დანართი 1
დამტკიცებულია
შპს თავისუფალი ხედვის აკადემიის
ხელმძღვანელიოს 2025 წლის 12.09 N 01/85 ბრძანებით

პერსონალურ მონაცემთა დაცვის პოლიტიკა

შესავალი

შპს „თავისუფალი ხედვის აკადემია" (შემდგომში „დაწესებულება") მნიშვნელოვან ყურადღებას აქცევს პერსონალური მონაცემების დაცვის უზრუნველყოფას. აღნიშნული პოლიტიკა შეესაბამება საქართველოს „პერსონალურ მონაცემთა დაცვის შესახებ" კანონს და განსაზღვრავს მონაცემთა დამუშავების პროცესებს, სუბიექტთა უფლებების პატივისცემისა და მონაცემთა უსაფრთხოების დაცვის პრინციპებზე დაყრდნობით.

პოლიტიკა მიზნად ისახავს მონაცემთა დამუშავების გამჭვირვალობასა და ლეგიტიმურობას, რაც სანდო ტექნიკური და ორგანიზაციული ზომების დაცვით ხორციელდება.

მონაცემთა სუბიექტის პერსონალური მონაცემების კატეგორიები

დაწესებულება ამუშავებს მონაცემთა სუბიექტების პერსონალურ ინფორმაციას მხოლოდ კონკრეტული მიზნებისთვის და საქართველოს „პერსონალურ მონაცემთა დაცვის შესახებ" კანონთან სრული შესაბამისობით. მონაცემთა კატეგორიები მოიცავს:

1. **იდენტიფიცირების ინფორმაცია** – სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი, მისამართი და საკონტაქტო დეტალები.
2. **ფინანსური ინფორმაცია** – გადახდების ისტორია, საბანკო რეკვიზიტები და სადაზღვევო კონტრაქტთან დაკავშირებული მონაცემები.
3. **ბიომეტრიული ინფორმაცია** – ფოტო, ვიდეოჩანაწერები ან სხვა ბიომეტრიული დეტალები, საჭიროებისამებრ.
4. **სამუშაო ინფორმაცია** – თანამშრომლების თანამდებობა, სამუშაო განრიგი და შრომითი პირობები.

ყველა მონაცემი მუშავდება მხოლოდ იმ მოცულობით, რაც მიზნის მისაღწევად აუცილებელია, დაცულია კანონით დადგენილი სტანდარტები და უსაფრთხოების მკაცრი ზომებით.

დამუშავების მიზანი

დაწესებულება პერსონალურ მონაცემებს ამუშავებს მხოლოდ კანონით განსაზღვრული და ლეგიტიმური მიზნებისთვის.

პერსონალური მონაცემები მუშავდება აკადემიური პროცესების ორგანიზებისთვის, რაც მოიცავს სტუდენტებისა და თანამშრომლების ადმინისტრაციული და აკადემიური საქმიანობის მართვას.

მონაცემთა დამუშავება ხდება სამართლებრივი ვალდებულებების შესრულების მიზნით, რაც გულისხმობს კანონით გათვალისწინებული ანგარიშგებისა და შესაბამისი სახელმწიფო ორგანოებისთვის ინფორმაციის მიწოდებას.

დაწესებულება მონაცემებს იყენებს ფინანსური ოპერაციების განსახორციელებლად, მათ შორის თანამშრომლებთან და სხვა მხარეებთან ანგარიშსწორებისთვის.

უსაფრთხოების უზრუნველსაყოფად, პერსონალური მონაცემები მუშავდება ვიდეო მონიტორინგის გამოყენებით.

დამუშავების პრინციპები

დაწესებულება პერსონალურ მონაცემებს ამუშავებს საქართველოს კანონმდებლობით გათვალისწინებული პრინციპების დაცვით. მონაცემთა დამუშავება ხორციელდება კანონიერად, სამართლიანად და გამჭვირვალედ, სუბიექტის უფლებებისა და ღირსების პატივისცემით.

მონაცემები მუშავდება მხოლოდ მკაფიოდ განსაზღვრული და ლეგიტიმური მიზნებისთვის, მათი მოცულობა ყოველთვის პროპორციულია დასახული მიზნის მისაღწევად.

დაწესებულება უზრუნველყოფს მონაცემთა სიზუსტესა და საჭიროების შემთხვევაში მათ განახლებას. არაზუსტი მონაცემები გასწორდება ან წაიშლება გაუმართლებელი დაყოვნების გარეშე.

პერსონალური მონაცემები ინახება მხოლოდ საჭირო ვადით და მიზნის მიღწეპერსონალური მონაცემები ინახება მხოლოდ საჭირო ვადით და მიზნის მიღწევის შემდეგ წაიშლება, განადგურდება ან დეპერსონალიზდება, თუ კანონით სხვა მოთხოვნები არ არის გათვალისწინებული.ვის შემდეგ წაიშლება, განადგურდება ან დეპერსონალიზდება, თუ კანონით სხვა მოთხოვნები არ არის გათვალისწინებული.

მონაცემთა უსაფრთხოების უზრუნველსაყოფად დაწესებულება იყენებს ტექნიკურ და ორგანიზაციულ ზომებს, რაც გამორიცხავს უნებართვო წვდომას ან მონაცემთა დაკარგვას.

მონაცემთა დამუშავების საფუძვლები

დაწესებულება პერსონალურ მონაცემებს ამუშავებს მხოლოდ საქართველოს „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით განსაზღვრული სამართლებრივი საფუძვლებით.

მონაცემთა დამუშავება დასაშვებია, თუ მონაცემთა სუბიექტმა გასცა თანხმობა, ან ეს აუცილებელია ხელშეკრულების შესრულებისთვის, სამართლებრივი ვალდებულებების შესასრულებლად, ან სუბიექტის მოთხოვნის საფუძველზე საჭირო პროცესების უზრუნველსაყოფად.

დამუშავება შესაძლებელია ლეგიტიმური ინტერესების დაცვით, თუ ეს არ ეწინააღმდეგება სუბიექტის უფლებებსა და თავისუფლებებს.

ასევე, მონაცემები მუშავდება, თუ ისინი საჯაროდ ხელმისაწვდომია ან სუბიექტმა თავად გახადა საჯაროდ ხელმისაწვდომი.

დაწესებულება უზრუნველყოფს ყველა სამართლებრივი საფუძვლის დაცვას მონაცემთა დამუშავების პროცესში.

განსაკუთრებული კატეგორიის მონაცემთა დამუშავების საფუძვლები

განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავება ხორციელდება მხოლოდ კანონით განსაზღვრული შემთხვევებში და მონაცემთა სუბიექტის უფლებების დაცვის პირობებით.

ასეთი მონაცემების დამუშავება დასაშვებია მხოლოდ სუბიექტის მკაფიო და წერილობითი თანხმობის საფუძველზე, ან კანონით განსაზღვრული მიზნების მისაღწევად.

დაწესებულება უზრუნველყოფს განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებას მხოლოდ იმ მოცულობით, რაც აუცილებელია, შესაბამისი ტექნიკური და ორგანიზაციული ზომების დაცვით, რაც გამორიცხავს მონაცემთა უნებართვო წვდომას და უზრუნველყოფს სუბიექტის კონფიდენციალურობას.

უფლებამოსილი პირის როლი მონაცემთა დამუშავებაში

დაწესებულება პერსონალურ მონაცემებს საჭიროების შემთხვევაში უფლებამოსილი პირის მეშვეობით ამუშავებს, საქართველოს „პერსონალურ მონაცემთა დაცვის შესახებ" კანონთან სრულ შესაბამისობაში.

უფლებამოსილი პირი მოქმედებს უნივერსიტეტის სახელით და ვალდებულია დაიცვას მონაცემთა კონფიდენციალურობა, უსაფრთხოების ზომები და განახორციელოს მონაცემთა დამუშავება მხოლოდ უნივერსიტეტის მითითებების ფარგლებში.

ასეთი პირის ჩართვის შემთხვევაში, მისი პასუხისმგებლობა მოიცავს მონაცემთა განადგურებას ან დაბრუნებას, როდესაც ისინი აღარ არის საჭირო.

მონაცემთა სუბიექტის უფლებები

დაწესებულება უზრუნველყოფს პერსონალური მონაცემების სუბიექტის უფლებების დაცვას საქართველოს „პერსონალურ მონაცემთა დაცვის შესახებ" კანონის შესაბამისად.

მონაცემთა სუბიექტს უფლება აქვს:

- მიიღოს ინფორმაცია მისი პერსონალური მონაცემების დამუშავების შესახებ;
- მოითხოვოს მონაცემების გასწორება, განახლება ან წაშლა, თუ ისინი არასწორია ან აღარ არის საჭირო;
- უარი განაცხადოს ავტომატიზებულ გადაწყვეტილებებზე, რომლებიც მასზე გავლენას ახდენს;
- მოითხოვოს მონაცემთა გადატანა ან მათი გადაცემა სხვა უფლებამოსილ პირისთვის;
- ნებისმიერ დროს გააუქმოს ადრე გაცემული თანხმობა.

მოთხოვნების განხილვა ხდება უნივერსიტეტის მიერ კანონმდებლობის შესაბამისად, თუმცა ზოგიერთ შემთხვევაში, შესაძლოა მათი დაკმაყოფილება ვერ მოხერხდეს, მაგალითად, თუ მოთხოვნა ეწინააღმდეგება უნივერსიტეტის სამართლებრივ ვალდებულებებს ან სხვა კანონიერ საფუძვლებს.

ვიდეო მონიტორინგი

დაწესებულებაში ვიდეო მონიტორინგი ხორციელდება უსაფრთხოების, ქონების დაცვისა და პროცესების გამჭვირვალობის უზრუნველსაყოფად, საქართველოს კანონმდებლობის სრული დაცვით.

ვიდეო მონიტორინგი შეიძლება განხორციელდეს ასევე საგამოცდო პროცესის დროს, საჭიროების მიხედვით. სუბიექტებს წინასწარ ეცნობებათ მონიტორინგის განხორციელების შესახებ, მათ შორის, გამაფრთხილებელი ნიშნებით ან სხვა შესაბამისი ფორმით.

ვიდეო ჩანაწერებზე წვდომა შეზღუდულია და გამოიყენება მხოლოდ ლეგიტიმური მიზნებისთვის. ჩანაწერების შენახვის ვადა განისაზღვრება შიდა პოლიტიკით, ხოლო მათი უსაფრთხოება უზრუნველყოფილია სათანადო ტექნიკური და ორგანიზაციული ზომებით.

მონაცემთა სუბიექტების უფლებები მონიტორინგის პროცესში მაქსიმალურად არის დაცული, რაც გამორიცხავს ჩანაწერების არასანქცირებულ გამოყენებას ან წვდომას.

პერსონალურ მონაცემთა დაცვის ოფიცერი

დაწესებულება პერსონალურ მონაცემთა დაცვის ოფიცერი უზრუნველყოფს მონაცემთა დამუშავების პროცესების კანონთან შესაბამისობას და სუბიექტთა უფლებების დაცვას.

ოფიცერი უწევს კონსულტაციას უნივერსიტეტს მონაცემთა დაცვის საკითხებზე და სთავაზობს რეკომენდაციებს. ის ასევე იღებს პრევენციულ ზომებს სამართალდარღვევების თავიდან ასაცილებლად.

მონაცემთა სუბიექტს შეუძლია დაუკავშირდეს ოფიცერს დამატებითი ინფორმაციის მისაღებად ან თავისი უფლებების გასარკვევად.

ინციდენტი

დაწესებულებაში პერსონალური მონაცემების უსაფრთხოების დარღვევის ან ინციდენტის შემთხვევაში მოქმედებს ინციდენტების მართვის პოლიტიკა, რომელიც უზრუნველყოფს სწრაფ და ეფექტურ რეაგირებას.

ინციდენტი შეიძლება მოიცავდეს მონაცემთა უნებართვო წვდომას, დაკარგვას, შეცვლას, გამჟღავნებას ან განადგურებას. მისი გამოვლენის შემთხვევაში, დაწესებულება დაუყოვნებლივ იღებს ზომებს მონაცემთა სუბიექტის უფლებების დაცვისა და ზიანის მინიმუმამდე შესამცირებლად.

დაწესებულება კანონმდებლობის შესაბამისად აცნობებს მონაცემთა სუბიექტებს, თუ ინციდენტი გავლენას ახდენს მათ მონაცემებზე. ინციდენტთან დაკავშირებული ინფორმაცია ინახება სპეციალურ ჩანაწერებში, რაც ხელს უწყობს მონაცემთა დაცვის პროცესების გაუმჯობესებას.

უსაფრთხოების დაცვა და მექანიზმები

დაწესებულება უზრუნველყოფს პერსონალური მონაცემების დაცვას ტექნიკური და ორგანიზაციული ზომებით, რომლებიც ხელს უშლიან მონაცემთა უნებართვო წვდომას, დაკარგვას, დაზიანებას ან უკანონო დამუშავებას.

მონაცემთა ფიზიკური უსაფრთხოებისთვის წვდომა შეზღუდულია მხოლოდ უფლებამოსილი პირებისთვის, ხოლო ვიდეო მონიტორინგი გამოიყენება კონფიდენციალურობის უზრუნველსაყოფად.

ტექნიკური უსაფრთხოება მოიცავს დაცული სისტემების გამოყენებას, რაც უზრუნველყოფს წვდომის კონტროლსა და ლოგირების შესაძლებლობას, გამორიცხავს არასანქცირებულ მოქმედებებს.

ორგანიზაციული უსაფრთხოების ზომებში შედის თანამშრომელთა რეგულარული ტრენინგი და შიდა პოლიტიკების პერიოდული გადახედვა.

დაწესებულება მუდმივად აუმჯობესებს უსაფრთხოების მექანიზმებს და ინციდენტების შემთხვევაში სწრაფად მოქმედებს მონაცემთა სუბიექტის უფლებების დასაცავად.

პასუხისმგებლობა

დაწესებულება პასუხისმგებელია პერსონალური მონაცემების დამუშავების კანონიერებასა და სუბიექტის უფლებების დაცვაზე საქართველოს „პერსონალურ მონაცემთა დაცვის შესახებ" კანონის შესაბამისად.

მონაცემთა დამუშავებაში ჩართული პირები ვალდებულნი არიან დაიცვან კონფიდენციალურობა და უსაფრთხოების პრინციპები. დარღვევის შემთხვევაში, პასუხისმგებლობა ეკისრებათ იმ პირებს, რომლებმაც ვერ უზრუნველყვეს დადგენილი წესების დაცვა.

დაწესებულება უზრუნველყოფს თანამშრომლების ინფორმირებას და ტრენინგს, ასევე პერიოდულად აკონტროლებს მონაცემთა დამუშავების პროცესებს. ინციდენტების შემთხვევაში, უზრუნველყოფილია სწრაფი რეაგირება და პრევენციული ღონისძიებების გატარება.

პოლიტიკის განახლება

დაწესებულება იტოვებს უფლებას, განაახლოს პერსონალურ მონაცემთა დაცვის პოლიტიკა კანონმდებლობის, რეგულაციების ან ორგანიზაციული საჭიროებების ცვლილების შესაბამისად. პოლიტიკის გადახედვა ხდება პერიოდულად, მაგრამ არაუგვიანეს ერთწლიანი ინტერვალისა.

განახლებული პოლიტიკა ამოქმედდება დამტკიცებისთანავე, თუ სხვა ვადა სპეციალურად არ არის განსაზღვრული.

წინამდებარე პოლიტიკაში გაუთვალისწინებელი შემთხვევები რეგულირდება საქართველოს კანონმდებლობით და დაწესებულების შიდა ნორმებით.