დამტკიცებულია შპს საქართველოს უნივერსიტეტის რექტორის საბჭოს 2026 წლის 22 ივნისის N16/26 ოქმით

მონაცემთა დაცვაზე ზეგავლენის შეფასება (DPIA)

დოკუმენტის ნომერი:

თარიღი:

დამუშავებისთვის პასუხისმგებელი პირი: შპს „საქართველოს უნივერსიტეტი“

პერსონალურ მონაცემთა დაცვის ოფიცერი: შპს „უსაფრთხო მონაცემთა გადაწყვეტილებები;“ ელ. ფოსტა: anatavkhelidze@safedata.ge

საკითხი: საგამოცდო ცენტრში სტუდენტთა იდენტიფიკაციისთვის ბიომეტრიული სისტემის დანერგვა

ნაწილი I. მონაცემთა დამუშავების პროცესი

1. მონაცემთა დამუშავების პროცესის აღწერა

საგამოცდო ცენტრში შესვლამდე სტუდენტების იდენტიფიცირება ხდება სახის გამოსახულების (ფოტოს) შედარების გზით უნივერსიტეტის ბაზაში არსებულ ფოტოსთან სპეციალიზებული აპარატის მეშვეობით. პროცესის მიზანია საგამოცდო პროცესის უსაფრთხოების დაცვა, აკადემიური კეთილსინდისიერების უზრუნველყოფა და სხვის მაგივრად გამოცდაზე შესვლის პრევენცია.

2. მონაცემთა კატეგორიები

2.1. პროცესის ფარგლებში მუშავდება შემდეგი კატეგორიის მონაცემები:

- **ბიომეტრიული:** სახის გამოსახულება;
- **მაიდენტიფიცირებელი:** სახელი, გვარი, სტუდენტის საიდენტიფიკაციო კოდი.

2.2. **მონაცემთა მიმღებები:** წვდომა აქვთ მხოლოდ უნივერსიტეტის რექტორის ბრძანებით განსაზღვრულ უფლებამოსილ პირებს, კერძოდ, სასწავლო ოფისის წარმომადგენლებსა და IT სამსახურის სპეციალისტს.

3. აუცილებლობისა და პროპორციულობის შეფასება

3.1. **ლეგიტიმური მიზანი:** საგამოცდო პროცესის უსაფრთხოების უზრუნველყოფა, აკადემიური თაღლითობის პრევენცია და უნივერსიტეტის შიდა რეგულაციების დაცვა.

3.2. **აუცილებლობის დასაბუთება:** საგამოცდო პროცესის მიმდინარეობისას საგამოცდო ცენტრში ფიქსირდება სტუდენტთა მაღალი ნაკადი. შესაბამისად, კრიტიკულად მნიშვნელოვანია პირის იდენტიფიცირებისა და ავთენტიფიკაციის პროცესის უტყუარობისა

და ოპერატიულობის უზრუნველყოფა, რათა გამოირიცხოს საგამოცდო პროცესში არაუფლებამოსილი პირის მონაწილეობა. აღნიშნული მექანიზმის დანერგვის აუცილებლობა კი ეფუძნება უნივერსიტეტის პრაქტიკაში დაფიქსირებულ პრეცედენტებს, კერძოდ, გამოვლინდა ფაქტები, როდესაც ადგილი ჰქონდა მესამე პირის მიერ სხვისი პირადობის დამადასტურებელი დოკუმენტის გამოყენებით გამოცდაზე დაშვების მცდელობას. აღნიშნულმა გარემოებებმა, ასევე უნივერსიტეტის შიდა რეგულაციებისა თუ აკადემიური კეთილსინდისიერების დაცვის მიზანმა, წარმოშვა იდენტიფიკაციის უფრო მაღალი სანდოობის მქონე, ბიომეტრიული სისტემის დანერგვის ობიექტური სამართლებრივი და პრაქტიკული საჭიროება.

3.3. **ალტერნატიული საშუალებები:** უნივერსიტეტმა განიხილა იდენტიფიკაციის პროცესის მხოლოდ პერსონალის მიერ მართვის შესაძლებლობა (სტუდენტური ბარათის ან პირადობის მოწმობის შემოწმება). თუმცა, სტუდენტთა დიდი რაოდენობიდან გამომდინარე (დაახლოებით 2000 სტუდენტი), ეს მეთოდი დაკავშირებულია არაპროპორციულად დიდ დროსთან, რაც აფერხებს საგამოცდო პროცესს. გარდა ამისა, ადამიანური ფაქტორით მართული კონტროლი შეიცავს სუბიექტურობისა და შეცდომის (მაგალითად, მსგავსი გარეგნობის პირის ან ყალბი დოკუმენტის გატარების) მაღალ რისკს. ბიომეტრიული იდენტიფიკაცია უზრუნველყოფს მონაცემთა მაღალ სიზუსტეს და მინიმუმამდე დაჰყავს უსაფრთხოების რისკები. ამასთან, პროპორციულობის დასაცავად, სისტემა დაფუძნებულია ნებაყოფლობით თანხმობაზე და სტუდენტს ყოველთვის აქვს ალტერნატიული ფიზიკური იდენტიფიკაციის არჩევის უფლება.

4. მონაცემთა მიმღები და მესამე პირებისთვის გადაცემა

4.1. მონაცემებზე წვდომა აქვთ მხოლოდ საქართველოს უნივერსიტეტის სასწავლო ოფისსა და IT სამსახურის სპეციალისტს საქართველოს უნივერსიტეტის რექტორის ბრძანების შესაბამისად.

4.2. მონაცემების გადაცემა მესამე პირებზე არ ხდება, გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა, როგორიცაა, მაგალითად, საგამოძიებო უწყებისთვის მონაცემების გადაცემა მოთხოვნის საფუძველზე.

5. პერსონალური მონაცემების შენახვის ვადები

მონაცემთა სახე	მონაცემთა შენახვის ვადა

ბიომეტრიული ფოტო (აპარატის მიერ გადაღებული)	არ ინახება. იშლება ავტომატურად, იდენტიფიკაციის პროცესის დასრულებისთანავე.
უნივერსიტეტის ბაზაში არსებული მონაცემები (ფოტო-სურათი)	არ ინახება.
ტექნოლოგიური / ლოგირების მონაცემები (Log files)	არ ინახება. წაიშლება ავტომატურად პროცესის დასრულებისთანავე.

6. მონაცემთა დამუშავების პრინციპები

6.1. **დამუშავების კანონიერების, სამართლიანობისა და გამჭვირვალობის პრინციპები:** უნივერსიტეტი მონაცემებს ამუშავებს სრულიად გამჭვირვალედ და სტუდენტის უფლებების მაქსიმალური პატივისცემით. დამუშავების საფუძველია სტუდენტის წინასწარი, წერილობითი/ელექტრონული თანხმობა. სტუდენტი ინფორმირებულია მონაცემთა დამუშავების მიზნის, ვადებისა და მისი უფლებების შესახებ სპეციალური თანხმობის ფორმის მეშვეობით. საგამოცდო ცენტრის შესასვლელთან თვალსაჩინო ადგილას განთავსებულია გამაფრთხილებელი ნიშნები.

6.2. **მიზნის შეზღუდვა და მონაცემთა მინიმიზაცია:** მონაცემთა დამუშავების მიზანია მხოლოდ იდენტიფიკაცია საგამოცდო პროცესისთვის. უნივერსიტეტი ამუშავებს მონაცემებს მხოლოდ იმ მინიმალური მოცულობით, რაც აუცილებელია ამ ლეგიტიმური მიზნის მისაღწევად (მხოლოდ ფოტოს შედარება).

6.3. **უსაფრთხოება, მთლიანობა და კონფიდენციალურობა:** უნივერსიტეტი უზრუნველყოფს მონაცემების საიმედო დაცვას არაავტორიზებული წვდომისგან, შეცვლისგან ან გამჟღავნებისგან. მონაცემებზე წვდომა აქვთ მხოლოდ ავტორიზებულ პირებს პერსონალური პაროლების გამოყენებით. სისტემა ავტომატურად აღრიცხავს შესვლის ან ცვლილების ყოველ მცდელობას. მონაცემები დაცულია დაშიფვრის თანამედროვე მეთოდებით.

6.4. **მონაცემთა შენახვის ვადის შეზღუდვა:** აპარატის მიერ იდენტიფიკაციისთვის გადაღებული ფოტოები არ ინახება და იშლება მომენტალურად. სტუდენტის სტატუსის შეწყვეტისთანავე ბაზიდან იშლება მისი საიდენტიფიკაციო შაბლონიც.

ნაწილი II. ადამიანის ძირითადი უფლებებისა და თავისუფლებების შეზღუდვის შესაძლო საფრთხეები და მათზე რეაგირება

უნივერსიტეტი ამუშავებს სტუდენტთა განსაკუთრებული კატეგორიის (ბიომეტრიულ) მონაცემებს. შესაბამისად, აუცილებელია რისკების იდენტიფიცირება და მათი შეფასება.

7. რისკების იდენტიფიცირება და შეფასება (Risk Assessment)

საფრთხე	**ალბათობა**	**გავლენა**	**რისკის დონე**
ბიომეტრიული მონაცემების გაჟონვა	დაბალი	მაღალი	საშუალო
მონაცემებზე არაუფლებამოსილი შიდა წვდომა	საშუალო	საშუალო	საშუალო
სისტემური შეცდომა (ცრუ იდენტიფიკაცია / ამოუცნობლობა)	საშუალო	საშუალო	საშუალო
მონაცემების შენახვის ვადების გადაცილება	დაბალი	დაბალი	დაბალი

8. რისკების შემცირების ზომები

8.1. **ტექნიკური დაცვა:** ბაზაში არსებული ფოტოები და შაბლონები არ ინახება.

8.2. **ლოკალური შენახვა:** მონაცემები ინახება უნივერსიტეტის ლოკალურ დაცულ სერვერზე და არ გადაეცემა გარე, არასანდო Cloud სერვერებს.

8.3. **წვდომის კონტროლი:** სისტემა აღრიცხავს (Log Files) მომხმარებლის ყოველ მოქმედებას. წვდომა მკაცრად შეზღუდულია.

8.4. **ვადების დაცვა:** სისტემაში ინტეგრირებულია ავტომატური წაშლის მექანიზმი იდენტიფიკაციის გავლისთანავე.

8.5. **ადამიანური ჩარევა:** თუ აპარატი ვერ ამოიცნობს სტუდენტს, ეს არ იწვევს გამოცდიდან ავტომატურ მოხსნას. ასეთ შემთხვევაში პირის იდენტიფიკაციას ახდენს უფლებამოსილი თანამშრომელი პირადობის მოწმობის ან სტუდენტური ბარათის საფუძველზე.

9. მონაცემთა სუბიექტის უფლებების დაცვა

9.1. სტუდენტები წინასწარ, დეტალურად არიან ინფორმირებულნი დამუშავების წესის შესახებ სპეციალური თანხმობის ფორმით.

9.2. სტუდენტს აქვს არჩევანი, უარი თქვას ბიომეტრიულ იდენტიფიკაციაზე ყოველგვარი ნეგატიური შედეგის გარეშე.

9.3. სრულად არის უზრუნველყოფილი საქართველოს კანონმდებლობით გათვალისწინებული უფლებები (წვდომის, შესწორების, წაშლის, თანხმობის გამოხმობის უფლება).

9.4. საგამოცდო ცენტრთან განთავსებულია შესაბამისი გამაფრთხილებელი ნიშნები.

10. ზეგავლენის შეფასებაში ჩართული სუბიექტები და გადასინჯვა

10.1. ზეგავლენის შეფასების პროცესში ჩართული იყვნენ უნივერსიტეტის პერსონალურ მონაცემთა დაცვის ოფიცერი, იურიდიული სამსახური, IT სამსახური.

10.2. უნივერსიტეტი ახორციელებს მონაცემთა დამუშავების პროცესისა და უსაფრთხოების სისტემების პერიოდულ მონიტორინგს. დოკუმენტი დაექვემდებარება გადასინჯვას ტექნოლოგიური პროცესის განახლების ან საქართველოს კანონმდებლობაში განხორციელებული ცვლილებების შემთხვევაში.

11. საბოლოო დასკვნა

დამუშავება არის პროპორციული და აუცილებელი საგამოცდო პროცესის უსაფრთხოებისა და აკადემიური კეთილსინდისიერების ლეგიტიმური მიზნების მისაღწევად. რისკები მინიმიზებულია ადეკვატური ტექნიკური და ორგანიზაციული ზომებით.

დამტკიცებულია შპს საქართველოს უნივერსიტეტის რექტორის საბჭოს 2026 წლის 22 ივნისის N16/26 ოქმით

გათვალისწინებულია ნებაყოფლობითი თანხმობისა და ალტერნატივის პრინციპი. პროცესი სრულ შესაბამისობაშია საქართველოს კანონმდებლობასთან და GDPR-ის მოთხოვნებთან.

რექტორი: _____

თარიღი: _____