პერსონალურ მონაცემთა დაცვის თვალსაზრისით საჯარო სექტორში გავრცელებული 10 მთავარი სისუსტე

საჯარო დაწესებულებებში მონაცემთა დამუშავების სისტემების მონიტორინგის შედეგებზე დაყრდნობით

საქართველოში მონაცემთა დაცვის კანონმდებლობის იმპლემენტაციაზე აქტიური მუშაობა 2014 წლიდან დაიწყო, მას შემდეგ რაც პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი (ამჯამად სახელმწიფო ინსპექტორის სამსახური) რეალურად ამოქმედდა.

კანონის იმპლემენტაციის მიზნით საჯარო თუ კერძო ორგანიზაციებმა არაერთი აქტივობა განახროციელეს. 2014 წელს აქტიურად შეივსო და ინსპექტორის აპარატს წარედგინა ფაილური სისტემების კატალოგები, გადამზადდა და სპეციალური ტრენინგი გაიარა არაერთმა მოხელემ/დასაქმებულმა, რიგმა დაწესებულებებმა შეიმუშავეს შიდაორგანიზაციული დოკუმენტები, დანიშნეს პერსონალურ მონაცეთა დაცვის საკითხებზე პასუხისმგებელი პირები თუ სტრუქტურული ერთეულები.

შესაბამისად, დღეისათვის მონაცემთა დამმუშავებლებში მონაცემთა დაცვის კანონმდებლობის ცნობადობა ამაღლებულია, დაწესებულებები ცდილობენ თავიდან აცილონ ჯარიმა მონაცემთა დამუშავების წესების დარღვევისათვის, ფორმალურად მოაწესრიგონ მონაცემთა დამუშავების საფუძვლები, მოიპოვონ მონაცემთა სუბიექტის თანხმობა, შექმნან რიგი შიდაორგანიზაციული დოკუმენტები და ა.შ

თუმცა ისიც უნდა აღინიშნოს, რომ მსგავსი მიდგომა საკითხის მხოლოდ ფრაგმენტულ მოწესრიგებას ემსახურება და თემაში გარკვეული გარე დამკვირვებლებისთვის კვლავ რჩება გარკვეული სკეპტიციზმის საფუძველი, რადგან ჯერ კიდევ არ ჩანს დაწესებულების მიერ საკითხისადმი სისტემური მიდგომა, მოანცემთა დაცვის პრინციპების ჯეროვანი გააზრება და მონაცემთა დაცვის, როგორც ყოველდღიური საქმიანობის ერთ-ერთი მნიშნველოვანი ასპექტის დანერგვა მიმდინარე პროცესებში. ამის ნაცვლად ჩვენ ვხედავთ აღმოჩენილი/გამოვლენილი შედეგების გადაჭრის მცდელობას და არა შედეგების გამომწვევ მიზეზებთან საბრძოლველ თანმიმდევრულ ნაბიჯებს.

2019 წლის აპრილიდან - 2020 წლის აგვისტომდე მონაკვეთში ინოვაციებისა და რეფორმების ცენტრმა (IRC) განახორციელა მონაცემთა დამუშავების 20-ზე მეტი სისტემის მონიტორინგი იმის გასარკვევად თუ რამდენად სერიოზულად ეკიდებიან დაწესებულები მონაცემთა დაცვის საკითხს. მონიტორინგის ფარგლებში არსებული პრაქტიკა შემოწმდა როგორც მოქმედ კანონმდებლობასთან შესაბამისობის კუთხით, ისე საუკეთესო ქართული და ევროპული პრაქტიკის გათვალისწინებით.

მიღებული შედეგების გაანალიზების საფუძველზე შესაძლებელი გახდა გამოგვეყო საჯარო დაწესებულებების მიერ მონაცემთა დამუშავების პროცესში ყველაზე გავრცელებული და მნიშვნელოვანი 10 სისუსტე.

1. მონაცემთა დამუშავების სისტემების (პროცესებისა და საშუალებების) ინვენტარიზაცია

მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის უზრუნველსაყოფად ერთ-ერთი პირველი ნაბიჯი, რომელიც მონაცემთა დამმუშავებელმა უნდა გადადგას, არის მონაცემთა ინვენტარიზაცია ანუ იმის გაანალიზება თუ სად და რა მონაცემებს აგროვებს, იყენებს თუ სხვაგვარად ამუშავებს ორგანიზაცია.

მონაცემთა ინვენტარიზაცია გულისხმობს თითეული მონაცემისთვის იმის განსაზღვრას, თუ რა არის:

- ამ მონაცემის დამუშავების მიზანი,
- დამუშავების საფუძველი,
- ვინ არის ასეთი მონაცემების სუბიექტი,
- რა არის მონაცემების მიღების წყარო ანუ საიდან მოვიდა/შემოვიდა მონაცემები ორგანიზაციაში,
- ვინ არის პასუხისმგებელი მონაცემებზე
- ვის შეიძლება ჰქონდეს წვდომა მონაცემებზე
- მონაცემების შენახვის ფორმატი - ქაღალდი/ელექტრონული
- მონაცემთა ორგანიზაციის გარეთ გადაცემის შესაძლებლობა/შემთხვევები
- მონაცემთა შენახვის ვადა
- მონაცემთა წაშლის/განადგურების წესი
- ამ კონკრეტული მონაცემების დამუშავებასთან დაკავშირებით არსებობს თუ არა რამე მარეგულირებელი დოკუმენტაცია

როგორც ჩატარებული მონიტორინგის შედეგად გამოიკვეთა, შესწავლილი ორგანიზაციების უმეტესობას მონაცემთა დაცვის მიზნებისათვის მსგავსი ინვენტარიზაცია არ ჩატარებულა. შესაძლებელია, ზოგიერთ ორგანიზაციას, მისი სტრუქტურის, სიდიდისა და სიმწიფის დონიდან გამომდინარე ცალკეული პროცესებისთვის აქვს დამტკიცებული სტანდარტული წესები, შიდაორგანიზაციული თუ ანგარიშგების მიზნებისთვის აღრიცხავს მასთან შესულ და გასულ კორეპონდენციას და ა.შ., მასთან არსებულ აქტივებს ინახავს დადგენილი წესით, თუმცა არცეთი აღნიშნული ღონისძიება არ არის გატარებული პერსონალურ მონაცემთა ინვენტარიზაციის მიზნებისთვის და არცერთი მსგავსი ღონისძიების გატარებისათვის გათვალისწინებული არ არის მონაცემთა დაცვის სპეციფიკა, რაც, თავის მხრივ, მონაცემთა

დაცვის სტანდარტს დაბლა სწევს და კანონმდებობასთან შესაბამისობის სათანადო დონეს ვერ უზრუნველყოფს.

2. მონაცემთა დამუშავების სისტემების ამოქმედებამდე მონაცემთა დამუშავების ზეგავლენისა და რისკების წინასწარი შეფასება (DPIA)

იმისთვის, რომ მონაცემთა უსაფრთხოებისათვის ადეკვატური ზომები იქნას მიღებული და მონაცემთა დამმუშავებელმა რეალურად შეასრულოს კანონით დაკისრებული ვალდებულებები, აუცილებელია მონაცემთა ამა თუ იმ ფორმით დამუშავების დაწყებამდე მან წინასწარ შეაფასოს მონაცემთა დამუშავებით გამოწვეული რისკები და მისი გავლენა ადამიანის ძირითად უფლებებზე. განსაკუთრებით მაშინ, თუ მონაცემთა კატეგორიის, მოცულობის მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, ამ უფლებებს მაღალი ალბათობით ექმნება გარკვეული საფრთხე.

რისკებზე დაფუძნებული მიდგომის თანახმად, ზეგავლენის შეფასების ჩატარება საჭიროა თუ მუშავდება დიდი რაოდენობით მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემები, ხორციელდება ქცევის სისტემატური და მასშტაბური მონიტორინგი, ადამიანისთვის არსებითად მნიშვნელოვანი შედეგი დგება პროფილირების საუფძველზე და ა.შ.

მიუხედავად იმისა, რომ აღნიშნულ ვალდებულებას მოქმედი კანონმდებლობა არ ითვალისწინებს, ის ევროპაში ფართოდ გავრცელებული პრაქტიკაა და საქართველოს პარლამენტში ინიცირებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტიც აწესებს მსგავს მიდგომას.

მონიტორინგის ჩატარების პროცესში გამოვლინდა, რომ არცერთ დაწესებულებას არ აქვს ჩატარებული მონაცემთა დამუშავების ზეგავლენა და არ აქვს იდენტიფიცირებული ის რისკები და მათთან გამკლავების გზები, რომელიც მონაცემთა ამა თუ იმ ფორმით დამუშავებას ახლავს თან. აღნიშნული მეტად საგულისხმოა იმ სისტემებთან მიმართებით, რომლებიც დაინიცირდა და ამოქმედდა სულ ცოტა ხნის წინ, მაშინ, როდესაც მონაცემთა დაცვის შედარებით ახალი კონცეპტებიც აღარ არის უცხო და ხელმიუწვდომელი მონაცემთა მსხვილი დამმუშავებლებისთვის. მონიტორინგის ფარგლებში მხოლოდ ერთ, EHR სისტემასთან მიმართებით აღნიშნა საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრომ, რომ მათ მსგავსი შეფასება ჩატარებული ჰქონდათ, თუმცა „ეს ყველაფერი არ არის ფორმალიზებული დოკუმენტის დონეზე, რადგან სადღეისოდ სამინისტროს არ ჰყავს ინფორმაციული უსაფრთხოების მენეჯერი“.

მსგავსი მიდგომა ვერ ჩაითვლება გატარებულ რეალურ ზომად და კანონთან თუ კარგ პრაქტიკასთან შესაბამის ღონისძიებად, რადგან შეუძლებელია მონაცემთა დამმუშავებელმა სისტემურად და სიღრმისეულად შეაფასოს მონაცემთა დამუშავების პროცესი, დეტალურად შეაფასოს მოსალოდნელი რისკები და მათი აღრიცხვისა და დოკუმენტირების გარეშე შექმნას მათზე რეაგირების ადეკვატური მექანიზმები, რადგანაც მონაცემთა დაცვა, მათი უსაფრთხოება და არსებულ რისკებზე რეაგირების მექანიზმები - ორგანიზაციულ-ტექნიკური ზომები არ შეიძლება იყოს ერთჯერადი და იმისთვის რომ ისინი იყოს ქმედითი, ეს აუცილებლად განგრძნობით პროცესს გულისხმობს.

შესაბამისად, მსგავსი მოცულობის და მნიშვნელობის სისტემის შექმნის, დანერგვისა და გაშვების დროს, მნიშვნელოვანია წინასწარ იქნას მოძიებული და გამოყოფილი ადეკვატური ფინანსური თუ ადამიანური რესურსი.

3. მონაცემთა დამუშავების არსებული პრაქტიკის შეფასება პერსონალურ მონაცემთა დაცვის კანონმდებლობის ჭრილში

მონიტორინგის ჩატარებისას მკაფიოდ გამომჟღავნდა ის გარემოება, რომ მონაცემთა დამმუშავებლების მიდგომა მონაცემთა დაცვის საკითხისადმი ძალიან ზედაპირული და ფრაგმენტულია. მიუხედავად იმისა, რომ ზოგიერთ უწყებას/დამმუშავებელს შექმნილი და დამტკიცებული აქვს მონაცემთა დაცვის პოლიტიკა თუ მონაცემთა დამუშავების მარეგულირებელი შიდაორგანიზაციული წესები, ისინი არ არის საკმარისად დეტალიზებული და მორგებული უწყებაში მონაცემთა დამუშავების კონკრეტულ შემთხვევებზე. მონაცემთა დამუშავების ძირითადი სისტემები მონაცემთა დაცვის კანონმდებლობის შემოღებამდეა შემუშავებული, შესაბამისად, არც აღნიშნულ სისტემებში და არც მონაცემთა დამუშვების დამკვიდრებულ პრაქტიკაში მონაცემთა დაცვის საკითხები იმთავითვე გათვალისწინებული არ არის. არ გამოვლენილა არცერთი შემთხვევა, როდესაც მონაცემთა დამუშავების დადგენილი პრაქტიკა რამე ფორმით გადაიხედა და/ან შეიცვალა პერსონალურ მონაცემთა დაცვის კანონის მოთხოვნების გათვალისწინებით.

4. მონაცემთა დამუშავების მიზნებისა და საფუძვლების იდენტიფიცირება და დოკუმენტირება

მონიტორინგის ფარგლებში ძირითადად ყურადღება გამახვილებული იყო საჯარო უწყებებზე, რომლებიც საკუთარი, კანონით განსაზღვრული უფლებამოსილებების განხორციელების ფარგლებში ამუშავებენ დიდი ოდენობით პერსონალურ, მათ შორის განსაკუთრებული კატეგორიის მონაცემებს. აღნიშნული თავისებურებიდან გამომდინარე,

შემომწებულ სისტემებთან მიმართებით, როგორც წესი, მონაცემთა დამუშავებისთვის ზოგადი მიზანი და საფუძველი არსებობს და მონაცემთა დამუშავებაც, მეტწილად, კანონშესაბამისია. თუმცა პრობლემა იჩენს თავს მიზნებისა და საფუძვლების დაკონკრეტების ნაწილში. არცერთ შემოწმებულ უწყებას დეტალურად არ აქვს იდენტიფიცირებული და დოკუმენტირებული მონაცემთა დამუშავების კონკრეტული მიზნები და საფუძვლები და მონაცემთა მოცულობა მათ მიმართ კრიტიკულად არ არის გაანალიზებული. პერსონალურ მონაცემთა დაცვის კანონმდებლობა კი სწორედ მსგავს კონკრეტიკას მოითხოვს. მონაცემები შეიძლება დამუშავდეს მხოლოდ მკაფიოდ განსაზღვრული კანონიერი მიზნის მისაღწევად, მხოლოდ იმ მოცულობით, რაც აუცილებელია აღნიშნული მიზნის მისაღწევად და მხოლოდ იმ შემთხვევაში თუ მონაცემთა დამუშავების თითოეული ეპიზოდისათვის (შეგროვება, გამოყენება, შენახვა, გადაცემა და ა.შ.) არსებობს კანონით გათვალისწინებული ერთი საფუძველი მაინც. ამიტომ, იმისათვის რომ მონაცემთა დამუშავება სრულ შესაბამისობაში იყოს კანონმდებლობასთან და მონაცემთა დამმუშავებელმა შეძლოს აღნიშნულის დემონსტრირება, აუცილებელია მას დეტალურად ჰქონდეს შეფასებული და იდენტიფიცირებული მონაცემთა დამუშავების მიზანი და საფუძველი მონაცემთა თითოეული ერთეულისათვის და მოახდინოს აღნიშნულის ასახვა შესაბამის დოკუმენტაციაში.

5. მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის ურთიერთობის რეგლამენტაცია კანონმდებლობის მოთხოვნათა შესაბამისად

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ადგენს მინიმალურ წესებს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ურთიერთობებისათვის. კანონმდებლობის თანახმად უფლებამოსილმა პირმა შეიძლება დაამუშაოს მონაცემები სამართლებრივი აქტის ან მონაცემთა დამმუშავებელთან დადებული წერილობითი ხელშეკრულების საფუძველზე, რომელიც უნდა შეესაბამებოდეს და ითვალისწინებდეს კანონის მოთხოვნებს, წესებსა და აკრძალვებს. ხოლო მონაცემთა დამმუშავებელი ვალდებულია დარწმუნდეს აღნიშნული წესების დაცვასა და უფლებამოსილი პირის მიერ მონაცემთა უსაფრთხოებისათვის სათანადო ზომების მიღების ფაქტში. მონაცემთა დამმუშავებლის ეს ვალდებულება იმ ფაქტიდან გამომდინარეობს, რომ მონაცემთა დამუშავებაზე და კანონის მოთხოვნების დაცვაზე კვლავ მონაცემთა დამმუშავებელია პასუხისმგებელი, მიუხედავად იმისა, რომ ფაქტობრივად მონაცემებთან შეხება უფლებამოსილ პირს აქვს.

მონიტორინგის ფარგლებში გამოიკვეთა, რომ ურთიერთობები მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის არასათანადოდ არის მოწესრიგებული. რიგ შემთხვევებში საერთოდ არ არსებობს ურთიერთობების მომწესრიგებელი რამე დოკუმენტი ან, თუ არსებობს,

ისინი ზოგადი და ბუნდოვანი ხასიათისაა და არ ითვალისწინებს კანონის მოთხოვნებს. ამგვარი ხელშეკრულებებით/მემორანდუმებით არ არის გათვალისწინებული კანონით დადგენილი წესები, მონაცემთა უსაფრთხოების სათანადო ზომები, მონაცემთა დამმუშავებლის მიერ პროცესის მონიტორინგის ეფექტიანი მექანიზმები და ა.შ.

6. მონაცემთა დამუშავების ვადების განსაზღვრა

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მე-4 მუხლის თანახმად მონაცემები უნდა დამუშავდეს მხოლოდ იმ ვადით, რაც აუცილებელია მონაცემთა დამუშავების მიზნების მისაღწევად. მიზნის მიღწევის შემდეგ მონაცემები უნდა წაიშლოს/განადგურდეს.

ჩატარებული მონიტორინგის ფარგლებში დადგინდა, უმეტესი მონაცემებისა და სისტემებისათვის არ არის განსაზღვრული კონკრეტული, კანონიერ მიზანთან შესაბამისი ვადები. ასევე, არ არსებობს მონაცემთა განდაგურებისა თუ დაარქივების სათანადო წესები. უმეტეს შემთხვევაში არ აქვთ დადგენილი მონაცემთა შენახვის/დაარქივების კონკრეტული ვადები ან არარელევანტურად ფართო დიაპაზონი აქვთ განსაზღვრული მონაცემთა შენახვისათვის (მაგ. 1 თვიდან 3 წლამდე ვადით).

ამგვარი მიდგომები, ერთი მხრივ, მოწმობს იმას, რომ ამა თუ იმ სისტემის დანერგვისას არ არის შეფასებული და გაანალიზებული მასში დამუშავებული თითოეული მონაცემის დამუშავების მიზანი და არ არის განსაზღვრული მიზნის ადეკვატური შენახვის ვადა. ასევე, პრობლემურია ის საკითხიც, რომ მონაცემთა სუბიექტისათვის არ არის განჭვრეტადი მის შესახებ რომელი მონაცემი რა ვადით შეიძლება იქნას შენახული.

ასევე, შესაძლებელია ცალკეულ შემთხვევებში არსებობდეს მონაცემთა დიდი ვადით ან უვადოდ შენახვის საჭიროება, თუმცა მსგავს შემთხვევაში იდენტიფიცირებული უნდა იყოს კონკრეტული საჭიროება, მონაცემთა დამუშავების საჭიროების მიზნიდან გამომდინარე კონკრეტული ვადები და მონაცემთა შენახვისა თუ განადგურების კონკრეტული წესები. თითოეული მონაცემის დამუშავების აუცილებლობის შეფასების შემდგომ, უნდა გაიმიჯნოს, რომელი მონაცემები საჭიროებს ხანგრძლივი ვადით (ან მუდმივად) შენახვას და რომელი არა.

მონაცემთა ყოველი კონკრეტული წყებისათვის კრიტიკულად უნდა შეფასდეს საჭიროა თუ არა მისი შენახვა, არსებობს თუ არა რამე ლეგიტიმური მიზანი მონაცემთა შემდგომი დამუშავებისათვის და მხოლოდ ასე იქნას მიღებული გადაწყვეტილებები.

აღნიშნული ინფორმაცია ადვილად ხელმისაწვდომი უნდა იყოს მონაცემთა სუბიექტისთვისაც.

7. მონაცემთა სუბიექტის უფლებების რეალიზაციის მექანიზმების არსებობა

მონაცემთა დაცვის ფილოსოფიის ერთ-ერთი საკვანძო საკითხია მონაცემთა სუბიექტი, როგორც მონაცემთა დამუშავების ცენტრალური ფიგურა. კანონმდებლობა მრავალ ისეთ მექანიზმსა და ვალდებულებას განსაზღვრავს მონაცემთა დამმუშავებლის მხარეს, რომელიც მონაცემთა სუბიექტის უფლებების განმტკიცებას და მის მიერ საკუთარ მონაცემებზე კონტროლის შენარჩუნებას ემსახურება. კანონმდებლობა მონაცემთა დამმუშავებელს ავალდებულებს კონკრეტული ზომების მიღებას და მონაცემთა სუბიექტის უფლების სათანადო რეალიზების ხელშეწყობას.

მონიტორინგის შედეგად დადგინდა, რომ უმეტეს შემთხვევაში პრობლემურია მონაცემთა სუბიექტის უფლების რეალიზების მექანიზმები, რაც გამოიხატება არა იმდენად კონკრეტულ ფაქტებში, როდესაც სუბიექტს შეეზღუდა მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული უფლებები, არამედ სისტემურ სურათში, როდესაც ეფექტიანი მექანიზმების არარსებობა, მონაცემთა წვდომების არასათანადო აღრიცხვა და ა.შ. ქმნის საფრთხეს მონაცემთა სუბიექტის მოთხოვნა ვერ დაკმაყოფილდეს ან მხოლოდ ნაწილობრივ დაკმაყოფილდეს.

8. პერსონალურ მონაცემთა დაცვისკენ მიმართული ორგანიზაციულ-ტექნიკური ზომები

მოქმედი კანონმდებლობა მონაცემთა უსაფრთხოების საკითხს მხოლოდ ერთ მუხლს უთმობს და საკმაოდ ზოგად ფორმულირებას გვთავაზობს - 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 შემთხვევი თი ან უკანონო დაკარგვისაგან... ასევე, მონაცემთა უსაფრთხოებისათვის მიღებული ზომები მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური უნდა იყოს.

ამგვარი ფორმულირება, ერთი მხრივ, ბუნდოვანია და ხშირად მონაცემთა დამმუშავებლებს უჭირთ იმის ზუსტად განსაზღვრა, თუ რა კონკრეტული ზომები იქნება მათ მიერ დამუშავებულ მონაცემებთან დაკავშირებული რისკების ადეკვატური. ხოლო, მეორე მხრივ, მონაცემთა დამმუშავებლებს უქმნის უსაფუძვლო განცდას, თითქოს სათანადოდ ასრულებენ კანონის მოთხოვნებს და მათ მიერ მონაცემთა დამუშავება შესაბამისობაშია კანონმდებლობასთან.

რეალურად კი, კარგი პრაქტიკის, ევროპული რეგულაციისა და ქართულ კანონმდებლობაში ინიცირებული ცვლილებების საფუძველზე შეიძლება ჩამოვთვალოთ ის მინიმალური ზომები, რომლებიც აუცილებლად უნდა მიიღოს მონაცემთა დამმუშავებელმა მონაცემთა უსაფრთხოების უზრუნველსაყოფად და რომელთა არარსებობის შემთხვევაში, შეუძლებელია მონაცემთა დაცულობაზე საუბარი, მიუხედავად იმისა, კონკრეტული დარღვევა/შემთხვევა დადგება თუ არა.

ასეთი ზომებია, მაგალითად:

- შესაბამისი პოლიტიკის დოკუმენტები
- მონაცემთა ინვენტარიზაცია
- მონაცემთა დამუშავების ზეგავლენის შეფასება (DPIA)
- მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში („Privacy by Design“) და მონაცემთა დაცვა პირველად პარამეტრად („Privacy by Default“)
- ფსევდონომიზაცია, მონაცემებთან წვდომის აღრიცხვა, მონაცემთა ლოგირება
- მონაცემთა დაცვის ოფიცერი
- მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა

მონაცემთა უსაფრთხოების უზრუნველსაყოფად აუცილებელი ორგანიზაციულ-ტექნიკური ზომების განსაზღვრისას დამმუშავებელმა და უფლებამოსილმა პირმა უნდა გაითვალისწინონ მონაცემთა კატეგორიები, მოცულობა, მონაცემთა დამუშავების მიზანი, ფორმა, საშუალებები და მონაცემთა სუბიექტის უფლებების დარღვევის შესაძლო საფრთხეები, ასევე, პერიოდულად შეაფასონ მონაცემთა უსაფრთხოების უზრუნველყოფის მიზნით მიღებული ტექნიკური და ორგანიზაციული ზომების ეფექტიანობა და საჭიროების შემთხვევაში, უზრუნველყონ მონაცემთა უსაფრთხოების დაცვისათვის ადეკვატური ზომების მიღება ან/და არსებულის განახლება.

ჩატარებული მონიტორინგის შედეგად დადგინდა, რომ მონაცემთა დამმუშავებლების უმეტესობას მონაცემთა უსაფრთხოებისათვის არ აქვს სათანადო და კომპლექსური ზომები მიღებული. საჯარო უწყებების მიერ მიღებული უსაფრთხოების ზომები ნაკარნახებია არა მონაცემთა დაცვის სპეციფიკიდან და საჭიროებებიდან გამომდინარე, არამედ ზოგადად დაწესებულებაში სხვა მონაცემებისა თუ ფასეულობის უსაფრთხოების დაცვით.

უწყებებს ძირითადად მიღებულია აქვთ ისეთი ზომები, როგორიცაა მაგ. სისტემებთან დაშვების ავტორიზაცია, თუმცა ავტორიზაციის წესები და სტანდარტები ყოველთვის არ არის სისტემაში არსებული მონაცემების სენსიტიურობის ადეკვატური. ასევე, ხშირ შემთხვევაში არ არსებობს მომხმარებლისა და პაროლების მართვის მომწესრიგებელი დოკუმენტი, რაც

დამატებით საფრთხეს ქმნის მონაცემების გაჟონვისა და მათზე არასანქცირებული წვდომის თვალსაზრისით.

ასევე, მონაცემთა უსაფრთხოებისათვის მიღებულ ზომებში შეიძლება ჩაითვალოს ფიზიკური უსაფრთხოებაც, თუმცა, როგორც უკვე აღინიშნა, ერთი მხრივ, ეს გულისხმობს ზოგად სტანდარტს შენობაში უსაფრთხოებისა დასაცავად და არ არის გათვალისწინებული მონაცემთა დაცვის თვალსაზრისით სენსიტიური არეები და, მეორე მხრივ, ფიზიკური უსაფრთხოება, როგორც წესი მიემართება გარედან მომავალ საფრთხეს და ვერ იცავს ორგანიზაციას ე.წ. ინსაიდერული რისკებისაგან.

მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული მონაცემთა უსაფრთხოების უზრუნველსაყოფად მისაღები ორგანიზაციული და ტექნიკური ზომები უწყებების მიერ ძალიან ფრაგმენტულად არის მიღებული. ზოგიერთ უწყებაში გათვალისწინებულია მონაცემთა ბაზებზე წვდომის ავტორიზაცია, ზოგიერთი დამმუშავებელი ახდენს მონაცემთა მიმართ შესრულებული ქმედებების ლოგირებას და ა.შ, თუმცა არცერთ უწყებაში არ აქვს ადგილი სიტუაციის დეტალურ ანალიზს, სათანადო შეფასებას და დამუშავებული მონაცემების ადეკვატური ზომების მიღებას.

9. როლებისა და პასუხისმგებლობების განსაზღვრა პერსონალურ მონაცემთა დაცვის სფეროში

როგორც უკვე აღინიშნა, მონაცემთა უსაფრთხოებისათვის მისაღები ერთ-ერთი ადეკვატური ზომაა პერსონალურ მონაცემთა მიმართ უწყების შიგნით კონკრეტული როლებისა და პასუხისმგებლობების განსაზღვრა. იმის გარკვევა, საკუთარი უფლებამოსილებებიდან გამომდინარე ვის რა მონაცემებზე სჭრიდება წვდომა და რა ფარგლებით. საკმარისი არ არის მონაცემთა დამუშავების კანონიერი საფუძვლის მოძიება და შესაბამისი საფუძვლის არსებობის გარეშე მონაცემთა არგაცემა. მონაცემთა სათანადოდ დასაცავად აუცილებელია, სისტემის შიგნითაც იყოს განაწილებული როლები და უფლებამოსილებების ფარგლები.

მონიტორინგის შედეგად გამოიკვეთა, რომ უმეტეს სისტემებში პერსონალურ მონაცემებზე წვდომის საკითხები არ აქვს დოკუმენტირებული ედა შესაბამისად რეგლამენტირებული. პრაქტიკულად სისტემბში არსებობს მომხმარებელთა განსხვავებული ტიპები, თუმცა არ არსებობს დოკუმენტი, რომელიც დაადგენს რომელ თანამშრომელს რომელი უფლებამოსილების ფაგლებში რა მონაცემებზე შეიძლება ჰქონდეს წვდომა და რა მოქმედებების განხორციელება შეუძლია ამ წვდომის ფარგლებში. მსგავსი მიდგომა კი ზრდის მონაცემებზე არასანქცირებული წვდომის, გადაჭარებებული დამუშავებისა და გაჟონვის შედარებით მაღალ რისკებს.

10. ადამიანური რესურსის მომზადების დონე/სისტემური მიდგომა

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ძალაში შესვლისა და ინსპექტორის სამსახურის (ყოფილი პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი) ამოქმედების შემდეგ, სამსახური რეგულარულ ტრენინგებს სთავაზობს სხვადასხვა დაინტერესებულ პირებს. ასევე, მრავალი სასწავლო ცენტრის სწავლების გეგმაშია გათვალისწიენბული პერსონალურ მონაცემთა დაცვის საკითხები.

მიუხედავად იმისა, რომ ასეთი ზოგადი ხასიათის ტრენინგები თითქმის ყველა უწყებაში ტარდება და/ან ჩატარებულა, ის ვერ იქნება მიჩნეული უწყების მიერ სისტემური მიდგომი ნაწილად და თანამშრომელთა სათანადო გადამზადებად.

ადამიანებს, რომელბსაც მუდმივად აქვთ შეხება პერსონალურ მონაცემებთან და რომლებისთვისაც პერსონალური, მათ შორის განსაკუთრებული კატეგორიის მონაცემების დამშავება ყოველდღიური საქმიანობის ნაწილს წარმოადგენს, მნიშვნელოვანია კარგად ჰქონდეთ გაცნობიერებული პერსონალურ მონაცემთა დაცვის მნიშნველობა, მონაცემთა დამუშავების პრინციპები, საკუთარი უფლება-მოვალეობები და მონაცემთა დაცვასთან დაკავშირებული სხვა საკითხები.

ამისთვის მნიშნველოვანია ორგანიზაციის/უწყების შიგნით არსებობდეს პერსონალურ მონაცემთა დამუშავების კონკრეტული გზამკვლევები და სასწავლო გეგმები, რომლებშიც გათვალისწინებული იქნება სამსახურის სპეციფიკა და მონაცემთა დაცვის ზოგადი პრინციპები თუ დებულებები „გადმოთარგმნილი“ და მორგებული იქნება თანამშრომლის ყოველდღიურ საქმიანობაზე.

მონიტორინგის შედეგად ირკვევა, რომ ამგვარი სპეციალიზებული სასწავლო კურსები/მასალები არცერთ უწყებაში არ არსებობს და არც თანამშრომელთა სავალდებულო გადამზადების ნაწილს წარმოადგენს.