სახელმძღვანელო რეკომენდაცია **4/2019**
25-ე მუხლის შესახებ

მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას

ვერსია 2.0

მიღებულია 2020 წლის 20 ოქტომბერს

წინამდებარე სახელმძღვანელო რეკომენდაციის თარგმანი მომზადდა გერმანიის საერთაშორისო თანამშრომლობის საზოგადოების (GIZ) საჯარო მმართველობის აღმოსავლეთ პარტნიორობის რეგიონული ფონდის პროექტის ფარგლებში და წარმოადგენს არაოფიციალურ თარგმანს.

ვერსიების შესახებ

ვერსია 1.0	2019 წლის 13 ნოემბერი	სახელმძღვანელო პრინციპების მიღება და საჯარო კონსულტაციების გამართვა
ვერსია 2.0	2020 წლის 20 ოქტომბერი	სახელმძღვანელო პრინციპების მიღება EDPB-ის მიერ, საჯარო კონსულტაციების შემდგომ

სარჩევი

ევროპის მონაცემთა დაცვის საბჭო:

ითვალისწინებს რა, ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაციას (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ, რომელიც აუქმებს 95/46/EC დირექტივას (შემდგომში, "GDPR"), კერძოდ, მის 70(1e) მუხლს;

ითვალისწინებს რა ევროპის ეკონომიკური ზონის შესახებ (EEA) შეთანხმებას, კერძოდ, მის XI დანართსა და 37-ე პროტოკოლს, რომელიც შესწორებულია EEA ერთობლივი კომიტეტის 2018 წლის 6 ივლისის N154/2018 გადაწყვეტილებით;

ითვალისწინებს რა საკუთარი რეგლამენტის მე-12 და 22-ე მუხლებს;

ამტკიცებს ქვემოთ წარმოდგენილ სახელმძღვანელო პრინციპებს.

რეზიუმე

ციფრული ტექნოლოგიების მზარდი გამოყენების პირობებში, საზოგადოებაში პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის უზრუნველსაყოფად მნიშვნელოვან როლს ასრულებს იმ მოთხოვნების შესრულება, რომლებიც უკავშირდება მონაცემთა დაცვის სტანდარტების გათვალისწინებას ახალი პროდუქტის ან მომსახურების შექმნის პროცესში და მონაცემთა დაცვას პირველად პარამეტრად (Data Protection by Design and by Default, შემდგომში „DPbDD").

წინამდებარე სახელმძღვანელო პრინციპები შეიცავს ზოგად მითითებებს DPbDD ვალდებულებასთან დაკავშირებით, რომელსაც ითვალისწინებს GDPR რეგულაციის 25-ე მუხლი. DPbDD არის ვალდებულება, რომელიც ვრცელდება ყველა დამუშავებისთვის პასუხისმგებელ პირზე, მისი მასშტაბისა და დამუშავების კომპლექსურობის მიუხედავად. DPbDD მოთხოვნების განხორციელების კუთხით, უაღრესად მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელ პირს ესმოდეს მონაცემთა დაცვის პრინციპები და მონაცემთა სუბიექტის უფლებები და თავისუფლებები.

ძირითად ვალდებულებას წარმოადგენს სათანადო ზომებისა და აუცილებელი დაცვის მექანიზმების განხორციელება, რათა უზრუნველყოფილი იქნეს მონაცემთა დაცვის პრინციპების ეფექტური იმპლემენტაცია და შესაბამისად, მონაცემთა სუბიექტის უფლებები და თავისუფლებები, ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა სტანდარტების დანერგვისა და მონაცემთა დაცვის პირველად პარამეტრად გათვალისწინების შედეგად. 25-ე მუხლი ადგენს ელემენტებს, რომლებიც დაკავშირებულია პრინციპებთან „მონაცემთა დაცვის სტანდარტების ახალი პროდუქტის ან მომსახურების შექმნის პროცესში გათვალისწინება" და „მონაცემთა

დაცვა პირველად პარამეტრად“. ეს ელემენტები, რომლებიც მხედველობაში უნდა იქნეს მიღებული დამუშავებისთვის პასუხისმგებელი პირის მიერ, დეტალურად არის განხილული წინამდებარე სახელმძღვანელო პრინციპებში.

25(1) მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა DPbDD უნდა გაითვალისწინოს ადრეული ეტაპიდანვე, დამუშავების ახალი ოპერაციის დაგეგმვის პროცესში. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია DPbDD განახორციელოს დამუშავებამდე და გააგრძელოს მისი უწყვეტად განხორციელება დამუშავების დროს. კერძოდ, მან რეგულარულად უნდა შეაფასოს არჩეული ღონისძიებებისა და დაცვის ღონისძიებების ეფექტურობა. DPbDD, აგრეთვე, ვრცელდება არსებულ სისტემებზე, რომლებიც პერსონალურ მონაცემებს ამუშავებენ.

სახელმძღვანელო პრინციპები, აგრეთვე, შეიცავს მითითებებს იმასთან დაკავშირებით, თუ როგორ უნდა განხორციელდეს მე-5 მუხლში წარმოდგენილი მონაცემთა დაცვის პრინციპები. კერძოდ, მასში ჩამოთვლილია DPbDD ელემენტები და პრაქტიკული მაგალითები საილუსტრაციოდ. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაითვალისწინოს შემოთავაზებული ზომების მიზანშეწონილობა კონკრეტული დამუშავების კონტექსტში.

ევროპის მონაცემთა დაცვის საბჭო (EDPB) უზრუნველყოფს რეკომენდაციებს იმის შესახებ, თუ როგორ უნდა ითანამშრომლონ დამუშავებისთვის პასუხისმგებელმა პირებმა, დამუშავებაზე უფლებამოსილმა პირებმა და მწარმოებლებმა DPbDD პრინციპების დანერგვისთვის. იგი წარმოების სფეროში მომუშავე დამუშავებისთვის პასუხისმგებელ პირებს, უფლებამოსილ პირებსა და მწარმოებლებს ურჩევს, გამოიყენონ DPbDD, როგორც კონკურენტული უპირატესობის მოპოვების შესაძლებლობა, თავიანთი პროდუქტების დამუშავებისთვის პასუხისმგებელი პირებისა და მონაცემთა სუბიექტების წინაშე რეკლამირებისას. იგი დამუშავებისთვის პასუხისმგებელ პირებს აგრეთვე, სთავაზობს, გამოიყენონ სერტიფიკაციები და ქცევის კოდექსები.

1. მოქმედების არეალი

1. სახელმძღვანელო პრინციპები ეხება დამუშავებისთვის პასუხისმგებელი პირების მიერ DPbDD პრინციპების განხორციელებას, GDPR-ის 25-ე მუხლით გათვალისწინებული ვალდებულების საფუძველზე.[1] წინამდებარე სახელმძღვანელო პრინციპები, შესაძლოა, აგრეთვე, სასარგებლო აღმოჩნდეს სხვა აქტორებისთვის, როგორებიც არიან დამუშავებაზე უფლებამოსილი პირები და პროდუქტების, სერვისებისა და აპლიკაციების მწარმოებლები (შემდგომში,

[1] წინამდებარე დოკუმენტში წარმოდგენილი ინტერპრეტაციები ეხება (EU) 2016/680 დირექტივის მე-20 მუხლს და 2018/1725 რეგულაციის 27-ე მუხლს.

„მწარმოებლები“), რომლებზეც პირდაპირ არ ვრცელდება 25-ე მუხლი, რათა მათ შექმნან GDPR-ის მოთხოვნებთან შესაბამისი პროდუქტები და სერვისები, რომლებიც დამუშავებისთვის პასუხისმგებელ პირებს მისცემს საშუალებას, შეასრულონ მონაცემთა დაცვის ვალდებულებები.[2] GDPR-ის პრეამბულის 78-ე პუნქტის თანახმად, DPbDD გათვალისწინებული უნდა იქნეს სახელმწიფო შესყიდვების კონტექსტში. მიუხედავად იმისა, რომ ყველა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მოახდინოს DPbDD-ის ინტეგრირება დამუშავებასთან დაკავშირებულ აქტივობებში, ეს პუნქტი ხელს უწყობს მონაცემთა დაცვის პრინციპების დანერგვას, ვინაიდან საჯარო უწყებები სხვებისთვის იქნებიან მაგალითის მიმცემნი. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, დამუშავების პროცესში უზრუნველყოს DPbDD ვალდებულებების შესრულება, დამუშავებაზე უფლებამოსილი პირებისა და ქვე-უფლებამოსილი პირების მიერ განხორციელებული დამუშავების პროცესში. შესაბამისად, მათ აღნიშნული უნდა გაითვალისწინონ ამ მხარეებთან ხელშეკრულების გაფორმებისას.

2. 25-ე მუხლით გათვალისწინებული მოთხოვნის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ მონაცემთა დაცვის სტანდარტების ინტეგრირება პერსონალური მონაცემების დამუშავების პროცესში (designed into the processing of personal data) და მათი გათვალისწინება პირველად პარამეტრად (as a default setting), დამუშავების განმავლობაში. DPbDD მოთხოვნები, აგრეთვე, ვრცელდება დამუშავების სისტემებზე, რომლებიც არსებობდა GDPR-ის ძალაში შესვლამდე. დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ დამუშავების მუდმივად განახლება GDPR-ის შესაბამისად. არსებული სისტემის DPbDD მოთხოვნებთან შესაბამისობის უზრუნველყოფასთან დაკავშირებით, იხ. 2.1.4 ქვეთავი. დებულების არსი მდგომარეობს მონაცემთა დაცვის *ახალი პროდუქტის ან მომსახურების შექმნის პროცესში* და *პირველად პარამეტრად* გათვალისწინების უზრუნველყოფაში, რაც ნიშნავს იმას, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა შეძლონ იმის დემონსტრირება, რომ მათ დამუშავების პროცესში აქვთ სათანადო

[2] GDPR-ის პრეამბულის 78-ე პუნქტი მკაფიოდ მიუთითებს აღნიშნულ საჭიროებაზე: *„იმ აპლიკაციების, მომსახურებისა და პროდუქტების შექმნის, შერჩევისა და გამოყენების პროცესში, რომლებიც მოიცავს/ეფუძნება პერსონალური მონაცემების დამუშავებას ან საჭიროებს პერსონალურ მონაცემთა დამუშავებას ამოცანების შესასრულებლად, უნდა მოხდეს ამ პროდუქტების, სერვისების და აპლიკაციების შემქმნელების წახალისება, რათა მათ, არსებული საუკეთესო პრაქტიკის გათვალისწინებით, გაითვალისწინონ მონაცემთა დაცვის უფლება პროდუქტების, სერვისების და აპლიკაციების შემუშავებისა და შექმნის ეტაპზე, რათა დამუშავებისთვის პასუხისმგებელმა პირებმა და დამუშავებაზე უფლებამოსილმა პირებმა შეძლონ მონაცემთა დაცვასთან დაკავშირებული ვალდებულებების შესრულება.“*

ზომები და პრინციპების, მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დაცვის ეფექტური მექანიზმები.

3. სახელმძღვანელო პრინციპების მე-2 თავი ყურადღებას ამახვილებს 25-ე მუხლით დადგენილი მოთხოვნების ინტერპრეტაციაზე და მიმოიხილავს ამ დებულებით დადგენილ სამართლებრივ ვალდებულებებს. მონაცემთა დაცვის სპეციფიური პრინციპების კონტექსტში DPbDD-ის გამოყენების მაგალითები წარმოდგენილია მე-3 თავში.

4. სახელმძღვანელო პრინციპები ეხება სერტიფიცირების მექანიზმის შექმნის შესაძლებლობას (მე-4 თავი), 25-ე მუხლთან შესაბამისობის დემონსტრირებისთვის, აგრეთვე, საზედამხედველო ორგანოების მიერ აღნიშნულ მუხლთან შესაბამისობის აღსრულებას (მე-5 თავი). და ბოლოს, სახელმძღვანელო პრინციპები დაინტერესებულ მხარეებს უზრუნველყოფს დეტალური რეკომენდაციებით DPbDD-ის წარმატებით განხორციელების შესახებ. EDPB ითვალისწინებს იმ გამოწვევებს, რომელთაც აწყდებიან მცირე და საშუალო ზომის საწარმოები (შემდგომში, SME საწარმოები), DPbDD ვალდებულებებთან შესაბამისობის კუთხით და უზრუნველყოფს დამატებით რეკომენდაციებს კონკრეტულად SME საწარმოებისთვის (მე-6 თავი).

2. 25-ე მუხლის 1-ლი და მე-2 პუნქტების ანალიზი: მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში და მონაცემთა დაცვა პირველად პარამეტრად

5. წინამდებარე თავის მიზანია, 25-ე მუხლის 1-ლი და მე-2 პუნქტებით დადგენილი მოთხოვნების მიმოხილვა და სახელმძღვანელო ინსტრუქციების უზრუნველყოფა. მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში და მონაცემთა დაცვა პირველად პარამეტრად წარმოადგენს ერთმანეთთან მჭიდროდ დაკავშირებულ კონცეფციებს, რომლებიც ამყარებენ ერთმანეთის მოქმედებას. მონაცემთა სუბიექტი უფრო მეტ სარგებელს მიიღებს პირველად პარამეტრად მონაცემთა დაცვის გათვალისწინებისგან, თუ ამავდროულად განხორციელდება მოთხოვნა, რომელიც გულისხმობს მონაცემთა დაცვის სტანდარტების გათვალისწინებას ახალი პროდუქტის ან მომსახურების შექმნის პროცესში და პირიქით.

6. DPbDD მოთხოვნები თანაბრად ვრცელდება ყველა დამუშავებისთვის პასუხისმგებელ პირებზე, როგორც მცირე ბიზნესებზე, ისე მულტინაციონალურ კომპანიებზე. შესაბამისად, DPbDD-ის განხორციელების კომპლექსურობა,

შესაძლოა, განსხვავდებოდეს მონაცემთა დამუშავების ინდივიდუალური ოპერაციიდან გამომდინარე. ამავდროულად, ნებისმიერ შემთხვევაში, DPbDD-ის განხორციელება პოზიტიურ შედეგებს მოუტანს როგორც დამუშავებისთვის პასუხისმგებელ პირს, ისე მონაცემთა სუბიექტს.

2.1 25-ე მუხლის 1-ლი პუნქტი: მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში

2.1.1 დამუშავებისთვის პასუხისმგებელი პირის ვალდებულება, დამუშავების პროცესში გაატაროს სათანადო ტექნიკური და ორგანიზაციული ზომები და უზრუნველყოს დაცვის მექანიზმების ინტეგრაცია

7. 25(1) მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაატაროს *სათანადო* ტექნიკური და ორგანიზაციული ზომები, რომელთა მიზანია განახორციელოს მონაცემთა დაცვის პრინციპები და მოახდინოს საჭირო დაცვის მექანიზმების ინტეგრაცია დამუშავების პროცესში, რათა შესრულდეს GDPR რეგულაციის მოთხოვნები და დაცული იქნეს მონაცემთა სუბიექტის უფლებები და თავისუფლებები. სათანადო ზომები და აუცილებელი დაცვის მექანიზმები ერთსა და იმავე მიზანს ემსახურება: მონაცემთა სუბიექტების უფლებების დაცვა და მათი პერსონალური მონაცემების დაცვის ინტეგრირება დამუშავების პროცესში.

8. ტექნიკური და ორგანიზაციული ზომები და აუცილებელი დაცვის მექანიზმები, შესაძლოა, ფართო თვალსაზრისით, გაგებული იქნეს, როგორც მეთოდი ან საშუალება, რომელსაც დამუშავებისთვის პასუხისმგებელი პირი იყენებს დამუშავების პროცესში. „სათანადო“ ნიშნავს, რომ ზომები და საჭირო დაცვის მექანიზმები დასახული მიზნის მიღწევისათვის შესაფერისი უნდა იყოს, ე.ი. ისინი უნდა უზრუნველყოფდეს მონაცემთა დაცვის პრინციპების *ეფექტურად* განხორციელებას.[3] ამრიგად, „სათანადოობის“ მოთხოვნა მჭიდროდ არის დაკავშირებული ეფექტურობის მოთხოვნასთან.

9. ტექნიკური და ორგანიზაციული ზომა და დაცვის მექანიზმი, შესაძლოა, გულისხმობდეს როგორც მოწინავე ტექნოლოგიური გადაწყვეტების გამოყენებას, ისე პერსონალის საბაზისო ტრენინგს. არსებული კონტექსტისა და დამუშავების მოცემულ შემთხვევასთან ასოცირებული რისკების გათვალისწინებით, შესაბამისი მაგალითები მოიცავს: პერსონალური მონაცემების ფსევდონიმიზაციას[4]; ხელმისაწვდომი პერსონალური მონაცემების შენახვას სტრუქტურირებული, გამოყენებადი, ელექტრონულად წაკითხვადი ფორმით; მონაცემთა სუბიექტისათვის დამუშავებაში ჩარევის

[3] „ეფექტურობა“ განხილულია ქვემოთ, 2.1.2 ქვეთავში.
[4] განმარტებულია GDPR-ის 4(5) მუხლში.

შესაძლებლობის უზრუნველყოფას; ინფორმაციის მიწოდებას პერსონალური მონაცემების შენახვის შესახებ; მავნე პროგრამების გამოვლენის სისტემების ქონას; დასაქმებულთა ტრენინგს საბაზისო „კიბერ-ჰიგიენის“ შესახებ; პირადი ცხოვრების ხელშეუხებლობისა და საინფორმაციო უსაფრთხოების მართვის სისტემების შექმნას; დამუშავებისთვის პასუხისმგებელ პირებზე ხელშეკრულების საფუძველზე ვალდებულების დაკისრებას, განახორციელოს სპეციფიური მონაცემთა მინიმიზაცია და ა.შ.

10. სტანდარტები, საუკეთესო პრაქტიკები და ქცევის კოდექსები, რომლებიც აღიარებულია დამუშავებისთვის პასუხისმგებელ პირთა სხვადასხვა კატეგორიების წარმომადგენელი ასოციაციების და სხვა ორგანოების მიერ, ხელს შეუწყობს სათანადო ზომების განსაზღვრას. ამავდროულად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გადაამოწმოს, თუ რამდენად შესაფერისია მოცემული ზომები დამუშავების კონკრეტულ შემთხვევაში.

2.1.2 შექმნილია დამუშავების პრინციპების ეფექტურად იმპლემენტაციისთვის და მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დასაცავად

11. *მონაცემთა დაცვის პრინციპები* წარმოდგენილია მე-5 მუხლში (შემდგომში, „პრინციპები“); მონაცემთა სუბიექტთა უფლებები და თავისუფლებები არის ფიზიკურ პირთა ფუნდამენტური უფლებები და თავისუფლებები, კერძოდ, მათი უფლება პერსონალური მონაცემების დაცვაზე, რაც 1(2) მუხლის თანახმად, წარმოადგენს GDPR-ის მიზანს (შემდგომში, „უფლებები“)[5]. მათი ზუსტი ფორმულირება ხელმისაწვდომია ევროკავშირის ფუნდამენტურ უფლებათა ქარტიაში. მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელ პირს ესმოდეს პრინციპებისა და უფლებების მნიშვნელობა, რაც GDPR-ით უზრუნველყოფილი დაცვის საფუძველია, კერძოდ, DPbDD ვალდებულების.

12. სათანადო ტექნიკური და ორგანიზაციული ზომების განხორციელებისას, ზომები და დაცვის მექანიზმები შემუშავებული უნდა იქნეს ზემოაღნიშნული პრინციპების ეფექტური განხორციელებისა და უფლებების დაცვის უზრუნველყოფის თვალსაზრისით.

ეფექტურობის შესახებ

13. ეფექტურობა „მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში“ კონცეფციის მნიშვნელოვანი შემადგენელი ნაწილია. პრინციპების ეფექტურად განხორციელების მოთხოვნა

[5] იხ. GDPR-ის პრეამბულის მეოთხე პუნქტი.

ნიშნავს, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა განახორციელონ საჭირო ზომები და დაცვის მექანიზმები ამ პრინციპების დასაცავად, რათა დაცული იქნეს მონაცემთა სუბიექტების უფლებები. თითოეულმა განხორციელებულმა ზომამ ხელი უნდა შეუწყოს დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დამუშავებისთვის გათვალისწინებული შედეგების მიღწევას. ეს დაკვირვება ორ შედეგს წარმოშობს.

14. პირველი, ეს ნიშნავს რომ 25-ე მუხლი არ ითხოვს რაიმე კონკრეტული ტექნიკური და ორგანიზაციული ზომების განხორციელებას, არამედ, შერჩეული ზომები და დაცვის მექანიზმები უნდა იყოს მონაცემთა დამუშავების მოცემულ შემთხვევაში მონაცემთა დაცვის პრინციპების ინტეგრაციის შესაბამისი. შესაბამისად, შემუშავებული ზომები და დაცვის მექანიზმები უნდა იყოს მყარი, ხოლო დამუშავებისთვის პასუხისმგებელ პირს უნდა შეეძლოს დამატებითი ზომების განხორციელება, გაზრდილი რისკის შესაბამისად.[6] ამრიგად, ზომების ეფექტურობა დამოკიდებული იქნება დამუშავების კონტექსტზე და გარკვეული ელემენტების შეფასებაზე, რაც მხედველობაში უნდა იქნეს მიღებული დამუშავების საშუალებების განსაზღვრისას. ეს ელემენტები ქვემოთ არის დეტალურად განხილული (ქვეთავი 2.1.3).

15. მეორე, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა შეძლონ დემონსტრირება იმისა რომ პრინციპები არის შენარჩუნებული.

16. განხორციელებული ზომები და დაცვის მექანიზმები უნდა იწვევდეს სასურველ შედეგს, მონაცემთა დაცვის თვალსაზრისით, ხოლო დამუშავებისთვის პასუხისმგებელ პირს უნდა ჰქონდეს განხორციელებული ტექნიკური და ორგანიზაციული ზომების ამსახველი დოკუმენტაცია.[7] აღნიშნულის საფუძველზე, დამუშავებისთვის პასუხისმგებელი პირი შეძლებს, განსაზღვროს „შესრულების ძირითადი ინდიკატორები“ (KPI), ეფექტურობის დემონსტრირების მიზნით. KPI არის გაზომვადი მაჩვენებელი, რომელსაც დამუშავებისთვის პასუხისმგებელი პირი ირჩევს, რათა წარმოაჩინოს დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დაცვის მიზნების

[6] „ფუნდამენტური პრინციპები, რომლებიც ვრცელდება დამუშავებისთვის პასუხისმგებელ პირებზე (ე.ი., ლეგიტიმურობა, მონაცემთა მინიმიზაცია, მიზნის შეზღუდვა, გამჭვირვალობა, მონაცემთა მთლიანობა, მონაცემთა სიზუსტე), იგივე უნდა დარჩეს, დამუშავებისა და მონაცემთა სუბიექტისათვის არსებული რისკების მიუხედავად. ამავდროულად, დამუშავების ხასიათისა და მასშტაბის სათანადოდ გათვალისწინება ამ პრინციპების გამოყენების განუყოფელი ნაწილია, რათა შესაძლებელი იყოს მათი [პრინციპების] გამოყენების მასშტაბის გაზრდა.“ 29-ე მუხლის სამუშაო ჯგუფი. „განცხადება მონაცემთა დაცვის სამართლებრივ ჩარჩოებში რისკზე დაფუძნებული მიდგომის შესახებ.“ WP 2018, 2014 წლის 30 მაისი, გვ.3, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[7] იხ. პრეამბულის პუნქტები 74 და 78.

განხორციელების ეფექტურობა. KPI შესაძლოა, იყოს *რაოდენობრივი*, როგორიცაა, ცრუ დადებითების ან ცრუ უარყოფითების პროცენტული რაოდენობა, საჩივრების რაოდენობის შემცირება, რეაგირების დროის შემცირება მონაცემთა სუბიექტის მიერ საკუთარი უფლების განხორციელებისას; ან *თვისებრივი*, როგორიცაა საქმიანობის შეფასება, შეფასების სკალების გამოყენება ან ექსპერტული შეფასებები. KPI-ს გარდა, დამუშავებისთვის პასუხისმგებელ პირს პრინციპების ეფექტურად განხორციელების დემონსტრირება შეუძლია იმ შემთხვევაში, თუ იგი დაასაბუთებს არჩეული ზომებისა და დაცვის მექანიზმების ეფექტურობის შეფასებას.

2.1.3 გასათვალისწინებელი ელემენტები

17. 25-ე მუხლის პირველ პუნქტში ჩამოთვლილია ელემენტები, რომლებიც დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს დამუშავების კონკრეტული ოპერაციისთვის შესაბამისი ზომების განსაზღვრისას. ქვემოთ წარმოდგენილია ინსტრუქციები ამ ელემენტების ახალი პროდუქტის ან მომსახურების შექმნის პროცესში გათვალისწინებასთან დაკავშირებით, მათ შორის, პირველადი პარამეტრების შემუშავებისას. ეს ელემენტები ხელს უწყობს იმის განსაზღვრას, თუ რამდენად შესაფერისია რაიმე ზომა პრინციპების ეფექტურად განხორციელებისთვის. ამრიგად, თითოეული ელემენტი არ წარმოადგენს თავად მიზანს, არამედ, ისინი არიან ფაქტორები, რომლებიც ერთობლიობაში უნდა იქნეს გათვალისწინებული, შესაბამისი მიზნის მისაღწევად.

2.1.3.1 „უახლესი ტექნოლოგიები“

18. „უახლესი ტექნოლოგიების“ კონცეფციას შევხვდებით ევროკავშირის სხვადასხვა კანონებში, მაგ., გარემოს დაცვის და პროდუქციის უსაფრთხოების შესახებ. GDPR-ში, „უახლეს ტექნოლოგიებზე“[8] მითითებას ვხვდებით არა

[8] იხ. გერმანიის ფედერალური საკონსტიტუციო სასამართლოს გადაწყვეტილება Kalkar-ის საქმეში, 1978 წ., https://germanlawarchive.iuscomp.org/?p=67, მის საფუძველზე შესაძლოა განისაზღვროს მეთოდოლოგია კონცეფციის ობიექტური განსაზღვრებისთვის. აღნიშნული გადაწყვეტილების შესაბამისად, „უახლესი ტექნოლოგიების“ წარმოადგენს ტექნოლოგიურ დონეს, რომლის ადგილიც არის „არსებულ სამეცნიერო ცოდნასა და კვლევას“ და „ტექნოლოგიების ზოგადად მიღებულ/აღიარებულ წესებს“ შორის. ამრიგად, შეიძლება ითქვას, რომ „უახლესი ტექნოლოგიები“ წარმოადგენს მომსახურების, ტექნოლოგიის ან პროდუქტის ტექნოლოგიურ დონეს, რომელიც ბაზარზე არსებობს და ყველაზე ეფექტური გზაა იდენტიფიცირებული მიზნების მისაღწევად.

მხოლოდ 32-ე მუხლში, რომელიც უსაფრთხოების ზომებს ეხება,[9] [10]არამედ, აგრეთვე, 25-ე მუხლში. შესაბამისად, აღნიშნული ბენჩმარკი ეხება ყველა ტექნიკურ და ორგანიზაცულ ზომას, რომელიც დამუშავებაში არის ინტეგრირებული.

19. 25-ე მუხლის კონტექსტში, „უახლეს ტექნოლოგიებზე“ მითითება დამუშავებისთვის პასუხისმგებელ პირებს აკისრებს ვალდებულებას, სათანადო ტექნიკური და ორგანიზაციული ზომების განსაზღვრისას, **გაითვალისწინონ** ბაზარზე ხელმისაწვდომი **ტექნოლოგიების სფეროში არსებული პროგრესი.** დამუშავებისთვის პასუხისმგებელ პირებს მოეთხოვებათ, იყვნენ ინფორმირებულები და ჰქონდეთ განახლებული ინფორმაცია ტექნოლოგიური განვითარებების შესახებ; რა სახის მონაცემთა დაცვის რისკებსა და შესაძლებლობებს ქმნის ტექნოლოგიები, დამუშავების პროცესში; როგორ უნდა განხორციელდეს და განახლდეს ზომები და დაცვის მექანიზმები, რომლებიც ამ პრინციპებისა და მონაცემთა სუბიექტის უფლებების *ეფექტურ იმპლემენტაციას* უზრუნველყოფს, განვითარებადი ტექნოლოგიური ლანდშაფტის გათვალისწინებით.

20. „უახლესი ტექნოლოგიები“ დინამიკური კონცეფციაა და შეუძლებელია მისი სტატიკურად განსაზღვრა, დროის რომელიმე მონაკვეთში, არამედ, მისი შეფასება უნდა მოხდეს უწყვეტად, ტექნოლოგიური პროგრესის კონტექსტში. ტექნოლოგიური წინსვლების გათვალისწინებით, დამუშავებისთვის პასუხისმგებელმა პირმა შესაძლოა გამოავლინოს ზომა, რომელიც წინათ ადეკვატურ დაცვას უზრუნველყოფდა, თუმცა, ამჟამად ვეღარ უზრუნველყოფს. ტექნოლოგიური ცვლილებების შესახებ განახლებული ინფორმაციის არ ქონა, შესაბამისად, გამოიწვევს 25-ე მუხლის მოთხოვნებთან შეუსაბამობას.

21. „უახლესი ტექნოლოგიების“ კრიტერიუმი არა მხოლოდ ტექნოლოგიურ, არამედ ორგანიზაციულ ზომებზეც ვრცელდება. სათანადო ორგანიზაციული ზომების არ არსებობამ, შესაძლოა, შეამციროს ან სრულად დააზიანოს არჩეული ტექნოლოგიის ეფექტურობა. ორგანიზაციული ზომების მაგალითები, შესაძლოა, მოიცავდეს შიდა პოლიტიკის მიღებას; განახლებულ ტრენინგს ტექნოლოგიების, უსაფრთხოებისა და მონაცემთა დაცვის შესახებ; და IT უსაფრთხოების მართვის პოლიტიკას.

22. სხვადასხვა სფეროებში არსებული და აღიარებული ჩარჩოები, სტანდარტები, სერტიფიცირებები, ქცევის კოდექსები და ა.შ. გარკვეულ როლს ასრულებს და მიუთითებს, თუ რა წარმოადგენს „უახლეს ტექნოლოგიებს“ მოცემულ

[99] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security
[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

სფეროში. თუ არსებობს ამგვარი სტანდარტები და ისინი უზრუნველყოფენ მონაცემთა სუბიექტების დაცვას მაღალ დონეზე, სამართლებრივი მოთხოვნების შესაბამისად (ან მათ მიღმა), დამუშავებისთვის პასუხისმგებელი პირები ვალდებულები არიან, ეს სტანდარტები გაითვალისწინონ მონაცემთა დაცვის ზომების შექმნისა და იმპლემენტაციის პროცესში.

2.1.3.1 „განხორციელების ხარჯები“

23. დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია, განხორციელების ხარჯები გაითვალისწინოს იმ სათანადო ტექნიკური და ორგანიზაციული ზომებისა და საჭირო დაცვის მექანიზმების არჩევისას და გამოყენებისას, რომლებიც უზრუნველყოფენ პრინციპების ეფექტურ იმპლემენტაციას, რათა მონაცემთა სუბიექტის უფლებები იქნეს დაცული. ხარჯები მიუთითებს ზოგადად რესურსებზე, როგორც დროზე, ისე ადამიანურ რესურსებზე.

24. ხარჯების ელემენტი არ მოითხოვს დამუშავებისთვის პასუხისმგებელი პირის მხრიდან არაპროპორციული ოდენობის რესურსების ხარჯვას იმ შემთხვევაში, თუ არსებობს ალტერნატიული და ამავდროულად, ეფექტური ზომები, რომლებიც ნაკლებ რესურსს მოითხოვენ. ამავდროულად, განხორციელების ხარჯები წარმოადგენს ფაქტორს, რომელიც გათვალისწინებული უნდა იქნეს პრინციპის „მონაცემთა სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში“ განხორციელებისას და არა ამ პრინციპის არ განხორციელების საფუძველი.

25. ამრიგად, არჩეული ზომები უნდა უზრუნველყოფდეს, რომ დამუშავებისთვის პასუხისმგებელ პირის მიერ გათვალისწინებული დამუშავების აქტივობა არ ითვალისწინებს დამუშავებას აღნიშნული პრინციპების დარღვევით, ხარჯის მიუხედავად. დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა შეძლონ ზოგადი ხარჯების მართვა, რათა ეფექტურად განახორციელონ ყველა პრინციპი და შესაბამისად, დაიცვან უფლებები.

2.1.3.3 „დამუშავების ხასიათი, მასშტაბი, კონტექსტი და მიზანი“

26. დამუშავებისთვის პასუხისმგებელი პირები ვალდებულები არიან, გაითვალისწინონ დამუშავების ხასიათი, მასშტაბი, კონტექსტი და მიზანი, საჭირო ზომების განსაზღვრისას.

27. ეს ფაქტორები ინტერპრეტირებული უნდა იქნეს თანმიმდევრულად, იმის გათვალისწინებით, თუ რა როლი აქვთ მათ GDPR-ის სხვა დებულებებში,

როგორიცაა, 24-ე, 32-ე და 35-ე მუხლები, დამუშავების პროცესში მონაცემთა დაცვის პრინციპების ინტეგრაციის მიზნით.

28. მოკლედ რომ ვთქვათ, „ხასიათის“ კონცეფცია გაგებული უნდა იქნეს, როგორც დამუშავების განუყოფელი მახასიათებლები.[11] „მასშტაბი“ მიუთითებს დამუშავების ზომასა და ფარგლებზე. „კონტექსტი“ დაკავშირებულია დამუშავების გარემოებებთან, რომლებიც შესაძლოა გავლენას ახდენდეს მონაცემთა სუბიექტის მოლოდინებზე, ხოლო „მიზანი“ ეხება დამუშავების მიზნებს.

2.1.3.4 „მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისათვის სავარაუდო რისკები“

29. GDPR-ის არაერთ დებულებაში მოქმედებს თანმიმდევრული, რისკზე დაფუძნებული მიდგომა, კერძოდ, 24-ე, 25-ე, 32-ე და 35-ე მუხლებში, რისი მიზანიც არის სათანადო ტექნიკური და ორგანიზაციული ზომების განხორციელება ფიზიკური პირების, მათი პერსონალური მონაცემების დასაცავად და GDPR-ის მოთხოვნების შესასრულებლად. დასაცავი აქტივები არ იცვლება (ფიზიკური პირები, მათი პერსონალური მონაცემების დაცვის გზით), ისევე, როგორც არ იცვლება რისკები/საფრთხეები (რომლებიც ემუქრება ფიზიკურ პირთა უფლებებს) და გასათვალისწინებელი პირობები (დამუშავების ხასიათი, მასშტაბი, კონტექსტი და მიზნები).

30. რისკის ანალიზის განხორციელებისას, 25-ე მუხლთან შესაბამისობის კუთხით, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მოახდინოს იმ რისკების იდენტიფიცირება, რომელსაც პრინციპების დარღვევა უქმნის მონაცემთა სუბიექტის უფლებებს, და განსაზღვროს მათი ალბათობა და სიმწვავე, რათა განახორციელოს ზომები, რომლებიც ეფექტურად უზრუნველყოფს იდენტიფიცირებული რისკების განეიტრალებას. რისკის შეფასებისას უაღრესად მნიშვნელოვანია დამუშავების სისტემატური და ამომწურავი შეფასება. მაგალითად, დამუშავებისთვის პასუხისმგებელი პირი აფასებს კონკრეტულ რისკებს, რომლებიც უკავშირდება ნებაყოფლობით გაცემული ნებართვის ნაკლებობას, რაც წარმოადგენს კანონიერების პრინციპის დარღვევას, ბავშვების და 18 წლამდე ახალგაზრდების პერსონალური მონაცემების დამუშავების პროცესში, როდესაც არ არსებობს სხვა სამართლებრივი საფუძველი, და ახორციელებს სათანადო ზომებს, რათა

[11] მაგალითად: პერსონალურ მონაცემთა განსაკუთრებული კატეგორიები, ავტომატური გადაწყვეტილებების მიღება, ძალაუფლებათა დისბალანსი, არა-განჭვრეტადი დამუშავება, სირთულეები, რომლებსაც მონაცემთა სუბიექტი აწყდება უფლებების განხორციელების კუთხით და ა.შ.

რეაგირება მოახდინოს და ეფექტურად გაანეიტრალოს იდენტიფიცირებული რისკები, რომლებიც ასოცირდება მონაცემთა სუბიექტების ამ ჯგუფთან.

31. „EDPB სახელმძღვანელო პრინციპები მონაცემთა დაცვის ზემოქმედების შეფასების (DPIA) შესახებ“[12], რომელიც ფოკუსირებას ახდენს იმის განსაზღვრაზე, თუ რამდენად შეუქმნის დამუშავების ოპერაცია მაღალ რისკს მონაცემთა სუბიექტს, აგრეთვე, უზრუნველყოფს ინსტრუქციებს მონაცემთა დაცვის რისკების შეფასების შესახებ და მონაცემთა დაცვის რისკის შეფასების განხორციელების გზებზე. სახელმძღვანელო პრინციპები სასარგებლო დოკუმენტია ყველა ზემოაღნიშნული მუხლის, მათ შორის, 25-ე მუხლის შესაბამისად, რისკის შეფასებისას.

32. რისკზე დაფუძნებული მიდგომა არ გამორიცხავს საბაზისო მონაცემების, საუკეთესო პრაქტიკებისა და სტანდარტების გამოყენებას. აღნიშნული სასარგებლო ინსტრუმენტებია დამუშავებისთვის პასუხისმგებელი პირებისთვის, რათა მათ მსგავს სიტუაციებში მსგავს რისკებზე მოახდინონ რეაგირება (დამუშავების ხასიათის, მასშტაბის, კონტექსტის და მიზნის შესაბამისად). ამავდროულად, ძალაში რჩება 25-ე მუხლით (ისევე, როგორც 24-ე, 32-ე და 35-ე მუხლის 7(c) პუნქტით) გათვალისწინებული ვალდებულება, მხედველობაში იქნეს მიღებული „მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისათვის სავარაუდო რისკები“. შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირები ვალდებულები არიან, აღნიშნული ინსტრუმენტების ხელმისაწვდომობისდა მიუხედავად, ყოველთვის განახორციელონ მონაცემთა დაცვასთან დაკავშირებული რისკების შეფასება ინდივიდუალურ შემთხვევებში, დამუშავების მოცემული აქტივობისთვის და შეაფასონ შესაძლო სათანადო ზომებისა და დაცვის მექანიზმების ეფექტურობა, რის შემდგომაც, შესაძლოა, საჭირო გახდეს „მონაცემთა დაცვის ზემოქმედების შეფასება“ (DPIA) ან არსებული DPIA-ს განახლება.

2.1.4 დროის ასპექტი

2.1.4.1 „დამუშავების საშუალებების განსაზღვრის დროს“

33. პრინციპი „მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში“ უნდა განხორციელდეს „დამუშავების საშუალებების განსაზღვრის დროს.“

[12] 29-ე მუხლის სამუშაო ჯგუფი, „სახელმძღვანელო პრინციპები მონაცემთა დაცვის ზეგავლენის შეფასების (DPIA) და იმის განსაზღვრის შესახებ, თუ „რამდენად გამოიწვევს მაღალ რისკს“ დამუშავება, 2016/679 რეგულაციის მიზნებისთვის.“ WP 248 rev.01, 2017 წლის 4 ოქტომბერი. ec.europa.eu/newsroom/document.cfm?doc_id=47711, აღიარებულია EDPB-ის მიერ.

34. „დამუშავების საშუალებები“ გულისხმობს დამუშავების დიზაინის როგორც ზოგად, ისე დეტალურ ელემენტებს, მათ შორის: არქიტექტურას, პროცედურებს, პროტოკოლებს, სქემებს და გარეგნულ მხარეს.

35. „დამუშავების საშუალებების განსაზღვრის დროს“ მიუთითებს დროის იმ პერიოდზე, როდესაც დამუშავებისთვის პასუხისმგებელი პირი იღებს გადაწყვეტილებას იმის შესახებ, თუ როგორ ჩატარდება დამუშავება, რა ფორმით და რა მექანიზმები იქნება გამოყენებული დამუშავებისთვის. სწორედ ამგვარი გადაწყვეტილებების მიღების პროცესში, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეაფასოს სათანადო ზომები და დაცვის მექანიზმები, რათა ეფექტურად განახორციელოს მონაცემთა სუბიექტების პრინციპები და უფლებები დამუშავების პროცესში, და გაითვალისწინოს ისეთი ელემენტები, როგორიცაა: უახლესი ტექნოლოგიები, განხორციელების ხარჯები, დამუშავების ხასიათი, მასშტაბი, კონტექსტი და მიზანი, და რისკები. ეს მოიცავს მონაცემთა დამუშავების კომპიუტერული უზრუნველყოფის, აპარატურის და სერვისების შესყიდვისა და განხორციელების დროს.

36. DPbDD-ის გათვალისწინება ადრეულ ეტაპზე უაღრესად მნიშვნელოვანია მონაცემთა სუბიექტების უფლებების დაცვისთვის და პრინციპების წარმატებით განხორციელებისთვის. ამასთან, ხარჯთეფექტურობის პერსპექტივიდან, დამუშავებისთვის პასუხისმგებელი პირის ინტერესშია, გაითვალისწინოს DPbDD ადრეულ ეტაპზე, ვიდე მოგვიანებით, ვინაიდან მოგვიანებით შემუშავებულ გეგმებსა და დამუშავების პროცესებში ცვლილებების შეტანა შესაძლოა იყოს რთული და გარკვეულ ხარჯებთან დაკავშირებული.

2.1.4.2 თავად დამუშავების დროს (მონაცემთა დაცვის მოთხოვნების შენარჩუნება და გადახედვა)

37. დამუშავების დაწყების შემდგომ, დამუშავებისთვის პასუხისმგებელ პირს აქვს უწყვეტი ვალდებულება, შეინარჩუნოს DPbDD პრინციპები, ე.ი. პრინციპების უწყვეტი ეფექტური იმპლემენტაცია, უფლებების დაცვის მიზნით, იყოს ინფორმირებული უახლესი ტექნოლოგიების შესახებ, შეაფასოს რისკის დონე და ა.შ. დამუშავების ოპერაციების ხასიათი, მასშტაბი და კონტექსტი და რისკი, შესაძლოა, დამუშავების პროცესში შეიცვალოს, რაც ნიშნავს იმას, რომ დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მოახდინოს საკუთარი დამუშავების ოპერაციების ხელახლა შეფასება, არჩეული ზომებისა და დაცვის მექანიზმების ეფექტურობის რეგულარული შეფასების და გადახედვის გზით.

38. დამუშავების ოპერაციის მოვლა-პატრონობის (maintain), გადახედვის და განახლების (საჭიროების შესაბამისად) ვალდებულება, აგრეთვე, ვრცელდება

უკვე არსებულ სისტემებზე. ეს ნიშნავს იმას, რომ GDPR-ის ძალაში შესვლამდე შექმნილი სისტემების გადახედვა და მოვლა-პატრონობა სავალდებულოა, რათა უზრუნველყოფილი იქნეს იმ ზომებისა და დაცვის მექანიზმების განხორციელება, რომლებიც ხელს უწყობენ პრინციპებისა და მონაცემთა სუბიექტების უფლებების ეფექტურად განხორციელებას, როგორც ეს განხილულია წინამდებარე სახელმძღვანელო პრინციპებში.

39. აღნიშნული ვალდებულება, აგრეთვე, ვრცელდება ნებისმიერ დამუშავებაზე, რომელიც ხორციელდება დამუშავებაზე უფლებამოსილი პირების საშუალებით. დამუშავებისთვის პასუხისმგებელ პირთა ოპერაციები რეგულარულად უნდა გადაიხედოს და შეფასდეს დამუშავებისთვის პასუხისმგებელი პირის მიერ, რათა უზრუნველყოფილი იქნეს პრინციპებთან უწყვეტი შესაბამისობა და დამუშავებისთვის პასუხისმგებელმა პირმა შეძლოს ამ მხრივ არსებული ვალდებულებების შესრულება.

2.2 მუხლი 25(2): მონაცემთა დაცვა პირველად პარამეტრად

2.2.1 პირველადი პარამეტრი ითვალისწინებს მხოლოდ იმ პერსონალური მონაცემების დამუშავებას, რომელიც საჭიროა თითოეული კონკრეტული მიზნისთვის

40. „პირველად პარამეტრად“, კომპიუტერულ მეცნიერებაში არსებული ფართოდ გავრცელებული განსაზღვრების თანახმად, ნიშნავს უკვე არსებულ ან წინასწარ შერჩეულ მახასიათებელს კონფიგურირებად პარამეტრებში, რომელიც მიენიჭება ელექტრონულ აპლიკაციას, კომპიუტერულ პროგრამას ან მოწყობილობას. ასეთ პარამეტრებს უწოდებენ „წინასწარ განსაზღვრულ“ ან „ქარხნულ“ პარამეტრებს, განსაკუთრებით, ელექტრონულ მოწყობილობებთან მიმართებით.

41. ამრიგად, ტერმინი „პირველად პარამეტრად“ პერსონალური მონაცემების დამუშავების კონტექსტში, მიუთითებს კონფიგურაციულ მახასიათებლებთან ან დამუშავების სისტემაში (ელექტრონული აპლიკაციები, მომსახურება ან მოწყობილობა ან დამუშავების მექანიკური პროცედურა) ინტეგრირებულ ან გათვალისწინებულ ვარიანტებთან დაკავშირებით არჩევანის გაკეთებას, რაც გავლენას ახდენს შეგროვებული მონაცემების რაოდენობაზე, მათი დამუშავების მასშტაბზე, შენახვის ვადაზე და მათ ხელმისაწვდომობაზე.

42. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, აარჩიოს დამუშავების პირველადი პარამეტრებისა და ვარიანტების იმგვარად განხორციელება, რომ პირველადი პარამეტრების მიხედვით განხორციელდეს მხოლოდ დამუშავება, რომელიც მკაცრად აუცილებელია დასახული, კანონიერი მიზნისთვის. ამრიგად, დამუშავებისთვის პასუხისმგებელი პირი უნდა დაეყრდნოს მის მიერ

დამუშავების აუცილებლობის შეფასებას, 6(1) მუხლით გათვალისწინებულ სამართლებრივ საფუძვლებთან დაკავშირებით. ეს ნიშნავს იმას, რომ პირველადი პარამეტრების მიხედვით, დამუშავებისთვის პასუხისმგებელმა პირმა არ უნდა შეაგროვოს იმაზე მეტი ინფორმაცია, ვიდრე ეს აუცილებელია; არ უნდა დაამუშაოს მონაცემები იმაზე მეტად, ვიდრე ეს აუცილებელია დამუშავების მიზნებისთვის; და არ უნდა შეინახოს მონაცემები იმაზე მეტი ხნით, ვიდრე საჭიროა. საბაზისო მოთხოვნა მდგომარეობს იმაში, რომ მონაცემთა დაცვა პირველად პარამეტრად იყოს გათვალისწინებული დამუშავებაში.

43. დამუშავებისთვის პასუხისმგებელ პირს მოეთხოვება, განსაზღვროს, თუ რა კონკრეტული, ცალსახა და ლეგიტიმური მიზნებისთვის ხდება მონაცემთა შეგროვება და დამუშავება.[13] ზომები ავტომატურად უნდა უზრუნველყოფდეს მხოლოდ იმ პერსონალური მონაცემების დამუშავებას, რომლებიც აუცილებელია დამუშავების თითოეული კონკრეტული მიზნისთვის. EDPS-ის „სახელმძღვანელო პრინციპები იმ ზომების საჭიროების და პროპორციულობის შეფასების შესახებ, რომლებიც ზღუდავს უფლებას მონაცემთა დაცვაზე“ სასარგებლო დოკუმენტია, რომელიც **დამუშავებისთვის პასუხისმგებელ პირებს** დაეხმარება გადაწყვეტილების მიღებაში, თუ რომელი მონაცემების დამუშავებაა აუცილებელი კონკრეტული მიზნის მისაღწევად.[14] [15] [16]

44. იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელი პირი იყენებს მესამე მხარის ან მასობრივი წარმოების კომპიუტერულ პროგრამას, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, განახორციელოს რისკის შეფასება პროდუქტთან დაკავშირებით და უზრუნველყოს, რომ ფუნქციები, რომელთაც არ აქვთ სამართლებრივი საფუძველი ან არ არიან თავსებადი დამუშავების განსაზღვრულ მიზნებთან, არის გამორთული.

45. იგივე საკითხების გათვალისწინებაა საჭირო იმ ორგანიზაციულ ზომებთან დაკავშირებით, რომლებიც ხელს უწყობენ დამუშავების ოპერაციებს. ისინი

[13] GDPR-ის მე-5 მუხლის პირველი პუნქტის (b), (c), (d) და (e) პუნქტები.

[14] EDPS. „სახელმძღვანელო პრინციპები, იმ ზომების საჭიროებისა და პროპორციულობის შეფასების შესახებ, რომლებიც ზღუდავს უფლებას მონაცემთა დაცვაზე.“ 2019 წლის 25 თებერვალი. edps.europa.eu/sites/edp/files/publication/19-02- 25_proportionality_guidelines_en.pdf

[15] ასევე, იხ. EDPS. „იმ ზომების აუცილებლობის შეფასება, რომლებიც ზღუდავს ფუნდამენტურ უფლებას პერსონალური მონაცემების დაცვაზე: ინსტრუმენტთა კრებული“, https://edps.europa.eu/data-protection/our-work/publications/papers/necessity- toolkit_en

[16] აუცილებლობის შესახებ დამატებით ინფორმაციასთან დაკავშირებით, იხილეთ 29-ე მუხლის სამუშაო ჯგუფის მოსაზრება: „მოსაზრება 06/2014 მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების ლეგიტიმური ინტერესების ცნების შესახებ, 95/46/EC დირექტივის მე-7 მუხლის შესაბამისად“. WP 217, 2014 წლის 9 აპრილი. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

უნდა შემუშავდეს იმგვარად, რაც უზრუნველყოფს თავიდანვე მხოლოდ იმ მინიმალური ოდენობის პერსონალური მონაცემების დამუშავებას, რომელიც აუცილებელია კონკრეტული ოპერაციებისთვის. აღნიშნული საკითხის გათვალისწინება განსაკუთრებით მნიშვნელოვანია, როდესაც მონაცემებზე წვდომა ეძლევა თანამშრომლებს, რომლებსაც სხვადასხვა როლები და მონაცემებზე წვდომის განსხვავებული საჭიროებები გააჩნიათ.

46. სათანადო „ტექნიკური და ორგანიზაციული ზომები“, მონაცემთა დაცვის პირველად პარამეტრად გათვალისწინების კონტექსტში, ამგვარად, გაგებული უნდა იქნეს სწორედ ისე, როგორც ეს განხილულია 2.1.1 ქვეთავში, თუმცა, კონკრეტულად მონაცემთა მინიმიზაციის პრინციპის განხორციელების ჭრილში.

47. ზემოაღნიშნული ვალდებულება, რომელიც გულისხმობს მხოლოდ კონკრეტული მიზნისთვის საჭირო პერსონალური მონაცემების დამუშავებას, ვრცელდება ქვემოთ წარმოდგენილ ელემენტებზე.

2.2.2 მონაცემთა მინიმიზაციის ვალდებულების განზომილებები

48. 25-ე მუხლის მე-2 პუნქტი შეიცავს მონაცემთა მინიმიზაციის ვალდებულების განზომილებათა ჩამონათვალს, ავტომატური დამუშავების შემთხვევაში და მიუთითებს, რომ ეს ვალდებულება [მხოლოდ კონკრეტული მიზნისთვის საჭირო პერსონალური მონაცემების დამუშავება] ვრცელდება შეგროვებული მონაცემების რაოდენობაზე, მონაცემთა დამუშავების მასშტაბებზე, შენახვის ვადებსა და წვდომაზე.

2.2.2.1 „შეგროვებული მონაცემების რაოდენობა“

49. დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა გაითვალისწინონ დამუშავების მიზნებისთვის საჭირო პერსონალური მონაცემების მოცულობა, ტიპები, კატეგორიები და დეტალურობა. მათ მიერ არჩეული [პროდუქტის ან მომსახურების] დიზაინი უნდა ითვალისწინებდეს უსაფრთხოებისა და კონფიდენციალურობის, მონაცემთა მინიმიზაციის და შენახვის შეზღუდვის პრინციპების განხორციელებასთან დაკავშირებით არსებულ მზარდ რისკებს, იმ შემთხვევაში, როდესაც ხდება დიდი ოდენობით დეტალური პერსონალური მონაცემების შეგროვება, რაც შედარებული უნდა იქნეს მონაცემთა სუბიექტების შესახებ უფრო მცირე ოდენობის და/ან ნაკლებად დეტალური ინფორმაციის შეგროვების შედეგად შემცირებულ რისკებთან. ნებისმიერ შემთხვევაში, პირველადი პარამეტრები არ უნდა ითვალისწინებდეს ისეთი პერსონალური მონაცემების შეგროვებას, რომელიც არ არის აუცილებელი დამუშავების კონკრეტული მიზნისთვის. სხვა სიტყვებით რომ ვთქვათ, თუ გარკვეული

კატეგორიის პერსონალური მონაცემები არ არის აუცილებელი ან თუ დეტალური მონაცემები არ არის საჭირო, რადგან ნაკლებად ჩაშლილი მონაცემებიც საკმარისია, მაშინ, არ უნდა მოხდეს რაიმე ზედმეტი პერსონალური მონაცემების შეგროვება.

50. ყველა მომსახურებაზე ვრცელდება ერთი და იგივე ავტომატური მოთხოვნები, იმის მიუხედავად, თუ რა სახის პლატფორმას ან მოწყობილობას იყენებენ ისინი. კერძოდ, დასაშვებია მხოლოდ მოცემული მიზნისთვის აუცილებელი პერსონალური მონაცემების შეგროვება.

2.2.2.2 „მონაცემთა დამუშავების მასშტაბი“

51. დამუშავების[17] ოპერაციები, რომლებიც ხორციელდება პერსონალურ მონაცემებთან მიმართებით, უნდა შემოიფარგლებოდეს იმით, რაც აუცილებელია. დამუშავების სხვადასხვა ოპერაციები უწყობს ხელს დამუშავების მიზნის მიღწევას. თუმცა, ის ფაქტი, რომ გარკვეული პერსონალური მონაცემები საჭიროა მიზნის მისაღწევად, არ ნიშნავს იმას, რომ მონაცემთა მიმართ დასაშვებია ყველა ტიპის და სიხშირის დამუშავების ოპერაციების განხორციელება. დამუშავებისთვის პასუხისმგებელმა პირებმა, აგრეთვე, უნდა გამოიჩინონ სიფრთხილე, რათა არ მოხდეს 6(4) მუხლით გათვალისწინებული „თავსებადი მიზნების“ ფარგლების გაფართოება, და გაითვალისწინონ, თუ რა სახის დამუშავება ხვდება მონაცემთა სუბიექტების გონივრული მოლოდინების ფარგლებში.

2.2.2.3 „მონაცემთა შენახვის ვადა“

52. დაუშვებელია შეგროვებული პერსონალური მონაცემები, თუ ეს არ წარმოადგენს აუცილებლობას დამუშავების მიზნისთვის და არ არსებობს სხვა თავსებადი მიზანი ან სამართლებრივი საფუძველი, 6(4) მუხლის შესაბამისად. მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, დაასაბუთოს, რომ მონაცემთა შენახვა არის აუცილებელი, ანგარიშვალდებულების პრინციპის შესაბამისად.

53. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, შეზღუდოს მონაცემთა შენახვის პერიოდი იმის მიხედვით, რაც საჭიროა დამუშავების მიზნისთვის. თუ პერსონალური მონაცემები აღარ არის საჭირო დამუშავების

[17] GDPR-ის 4(2) მუხლის თანახმად, მონაცემთა დამუშავება მოიცავს ისეთ ქმედებას, როგორიცაა: შეგროვება, აღრიცხვა/ჩაწერა, ორგანიზება, სტრუქტურირება, შენახვა, ადაპტაცია ან შეცვლა, ამოღება, გაცნობა, გამოყენება, გამჟღავნება გადაცემის, გავრცელების ან ხელმისაწვდომობის სხვაგვარად უზრუნველყოფის გზით, დაჯგუფება ან კომბინირება, შეზღუდვა, წაშლა ან განადგურება.

მიზნებისთვის, მაშინ ავტომატურად უნდა მოხდეს მისი წაშლა ან ანონიმიზება. ამრიგად, შენახვის ვადა დამოკიდებულია დამუშავების მიზანზე. აღნიშნული ვალდებულება პირდაპირ არის დაკავშირებული შენახვის შეზღუდვის პრინციპთან, 5(1)(e) მუხლის შესაბამისად, და იგი ავტომატურად უნდა განხორციელდეს, ე.ი., დამუშავებისთვის პასუხისმგებელ პირს დამუშავების პროცესში ინტეგრირებული უნდა ჰქონდეს სისტემატური პროცედურები, რომლებიც უზრუნველყოფს მონაცემთა წაშლას ან ანონიმიზებას.

54. პერსონალური მონაცემების ანონიმიზება[18] წარმოადგენს წაშლის ალტერნატიულ საშუალებას, იმ შემთხვევაში, თუ მოხდება ყველა რელევანტური კონტექსტური ელემენტების გათვალისწინება, ხოლო რეგულარულად შეფასდება რისკის სიმწვავე და ალბათობა, მათ შორის, ხელახლა იდენტიფიცირების რისკისა.[19]

2.2.2.4 „მონაცემთა წვდომა“

55. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, საჭიროების შეფასების საფუძველზე, შეზღუდოს, თუ ვის აქვს წვდომა პერსონალურ მონაცემებზე და რა ტიპის წვდომა და აგრეთვე, უზრუნველყოს, რომ პერსონალური მონაცემები რეალურად იყოს ხელმისაწვდომი მათთვის, ვისაც ეს მონაცემები ესაჭიროება, მაგალითად, კრიტიკულ სიტუაციებში. დამუშავების მიმდინარეობისას, მონაცემთა გადაცემის მთლიანი პროცესის ფარგლებში, უნდა მოქმედებდეს წვდომის მეთვალყურეობის საშუალებები.

56. 25(2) მუხლის თანახმად, უზრუნველყოფილი უნდა იქნეს ფიზიკური პირების განუსაზღვრელი რაოდენობისთვის პერსონალური მონაცემების პირველად პარამეტრად ხელმისაწვდომობის შეზღუდვა, ადამიანური ძალის ჩარევის გარეშე. დამუშავებისთვის პასუხისმგებელმა პირმა პირველად პარამეტრად უნდა შეზღუდოს მისაწვდომობა და მონაცემთა სუბიექტს უნდა მისცეს შესაძლებლობა, განახორციელოს ჩარევა მისი პერსონალური მონაცემების გამოქვეყნებამდე ან ფიზიკური პირების განუსაზღვრელი რაოდენობისთვის სხვაგვარი ხელმისაწვდომობის უზრუნველყოფამდე.

[18] 29-ე მუხლის სამუშაო ჯგუფი. “დასკვნა 05/2014 ანონიმიზაციის ტექნიკებზე”. WP 216, 2014 წლის 10 აპრილი. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[19] იხ. GDPR-ის 4(1) მუხლი, პრეამბულის 26-ე პუნქტი. 29-ე მუხლის სამუშაო ჯგუფი. “დასკვნა 05/2014 ანონიმიზაციის ტექნიკებზე”. იხ. ქვესექცია „შენახვის შეზღუდვის“ შესახებ, რომლის მიხედვითაც დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს განხორციელებული ანონიმიზების მექანიზმების ეფექტურობა.

57. პერსონალური მონაცემების მისაწვდომობის უზრუნველყოფა ფიზიკური პირების განუსაზღვრელი რაოდენობისთვის, სავარაუდოდ, გამოიწვევს პერსონალური მონაცემების იმაზე მასშტაბურ გავრცელებას, ვიდრე ეს თავდაპირველად იყო განზრახული. ეს განსაკუთრებით რელევანტურია ინტერნეტისა და საძიებო სისტემების კონტექსტში. ეს ნიშნავს, რომ დამუშავებისთვის პასუხისმგებელმა პირმა პირველად პარამეტრად, მონაცემთა სუბიექტებს უნდა მისცეს შესაძლებლობა, განახორციელონ ჩარევა მანამ, სანამ პერსონალური მონაცემები ღია ინტერნეტში გახდება ხელმისაწვდომი. ეს განსაკუთრებით მნიშვნელოვანია, როდესაც საქმე ეხება ბავშვებს და მოწყვლად ჯგუფებს.

58. დამუშავების სამართლებრივი საფუძვლების შესაბამისად, ინტერვენციის განხორციელების შესაძლებლობა განსხვავდება დამუშავების კონტექსტის მიხედვით. მაგალითად, პერსონალური მონაცემების საჯაროდ გამოქვეყნებისთვის მონაცემთა სუბიექტისგან თანხმობის გამოთხოვნა ან მონაცემთა დაცვის იმგვარი პარამეტრების უზრუნველყოფა, რომელიც მონაცემთა სუბიექტებს საშუალებას მისცემს, თავად აკონტროლონ საკუთარი მონაცემების საჯარო ხელმისაწვდომობა.

59. იმ შემთხვევაშიც, თუ პერსონალური მონაცემები საჯაროდ ხელმისაწვდომი გახდა მონაცემთა სუბიექტის თანხმობის და ინფორმირებულობის საფუძველზე, ეს არ ნიშნავს იმას, რომ ნებისმიერ სხვა დამუშავებისთვის პასუხისმგებელ პირს, რომელსაც აქვს წვდომა ამ მონაცემებზე, უფლება აქვს, მონაცემები საკუთარი მიზნებისთვის თავად დაამუშაოს - ამ შემთხვევაში, უნდა არსებობდეს შესაბამისი სამართლებრივი საფუძველი.[20]

3. მონაცემთა დაცვის პრინციპების განხორციელება პერსონალური მონაცემების დამუშავებისას, „მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში და მონაცემთა დაცვა პირველად პარამეტრად“ პრინციპის საფუძველზე

60. დამუშავების აქტივობების ფორმირების ყველა ეტაპზე, მათ შორის: შესყიდვა, ტენდერები, აუთსორსინგი, განვითარება, მხარდაჭერა, მოვლა-პატრონობა, ტესტირება, შენახვა, წაშლა და ა.შ., დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს DPbDD-ის სხვადასხვა ელემენტები, რომლებიც

[20] იხ. საქმე Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland no. 931/13.

წინამდებარე თავში განხილულია კონკრეტული მაგალითების გამოყენებით, ამ პრინციპების იმპლემენტაციის კონტექსტში.[21] [22] [23]

61. საჭიროა, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა განახორციელონ კონკრეტული პრინციპები, რათა უზრუნველყონ DPbDD მოთხოვნებთან შესაბამისობა. ეს პრინციპებია: გამჭვირვალობა, კანონიერება, სამართლიანობა, მიზნის შეზღუდვა, მონაცემთა მინიმიზაცია, სიზუსტე, შენახვის შეზღუდვა, უსაფრთხოება და კონფიდენციალურობა და ანგარიშვალდებულება. ეს პრინციპები ჩამოყალიბებულია GDPR-ის მე-5 მუხლში და პრეამბულის 39-ე პუნქტში. DPbDD-ის განხორციელების გზების შესახებ სრული ინფორმირებულობა მოითხოვს თითოეული ამ პრინციპის მნიშვნელობის გააზრებას.

62. DPbDD-ის ამოქმედების მაგალითებთან ერთად, ჩვენ შევიმუშავეთ **DPbDD-ის ძირითადი ელემენტების** ჩამონათვალი თითოეულ პრინციპთან დაკავშირებით. თითოეული მაგალითი ეხება მონაცემთა დაცვის კონკრეტულ პრინციპს, თუმცა, ეს მაგალითები მჭიდროდ არის დაკავშირებული სხვა შესაბამის პრინციპებთან. EDPB ხაზს უსვამს, რომ აქ წარმოდგენილი ძირითადი ელემენტები და მაგალითები არც ამომწურავია და არც სავალდებულო ძალის მქონე, არამედ, მათი მიზანია, უზრუნველყოს სახელმძღვანელო ელემენტები თითოეულ პრინციპთან დაკავშირებით. დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა შეაფასონ, თუ როგორ უნდა უზრუნველყონ პრინციპებთან შესაბამისობა, დამუშავების კონკრეტული ოპერაციის კონტექსტში.

63. მართალია, წინამდებარე სექცია ყურადღებას ამახვილებს პრინციპები იმპლემენტაციაზე, დამუშავებისთვის პასუხისმგებელმა პირმა, ამავდროულად, უნდა უზრუნველყოს მონაცემთა სუბიექტების უფლებების დაცვის შესაფერისი და ეფექტური გზების განხორციელება, GDPR-ის III თავის შესაბამისად, თუ ამას სავალდებულოდ არ ითხოვს თავად პრინციპები.

64. ანგარიშვალდებულების პრინციპი არის ყოვლისმომცველი: კერძოდ, ამ პრინციპის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს ეკისრება პასუხისმგებლობა, აირჩიოს საჭირო ტექნიკა და ორგანიზაციული ზომები.

[21] დამატებითი მაგალითებისთვის, იხ: Norwegian Data Protection Authority. “Software Development with Data Protection by Design and by Default”. 2017 წლის 28 ნოემბერი. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

3.1 გამჭვირვალობა[24]

65. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტს მიაწოდოს ინფორმაცია მკაფიოდ და ღიად იმის შესახებ, თუ როგორ მოახდენს პერსონალური მონაცემების შეგროვებას, გამოყენებას და გაზიარებას. გამჭვირვალობა გულისხმობს მონაცემთა სუბიექტის მხარდაჭერას, გაიაზროს და საჭიროების შემთხვევაში, გამოიყენოს მე-15-22-ე მუხლებით გათვალისწინებული უფლებები. ეს პრინციპი გათვალისწინებულია მე-12, მე-13, მე-14 და 34-ე მუხლებით. ამ მუხლების განხორციელებას, აგრეთვე, ხელს უნდა უწყობდეს გამჭვირვალობის პრინციპის უზრუნველყოფისთვის დანერგილი ზომები და დაცვის მექანიზმები.

66. გამჭვირვალობის პრინციპთან დაკავშირებით, მოქმედებს შემდეგი ძირითადი DPbDD ელემენტები:
    - მკაფიოობა - ინფორმაცია უნდა იყოს მკაფიო და მარტივ ენაზე წარმოდგენილი, ლაკონური და გასაგები.
    - სემანტიკა - კომუნიკაციას უნდა იყოს სამიზნე აუდიტორიისათვის მკაფიოდ გასაგები.
    - მისაწვდომობა - ინფორმაცია ადვილად მისაწვდომი უნდა იყოს მონაცემთა სუბიექტისათვის.
    - კონტექსტუალური - ინფორმაცია მონაცემთა სუბიექტს უნდა მიეწოდოს შესაბამის დროს და შესაბამისი ფორმით.
    - რელევანტუროობა - ინფორმაცია უნდა იყოს კონკრეტული მონაცემთა სუბიექტისათვის რელევანტური და მისთვის შესაფერისი.
    - უნივერსალური დიზაინი - ინფორმაცია მისაწვდომი უნდა იყოს ყველა მონაცემთა სუბიექტისათვის, ითვალისწინებდეს ელექტრონულად წაკითხვად ენებს, რაც ხელს შეუწყობს და ავტომატურს გახდის წაკითხვადობას და მკაფიოობას.
    - გასაგები - მონაცემთა სუბიექტებს უნდა ჰქონდეთ სათანადო წარმოდგენა იმაზე, თუ რას უნდა მოელოდნენ მათი პერსონალური მონაცემების დამუშავებასთან დაკავშირებით, განსაკუთრებით, როდესაც მონაცემთა სუბიექტები ბავშვები ან სხვა მოწყვლადი ჯგუფები არიან.
    - სხვადასხვა არხების გამოყენება - ინფორმაციის მიწოდება უნდა მოხდეს სხვადასხვა არხებით და მედია საშუალებებით, არა მხოლოდ ტექსტობრივი ინფორმაციის, რაც ხელს შეუწყობს ინფორმაციის მონაცემთა სუბიექტამდე ეფექტურად მიტანას.

[24] გამჭვირვალობის კონცეფცია განმარტებულია 29-ე მუხლის სამუშაო ჯგუფის დოკუმენტში „სახელმძღვანელო პრინციპები გამჭვირვალობის შესახებ, 2016/679 რეგულაციის თანახმად“. WP 260 rev.01, 2018 წლის 11 აპრილი. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 - აღიარებულია EDPB-ის მიერ.

- მრავალშრიანი - ინფორმაცია უნდა იყოს მრავალშრიანი, რაც უზრუნველყოფს ბალანსის დამყარებას ინფორმაციის სისრულესა და გააზრებას შორის, მონაცემთა სუბიექტების გონივრული მოლოდინების შესაბამისად.

მაგალითი[25]

დამუშავებისთვის პასუხისმგებელი პირი საკუთარი ვებგვერდისთვის მონაცემთა დაცვის პოლიტიკის შემუშავებას ახორციელებს, რათა შეასრულოს გამჭვირვალობასთან დაკავშირებული მოთხოვნები. მონაცემთა დაცვის პოლიტიკა არ უნდა შეიცავდეს მოცულობით ინფორმაციას, რომელიც საშუალო მონაცემთა სუბიექტისათვის რთული აღსაქმელი და გასააზრებელია. არამედ, ინფორმაცია მკაფიო და ლაკონური ენით უნდა იყოს დაწერილი და ვებგვერდის მომხმარებელს უნდა უადვილებდეს იმის გააზრებას, თუ როგორ მუშავდება მათი პერსონალური მონაცემები. შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი ინფორმაციას წარმოადგენს მრავალშრიანი ფორმით, სადაც ხაზგასმულია ყველაზე მნიშვნელოვანი საკითხები. უფრო დეტალური ინფორმაცია კი ადვილად არის ხელმისაწვდომი. ჩამოსაშლელი მენიუები და სხვა გვერდებზე გადასასვლელი ბმულები უზრუნველყოფილია პოლიტიკაში გამოყენებული სხვადასხვა პუნქტების და კონცეფციების განსამარტად. დამუშავებისთვის პასუხისმგებელი პირი აგრეთვე, უზრუნველყოფს ინფორმაციის მიწოდებას სხვადასხვა არხებით, ვიდეო-კლიპების საშუალებით განმარტავს წერილობით ინფორმაციაში წარმოდგენილ ყველაზე მნიშვნელოვან საკითხებს. სხვადასხვა გვერდებს შორის სინერგია სასიცოცხლოდ მნიშვნელოვანია იმისათვის, რომ მრავალშრიანმა მიდგომამ შეამციროს და არ გაამძაფროს მონაცემთა სუბიექტის დაბნეულობა.

მონაცემთა დაცვის პოლიტიკა მონაცემთა სუბიექტებისთვის ადვილად მისაწვდომი უნდა იყოს. ამრიგად, მონაცემთა დაცვის პოლიტიკა ხელმისაწვდომია და ხილვადია მოცემული ვებსაიტის ყველა გვერდზე, რათა მონაცემთა სუბიექტს ყოველთვის შეეძლოს ერთი დაწკაპუნებით გადასვლა ინფორმაციაზე. წარმოდგენილი ინფორმაცია შემუშავებულია საუკეთესო პრაქტიკის და უნივერსალური დიზაინის სტანდარტების შესაბამისად, რათა იგი ყველასათვის იყოს ხელმისაწვდომი.

ამას გარდა, საჭირო ინფორმაცია წარმოდგენილი უნდა იქნეს სწორ კონტექსტში, შესაბამის დროს. ვინაიდან დამუშავებისთვის პასუხისმგებელი პირი ვებგვერდზე შეგროვებული მონაცემების გამოყენებით ახორციელებს დამუშავების სხვადასხვა ოპერაციებს, მხოლოდ ვებსაიტზე განთავსებული მონაცემთა დაცვის ზოგადი პოლიტიკა არ არის საკმარისი, რათა დამუშავებისთვის პასუხისმგებელმა პირმა დააკმაყოფილოს გამჭვირვალობის მოთხოვნა. შესაბამისად, დამუშავებისთვის

[25] მონაცემთა დაცვის სააგენტომ საფრანგეთში გამოაქვეყნა რამდენიმე მაგალითი, რომლებიც ასახავს მომხმარებლების ინფორმირების საუკეთესო პრაქტიკას და გამჭვირვალობის სხვა პრინციპებს: https://design.cnil.fr/en/.

პასუხისმგებელი პირი ქმნის ინფორმაციის ნაკადს, მონაცემთა სუბიექტს წარუდგენს რელევანტურ ინფორმაციას შესაბამის კონტექსტებში და ამისათვის იყენებს, მაგ., ინფორმაციულ ამონარიდებს ან პოპ-აპ ფანჯრებს. მაგალითად, როდესაც იგი მონაცემთა სუბიექტს სთხოვს, შეიყვანოს პერსონალური მონაცემები, ამავდროულად მას აწვდის ინფორმაციას, თუ როგორ მოხდება პერსონალური მონაცემების დამუშავება და რატომ არის პერსონალური მონაცემების აუცილებელი დამუშავებისთვის.

3.2 კანონიერება

67. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მოახდინოს ქმედითი სამართლებრივი საფუძვლის იდენტიფიცირება პერსონალური მონაცემების დასამუშავებლად. გამოყენებული ზომები და დაცვის მექანიზმები ხელს უნდა უწყობდეს დამუშავების მთლიანი ცხოვრების ციკლის დამუშავების შესაბამის სამართლებრივ საფუძველთან შესაბამისობაში მოყვანას.

68. კანონიერების პრინციპთან დაკავშირებით, მოქმედებს შემდეგი ძირითადი DPbDD ელემენტები:
    - რელევანტურობა - დამუშავების მიმართ გამოყენებული უნდა იქნეს სწორი სამართლებრივი საფუძველი.
    - დიფერენციაცია[26] - თითოეული დამუშავების აქტივობის მიმართ გამოყენებული სამართლებრივი საფუძველი უნდა იყოს დიფერენცირებული.
    - კონკრეტული მიზანი - სათანადო სამართლებრივი საფუძველი მკაფიოდ უნდა იყოს დაკავშირებული დამუშავების კონკრეტულ მიზანთან.[27]
    - აუცილებლობა - დამუშავება უნდა იყოს აუცილებელი და უპირობოდ მნიშვნელოვანი კონკრეტული მიზნისთვის, რათა იგი იყოს კანონიერი.
    - ავტონომია - მონაცემთა სუბიექტს უნდა მიენიჭოს ავტონომიის ყველაზე მაღალი ხარისხი, რამდენადაც ეს შესაძლებელია, რათა სამართლებრივი საფუძვლის ფარგლებში მან შეძლოს კონტროლის დამყარება საკუთარ პერსონალურ მონაცემებზე.

[26] EDPB. "სახელმძღვანელო პრინციპები 2/2019 პერსონალური მონაცემების დამუშავების შესახებ, GDPR-ის 6(1)(b) მუხლის შესაბამისად, მონაცემთა სუბიექტებისათვის ონლაინ სერვისების უზრუნველყოფის კონტექსტში." ვერსია 2.0, 2019 წლის 8 ოქტომბერი. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

[27] იხ. სექცია შეზღუდვის შესახებ, ქვემოთ.

- თანხმობის მოპოვება - თანხმობა უნდა იყოს ნებაყოფლობითი, კონკრეტული, ინფორმირებული და მკაფიო.[28] განსაკუთრებული ყურადღება უნდა გამახვილდეს ბავშვების და ახალგაზრდების ქმედუნარიანობაზე ინფორმირებული თანხმობის გაცემის კუთხით.
- თანხმობის უკან გახმობა - თუ სამართლებრივ საფუძველს წარმოადგენს თანხმობა, დამუშავება უნდა იძლეოდეს თანხმობის უკან გახმობის შესაძლებლობას. თანხმობის უკან გახმობა უნდა იყოს ისეთივე მარტივი, როგორც თანხმობის მიცემა. წინააღმდეგ შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირის თანხმობის მექანიზმი არ იქნება GDPR-თან შესაბამისობაში.[29]
- ინტერესთა დაბალანსება - თუ სამართლებრივ საფუძველს წარმოადგენს ლეგიტიმური ინტერესები, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს ინტერესთა დაბალანსება და განსაკუთრებული ყურადღება მიაქციოს ძალთა დისბალანსს, განსაკუთრებით, 18 წლამდე ბავშვების და სხვა მოწყვლადი ჯგუფების შემთხვევაში. უნდა არსებობდეს ზომები და დაცვის მექანიზმები, რომლებიც გაანეიტრალებს მონაცემთა სუბიექტებზე უარყოფით ზემოქმედებას.
- წინასწარ განსაზღვრა - სამართლებრივი საფუძველი უნდა დადგინდეს მანამ, სანამ დაიწყება დამუშავება.
- შეწყვეტა - თუ სამართლებრივი საფუძველი აღარ მოქმედებს, დამუშავება შესაბამისად უნდა შეწყდეს.
- კორექტივების შეტანა - თუ დამუშავების სამართლებრივ საფუძველში განხორციელდა ლეგიტიმური ცვლილება, მაშინ დამუშავებაში შეტანილი უნდა იქნეს კორექტივები, ახალი სამართლებრივი საფუძვლის შესაბამისად.[30]
- პასუხისმგებლობის განაწილება - როდესაც გათვალისწინებულია ერთობლივი დამუშავება, მხარეებმა მკაფიოდ და გამჭვირვალედ უნდა განსაზღვრონ თავიანთი პასუხისმგებლობები მონაცემთა სუბიექტის მიმართ და შექმნან დამუშავების ზომები აღნიშნული განაწილების შესაბამისად.

მაგალითი

[28] იხ. სახელმძღვანელო პრინციპები 05/2020 თანხმობის შესახებ, 2016/679 რეგულაციის შესაბამისად. https://edpb.europa.eu/our-work- tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] იხ. სახელმძღვანელო პრინციპები 05/2020 თანხმობის შესახებ, 2016/679 რეგულაციის შესაბამისად, გვ. 24. https://edpb.europa.eu/our-work- tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[30] თუ თავდაპირველი სამართლებრივი საფუძველი არის თანხმობა, იხ. სახელმძღვანელო პრინციპები 05/2020 თანხმობის შესახებ 2016/679 რეგულაციის შესაბამისად. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under- regulation-2016679_en

ბანკი აპირებს, რომ სასესხო განაცხადების მართვის ეფექტურობის გასაუმჯობესებლად შეიმუშაოს შესაბამისი მომსახურება. იდეა მდგომარეობს იმაში, რომ ბანკი მომხმარებლებისგან ითხოვს ნებართვას, რომლის საფუძველზეც შეძლებს, პირდაპირ საგადასახადო ორგანოსგან მომხმარებლის შესახებ გამოითხოვოს ინფორმაცია. ეს მაგალითი არ ითვალისწინებს სხვა წყაროებიდან მიღებული პერსონალური მონაცემების დამუშავებას.

პერსონალური მონაცემების მოპოვება მონაცემთა სუბიექტის ფინანსური მდგომარეობის შესახებ აუცილებელია, რათა გადაიდგას ნაბიჯები, მონაცემთა სუბიექტის მოთხოვნით, სასესხო ხელშეკრულების გაფორმებამდე.[31] ამავდროულად, პერსონალური მონაცემების პირდაპირ საგადასახადო ორგანოსგან შეგროვება არ წარმოადგენს აუცილებლობას, რადგან მომხმარებელს შეუძლია, ხელშეკრულება გააფორმოს მას შემდეგ, რაც თავად მიაწვდის ბანკს საგადასახადო ორგანოსგან მიღებულ ინფორმაციას. ამავდროულად, ბანკს ლეგიტიმური ინტერესი აქვს დოკუმენტაციის პირდაპირ საგადასახადო ორგანოსგან მიღებაში, რათა, მაგალითად, უზრუნველყოფილი იქნეს სასესხო განაცხადის ეფექტურად დამუშავება. ბანკებისათვის განმცხადებელთა პერსონალურ მონაცემებზე ამგვარი პირდაპირი წვდომის უზრუნველყოფა წვდომის უფლებების გამოყენებასთან ან ბოროტად გამოყენებასთან დაკავშირებით გარკვეულ რისკებს წარმოშობს.

კანონიერების პრინციპის განხორციელებისას, დამუშავებისთვის პასუხისმგებელი პირი აცნობიერებს, რომ ამ კონტექსტში იგი ვერ შეძლებს „აუცილებელია ხელშეკრულებისთვის“ საფუძვლის გამოყენებას დამუშავების იმ ნაწილისთვის, რომელიც გულისხმობს პერსონალური მონაცემების პირდაპირ საგადასახადო ორგანოსგან მიღებას. ის ფაქტი, რომ დამუშავების მოცემული შემთხვევა ქმნის საფრთხეს იმისა, რომ მონაცემთა სუბიექტი ნაკლებად იქნება ჩართული საკუთარი მონაცემების დამუშავებაში, კიდევ ერთი რელევანტური ფაქტორია, რომელიც დამუშავების კანონიერების შესაფასებლად უნდა იქნეს გათვალისწინებული. ბანკი ასკვნის, რომ დამუშავების ეს ნაწილი უნდა დაეყრდნოს სხვა სამართლებრივ საფუძველს. წევრ სახელმწიფოში, სადაც დამუშავებისთვის პასუხისმგებელი პირი მდებარეობს, მოქმედებს ეროვნული კანონმდებლობა, რომელიც ბანკს საშუალებას აძლევს, პირდაპირ საგადასახადო ორგანოებისგან მოიპოვოს ინფორმაცია იმ შემთხვევაში, თუ მონაცემთა სუბიექტი წინასწარ გასცემს თანხმობას ამასთან დაკავშირებით.

შესაბამისად, ბანკი დამუშავების შესახებ ინფორმაციას განათავსებს განცხადებათა ონლაინ პლატფორმაზე, რათა მონაცემთა სუბიექტისათვის გასაგები იყოს, თუ რომელი დამუშავებაა სავალდებულო და რომელი არასავალდებულო. დამუშავების ვარიანტები არ იძლევა ავტომატურად მონაცემების პირდაპირ სხვა წყაროებიდან (გარდა მონაცემთა სუბიექტისა) მოპოვების შესაძლებლობას, ხოლო მონაცემთა

[31] იხ. GDPR-ის 6(1)(b) მუხლი.

პირდაპირი მოპოვების ვარიანტის შესახებ წარმოდგენილია იმგვარად, რომ მონაცემთა სუბიექტს არ ართმევს უარის თქმის შესაძლებლობას. პირდაპირ სხვა დამუშავებისთვის პასუხისმგებელი პირისგან მიღებული მონაცემების დამუშავებაზე ნებისმიერი თანხმობა არის კონკრეტულ ინფორმაციაზე წვდომის დროებითი უფლება.

გაცემული თანხმობა მუშავდება ელექტრონულად, დოკუმენტირებადი ფორმით, ხოლო მონაცემთა სუბიექტები უზრუნველყოფილები არიან მარტივი საშუალებით, აკონტროლონ, თუ რაზე გასცეს თანხმობა და უკან გაიხმონ იგი.

დამუშავებისთვის პასუხისმგებელმა პირმა წინასწარ შეაფასა DPbDD მოთხოვნები და პლატფორმის შესყიდვისთვის გამოცხადებული ტენდერის სპეციფიკაციებში გაითვალისწინა ყველა შესაბამისი კრიტერიუმი. დამუშავებისთვის პასუხისმგებელი პირისთვის ცნობილია, რომ თუ იგი არ გაითვალისწინებს DPbDD მოთხოვნებს ტენდერში, შესაძლოა, მონაცემთა დაცვის განხორციელება შემდგომ დაგვიანებული იყოს ან ძალიან ძვირი დაჯდეს.

3.3 სამართლიანობა

69. სამართლიანობა ყოვლისმომცველი პრინციპია, რომლის თანახმადაც პერსონალური მონაცემები არ უნდა დამუშავდეს იმგვარად, რაც მონაცემთა სუბიექტს მიაყენებს უსამართლო ზიანს, გამოიწვევს უკანონო დისკრიმინაციას მის მიმართ, იქნება მისთვის მოულოდნელი ან დამაბნეველი. ზომები და დაცვის მექანიზმები, რომლებიც უზრუნველყოფს სამართლიანობის პრინციპის განხორციელებას, აგრეთვე, ხელს უწყობს მონაცემთა სუბიექტების უფლებებს და თავისუფლებებს, კერძოდ, ინფორმაციის უფლებას (გამჭვირვალობა), ინტერვენციის განხორციელების უფლებას (წვდომა, წაშლა, მონაცემთა პორტირება, გასწორება) და დამუშავების შეზღუდვის უფლებას (უფლება, არ დაექვემდებაროს ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღებას და მონაცემთა სუბიექტების დისკრიმინაციის აკრძალვა ამგვარ პროცესებში).

70. სამართლიანობის პრინციპთან დაკავშირებით, მოქმედებს შემდეგი ძირითადი DPbDD ელემენტები:
    - ავტონომია - მონაცემთა სუბიექტებს უნდა მიენიჭოთ ყველაზე მაღალი ხარისხის ავტონომია, რამდენადაც შესაძლებელია, რათა თავად განსაზღვრონ საკუთარი პერსონალური მონაცემების გამოყენება და აგრეთვე, მონაცემთა გამოყენების ან დამუშავების ფარგლები და პირობები.

- ინტერაქცია - მონაცემთა სუბიექტებს უნდა შეეძლოთ კომუნიკაციისა და საკუთარი უფლებების განხორციელება, დამუშავებაზე პასუხისმგებელი პირის მიერ მათი პერსონალური მონაცემების დამუშავებასთან დაკავშირებით.
- მოლოდინი - დამუშავება უნდა შეესაბამებოდეს მონაცემთა სუბიექტების გონივრულ მოლოდინებს.
- დისკრიმინაციის აკრძალვა - დამუშავებისთვის პასუხისმგებელმა პირმა უსამართლო დისკრიმინაცია არ უნდა განახორციელოს მონაცემთა სუბიექტების მიმართ.
- ექსპლუატაციის აკრძალვა - დამუშავებისთვის პასუხისმგებელმა პირმა არ უნდა მოახდინოს მონაცემთა სუბიექტების საჭიროებების ან მოწყვლადობის ექსპლუატაცია.
- მომხმარებლის არჩევანი - დამუშავებისთვის პასუხისმგებელმა პირმა საკუთარი მომხმარებლების არჩევანი უსამართლოდ არ უნდა შეზღუდოს. როდესაც სერვისი, რომელიც ამუშავებს პერსონალურ მონაცემებს არის კერძო საკუთრება, ამან შესაძლოა, მომხმარებელს შეუზღუდოს სერვისის არჩევანი უსამართლოდ, თუ მონაცემთა სუბიექტს არ შეეძლება მონაცემთა პორტირების უფლების განხორციელება, მე-20 მუხლის შესაბამისად.
- ძალთა ბალანსი - ძალთა ბალანსი უნდა წარმოადგენდეს დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის არსებული ურთიერთობის ძირითად მიზანს. ძალთა დისბალანსი თავიდან უნდა იქნეს აცილებული. თუ ეს შეუძლებელია, საჭიროა დისბალანსის აღიარება და გათვალისწინება და სათანადო საპასუხო ზომების მიღება.
- რისკის გადაცემის დაუშვებლობა - დამუშავებისთვის პასუხისმგებელმა პირმა საწარმოს რისკები არ უნდა გადასცეს მონაცემთა სუბიექტებს.
- არ მოტყუება - მონაცემთა დამუშავების შესახებ ინფორმაცია და ვარიანტები მონაცემთა სუბიექტს უნდა განემარტოს ობიექტურად და ნეიტრალურად. თავიდან უნდა იქნეს აცილებული შეცდომაში შემყვანი ან მანიპულაციური ენის ან დიზაინის გამოყენება.
- უფლებების პატივისცემა - დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, პატივი სცეს მონაცემთა სუბიექტების ფუნდამენტურ უფლებებს და განახორციელოს სათანადო ზომები და დაცვის მექანიზმები. მან არ უნდა შეზღუდოს აღნიშნული უფლებები, გარდა იმ შემთხვევისა, თუ ეს ცალსახად არის გამართლებული კანონის შესაბამისად.
- ეთიკური - დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, აღიქვას დამუშავების ფართო გავლენა ფიზიკური პირების უფლებებზე და ღირსებაზე.

- კეთილსინდისიერება - დამუშავებისთვის პასუხისმგებელმა პირმა ხელმისაწვდომი უნდა გახადოს ინფორმაცია იმის შესახებ, თუ როგორ ამუშავებს პერსონალურ მონაცემებს; უნდა მოიქცეს ისე, როგორც აცხადებს, რომ მოიქცევა და შეცდომაში არ უნდა შეიყვანოს მონაცემთა სუბიექტი.
- ადამიანური ინტერვენცია - დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს *კვალიფიციური* ადამიანური ინტერვენციის განხორციელება, რომელიც მოახდენს ყველა იმ მიკერძოების გამოვლენას, რომელსაც ქმნიან კომპიუტერული ტექნოლოგიები, რაც შეესაბამება მონაცემთა სუბიექტის უფლებას, არ დაექვემდებაროს ავტომატური ინდივიდუალური გადაწყვეტილებების მიღებას (მუხლი 22).[32]
- სამართლიანი ალგორითმები - რეგულარულად შეაფასოს, ფუნქციონირებს თუ არა ალგორითმები მიზნების შესაბამისად და შეიტანოს კორექტივები ალგორითმებში, გამოვლენილი მიკერძოებების გასანეიტრალებლად და უზრუნველყოს დამუშავების სამართლიანობა. მონაცემთა სუბიექტები ინფორმირებულები უნდა იყვნენ მათი პერსონალური მონაცემების ალგორითმების საფუძველზე დამუშავების შესახებ, რის საფუძველზეც მონაცემთა სუბიექტებთან მიმართებით ხორციელდება პროგნოზირება და ანალიზი, მაგალითად, სამუშაოს შესრულების ეფექტურობის, ეკონომიკური მდგომარეობს, ჯანმრთელობის, პერსონალური პრეფერენციების, საიმედოობის ან ქცევის, ადგილმდებარეობის ან გადაადგილებების შესახებ.[33]

<u>მაგალითი 1</u>

დამუშავებისთვის პასუხისმგებელი პირი იყენებს საძიებო სისტემას, რომელიც ძირითადად ამუშავებს მომხმარებლის მიერ გენერირებულ პერსონალურ მონაცემებს. დამუშავებისთვის პასუხისმგებელი პირი სარგებელს იღებს დიდი მოცულობით პერსონალური მონაცემების ფლობის და ამ მონაცემების მიზნობრივი რეკლამებისთვის გამოყენების შედეგად. შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირს სურს, რომ გავლენა მოახდინოს მონაცემთა სუბიექტებზე, რათა გაზარდოს მათი პერსონალური მონაცემების შეგროვების და გამოყენების მასშტაბები.

[32] იხ. სახელმძღვანელო პრინციპები ავტომატიზებული ინდივიდუალური გადაწყვეტილებების მიღების და პროფილირების შესახებ, 2016/79 რეგულაციის მიზნებისთვის.
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826
[33] იხ. GDPR-ის პრეამბულა, პუნქტი 71.

სამართლიანობის პრინციპის განხორციელებისას, დამუშავების ხასიათის, ფარგლების, კონტექსტის და მიზნის გათვალისწინებით, დამუშავებისთვის პასუხისმგებელი პირი აცნობიერებს, რომ დაუშვებელია ვარიანტების წარდგენა იმგვარად, რაც მონაცემთა სუბიექტს უბიძგებს, რომ დამუშავებისთვის პასუხისმგებელ პირს მისცეს უფლება შეაგროვოს იმაზე მეტი პერსონალური მონაცემები, ვიდრე მონაცემები, რომელთა დამუშავების უფლებასაც მისცემდა, ვარიანტები თანასწორი ან ნეიტრალური ფორმით რომ ყოფილიყო წარმოდგენილი. ეს ნიშნავს იმას, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დამუშავების ვარიანტები არ უნდა წარადგინოს იმგვარად, რაც მონაცემთა სუბიექტს ხელს უშლის საკუთარი მონაცემების გაზიარებისგან თავის შეკავებაში ან მონაცემთა დაცვის პარამეტრებში შესწორების შეტანაში და დამუშავების შეზღუდვაში. ეს მაგალითები დიზაინის „შეცდომაში შემყვანი მოდელების“ (dark patterns) მაგალითებია, რაც 25-ე მუხლის სულისკვეთებას ეწინააღმდეგება. დამუშავების პირველადი პარამეტრები არ უნდა იყოს ინვაზიური, ხოლო შემდგომი დამუშავების შესაძლებლობა წარმოდგენილი უნდა იყოს იმგვარი ფორმით, რაც მონაცემთა სუბიექტს არ განაცდევინებს ზეწოლას თანხმობის მისაცემად. ამრიგად, დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტს წარუდგენს ორ ვარიანტს - გააკეთოს არჩევანი თანხმობის გაცემას ან თანხმობის გაცემისგან თავის შეკავებას შორის. ამ ვარიანტებს წარადგენს თანაბრად ხილული ფორმით და მონაცემთა სუბიექტს ზუსტად განუმარტავს თითოეული არჩევანის შედეგებს.

<u>მაგალითი 2</u>

დამუშავებისთვის პასუხისმგებელი პირი პერსონალურ მონაცემებს ამუშავებს სტრიმინგის სერვისის მიზნებისთვის, რათა მომხმარებლებმა გააკეთონ არჩევანი მომსახურების სტანდარტულ და პრემიუმ პაკეტებს შორის. პრემიუმ პაკეტის ფარგლებში, გამომწერები პრიორიტეტულ მომხმარებელთა მომსახურებას.

სამართლიანობის პრინციპთან დაკავშირებით, დაუშვებელია, რომ პრიორიტეტულ მომხმარებელთა სერვისმა, რომელიც პრემიუმ პაკეტის გამომწერები სარგებლობენ, დისკრიმინაციას დაუქვემდებაროს სტანდარტული პაკეტის გამომწერები, საკუთარი უფლებების განხორციელებაზე წვდომის კუთხით, GDPR-ის მე-12 მუხლის თანახმად. ეს ნიშნავს იმას, რომ მართალია პრემიუმ პაკეტის გამომწერები იღებენ პრიორიტეტულ მომსახურებას, დაუშვებელია, რომ ამგვარმა უპირატესობამ გამოიწვიოს რეგულარული პაკეტის გამომწერთა მოთხოვნაზე დროული რეაგირებისთვის სათანადო ზომების ნაკლებობა. კერძოდ, რეაგირება უნდა განხორციელდეს დაუსაბუთებელი გაჭიანურების გარეშე და ნებისმიერ შემთხვევაში, რეაგირების ვადა არ უნდა აღემატებოდეს მოთხოვნის მიღებიდან ერთ თვეს.

პრიორიტეტული მომხმარებლები დამატებით საფასურს იხდიან უკეთესი სერვისის მისაღებად, თუმცა, ყველა მონაცემთა სუბიექტს უნდა ჰქონდეს თანაბარი და დისკრიმინაციის გარეშე წვდომა, რათა მოხდეს მათი უფლებებისა და თავისუფლებების აღსრულება, მე-12 მუხლის მოთხოვნათა შესაბამისად.

3.4 მიზნის შეზღუდვა[34]

71. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემები შეაგროვოს კონკრეტული, ცალსახა და ლეგიტიმური მიზნებისთვის და არ მოახდინოს მონაცემთა შემდგომი დამუშავება იმგვარად, რაც არ იქნება თავსებადი მათი შეგროვების მიზანთან.[35] შესაბამისად, დამუშავების დიზაინი უნდა განისაზღვროს იმის მიხედვით, თუ რა არის აუცილებელი დამუშავების მიზნების მისაღწევად. თუ განხორციელდება დამატებითი დამუშავება, დამუშავებისთვის პასუხისმგებელმა პირმა პირველ რიგში, უნდა უზრუნველყოს, რომ დამუშავების მიზნები თავსებადია თავდაპირველ მიზნებთან და შესაბამისად დაგეგმოს დამუშავება. ის, თუ რამდენად თავსებადია ახალი მიზანი თავდაპირველ მიზანთან, უნდა შეფასდეს 6(4) მუხლში წარმოდგენილი კრიტერიუმების შესაბამისად.

72. მიზნის შეზღუდვასთან დაკავშირებით, მოქმედებს შემდეგი ძირითადი DPbDD ელემენტები:
    - წინასწარ განსაზღვრა - ლეგიტიმური მიზნები უნდა განისაზღვროს დამუშავების დაგეგმვამდე.
    - კონკრეტულობა - მიზნები კონკრეტულად და ცალსახად უნდა მიუთითებდეს, თუ რატომ ხდება პერსონალური მონაცემების დამუშავება.
    - მიზანზე ორიენტირებულობა - დამუშავების მიზანზე დაყრდნობით უნდა დაიგეგმოს დამუშავება და განისაზღვროს დამუშავების საზღვრები.
    - აუცილებლობა - მიზანი განსაზღვრავს, თუ რომელი პერსონალური მონაცემების დამუშავებაა აუცილებელი.
    - თავსებადობა - ნებისმიერი ახალი მიზანი თავსებადი უნდა იყოს იმ თავდაპირველ მიზანთან, რისთვისაც შეგროვდა მონაცემები და მის

[34] 29-ე მუხლის სამუშაო ჯგუფმა უზრუნველყო სახელმძღვანელო მითითებები მიზეზის შეზღუდვის პრინციპის მნიშვნელობასთან დაკავშირებით, 95/46/EC დირექტივის შესაბამისად. მართალია აღნიშნული დასკვნა არ არის დამტკიცებული EDBP-ს მიერ, იგი მაინც რელევანტურია, რადგან GDPR-ით გათვალისწინებული პრინციპი იგივენაირად არის ჩამოყალიბებული. 29-ე მუხლის სამუშაო ჯგუფი. „დასკვნა 03/13 მიზნის შეზღუდვის თაობაზე“. WP 203, 2013 წლის 2 აპრილი. ec.europa.eu/justice/article-29/documentation/opinion- recommendation/files/2013/wp203_en.pdf

[35] GDPR-ის 5(1)(b) მუხლი.

საფუძველზე უნდა განხორციელდეს შესაბამისი ცვლილებები დიზაინში.

- შემდგომი დამუშავების შეზღუდვა - დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, თავი შეიკავოს მონაცემთა წყებების დაკავშირებისგან ან რაიმე შემდგომი დამუშავებისგან, ახალი არათავსებადი მიზნებისთვის.
- ხელახლა გამოყენების შეზღუდვა - დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გამოიყენოს ტექნიკური ზომები, მათ შორის, ჰეშირება და დაშიფვრა, რათა შეზღუდოს პერსონალური მონაცემების შესაძლო ხელმეორე გამოყენება. დამუშავებისთვის პასუხისმგებელ პირს, აგრეთვე, უნდა ჰქონდეს ორგანიზაციული ზომები, როგორიცაა პოლიტიკა და სახელშეკრულებო ვალდებულებები, რომელიც შეზღუდავს პერსონალური მონაცემების ხელახლა გამოყენებას.
- გადახედვა - დამუშავებისთვის პასუხისმგებელმა პირმა რეგულარულად უნდა შეაფასოს, თუ რამდენად არის დამუშავება აუცილებელი იმ მიზნებისთვის, რისთვისაც შეგროვდა მონაცემები და დამუშავების სქემა (დიზაინი) შეაფასოს მიზნის შეზღუდვის პრინციპის საფუძველზე.

<u>მაგალითი</u>

დამუშავებისთვის პასუხისმგებელი პირი საკუთარი მომხმარებლების შესახებ ამუშავებს პერსონალურ მონაცემებს. დამუშავების მიზანია ხელშეკრულების პირობების შესრულება, ე.ი. საქონლის მიწოდება სწორ მისამართზე და თანხის მიღება. პერსონალური მონაცემები, რომლებიც ინახება, მოიცავს: ყიდვის ისტორიას, სახელს, მისამართს, ელ-ფოსტის მისამართს და ტელეფონის ნომერს.

დამუშავებისთვის პასუხისმგებელი პირი განიხილავს მომხმარებელთა ურთიერთობის მართვის (CRM) პროდუქტის შესყიდვას, რათა ერთ ადგილას მოაგროვოს მომხმარებელთა შესახებ მონაცემები, რომლებიც ეხება გაყიდვებს, მარკეტინგს და მომხმარებლის მომსახურებას. პროდუქტი იძლევა ყველა სატელეფონო ზარის, აქტივობის, დოკუმენტის, იმეილისა და მარკეტინგული კამპანიების შენახვის შესაძლებლობას, რათა კომპანიას მომხმარებლის შესახებ ჰქონდეს 360 გრადუსიანი სურათი. ამას გარდა, CRM-ში ხორციელდება ავტომატური ანალიზი მომხმარებლის მსყიდველუნარიანობის შესახებ, საჯარო ინფორმაციის გამოყენებით. ამ ანალიზის მიზანია, სარეკლამო აქტივობების უკეთ მორგება მომხმარებლებზე. ეს აქტივობები არ წარმოადგენს დამუშავების თავდაპირველი კანონიერი მიზნის შემადგენელ ნაწილს.

იმისათვის, რომ დაცული იქნეს მიზნის შეზღუდვის პრინციპი, დამუშავებისთვის პასუხისმგებელი პირი პროდუქტის პროვაიდერს მიმართავს თხოვნით, შეადგინოს

CRM-ით გათვალისწინებული პერსონალურ მონაცემთა დამუშავების აქტივობების სქემა (რუკა) და ისინი დამუშავებისთვის პასუხისმგებელი პირისთვის რელევანტურ მიზნებს დაუკავშიროს.

სქემის შედეგების საფუძველზე, დამუშავებისთვის პასუხისმგებელი პირი ახდენს შეფასებას, თუ რამდენად თავსებადია მარკეტინგისა და მიზნობრივი რეკლამის ახალი მიზნები თავდაპირველ მიზანთან, რომელიც განისაზღვრა მონაცემების შეგროვების დროს და რამდენად არსებობს საკმარისი სამართლებრივი საფუძველი შესაბამისი დამუშავებისთვის. თუ შეფასების შედეგად დამუშავებისთვის პასუხისმგებელი პირი ვერ მიიღებს დადებით პასუხს, მან არ უნდა დაიწყოს შესაბამისი ფუნქციონალების გამოყენება. მეორეს მხრივ, დამუშავებისთვის პასუხისმგებელ პირს შეუძლია, გამოტოვოს აღნიშნული შეფასება და უბრალოდ არ გამოიყენოს პროდუქტის ზემოთ აღწერილი ფუნქციონალები.

3.5 მონაცემთა მინიმიზაცია

73. უნდა დამუშავდეს მხოლოდ ის პერსონალური მონაცემები, რომლებიც არის დამუშავების მიზნების ადეკვატური, შესაბამისი და იმ მოცულობის, რომელიც **აუცილებელია** ამ მიზნების მისაღწევად.[36] შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, წინასწარ განსაზღვროს, თუ რომელია დამუშავების სისტემების დასაშვები მახასიათებლები და პარამეტრები და მათი მხარდამჭერი ფუნქციები. მონაცემთა მინიმიზაცია განამტკიცებს და მოქმედებაში მოიყვანს აუცილებლობის პრინციპს. შემდგომი დამუშავების პროცესში, დამუშავებისთვის პასუხისმგებელმა პირმა პერიოდულად უნდა შეაფასოს, დამუშავებული პერსონალური მონაცემები არის თუ არა კვლავ ადეკვატური, რელევანტური და აუცილებელი, ან ხომ არ უნდა მოხდეს მონაცემთა წაშლა ან ანონიმიზება.

74. დამუშავებისთვის პასუხისმგებელმა პირებმა პირველ რიგში უნდა განსაზღვრონ, საერთოდ ესაჭიროებათ თუ არა პერსონალური მონაცემების დამუშავება შესაბამისი მიზნებისთვის. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეაფასოს, რელევანტური მიზნების მიღწევა არის თუ არა შესაძლებელი ნაკლები პერსონალური მონაცემების დამუშავებით, ან ნაკლებად დეტალიზებული ან აგრეგირებული პერსონალური მონაცემების ქონით ან საერთოდ პერსონალური მონაცემების დამუშავების გარეშე.[37] ამგვარი შეფასება უნდა განხორციელდეს ნებისმიერი დამუშავების წინ, თუმცა, მისი

[36] GDPR-ის 5(1)(c) მუხლი.

[37] GDPR-ის პრეამბულის 39-ე პუნქტის თანახმად: „... პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, თუ დამუშავების მიზნის გონივრულობის ფარგლებში მიღწევა შეუძლებელია სხვა საშუალებებით.“

განხორციელება, აგრეთვე, შესაძლებელია, დამუშავების ცხოვრების ციკლის ნებისმიერ ეტაპზე. აღნიშნული მე-11 მუხლთან შესაბამისობაშია.

75. მინიმიზება, შესაძლოა, აგრეთვე, მიუთითებდეს იდენტიფიცირების ხარისხზე. თუ დამუშავების მიზანი არ მოითხოვს, რომ მონაცემთა საბოლოო წყება მიუთითებდეს იდენტიფიცირებულ ან იდენტიფიცირებად პირზე (მაგ., როდესაც მონაცემები მუშავდება სტატისტიკური მიზნებისთვის), თუმცა, დამუშავების საწყისი ეტაპი მოითხოვს ამას (მაგ., მონაცემთა აგრეგირებამდე), მაშინ, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, წაშალოს პერსონალური მონაცემები ან მოახდინოს მათი ანონიმიზება, როგორც კი იდენტიფიცირება აღარ იქნება საჭირო. ან, თუ უწყვეტი იდენტიფიცირებას მოითხოვს დამუშავების სხვა აქტივობები, უნდა მოხდეს პერსონალურ მონაცემთა ფსევდონიმიზაცია, რათა შემცირდეს მონაცემთა სუბიექტების უფლებების მიმართ არსებული რისკები.

76. მონაცემთა მინიმიზაციასთან დაკავშირებით, მოქმედებს შემდეგი ძირითადი DPbDD ელემენტები:
    - დამუშავებისგან თავის შეკავება - პერსონალური მონაცემების დამუშავებისგან საერთოდ თავის შეკავება, თუ ეს შესაძლებელია შესაბამისი მიზნის გათვალისწინებით.
    - მოცულობის შეზღუდვა - შეგროვებული პერსონალური მონაცემების მოცულობის შეზღუდვა იმ დოზით, რა დოზითაც აუცილებელია შესაბამისი მიზნისთვის.
    - წვდომის შეზღუდვა - მონაცემთა დამუშავების პროცესის ფორმირება იმგვარად, რომ საკუთარი ფუნქციების შესასრულებლად ადამიანთა მინიმალურ რაოდენობას ესაჭიროებოდეს პერსონალურ მონაცემებზე წვდომა, და წვდომის შეზღუდვა შესაბამისად.
    - რელევანტურობა - პერსონალური მონაცემები უნდა იყოს დამუშავებისთვის რელევანტური, ხოლო დამუშავებისთვის პასუხისმგებელ პირს უნდა შეეძლოს ამ რელევანტურობის დემონსტრირება.
    - აუცილებლობა - პერსონალურ მონაცემთა თითოეული კატეგორია უნდა იყოს აუცილებელი კონკრეტული მიზნებისთვის და უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, თუ შეუძლებელია ამ მიზნის სხვა საშუალებებით მიღწევა.
    - აგრეგირება - შესაძლებლობის შემთხვევაში, აგრეგირებული მონაცემების გამოყენება.
    - ფსევდონიმიზაცია - პერსონალური მონაცემების ფსევდონიმიზაცია, როგორც კი აღარ იქნება საჭირო პირდაპირ იდენტიფიცირებადი პერსონალური მონაცემების ქონა, და იდენტიფიცირების გასაღებთა ცალ-ცალკე შენახვა.

- ანონიმიზაცია და წაშლა - თუ პერსონალური მონაცემები არ არის ან აღარ არის აუცილებელი მიზნისთვის, უნდა განხორციელდეს მათი ანონიმიზება ან წაშლა.
- მონაცემთა ნაკადი - მონაცემთა ნაკადი უნდა იყოს იმდენად ეფექტური, რომ არ შეიქმნას იმაზე მეტი ასლები, ვიდრე საჭიროა.
- „უახლესი ტექნოლოგიები“ - დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, განახლებული და სათანადო ტექნოლოგიები გამოიყენოს მონაცემთა დამუშავების თავიდან ასაცილებლად და მონაცემთა მინიმიზაციისთვის.

<u>მაგალითი 1</u>

წიგნების მაღაზიას სურს, რომ შემოსავლები გაზარდოს წიგნების ონლაინ გაყიდვის გზით. წიგნების მაღაზიის მეპატრონემ გადაწყვიტა, შექმნას სტანდარტული ფორმა ონლაინ შეკვეთებისთვის. იმისათვის, რომ მომხმარებლებმა მაღაზიას ყველა საჭირო ინფორმაცია მიაწოდონ, მეპატრონემ ფორმაში არსებულ ყველა ველი სავალდებულო გახადა (თუ მომხმარებელი ყველა ველს არ შეავსებს, იგი ვერ შეძლებს შეკვეთის განთავსებას). ვებ-მაღაზიის მფლობელი თავდაპირველად იყენებს კონტაქტის სტანდარტულ ფორმას, რომელიც მომხმარებლებისგან ითხოვს ისეთ ინფორმაციას, როგორიცაა: მომხმარებლის დაბადების თარიღი, ტელეფონის ნომერი და საცხოვრებელი მისამართი. ამავდროულად, ფორმაში არსებული ყველა ველი არ არის აუცილებელი წიგნების გაყიდვის და მიწოდებისთვის. ამ კონკრეტულ შემთხვევაში, თუ მონაცემთა სუბიექტი პროდუქტის ღირებულებას გადაიხდის წინასწარ, მისი დაბადების თარიღი და ტელეფონის ნომერი არ არის საჭირო პროდუქტის შესაძენად. ეს ნიშნავს იმას, რომ შეკვეთის ფორმაში, აღნიშნული ველები სავალდებულოს არ უნდა წარმოადგენდეს, გარდა იმ შემთხვევისა, თუ დამუშავებისთვის პასუხისმგებელ პირს შეუძლია, მკაფიოდ დაადასტუროს მათი შევსების აუცილებლობა. ამას გარდა, ზოგ სიტუაციაში, შესაძლოა, მისამართის მითითება არ იყოს აუცილებელი. მაგალითად, როდესაც მომხმარებელი ელექტრონულ წიგნს უკვეთავს, მას შეუძლია პროდუქტის ჩამოტვირთვა პირდაპირ თავის მოწყობილობაზე.

ვებ-მაღაზიის მფლობელმა, შესაბამისად, გადაწყვიტა ორი ვებ-ფორმის შექმნა: ერთი წიგნების შესაკვეთად, სადაც მომხმარებელი მისამართს მიუთითებს, ხოლო მეორე კი ელექტრონული წიგნების შეკვეთისთვის. ეს უკანასკნელი არ შეიცავს მომხმარებლის მისამართის შესახებ ველს.

<u>მაგალითი 2</u>

საზოგადოებრივი ტრანსპორტის კომპანიას სურს სტატისტიკური ინფორმაციის შეგროვება მგზავრთა გადაადგილების მარშრუტების შესახებ, რის საფუძველზეც იგი აპირებს, რომ გააუმჯობესოს საზოგადოებრივი ტრანსპორტის განრიგი და მატარებლებისთვის სათანადო მარშრუტები განსაზღვროს. მგზავრები სატრანსპორტო საშუალებაზე ასვლისას და ჩამოსვლისას ვალდებულები არიან, თავიანთი ბილეთი გაატარონ სპეციალურ წამკითხველში. დამუშავებისთვის პასუხისმგებელმა პირმა შეაფასა ის საფრთხეები, რომელსაც შესაბამისი მონაცემების შეგროვება უქმნის მგზავრთა უფლებებს და თავისუფლებებს და დაადგინა, რომ იმ მგზავრთა იდენტიფიცირება, რომლებიც მეჩხერად დასახლებულ ადგილებში ცხოვრობენ ან მუშაობენ, შესაძლებელია მხოლოდ ერთი მარშრუტის (ცალი გზის) შესახებ მონაცემთა დამუშავებით. ბილეთის იდენტიფიკატორის შენახვა კი არ წარმოადგენს საჭიროებას საზოგადოებრივი ტრანსპორტის განრიგის და მარშრუტის ოპტიმიზაციის მიზნებისთვის. შესაბამისად, მგზავრობის დასრულების შემდეგ, დამუშავებისთვის პასუხისმგებელი პირი ინახავს მხოლოდ გადაადგილების ინდივიდუალურ მარშრუტს, რათა შეუძლებელი იყოს რამდენიმე გადაადგილების ერთ ბილეთთან დაკავშირება.

თუ მაინც არსებობს საზოგადოებრივი ტრანსპორტით გადაადგილების შესახებ მონაცემების საფუძველზე პირის იდენტიფიცირების რისკი, დამუშავებისთვის პასუხისმგებელი პირი ახორციელებს სტატისტიკურ ზომებს ამ რისკის შესამცირებლად, მაგალითად, მარშრუტის დაწყების და დასრულების დროის შესახებ მონაცემების წაშლა.

<u>მაგალითი 3</u>

საკურიერო კომპანიას სურს, შეაფასოს საკუთარი საქმიანობის ეფექტიანობა - კერძოდ, მიწოდების დრო, დატვირთულობა და საწვავის მოხმარება, რისთვისაც საჭიროა კომპანიის მიერ საკუთარი თანამშრომლების (მძღოლები) და მომხმარებლების (მისამართები, მიტანილი ნივთების რაოდენობა და ა.შ.) გარკვეული პერსონალური მონაცემების დამუშავება. დამუშავების ოპერაცია მოიცავს გარკვეულ რისკებს, კერძოდ: დასაქმებულთა მონიტორინგის რისკი, რაც მოითხოვს სამართლებრივი დაცვის სპეციფიურ მექანიზმებს, და მომხმარებელთა ჩვევების მონიტორინგი, რასაც კომპანია განახორციელებს დროის გარკვეულ მონაკვეთში მიწოდებული ნივთების შესახებ მონაცემების დამუშავებით. ამ რისკების მნიშვნელოვნად შემცირება შესაძლებელია დასაქმებულთა და მომხმარებელთა ფსევდონიმიზაციით. კერძოდ, თუ განხორციელდება ფსევდონიმიზაციის გასაღებთა ხშირი როტაცია, ხოლო დეტალური მისამართების ნაცვლად დამუშავებისთვის პასუხისმგებელი პირი განიხილავს მაკრო-ტერიტორიებს, იგი მოახდენს მონაცემთა ეფექტურ მინიმიზაციას და შეძლებს,

ფოკუსირება მოახდინოს მხოლოდ მიწოდების პროცესზე და რესურსების ოპტიმიზაციის მიზანზე, ისე, რომ არ გადაკვეთოს ფიზიკურ პირთა (მომხმარებლები და დასაქმებულები) მონიტორინგის (ზედამხედველობის) ზღვარი.

მაგალითი 4

საავადმყოფო აგროვებს მონაცემებს საკუთარი პაციენტების შესახებ, საავადმყოფოს საინფორმაციო სისტემაში (ჯანმრთელობის შესახებ ელექტრონული ჩანაწერები). საავადმყოფოს თანამშრომლებს ესაჭიროებათ პაციენტთა ფაილებზე წვდომა, რათა მიიღონ ინფორმირებული გადაწყვეტილებები პაციენტებზე ზრუნვისა და მათი მკურნალობის შესახებ, მოახდინონ დიაგნოზის და განხორციელებული ზრუნვისა და მკურნალობის დოკუმენტირება. პირველადი პარამეტრების თანახმად, პაციენტის მონაცემებზე წვდომა აქვთ მხოლოდ იმ სპეციალიზებული დეპარტამენტის თანამშრომლებს, სადაც პაციენტი მკურნალობს. ადამიანთა ჯგუფი, რომელსაც პაციენტის ფაილზე აქვს წვდომა, ფართოვდება იმ შემთხვევაში, თუ მკურნალობაში ერთვება სხვა დიაგნოსტიკური განყოფილება ან დეპარტამენტი. პაციენტის გაწერის შემდეგ, მონაცემებზე წვდომა უნარჩუნდება მხოლოდ დასაქმებულთა მცირე ზომის ჯგუფს სპეციალიზებულ დეპარტამენტში, რომლებიც გასცემენ კონსულტაციას ან სამედიცინო ინფორმაციას, მათ შორის სხვა სამედიცინო მომსახურების მიმწოდებლის მოთხოვნის საფუძველზე, შესაბამისი პაციენტის თანხმობის შემთხვევაში.

3.6 სიზუსტე

77. პერსონალური მონაცემები უნდა უყოს ზუსტი და განახლებული, და ყველა გონივრული ნაბიჯი უნდა გადაიდგას, რათა პერსონალური მონაცემები, რომლებიც არ არის ზუსტი - იმ მიზეზების გათვალისწინებით, რისთვისაც ხდება მათი დამუშავება - წაიშალოს ან გასწორდეს დაყოვნების გარეშე.[38]

78. აღნიშნული მოთხოვნები გათვალისწინებული უნდა იქნეს მონაცემთა გამოყენების კონკრეტული შემთხვევის შედეგებთან და რისკებთან მიმართებით. მცდარი პერსონალური მონაცემები, შესაძლოა, საფრთხეს უქმნიდეს მონაცემთა სუბიექტების უფლებებს და თავისუფლებებს - მაგალითად, გამოიწვიოს არასწორი დიაგნოზი ან მკურნალობა, ან პირის არასწორი გამოსახულების შემთხვევაში, შესაძლოა მიღებული იქნეს მცდარი

[38] GDPR-ის 5(1)(d) მუხლი

გადაწყვეტილებები მექანიკურად, ავტომატურად ან ხელოვნური ინტელექტის საშუალებით.

79. მონაცემთა სიზუსტის პრინციპთან დაკავშირებით, მოქმედებს შემდეგი ძირითადი DPbDD ელემენტები:
    - მონაცემთა წყარო - პერსონალური მონაცემების წყაროები უნდა იყოს სანდო, მონაცემთა სიზუსტის ჭრილში;
    - სიზუსტე - პერსონალური მონაცემების შემადგენელი თითოეული ელემენტი უნდა იყოს იმდენად ზუსტი, რამდენადაც ეს აუცილებელია კონკრეტული მიზნებისთვის.
    - გაზომვადი სიზუსტე - ცრუ დადებითების/უარყოფითების რაოდენობის შემცირება, მაგალითად, მიკერძოებები ავტომატური გადაწყვეტილებების ან ხელოვნური ინტელექტის შემთხვევაში.
    - ვერიფიკაცია - მონაცემთა ხასიათიდან გამომდინარე, იმის გათვალისწინებით, თუ რამდენად ხშირად შეიძლება შეიცვალოს მონაცემები, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გადაამოწმოს პერსონალური მონაცემების სიზუსტე მონაცემთა სუბიექტთან, დამუშავების სხვადასხვა ეტაპებამდე და ეტაპებზე (მაგ., როდესაც მოქმედებს ასაკთან დაკავშირებული მოთხოვნები).
    - წაშლა/გასწორება - დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, დაყოვნების გარეშე წაშალოს ან გაასწოროს უზუსტო მონაცემები. დამუშავებისთვის პასუხისმგებელმა პირმა განსაკუთრებით უნდა უზრუნველყოს აღნიშნული, თუ მონაცემთა სუბიექტები არიან ან იყვნენ ბავშვები და მოგვიანებით, მათ მოისურვეს ამ პერსონალური მონაცემების წაშლა.[39]
    - შეცდომის გავრცელების თავიდან აცილება - დამუშავებისთვის პასუხისმგებელი პირები ვალდებულები არიან, გამოასწორონ დამუშავების ჯაჭვში დაგროვილი შეცდომის შედეგები.
    - წვდომა - საჭიროა მონაცემთა სუბიექტების უზრუნველყოფა პერსონალური მონაცემების შესახებ ინფორმაციით და მათზე ეფექტური წვდომით, GDPR-ის მე-12 და მე-15 მუხლების შესაბამისად, რათა მათ აკონტროლონ მონაცემთა სიზუსტე და გაასწორონ ისინი, საჭიროების შესაბამისად.
    - უწყვეტი სიზუსტე - პერსონალური მონაცემები უნდა იყოს ზუსტი, დამუშავების ყველა ეტაპზე, ხოლო სიზუსტის შემოწმება უნდა განხორციელდეს კრიტიკული მნიშვნელობის ნაბიჯების გადადგმის დროს.
    - განახლებული - პერსონალური მონაცემები უნდა იყოს განახლებული, თუ ეს აუცილებელია დამუშავების მიზნისთვის.

[39] Cf. პრეამბულა, პუნქტი 65.

- მონაცემთა დიზაინი - ტექნოლოგიური და ორგანიზაციული დიზაინის მახასიათებელთა გამოყენება, უზუსტობის შესამცირებლად, მაგალითად, ლაკონიური, წინასწარ დადგენილი არჩევანის შეთავაზება, ტექსტის ცარიელი ველების ნაცვლად.

მაგალითი 1

სადაზღვევო კომპანიას სურს, გამოიყენოს ხელოვნური ინტელექტი (AI), რათა მოახდინოს მომხმარებელთა პროფილირება და აღნიშნულის საფუძველზე მიიღოს გადაწყვეტილებები სადაზღვევო რისკის გამოანგარიშებისას. ტექნოლოგიური გადაწყვეტების განვითარების გზების განსაზღვრისას, კომპანია ახდენს დამუშავების საშუალებების განსაზღვრას და ვალდებულია, მომწოდებლისგან AI აპლიკაციის არჩევისას და ხელოვნური ინტელექტის წვრთნის შესახებ გადაწყვეტილების მიღებისას გაითვალისწინოს პრინციპი „მონაცემთა დაცვა პირველად პარამეტრად“.

ხელოვნური ინტელექტის წვრთნის გზების განსაზღვრისას, დამუშავებისთვის პასუხისმგებელ პირს უნდა ჰქონდეს ზუსტი მონაცემები, რათა მიაღწიოს ზუსტ შედეგებს. შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, უზრუნველყოს ხელოვნური ინტელექტის წვრთნისთვის გამოყენებული მონაცემების სიზუსტე.

იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელ პირს აქვს ქმედითი სამართლებრივი საფუძველი ხელოვნური ინტელექტის წვრთნისთვის, არსებულ მომხმარებელთა დიდი ჯგუფის პერსონალური მონაცემების გამოყენებით, იგი ირჩევს მომხმარებელთა ჯგუფს, რომელიც პოპულაციის რეპრეზენტაციულია, მიკერძოების თავიდან ასაცილებლად.

ამის შემდგომ, მომხმარებლის შესახებ მონაცემების შეგროვება ხდება მონაცემთა დამუშავების სისტემის საშუალებით, მათ შორის, მონაცემები დაზღვევის ტიპის (მაგ., ჯანმრთელობის, სახლის, სამოგზაურო და ა.შ.) შესახებ, და მონაცემები საჯარო რეესტრებიდან, რომელზეც დამუშავებისთვის პასუხისმგებელ პირს კანონიერად მიუწვდება ხელი. ხელოვნური ინტელექტის მოდელის წვრთნისთვის განკუთვნილი სისტემისთვის გადაცემამდე ხორციელდება ყველა ამ მონაცემის ფსევდონიმიზაცია.

იმისათვის, რომ ხელოვნური ინტელექტის წვრთნისთვის გამოყენებული მონაცემები იყოს მაქსიმალურად ზუსტი, დამუშავებისთვის პასუხისმგებელი პირი მონაცემებს აგროვებს მხოლოდ მონაცემთა იმ წყაროებიდან, სადაც დაცულია სწორი და განახლებული ინფორმაცია.

სადაზღვევო კომპანია ტესტავს ხელოვნურ ინტელექტს, რათა დაადგინოს, თუ რამდენად საიმედოა იგი და რამდენად უზრუნველყოფს არადისკრიმინაციულ

შედეგებს, როგორც განვითარების ეტაპზე, ისე პროდუქტის გაშვებამდე. ხელოვნური ინტელექტის წვრთნის დასრულების და ამოქმედების შემდეგ, სადაზღვევო კომპანია შედეგებს იყენებს დაზღვევის რისკის შესაფასებლად, თუმცა, დაზღვევის მინიჭებაზე გადაწყვეტილების მიღებაში იგი მხოლოდ ხელოვნური ინტელექტის მონაცემებს არ ეყრდნობა, გარდა იმ შემთხვევისა, თუ გადაწყვეტილება მიღებულია GDPR-ის 22(2) მუხლით გათვალისწინებული გამონაკლისის შესაბამისად.

სადაზღვევო კომპანია რეგულარულად ახდენს ხელოვნური ინტელექტიდან მიღებული შედეგების გადახედვას, რაც ხელს უწყობს შედეგების საიმედოობას და საჭიროების შემთხვევაში, საჭირო შესწორებების შეტანას ალგორითმში.

მაგალითი 2

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი არის სამედიცინო დაწესებულება, რომელიც კლიენტის რეესტრებში დაცული პერსონალური მონაცემების უსაფრთხოებისა და სიზუსტის უზრუნველსაყოფად შესაბამის მეთოდებს ეძებს.

როდესაც დაწესებულებაში ერთდროულად მოდის ორი ადამიანი და ისინი ერთსა და იმავე მკურნალობას იღებენ, შესაძლოა დაწესებულებას ერთმანეთში აერიოს პაციენტები, თუ მათი გარჩევის ერთადერთ საშუალებს წარმოადგენს სახელი. სიზუსტის უზრუნველსაყოფად, დამუშავებისთვის პასუხისმგებელ პირს ესაჭიროება თითოეული პირის უნიკალური იდენტიფიკატორი. შესაბამისად, მას კლიენტისგან ესაჭიროება სხვა მონაცემებიც, გარდა სახელისა.

დაწესებულება რამდენიმე სისტემას იყენებს, რომლებიც შეიცავენ კლიენტთა პერსონალურ ინფორმაციას. მან უნდა უზრუნველყოს, რომ კლიენტის შესახებ ინფორმაცია არის სწორი, ზუსტი და თანმიმდევრული ყველა სისტემაში, ნებისმიერ დროს. დაწესებულებამ მოახდინა რამდენიმე რისკის იდენტიფიცირება, რომლებიც შესაძლოა წარმოიშვას ერთ სისტემაში ინფორმაციის შეცვლის შემთხვევაში, როდესაც ინფორმაციის შეცვლა სხვა სისტემებში არ ხდება.

დამუშავებისთვის პასუხისმგებელმა პირმა გადაწყვიტა, აღნიშნულ რისკზე საპასუხოდ გამოიყენოს ჰეშირების ტექნიკა, რომელიც მკურნალობის ჟურნალში მონაცემთა უსაფრთხოებას უზრუნველყოფს. მკურნალობის ჟურნალში წარმოებული ჩანაწერებისთვის და შესაბამისი კლიენტისთვის იქმნება კრიფტოგრაფული დროის აღნიშვნა, რომლის შეცვლაც შეუძლებელია, რათა ნებისმიერი ცვლილება იქნეს დაფიქსირებული, დაკავშირებული და მიკვლეული.

3.7 შენახვის ვადის შეზღუდვა

80. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, უზრუნველყოს პერსონალური მონაცემების შენახვა იმ ფორმით, რაც იძლევა მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობას არა უმეტეს იმ დროისა, რაც აუცილებელია პერსონალური მონაცემების დამუშავების მიზნებისთვის.[40] სასიცოცხლოდ მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა ზუსტად იცოდეს, თუ რომელ პერსონალურ მონაცემებს ამუშავებს კომპანია და რატომ. დამუშავების მიზანი უნდა იყოს ძირითადი კრიტერიუმი პერსონალური მონაცემების შენახვის ვადის შესახებ გადაწყვეტილების მისაღებად.

81. ზომები და დაცვის მექანიზმები, რომლებიც ახორციელებს შენახვის ვადის შეზღუდვის პრინციპს, უნდა განამტკიცებდეს მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებს, კერძოდ, წაშლის უფლებას და დამუშავების შეწყვეტის მოთხოვნის უფლებას.

82. შენახვის ვადის შეზღუდვასთან დაკავშირებით, მოქმედებს შემდეგი ძირითადი DPbDD ელემენტები:
    - წაშლა და ანონიმიზაცია - დამუშავებისთვის პასუხისმგებელ პირს უნდა გააჩნდეს მკაფიო შიდა პროცედურები და ფუნქციონალობები მონაცემთა წაშლისთვის და/ან ანონიმიზაციისთვის.
    - ანონიმიზაციის/წაშლის ეფექტურობა - დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, უზრუნველყოს, რომ შეუძლებელი იყოს ანონიმიზებული მონაცემების ხელახლა იდენტიფიცირება ან წაშლილი მონაცემების აღდგენა, და უნდა შეამოწმოს თუ რამდენად შესაძლებელია აღნიშნული.
    - ავტომატიზება - გარკვეული პერსონალური მონაცემების წაშლა უნდა ხორციელდებოდეს ავტომატურად.
    - შენახვის კრიტერიუმები - დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, დაადგინოს, თუ რა მონაცემები და შენახვის რა ვადაა აუცილებელი მოცემული მიზნისთვის.
    - დასაბუთება - დამუშავებისთვის პასუხისმგებელ პირს უნდა შეეძლოს, დაასაბუთოს, თუ რატომ არის შენახვის კონკრეტული ვადა აუცილებელი კონკრეტული მიზნისთვის და მოცემული პერსონალური მონაცემებისთვის და უნდა შეეძლოს, წარმოადგინოს შენახვის ვადის რაციონალური და სამართლებრივი საფუძველი.
    - შენახვის პოლიტიკის აღსრულება - დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მოახდინოს შენახვის შიდა პოლიტიკის აღსრულება და

[40] GDPR-ის მუხლი 5(1)(c)

შეამოწმოს, თუ რამდენად ახორციელებს ორგანიზაცია პრაქტიკაში თავის პოლიტიკას.

- სარეზერვო ასლები/ჩანაწერები - დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, დაადგინოს, თუ რომელი პერსონალური მონაცემები და შენახვის რა ვადა არის აუცილებელი სარეზერვო ასლების/ჩანაწერების შესაქმნელად.
- მონაცემთა მიმოცვლა - დამუშავებისთვის პასუხისმგებელი პირი სიფრთხილით უნდა მოეკიდოს პერსონალური მონაცემების მიმოცვლის საკითხს და მათი ასლების შენახვას და მიზნად დაისახოს მონაცემთა „დროებითი“ შენახვის შეზღუდვა.

მაგალითი

დამუშავებისთვის პასუხისმგებელი პირი აგროვებს პერსონალურ მონაცემებს, ხოლო დამუშავების მიზანია მონაცემთა სუბიექტის წევრობის ადმინისტრირება. პერსონალური მონაცემები უნდა წაიშალოს მას შემდეგ, რაც მონაცემთა სუბიექტი შეწყვეტს წევრობას, ხოლო მონაცემთა შემდგომი შენახვისთვის სამართლებრივი საფუძველი არ არსებობს.

პირველ რიგში, დამუშავებისთვის პასუხისმგებელი პირი შეიმუშავებს მონაცემთა შენახვისა და წაშლის შიდა პროცედურებს, რომლის თანახმადაც დასაქმებულებმა მექანიკურად უნდა წაშალონ პერსონალური მონაცემები მას შემდეგ, რაც ამოიწურება შენახვის ვადა. დასაქმებული მისდევს ნებისმიერი მოწყობილობებიდან, სარეზერვო ასლებიდან, ჩანაწერებიდან, ელ-ფოსტიდან და მონაცემთა შენახვის სხვა საშუალებებიდან მონაცემების რეგულარულად წაშლის და გასწორების პროცედურას.

იმისათვის, რომ წაშლა ყოფილიყო უფრო ეფექტური და ნაკლებად მიდრეკილი შეცდომებისკენ, დამუშავებისთვის პასუხისმგებელმა პირმა არსებული მექანიკური სისტემა ჩაანაცვლა ავტომატური სისტემით, რათა მონაცემთა წაშლა მოხდეს ავტომატურად, საიმედოდ და უფრო რეგულარულად. სისტემა მოწყობილია იმგვარად, რომ იგი მისდევს მონაცემთა წაშლის მოცემულ პროცედურას, რეგულარული ინტერვალებით, რათა პერსონალური მონაცემები წაიშალოს კომპანიის მონაცემთა შენახვის ყველა საშუალებიდან. დამუშავებისთვის პასუხისმგებელი პირი ახორციელებს შენახვის პროცედურის რეგულარულ გადახედვას და ტესტირებას და უზრუნველყოფს მის შესაბამისობას შენახვის განახლებულ პოლიტიკასთან.

3.8 უსაფრთხოება და კონფიდენციალურობა

83. უსაფრთხოების და კონფიდენციალურობის პრინციპი მოიცავს მონაცემთა არაავტორიზებული ან უკანონო დამუშავებისგან და შემთხვევით დაკარგვისგან, განადგურებისგან ან დაზიანებისგან დაცვას, სათანადო ტექნიკური ან ორგანიზაციული ზომების გამოყენების გზით. პერსონალური მონაცემების უსაფრთხოება მოითხოვს სათანადო ზომების შემუშავებას მონაცემთა უსაფრთხოების დარღვევის ინციდენტთა პრევენციისა და მართვისთვის; მონაცემთა დამუშავებასთან დაკავშირებული დავალებების სათანადო განხორციელების უზრუნველყოფას და სხვა პრინციპებთან შესაბამისობას; და ფიზიკურ პირთა უფლებების ეფექტური განხორციელების ხელშეწყობას.

84. პრეამბულის 78-ე პუნქტის თანახმად, DPbDD პრინციპების შესაბამისად განხორციელებული ერთ-ერთი ღონისძიება, შესაძლოა, მოიცავდეს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების „შესაძლებლობას, შექმნას და გააუმჯობესოს უსაფრთხოების პარამეტრები“. DPbDD პრინციპების შესაბამისად განხორციელებულ სხვა ღონისძიებებთან ერთად, პრეამბულის 78-ე პუნქტი დამუშავებისთვის პასუხისმგებელ პირებს აკისრებს პასუხისმგებლობას, უზრუნველყონ უწყვეტი შეფასება იმისა, თუ რამდენად იყენებენ ისინი დამუშავების შესაფერის საშუალებებს, დროის ნებისმიერ მონაკვეთში, და რამდენად უზრუნველყოფს არჩეული ზომები არსებული სუსტი მოწყვლადობის განეიტრალებას. ამას გარდა, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა განახორციელონ პერსონალური მონაცემების გარემომცველი და დამცავი საინფორმაციო უსაფრთხოების ზომების და უსაფრთხოების დარღვევის შემთხვევებზე რეაგირების პროცედურის რეგულარული გადახედვა.

85. კონფიდენციალურობასთან დაკავშირებით, მოქმედებს შემდეგი ძირითადი DPbDD ელემენტები:
    - საინფორმაციო უსაფრთხოების მართვის სისტემა (ISMS) - ინფორმაციის უსაფრთხოების პოლიტიკისა და პროცედურების მართვის ოპერატიული საშუალებების ქონა.
    - რისკის ანალიზი - პერსონალურ მონაცემთა უსაფრთხოების დარღვევის რისკების შეფასება იმის გათვალისწინებით, თუ რა გავლენა აქვს ამ რისკებს ფიზიკურ პირთა უფლებებზე და იდენტიფიცირებულ რისკებთან ბრძოლა. რისკის შეფასების პროცესში გამოყენებისთვის, შემუშავებულ კომპიუტერულ პროგრამასთან მიმართებით კომპლექსური, სისტემატური და რეალისტური „საფრთხის მოდელირების“ და თავდასხმის ზედაპირული ანალიზის შემუშავება და შენარჩუნება, თავდასხმის ვექტორების შესამცირებლად და სუსტი

მხარეების ან მოწყვლადობის ბოროტად გამოყენების შესაძლებლობების მინიმუმამდე დასაყვანად.

- მოვლა-პატრონობა - კომპიუტერული პროგრამის, კომპიუტერული მოწყობილობების, სისტემებისა და სერვისების და ა.შ. რეგულარული შეფასება და ტესტირება, დამუშავების მხარდამჭერ სისტემებში სისუსტეების იდენტიფიცირების მიზნით.
- წვდომაზე კონტროლის მართვა - მხოლოდ ავტორიზებულ პერსონალს უნდა ჰქონდეს წვდომა იმ პერსონალურ მონაცემებზე, რომლებიც აუცილებელია დამუშავებასთან დაკავშირებული ფუნქციების შესასრულებლად, ხოლო დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს ავტორიზებული პერსონალის წვდომის პრივილეგიების დიფერენცირება.
    i. წვდომის შეზღუდვა (აგენტები) - მონაცემთა დამუშავების ფორმირება იმგვარად, რომ მინიმალური ოდენობის ადამიანებს ესაჭიროებოდეთ პერსონალურ მონაცემებზე წვდომა საკუთარი ფუნქციების შესასრულებლად, და წვდომის შეზღუდვა შესაბამისად.
    ii. წვდომის შეზღუდვა (შინაარსი) - დამუშავების თითოეული ოპერაციის კონტექსტში, წვდომის შეზღუდვა, რათა წვდომა შემოიფარგლებოდეს მონაცემთა კრებულში არსებული მხოლოდ იმ მახასიათებლებით, რომლებიც საჭიროა კონკრეტული ოპერაციის შესასრულებლად. ამას გარდა, აღნიშნული გულისხმობს იმ მონაცემთა სუბიექტების შესახებ მონაცემებზე წვდომის შეზღუდვას, რომლებიც შესაბამისი დასაქმებულის საქმიანობის სფეროში ხვდებიან.
    iii. წვდომის სეგრეგაცია - მონაცემთა დამუშავების ფორმირება იმგვარად, რომ არც ერთ ინდივიდს არ ესაჭიროებოდეს მონაცემთა სუბიექტის შესახებ შეგროვებულ მონაცემებზე ყოვლისმომცველი წვდომის ქონა, განსაკუთრებით, მონაცემთა სუბიექტების კონკრეტული კატეგორიის შესახებ ყველა პერსონალურ მონაცემებზე.
- უსაფრთხო გადაცემა - გადაცემა დაცული უნდა იქნეს არაავტორიზებული ან შემთხვევითი წვდომისა და ცვლილებებისგან.
- უსაფრთხო შენახვა - შენახული მონაცემები დაცული უნდა იქნეს არაავტორიზებული წვდომისა და ცვლილებებისგან. უნდა არსებობდეს პროცედურები, რომლის საფუძველზეც შეფასდება ცენტრალიზებული ან დეცენტრალიზებული შენახვის რისკი და ის, თუ პერსონალური მონაცემების რომელ კატეგორიებზე ვრცელდება აღნიშნული. ზოგიერთი მონაცემები, შესაძლოა, საჭიროებდეს უსაფრთხოების დამატებით ზომებს ან სხვა მონაცემებისგან იზოლირებას.

- ფსევდონიმიზაცია - პერსონალური მონაცემები და სარეზერვო ასლები/ჩანაწერები ფსევდონიმიზებული უნდა იქნეს, რაც წარმოადგენს უსაფრთხოების ზომას მონაცემთა უსაფრთხოების დარღვევის პოტენციური რისკების შესამცირებლად, მაგალითად, ჰეშირების ან დაშიფვრის გამოყენება.
- სარეზერვო ასლები / ჩანაწერები - სარეზერვო ასლების და ჩანაწერების წარმოება იმდენად, რამდენადაც ეს აუცილებელია საინფორმაციო უსაფრთხოებისთვის, უსაფრთხოების რეგულარული კონტროლის სახით აუდიტორული ჩანაწერების და მოვლენის მონიტორინგის გამოყენება. სარეზერვო ასლები/ჩანაწერები დაცული უნდა იქნეს არაავტორიზებული და შემთხვევითი წვდომისა და ცვლილებისგან და გადახედილი უნდა იქნეს რეგულარულად, ხოლო ინციდენტებზე რეაგირება დაუყოვნებლივ უნდა განხორციელდეს.
- კატასტროფის შემდგომი აღდგენა / ბიზნესის უწყვეტობა - საინფორმაციო სისტემის კატასტროფის შემდგომი აღდგენის და ბიზნესის უწყვეტობის მოთხოვნების გათვალისწინება, რათა აღდგეს პერსონალურ მონაცემებზე წვდომა მნიშვნელოვანი ინციდენტების შემდგომ.
- რისკის შესაბამისი დაცვა - პერსონალური მონაცემების ყველა კატეგორია დაცული უნდა იქნეს ზომებით, რომლებიც შეესაბამება უსაფრთხოების დარღვევის რისკს. მონაცემები, რომლებიც განსაკუთრებულ რისკებს მოიცავს, შესაძლებლობის შემთხვევაში, უნდა განცალკევდეს დანარჩენი პერსონალური მონაცემებისგან.
- უსაფრთხოების ინციდენტზე რეაგირების მართვა - რუტინების, პროცედურებისა და რესურსების არსებობა მონაცემთა უსაფრთხოების დარღვევების გამოსავლენად, აღსაკვეთად, რეაგირების, შეტყობინების და გამოცდილების მიღებისთვის.
- ინციდენტის მართვა - დამუშავებისთვის პასუხისმგებელ პირს უნდა გააჩნდეს პროცესები მონაცემთა უსაფრთხოების დარღვევის შემთხვევებსა და ინციდენტებზე რეაგირებისთვის, რათა დამუშავების სისტემა იყოს უფრო მტკიცე. აღნიშნული მოიცავს შეტყობინების პროცედურებს, როგორიცაა, საზედამხედველო ორგანოსთვის შეტყობინების და მონაცემთა სუბიექტების ინფორმირების მართვა.

<u>მაგალითი</u>

დამუშავებისთვის პასუხისმგებელ პირს სურს, ამოიღოს დიდი ოდენობით პერსონალური მონაცემები სამედიცინო მონაცემთა ბაზებიდან, რომლებიც შეიცავენ ელექტრონულ (პაციენტთა) სამედიცინო ჩანაწერებს, და ეს მონაცემები გადაიტანოს კომპანიის მონაცემთა ბაზის სპეციალურ სერვერზე, რათა ამოღებული მონაცემები

დამუშავდეს ხარისხის უზრუნველყოფის მიზნებისთვის. კომპანიამ შეაფასა ამონაწერთა სერვერისკენ გადამისამართებასთან დაკავშირებული რისკი იმის გათვალისწინებით, რომ სერვერი ხელმისაწვდომია კომპანიის ყველა დასაქმებულისთვის და დაადგინა, რომ აღნიშნული მნიშვნელოვან რისკს უქმნის მონაცემთა სუბიექტების უფლებებს და თავისუფლებებს. ვინაიდან კომპანიაში არსებობს მხოლოდ ერთი დეპარტამენტი, რომელსაც პაციენტთა მონაცემებიდან ამონაწერების დამუშავება ესაჭიროება, დამუშავებისთვის პასუხისმგებელმა პირმა გადაწყვიტა, სპეციალურ სერვერზე წვდომა შეზღუდოს და წვდომა მისცეს მხოლოდ შესაბამისი დეპარტამენტის თანამშრომლებს. ამას გარდა, რისკის კიდევ უფრო შესამცირებლად, მონაცემთა სერვერზე გადაცემამდე განხორციელდება მათი ფსევდონომიზაცია.

წვდომის რეგულირების და მავნე პროგრამების შედეგად მიყენებული ზიანის შესარბილებლად, კომპანიამ გადაწყვიტა ქსელის სეგრეგირება და სერვერზე წვდომის კონტროლის მექანიზმების შექმნა. ამას გარდა, კომპანიამ აამოქმედა უსაფრთხოების მონიტორინგი და ჩარევის გამოვლენისა და პრევენციის სისტემა და მოახდინა მისი იზოლირება იმ სისტემებისგან, რომელთა გამოყენებაც ხდება რუტინულად. აუდიტის ავტომატიზებული სისტემა ახორციელებს წვდომისა და ცვლილებების მონიტორინგს. გამოყენების გარკვეულ შემთხვევებთან დაკავშირებით ხდება შეტყობინებებისა და ავტომატური განგაშის სიგნალის ამოქმედება. დამუშავებისთვის პასუხისმგებელი პირი უზრუნველყოფს, რომ მომხმარებლებს მონაცემებზე წვდომა ჰქონდეთ საჭიროების შესაბამისად (need to know basis) და სათანადო დონეზე. არასათანადო გამოყენების შემთხვევების გამოვლენა ხდება სწრაფად და ადვილად.

ზოგჯერ, საჭიროა ამონაწერის შედარება ახალ ამონაწერთან, რის გამოც იგი სამი თვის ვადით უნდა იქნეს შენახული. დამუშავებისთვის პასუხისმგებელი პირი იღებს გადაწყვეტილებას მათი ცალკე მონაცემთა ბაზაში მოთავსების შესახებ, იმავე სერვერზე, და მათ შესანახად უზრუნველყოფს გამჭვირვალე და დიფერენცირებულ დაშიფვრას. დიფერენცირებული დაშიფვრის გასაღებები შენახულია უსაფრთხოების სპეციალურ მოდულებში, რომელთა გამოყენება შესაძლებელია მხოლოდ ავტორიზებული პერსონალის მიერ, თუმცა, შეუძლებელია მათი ამოღება (ამოკრეფვა).

მოსალოდნელ ინციდენტებზე რეაგირება სისტემას უფრო მტკიცესა და სანდოს ხდის. მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს ესმის, რომ პრევენციული და ეფექტური ზომები და დაცვის მექანიზმები ინტეგრირებული უნდა იქნეს პერსონალური მონაცემების დამუშავების ყველა ოპერაციაში, რომელსაც იგი განახორციელებს ახლა და მომავალში, ხოლო აღნიშნული [ზომებისა და დაცვის მექანიზმების ინტეგრირება] ხელს შეუწყობს სამომავლოდ მონაცემთა უსაფრთხოების დარღვევის ინციდენტთა პრევენციას.

დამუშავებისთვის პასუხისმგებელი პირი უსაფრთხოების აღნიშნული ზომების დანერგვას ახორციელებს მონაცემთა სიზუსტის, მთლიანობის და კონფიდენციალურობის უზრუნველყოფისთვის და ამავდროულად, კიბერთავდასხმების გზით მავნე პროგრამების გავრცელების პრევენციისა და გადაწყვეტის (პრობლემის გადაჭრის გზის) სიმტკიცის ხელშეწყობისთვის. მტკიცე უსაფრთხოების ზომების არსებობა ხელს უწყობს ნდობის ჩამოყალიბებას მონაცემთა სუბიექტებთან.

3.9 ანგარიშვალდებულება[41]

86. ანგარიშვალდებულების პრინციპის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი პასუხისმგებელია და უნდა შეეძლოს ყველა ზემოაღნიშნულ პრინციპთან შესაბამისობის უზრუნველყოფა.

87. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეძლოს ყველა პრინციპთან შესაბამისობის დემონსტრირება. ამ მიზნით, მას შეუძლია წარმოაჩინოს, თუ რა შედეგები გამოიღო მონაცემთა სუბიექტების უფლებების დასაცავად მიღებულმა ზომებმა და რატომ არის ეს ზომები შესაფერისი და ეფექტური. მაგალითად, რატომ არის კონკრეტული ზომა შესაფერისი შენახვის ვადის შეზღუდვის პრინციპის ეფექტურად განხორციელებისთვის.

88. პერსონალური მონაცემების პასუხისმგებლიანად დამუშავება დამუშავებისთვის პასუხისმგებელი პირებისგან მოითხოვს მონაცემთა დაცვის შესახებ ცოდნას და განხორციელების შესაძლებლობას. კერძოდ, დამუშავებისთვის პასუხისმგებელ პირს უნდა ესმოდეს GDPR-ით გათვალისწინებული მონაცემთა დაცვის ვალდებულებები, რომლებიც დამუშავებისთვის პასუხისმგებელ პირებზე ვრცელდება და უნდა შეძლოს ამ ვალდებულებების შესრულება.

4. 25-ე მუხლის მესამე პუნქტი: სერტიფიცირება

89. 25-ე მუხლის მესამე პუნქტის თანახმად, 42-ე მუხლის შესაბამისად დამტკიცებული სერტიფიცირების მექანიზმი შეიძლება იყოს გამოყენებული, როგორც DPbDD მოთხოვნებთან შესაბამისობის დასაბუთება. მეორეს მხრივ, დოკუმენტები, რომლებიც ადასტურებს DPbDD მოთხოვნებთან შესაბამისობას,

[41] იხ. პრეამბულა, პუნქტი 74, რომლის მიხედვითაც დამუშავებისთვის პასუხისმგებელ პირებს მოეთხოვებათ მათი ზომების ეფექტურობის დემონსტრირება.

გამოდგება სერტიფიცირების პროცესში. აღნიშნული ნიშნავს იმას, რომ თუ დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ წარმოებული ოპერაცია სერტიფიცირებულია 42-ე მუხლის თანახმად, საზედამხედველო ორგანოებმა აღნიშნული მხედველობაში უნდა მიიღონ GDPR-თან შესაბამისობის შეფასებისას, კონკრეტულად, DPbDD მოთხოვნების ჭრილში.

90. როდესაც დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ განხორციელებული ოპერაცია არის სერტიფიცირებული 42-ე მუხლის შესაბამისად, ელემენტები, რომლებიც ხელს უწყობს 25-ე მუხლის პირველ და მეორე პუნქტებთან შესაბამისობის დემონსტრირებას არის დაგეგმვის (დიზაინის) პროცესები, ე.ი., მონაცემთა დაცვის პრინციპების განსახორციელებლად, დამუშავების საშუალებების, მართვის და ტექნიკური და ორგანიზაციული ზომების განსაზღვრის პროცესი. მონაცემთა დაცვის სერტიფიცირების კრიტერიუმები განისაზღვრება სერტიფიცირების ორგანოების ან სერტიფიცირების სქემის მფლობელთა მიერ, რომელსაც შემდგომ ამტკიცებს შესაბამისი საზედამხედველო ორგანო ან EDPB. სერტიფიცირების მექანიზმების შესახებ დამატებითი ინფორმაციის მისაღებად, გირჩევთ, იხილოთ EDPB სახელმძღვანელო პრინციპები სერტიფიცირების შესახებ[42] და სხვა რელევანტური სახელმძღვანელო დოკუმენტები, რომლებიც EDPB-ის ვებსაიტზეა გამოქვეყნებული.

91. მაშინაც კი, როდესაც დამუშავების ოპერაციას 42-ე მუხლის შესაბამისად ენიჭება სერტიფიცირება, დამუშავებისთვის პასუხისმგებელი პირი კვლავ პასუხისმგებელია DPbDD კრიტერიუმებთან (25-ე მუხლის თანახმად) შესაბამისობის უწყვეტ მონიტორინგსა და გაუმჯობესებაზე.

5. 25-ე მუხლის აღსრულება და შედეგები

92. საზედამხედველო ორგანოები უფლებამოსილები არიან, 25-ე მუხლთან შესაბამისობა შეაფასონ 58-ე მუხლში წარმოდგენილი პროცედურების თანახმად. დარღვევის გამოსასწორებლად ღონისძიებების გატარების უფლებამოსილება დადგენილია 58-ე მუხლის მეორე პუნქტში და მოიცავს: გაფრთხილების ან საყვედურის გამოცხადებას; პროცესის რეგულაციასთან

[42] EDPB. „სახელმძღვანელო პრინციპები 1/2018 სერტიფიცირებისა და სერტიფიცირების კრიტერიუმების რეგულაციის 42-ე და 43-ე მუხლების შესაბამისად იდენტიფიცირების შესახებ“, ვერსია 3.0, 2019 წლის 4 ივნისი.
edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

შესაბამისობაში მოყვანის დავალებას; დამუშავების შეზღუდვას ან აკრძალვას; ადმინისტრაციულ ჯარიმებს; და ა.შ.

93. DPbDD დამატებითი ფაქტორია, რომლის საფუძველზეც განისაზღვრება ფულადი სანქციების დონე GDPR-ის დარღვევის შემთხვევებში, იხ. მუხლი 83(4).[43] [44]

6. რეკომენდაციები

94. 25-ე მუხლი ამ საკითხზე პირდაპირ არ მიუთითებს, თუმცა, აღიარებულია, რომ **დამუშავებაზე უფლებამოსილი პირებს** და მწარმოებლებს მნიშვნელოვანი წვლილი შეაქვთ DPbDD პრინციპების ამოქმედებაში. შესაბამისად, ისინი უნდა იყვნენ ინფორმირებულები, რომ **დამუშავებისთვის პასუხისმგებელ პირებს** მოეთხოვებათ, პერსონალური მონაცემები დაამუშაონ მხოლოდ იმ სისტემებისა და ტექნოლოგიების გამოყენებით, რომლებშიც ინტეგრირებულია მონაცემთა დაცვა.

95. როდესაც მონაცემთა დამუშავება ხდება **დამუშავებისთვის პასუხისმგებელი** პირების სახელით ან ხდება გადაწყვეტების უზრუნველყოფა **დამუშავებისთვის პასუხისმგებელი პირებისთვის, დამუშავებაზე უფლებამოსილმა პირებმა** და მწარმოებლებმა უნდა გამოიყენონ თავიანთი ექსპერტული ცოდნა და გამოცდილება, რათა დაამყარონ ნდობა მომხმარებლებთან და გაუწიონ მათ ხელმძღვანელობა (მათ შორის, მცირე და საშუალო საწარმოებს), ისეთი გადაწყვეტების შემუშავებაში/შესყიდვაში, რომლებშიც ინტეგრირებულია მონაცემთა დაცვა. ეს თავის მხრივ, ნიშნავს პროდუქტისა და მომსახურების შექმნას იმგვარად, რაც ხელს უწყობს **დამუშავებისთვის პასუხისმგებელ პირთა** საჭიროებების დაკმაყოფილებას.

96. მნიშვნელოვანია იმის გათვალისწინება, რომ 25-ე მუხლის განხორციელებისას, ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მთავარი ამოცანას წარმოადგენს მონაცემთა სუბიექტის უფლებების დაცვის პრინციპის

[43] GDPR-ის 83(2)(d) მუხლის თანახმად, GDPR-ის დარღვევის შემთხვევებში ჯარიმების დაკისრების ან მისი ოდენობის განსაზღვრისას, „სათანადო ყურადღება“ უნდა მიექცეს „მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის პასუხისმგებლობის ფარგლები მათ მიერ 25-ე და 32-ე მუხლის შესაბამისად უსაფრთხოებისთვის მიღებული ორგანიზაციული და ტექნიკური ზომების გათვალისწინებით.“

[44] ჯარიმების შესახებ დამატებითი ინფორმაცია ხელმისაწვდომია 29-ე მუხლის სამუშაო ჯგუფის დოკუმენტში, „სახელმძღვანელო პრინციპები 2016/679 რეგულაციის მიზნებისთვის ადმინისტრაციული ჯარიმების გამოყენების და დადგენის შესახებ“. WP 253, 2017 წლის 3 ოქტომბერი. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 - აღიარებულია EDPB-ის მიერ.

იმპლემენტაცია მონაცემთა დამუშავების შესაბამის ღონისძიებებში. DPbDD პრინციპების მიღების ხელშეწყობის და მათი გამოყენების გაუმჯობესების მიზნით, ჩვენ დამუშავებისთვის პასუხისმგებელ პირებს, ისევე, როგორც მწარმოებლებსა და დამუშავებაზე უფლებამოსილ პირებს მივმართავთ შემდეგი რეკომენდაციებით:

- დამუშავებისთვის პასუხისმგებელმა პირებმა მონაცემთა დაცვის შესახებ უნდა იფიქრონ დამუშავების ოპერაციის დაგეგმვის *საწყისი ეტაპებიდანვე,* სანამ მოხდება დამუშავების ღონისძიებების განსაზღვრა.
- იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელ პირს ჰყავს მონაცემთა დაცვის ოფიცერი (DPO), EDPB-ის რეკომენდაციაა, DPO აქტიურად ჩაერთოს DPbDD პრინციპების შესყიდვისა და განვითარების პროცედურებში და დამუშავების ცხოვრების მთლიან ციკლში ინტეგრაციის კუთხით.
- დამუშავების ოპერაცია, შესაძლოა, იყოს *სერტიფიცირებული.* დამუშავების ოპერაციის სერტიფიცირების შესაძლებლობა დამუშავებისთვის პასუხისმგებელ პირს უზრუნველყოფს დამატებითი ღირებულებით, მწარმოებლებისგან / უფლებამოსილი პირებისგან დამუშავების სხვადასხვა პროგრამების, მოწყობილობების, სერვისების და/ან სისტემების არჩევისას. შესაბამისად, მწარმოებლები დამუშავების გადაწყვეტების შემუშავების ცხოვრების ციკლში DPbDD პრინციპების დემონსტრირებას უნდა ესწრაფოდნენ. სერტიფიცირების ბეჭედი მონაცემთა სუბიექტებს, აგრეთვე, გაუადვილებს არჩევანის გაკეთებას სხვადასხვა პროდუქტებს და სერვისებს შორის. დამუშავების პროცესის სერტიფიცირება მწარმოებლებს, დამუშავებაზე უფლებამოსილ პირებსა და დამუშავებისთვის პასუხისმგებელ პირებს გარკვეული კონკურენტული უპირატესობით უზრუნველყოფს და გააუმჯობესებს მონაცემთა სუბიექტების ნდობას მათი პერსონალური მონაცემების დამუშავების მიმართ. თუ სერტიფიცირება არ არის ხელმისაწვდომი, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა მოიძიონ სხვა გარანტიები, რომ მწარმოებლები ან დამუშავებაზე უფლებამოსილი პირები შეასრულებენ DPbDD-ის მოთხოვნებს.
- დამუშავებისთვის პასუხისმგებელმა პირებმა, დამუშავებაზე უფლებამოსილ პირებმა და მწარმოებლებმა უნდა გაითვალისწინონ თავიანთი ვალდებულება, 18 წლამდე ასაკის ბავშვები და სხვა მოწყვლადი ჯგუფები უზრუნველყონ სპეციალური დაცვით, DPbDD პრინციპების შესრულებისას.
- მწარმოებლებმა და დამუშავებაზე უფლებამოსილმა პირებმა ხელი უნდა შეუწყონ DPbDD-ის იმპლემენტაციას, რათა დამუშავებისთვის პასუხისმგებელ პირს დაეხმარონ 25-ე მუხლით დადგენილი ვალდებულებების შესრულებაში. მეორეს მხრივ, დამუშავებისთვის პასუხისმგებელმა პირებმა არ უნდა აირჩიონ მწარმოებლები ან

დამუშავებაზე უფლებამოსილი პირები, რომლებიც არ უზრუნველყოფენ სისტემებს, რომლებიც დამუშავებისთვის პასუხისმგებელ პირს საშუალებას აძლევს ან ეხმარება 25-ე მუხლის მოთხოვნების შესრულებაში, რადგან შესაბამისი პრინციპების განუხორციელებლობისთვის დამუშავებისთვის პასუხისმგებელი პირი იქნება პასუხისმგებელი.

- მწარმოებლებმა და დამუშავებაზე უფლებამოსილმა პირებმა აქტიური როლი უნდა შეასრულონ „უახლესი ტექნოლოგიების“ კრიტერიუმის დაკმაყოფილების კუთხით და დამუშავებისთვის პასუხისმგებელ პირებს შეატყობინონ „უახლეს ტექნოლოგიებში“ განხორციელებული ცვლილებების შესახებ, თუ აღნიშნული გავლენას ახდენს მოქმედი ღონისძიებების ეფექტურობაზე. დამუშავებისთვის პასუხისმგებელმა პირებმა აღნიშნული მოთხოვნა უნდა გაითვალისწინონ ხელშეკრულებაში ერთ-ერთი პუნქტის სახით, რათა უზრუნველყოფილი იქნეს მათი ინფორმირება.
- EDPB დამუშავებისთვის პასუხისმგებელ პირებს მიმართავს რეკომენდაციით, მწარმოებლებს და დამუშავებაზე უფლებამოსილ პირებს მოსთხოვოს დემონსტრირება იმისა, თუ რამდენად უწყობს კომპიუტერული ტექნიკა, კომპიუტერული პროგრამები, სერვისები ან სისტემები დამუშავებისთვის პასუხისმგებელ პირს ხელს, შეასრულოს ანგარიშვალდებულების მოთხოვნები, DPbDD-ის შესაბამისად, მაგალითად, პრინციპებისა და უფლებების განმახორციელებელი ზომებისა და დაცვის მექანიზმების ეფექტურობის დემონსტრირებისთვის საქმიანობის შესრულების ძირითადი ინდიკატორების გამოყენების გზით.
- EDPB ხაზს უსვამს პრინციპებისა და უფლებების ეფექტურად განხორციელებისთვის ჰარმონიზებული მიდგომის საჭიროებას და იმ ასოციაციებს და ორგანოებს, რომლებიც მე-40 მუხლის შესაბამისად ამზადებენ ქცევის კოდექსებს, მიმართავს რეკომენდაციით, კოდექსებში, აგრეთვე, გაითვალისწინონ სექტორის შესაბამისი ინსტრუქციები DPbDD-ის შესახებ.
- დამუშავებისთვის პასუხისმგებელი პირები მონაცემთა სუბიექტებს სამართლიანად უნდა მოექცნენ და უნდა უზრუნველყონ გამჭვირვალობა იმასთან დაკავშირებით, თუ როგორ აფასებენ DPbDD-ის განხორციელებას და როგორ ადასტურებენ მის ეფექტურობას. აღნიშნული ვალდებულება მსგავსია დამუშავებისთვის პასუხისმგებელ პირთა ვალდებულებისა, დაადასტურონ GDPR-თან შესაბამისობა, ანგარიშვალდებულების პრინციპის ჭრილში.
- მონაცემთა დაცვის ტექნოლოგიები (PET), რომელთაც მიაღწიეს უახლესი ტექნოლოგიების სიმწიფის დონეს, შესაძლოა გამოყენებული იქნეს ღონისძიების სახით, DPbDD მოთხოვნების შესაბამისად, თუ ეს

მიზანშეწონილია რისკზე დაფუძნებული მიდგომის ფარგლებში. თავად PET შესაძლოა, არ მოიცავდეს 25-ე მუხლით დადგენილ ვალდებულებებს. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეაფასოს, თუ რამდენად მიზანშეწონილია და ეფექტურია მოცემული ზომა, მონაცემთა დაცვის პრინციპებისა და მონაცემთა სუბიექტების უფლებების განხორციელების კუთხით.

- სისტემები, რომლებიც რეგულაციის ამოქმედებამდე არსებობდნენ, DPbDD-სთან დაკავშირებით, ექვემდებარებიან იგივე ვალდებულებებს, რასაც ახალი სისტემები. იმ შემთხვევაში, თუ რეგულაციის ამოქმედებამდე არსებული სისტემა ჯერ არ აკმაყოფილებს DPbDD მოთხოვნებს, ხოლო შესაბამისი ვალდებულებების შესასრულებლად შეუძლებელია ცვლილებების განხორციელება, ეს ნიშნავს, რომ სისტემა ვერ აკმაყოფილებს GDPR-ით დადგენილ ვალდებულებებს და დაუშვებელია მისი გამოყენება პერსონალური მონაცემების დასამუშავებლად.
- 25-ე მუხლი არ ითვალისწინებს ზღვარის შემცირებას მცირე და საშუალო საწარმოებისთვის. ქვემოთ წარმოდგენილი საკითხები ხელს შეუწყობს მცირე და საშუალო საწარმოების შესაბამისობას 25-ე მუხლთან:
    i. რისკის შეფასებების განხორციელება ადრეულ ეტაპზე
    ii. მცირე მასშტაბის დამუშავებით დაწყება - მისი მასშტაბისა და კომპლექსურობის გაფართოება შემდგომ
    iii. მწარმოებლების და დამუშავებაზე უფლებამოსილი პირების მიერ DPbDD მოთხოვნებთან შესაბამისობის გარანტიების მოძიება, როგორიცაა, სერტიფიცირება და ქცევის კოდექსების დაცვა
    iv. იმ პარტნიორებთან თანამშრომლობა, რომელთაც [მონაცემთა დაცვის/რეგულაციის მოთხოვნებთან შესაბამისობის კუთხით] კარგი ისტორია აქვთ
    v. მონაცემთა დაცვის ორგანოებთან კომუნიკაციის ქონა
    vi. მონაცემთა დაცვის ორგანოებისა და EDPB-ს სახელმძღვანელო დოკუმენტების წაკითხვა
    vii. ხელმისაწვდომობის შემთხვევაში, ქცევის კოდექსების დაცვა
    viii. დახმარებისა და კონსულტაციის მისაღებად, პროფესიონალებისათვის მიმართვა.

ევროპის მონაცემთა დაცვის საბჭოს სახელით

თავმჯდომარე

(ანდრეა იელინეკი)