პერსონალურ მონაცემთა
დაცვის ინსპექტორის აპარატი

რეკომენდაციები ბიომეტრიულ მონაცემთა დამუშავების შესახებ

წინამდებარე დოკუმენტი შემუშავებულია პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის, მონაცემთა დაცვის ევროპული სტანდარტებისა და საერთაშორისო პრაქტიკის ანალიზის საფუძველზე. დოკუმენტი სარეკომენდაციო ხასიათისაა და განკუთვნილია როგორც საჯარო, ისე კერძო ორგანიზაციებისთვის, რომლებიც ამუშავებენ ბიომეტრიულ მონაცემებს.

რეკომენდაციის მიზანია მონაცემთა დამმუშავებელს განუმარტოს კანონისმიერი ვალდებულებები და ბიომეტრიული მონაცემების დამუშავების პროცესში გასათვალისწინებელი საკითხები.

I. შესავალი

ბიომეტრიული მონაცემების გამოყენების მზარდი დინამიკა თავისთავად წარმოშობს მისი რეგულირებისა და შეფასების ეფექტური მეთოდების დანერგვის საჭიროებას. პრაქტიკაში ბიომეტრიული მონაცემები ძირითადად გამოიყენება სახელმწიფო საზღვრების კონტროლის, მიგრაციის მართვის, პასპორტების დამზადების, საიდუმლო ინფორმაციის დაცვის, ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფისა და სხვა მიზნებისთვის. ბიომეტრიული მონაცემების გამოყენებას აქვს მნიშვნელოვანი პრაქტიკული უპირატესობები, ამასთან თითოეული ფიზიკური პირისთვის ამ მონაცემების უნიკალური და მუდმივი ხასიათიდან გამომდინარე, მნიშვნელოვანია, მონაცემთა დამმუშავებლის მხრიდან სიღრმისეულად იქნეს გაანალიზებული საერთაშორისო თუ ქვეყნის შიდა კანონმდებლობით დადგენილი პრინციპები და მოთხოვნები.

პრაქტიკაში, განსხვავებული მიზნითა და საფუძვლით ბიომეტრიული მონაცემების შეგროვება და დამუშავება, ხშირად წარმოშობს ბიომეტრიული სისტემების აუცილებლობასთან დაკავშირებულ კითხვებს. ბიომეტრიული მონაცემების დამუშავების კანონიერება, ადეკვატურობა და პროპორციულობა წარმოადგენს „პერსონალური მონაცემების დაცვის შესახებ“ საქართველოს კანონის რეგულირების სფეროს. კანონი ამომწურავად განსაზღვრავს აღნიშნული ტიპის მონაცემთა დამუშავების კანონიერ საფუძვლებს, პრინციპებს, მიზნებს, უსაფრთხოებას, მონაცემთა სუბიექტის უფლებებსა და პერსონალურ მონაცემთა დაცვის ინსპექტორისადმი ინფორმაციის მიწოდების ვალდებულებას.

II. რა არის ბიომეტრიული მონაცემი

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „გ“ ქვეპუნქტის თანახმად, **ბიომეტრიული მონაცემი არის ფიზიკური, ფსიქიკური ან ქცევის მახასიათებელი, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისათვის და რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება (თითის ანაბეჭდი, ტერფის ანაბეჭდი, თვალის ფერადი გარსი, თვალის ბადურის გარსი (თვალის ბადურის გამოსახულება), სახის მახასიათებელი).**

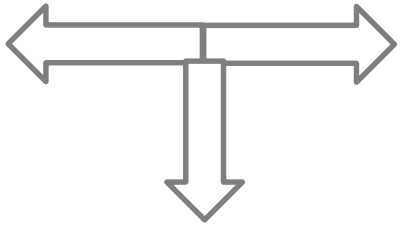
გასათვალისწინებელია ის გარემოებაც, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, **ბიომეტრიული მონაცემი განსაკუთრებული კატეგორიის მონაცემს წარმოადგენს მხოლოდ მაშინ, როდესაც ის იძლევა ფიზიკური პირის იდენტიფიცირების საშუალებას განსაკუთრებული კატეგორიის მონაცემის ნიშნით, როგორიცაა** რასობრივი ან ეთნიკური

კუთვნილება, ჯანმრთელობის მდგომარეობა, ნასამართლობა და სხვა. შესაბამისად მათი დამუშავების დროს აუცილებელია კანონის მე-6 მუხლით გათვალისწინებული ერთ-ერთი საფუძვლის არსებობა მაინც - მაგალითად მონაცემთა სუბიექტის წერილობითი თანხმობა.

საერთაშორისო პრაქტიკაში, ბიომეტრიული მონაცემების დამუშავებისას, ყველაზე ხშირად გამოიყენება ადამიანის ქცევითი და ფიზიკური მახასიათებლები:

ქცევითი მახასიათებლები

ხელწერა, ხმა, სიარულის მანერა და სხვა...



ფიზიკური მახასიათებლები

თითის ანაბეჭდი, სახის ნაკვთები, თვალის ფერადი გარსი, თვალის ბადურის გარსი და სხვა...

ბიომეტრიული მახასიათებლები არის მუდმივი, უნიკალური, არატრანსფორმირებადი, ძნელად წარმოებადი ან გაყალბებადი, შესაცვლელად რთული.

III. ბიომეტრიული მონაცემების დამუშავება

“პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონის მე-2 მუხლის მიხედვით, დამუშავება გულისხმობს მონაცემებზე განხორციელებულ ნებისმიერ ქმედებას, მაგალითად, მონაცემთა შეგროვება, ჩაწერა, ფოტოზე აღბეჭდვა, აუდიო/ვიდეოჩაწერა, ორგანიზება, შენახვა, შეცვლა, აღდგენა, გამოყენება, გამჟღავნება, დაჯგუფება, კომბინაცია, დაბლოკვა,

წაშლა, განადგურება და სხვა. დამუშავება შესაძლებელია განხორციელდეს როგორც ავტომატურად (კომპიუტერული პროგრამის გამოყენებით), ისე არაავტომატურად (ჟურნალის წარმოება, მონაცემების ხელით შეყვანა) ან ნახევრად ავტომატური გზით.

იმისთვის, რომ ბიომეტრულ მონაცემთა დამუშავება იყოს კანონიერი, უნდა არსებობდეს მათი დამუშავების სამართლებრივი საფუძველი, მკაცრად განსაზღვრული კანონიერი მიზანი/მიზნები და დაცული უნდა იყოს კანონით გათვალისწინებული პრინციპები.

- ბიომეტრულ მონაცემთა დამუშავების კანონიერი მიზნები და სამართლებრივი საფუძვლები

ბიომეტრულ მონაცემთა სპეციფიკიდან გამომდინარე, კანონი ცალკე არეგულირებს ასეთი ტიპის მონაცემთა დამუშავებასთან დაკავშირებულ საკითხებს და მკაცრად განსაზღვრავს იმ მიზნებს, რომელთა მიღწევისთვისაც შესაძლებელია მათი დამუშავება.

საჯარო დაწესებულების მიერ ბიომეტრიულ მონაცემთა დამუშავება შეიძლება მხოლოდ **პირის უსაფრთხოებისა** და **საკუთრების დაცვის** მიზნებისათვის, აგრეთვე, **საიდუმლო ინფორმაციის გამჟღავნების თავიდან აცილების მიზნით,** თუ აღნიშნული მიზნის მიღწევა სხვა საშუალებებით შეუძლებელია, ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან. *მაგალითად: საჯარო დაწესებულების მიერ თანამშრომელთა შენობაში შესვლისა და გასვლის კონტროლი (დასაქმებულთა მხრიდან სამსახურში გამოცხადების აღრიცხვის მიზნით), თითის ანაბეჭდის გამოყენებით, ცალსახად ჩაითვლება არაადეკვატურ და არაპროპორციულ საშუალებად. შესაბამისად,* ***დასაქმებულის კონტროლის მიზნებისათვის ბიომეტრული მონაცემების დამუშავება არამართლზომიერია****. თუმცა, თითის ანაბეჭდის გამოყენებით* ***ფიზიკური შეღწევა შენობის იმ კონკრეტულ ნაწილში/ფლიგელში, სადაც ინახება საიდუმლოების შემცველი ინფორმაცია, ჩაითვლება მიზნის მიღწევის პროპორციულ საშუალებად.***

> "პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-9 მუხლის მეორე პუნქტის თანახმად, კანონიერად მიიჩნევა ბიომეტრიულ მონაცემთა დამუშავება პირადობის დამადასტურებელი დოკუმენტის გაცემის ან სახელმწიფო საზღვრის გადამკვეთი პირის იდენტიფიკაციის მიზნებისათვის.

კერძო დაწესებულებისა და ფიზიკური პირის მიერ, ბიომეტრიულ მონაცემთა დამუშავება შეიძლება მხოლოდ იმ შემთხვევაში, თუ ეს აუცილებელია **საქმიანობის განხორციელებისათვის**, **უსაფრთხოებისა** და **საკუთრების დაცვის**, ასევე **საიდუმლო ინფორმაციის გამჟღავნების თავიდან აცილების მიზნებისათვის**, თუკი აღნიშნული მიზნის მიღწევა სხვა საშუალებებით

შეუძლებელია, ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან. *მაგალითად: კონკრეტული ბანკისათვის, თითოეულ ფილიალში განთავსებული საცავის უსაფრთხოების უზრუნველყოფისათვის შეიძლება დამუშავდეს ბიომეტრიული მონაცემები, ნაცვლად ცალკე სამტატო ერთეულით გათვალისწინებული პასუხისმგებელი პირის გამოყოფისა, რომელიც ვალდებული იქნება უზრუნველყოს რამდენიმე საცავის უსაფრთხოება, აღნიშნული გარემოება ბანკისათვის შეიძლება დაკავშირებული იყოს არაპროპორციულად დიდ ძალისხმევასთან.*

ბიომეტრულ მონაცემთა დამუშავების მართლზომიერებისთვის, აუცილებელია დამუშავების სამართლებრივი საფუძვლის არსებობა. იმ შემთხვევაში თუ ბიომეტრული მონაცემი არ არის განსაკუთრებული კატეგორიის მონაცემი, მონაცემთა დამმუშავებელმა უნდა იხელმძღვანელოს პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მე-5 მუხლში მოცემული საფუძვლებით. ხოლო თუ ბიომეტრული მონაცემები განსაკუთრებული კატეგორიისა, მაშინ მათი დამუშავება შესაძლებელია მხოლოდ პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მე-6 მუხლის მე-2 პუნქტით განსაზღვრული ერთ-ერთი საფუძვლის არსებობის შემთხვევაში.

! აუცილებელია, რომ მონაცემთა დამმუშავებლმა განსაზღვროს ბიომეტრიულ მონაცემთა დამუშავების კანონიერი საფუძველი, წინააღმდეგ შემთხვევაში მონაცემთა დამუშავება ჩაითვლება კანონსაწინააღმდეგოდ.

➢ ბიომეტრიულ მონაცემთა დამუშავების პრინციპები

მონაცემთა დამმუშავებელმა პერსონალური მონაცემების დამუშავებისას პატივი უნდა სცეს სამართლიანობისა და კანონიერების დაცვის პრინციპს, მონაცემთა სუბიექტის კონსტიტუციით გარანტირებულ უფლებებსა და თავისუფლებებს, მათ შორის, ადამიანის პატივისა და ღირსების, პირადი და ოჯახური ცხოვრების ხელშეუხებლობისა და პიროვნების თავისუფალი განვითარების უფლებებს.

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მე-4 მუხლში მოცემულია ის პრინციპები, რომელთა დაცვაც სავალდებულოა პერსონალურ მონაცემთა დამუშავებისას, როგორც კერძო/ფიზიკური პირისათვის, ასევე საჯარო დაწესებულებისათვის.

მონაცემთა დამუშავებისას დაცულ უნდა იქნას შემდეგი პრინციპები:

- **სამართლიანობისა და კანონიერების პრინციპი**

  მონაცემები უნდა დამუშავდეს სამართლიანად და კანონიერად, იმგვარად, რომ არ შეილახოს მონაცემთა სუბიექტის პატივი და ღირსება. *მაგალითად: ფოტოს სტუდიის მიერ, მოქალაქის ბიომეტრიული ფოტოს გამოქვეყნება საჯაროდ, ვებ-საიტზე ან სოციალური ქსელში განთავსება დამცინავი/იუმორისტული მიზნებისათვის, ჩაითვლება პირის პატივისა და ღირსების შემლახველ ქმედებად, ასევე სამართლიანობისა და კანონიერების პრინციპის არსებით დარღვევად.*

- **კანონიერი მიზნის პრინციპი**

  მონაცემები უნდა დამუშავდეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული კანონიერი მიზნებისათვის. დაუშვებელია მონაცემთა დამუშავება სხვა, თავდაპირველ მიზანთან არათავსებადი მიზნით. ყოველი დამუშავებისათვის უნდა არსებობდეს ახალი მიზანი. *მაგალითად, ფოტო სტუდიის მიერ, საკუთარი საქმიანობის განხორციელების მიზნით, კლიენტისათვის გადაღებული ფოტო ჩაითვლება დამოუკიდებელ მიზნად, ხოლო აღნიშნული ფოტოს რეკლამისათვის გამოყენება (პრაქტიკაში ხშირია ფოტო სტუდიის მიერ რეკლამისათვის კლიენტისათვის გადაღებული ფოტოს გამოყენება) ჩაითვლება ახალ, თავდაპირველ მიზანთან შეუთავსებლად.*

- **ადეკვატურობისა და პროპორციულობის პრინციპი**

  მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. მონაცემები უნდა იყოს იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევადაც მუშავდება ისინი. *მაგალითად: დაწესებულების მხრიდან დასაქმებულ პირთა სამსახურში გამოცხადების კონტროლის მიზნით თითის ანაბეჭდის გამოყენება, ჩაითვლება არაადეკვატურ და არაპროპორციულ საშუალებად იმ მიზანთან, რომელიც შესაძლოა მიიღწეს ბიომეტრიული მონაცემების გამოყენების გარეშე.*

- მონაცემები უნდა იყოს ნამდვილი და ზუსტი, რომელიც საჭიროების შემთხვევაში უნდა განახლდეს. კანონიერი საფუძვლის გარეშე შეგროვებული და დამუშავების მიზანთან შეუსაბამო მონაცემები უნდა დაიბლოკოს, წაიშალოს ან/და განადგურდეს.

- მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად. მას შემდეგ რაც დამუშავების მიზანი მიიღწევა მონაცემები უნდა დაიბლოკოს, წაიშალოს ან განადგურდეს, ან შენახულ იქნეს პირის იდენტიფიცირების გამომრიცხავი ფორმით. *მაგალითად: თუ თანამშრომელი გათავისუფლდა ან დატოვა დაკავებული თანამდებობა, დაწესებულება ვალდებულია წაშალოს ან გაანადგუროს ის ბიომეტრიული მონაცემი, რომელიც მუშავდებოდა ამ პირის თანამდებობაზე ყოფნის პერიოდში, წინააღმდეგ შემთხვევაში ბიომეტრიული მონაცემის შენახვის ფაქტი ჩაითვლება ადეკვატურობისა და პროპორციულობის პრინციპის დარღვევად.*

! მნიშვნელოვანია, რომ ყველა საჯარო და კერძო დაწესებულამ განსაკუთრებული სიმკაცრით შეაფასოს ბიომეტრულ მონაცემთა შენახვის აუცილებლობა და საჭიროებებიდან გამომდინარე განსაზღვროს შენახვის კონკრეტული ვადა.

IV. ბიომეტრულ მონაცემთა დამუშავების მეთოდები

ტექნოლოგიების განვითარებამ წარმოშვა ბიომეტრიული მონაცემების დამუშავების სხვადასხვა მეთოდი, რომელიც შესაძლოა გამოიყენებოდეს კომბინირებულადაც. მაგალითად, ზოგიერთი სისტემა ერთდროულად იყენებს ხმისა და სახის ამოცნობის მეთოდებს. ტექნოლოგიურ პროგრესთან ერთად იზრდება ბიომეტრიული მონაცემების გამოყენების საფრთხე მონაცემთა სუბიექტის ნებართვის და ინფორმირებულობის გარეშე.

მსოფლიო პრაქტიკაში გამოიყენება ბიომეტრიული მონაცემების დამუშავების ორი ძირითადი მეთოდი, ესენია **ვერიფიკაცია** და **იდენტიფიკაცია,** მათ შორის სხვაობა არსებითია. ყველაზე ხშირად სწორედ ამ ორი მეთოდის გამოყენებით ხდება ბიომეტრიული მონაცემების დამუშავება როგორც ფიზიკურ, ასევე ვირტუალურ სივრცეში (წვდომა კონკრეტულ სერვერზე ან სისტემაზე) შეღწევის კონტროლის მიზნით.

იდენტიფიკაციის მეთოდი გულისხმობს ბიომეტრიული მონაცემების ავთენტურობის შემოწმებას მონაცემთა ბაზაში არსებულ ინფორმაციასთან და ხშირად მოიხსენიება სახელით ***ერთი-მრავალთან***, რაც გულისხმობს ბიომეტრიული სისტემის მიერ იმის დადგენას ეკუთვნის, თუ არა კონკრეტული ბიომეტრიული მონაცემი (თითის ანაბეჭდი, ხმა, ხელწერა, ა.შ) კონკრეტულ პიროვნებას. შესაბამისად, სისტემა ადარებს კონკრეტულ ბიომეტრიულ მონაცემს ბაზაში არსებულ ყველა ნიმუშს. იდენტიფიკაციის მეთოდის დროს, მონაცემთა ბაზის არსებობა თავისთავად წარმოადგენს უსაფრთხოების შედარებით დაბალ დონეს, რადგან არსებობს მონაცემთა არაკანონიერი გზით გამოყენების საფრთხე.

ვერიფიკაციის მეთოდი გულისხმობს ბიომეტრიული მონაცემების ავთენტურობის შემოწმებას მონაცემთა ბაზის გამოყენების გარეშე. კერძოდ, ბიომეტრიული მონაცემების შემცველ მატარებელზე (მაგალითად სამსახურებრივი ბარათი, რომელიც დამზადებულია კონკრეტული პირისათვის და შეიცავს აღნიშნული პიროვნების ბიომეტრიულ მონაცემს) დატანილ ბიომეტრიულ მონაცემს სისტემა ადარებს ბაზაში არსებულ, კონკრეტულად ამ ბარათის მფლობელის ბიომეტირულ მონაცემს. აღნიშნული მეთოდი მოიხსენიება სახელით ***ერთი-ერთთან***. ითვლება, რომ ვერიფიკაციის მეთოდი უფრო უსაფრთხოა, რადგან ის მონაცემთა ბაზა, რომლის საშუალებითაც ფუნქციონირებს სისტემა არ იძლევა კონკრეტულ მონაცემზე წვდომის საშუალებას, მასში არსებული ყოველი მონაცემი დაშიფრულია და აქტიურდება მხოლოდ მონაცემთა სუბიექტის მხრიდან ზემოთხსენებული მატარებლის გამოყენებისას. ამ მეთოდით ბიომეტრიული მონაცემების დამუშავება უფრო ძვირადღირებულია, ვიდრე იდენტიფიკაციის მეთოდით, თუმცა ის უზრუნველყოფს უსაფრთხოების უფრო მაღალ დონეს და საჭიროებს შესაბამის პროგრამულ მხარდაჭერას. ამასთან, ვერიფიკაციის დროს, პიროვნება თავად ფლობს საკუთარი ბიომეტრიული მონაცემების შემცველ მოწყობილობას (სამსახურებრივი ბარათი, ID ბარათი თუ სხვა), რაც ამცირებს მასზე არაავტორიზებულ წვდომის საფრთხეს.

V. უსაფრთხოების ზომები და მონაცემთა დამმუშავებლის ვალდებულებები

მონაცემთა დამმუშავებლის მხრიდან სრულად უნდა იქნას გააზრებული ბიომეტრიულ მონაცემთა დამუშავებისა და მათი უსაფრთხოების უზრუნველყოფის მნიშვნელობა. რეკომენდებულია, რომ დაწესებულების მხრიდან მოხდეს საჭიროებათა წინასწარი შეფასება და აღნიშნულის საფუძველზე განისაზღვროს ბიომეტრიულ მონაცემთა დამუშავებისა და დაცვის კონკრეტული მეთოდები და საშუალებები. დაწესებულების მიერ დეტალურად უნდა იქნას შეფასებული ბიომეტრიულ მონაცემთა დაცულობის უზრუნველსაყოფად საჭირო სამი კომპონენტი - **გარემო, მიზანი და ეფექტურობა.** მონაცემთა

დამმუშავებელი ვალდებულია, მიიღოს უსაფრთხოების ისეთი ზომები, რომლებიც მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური იქნება. პირი, რომელიც უშუალოდ მონაწილეობს მონაცემთა დამუშავებაში, ვალდებულია, არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს. ამასთანავე, პირი ვალდებულია, დაიცვას მონაცემთა საიდუმლოება, მათ შორის, მისი სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგაც.

ბიომეტრიულ მონაცემთა უსაფრთხოების დაცვის უზრუნველსაყოფად, მონაცემთა დამმუშავებელმა ობიექტურად უნდა განსაზღვროს არსებული გარემო, მიზანი და აქედან გამომდინარე შეარჩიოს უსაფრთხოების უზრუნველყოფის ეფექტური საშუალებები. კერძოდ, მონაცემთა დამმუშავებლის მხრიდან უნდა შეფასდეს:

- **გარემო**

მნიშვნელოვანია, რომ დაწესებულებამ ადეკვატურად შეაფასოს ის გარემო, რომელშიც გეგმავს ბიომეტრულ მონაცემთა დამუშავებას. მთავარი შეკითხვა, რომელსაც მონაცემთა დამმუშავებელმა უნდა გასცეს პასუხი არის ის, თუ **რამდენად აუცილებელია ამა თუ იმ გარემოსთვის ბიომეტრიული მონაცემების დამუშავება?**

- **მიზანი**

მონაცემთა დამმუშავებლის მხრიდან საჭიროა გაანალიზებულ იქნას ის მიზანი, რომლის მისაღწევადაც გეგმავს ბიომეტრიული მონაცემების დამუშავებას. პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის თანახმად, პირის უსაფრთხოების, საკუთრების დაცვის, აგრეთვე, საიდუმლო ინფორმაციის თავიდან აცილებისა და საქმიანობის განხორციელების მიზნისათვის, დაწესებულებას უფლება აქვს დაამუშაოს ბიომეტრიული მონაცემი, თუმცა მხედველობაში უნდა იქნას მიღებული მიზნის მისაღწევი ის საშუალება, რომელიც უზრუნველყოფს ნაკლებ ჩარევას პირის პირად ცხოვრებასა და პერსონალური მონაცემების დაცვის უფლებებში. მთავარი შეკითხვა, რომელსაც მონაცემთა დამმუშავებელმა უნდა გასცეს პასუხი: **შესაძლებელია თუ არა მიზნის მიღწევა სხვა საშუალებით?**

- **ეფექტურობა**

დაწესებულების მიერ, ბიომეტრიულ მონაცემთა დამუშავება ქმნის ამ მონაცემთა უსაფრთხოების ეფექტური ზომების დანერგვის აუცილებლობას. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლის თანახმად, მონაცემთა დამმუშავებელი ვალდებულია მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა

დაცვას შემთხვევით ან უკანონო განადგურებისგან, შეცვლისგან, გამჟღავნებისგან, მოპოვებისგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისგან. ამასთან ერთად, 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 ცვლილებასთან დაკავშირებული ყველა მოქმედების აღრიცხვა. მთავარი შეკითხვა, რომელსაც მონაცემთა დამმუშავებელმა პასუხი უნდა გასცეს: **რამდენად არის მზად დაწესებულება, უზრუნველყოს მონაცემთა ეფექტურად დაცვისათვის საჭირო ყველა ორგანიზაციულ-ტექნიკური ზომის მიღება?**

! პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მე-10 მუხლის მიხედვით, თუ კანონით სხვა რამ არ არის დადგენილი, ბიომეტრიულ მონაცემთა გამოყენებამდე მონაცემთა დამმუშავებელმა პერსონალურ მონაცემთა დაცვის ინსპექტორს უნდა მიაწოდოს იგივე ინფორმაცია, რომელიც მიეწოდება მონაცემთა სუბიექტს, კერძოდ, მონაცემთა დამუშავების მიზნისა და მონაცემთა დასაცავად მიღებული უსაფრთხოების ზომების შესახებ.

VI. მონაცემთა სუბიექტის უფლებები

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის თანახმად, მონაცემთა სუბიექტს აქვს **ინფორმაციის მიღების უფლება**. მონაცემთა სუბიექტს უფლება აქვს, მონაცემთა დამმუშავებელს მოსთხოვოს ინფორმაცია მის შესახებ მონაცემთა დამუშავების თაობაზე. კერძოდ, მონაცემთა დამმუშავებელი ვალდებულია მონაცემთა სუბიექტს მიაწოდოს შემდეგი სახის ინფორმაცია:

- რა ტიპის ბიომეტრული მონაცემები მუშავდება;
- ბიომეტრულ მონაცემთა დამუშავების მიზანი;
- ბიომეტრულ მონაცემთა დამუშავების სამართლებრივი საფუძველი;
- ბიომეტრულ მონაცემთა შეგროვების წყარო;
- ხდება თუ არა ბიომეტრულ მონაცემთა მესამე პირებზე გაცემა, გაცემის საფუძველი და მიზანი.

მონაცემთა სუბიექტს უფლება აქვს მონაცემთა დამმუშავებელს მოსთხოვოს **ინფორმაციის გასწორება, განახლება, დამატება, წაშლა ან განადგურება.** მონაცემთა დამმუშავებელი ვალდებულია, მონაცემთა სუბიექტის განცხადების საფუძველზე, 15 დღის ვადაში, მიიღოს შესაბამისი ზომები და აცნობოს მას მიღებული გადაწყვეტილების შესახებ.

პერსონალურ მონაცემთა დამუშავების ერთ-ერთი კანონიერი საფუძველია მონაცემთა სუბიექტის თანხმობა, რაც პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონით განმარტებულია, როგორც შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა განსაზღვრული მიზნით დამუშავებაზე ზეპირად, სატელეკომუნიკაციო ან სხვა შესაბამისი საშუალებით გამოხატული ნებაყოფლობითი თანხმობა, რომლითაც შესაძლებელია ნათლად დადგინდეს მონაცემთა სუბიექტის ნება. ამავე კანონის მე-6 მუხლის მიხედვით, განსაკუთრებული კატეგორიის მონაცემთა დამუშავებისათვის სავალდებულოა მონაცემთა სუბიექტის წერილობითი თანხმობა. მონაცემთა დამუშავებაზე მონაცემთა სუბიექტის თანხმობის არსებობასთან დაკავშირებით დავის წარმოშობის შემთხვევაში მონაცემთა დამმუშავებელს ეკისრება მონაცემთა სუბიექტის თანხმობის ფაქტის არსებობის მტკიცების ტვირთი.

მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, განმარტების გარეშე უარი განაცხადოს მის მიერვე მიცემულ თანხმობაზე და მოითხოვოს მონაცემთა დამუშავების შეწყვეტა ან/და დამუშავებულ მონაცემთა განადგურება. განცხადების წარდგენიდან 5 დღის ვადაში, მონაცემთა დამმუშავებელმა უნდა შეწყვიტოს მონაცემთა დამუშავება ან/და გაანადგუროს მონაცემები, თუ არ არსებობს მონაცემთა დამუშავების სხვა საფუძველი.

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მიხედვით, მონაცემთა სუბიექტს უფლება აქვს, უფლებების დარღვევის შემთხვევაში კანონით დადგენილი წესით მიმართოს პერსონალურ მონაცემთა დაცვის ინსპექტორს ან სასამართლოს, ხოლო თუ მონაცემთა დამმუშავებელი საჯარო დაწესებულებაა, საჩივრის წარდგენა შესაძლებელია ასევე იმავე ან ზემდგომ ადმინისტრაციულ ორგანოში. ასევე, მონაცემთა სუბიექტს უფლება აქვს, საქმის განმხილველ ორგანოს მოსთხოვოს მონაცემთა დაბლოკვა გადაწყვეტილების გამოტანამდე. მონაცემთა სუბიექტს უფლება აქვს, ზემდგომი ადმინისტრაციული ორგანოს ან პერსონალურ მონაცემთა დაცვის ინსპექტორის გადაწყვეტილება კანონით დადგენილი წესით გაასაჩივროს სასამართლოში.

ხშირად დასმული კითხვები ბიომეტრიულ მონაცემთა დამუშავებასთან დაკავშირებით

მსოფლიოში, რომელია ყველაზე ხშირად დამუშავებადი ბიომეტრიული მონაცემები?

- *ბიომეტრიული მონაცემებიდან პრაქტიკაში ყველაზე ხშირად მუშავდება თითის ანაბეჭდი,თვალის გარსი, ხმა, სახის მახასიათებლები, ხელწერა, „ხელის გეომეტრია“. ბიომეტრიულ მონაცემთა სხვა ვარიაციები, მეცნიერთა მიერ, გადიან ტესტირებისა და შეფასების ეტაპს*

შეუძლია თუ არა ადამიანს შეცვალოს თავისი ბიომეტრიული მონაცემი?

- *ბიომეტრიული მონაცემის შეცვლა ან შენიღბვა მიიღწევა დიდი ძალისხმევის ხარჯზე (გამოვლენილია თითის დამახინჯების ან ქირურგიული ჩარევით თითის ანაბეჭდის შეცვლის ცალკეული შემთხვევები). შესაძლებელია, აგრეთვე, შეცვლილ იქნას ქცევითი მახასიათებელი (სიარულისა და საუბრის მანერა, ა.შ.)*

განარჩევს თუ არა სისტემა ერთმანეთისაგან ტყუპების ბიომეტრიულ მონაცემებს?

- *მიუხედავად იმისა, რომ იდენტური ტყუპები თვალით არ განირჩევიან ერთმანეთისგან, მათ ფიზიკურ და ქცევით მახასიათებლებს შორის სხვაობა მარტივად დგინდება ბიომეტრიული სისტემებით*

რამდენად აგვარებს უსაფრთხოების პრობლემას ბიომეტრიული სისტემები?

- *ბიომეტრიული სისტემა წარმოადგენს მხოლოდ უსაფრთხოების საერთო სისტემის ნაწილს. ცალკე აღებული ბიომეტრიული სისტემა ვერ გადაჭრის უსაფრთხოების პრობლემას*

როგორია ბიომეტრიული სისტემების მუშაობის სპეციფიკა?

- *ბიომეტრიული სისტემების მუშაობა ეფუძნება 4 ნაბიჯს: მონაცემთა შეგროვება, ექსტრაქცია, შედარება, გადაწყვეტა. შეგროვების ეტაპზე სისტემა, სენსორის მეშვეობით, აფიქსირებს ბიომეტრიულ თვისებებს და გარდაქმნის მათ ციფრულ ფორმატში. ექსტრაქციის ეტაპი გარდაქმნის ციფრულ ფორმატში არსებულ მონაცემს*

კომპაქტურ ნიმუშად. შედარების ეტაპზე სისტემა ზომავს და ახდენს ნიმუშის შედარებას მონაცემთა ბაზაში არსებულ სხვა ნიმუშებთან. შედარების ეტაპზე დაფუძნებით, სისტემა იღებს გადაწყვეტილებას რამდენად შეესაბამება წარდგენილი ნიმუში სისტემაში არსებულ სხვა ნიმუშებს და იძლევა ფიზიკურ თუ ვირტუალურ სერვერებზე შეღწევის უფლებას

აღნიშნული რეკომენდაცია წარმოადგენს ზოგადი ხასიათის დოკუმენტს, რომელიც ვერ ჩაანაცვლებს პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონმდებლობას. კონკრეტული გარემოებებიდან გამომდინარე, იხილეთ არსებული საკითხის მარეგულირებელი ნორმატიული აქტები.