მონაცემთა დამუშავებასთან დაკავშირებულ განცხადებებს, საჩივრებს და გასცემს შესაბამის რეკომენდაციებს;

დ) მონაცემთა დამუშავების კანონთან მუდმივად შესაბამისობის უზრუნველსაყოფად ორგანიზაციას წარუდგენს თავის მოსაზრებებს, რეკომენდაციებს მონაცემთა ეფექტიანად და უსაფრთხოდ დამუშავების მეთოდების, ღონისძიებების დანერგვის თაობაზე;

ე) უზრუნველყოფს ორგანიზაციის თანამშრომლებისათვის შესაბამისი ტრენინგების, სასწავლო პრაქტიკული სახის კურსების ჩატარებასა და სათანადო რეკომენდაციების გაცემას მონაცემთა დამუშავების პროცესთან დაკავშირებულ აქტუალურ საკითხებთან მიმართებით;

ვ) საჭიროების შემთხვევაში თანამშრომლობს სახელმწიფო აუდიტის სამსახურთან;

ზ) პერსონალურ მონაცემთა დაცვის საკითხების ეფექტიანად უზრუნველსაყოფად ახორციელებს კანონმდებლობით, მათ შორის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, მისთვის დაკისრებულ სხვა უფლება - მოვალეობებს.

პერსონალურ მონაცემთა დაცვის ოფიცერთან კონსულტირების მექანიზმის გამოყენება:

ორგანიზაცია იღებს ყველა აუცილებელ ზომას საფრთხეების არსებითად შესამცირებლად და კონსულტაციის მიზნით მიმართავს პერსონალურ მონაცემთა დაცვის ოფიცერს.