29-ე მუხლის მონაცემთა დაცვის სამუშაო ჯგუფი

17/EN
WP260 rev.01

29-ე მუხლის სამუშაო ჯგუფი

სახელმძღვანელო რეკომენდაცია გამჭვირვალობის პრინციპის შესახებ, 2016/679 რეგულაციის მიხედვით

მიღების თარიღი: 2017 წლის 29 ნოემბერი
ბოლო გადახედვის თარიღი: 2018 წლის 11 აპრილი

პერსონალური მონაცემების დამუშავებასთან დაკავშირებით ფიზიკურ პირთა უფლებების დაცვის შესახებ სამუშაო ჯგუფი

შექმნილია ევროპული პარლამენტის და საბჭოს 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივის საფუძველზე.

აღნიშნული დირექტივის 29-ე და 30-ე მუხლების გათვალისწინებით,

სამუშაო ჯგუფის რეგლამენტზე დაყრდნობით,

სამუშაო ჯგუფი ამტკიცებს ქვემოთ წარმოდგენილ სახელმძღვანელო პრინციპებს:

სამუშაო ჯგუფი შექმნილია 95/46/EC დირექტივის 29-ე მუხლის საფუძველზე. იგი დამოუკიდებელი ევროპული საკონსულტაციო ორგანოა, რომელიც მუშაობს მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის საკითხებზე. მისი ფუნქციები აღწერილია 95/46/EC დირექტივის 30-ე მუხლში და 2002/58/EC დირექტივის მე-15 მუხლში.

სამდივნო უზრუნველყოფილია ევროკომისიის ფუნდამენტური უფლებებისა და მოქალაქეობის დირექტორატის მიერ, მართლმსაჯულების გენერალური დირექტორატი, ბელგია, ოფისი No MO-59 02/013.

ვებგვერდი: http://ec.europa.eu/newsroom/article29/news.cfm?item type=1358&tpa id=6936

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

სარჩევი

შესავალი 4

გამჭვირვალობის მნიშვნელობა 7

გამჭვირვალობის ელემენტები, GDPR-ის თანახმად 8

„მოკლე, გამჭვირვალე, გასაგები და მარტივად ხელმისაწვდომი“ 9

„ნათელი და მარტივი ენა“ 11

„წერილობით ან სხვა ფორმით“ 16

„... ინფორმაციის მიწოდება შესაძლებელია ზეპირი ფორმით“ 18

„უფასო“ 19

ინფორმაცია, რომელიც უნდა მიეწოდოს მონაცემთა სუბიექტს - მე-13 და მე-14 მუხლები 20

შინაარსი 20

„სათანადო ზომები“ 20

ინფორმაციის მიწოდების ოპერატიულობა 21

მე-13 და მე-14 მუხლებით გათვალისწინებულ ინფორმაციაში ცვლილებების განხორციელება 24

მე-13 და მე-14 მუხლით გათვალისწინებულ ინფორმაციაში განხორციელებული ცვლილებების შესახებ მონაცემთა სუბიექტებისთვის შეტყობინების ვადები 26

მოდალობები - ინფორმაციის მიწოდების ფორმატი 27

მრავალშრიანი მიდგომა ციფრულ გარემოში და მრავალშრიანი განაცხადები/შეტყობინებები კონფიდენციალობის შესახებ 28

მრავალშრიანი მიდგომა არა-ციფრულ გარემოში 30

„მიწოლის“ და „გამოქაჩვის“ შეტყობინებები 31

სხვა ტიპის „შესაფერისი ზომები“ 32

ინფორმაცია პროფილირების და ავტომატიზებული გადაწყვეტილების მიღების შესახებ 34

სხვა საკითხები - რისკები, წესები და დაცვის მექანიზმები 34

შემდგომ დამუშავებასთან დაკავშირებული ინფორმაცია 36

ვიზუალიზაციის ინსტრუმენტები 38

სერტიფიცირების მექანიზმები, ბეჭდები და ნიშნები 40

მონაცემთა სუბიექტების უფლებების განხორციელება 41

გამონაკლისები ინფორმაციის უზრუნველყოფის ვალდებულებიდან 42

გამონაკლისები მე-13 მუხლით დადგენილი ვალდებულებებიდან 42

გამონაკლისები მე-14 მუხლით დადგენილი ვალდებულებებიდან.....*44*
„ინფორმაციის მიწოდება შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ/გაუმართლებელ ძალისხმევასთან“.....44
„შეუძლებელია“ 45
„შეუძლებელია მონაცემთა წყაროს შესახებ ინფორმაციის მიწოდება“.....46
„არაპროპორციულად დიდი ძალისხმევა“.....46
„მნიშვნელოვნად დააზიანებს მიზნების მიღწევას“ 49
„მონაცემთა შეგროვება ან გაცემა ცალსახად არის დადგენილი კანონით“ 50
„კონფიდენციალურობა, რომელიც საიდუმლოების დაცვის ვალდებულებიდან მომდინარეობს“51

შეზღუდვები მონაცემთა სუბიექტის უფლებებზე 52

გამჭვირვალობა და მონაცემთა უსაფრთხოების დარღვევა 54

დანართი 55

ინფორმაცია, რომელიც მონაცემთა სუბიექტს უნდა მიაწოდოს დამუშავებისთვის პასუხისმგებელმა პირმა მე-13 და მე-14 მუხლების თანახმად..... 55

შესავალი

1. წინამდებარე სახელმძღვანელო პრინციპები წარმოადგენს პრაქტიკულ ინსტრუქციებს ინტერპრეტაციასთან დაკავშირებით, რომელიც მოამზადა 29-ე მუხლის სამუშაო ჯგუფმა (WP29), გამჭვირვალობის ახალი ვალდებულების შესახებ, რომელიც უკავშირდება მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR)[1] თანახმად პერსონალური მონაცემების დამუშავებას. გამჭვირვალობა GDPR-ით გათვალისწინებული ყოვლისმომცველი ვალდებულებაა, რომელიც სამ ძირითად სფეროზე ვრცელდება: (1) ინფორმაციის მიწოდება მონაცემთა სუბიექტებისთვის, სამართლიან დამუშავებასთან დაკავშირებით; (2) მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთა კომუნიკაცია მონაცემთა სუბიექტებთან, ამ უკანასკნელთათვის GDPR-ით გათვალისწინებული უფლებების შესახებ; და (3) მონაცემთა სუბიექტების უფლებების განხორციელების ხელშეწყობა მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთა მიერ.[2] იმის გათვალისწინებით, რომ გამჭვირვალობის ვალდებულებასთან შესაბამისობა წარმოადგენს ევროკავშირის 2016/680 დირექტივის[3] საფუძველზე მონაცემთა დამუშავებასთან დაკავშირებულ მოთხოვნას,[4] წინამდებარე სახელმძღვანელო პრინციპები, აგრეთვე, ვრცელდება აღნიშნული პრინციპის ინტერპრეტაციაზე. სახელმძღვანელო პრინციპები, მსგავსად WP29-ის მიერ შემუშავებული სხვა სახელმძღვანელო პრინციპებისა, ზოგადად განკუთვნილია და ვრცელდება მონაცემთა **დამუშავებისთვის პასუხისმგებელ პირებზე** მათი სექტორული, ინდუსტრიული თუ მარეგულირებელი თავისებურებების მიუხედავად. შეუძლებელია, რომ სახელმძღვანელო პრინციპები ითვალისწინებდეს ყველა იმ ნიუანსს და ცვლადს, რომელიც წარმოიშობა კონკრეტულ სექტორში, ინდუსტრიაში თუ რეგულირებად სფეროში მოქმედი გამჭვირვალობის ვალდებულების კონტექსტში. ამავდროულად, სახელმძღვანელო პრინციპების მიზანია,

[1] ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის № 95/46/EC დირექტივა პერსონალურ მონაცემთა დამუშავებასა და აღნიშნულ მონაცემთა თავისუფლად მოძრაობასთან დაკავშირებით ფიზიკური პირების უფლებების დაცვის შესახებ.

[2] ეს საახელმძღვანელო პრინციპები ადგენს ზოგად პრინციპებს მონაცემთა სუბიექტების უფლებების განხორციელების შესახებ და არ ითვალისწინებს კონკრეტულ მოდალობებს თითოეული ინდივიდუალური მონაცემთა სუბიექტის უფლებებთან დაკავშირებით.

[3] ევროპარლამენტის და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680 უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ, რომელიც აუქმებს საბჭოს ჩარჩო გადაწყვეტილებას 2008/977/JHA.

[4] გამჭვირვალობა არ არის იმ პრინციპთაგანი, რომელიც ეხება მონაცემთა დამუშავებას და გათვალისწინებულია ევროკავშირის 2016/680 დირექტივის მე-4 მუხლით; ამავდროულად, პრეამბულის 26-ე პუნქტის თანახმად, პერსონალური მონაცემების დამუშავება უნდა იყოს „კანონიერი, სამართლიანი და გამჭვირვალე“ შესაბამის ფიზიკურ პირებთან მიმართებით.

დამუშავებისთვის პასუხისმგებელ პირებს დაეხმაროს, მაღალ დონეზე, იმის გააზრებაში, თუ რას გულისხმობს გამჭვირვალობის ვალდებულება პრაქტიკაში, WP29-ის ინტერპრეტაციის თანახმად, და რა მიდგომას უნდა იყენებდნენ ისინი იმისათვის, რომ მათ უზრუნველყონ, როგორც გამჭვირვალობა, ისე გამჭვირვალობის მიზნით მიღებული ზომების სამართლიანობა და ანგარიშვალდებულება.

2. გამჭვირვალობა არის ევროკავშირის სამართლის მახასიათებელი პრინციპი, რომელიც დიდი ხნის წინ დამკვიდრდა.[5] იგი ეხება ნდობის ხელშეწყობას იმ პროცესის მიმართ, რომელიც გავლენას ახდენს მოქალაქეებზე. კერძოდ, მოქალაქეებს უნდა ესმოდეთ ამ პროცესების არსი და საჭიროების შემთხვევაში, უნდა შეძლონ მათი გასაჩივრება. იგი, აგრეთვე, წარმოადგენს სამართლიანობის პრინციპის გამოხატულებას პერსონალური მონაცემების დამუშავებასთან დაკავშირებით, რომელიც გათვალისწინებულია ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლით. GDPR-ის თანახმად (მუხლი 5(1)(a)[6]), გარდა იმ მოთხოვნისა, რომ მონაცემები კანონიერად და სამართლიანად უნდა იქნას დამუშავებული, გამჭვირვალობა, აგრეთვე, წარმოადგენს აღნიშნული პრინციპების ფუნდამენტურ ასპექტს.[7] გამჭვირვალობა განუყოფლად არის დაკავშირებული სამართლიანობასთან და ანგარიშვალდებულების ახალ პრინციპთან, რომელსაც GDPR-ი შეიცავს. 5.2 მუხლიდან მომდინარეობს, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა ნებისმიერ მომენტში უნდა შეძლოს იმის დემონსტრირება, რომ პერსონალური მონაცემების დამუშავება ხდება გამჭვირვალედ, მონაცემთა სუბიექტთან მიმართებით.[8] აღნიშნულთან დაკავშირებულია ანგარიშვალდებულების პრინციპი, რომელიც მოითხოვს დამუშავების ოპერაციების გამჭვირვალობას, რათა

[5] TEU-ს 1-ლი მუხლი მიუთითებს გადაწყვეტილებების „მაქსიმალურად ღიად და მოქალაქეებთან მაქსიმალურად მჭიდრო კონსულტაციის საფუძველზე“ მიღებაზე; 11(2) მუხლის თანახმად, „დაწესებულებებმა უნდა შეინარჩუნონ ღია, გამჭვირვალე და რეგულარული დიალოგი ასოციაციებისა და სამოქალაქო საზოგადოების წარმომადგენლებთან“; TFEU-ს მე-15 მუხლი სხვა საკითხებთან ერთად, ეხება ევროკავშირის მოქალაქეთა უფლებას, ჰქონდეთ წვდომა ევროკავშირის დაწესებულებების, ორგანოებისა და უწყებების დოკუმენტებზე და ევროკავშირის დაწესებულებების, ორგანოების, ოფისებისა და უწყებების მოთხოვნებზე, რათა მათი წარმოებები იყოს გამჭვირვალე.

[6] „პერსონალური მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად და გამჭვირვალედ, მონაცემთა სუბიექტთან მიმართებით.“

[7] დირექტივაში 95/46/EC გამჭვირვალობა მხოლოდ ნაგულისხმევია პრეამბულის 38-ე პუნქტში, რომლის თანახმადაც მონაცემთა დამუშავება უნდა იყოს სამართლიანი, თუმცა, მასზე ცალსახად არ მიუთითებს ექვივალენტური მუხლი 6(1)(a).

[8] GDPR-ის 5.2 მუხლის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები ვალდებულია, მოახდინოს გამჭვირვალობის დემონსტრირება (ხუთ სხვა პრინციპთან ერთად, რომელიც უკავშირდება მონაცემთა დამუშავებას და წარმოდგენილია 5.1 მუხლში), ანგარიშვალდებულების პრინციპის ფარგლებში.

დამუშავებისთვის პასუხისმგებელმა პირებმა შეძლონ GDPR-ით დადგენილ ვალდებულებებთან შესაბამისობის დემონსტრირება.[9]

3. GDPR-ის პრეამბულის 171-ე პუნქტის შესაბამისად, თუ დამუშავება 2018 წლის 25 მაისიდანუკვე მიმდინარეობს, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია უზრუნველყოს დამუშავების შესაბამისობა 2018 წლის 25 მაისის მდგომარეობით არსებულ გამჭვირვალობის ვალდებულებებთან (GDPR-ით დადგენილ სხვა ვალდებულებებთან ერთად). აღნიშნული ნიშნავს იმას, რომ 2018 წლის 25 მაისამდე, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა გადახედონ ყველა იმ ინფორმაციას, რომელიც მიაწოდეს მონაცემთა სუბიექტებს, მათი პერსონალური მონაცემების დამუშავების შესახებ (მაგ., კონფიდენციალობის განაცხადის/შეტყობინების და ა.შ. სახით), რათა უზრუნველყონ გამჭვირვალობასთან დაკავშირებულ მოთხოვნებთან შესაბამისობა, ხოლო ეს მოთხოვნები განხილულია წინამდებარე სახელმძღვანელო პრინციპებში. იმ შემთხვევაში, თუ ამგვარ ინფორმაციაში განხორციელდება რაიმე შესწორებები ან დამატებები, დამუშავებისთვის პასუხისმგებელი პირები ვალდებულები არიან, მონაცემთა სუბიექტებს მკაფიოდ განუმარტონ, რომ ეს ცვლილებები განხორციელდა GDPR-ის მოთხოვნებთან შესაბამისობის მიზნით. WP29 გასცემს რეკომენდაციას, რომ ასეთი ცვლილებების ან დამატებების შესახებ აქტიურად მიეწოდოს ინფორმაცია მონაცემთა სუბიექტებს, თუმცა, როგორც მინიმუმ, დამუშავებისთვის პასუხისმგებელმა პირებმა ეს ინფორმაცია საჯაროდ ხელმისაწვდომი უნდა გახადონ (მაგ., გამოაქვეყნონ თავიანთ ვებგვერდზე). თუ ცვლილებები და დამატებები იქნება არსებითი ან მატერიალური მნიშვნელობის, მაშინ, 29-32 პუნქტების შესაბამისად (იხ. ქვემოთ), დამუშავებისთვის პასუხისმგებელი პირები ვალდებულები არიან, ასეთი ცვლილებების შესახებ აქტიურად მიაწოდონ ინფორმაცია მონაცემთა სუბიექტებს.

4. გამჭვირვალობა, თუ მასთან დაკავშირებული მოთხოვნები დაცულია მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ, მონაცემთა სუბიექტებს აძლიერებს, რათა მათ მოითხოვონ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისა და და **დამუშავებაზე** უფლებამოსილი პირების ანგარიშვალდებულება და თავად აკონტროლონ თავიანთი პერსონალური მონაცემები, მაგალითად, ინფორმირებული თანხმობის უზრუნველყოფის ან უკან გახმობის და მათი, როგორც მონაცემთა სუბიექტის უფლებების

[9] მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთა ვალდებულებას, მიიღონ ტექნიკური და ორგანიზაციული ზომები, რათა უზრუნველყონ და შეძლონ დემონსტრირება იმისა, რომ დამუშავება ხორციელდება GDPR-თან შესაბამისობაში, ადგენს 24.1 მუხლი.

განხორციელების გზით.[10] GDPR-ის თანახმად, გამჭვირვალობის კონცეფცია არის მომხმარებელზე ორიენტირებული და არ წარმოადგენს მხოლოდ ლეგალურ ცნებას. მისი განხორციელება ხდება მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებზე და **დამუშავებაზე** უფლებამოსილ პირებზე კონკრეტული მოთხოვნების დაწესების გზით, რომლებსაც სხვადასხვა მუხლები შეიცავს. პრაქტიკული (ინფორმირებასთან დაკავშირებული) მოთხოვნები წარმოდგენილია GDPR-ის 12-14 მუხლებში. ამავდროულად, ინფორმაციის ხარისხი, ხელმისაწვდომობა და გასაგებობა ისეთივე მნიშვნელოვანია, როგორც გამჭვირვალობასთან დაკავშირებული იმ ინფორმაციის შინაარსი, რომელიც მონაცემთა სუბიექტებისათვის უნდა იქნას უზრუნველყოფილი.

5. GDPR-ის გამჭვირვალობის მოთხოვნები ვრცელდება დამუშავების სამართლებრივი საფუძვლისდა მიუხედავად, დამუშავების სიცოცხლის ციკლის ნებისმიერ ეტაპზე. აღნიშნული მკაფიოდ მომდინარეობს მე-12 მუხლიდან, რომლის თანახმადაც გამჭვირვალობა ვრცელდება მონაცემთა დამუშავების ციკლის შემდეგ ეტაპებზე:
    - მონაცემთა დამუშავების ციკლის დაწყებამდე ან დაწყებისას, ე.ი., როდესაც პერსონალური მონაცემების შეგროვება ხდება მონაცემთა სუბიექტისგან ან ხდება მონაცემების სხვაგვარად მოპოვება;
    - დამუშავების მთლიანი პერიოდის მანძილზე, ე.ი. როდესაც ხორციელდება კომუნიკაცია მონაცემთა სუბიექტებთან, მათი უფლებების შესახებ; და
    - კონკრეტულ მომენტებში, დამუშავების მიმდინარეობისას, მაგალითად, როდესაც ადგილი აქვს მონაცემთა უსაფრთხოების დარღვევას ან დამუშავებაში არსებითი ცვლილებების განხორციელებას.

გამჭვირვალობის მნიშვნელობა

6. გამჭვირვალობა არ არის განმარტებული GDPR-ში. დირექტივის პრეამბულის 39-ე პუნქტი ინფორმაციული ხასიათისაა და აღწერს გამჭვირვალობის პრინციპის მნიშვნელობას და გავლენას მონაცემთა დამუშავების კონტექსტში:

[10] მაგ., იხ. გენერალური ადვოკატის, კრუზ ვილალონის მოსაზრება (2015 წლის 9 ივლისი) Bara-ს საქმეში (საქმე C-201/14), პ.74: *„პერსონალური მონაცემების დამუშავების შესახებ მონაცემთა სუბიექტების ინფორმირების მოთხოვნა, რომელიც უზრუნველყოფს ყველა დამუშავების გამჭვირვალობას, კიდევ უფრო მნიშვნელოვანია იმის გათვალისწინებით, რომ იგი გავლენას ახდენს მონაცემთა სუბიექტების მიერ დამუშავებულ მონაცემებზე წვდომის უფლების განხორციელებაზე, რომელზეც მიუთითებს 95/46 დირექტივის მე-12 მუხლი, და ამ მონაცემების დამუშავების შეწყვეტის მოთხოვნის უფლების განხორციელებაზე, რომელსაც ითვალისწინებს ამავე დირექტივის მე-14 მუხლი.“*

„ფიზიკური პირებისთვის უნდა იყოს ნათელი, რომ ხდება მათთან დაკავშირებული პერსონალური მონაცემების შეგროვება, გამოყენება, გაცნობა ან სხვა სახით დამუშავება. მათთვის ასევე უნდა იყოს ცნობილი, თუ რა მოცულობით ხდება ან მოხდება მათი პერსონალური მონაცემების დამუშავება. გამჭვირვალობის პრინციპის მოთხოვნაა, რომ ნებისმიერი ინფორმაცია და კომუნიკაცია, რომელიც უკავშირდება პერსონალური მონაცემების დამუშავებას, უნდა იყოს ადვილად ხელმისაწვდომი და გასაგები, ასევე, ნათლად და მარტივი ენით გადმოცემული. კერძოდ, ეს პრინციპი ვრცელდება მონაცემთა სუბიექტებისთვის დამუშავებისთვის პასუხისმგებელი პირმა პირის ვინაობისა და დამუშავების მიზნების შესახებ მიწოდებულ ინფორმაციაზე, და დამატებით ინფორმაციაზე, რომელიც უზრუნველყოფს შესაბამისი ფიზიკური პირების შესახებ ინფორმაციის გამჭვირვალე დამუშავებას და მათ უფლებას მიიღონ მათი პერსონალური მონაცემების დამუშავების დადასტურება და დამუშავებული მონაცემები.“

გამჭვირვალობის ელემენტები, GDPR-ის თანახმად

7. GDPR-ში გამჭვირვალობასთან დაკავშირებული ძირითადი მუხლები (ვინაიდან ისინი ვრცელდება მონაცემთა სუბიექტის უფლებებზე) წარმოდგენილია III თავში (მონაცემთა სუბიექტის უფლებები). მე-12 მუხლი ადგენს ზოგად წესს, რომელიც ვრცელდება: მონაცემთა სუბიექტებისთვის ინფორმაციის მიწოდებაზე (მუხლები 13-14); მონაცემთა სუბიექტებთან მათი უფლებების განხორციელების შესახებ კომუნიკაციაზე (მუხლები 15-22); და მონაცემთა უსაფრთხოების დარღვევის შეტყობინების შესახებ (მუხლი 34). კერძოდ, მე-12 მუხლის თანახმად, შესაბამისი ინფორმაცია ან კომუნიკაცია უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

    - უნდა იყოს მოკლე, გამჭვირვალე, გასაგები და მარტივად ხელმისაწვდომი (მუხლი 12.1);
    - გამოყენებული უნდა იქნას ნათელი და მარტივი ენა (მუხლი 12.1);
    - ნათელი და მარტივი ენის გამოყენების შესახებ მოთხოვნა განსაკუთრებით მნიშვნელოვანია, როდესაც საქმე ეხება ინფორმაციის ბავშვებისთვის მიწოდებას (მუხლი 12.1);
    - ინფორმაციის მიწოდება უნდა მოხდეს წერილობით, „ან სხვა ფორმით, მათ შორის, სათანადო შემთხვევებში, ელექტრონულად“ (მუხლი 12.1);
    - მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში, ინფორმაციის მიწოდება შესაძლებელია ზეპირი ფორმით (მუხლი 12.1); და
    - ინფორმაციის მიწოდება უნდა განხორციელდეს უსასყიდლოდ (მუხლი 12.5).

„მოკლე, გამჭვირვალე, გასაგები და მარტივად ხელმისაწვდომი“

8. მოთხოვნა, რომ მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდება და მასთან კომუნიკაცია განხორციელდეს „მოკლედ და გამჭვირვალედ“ ნიშნავს იმას, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა ინფორმაცია/კომუნიკაცია ეფექტურად და ლაკონურად უნდა წარმოადგინონ, რათა არ გამოიწვიონ ინფორმაციისგან გადატვირთვა აღნიშნული ინფორმაცია მკაფიოდ უნდა იქნას გამიჯნული სხვა სახის ინფორმაციისგან, რომელიც არ ეხება კონფიდენციალობის დაცვას, მაგ., სახელშეკრულებო პირობები ან სარგებლობის ზოგადი პირობები. ონლაინ კონტექსტში, კონფიდენციალობის მრავალშრიანი განაცხადის/შეტყობინების გამოყენება შესაძლებლობას მისცემს მონაცემთა სუბიექტს, გადავიდეს განაცხადის / შეტყობინების კონკრეტულ ნაწილზე, რომელზეც სურს, რომ ჰქონდეს დაუყოვნებლივ წვდომა და მას არ მოუწევს დიდი მოცულობის ტექსტის დათვალიერება, კონკრეტული საკითხების მოძებნის მიზნით.

9. მოთხოვნა, რომ ინფორმაცია იყოს „გასაგები“ ნიშნავს იმას, რომ ინფორმაციის გაგება უნდა შეეძლოს სამიზნე აუდიტორიის საშუალო წევრს. გასაგები არის თუ არა ინფორმაცია მჭიდროდ არის დაკავშირებული მკაფიო და მარტივი ენის გამოყენების მოთხოვნასთან. ანგარიშვალდებული დამუშავებისთვის პასუხისმგებელი პირი ინფორმირებულია იმ ადამიანების თაობაზე, რომლის შესახებაც იგი ინფორმაციას აგროვებს და მას შეუძლია, რომ ეს ცოდნა გამოიყენოს იმის დასადგენად, თუ რა იქნება აუდიტორიისთვის გასაგები. მაგალითად, დამუშავებისთვის პასუხისმგებელი პირი, რომელიც პრაქტიკოსი სპეციალისტების შესახებ აგროვებს პერსონალურ მონაცემებს, ჩათვლის, რომ მის აუდიტორიას უფრო მეტი ესმის, ვიდრე პირი, რომელიც ბავშვების შესახებ აგროვებს პერსონალურ მონაცემებს. თუ დამუშავებისთვის პასუხისმგებელი პირი არ არის დარწმუნებული თუ რამდენად გაიგებს აუდიტორია შინაარსს ინფორმაციის გამჭვირვალობა და მომხმარებლისათვის განკუთვნილი ინტერფეისების/შეტყობინებების/პოლიტიკას და ა.შ. ეფექტურობასთან დაკავშირებით, მას აღნიშნულის შემოწმება შეუძლია - მაგ., ისეთი მექანიზმების გამოყენების გზით, როგორებიცაა, მომხმარებელთა პანელები, წაკითხვადობის გატესტვა, ფორმალური და არაფორმალური ინტერაქციები და დიალოგი შესაბამის ჯგუფებთან, მომხმარებელთა ადვოკატირების ჯგუფებთან და მარეგულირებელ ორგანოებთან, საჭიროების შესაბამისად.

10. გამჭვირვალობასთან დაკავშირებული ცენტრალური საკითხი, რომლებიც ამ დებულებებშია წარმოდგენილი, არის ის, რომ მონაცემთა სუბიექტს უნდა შეეძლოს წინასწარ განსაზღვრა, თუ რას მოიცავს დამუშავების ფარგლები და შედეგები და მათთვის მოგვიანებით არ უნდა იყოს გასაკვირი მათი

პერსონალური მონაცემების გამოყენების გზები. აღნიშნული სამართლიანობის მნიშვნელოვანი ასპექტია, GDPR-ის 5.1 მუხლის შესაბამისად, და მართლაც არის დაკავშირებული პრეამბულის 39-ე პუნქტთან, რომლის თანახმად: *„ფიზიკური პირები ინფორმირებულები უნდა იყვნენ პერსონალური მონაცემების დამუშავებასთან დაკავშირებული რისკების, წესების, დაცვის მექანიზმების და უფლებების შესახებ...“* კერძოდ, მონაცემთა კომპლექსური, ტექნიკური ან მოულოდნელი დამუშავების შემთხვევაში, WP29-ის პოზიცია მდგომარეობს შემდეგში: მე-13 და მე-14 მუხლებით გათვალისწინებული ინფორმაციის უზრუნველყოფასთან ერთად (ამ საკითხს წინამდებარე დოკუმენტი მოგვიანებით განიხილავს), დამუშავებისთვის პასუხისმგებელმა პირებმა ცალკე, მკაფიო ენით უნდა ჩამოაყალიბონ დამუშავების ყველაზე მნიშვნელოვანი შედეგები: სხვა სიტყვებით რომ ვთქვათ, რა გავლენა აქვს კონფიდენციალობის განაცხადში / შეტყობინებაში აღწერილ დამუშავებას მონაცემთა სუბიექტზე? ანგარიშვალდებულების პრინციპის შესაბამისად და პრეამბულის 39-ე პუნქტის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა შეაფასონ, მოცემული ტიპის დამუშავებაში მონაწილე ფიზიკური პირები ხომ არ იმყოფებიან რაიმე კონკრეტული რისკების წინაშე, რის შესახებაც მონაცემთა სუბიექტს უნდა ეცნობოს. აღნიშნული ხელს შეუწყობს დამუშავების იმ სახეობების იდენტიფიცირებას, რომელთაც შესაძლოა ყველაზე მნიშვნელოვანი გავლენა ჰქონდეს მონაცემთა სუბიექტების ფუნდამენტურ უფლებებზე და თავისუფლებებზე, მათი პერსონალური მონაცემების დაცვის ჭრილში.

11. „მარტივად ხელმისაწვდომობის“ ელემენტი ნიშნავს იმას, რომ მონაცემთა სუბიექტს არ უნდა უწევდეს ინფორმაციის მოძიება; მათთვის დაუყოვნებლივ უნდა იყოს ნათელი, თუ სად და როგორ შეიძლება ამ ინფორმაციის მიღება, მაგალითად, მონაცემთა სუბიექტთათვის ინფორმაციის პირდაპირ მიწოდების გზით ან ინფორმაციაზე ბმულის მიწოდებით, ინფორმაციის მკაფიოდ მონიშვნით ან ნეიტრალური ენით ფორმულირებულ კითხვაზე პასუხის სახით (მაგ., კონფიდენციალობის მრავალშრიანი განაცხადი/შეტყობინება, ხშირად დასმული კითხვები, კონტექსტუალური პოპ-აპ (pop-ups) ფანჯრები, რომლებიც აქტიურდება მას შემდეგ, რაც მონაცემთა სუბიექტი შეავსებს ონლაინ ფორმას, ან ციფრულ ინტერაქტიულ კონტექსტში - ჩატბოტის ინტერფეისის საშუალებით და ა.შ. ეს მექანიზმები ქვემოთ უფრო დეტალურად არის განხილული, მათ შორის, 33-ე-მე-40 პუნქტებში).

მაგალითი
ყველა ორგანიზაცია, რომელსაც აქვს საკუთარი ვებსაიტი, ვალდებულია, მასზე აქვეყნებდეს კონფიდენციალობის **შესახებ** განაცხადს/შეტყობინებას, ხოლო განაცხადის/შეტყობინების პირდაპირი ბმული ნათლად უნდა ჩანდეს ვებსაიტის თითოეულ გვერდზე, ფართოდ გავრცელებული ტერმინის ქვეშ

(მაგ., „კონფიდენციალობის დაცვა“, „კონფიდენციალობის პოლიტიკა“ ან „მონაცემთა დაცვის შესახებ შეტყობინება“). მარტივი ხელმისაწვდომობის მოთხოვნას ეწინააღმდეგება ტექსტის/ბმულის განთავსება იმგვარად ან ფერთა იმგვარი სქემის გამოყენება, რაც მას ნაკლებად შესამჩნევს ხდის ან ართულებს მის პოვნას ვებგვერდზე.

აპლიკაციების შემთხვევაში, საჭირო ინფორმაცია ხელმისაწვდომი უნდა იყოს ონლაინ მაღაზიაში, ჩამოტვირთამდე. აპლიკაციის დაყენების (ინსტალაციის) შემდეგ, ინფორმაცია აპლიკაციაში კვლავ მარტივად უნდა იყოს ხელმისაწვდომი. ამ მოთხოვნის დაკმაყოფილების ერთ-ერთი გზაა უზრუნველყოფა, რომ ინფორმაცია არ იყოს „ორზე მეტი დაწკაპუნების“ იქით (მაგ., აპლიკაციის მენიუში შესაძლებელია „კონფიდენციალობის დაცვის“/“მონაცემთა დაცვის“ ოფციის გათვალისწინება). ამას გარდა, კონფიდენციალობის შესახებ ინფორმაცია უნდა იყოს კონკრეტულ აპლიკაციაზე მორგებული და არ უნდა წარმოადგენდეს კონფიდენციალობის შესახებ იმ კომპანიის ზოგადი პოლიტიკის განაცხადს, რომელიც ფლობს აპლიკაციას ან მას საზოგადოებისათვის ხელმისაწვდომს ხდის.

WP29-ის რეკომენდაციის თანახმად, საუკეთესო პრაქტიკას წარმოადგენს ონლაინ კონტექსტში პერსონალური მონაცემების შეგროვების ადგილზე კონფიდენციალობის განაცხადის/შეტყობინების ბმულის განთავსება ან აღნიშნული ინფორმაციის ხელმისაწვდომობის უზრუნველყოფა იმავე გვერდზე, სადაც ხდება პერსონალური მონაცემების შეგროვება.

„ნათელი და მარტივი ენა“

12. წერილობით ინფორმაციასთან დაკავშირებით (და იმ შემთხვევაში, თუ წერილობითი ინფორმაციის მიწოდება ხდება ზეპირი ფორმით ან აუდიო/აუდიოვიზუალური მეთოდებით, მათ შორის, მხედველობის შეზღუდვის მქონე მონაცემთა სუბიექტებისთვის), დამუშავებისთვის პასუხისმგებელი პირი უნდა მისდევდეს საუკეთესო პრაქტიკებს და წერილობითი ინფორმაცია უნდა იყოს მკაფიოდ ფორმულირებული.[11] ენასთან დაკავშირებული მსგავსი მოთხოვნა (ნათელი, გასაგები ენა“) ევროკავშირის კანონმდებელს აქამდეც გამოუყენებია[12] და მასზე ცალსახად მიუთითებს GDPR-

[11] იხ. How to Write Clearly by the European Commission (2011), ხელმისაწვდომია: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.

[12] დირექტივა 93/13/EEC, მე-5 მუხლი მომხმარებელთა ხელშეკრულებებში უსამართლო პირობების შესახებ, 1993 წლის 5 აპრილი.

ის პრეამბულის 42-ე პუნქტი.[13] ნათელი და მარტივი ენის შესახებ მოთხოვნა ნიშნავს იმას, რომ ინფორმაცია მაქსიმალურად მარტივი ფორმით უნდა იქნას მიწოდებული და არ უნდა იქნას გამოყენებული რთული წინადადებები და ენობრივი სტრუქტურები. ინფორმაცია უნდა იყოს კონკრეტული და განსაზღვრული; იგი არ უნდა იყოს ფორმულირებული აბსტრაქტულად ან ამბივალენტურად და არ უნდა ტოვებდეს სივრცეს განსხვავებული ინტერპრეტაციებისთვის. კერძოდ, პერსონალური მონაცემების დამუშავების მიზანი და სამართლებრივი საფუძველი უნდა იყოს მკაფიო.

ცუდი პრაქტიკის მაგალითები

ქვემოთ წარმოდგენილი ფრაზები ნათლად არ აღწერს დამუშავების მიზნებს:

- *„თქვენი პერსონალური მონაცემები შესაძლოა გამოვიყენოთ ახალი სერვისების შემუშავებისთვის“* (არ არის ნათელი, თუ რაში მდგომარეობს „სერვისები“ და როგორ მოხდება მონაცემების გამოყენება მათი შემუშავებისთვის);
- *„თქვენი პერსონალური მონაცემები შესაძლოა კვლევის მიზნებისთვის გამოვიყენოთ“* (არ არის ნათელი, თუ რა სახის „კვლევა“ იგულისხმება); და
- *„თქვენი პერსონალური მონაცემები შესაძლოა გამოვიყენოთ პერსონალიზებული სერვისების შეთავაზების მიზნით“* (ბუნდოვანია, თუ რას მოიცავს „პერსონალიზაცია“).

კარგი პრაქტიკის მაგალითები[14]

- *„თქვენი შოპინგის ისტორიას შევინახავთ და თქვენს მიერ შეძენილი პროდუქტების შესახებ დეტალურ ინფორმაციას გამოვიყენებთ იმისათვის, რომ შემოგთავაზოთ სხვა პროდუქტები, რომელიც ჩვენი აზრით, თქვენ დაგაინტერესებთ“* (ნათელია, თუ რა ტიპის მონაცემების დამუშავება განხორციელდება, და რომ მონაცემთა სუბიექტი დაექვემდებარება პროდუქციის მიზნობრივ რეკლამებს, რისთვისაც გამოყენებული იქნება მათი მონაცემები);

[13] პრეამბულის 42-ე პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელი პირის მიერ წინასწარ შედგენილი თანხმობის განაცხადი უნდა იყოს გასაგები და გადმოცემული ადვილად ხელმისაწვდომი ფორმით, ნათელი და მარტივი ენით და არ უნდა შეიცავდეს უსამართლო პირობებს.

[14] გამჭვირვალობის მოთხოვნა არსებობს იმ მოვალეობისგან დამოუკიდებლად, რომელიც მონაცემთა დამმუშავებლებს ავალდებულებს, უზრუნველყონ დამუშავების სათანადო სამართლებრივი საფუძველი, მე-6 მუხლის შესაბამისად.

- *„თქვენს მიერ ჩვენს ვებსაიტზე განხორციელებული ვიზიტების და ვებსაიტის სხვადასხვა სექციებში გადაადგილების შესახებ ინფორმაციას შევინახავთ და შევაფასებთ ანალიტიკური მიზნებისთვის, რათა შევისწავლოთ, თუ როგორ იყენებენ ადამიანები ჩვენს ვებსაიტს, იმისათვის, რომ მისი გამოყენება გახდეს უფრო ინტუიციური“* (ნათელია, თუ რა ტიპის მონაცემები დამუშავდება და რა ტიპის ანალიზს განახორციელებს დამუშავებისთვის პასუხისმგებელი პირი); და
- *ჩვენ შევინახავთ ინფორმაციას იმის შესახებ, თუ რომელ სტატიებზე დააწკაპუნეთ, რათა შემდეგ გამოვიყენოთ ეს ინფორმაცია მიზნობრივი რეკლამისთვის, თქვენი ინტერესების შესაბამისად, ხოლო თქვენი ინტერესების იდენტიფიცირებას მოვახდენთ თქვენს მიერ წაკითხული სტატიების მიხედვით“* (ნათელია, თუ რას მოიცავს პერსონალიზაცია და როგორ მოხდება მონაცემთა სუბიექტის ინტერესების იდენტიფიცირება).

13. თავიდან უნდა იქნას აცილებული ისეთი ენობრივი კვალიფიკატორები, როგორიცაა: „შესაძლოა“, „სავარაუდოდ“, „ზოგიერთი“, „ხშირად“. თუ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი განუსაზღვრელ ენას იყენებს, ანგარიშვალდებულების პრინციპის შესაბამისად, მან უნდა დაასაბუთოს, თუ რატომ არის აუცილებელი ამგვარი ენის გამოყენება და უქმნის თუ არა იგი საფრთხეს დამუშავების სამართლიანობის პრინციპს. აბზაცები და წინადადებები კარგად უნდა იყოს სტრუქტურირებული, ხოლო იერარქიული ურთიერთმიმართების აღსანიშნავად გამოყენებული უნდა იქნას მსხვილი წერტილები და შეწევა. ტექსტი გადმოცემული უნდა იყოს აქტიური და არა პასიური ფორმით და თავიდან უნდა იქნას აცილებული ზედმეტი არსებითი სახელების გამოყენება. მონაცემთა სუბიექტისათვის მიწოდებული ინფორმაცია არ უნდა შეიცავდეს ზედმეტად ლეგალურ, ტექნიკურ ან სპეციალიზებულ ენას და ტერმინოლოგიას. თუ ინფორმაციის თარგმნა ხდება ერთ ან რამოდენიმე ენაზე, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს თარგმანის სიზუსტე და ფრაზეოლოგიისა და სინტაქსის გამართულობა, რათა მომხმარებელს არ მოუწიოს თარგმნილი ტექსტის გაშიფვრა და არ მოხდეს მისი განსხვავებულად ინტერპრეტაცია. (ტექსტის ერთ ან რამდენიმე ენაზე თარგმნა საჭიროა, თუ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის სამიზნეს[15] წარმოადგენს ამ ენებზე მოსაუბრე მონაცემთა სუბიექტები).

[15] მაგალითად, როდესაც დამუშავებისთვის პასუხისმგებელი პირიახდენს მოცემულ ენაზე შედგენილი ვებსაიტის ოპერირებას და/ან აქვს ვებგვერდის კონკრეტული ქვეყნისთვის შექმნილი ვერსია, და/ან ხელს უწყობს კონკრეტული წევრი სახელმწიფოს ვალუტაში საქონლის ან მომსახურების შეძენას. ეს

ინფორმაციის მიწოდება ბავშვების და სხვა მოწყვლადი ადამიანებისთვის

14. იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელი პირის სამიზნეს წარმოადგენს ბავშვები[16] ან თუ დამუშავებისთვის პასუხისმგებელმა პირებმა იცის ან უნდა იცოდეს, რომ მისი საქონელი/სერვისები განსაკუთრებით ბავშვების მიერ გამოიყენება (მათ შორის, იმ შემთხვევებში, როდესაც დამუშავებისთვის პასუხისმგებელი პირი ეყრდნობა ბავშვის თანხმობას)[17], დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია უზრუნველყოს, რომ გამოყენებული ენის სტილი, ტონი და სიტყვები არის შესაფერისი და რეზონირებს ბავშვებთან, რათა ადრესატი, რომელიც არის ბავშვი, მიხვდეს, რომ გზავნილი/ინფორმაცია მათკენ არის მიმართული.[18] ბავშვზე ორიენტირებული ენის გამოყენების მაგალითი შეგიძლიათ იხილოთ დოკუმენტში „გაეროს კონვენცია ბავშვის უფლებების შესახებ, ბავშვისთვის გასაგები ენით“, რომელიც, დედნისგან განსხვავებით, არ იყენებს სამართლებრივ ენას.[19]

15. WP29-ის პოზიციის თანახმად, გამჭვირვალობა არის ცალკე მდგომი უფლება, რომელიც ბავშვებზე და ზრდასრულებზე თანაბრად ვრცელდება. WP29 ხაზს უსვამს, რომ ბავშვები არ კარგავენ მონაცემთა სუბიექტის უფლებას გამჭვირვალობაზე მხოლოდ იმიტომ, რომ თანხმობა გასცა მშობლის პასუხისმგებლობის მქონე პირმა, ისეთ სიტუაციაში, რომელზეც ვრცელდება GDPR-ის მე-8 მუხლი. ასეთ თანხმობას, ხშირ შემთხვევაში, მშობლის პასუხისმგებლობის მქონე პირი გასცემს ერთჯერადად, თუმცა, ბავშვი (სხვა მონაცემთა სუბიქტის მსგავსად) ინარჩუნებს უფლებას გამჭვირვალობაზე, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთან ჩართულობის ფარგლებში. აღნიშნული შეესაბამება ბავშვის უფლებების შესახებ გაეროს კონვენციის მე-13 მუხლს, რომლის მიხედვითაც ბავშვს აქვს გამოხატვის

ყოველივე ნიშნავს იმას, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის სამიზნეს წარმოადგენს აღნიშნულ წევრ სახელმწიფოში მცხოვრები მონაცემთა სუბიექტები.

[16] ტერმინი „ბავშვი“ არ არის განმარტებული GDPR-ში, თუმცა, WP29 ითვალისწინებს, რომ ბავშვის უფლებების შესახებ გაეროს კონვენციის თანახმად, რომელიც რატიფიცირებული აქვს ევროკავშირის წევრ ყველა ქვეყანას, ბავშვი არის 18 წლამდე ასაკის პირი.

[17] ე.ი., 16 წელს მიღწეული პირი (ან თუ GDPR-ის 8.1 მუხლის შესაბამისად, წევრ სახელმწიფოში მოქმედი შიდასახელმწიფოებრივი კანონი ადგენს საინფორმაციო საზოგადოების სერვისების უზრუნველყოფაზე თანხმობის კონკრეტულ ასაკს 13-დან 16 წლამდე, ამ ასაკს მიღწეული ბავშვები).

[18] პრეამბულის 38-ე პუნქტის თანახმად: „არასრულწლოვნები სარგებლობენ პერსონალური მონაცემების დაცვის განსაკუთრებული უფლებით, რადგან მათთვის შეიძლება ნაკლებად იყოს ცნობილი ის რისკები, შედეგები, დაცვის მექანიზმები და მათი უფლებები, რომლებიც უკავშირდება პერსონალური მონაცემების დამუშავებას.“ პრეამბულის 58-ე პუნქტის თანახმად: „არასრულწლოვანთა განსაკუთრებული დაცვის საჭიროებიდან გამომდინარე ნებისმიერი ინფორმაცია, რომელიც არასრულწლოვანისთვის არის განკუთვნილი, უნდა იყოს ნათლად და არასრულწლოვანისთვის მარტივად და გასაგებად გადმოცემული.“

[19] https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf.

თავისუფლება, რაც მოიცავს ყველა სახის ინფორმაციის და იდეების მოძიების, მიღების და გაცემის უფლებას.[20] მნიშვნელოვანია აღინიშნოს, რომ მართალია კონკრეტული ასაკის ბავშვი პირადად არ გასცემს თანხმობას,[21] მე-8 მუხლი *არ ითვალისწინებს* გამჭვირვალობის მიზნით მიღებული ზომების მიმართვას მშობლის პასუხისმგებლობის მქონე პირისკენ, რომელიც გასცემს თანხმობას ბავშვის სახელით. შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები ვალდებულები არიან, ბავშვებისთვის განკუთვნილი გამჭვირვალობის ზომების გამოყენებთ (მუხლი 12.1, გამყარებულია პრეამბულის 38-ე და 58-ე პუნქტებით), უზრუნველყონ, რომ თუ მათი სამიზნე არიან ბავშვები ან თუ მათთვის ცნობილია, რომ მათი საქონელს და მომსახურებებს განსაკუთრებით წერა-კითხვის ასაკს მიღწეული ბავშვები იყენებენ, ინფორმაციის და კომუნიკაციის გადაცემა ხდება მკაფიო და მარტივი ენით ან იმ მედიუმის გამოყენებით, რომელიც ბავშვებისთვის მარტივად აღქმადია. ამავდროულად, ეჭვის გამორიცხვის მიზნით, WP29 ითვალისწინებს, რომ პატარა ასაკის ან წერა-კითხვის ასაკს მიუღწეველი ბავშვების შემთხვევაში, გამჭვირვალობის ზომები, შესაძლოა, აგრეთვე, მიმართული იყოს მშობლის პასუხისმგებლობის მქონე პირებისკენ, იმის გათვალისწინებით, რომ აღნიშნული ბავშვები, უმეტეს შემთხვევაში, ვერ გაიაზრებენ გამჭვირვალობასთან დაკავშირებული ყველაზე მარტივი წერილობითი ან არა-წერილობითი გზავნილების მნიშვნელობას.

16. თუ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის ცნობილია, რომ მათ საქონელს / მომსახურებას იყენებენ საზოგადოების სხვა მოწყვლადი წევრები (ან ისინი წარმოადგენენ მათი საქონლის/მომსახურების სამიზნე აუდიტორიას), მათ შორის, შშმ პირები ან ადამიანები, რომლებიც გარკვეულ სირთულეებს აწყდებიან ინფორმაციის ხელმისაწვდომობის კუთხით, აღნიშნული მონაცემთა სუბიექტების მოწყვლადობა გათვალისწინებული უნდა იქნას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის დამუშავებისთვის პასუხისმგებელი პირის მიერ, როდესაც იგი ახორციელებს შეფასებას, თუ როგორ უზრუნველყოს მონაცემთა აღნიშნულ სუბიექტებთან მიმართებით, გამჭვირვალობასთან დაკავშირებული ვალდებულებების შესრულება.[22] აღნიშნული დაკავშირებულია დამუშავებისთვის პასუხისმგებელი პირის მიერ

[20] ბავშვის უფლებების შესახებ გაეროს კონვენციის მე-13 მუხლის თანახმად: „ბავშვს უფლება აქვს თავისუფლად გამოხატოს თავისი აზრი; ეს უფლება შეიცავს ნებისმიერი სახის ინფორმაციისა და იდეის მოძიების, მიღების და გადაცემის თავისუფლებას საზღვრების მიუხედავად, ზეპირი, წერილობითი ან ბეჭდვითი ფორმით, ხელოვნების ნაწარმოების ფორმით ან ბავშვის არჩევანის შესაბამისად სხვა საშუალებების დახმარებით.“

[21] იხ. შენიშვნა 17 ზემოთ.

[22] მაგალითად, გაეროს კონვენცია შშმ პირთა უფლებების შესახებ მოითხოვს, რომ დახმარებისა და მხარდაჭერის სათანადო ფორმები იქნას უზრუნველყოფილი შშმ პირებისთვის, რათა მათ ჰქონდეთ ინფორმაციაზე წვდომა.

აუდიტორიის გაგების დონის შეფასების საჭიროებასთან, რაც მე-9 პუნქტშია განხილული.

„წერილობით ან სხვა ფორმით“

17. 12.1 მუხლის თანახმად, მონაცემთა სუბიექტებისთვის ინფორმაციის მიწოდების და კომუნიკაციის დამყარების პირველადი ფორმაა წერილობითი ფორმა.[23] (12.7 მუხლის თანახმად, ინფორმაციის მიწოდებისას შესაძლებელია გამოყენებული იქნას სტანდარტიზებული სიმბოლოები, ხოლო ეს საკითხი განხილულია ვიზუალიზაციის ინსტრუმენტების შესახებ სექციაში, პუნქტები 49-53). ამავდროულად. GDPR-ი დაკონკრეტების გარეშე ითვალისწინებს სხვა „საშუალებების“, მათ შორის, ელექტრონული საშუალებების გამოყენებას. WP29-ის პოზიცია წერილობით ელექტრონულ საშუალებებთან დაკავშირებით არის ის, რომ თუ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ახორციელებს ვებსაიტის მოვლა-პატრონობას (ან ნაწილობრივ ან სრულად ოპერირებს ვებსაიტის საშუალებით), WP29-ის რეკომენდაციაა, გამოყენებული იქნას კონფიდენციალობის მრავალშრიანი განაცხადი / შეტყობინება, რომელიც ვებსაიტის ვიზიტორებს საშუალებას მისცემს, გადავიდნენ განაცხადის / შეტყობინების რელევანტურ, მათთვის საინტერესო ნაწილზე (კონფიდენციალობის მრავალშრიანი განაცხადის / შეტყობინების თაობაზე იხ. პუნქტები 35-37).[24] ამავდროულად, ის ინფორმაცია, რომელთა ადრესატებიც არიან მონაცემთა სუბიექტები, სრულად უნდა იყოს მათთვის ხელმისაწვდომი, ერთ ადგილას ან ერთი სრული დოკუმენტის სახით (ციფრულ ან ფიზიკურ ფორმატში), რომელიც მარტივად იქნება ხელმისაწვდომი მონაცემთა სუბიექტისათვის იმ შემთხვევაში, თუ იგი მოისურვებს, სრულად გაეცნოს იმ ინფორმაციას, რომლის ადრესატიც არის თავად. მნიშვნელოვანია აღინიშნოს, რომ მრავალშრიანი მიდგომის გამოყენება არ ეხება მხოლოდ წერილობით ელექტრონულ საშუალებებს, რომლებიც მონაცემთა სუბიექტებისთვის ინფორმაციის მიწოდებისთვის გამოიყენება. როგორც 35-36 პუნქტებში და 38-ე პუნქტშია განხილული, მრავალშრიანი მიდგომა, შესაძლოა, აგრეთვე გამოყენებული იქნას სხვადასხვა *მეთოდების* კომბინაციის გამოყენების შემთხვევაში, დამუშავებასთან მიმართებით გამჭვირვალობის უზრუნველსაყოფად.

18. რა თქმა უნდა, მრავალშრიანი ციფრული განცხადებების / შეტყობინებების გამოყენება არ წარმოადგენს ერთადერთ წერილობით ელექტრონულ

[23] 12.1 მუხლი მიუთითებს „ენაზე“ და აცხადებს, რომ ინფორმაცია უზრუნველყოფილი უნდა იქნას წერილობითი ფორმით ან სხვა ფორმით, მათ შორის, სათანადო შემთხვევებში, ელექტრონულად.

[24] WP29 ითვალისწინებს მრავალშრიანი მიდგომის დადებით მხარეებს, რაც ხაზგასმულია დასკვნაში No 10/2004, რომელიც ეხება ინფორმაციის უფრო მეტად ჰარმონიზებული ფორმით უზრუნველყოფას და დასკვნაში No 02/2013, რომელიც ეხება ჭკვიანურ მოწყობილობებზე არსებულ აპლიკაციებს.

საშუალებას, რომელიც დამუშავებისთვის პასუხისმგებელი პირებისთვის არის ხელმისაწვდომი. სხვა ელექტრონული საშუალებებია „დროული“ („just-in-time“) კონტექსტუალური პოპ-აპ შეტყობინებები, 3D შეტყობინებები, რომლებიც იხსნება შეხებით ან მაუსის ისრის კონკრეტულ ადგილზე მიტანით (hover-over) და დაფები. არა-წერილობითი ელექტრონული საშუალებები, რომელთა გამოყენებაც შესაძლებელია მრავალშრიან განცხადებასთან / შეტყობინებასთან ერთად, მოიცავს: ვიდეოები და სმარტფონები ან IoT ხმოვანი შეტყობინებები.[25] სხვა, არა-ელექტრონული ფორმები, აგრეთვე, მოიცავს: ნახატებს, ინფოგრაფიკებს და ფლოუჩარტებს. თუ გამჭვირვალობისთვის საჭირო ინფორმაციის ადრესატი კონკრეტულად ბავშვია, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს, თუ რა ტიპის საშუალებები იქნება ბავშვებისათვის მისაწვდომი (მაგ., კომიქსები/მულტფილმები, პიქტოგრამები, ანიმაციები და სხვა).

19. უაღრესად მნიშვნელოვანია, რომ ინფორმაციის მიწოდების არჩეული მეთოდ(ებ)ი იყოს კონკრეტული გარემოებებისთვის შესაფერისი, - ე.ი., დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის ინტერაქციის ან მონაცემთა სუბიექტის შესახებ ინფორმაციის შეგროვების ფორმის შესაბამისი. მაგალითად, ინფორმაციის მხოლოდ ელექტრონული, წერილობითი ფორმატით უზრუნველყოფა, როგორიცაა, კონფიდენციალობის ონლაინ განაცხადი / შეტყობინება, შესაძლოა, არ წარმოადგენდეს შესაფერის / გამოყენებად საშუალებას, თუ მოწყობილობას, რომლითაც ხდება პერსონალური მონაცემების შეგროვება, არ აქვს ეკრანი (მაგ., IoT მოწყობილობები / ჭკვიანი მოწყობილობები), რომელზეც მომხმარებელი შეძლებს, გაეცნოს წერილობით ინფორმაციას. ასეთ შემთხვევაში, გათვალისწინებული უნდა იქნას შესაფერისი ალტერნატიული *დამატებითი* საშუალების გამოყენება, მაგალითად, კონფიდენციალობის განაცხადის / შეტყობინების გადაცემა ფიზიკური დოკუმენტის სახით - მაგ., ინსტრუქციის სახელმძღვანელოს სახით ან URL მისამართის (ე.ი., ვებსაიტის კონკრეტული გვერდი) დატანა ინსტრუქციის სახელმძღვანელოში ან შეფუთვაზე, სადაც ხელმისაწვდომი იქნება კონფიდენციალობის ონლაინ განაცხადი / შეტყობინება. დამატებით, შესაძლებელია ინფორმაციის მიწოდება აუდიო (ზეპირი) ფორმით, თუ უეკრანო მოწყობილობას აქვს აუდიო შესაძლებლობები. WP29-ს დასკვნა „საგანთა ინტერნეტის სფეროში ბოლოდროინდელი განვითარებების შესახებ“ შეიცავს რეკომენდაციებს გამჭვირვალობის და მონაცემთა სუბიექტებისთვის ინფორმაციის მიწოდების შესახებ[26] (როგორიცაა QR კოდების გამოყენება,

[25] ელექტრონული საშუალებების აღნიშნული მაგალითები არ არის ამომწურავი. მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს შეუძლიათ ახალი, ინოვაციური მეთოდების შემუშავება, მე-12 მუხლით გათვალისწინებული მოთხოვნების შესასრულებლად.

[26] WP29-ის დასკვნა 8/2014, მიღებულია 2014 წლის 16 სექტემბერს.

რომლებიც დაბეჭდილია საგანთა ინტერნეტის ობიექტებზე, ხოლო QR კოდის დასკანერებით, მომხმარებელი შეძლებს, გაეცნოს გამჭვირვალობისთვის საჭირო ინფორმაციას). აღნიშნული რეკომენდაციები თანხვედრაშია GDPR-ის მოთხოვნებთან.

„... ინფორმაციის მიწოდება შესაძლებელია ზეპირი ფორმით“

20. 12.1 მუხლი კონკრეტულად მიუთითებს, რომ მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში, ინფორმაციის მიწოდება შესაძლებელია ზეპირი ფორმით, თუ მონაცემთა სუბიექტის ვინაობა სხვა საშუალებებით დასტურდება. სხვა სიტყვებით რომ ვთქვათ, გამოყენებული საშუალებები უნდა იყოს უფრო მეტი, ვიდრე დაყრდნობა შესაბამისი პირის განცხადებაზე, რომ იგი წარმოადგენს კონკრეტული ვინაობის ადამიანს, ხოლო აღნიშნული საშუალებები დამუშავებისთვის პასუხისმგებელ პირს უნდა აძლევდეს შესაძლებლობას, მოახდინოს მონაცემთა სუბიექტის ვინაობის გადამოწმება, საკმარისი დამაჯერებლობით. მონაცემთა სუბიექტის ვინაობის შემოწმების მოთხოვნა ზეპირი ფორმით ინფორმაციის გადაცემამდე მხოლოდ იმ ინფორმაციაზე ვრცელდება, რომელიც დაკავშირებულია მონაცემთა სუბიექტის მიერ მე-15-22-ე და 34-ე მუხლებით გათვალისწინებული უფლებების განხორციელებაზე. აღნიშნული წინაპირობა ვერ გავრცელდება კონფიდენციალობის პოლიტიკის შესახებ ზოგადი ინფორმაციის მიწოდებაზე, მე-13 და მე-14 მუხლების შესაბამისად, რადგან აღნიშნული მუხლებით გათვალისწინებული ინფორმაცია მომავალი მომხმარებლებისთვის უნდა იყოს ხელმისაწვდომი (ვისი ვინაობის შემოწმების შესაძლებლობაც არ აქვს დამუშავებისთვის პასუხისმგებელ პირს ამრიგად, მე-13 და მე-14 მუხლებით გათვალისწინებული ინფორმაციის მიწოდება შესაძლებელია სხვა ზეპირი ფორმით, ისე, რომ დამუშავებისთვის პასუხისმგებელმა პირმა არ მოითხოვოს მონაცემთა სუბიექტის ვინაობის დადასტურება.

21. მე-13 და მე-14 მუხლებით მოთხოვნილი ინფორმაციის ზეპირი მიწოდება სულაც არ ნიშნავს პირისპირ (ე.ი., პირადად ან ტელეფონით) მიწოდებულ ზეპირ ინფორმაციას. წერილობითი საშუალებების გარდა, შესაძლებელია ავტომატური ზეპირი ინფორმაციის მიწოდება, განსაკუთრებით მაშინ, როდესაც საქმე ეხება საინფორმაციო საზოგადოების სერვისის მიმწოდებლებთან მხედველობის დარღვევის მქონე მონაცემთა სუბიექტების ინტერაქციას ან უეკრანო ჭკვიან მოწყობილობებს, რაც განხილულია ზემოთ, მე-19 პუნქტში. როდესაც დამუშავებისთვის პასუხისმგებელი პირი ირჩევს მონაცემთა სუბიექტისათვის ინფორმაციის ან კომუნიკაციის ზეპირი ფორმით მიწოდებას ან მონაცემთა სუბიექტი ითხოვს ზეპირი ინფორმაციის ან კომუნიკაციის მიწოდებას, WP29-ის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს უნდა მისცეს შესაძლებლობა, ხელახლა მოუსმინოს

წინასწარ ჩაწერილ შეტყობინებებს. ეს უაღრესად მნიშვნელოვანია, როდესაც ზეპირი ინფორმაციის შესახებ მოთხოვნა დაკავშირებულია მხედველობის დარღვევის მქონე მონაცემთა სუბიექტებთან ან სხვა მონაცემთა სუბიექტებთან, რომელთაც აღენიშნებათ გარკვეული სირთულე ინფორმაციის წერილობითი ფორმით მიღების და გააზრების კუთხით. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს ჩანაწერის ქონა და შეძლოს წარმოადგინოს (ხელმისაწვდომობის მოთხოვნასთან შესაბამისობის მიზნებისთვის): (i) მოთხოვნა ინფორმაციის ზეპირი ფორმით მიღების შესახებ, (ii) მეთოდი, რომლის გამოყენებითაც მოხდა მონაცემთა სუბიექტის ვინაობის გადამოწმება (საჭიროების მიხედვით, იხ. პუნქტი 20 ზემოთ) და (iii) ფაქტი, რომ ინფორმაცია მიეწოდა მონაცემთა სუბიექტს.

„უფასო“

22. 12.5 მუხლის თანახმად,[27] ზოგადად, უფასოა დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდება მე-13 და მე-14 მუხლების შესაბამისად ან კომუნიკაციები და მოქმედებები, რომლებიც ხორციელდება მე-15-22-ე მუხლების (მონაცემთა სუბიექტების უფლებების შესახებ) და 34-ე მუხლის (მონაცემთა სუბიექტისათვის მონაცემთა უსაფრთხოების დარღვევის **შესახებ** შეტყობინება).[28] გამჭვირვალობის აღნიშნული ასპექტი, აგრეთვე, ნიშნავს იმას, რომ გამჭვირვალობის მოთხოვნების ფარგლებში ინფორმაციის უზრუნველყოფა ვერ იქნება დამოკიდებული ფინანსურ ტრანზაქციებზე, მაგალითად, მომსახურების ან საქონლის შესყიდვაზე ან თანხის გადახდაზე.[29]

---

[27] კერძოდ, „მე-13 და მე-14 მუხლებით გათვალისწინებული ინფორმაციის მიწოდება და ასევე ნებისმიერი კომუნიკაცია და ღონისძიებები 15-22 და 34-ე მუხლების თანახმად განხორციელებული კომუნიკაცია და ღონისძიებები უნდა განხორციელდეს უსასყიდლოდ.“

[28] ამავდროულად, 12.5 მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს შეუძლია დააწესოს გონივრული საფასური, თუ, მაგალითად, მონაცემთა სუბიექტის მოთხოვნა მე-13 და მე-14 მუხლებით გათვალისწინებულ ინფორმაციასთან დაკავშირებით ან მე-15-22-ე და 34-ე მუხლებით გათვალისწინებულ უფლებებთან დაკავშირებით გადაჭარბებული ან ცალსახად დაუსაბუთებელია. (ამას გარდა, 15.3 მუხლით გათვალისწინებული ხელმისაწვდომობის უფლებასთან დაკავშირებით, დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია, დააწესოს გონივრული საფასური ადმინისტრაციული ხარჯების გათვალისწინებით, როდესაც მონაცემთა სუბიექტი ითხოვს დამატებით ასლებს).

[29] მაგალითად, თუ მონაცემთა სუბიექტის შესახებ პერსონალური მონაცემების შეეგროვება ხდება შესყიდვასთან დაკავშირებით, მე-13 მუხლით გათვალისწინებული ინფორმაცია მას უნდა მიეწოდოს თანხის გადახდამდე და იმ მომენტში, როდესაც ხდება ინფორმაციის შეგროვება, და არა მას შემდეგ, რაც დასრულდება ტრანზაქცია. ამავდროულად, როდესაც მონაცემთა სუბიექტს მიეწოდება უფასო სერვისები, მე-13 მუხლით გათვალისწინებული ინფორმაცია მას უნდა მიეწოდოს დარეგისტრირებამდე და არა დარეგისტრირების შემდეგ, რადგან 13.1 მუხლის თანახმად, ინფორმაციის მიწოდება უნდა მოხდეს „პერსონალური მონაცემების მოპოვების მომენტში“.

ინფორმაცია, რომელიც უნდა მიეწოდოს მონაცემთა სუბიექტს - მე-13 და მე-14 მუხლები

შინაარსი

23. GDPR-ში ჩამოთვლილია, თუ რა კატეგორიების ინფორმაცია უნდა მიეწოდოს მონაცემთა სუბიექტს, პერსონალური მონაცემების დამუშავების კონტექსტში, იმ შემთხვევაში, როდესაც მონაცემების შეგროვება ხდება უშუალოდ მონაცემთა სუბიექტისგან (მუხლი 13) ან სხვა წყაროსგან (მუხლი 14). დანართის სახით წარმოდგენილი ცხრილი მოკლედ მიმოიხილავს, თუ რა კატეგორიების ინფორმაცია უნდა მიეწოდოს მონაცემთა სუბიექტს, მე-13 და მე-14 მუხლების შესაბამისად. მასში, აგრეთვე, გათვალისწინებულია აღნიშნული მოთხოვნების ხასიათი, ფარგლები და შინაარსი. ნათლად რომ განვმარტოთ, WP29-ის პოზიციის თანახმად, ინფორმაცია, რომელიც დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს უნდა მიაწოდოს მე-13 მუხლის 1-ლი და მე-2 პუნქტის თანახმად და ინფორმაცია, რომელიც უნდა მიაწოდოს მე-14 მუხლის თანახმად, ერთმანეთისგან არ განსხვავდება სტატუსის მიხედვით.

„სათანადო ზომები“

24. მნიშვნელოვანია როგორც იმ ინფორმაციის შინაარსი, რომელიც დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს უნდა მიაწოდოს მე-13 და მე-14 მუხლების შესაბამისად, ისე მისი ფორმა და მანერა. შეტყობინებას, რომელიც ასეთ ინფორმაციას შეიცავს, ხშირად უწოდებენ მონაცემთა დაცვის შესახებ შეტყობინებას, კონფიდენციალობის შესახებ შეტყობინებას, კონფიდენციალობის პოლიტიკას, კონფიდენციალობის განაცხადს ან შეტყობინებას მონაცემთა სამართლიანი დამუშავების შესახებ. GDPR-ი არ ითვალისწინებს ამ ინფორმაციის მონაცემთა სუბიექტისათვის მიწოდების კონკრეტულ ფორმატს ან მოდალობას, თუმცა, მასში მკაფიოდ არის მითითებული, რომ დამუშავებისთვის პასუხისმგებელ პირს ევალება „სათანადო ზომების“ მიღება გამჭვირვალობისთვის საჭირო ინფორმაციის უზრუნველყოფის კუთხით. ეს ნიშნავს იმას, რომ დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს მონაცემთა შეგროვებასთან და დამუშავებასთან დაკავშირებული ყველა გარემოება და ისე მიიღოს გადაწყვეტილება ინფორმაციის უზრუნველყოფის შესაფერისი მოდალობისა და ფორმატის შესახებ. კერძოდ, სათანადო ზომები უნდა შეფასდეს პროდუქტის/სერვისის მომხმარებლის გამოცდილების გათვალისწინებით. ეს ნიშნავს გამოყენებული მოწყობილობის (თუ საჭიროა), მომხმარებლის

ინტერფეისების / დამუშავებისთვის პასუხისმგებელ პირთან მისი ინტერაქციების ხასიათის (მომხმარებლის „მოგზაურობა“) და ამ ფაქტორებთან დაკავშირებული შეზღუდვების გათვალისწინებას. როგორც მე-17 პუნქტშია აღნიშნული, WP29-ის რეკომენდაციის თანახმად, როდესაც დამუშავებისთვის პასუხისმგებელი პირი წარმოდგენილია ონლაინ სივრცეში, მან უნდა უზრუნველყოს კონფიდენციალობის შესახებ მრავალშრიანი ონლაინ განაცხადი/შეტყობინება.

25. ინფორმაციის მიწოდების ყველაზე შესაფერისი მოდალობის იდენტიფიცირების მიზნით, „ლაივში გასვლამდე“ მიზანშეწონილია, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა მოსინჯონ სხვადასხვა მოდალობები და გატესტონ ისინი მომხმარებლებთან (მაგ., მომხმარებელთა გამოკითხვები და სხვა სტანდარტიზებული ტესტები წაკითხვადობის და ხელმისაწვდომობის შესახებ), რათა მიიღონ მომხმარებელთა უკუკავშირი, თუ რამდენად არის შემოთავაზებული საშუალება მისაწვდომი, გასაგები და ადვილად გამოყენებადი. (დამატებით, ტესტირების შესახებ იხ. კომენტარები ზემოთ, პ.9). ამ მიდგომის დოკუმენტირება დამუშავებისთვის პასუხისმგებელ პირებს, აგრეთვე, დაეხმარება ანგარიშვალდებულებასთან დაკავშირებული მოვალეობების შესრულებაში. კერძოდ, ისინი შეძლებენ, მოახდინონ დემონსტრირება იმისა, რომ ინფორმაციის მიწოდებისთვის არჩეული ინსტრუმენტი/მიდგომა წარმოადგენს ყველაზე შესაფერისს მოცემული გარემოებების გათვალისწინებით.

ინფორმაციის მიწოდების ოპერატიულობა

26. მე-13 და მე-14 მუხლები ადგენს ინფორმაციას, რომელიც დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მიაწოდოს მონაცემთა სუბიექტს, დამუშავების ციკლის დაწყებისას.[30] მე-13 მუხლი ვრცელდება იმ შემთხვევებზე, როდესაც მონაცემების შეგროვება ხდება მონაცემთა სუბიექტისგან. აღნიშნული მოიცავს პერსონალურ მონაცემებს:

- რომლებიც მონაცემთა სუბიექტმა გაცნობიერებულად გადასცა მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს (მაგ., ონლაინ ფორმის შევსებისას); ან

[30] სამართლიანობის და მიზნის შეზღუდვის პრინციპების გათვალისწინებით, ორგანიზაცია, რომელიც პერსონალურ მონაცემებს აგროვებს მონაცემთა სუბიექტისგან, ვალდებულია, ყოველთვის მიუთითოს დამუშავების მიზნები, მონაცემთა შეგროვების მომენტში. თუ მიზანი მოიცავს მეორადი პერსონალური მონაცემების შექმნას (inferred personal data), ამგვარი პერსონალური მონაცემების შექმნის და შემდგომ დამუშავების მიზანი და დამუშავებული მეორადი პერსონალური მონაცემების კატეგორიები ყოველთვის უნდა განემარტოს მონაცემთა სუბიექტს, შეგროვების დროს ან ახალი მიზნის საფუძველზე მონაცემთა შემდგომ დამუშავებამდე, 13.3 და 14.4 მუხლების შესაბამისად.

- მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა მოიპოვა მონაცემთა სუბიექტისგან, დაკვირვების გზით (მაგ., მონაცემთა ავტომატურად მოპოვების მოწყობილობების ან კომპიუტერული პროგრამების გამოყენების გზით, მათ შორის: კამერები, ქსელური მოწყობილობა, Wi-Fi მონიტორინგი, RFID (რადიო სიხშირის იდენტიფიკაცია) და სხვა ტიპის სენსორები).

მე-14 მუხლი ვრცელდება ისეთ შემთხვევებზე, როდესაც მონაცემები არ არის მოპოვებული მონაცემთა სუბიექტისგან. ეს მოიცავს პერსონალურ მონაცემებს, რომლებიც დამუშავებისთვის პასუხისმგებელმა პირმა მოიპოვა ისეთი წყაროებიდან, როგორიცაა:

- სხვა დამუშავებისთვის პასუხისმგებელი პირი რომელიც არის მესამე მხარე;
- საჯაროდ ხელმისაწვდომი წყაროები;
- მონაცემთა ბროკერები; ან
- სხვა მონაცემთა სუბიექტები.

27. რაც შეეხება ამ ინფორმაციის მიწოდების დროულობას, მისი დროულად მიწოდება გამჭვირვალობის ვალდებულების და მონაცემების სამართლიანად დამუშავების ვალდებულების სასიცოცხლო შემადგენელი ელემენტია. იმ შემთხვევაში, თუ მოქმედებს მე-13 მუხლი, მისი პირველი პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა ინფორმაციის მიწოდება უნდა უზრუნველყოს *„პერსონალური მონაცემების მოპოვების დროს“*. პერსონალური მონაცემების ირიბად მოპოვების შემთხვევაში, მე-14 მუხლის თანახმად, მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდების ვადები დადგენილია ამავე მუხლის მე-3 პუნქტის (a) – (c) ქვეპუნქტებში:

- ზოგადი მოთხოვნის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს ინფორმაცია უნდა მიაწოდოს პერსონალური მონაცემების შეგროვებიდან „გონივრულ ვადაში“, მაგრამ არაუგვიანეს ერთი თვისა, „მონაცემების დამუშავების სპეციფიური გარემოებების გათვალისწინებით“ (მუხლი 14.3(a)).

- 14.3(a) მუხლით დადგენილი ზოგადი ერთთვიანი ვადა შესაძლებელია შეიცვალოს 14.3(b)[31] მუხლის საფუძველზე, რომელიც ითვალისწინებს ისეთ სიტუაციას, როდესაც მონაცემები გამოიყენება მონაცემთა

[31] სიტყვები *„თუ პერსონალური მონაცემები გამოიყენება..“* 14.3(b) მუხლში მიუთითებს ზოგად პოზიციაზე, 14.3(a) მუხლით გათვალისწინებულ მაქსიმალურ ვადასთან დაკავშირებით, თუმცა, არ ანაცვლებს მას.

სუბიექტთან კომუნიკაციისთვის. ასეთ შემთხვევაში, ინფორმაციის მიწოდება უნდა მოხდეს არაუგვიანეს მონაცემთა სუბიექტთან კავშირის პირველად დამყარებისას. თუ პირველი კომუნიკაციის დამყარება ხდება პერსონალური მონაცემების მოპოვებიდან ერთთვიანი ვადის გასვლამდე, მაშინ დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს ინფორმაცია უნდა მიაწოდოს, *არა უგვიანეს,* მონაცემთა სუბიექტთან კომუნიკაციის პირველად დამყარებისას, მიუხედავად იმისა, რომ ჯერ არ არის გასული მონაცემების მოპოვებიდან ერთი თვე. თუ მონაცემთა სუბიექტთან კავშირის პირველად დამყარება ხორციელდება პერსონალური მონაცემების მოპოვებიდან ერთ თვეზე მეტი ხნის შემდეგ, მე-14 მუხლის მე-3 პუნქტის (a) ქვეპუნქტი მაინც მოქმედებს, რომლის მიხედვითაც მე-14 მუხლით გათვალისწინებული ინფორმაცია მონაცემთა სუბიექტს უნდა მიეწოდოს არაუგვიანეს მისი მოპოვებიდან ერთი თვის ვადაში.

- 14.3(a) მუხლით დადგენილი ზოგადი ერთთვიანი ვადა შესაძლებელია შეიცვალოს 14.3(c)[32] მუხლის საფუძველზე, რომელიც ითვალისწინებს ისეთ სიტუაციას, როდესაც მონაცემები გამიზნულია სხვა მიმღებისთვის გადასაცემად (მესამე მხარე ან სხვა).[33] ასეთ დროს, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს ინფორმაცია უნდა მიაწოდოს არაუგვიანეს მონაცემების პირველად გადაცემის მომენტისა. ამ შემთხვევაში, თუ გადაცემას ადგილი აქვს ერთთვიანი ვადის გასვლამდე, ინფორმაციის მიწოდება უნდა მოხდეს არაუგვიანეს პირველად გადაცემის მომენტისა, მიუხედავად იმისა, რომ მონაცემთა მოპოვების შემდეგ ერთთვიანი პერიოდი არ არის გასული. მსგავსად 14.3(b) მუხლთან დაკავშირებით სამუშაო ჯგუფის პოზიციისა, ამ შემთხვევაშიც, თუ პერსონალური მონაცემების გადაცემას ადგილი აქვს პერსონალური მონაცემების მოპოვებიდან ერთი თვის გასვლის შემდეგ, მე-14 მუხლის მე-3 პუნქტის (a) ქვეპუნქტი მაინც მოქმედებს, რომლის მიხედვითაც მე-14 მუხლით გათვალისწინებული ინფორმაცია მონაცემთა სუბიექტს უნდა მიეწოდოს არაუგვიანეს მისი მოპოვებიდან ერთი თვის ვადაში.

---

[32] სიტყვები *„თუ გათვალისწინებულია [მონაცემთა] გადაცემა სხვა მიმღებისთვის...“* 14.3(c) მუხლში მიუთითებს ზოგად პოზიციაზე, 14.3(a) მუხლით გათვალისწინებულ მაქსიმალურ ვადასთან დაკავშირებით, თუმცა, არ ანაცვლებს მას.

[33] 4.9 მუხლში განამრტებულია „მიმღები“. ამ განმარტების თანახმად, არ არის აუცილებელი რომ მიმღები, ვისაც გადაეცემა პერსონალური მონაცემები, შესაძლოა არ წარმოადგენდეს მესამე მხარეს. შესაბამისად, მიმღები შესაძლოა იყოს დამუშავებისთვის პასუხისმგებელი პირი ერთობლივი დამუშავებისთვის პასუხისმგებელი პირი ან დამუშავებაზე უფლებამოსილი პირი.

28. ამრიგად, ნებისმიერ შემთხვევაში, მე-14 მუხლით გათვალისწინებული ინფორმაციის მონაცემთა სუბიექტისთვის მიწოდების მაქსიმალური ვადაა ერთი თვე. ამავდროულად, სამართლიანობის და ანგარიშვალდებულების პრინციპები, რომელთაც ითვალისწინებს GDPR-ი, ითხოვს, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა ყოველთვის გაითვალისწინონ მონაცემთა სუბიექტების გონივრული მოლოდინები, მონაცემთა დამუშავების გავლენა მათზე და მათი შესაძლებლობა, განახორციელონ თავიანთი უფლებები დამუშავებასთან მიმართებით. სწორედ აღნიშნულის საფუძველზე უნდა გადაწყვიტოს დამუშავებისთვის პასუხისმგებელმა პირმა, თუ რა ეტაპზე მიაწვდის იგი მონაცემთა სუბიექტს მე-14 მუხლით გათვალისწინებულ ინფორმაციას. ანგარიშვალდებულების პრინციპის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მოახდინოს საკუთარი გადაწყვეტილების დასაბუთება და დაასახელოს მიზეზი, თუ რატომ მიაწოდა მონაცემთა სუბიექტს ინფორმაცია იმ კონკრეტულ დროს. პრაქტიკაში, შესაძლებელია რთული იყოს ამ მოთხოვნების შესრულება ინფორმაციის 'ბოლო მომენტში' მიწოდების შემთხვევაში. ამ მხრივ, პრეამბულის 39-ე პუნქტი, სხვა საკითხებთან ერთად, ითვალისწინებს, რომ მონაცემთა სუბიექტებს დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გააცნოს „პერსონალური მონაცემების დამუშავებასთან დაკავშირებული რისკები, წესები, დაცვის მექანიზმები და უფლებები. და მათი უფლებების რეალიზების გზები." მე-60 პუნქტი აგრეთვე მიუთითებს მოთხოვნაზე, რომ მონაცემთა სუბიექტს მიეწოდოს ინფორმაცია დამუშავების ოპერაციის და მისი მიზნების შესახებ, სამართლიანი და გამჭვირვალე დამუშავების პრინციპების კონტექსტში. ამ მიზეზების გამო, WP29-ის პოზიცია მდგომარეობს იმაში, რომ თუ ეს შესაძლებელია, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა, სამართლიანობის პრინციპის შესაბამისად, მონაცემთა სუბიექტს ინფორმაცია უნდა მიაწოდონ დადგენილი ვადების გასვლამდე დიდი ხნით ადრე. 30-ე-31-ე და 48-ე პუნქტები შეიცავენ დამატებით კომენტარებს დამუშავების ოპერაციების შესახებ მონაცემთა სუბიექტის ინფორმირების და ამ ოპერაციების ამოქმედების ვადების მიზანშეწონილობასთან დაკავშირებით.

მე-13 და მე-14 მუხლებით გათვალისწინებულ ინფორმაციაში ცვლილებების განხორციელება

29. გამჭვირვალობის კუთხით ანგარიშვალდებულება ვრცელდება არა მხოლოდ პერსონალური მონაცემების შეგროვების მომენტზე, არამედ, დამუშავების ცხოვრების ციკლზე, მიუხედავად იმისა, თუ რა სახის ინფორმაციის ან კომუნიკაციის მიწოდებასთან გვაქვს საქმე. იგივე მოთხოვნები ვრცელდება კონფიდენციალურობის არსებული განაცხადის / შეტყობინების შინაარსში ცვლილებების განხორციელების შემთხვევებზე. დამუშავებისთვის

პასუხისმგებელი პირი ვალდებულია, მისდიოს იგივე პრინციპებს თავდაპირველი კონფიდენციალობის განაცხადის / შეტყობინების და მასში შემდგომ განხორციელებული არსებითი ან მატერიალური ცვლილებების შესახებ ინფომაციის მიწოდებისას. ფაქტორები, რომლებიც დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინონ იმის შეფასებისას, თუ რამდენად არის განხორციელებული ცვლილება არსებითი ან მატერიალური, მოიცავს: გავლენა მონაცემთა სუბიექტებზე (მათ შორის, მონაცემთა სუბიექტების შესაძლებლობა, განახორციელოს თავისი უფლებები) და რამდენად მოულოდნელი/გასაკვირი იქნება განხორციელებული ცვლილება მონაცემთა სუბიექტებისთვის. კონფიდენციალობის განაცხადში/შეტყობინებაში განხორციელებული ცვლილებები, რომლის შესახებაც აუცილებელია მონაცემთა სუბიექტების ინფორმირება, *inter alia*, მოიცავს: დამუშავების მიზნის ცვლილება; დამუშავებისთვის პასუხისმგებელი პირის ვინაობის ცვლილება; მონაცემთა სუბიექტის მიერ, დამუშავებასთან მიმართებით, საკუთარი უფლებების განხორციელების გზების ცვლილება. მეორეს მხრივ, WP29-ის თანახმად, კონფიდენციალობის განაცხადში / შეტყობინებაში განხორციელებული ცვლილებები, რომელიც არ წარმოადგენს არსებით ან მატერიალურ ცვლილებებს, მოიცავს, მაგალითად, მართლწერის შეცდომების გასწორებას ან სტილისტურ/გრამატიკულ ცვლილებებს. ვინაიდან არსებული მომხმარებლების უმეტესობა მხოლოდ თვალს გადაავლებს კონფიდენციალობის განაცხადში / შეტყობინებაში განხორციელებული ცვლილებების შესახებ ინფორმაციას, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მიიღოს ყველა საჭირო ზომა, რათა ამ ცვლილებების მიწოდება მოხდეს იმგვარად, რაც უზრუნველყოფს მიმღებთა უმრავლესობის მიერ მათ შემჩნევას. აღნიშნული ნიშნავს, მაგალითად, ცვლილებების შესახებ შეტყობინების სათანადო მოდალობის გამოყენებით მიწოდებას (მაგ., ელ-ფოსტა, ნაბეჭდი წერილი, პოპ-აპ ფანჯარა ვებგვერდზე ან სხვა მოდალობა, რომელიც ეფექტურად მიმართავს მონაცემთა სუბიექტის ყურადღებას ცვლილებებისკენ). ეს მოდალობები მონაცემთა სუბიექტს მხოლოდ ცვლილებების შესახებ ინფორმაციის უნდა აწვდიდდეს (მაგ., არ უნდა შეიცავდეს პირდაპირი მარკეტინგის მასალებს), ხოლო ამგვარი კომუნიკაცია უნდა აკმაყოფილებდეს მე-12 მუხლით დადგენილ მოთხოვნებს ლაკონურობასთან, გამჭვირვალობასთან, გასაგებობასთან, მარტივად ხელმისაწვდომობასთან და ნათელი და მარტივი ენის გამოყენებასთან დაკავშირებით. კონფიდენციალობის განაცხადში მითითება იმაზე, რომ მონაცემთა სუბიექტმა რეგულარულად უნდა შეამოწმოს კონფიდენციალობის განაცხადი, რათა გაეცნოს ცვლილებებს ან განახლებებს არა მხოლოდ არასაკმარისია, არამედ, აგრეთვე, უსამართლოა, 5.1(a) მუხლის კონტექსტში. დამატებითი რეკომენდაციები მონაცემთა სუბიექტებისათვის ცვლილებების შეტყობინების ოპერატიულობასთან დაკავშირებით წარმოდგენილია ქვემოთ, 30-ე და 31-ე პუნქტებში.

მე-13 და მე-14 მუხლით გათვალისწინებულ ინფორმაციაში განხორციელებული ცვლილებების შესახებ მონაცემთა სუბიექტებისთვის შეტყობინების ვადები

30. GDPR-ი არაფერს ამბობს იმ ინფორმაციაში განხორციელებული ცვლილებების შეტყობინების ვადებთან (და მეთოდებთან) დაკავშირებით, რომელიც მონაცემთა სუბიექტს დამუშავებისთვის პასუხისმგებელმა პირმა მიაწოდა მე-13 და მე-14 მუხლების თანახმად (გარდა დამუშავების შემდგომი მიზნისა, რა შემთხვევაშიც ინფორმაცია ამ მიზნის შესახებ შემდგომი დამუშავების დაწყებამდე უნდა მიაწოდოს დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს, მე-13.3 და მე-14.4 მუხლების შესაბამისად - იხ. პუნქტი 45 ქვემოთ). ამავდროულად, როგორც ზემოთ აღინიშნა, მე-14 მუხლით გათვალისწინებული ინფორმაციის მიწოდების ვადების კონტექსტში, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს სამართლიანობის და ანგარიშვალდებულების პრინციპები, მონაცემთა სუბიექტის გონივრული მოლოდინების ჭრილში, და ამ ცვლილებების პოტენციური გავლენა მონაცემთა სუბიექტზე. თუ განხორციელებული ცვლილება მიანიშნებს ფუნდამენტურ ცვლილებაზე დამუშავების ხასიათში (მაგ., მიმღებთა კატეგორიების გაფართოება ან მესამე ქვეყნისთვის გადაცემის შემოღება) ან ცვლილებაზე, რომელიც შესაძლოა არ იყოს ფუნდამენტური, დამუშავების პროცესის ჭრილში, თუმცა, იყოს რელევანტური მონაცემთა სუბიექტისთვის და გავლენას ახდენდეს მასზე, მაშინ, დამუშავებისთვის პასუხისმგებელმა პირმა ეს ინფორმაცია მონაცემთა სუბიექტს უნდა მიაწოდოს ცვლილების განხორციელებამდე საკმაო ხნით ადრე, ხოლო ცვლილებების მიმართ მონაცემთა სუბიექტის ყურადღების მიმართვის მეთოდი უნდა იყოს მკაფიო და ეფექტური. აღნიშნული უზრუნველყოფს, რომ მონაცემთა სუბიექტს არ „გამორჩეს“ ცვლილება და მას მისცემს გონივრულ ვადას, რათა (ა) განიხილოს ცვლილების ხასიათი და ზეგავლენა და (ბ) ცვლილებასთან მიმართებით განახორციელოს საკუთარი უფლებები, რომელთაც უზრუნველყოფს GDPR-ი (მაგ., უკან გაიხმოს თანხმობა ან მოითხოვოს დამუშავების შეწყვეტა).

31. მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა სიფრთხილით უნდა შეაფასოს თითოეულ იმ სიტუაციასთან დაკავშირებული გარემოებები და კონტექსტი, რომელიც მოითხოვს გამჭვირვალობისთვის საჭირო ინფორმაციის განახლებას, მათ შორის, ცვლილებების შესაძლო გავლენა მონაცემთა სუბიექტზე და ცვლილებების შესახებ ინფორმაციის მიწოდების მოდალობები, და უნდა შეეძლოს დემონსტრირება იმისა, რომ ცვლილებების შესახებ შეტყობინების ვადა და ცვლილების ამოქმედება აკმაყოფილებს სამართლიანობის პრინციპს. ამას გარდა, WP29-ის პოზიციის თანახმად, სამართლიანობის პრინციპის შესაბამისად, ამგვარი ცვლილებების შესახებ

მონაცემთა სუბიექტისთვის შეტყობინების შემთხვევაში, დამუშავებისთვის პასუხისმგებელმა პირმა, აგრეთვე, უნდა განმარტოს, თუ რა სავარაუდო გავლენა ექნება ამ ცვლილებებს მონაცემთა სუბიექტებზე. ამავდროულად, გამჭვირვალობის მოთხოვნებთან შესაბამისობა არ ნიშნავს ისეთ სიტუაციაზე „თვალის დახუჭვას“, როდესაც დამუშავებაში განხორციელებული ცვლილებები იმდენად მნიშვნელოვანია, რომ იგი აბსოლუტურად ცვლის დამუშავების ხასიათს. WP29 ხაზს უსვამს, რომ GDPR-ით გათვალისწინებული ყველა სხვა წესები, მათ შორის, თავდაპირველ მიზანთან შეუთავსებელ შემდგომ დამუშავებასთან დაკავშირებით, კვლავ ვრცელდება იმის მიუხედავად, შესრულდა თუ არა გამჭვირვალობასთან დაკავშირებული ვალდებულებები.

32. ამას გარდა, მაშინაც კი, თუ არსებითად არ იცვლება გამჭვირვალობასთან დაკავშირებული ინფორმაცია (მაგ., ინფორმაცია, რომელსაც შეიცავს კონფიდენციალურობის განაცხადი/შეტყობინება), მონაცემთა სუბიექტები, რომლებიც მომსახურებას დიდი ხანია იყენებენ, სავარაუდოდ, ვერ შეძლებენ, გაიხსენონ მათთვის მე-13 და/ან მე-14 მუხლის თანახმად თავდაპირველად მიწოდებული ინფორმაცია. WP29-ის რეკომენდაციის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა ხელი უნდა შეუწყონ მონაცემთა სუბიექტების უწყვეტ და მარტივ წვდომას ინფორმაციაზე, რათა მათ შეძლონ, ხელახლა გაეცნონ მონაცემთა დაცვის ფარგლებს. ანგარიშვალდებულების პრინციპის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა აგრეთვე, უნდა განიხილონ თუ რამდენად და რა პერიოდულობით არის მიზანშეწონილი მონაცემთა სუბიექტებისთვის მკაფიო შეხსენებების გაგზავნა კონფიდენციალობის განაცხადთან / შეტყობინებასთან დაკავშირებით და იმის შესახებ, თუ სად არის აღნიშნული განაცხადი / შეტყობინება ხელმისაწვდომი.

მოდალობები - ინფორმაციის მიწოდების ფორმატი

33. მე-13 და მე-14 მუხლები მიუთითებს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მოვალეობაზე, *„მონაცემთა სუბიექტს მიაწოდოს ყველა ქვემოთ წარმოდგენილი ინფორმაციით ...“* ამ შემთხვევაში, მოქმედების აღმნიშვნელი სიტყვაა „მიაწოდოს“. ეს ნიშნავს, რომ დამუშავებისთვის პასუხისმგებელმა პირმა აქტიური ნაბიჯები უნდა გადასცა მონაცემთა სუბიექტის შესაბამისი ინფორმაციით უზრუნველყოფისთვის ან აქტიურად უნდა გადაამისამართოს მონაცემთა სუბიექტი ამ ინფორმაციის მდებარეობის ადგილისკენ (მაგ., პირდაპირი ბმულის საშუალებით, QR კოდის გამოყენებით და ა.შ.). მონაცემთა სუბიექტს არ უნდა უწევდეს სხვა ინფორმაციასთან ერთად (როგორიცაა, ვებსაიტის ან აპლიკაციის გამოყენების წესები და პირობები), აღნიშნული მუხლებით გათვალისწინებული ინფორმაციის აქტიურად ძიება. მე-11 პუნქტში წარმოდგენილი მაგალითები სწორედ ამ საკითხს ეხება. როგორც მე-17 პუნქტშია მითითებული, WP29-ის რეკომენდაციის თანახმად,

ინფორმაცია, რომლის ადრესატსაც მონაცემთა სუბიექტები წარმოადგენენ, მათთვის, აგრეთვე, ხელმისაწვდომი უნდა იყოს ერთ ადგილას ან ერთი სრული დოკუმენტის სახით (მაგ., ციფრული ფორმით, ვებსაიტზე ან დაბეჭდილი ფორმით), რომელიც ადვილად იქნება ხელმისაწვდომი იმ შემთხვევაში, თუ მონაცემთა სუბიექტები მოისურვებენ, რომ ინფორმაციას გაეცნონ მთლიანობაში.

34. საჭიროა ბალანსის დაცვა ერთის მხრივ, მონაცემთა სუბიექტებისთვის ამომწურავი ინფორმაციის უზრუნველყოფის და მეორეს მხრივ, ამ ინფორმაციის მოკლე (ლაკონური), გამჭვირვალე, გასაგები და ადგილად ხელმისაწვდომი ფორმით მიწოდების მოთხოვნებს შორის, რომელთაც GDPR-ი ითვალისწინებს. როგორც ასეთი, ანგარიშვალდებულებისა და სამართლიანობის ფუნდამენტური პრინციპების გათვალისწინებით, დამუშავებისთვის პასუხისმგებელი პირები ვალდებულები არიან, თავად გააანალიზონ მათ მიერ განხორციელებული პერსონალური მონაცემების დამუშავების ხასიათი, გარემოებები, ფარგლები და კონტექსტი და მიიღონ გადაწყვეტილება, GDPR-ის სამართლებრივი მოთხოვნების ფარგლებში და წინამდებარე დოკუმენტში, განსაკუთრებით, 36-ე პუნქტში წარმოდგენილი რეკომენდაციების გათვალისწინებით, თუ როგორ უზრუნველყონ მონაცემთა სუბიექტებისათვის მისაწოდებელი ინფორმაციის პრიორიტეტულობა, რამდენად დეტალური უნდა იყოს ეს ინფორმაცია და მიწოდების რა მეთოდები უნდა იქნას გამოყენებული.

მრავალშრიანი მიდგომა ციფრულ გარემოში და მრავალშრიანი განაცხადები/შეტყობინებები კონფიდენციალობის შესახებ

35. ციფრულ კონტექსტში, იმ ინფორმაციის მოცულობის გათვალისწინებით, რომელიც დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მიაწოდოს მონაცემთა სუბიექტს, მიზანშეწონილია დამუშავებისთვის პასუხისმგებელი პირის მიერ მრავალშრიანი მიდგომის გამოყენება, რომლის მიხედვითაც ისინი მიმართავენ სხვადასხვა მეთოდებს გამჭვირვალობის უზრუნველსაყოფად. WP29-ის რეკომენდაციის თანახმად, გამოყენებული უნდა იქნას კონფიდენციალობის მრავალშრიანი განაცხადები/შეტყობინებები, რომელიც ერთი შეტყობინების სახით ეკრანზე მთლიანი ინფორმაციის გამოტანის ნაცვლად, უზრუნველყოფს სხვადასხვა კატეგორიის ინფორმაციის ბმულებს, რაც მონაცემთა სუბიექტს თავიდან ააცილებს ინფორმაციით გადაღლას. მრავალშრიანი კონფიდენციალობის განაცხადი / შეტყობინება უზრუნველყოფს ბალანსს ინფორმაციის ამომწურავობასა და გააზრებადობას შორის. განსაკუთრებით აღსანიშნავია, რომ იგი მომხმარებელს მისცემს საშუალებას, პირდაპირ გადავიდეს განაცხადის / შეტყობინების იმ ნაწილზე, რომლის

წაკითხვაც სურს. უნდა ითქვას, რომ მრავალშრიანი განაცხადები/შეტყობინებები არ წარმოადგენს უბრალოდ ერთმანეთში ჩამალულ (nested) გვერდებს, საიდანაც შესაბამისი ინფორმაციის მიღება რამოდენიმე დაწკაპუნებას საჭიროებს. არამედ, კონფიდენციალობის განაცხადის / შეტყობინების პირველი შრის დიზაინი და სქემა უნდა იყოს იმგვარი, რომ მონაცემთა სუბიექტს მკაფიოდ შეეძლოს დანახვა, თუ რა ინფორმაციაა მისთვის ხელმისაწვდომი მისი პერსონალური მონაცემების დამუშავების შესახებ და კონფიდენციალობის განაცხადის / შეტყობინების შრეების ფარგლებში კონკრეტულად სად/როგორ შეძლებს დეტალური ინფორმაციის მიღებას. მნიშვნელოვანია, რომ ინფორმაცია, რომელსაც მრავალშრიანი შეტყობინების სხვადასხვა შრე შეიცავს იყოს თანმიმდევრული. შრეები არ უნდა შეიცავდეს ისეთ ინფორმაციას, რომელიც ერთმანეთთან წინააღმდეგობაშია.

36. რაც შეეხება პირველი მოდალობის შინაარსს, რომელსაც დამუშავებისთვის პასუხისმგებელი პირი იყენებს, რათა მონაცემთა სუბიექტს მიაწოდოს ინფორმაცია მრავალშრიანი მიდგომის საფუძველზე (სხვა სიტყვებით რომ ვთქვათ, ის ძირითადი გზა, რითაც დამუშავებისთვის პასუხისმგებელ პირს პირველადი კონტაქტი აქვს მონაცემთა სუბიექტთან), ან მრავალშრიანი კონფიდენციალობის განაცხადის / შეტყობინების პირველი შრის შინაარსს, WP29-ის რეკომენდაციის თანახმად, პირველი შრე / მოდალობა უნდა შეიცავდეს დეტალურ მონაცემებს დამუშავების მიზეზების და დამუშავებისთვის პასუხისმგებელი პირისვინაობის შესახებ და მონაცემთა სუბიექტის უფლებების აღწერას (ამას გარდა, მონაცემთა სუბიექტის ყურადღება აღნიშნული ინფორმაციისკენ უნდა იყოს მიმართული პერსონალური მონაცემების შეგროვების მომენტში, მაგ., ეკრანზე იქნას გამოტანილი მაშინ, როდესაც მონაცემთა სუბიექტი ავსებს ონლაინ ფორმას). აღნიშნული ინფორმაციის წინასწარ მიწოდების მნიშვნელობა მომდინარეობს პრეამბულის 39-ე პუნქტიდან.[34] დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეძლოს დასაბუთება, თუ რატომ გადაწყვიტა კონკრეტული დამატებითი ინფორმაციისთვის პრიორიტეტის მინიჭება. ამავდროულად, WP29-ის პოზიცია მდგომარეობს იმაში, რომ სამართლიანობის პრინციპის შესაბამისად, გარდა წინამდებარე პუნქტში აღწერილი ინფორმაციისა, პირველი შრე / მოდალობა, აგრეთვე, უნდა შეიცავდეს ინფორმაციას იმ დამუშავების შესახებ, რომელსაც ყველაზე მეტი გავლენა აქვს მონაცემთა სუბიექტზე და რომელიც შესაძლოა

[34] პრეამბულის 39-ე პუნქტის თანახმად, „კერძოდ, ეს პრინციპი ვრცელდება მონაცემთა სუბიექტებისთვის დამუშავებისთვის პასუხისმგებელი პირის ვინაობისა და დამუშავების მიზნების შესახებ მიწოდებულ ინფორმაციაზე, და დამატებით ინფორმაციაზე, რომელიც უზრუნველყოფს შესაბამისი ფიზიკური პირების შესახებ ინფორმაციის გამჭვირვალე დამუშავებას და მათ უფლებას მიიღონ მათი პერსონალური მონაცემების დამუშავების დადასტურება და დამუშავებული მონაცემები.“

მონაცემთა სუბიექტისათვის გასაკვირი აღმოჩნდეს. შესაბამისად, მონაცემთა სუბიექტმა, პირველ შრეში / მოდალობაში წარმოდგენილ ინფორმაციაზე დაყრდნობით უნდა შეძლოს იმის გააზრება, თუ რა გავლენა ექნება დამუშავებას მონაცემთა სუბიექტზე (აგრეთვე, იხ. ზემოთ, პუნქტი 10).

37. ციფრულ კონტექსტში, გარდა კონფიდენციალობის მრავალშრიანი ონლაინ განაცხადის / შეტყობინების უზრუნველყოფისა, დამუშავებისთვის პასუხისმგებელ პირებს აგრეთვე, შეუძლიათ გადაწყვიტონ გამჭვირვალობის *დამატებითი* ინსტრუმენტების გამოყენება (მაგალითები წარმოდგენილია ქვემოთ), რომელიც ინდივიდუალურ მონაცემთა სუბიექტს მასზე მორგებულ ინფორმაციას მიაწვდის. კერძოდ, ეს ინფორმაცია იქნება მორგებული ინდივიდუალური მონაცემთა სუბიექტის პოზიციასთან და იმ საქონელთან/სერვისებთან, რომლითაც სარგებლობს მონაცემთა სუბიექტი. WP29-ი მრავალშრიანი ონლაინ კონფიდენციალობის განაცხადის / შეტყობინების გამოყენების რეკომენდაციას იძლევა, თუმცა, უნდა ითქვას, რომ ეს რეკომენდაცია არ გამორიცხავს გამჭვირვალობის მოთხოვნებთან შესაბამისობის ინოვაციური მეთოდების შემუშავებას და გამოყენებას.

მრავალშრიანი მიდგომა არა-ციფრულ გარემოში

38. მონაცემთა სუბიექტებისთვის გამჭვირვალობასთან დაკავშირებული ინფორმაციის უზრუნველყოფისადმი მრავალშრიანი მიდგომა, შესაძლოა, აგრეთვე, გამოყენებული იქნას ოფლაინ / არა-ციფრულ გარემოში (ე.ი., რეალური სამყაროს გარემოში, როგორიცაა, პირისპირ ან სატელეფონო კომუნიკაცია), სადაც დამუშავებისთვის პასუხისმგებელ პირს ინფორმაციის უზრუნველყოფის მიზნით შეუძლია გამოიყენოს სხვადასხვა მოდალობები (ასევე, იხ. 33-ე-37-ე პუნქტები და 39-ე-მე-40 პუნქტები ინფორმაციის მიწოდების სხვადასხვა მოდალობების შესახებ). ეს მიდგომა არ უნდა აგვერიოს კონფიდენციალობის მრავალშრიანი განაცხადის / შეტყობინების საკითხთან, რომელიც ცალკეა. რა ფორმატებიც არ უნდა იქნას გამოყენებული მრავალშრიანი მიდგომის ფარგლებში, WP29-ის რეკომენდაცია მდგომარეობს იმაში, რომ პირველი „შრე“ (კერძოდ, ძირითადი საშუალება, რომლითაც დამუშავებისთვის პასუხისმგებელი პირი პირველ კონტაქტს ამყარებს მონაცემთა სუბიექტთან), როგორც წესი, უნდა გადმოსცემდეს ყველაზე მნიშვნელოვან ინფორმაციას (იხ. პუნქტი 36 ზემოთ), კერძოდ: დამუშავების მიზნების შესახებ დეტალური ინფორმაცია, დამუშავებისთვის პასუხისმგებელი პირის ვინაობა და მონაცემთა სუბიექტის უფლებების არსებობა, ისევე, როგორც ინფორმაცია დამუშავების ყველაზე მნიშვნელოვანი გავლენის შესახებ და დამუშავება, რომელიც შესაძლოა მოულოდნელი აღმოჩნდეს მონაცემთა სუბიექტისთვის. მაგალითად, როდესაც დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტთან პირველ

კონტაქტს ამყარებს ტელეფონით, ამ ინფორმაციის მიწოდება შესაძლებელია სატელეფონო ზარის მიმდინარეობისას, ხოლო მე-13/მე-14 მუხლით გათვალისწინებული ინფორმაციის მიწოდება შესაძლებელია დამატებითი, განსხვავებული საშუალებებით, მაგალითად, კონფიდენციალობის პოლიტიკის ელ-ფოსტის საშუალებით გაგზავნით და/ან მონაცემთა სუბიექტს შესაძლოა გაეგზავნოს დამუშავებისთვის პასუხისმგებელი პირის მრავალშრიანი, ონლაინ კონფიდენციალობის განაცხადის / შეტყობინების ბმული.

„მიწოლის“ და „გამოქაჩვის“ შეტყობინებები

39. გამჭვირვალობისთვის საჭირო ინფორმაციის მიწოდების კიდევ ერთი შესაძლო გზაა „მიწოლის“ და „გამოქაჩვის“ შეტყობინებების გამოყენება. „მიწოლის“ შეტყობინება გულისხმობს გამჭვირვალობისთვის საჭირო „დროული“ ინფორმაციის მიწოდებას, ხოლო „გამოქაჩვის“ შეტყობინება ინფორმაციის ხელმისაწვდომობას ხელს უწყობს ისეთი მეთოდებით, როგორიცაა, ნებართვის მართვა, გამჭირვალობის დაფები და „გაიგე მეტი“-ის გაკვეთილები. კონფიდენციალობის. აღნიშნული მომხმარებელზე უფრო მეტად ორიენტირებულ გამოცდილებას ქმნის, გამჭვირვალობის ჭრილში.
    - კონფიდენციალობის დაფა (dashboard) არის ერთი კონკრეტული წერტილი, საიდანაც მონაცემთა სუბიექტს შეუძლია, გაეცნოს „კონფიდენციალობის შესახებ ინფორმაციას“ და მართოს საკუთარი პრეფერენციები კონფიდენციალობასთან დაკავშირებით, კერძოდ, დაუშვას ან არ დაუშვას საკუთარი მონაცემების გამოყენება მოცემული სერვისის მიერ. აღნიშნული განსაკუთრებით სასარგებლოა, როდესაც მონაცემთა სუბიექტი ერთი და იგივე სერვისს იყენებს სხვადასხვა მოწყობილობებზე, რადგან აღნიშნული მათ აძლევს საკუთარ პერსონალურ მონაცემებზე წვდომას და მისი კონტროლის შესაძლებლობას, იმის მიუხედავად, თუ როგორ იყენებს იგი სერვისს. მონაცემთა სუბიექტის შესაძლებლობა, მანუალურად შეიტანოს ცვლილებები კონფიდენციალობის პარამეტრებში, კონფიდენციალობის დაფის გამოყენების გზით, აგრეთვე აადვილებს კონფიდენციალობის განაცხადის / შეტყობინების პერსონალიზებას, რათა იგი ასახავდეს დამუშავების მხოლოდ იმ ტიპებს, რომლებიც იმ კონკრეტულ მონაცემთა სუბიექტთან მიმართებით მიმდინარეობს. კონფიდენციალობის დაფის სერვისის არსებულ არქიტექტურაში გათვალისწინება (მაგ., იგივე დიზაინის ან ბრენდირების გამოყენება, რომელიც სერვისის დანარჩენ ნაწილში გამოიყენება) მიზანშეწონილია, რადგან იგი უზრუნველყოფს მისი წვდომის და გამოყენების ინტუიციურობას და შესაძლოა ხელი შეუწყოს მომხმარებლის მიერ ამ ინფორმაციის გაცნობას სწორედ ისე, როგორც სერვისის სხვა ასპექტებთან მიმართებით. აღნიშნული

ეფექტური გზაა იმის საჩვენებლად, რომ „კონფიდენციალობის შესახებ ინფორმაცია“ არის სერვისის საჭირო და განუყოფელი ნაწილი და არა სამართლებრივი ჟარგონების ვრცელი ჩამონათვალი.

- <u>დროული</u> შეტყობინება გამოიყენება კონფიდენციალობის შესახებ კონკრეტული ინფორმაციის მიწოდებისთვის, სპეციალური (ad hoc) ფორმით, როდესაც მიზანშეწონილია მონაცემთა სუბიექტის მიერ ამ ინფორმაციის წაკითხვა. აღნიშნული მეთოდი სასარგებლოა მონაცემთა დამუშავების პროცესის სხვადასხვა ეტაპებზე ინფორმაციის მიწოდებისთვის; იგი ხელს უწყობს ინფორმაციის უზრუნველყოფას „ადვილად გადამუშავებადი“ პორციების სახით და ამცირებს კონფიდენციალობის ერთ განაცხადზე/შეტყობინებაზე დამოკიდებულებას, რომელიც შესაძლოა შეიცავდეს კონტექსტის გარეშე რთულად გასაგებ ინფორმაციას. მაგალითად, თუ მონაცემთა სუბიექტი ყიდულობს პროდუქტს ონლაინ სივრცეში, შესაძლებელია მოკლე განმარტებითი ინფორმაციის უზრუნველყოფა პოპ-აპ ფანჯრების გამოყენებით, რომლებიც შესაბამის ველებთან იქნება დაკავშირებული. ინფორმაცია, რომელიც დაკავშირებული იქნება იმ ველთან, სადაც მონაცემთა სუბიექტს შეყავს ტელეფონის ნომერი, შეიძლება განმარტავდეს, მაგალითად, რომ მონაცემები შეგროვება ხდება მხოლოდ შესყიდული ნივთის შესახებ დასაკავშირებლად და ეს მონაცემები გადაეცემა მხოლოდ მიწოდების სერვისს.

სხვა ტიპის „შესაფერისი ზომები“

40. იმის გათვალისწინებით, რომ ევროკავშირში ინტერნეტის ხელმისაწვდომობა არის მაღალი და მონაცემთა სუბიექტებს ინტერნეტში შესვლა შეუძლიათ ნებისმიერ დროს, სხვადასხვა ადგილებიდან და სხვადასხვა მოწყობილობების გამოყენებით, როგორც ზემოთ აღინიშნა, WP29-ის პოზიცია მდგომარეობს იმაში, რომ გამჭვირვალობისთვის საჭირო ინფორმაციის მიწოდებისთვის „შესაფერისი ზომები“ იმ დამუშავებისთვის პასუხისმგებელი პირების შემთხვევაში, რომლებიც ციფრულ/ონლაინ სფეროში არიან წარმოდგენილები, გულისხმობს ამომწურავი ელექტრონული კონფიდენციალობის განაცხადის/შეტყობინების გაცნობას მონაცემთა სუბიექტისთვის. ამავდროულად, მონაცემთა შეგროვებასთან და დამუშავებასთან დაკავშირებული გარემოებებიდან გამომდინარე, დამუშავებისთვის პასუხისმგებელ პირს შესაძლოა, დასჭირდეს დამატებით (ან ალტერნატიული საშუალების სახით, თუ დამუშავებისთვის პასუხისმგებელი პირი არ არის წარმოდგენილი ციფრულ/ონლაინ სივრცეში) სხვა მოდალობების და ფორმატების გამოყენება, ინფორმაციის მიწოდების მიზნით. მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდების სხვა შესაძლო გზები, რომლებიც ქვემოთ ჩამოთვლილ განსხვავებულ გარემოებებთან არის

დაკავშირებული, შესაძლოა მოიცავდეს ქვემოთ ჩამოთვლილ (კონკრეტული გარემოებებისთვის შესაფერის) საშუალებებს. როგორც ზემოთ აღინიშნა, დამუშავებისთვის პასუხისმგებელ პირებს შეუძლიათ მიმართონ მრავალშრიანი მიდგომას, თუ ისინი განსხვავებული მეთოდების კომბინაციის გამოყენებას გადაწყვეტენ. ამავდროულად, მათ უნდა უზრუნველყონ, რომ პირველი მოდალობა, რომელიც მონაცემთა სუბიექტთან კომუნიკაციისთვის გამოიყენება, ყოველთვის შეიცავდეს ყველაზე მნიშვნელოვან ინფორმაციას (იხ. პუნქტები 36 და 38).

a. <u>ნაბეჭდი დოკუმენტი, მაგალითად, ფოსტის საშუალებით ხელშეკრულების გაგზავნა:</u> წერილობითი განმარტებები, ლიფლეტები, სახელშეკრულებო დოკუმენტაციაში წარმოდგენილი ინფორმაცია, კარიკატურები, ინფოგრაფიკები და ფლოუჩარტები;

<u>b. სატელეფონო გარემო:</u> ზეპირი განმარტებები რეალური ადამიანის მიერ, რაც ინტერაქციას და კითხვებზე პასუხის გაცემას უწყობს ხელს, ან ავტომატური თუ წინასწარ ჩაწერილი ინფორმაცია, რომელიც მომხმარებელს საშუალებას აძლევს, მოისმინოს უფრო დეტალური ინფორმაცია;

<u>c. ჭკვიანი ტექნოლოგია ეკრანის გარეშე / საგნების ინტერნეტის გარემო, როგორიცაა, Wi-Fi მონიტორინგის ანალიტიკა:</u> პიქტოგრამები, QR კოდები, ხმოვანი გაფრთხილებები, წერილობითი დეტალები, რომლებიც ინკორპორირებულია მომხმარებლის ნაბეჭდ ინსტრუქციებში, ვიდეოები, რომლებიც ინკორპორირებულია მომხმარებლის ციფრულ ინსტრუქციებში, SMS-ით ან ელ-ფოსტით გაგზავნილი შეტყობინებები, თვალსაჩინო ადგილას განთავსებული დაფები, რომლებიც ინფორმაციას შეიცავს, საჯარო ნიშნები ან კამპანიები საზოგადოების ინფორმირების მიზნით;

<u>d. პირისპირ გარემო, როგორიცაა, გამოკითხვაში მონაწილეობის მიღება, სერვისისთვის პირადად დარეგისტრირება:</u> ზეპირი ან წერილობითი განმარტებები, რომლებიც მონაცემთა სუბიექტს დაბეჭდილი ან ელექტრონული ფორმით გადაეცემა;

<u>e. „რეალური ცხოვრების“ გარემო, სადაც მიმდინარეობს ჩაწერა CCTV-ის (ვიდეო სამეთვალყურეო სისტემები)/დრონის გამოყენებით:</u> თვალსაჩინო ადგილას განთავსებული დაფები, რომლებიც შეიცავს ინფორმაციას, საჯარო ნიშნები, კამპანიები საზოგადოების ინფორმირების მიზნით ან შეტყობინების გამოქვეყნება გაზეთში / მედიის საშუალებით.

ინფორმაცია პროფილირების და ავტომატიზებული გადაწყვეტილების მიღების შესახებ

41. ინფორმაცია ავტომატიზებული გადაწყვეტილების მიღების, მათ შორის, პროფილირების არსებობის შესახებ, რომელზეც მიუთითებს 22-ე მუხლის 1-ლი და მე-4 პუნქტები, იმ არსებით ინფორმაციასთან ერთად, რომელიც ეხება გამოყენებულ ლოგიკას და მონაცემთა სუბიექტზე დამუშავების მნიშვნელოვან და გათვალისწინებულ შედეგებს, წარმოადგენს იმ სავალდებულო ინფორმაციას, რომელიც დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს უნდა მიაწოდოს 13.2(f) და 14.2(g) მუხლების შესაბამისად. WP29-მ შეიმუშავა სახელმძღვანელო პრინციპები ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღების და პროფილირების შესახებ[35], რომელიც შეიცავს დამატებით მითითებებს იმის შესახებ, თუ როგორ უნდა იქნას უზრუნველყოფილი გამჭვირვალობა კონკრეტულად პროფილირების დროს. აღსანიშნავია, რომ გარდა გამჭვირვალობის სპეციფიური მოთხოვნებისა, რომელიც ვრცელდება ავტომატიზებულ გადაწყვეტილების მიღებაზე 13.2(f) და 14.2(g) მუხლების თანახმად, ამ სახელმძღვანელო პრინციპებში წარმოდგენილი კომენტარები ეხება პერსონალური მონაცემების დამუშავების შედეგების შესახებ მონაცემთა სუბიექტების ინფორმირების მნიშვნელობას, და ზოგად პრინციპს, რომ მონაცემთა სუბიექტებისათვის მოულოდნელი არ უნდა იყოს მათი პერსონალური მონაცემების დამუშავება, რაც თანაბრად ვრცელდება ზოგადად პროფილირებაზე (არა მხოლოდ პროფილირებაზე, რომელსაც ითვალისწინებს 22-ე მუხლი[36]), როგორც დამუშავების ტიპზე.[37]

სხვა საკითხები - რისკები, წესები და დაცვის მექანიზმები

42. GDPR-ის პრეამბულის 39-ე პუნქტი, აგრეთვე, მიუთითებს გარკვეული ინფორმაციის მიწოდებაზე, რომელსაც პირდაპირ არ ითვალისწინებს მე-13 და მე-14 მუხლები (იხ. 28-ე პუნქტი ზემოთ). კერძოდ, მონაცემთა სუბიექტებს უნდა მიეწოდოს ინფორმაცია რისკების, წესების და დაცვის მექანიზმების შესახებ, პერსონალური მონაცემების დამუშავებასთან მიმართებით, რაც დაკავშირებულია სხვადასხვა საკითხებთან. ეს საკითხები მოიცავს მონაცემთა

[35] სახელმძღვანელო პრინციპები ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღების და პროფილირების შესახებ, 2016/679 რეგულაციის მიზნებისთვის, WP251.

[36] აღნიშნული ვრცელდება გადაწყვეტილებების იღებაზე მხოლოდ ავტომატიზებული დამუშავების საფუძველზე, მათ შორის, პროფილირების საფუძველზე, რასაც გარკვეული სამართლებრივი შედეგები მოაქვს მონაცემთა სუბიექტთან დაკავშირებით ან მნიშვნელოვან გავლენას ახდენს მასზე.

[37] პრეამბულის მე-60 პუნქტი, რომელიც ამ შემთხვევაშია რელევანტური, აცხადებს: „დამატებით, მონაცემთა სუბიექტი ინფორმირებული უნდა იქნას პროფილირების არსებობის და ამგვარი პროფილირების შედეგების შესახებ.“

დაცვის ზეგავლენის შეფასებებს (DPIA). მონაცემთა დაცვის ზეგავლენის შეფასებების თაობაზე WP29-ის სახელმძღვანელო პრინციპების თანახმად,[38] დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა განიხილონ DPIA-ს (ან მისი ნაწილის) გამოქვეყნების შესაძლებლობა, რათა ხელი შეუწყონ ნდობას დამუშავების პროცესში და მოახდინონ გამჭვირვალობის და ანგარიშვალდებულების დემონსტრირება, თუმცა, ამგვარი შეფასებების გამოქვეყნება სავალდებულო არ არის. ამას გარდა, ქცევის კოდექსის დაცვა (მე-40 მუხლი) ხელს უწყობს გამჭვირვალობის დემონსტრირებას, რადგან ქცევის კოდექსის შემუშავება შესაძლებელია კონკრეტულად GDPR-ის გამოყენების დემონსტრირების მიზნით, შემდეგი მიმართულებებით: სამართლიანი და გამჭვირვალე დამუშავება; საზოგადოებისა და მონაცემთა სუბიექტებისთვის ინფორმაციის მიწოდება; და ინფორმაციის მიწოდება ბავშვებისთვის და მათი დაცვა; და სხვა საკითხები.

43. გამჭვირვალობასთან დაკავშირებულია კიდევ ერთი მნიშვნელოვანი საკითხი - **მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას („Privacy by Design“) („Privacy by Default“)** (25-ე მუხლის მოთხოვნების შესაბამისად). ამ პრინციპების თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა მონაცემთა დაცვის საკითხები თავიდანვე უნდა გაითვალისწინონ დამუშავების ოპერაციებში და სისტემებში, ნაცვლად მონაცემთა დაცვის მოთხოვნებთან შესაბამისობის ბოლო მომენტში გათვალისწინებისა. პრეამბულის 78-ე პუნქტი მიუთითებს დამუშავებისთვის პასუხისმგებელი პირების მიერ ისეთი ზომების მიღებაზე, რომელიც უზრუნველყოფს მონაცემთა დაცვის პრინციპებთან შესაბამისობას, კერძოდ, მონაცემთა დაცვის სტანდარტების გათვალისწინებას ახალი პროდუქტის ან მომსახურების შექმნის პროცესში და მონაცემთა დაცვას პირველად პარამეტრად. აღნიშნული მოიცავს ზომებს, რომლებიც დაკავშირებულია პერსონალური მონაცემების დამუშავების და ფუნქციის გამჭვირვალობასთან.

44. ამას გარდა, ერთობლივი დამუშავებისთვის პასუხისმგებელი პირების საკითხი დაკავშირებულია რისკების, წესების და დაცვის მექანიზმების შესახებ მონაცემთა სუბიექტების ინფორმირებასთან. 26.1-ე მუხლის თანახმად, ერთობლივმა დამუშავებისთვის პასუხისმგებელმა პირებმა გამჭვირვალედ უნდა განსაზღვრონ თავიანთი პასუხისმგებლობები GDPR-თან შესაბამისობის უზრუნველსაყოფად, დამუშავებისთვის პასუხისმგებელ პირებს ,შორის შეთანხმების საფუძველზე, განსაკუთრებით, მონაცემთა სუბიექტების მიერ

[38] „სახელმძღვანელო პრინციპები მონაცემთა დაცვის ზეგავლენის შეფასების შესახებ და იმის შეფასების შესახებ, გამოიწვევს თუ არა დამუშავება მაღალ რისკს, 2016/679 რეგულაციის მიზნებისთვის, WP 248, rev.1

უფლებების რეალიზებისა და მე-13 და მე-14 მუხლების შესაბამისად სუბიექტების ინფორმირების თვალსაზრისით. 26.2-ე მუხლი, აგრეთვე, ითხოვს, რომ აღნიშნული შეთანხმების არსი ხელმისაწვდომი უნდა იყოს მონაცემთა სუბიექტისათვის. სხვა სიტყვებით რომ ვთქვათ, მონაცემთა სუბიექტისათვის აბსოლუტურად ნათელი უნდა იყოს, თუ რომელ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს უნდა მიმართოს იმ შემთხვევაში, თუ GDPR-ით დადგენილი ერთი ან მეტი უფლების განხორციელებას მოისურვებს.[39]

შემდგომ დამუშავებასთან დაკავშირებული ინფორმაცია

45. მე-13 და მე-14 მუხლები შეიცავს დებულებას,[40] რომლის თანახმადაც მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს მოეთხოვება მონაცემთა სუბიექტის ინფორმირება იმ შემთხვევაში, თუ იგი აპირებს განახორციელოს მათი პერსონალური მონაცემების შემდგომი დამუშავება იმ მიზნით, რომელიც განსხვავდება მონაცემთა შეგროვების/მოპოვების მიზნისგან. ასეთ შემთხვევაში, *„მონაცემთა შემდგომ დამუშავებამდე* დამუშავებისთვის პასუხისმგებელმა პირმა *მონაცემთა სუბიექტს უნდა აცნობოს განსხვავებული მიზნის შესახებ და მიაწოდოს სხვა შესაბამისი დამატებითი ინფორმაცია, მე-2 პუნქტის შესაბამისად.“* ეს დებულებები იწვევს კონკრეტულად 5.1(b) მუხლით გათვალისწინებული პრინციპის ამოქმედებას, რომლის თანახმადაც პერსონალური მონაცემების შეგროვება უნდა მოხდეს კონკრეტული, მკაფიოდ განსაზღვრული და კანონიერი მიზნებისთვის, ხოლო შემდგომი დამუშავება, რომელიც შეუთავსებელია ამ მიზნებთან არის დაუშვებელი.[41] 5.1(b) მუხლის მეორე ნაწილში მითითებულია, რომ მონაცემთა შემდგომი დამუშავება საჯარო ინტერესისათვის არქივირების მიზნით, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებისათვის 89-ე მუხლის პირველი პუნქტის შესაბამისად არ უნდა ჩაითვალოს თავდაპირველ მიზანთან შეუთავსებელ მიზნად. როდესაც პერსონალური მონაცემების შემდგომი დამუშავება ხდება იმ მიზნებისთვის, რომელიც შეუთავსებელია თავდაპირველ მიზნებთან (ამ სკაითხს ეხება 6.4 მუხლი[42]), გამოიყენება 13.3 და 14.4 მუხლები. ამ მუხლებით

[39] 26.3 მუხლის თანახმად, შეთახმების პირობების მიუხედავად, მონაცემთა სუბიექტი უფლებამოსილია, ისარგებლოს ამ რეგულაციით გარანტირებული უფლებებით თითოეულ დამმუშავებელთან მიმართებით და მის წინააღმდეგ.

[40] კერძოდ, მე-13 მუხლის მესამე პუნქტი და მე-14 მუხლის მეოთხე პუნქტი, რომლებიც იდენტურად არის ფორმულირებული, გარდა სიტყვისა „შეგროვება“, რომელიც მე-13 მუხლში არის გამოყენებული, ხოლო მე-14 მუხლში იგი ჩანაცვლებულია სიტყვით „მოპოვება’.

[41] ამ პრინციპთან დაკავშირებით, იხ., მაგალითად: პრეამბულის პუნქტები 47, 50, 61, 156, 158; მუხლი 6.4 და 89.

[42] 6.4 მუხლში წარმოდგენილია იმ ფაქტორების არა-ამომწურავი ჩამონათვალი, რომლებიც გათვალისწინებული უნდა იქნას იმის დადგენისას, თუ რამდენად თავსებადია სხვა მიზნით დამუშავება

გათვალისწინებული მოთხოვნა, რომ მონაცემთა სუბიექტი ინფორმირებული უნდა იყოს შემდგომი დამუშავების შესახებ, ეხმიანება GDPR-ში წარმოდგენილ პოზიციას, რომ მონაცემთა სუბიექტს უნდა ჰქონდეს გონივრული მოლოდინი პერსონალური მონაცემების შეგროვების დროს და კონტექსტში, რომ ადგილი ექნება მონაცემთა დამუშავებას კონკრეტული მიზნისთვის.[43] სხვა სიტყვებით რომ ვთქვათ, მონაცემთა სუბიექტისათვის მოულოდნელი (გასაკვირი) არ უნდა იყოს მათი პერსონალური მონაცემების დამუშავების მიზანი.

46. 13.3 და 14.4 მუხლები მიუთითებს *„მე-2 პუნქტში მითითებული ნებისმიერი დამატებითი რელევანტური ინფორმაციის“* მიწოდებაზე, რაც ერთი შეხედვით, შესაძლოა განმარტებული იქნას, როგორც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისთვის გარკვეული დისკრეციის მინიჭება, თავად გადაწყვიტოს, თუ მე-2 ქვეპუნქტში (მე-13 ან მე-14 მუხლის) მითითებული ინფორმაციის რა მოცულობა და კატეგორიები უნდა მიეწოდოს მონაცემთა სუბიექტს. (პრეამბულის 61-ე პუნქტი აღნიშნულზე მიუთითებს, როგორც *„სხვა აუცილებელი ინფორმაცია“*). თუმცა, იგულისხმება, რომ აღნიშნულ ქვეპუნქტში მითითებული ყველა ინფორმაცია უნდა მიეწოდოს მონაცემთა სუბიექტს, გარდა იმ შემთხვევისა, თუ რომელიმე კატეგორია არ არსებობს ან არსებულ სიტუაციას არ ეხება.

47. WP29-ის რეკომენდაციის თანახმად, გამჭვირვალობის, სამართლიანობის და ანგარიშვალდებულების უზრუნველსაყოფად, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა განიხილონ მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდება კონფიდენციალობის პოლიტიკაში / შეტყობინებაში, 6.4 მუხლის თანახმად განხორციელებული თავსებადობის ანალიზის საფუძველზე,[44] იმ შემთხვევაში, თუ დამუშავების ახალი მიზანი არ ეყრდნობა თანხმობას ან ეროვნულ/ევროკავშირის სამართალს. (სხვა სიტყვებით რომ ვთქვათ, განმარტება იმის შესახებ, თუ რამდენად თავსებადია სხვა მიზანი ან მიზნები თავდაპირველ მიზანთან). აღნიშნული მონაცემთა სუბიექტს მისცემს შესაძლებლობას, განიხილოს შემდგომი დამუშავების თავსებადობის საკითხი და უზრუნველყოფილი დაცვის მექანიზმები და გადაწყვიტოს, განახორციელოს

მონაცემთა თავდაპირველად შეგროვების მიზანთან, კერძოდ: ა) მონაცემების შეგროვების თავდაპირველ მიზანსა და შემდგომი დამუშავების მიზანს შორის ნებისმიერი კავშირი; ბ) მიზეზი, რის საფუძველზეც შეგროვდა პერსონალური მონაცემები, განსაკუთრებით, მონაცემთა სუბიექტსა და დამმუშავებელს შორის ურთიერთობა; გ) პერსონალური მონაცემების შინაარსი/ხასიათი, განსაკუთრებით, მუშავდება თუ არა განსაკუთრებული კატეგორიის პერსონალური მონაცემები მე-9-ე მუხლის შესაბამისად, ან ნასამართლობასთან და სისხლის სამართლის დანაშაულებთან დაკავშირებული პერსონალური მონაცემები მე-10-ე მუხლის შესაბამისად; დ) შემდგომი დამუშავების სავარაუდო შედეგები მონაცემთა სუბიექტებისთვის; ე) უსაფრთხოების სათანადო გარანტიების არსებობა, რაც შესაძლოა მოიცავდეს დაშიფრვას ან ფსევდონიმიზაციას.

[43] პრეამბულა, პუნქტები 47 და 50.

[44] პრეამბულა, პუნქტი 50.

თუ არა საკუთარი უფლებები, მაგ., უფლება დამუშავების შეზღუდვაზე ან დამუშავების შეწყვეტის მოთხოვნის უფლება და სხვა.[45] თუ დამუშავებისთვის პასუხისმგებელი პირი გადაწყვეტს, ამგვარი ინფორმაცია არ შეიტანოს კონფიდენციალობის განაცხადში / შეტყობინებაში, WP29-ის რეკომენდაციის თანახმად, მან მონაცემთა სუბიექტს მკაფიოდ უნდა განუმარტოს, რომ მას ამ ინფორმაციის მიღება მოთხოვნის საფუძველზე შეუძლია.

48. მონაცემთა სუბიექტის უფლებების განხორციელებასთან დაკავშირებულია ვადების საკითხი. როგორც ზემოთ ითქვა, ინფორმაციის უზრუნველყოფა დროულად მე-13 და მე-14 მუხლებით გათვალისწინებული განჭვრეტადობის მოთხოვნების სასიცოცხლო ელემენტია და არსებითად არის დაკავშირებული დამუშავების კონცეფციასთან. ინფორმაცია შემდგომი დამუშავების შესახებ „შემდგომ დამუშავებამდე“ უნდა მიეწოდოს მონაცემთა სუბიექტს. WP29-ის პოზიცია მგომარეობს იმაში, რომ გონივრული ვადა უნდა გავიდეს შეტყობინებიდან დამუშავების დაწყებამდე და მონაცემთა სუბიექტის მიერ შეტყობინების მიღებისთანავე არ უნდა იქნას დამუშავება დაწყებული. აღნიშნული მონაცემთა სუბიექტს აძლევს ეფექტურ შესაძლებლობას, დაფიქრდეს შემდგომი დამუშავების შესახებ (და სავარაუდოდ, განახორციელოს საკუთარი უფლებები შემდგომ დამუშავებასთან მიმართებით. ის, თუ რა იქნება აღნიშნული გონივრული პერიოდი, დამოკიდებულია კონკრეტულ გარემოებებზე. სამართლიანობის პრინციპის თანახმად, რაც უფრო მეტად ინვაზიურია (ან ნაკლებად მოსალოდნელია) შემდგომი დამუშავება, მით მეტი დრო უნდა გავიდეს შეტყობინებიდან დამუშავების დაწყებამდე. მსგავსად აღნიშნულისა, ანგარიშვალდებულების პრინციპის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს უნდა შეეძლოთ მოცემულ გარემოებებში ინფორმაციის მიწოდების ვადების შესახებ მიღებული გადაწყვეტილების დასაბუთება და დემონსტრირება იმისა, თუ რამდენად სამართლიანია ეს ვადები მონაცემთა სუბიექტების მიმართ. (აგრეთვე, იხ. კომენტარები გონივრული ვადების დადგენასთან დაკავშირებით, პ. 30-32).

ვიზუალიზაციის ინსტრუმენტები

49. GDPR-ით გათვალისწინებული გამჭვირვალობის პრინციპი ვრცელდება არა მხოლოდ ენობრივ კომუნიკაციაზე (წერილობითზე ან ზეპირზე). GDPR-ი ითვალისწინებს საჭიროების შემთხვევაში, ვიზუალიზაციის ინსტრუმენტების გამოყენებას (კერძოდ, პიქტოგრამები, სერტიფიცირების მექანიზმები,

[45] პრეამბულა, პუნქტი 63. აღნიშნული მონაცემთა სუბიექტს მისცემს შესაძლებლობას, განახორციელოს წვდომის უფლება, რათა იყოს ინფორმირებული დამუშავების კანონიერების შესახებ და შეძლოს მისი (კანონიერების) გადამოწმება.

მონაცემთა დაცვის ბეჭდები და ნიშნები). პრეამბულის 58-ე პუნქტის[46] თანახმად, იმ ინფორმაციის ხელმისაწვდომობა, რომლის ადრესატიც არის საზოგადოება ან მონაცემთა სუბიექტები, განსაკუთრებით მნიშვნელოვანია ონლაინ გარემოში.[47]

50. პრეამბულის მე-60 პუნქტის თანახმად, შესაძლებელია მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდება „სტანდარტიზებულ სიმბოლოებთან (პიქტოგრამებთან)" კომბინაციაში, რაც მრავალშრიანი მიდგომის გამოყენების საშუალებას იძლევა. ამავდროულად, სიმბოლოების გამოყენებამ არ უნდა ჩაანაცვლოს მონაცემთა სუბიექტის უფლებების განხორციელებისთვის საჭირო ინფორმაცია და არ უნდა იქნას გამოყენებული, როგორც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მე-13 და მე-14 მუხლებით დადგენილ ვალდებულებებთან შესაბამისობის მაგიერი. 12.7 მუხლი ეხება ამგვარი სიმბოლოების გამოყენებას და ადგენს, რომ:

> *„მე-13-ე და მე-14-ე მუხლების თანახმად მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდებისას შეიძლება ამავდროულად გამოყენებულ იქნას სტანდარტიზებული სიმბოლოები, რათა თვალსაჩინოდ, გასაგებად და ნათლად იქნას აღწერილი დაგეგმილი მონაცემთა დამუშავების პროცესი. ელექტრონული ფორმით წარმოდგენილი სიმბოლოები უნდა იყოს ელექტრონულად წაკითხვადი."*

51. 12.7 მუხლის თანახმად, *„ელექტრონული ფორმით წარმოდგენილი სიმბოლოები უნდა იყოს ელექტრონულად წაკითხვადი"*, რაც ნიშნავს იმას, რომ შესაძლოა გარკვეულ შემთხვევებში სიმბოლოები არ იყოს ელექტრონული ფორმით წარმოდგენილი,[48] მაგალითად, სიმბოლოები ფიზიკურ

---

[46] „ამგვარი ინფორმაცია შეიძლება წარმოდგენილ იქნას ელექტრონული სახით, ვებ-გვერდზე, როცა მიმართვის ადრესატი საზოგადოებაა. ეს განსაკუთრებით მნიშვნელოვანია სიტუაციებში, როცა აქტორების სიმრავლე და არსებული პრაქტიკის ტექნოლოგიური სირთულე აძნელებს მონაცემთა სუბიექტის მიერ იმის გარკვევას, თუ ვინ და რა მიზნით აგროვებს მასთან დაკავშირებულ მონაცემებს, მაგალითად ონლაინ რეკლამირების შემთხვევაში."

[47] ამ კონტექსტში, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა გაითვალისწინონ მსხედველობის დარღვევის მქონე მონაცემთა სუბიექტები (მაგ., დალტონიზმის მქონე).

[48] GDPR-ში წარმოდგენილია „ელექტრონულად წაკითხვადის" განმარტება, თუმცა, დირექტივა 2013/37/EU17 „ელექტრონულად წაკითხვადს" განმარტავს შემდეგნაირად:

> *„ფაილის ფორმატი, რომლის სტრუქტურაც არის იმგვარი, რომ კომპიუტერულ აპლიკაციებს ადვილად შეუძლიათ მოახდინონ კონკრეტული მონაცემების იდენტიფიცირება, ამოცნობა და ამოღება, მათ შორის, ფაქტების შესახებ ინდივიდუალური განცხადებების და მათი შიდა სტრუქტურის. მონაცემები, რომლებიც დაშიფრულია ელექტრონულად წაკითხვად ფაილებში წარმოადგენს ელექტრონულად წაკითხვად მონაცემებს. ელექტრონულად წაკითხვადი ფორმატები შესაძლოა იყოს საჯარო ან ვინმეს საკუთრებაში არსებული; ისინი შესაძლოა მოიცავდეს ან არ მოიცავდეს ფორმალურ სტანდარტებს. დოკუმენტები, რომლებიც დაშიფრულია იმგვარი ფორმატის ფაილში, რაც ზღუდავს ავტომატურ დამუშავებას, იმის გამო,*

დოკუმენტებზე, საგნების ინტერნეტში ჩართულ მოწყობილობებზე ან საგნების ინტერნეტში ჩართული მოწყობილობის შეფუთვაზე, შეტყობინებები საზოგადოებრივ ადგილებში Wi-Fi-ის მონიტორინგის შესახებ, QR კოდები და შეტყობინებები ვიდეო სამეთვალყურეო სისტემების შესახებ.

52. ნათელია, რომ სიმბოლოების გამოყენების მიზანია მონაცემთა სუბიექტთათვის გამჭვირვალობის გაზრდა და დიდი მოცულობის წერილობითი ინფორმაციის მონაცემთა სუბიექტისათვის წარდგენის საჭიროების შემცირება. ამავდროულად, სიმბოლოების გამოყენება იმისათვის, რომ მონაცემთა სუბიექტებს მე-13 და მე-14 მუხლებით დადგენილი ინფორმაცია ეფექტურად წარედგინოს, დამოკიდებულია სიმბოლოების / გამოსახულებების სტანდარტიზაციაზე, რომლებიც საყოველთაოდ იქნება გამოყენებული და აღიარებული ევროკავშირის მასშტაბით, როგორც შესაბამისი ინფორმაციის შემოკლებული ვერსია. ამ მხრივ, GDPR-ი კომისიას აკისრებს სიმბოლოთა კოდექსის შემუშავების პასუხისმგებლობას, თუმცა, საბოლოოდ, ევროპის მონაცემთა დაცვის საბჭო უფლებამოსილია, კომისიის მოთხოვნის საფუძველზე ან საკუთარი ინიციატივით, კომისიას წარუდგინოს მოსაზრება ამგვარი სიმბოლოების შესახებ.[49] WP29 ითვალისწინებს, რომ პრეამბულის 166-ე პუნქტის შესაბამისად, სიმბოლოთა კოდექსის შემუშავება უნდა ეყრდნობოდეს მტკიცებულებაზე დაფუძნებულ მიდგომას, ხოლო ამგვარ სტანდარტიზაციამდე აუცილებელია ფართომასშტაბიანი კვლევის ჩატარება, ინდუსტრიის წარმომადგენლებთან და ფართო საზოგადოებასთან ერთად, მოცემულ კონტექსტში სიმბოლოების ეფექტურობასთან დაკავშირებით.

სერტიფიცირების მექანიზმები, ბეჭდები და ნიშნები

53. სტანდარტიზებული სიმბოლოების გამოყენების გარდა, GDPR-ი (მუხლი 42), აგრეთვე, ითვალისწინებს მონაცემთა დაცვის სერტიფიცირების მექანიზმების,

---

რომ შეუძლებელია მონაცემების ამ ფაილიდან ამოღება (ან ადვილად ამოღება), არ უნდა იქნას მიჩნეული ელექტრონულად წაკითხვად ფორმატში განთავსებულ მონაცემებად. წევრმა სახელმწიფოებმა, საჭიროების შესაბამისად, ხელი უნდა შეუწყონ ღია, ელექტრონულად წაკითხვადი ფორმატების გამოყენებას.“

[49] 12.8 მუხლის თანახმად, ევროკომისია უფლებამოსილია 92-ე მუხლის შესაბამისად მიიღოს დელეგირებული აქტები სტანდარტიზებული სიმბოლოებით გადმოცემული ინფორმაციისა და სტანდარტიზებული სიმბოლოების მიწოდების პროცედურის დადგენის მიზნით. პრეამბულის 166-ე პუნქტი (რომელიც ეხება ზოგადად კომისიის დელეგირებულ აქტებს) შეიცავს ინსტრუქციებს და ადგენს, რომ კომისიამ უნდა განახორციელოს სათანადო კონსულტაციები მოსამზადებელი სამუშაოს ფარგლებში, მათ შორის, ექსპერტულ დონეზე. ამავდროულად, ევროპის მონაცემთა დაცვის საბჭო (EDPB) აგრეთვე, მნიშვნელოვან საკონსულტაციო როლს ასრულებს სიმბოლოთა სტანდარტიზაციასთან დაკავშირებით, რადგან 70.1(r) მუხლის თანახმად, EDPB-მ, საკუთარი ინიციატივის საფუძველზე ან საჭიროების შესაბამისად, კომისიის მოთხოვნის საფუძველზე, კომისიას უნდა წარუდგინოს მოსაზრებები სიმბოლოების შესახებ.

მონაცემთა დაცვის ბეჭდებისა და ნიშნების გამოყენებას, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისა და დამუშავებაზე უფლებამოსილი პირების მიერ GDPR-თან შესაბამისობის სადემონსტრაციოდ და მონაცემთა სუბიექტებისთვის გამჭვირვალობის გაზრდის მიზნით.[50] WP29 შესაბამის დროს გამოსცემს სახელმძღვანელო პრინციპებს სერტიფიცირების მექანიზმების შესახებ.

მონაცემთა სუბიექტების უფლებების განხორციელება

54. გამჭვირვალობა მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს სამმაგ ვალდებულებას აკისრებს, GDPR-ით მონაცემთა სუბიექტისათვის გათვალისწინებულ უფლებებთან მიმართებით. კერძოდ, ისინი ვალდებულები არიან:[51]

    - მონაცემთა სუბიექტებს მიაწოდონ ინფორმაცია თავიანთი უფლებების შესახებ[52] (13.2(b) და 14.2(c) მუხლების შესაბამისად);
    - დაიცვან გამჭვირვალობის პრინციპი (ე.ი., კომუნიკაციების ხარისხთან დაკავშირებით, 12.1 მუხლის შესაბამისად), როდესაც ისინი მონაცემთა სუბიექტებს აწვდიან უფლებებს მე-15-34-ე მუხლებით გათვალისწინებული მონაცემთა სუბიექტების უფლებების შესახებ; და
    - ხელი შეუწყონ მონაცემთა სუბიექტების იმ უფლებების განხორციელებას, რომელთაც იცავს მე-15-22-ე მუხლები.

55. GDPR-ის მოთხოვნები ამ უფლებების განხორციელებასთან და საჭირო ინფორმაციის ხასიათთან დაკავშირებით შექმნილია იმისათვის, რომ მონაცემთა სუბიექტების პოზიცია იყოს ეფექტური იმისათვის, რომ მათ შეძლონ თავიანთი უფლებების დაცვა და მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისგან ანგარიშვალდებულების მოთხოვნა მათი პერსონალური მონაცემების დამუშავებასთან დაკავშირებით. პრეამბულის 59-ე პუნქტი ხაზს უსვამს, რომ *„უზრუნველყოფილი უნდა იქნას მოდალობები, რომელიც ხელს შეუწყობს მონაცემთა სუბიექტის უფლებების განხორციელებას“*, ხოლო მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა აგრეთვე უნდა *„უზრუნველყოს მოთხოვნების ელექტრონული ფორმით წარდგენის შესაძლებლობა, განსაკუთრებით მაშინ, როდესაც პერსონალური მონაცემების დამუშავება ხდება ელექტრონულად.“* მოდალობები, რომელსაც

[50] იხ. პრეამბულა, პუნქტი 100.

[51] მონაცემთა სუბიექტის უფლებების შესახებ GDPR-ის სექციის თანახმად (კერძოდ, სექცია 1, თავი III, მუხლი 12)

[52] მონაცემებზე წვდომა, მონაცემების გასწორება, დაბლოკვა, წაშლა ან განადგურება, მონაცემთა დამუშავების შეწყვეტა და ასევე მონაცემთა გადატანა

უზრუნველყოფს დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტის მიერ უფლებების განხორციელებასთან დაკავშირებით უნდა იყოს კონტექსტისა და დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის ურთიერთობის და ინტერაქციების შესაფერისი. ამ მიზნით, მიზანშეწონილია, მონაცემთა დამმუშავებელმა განიხილოს მონაცემთა სუბიექტის უფლებების განსახორციელებლად ერთი ან რამდენიმე სხვადასხვა მოდალობის უზრუნველყოფა, მონაცემთა სუბიექტსა და დამმუშავებელს შორის ინტერაქციის სხვადასხვა გზების შესაბამისად.

მაგალითი

ჯანდაცვის პროვაიდერი იყენებს ელექტრონულ ფორმას თავის ვებ-გვერდზე, ხოლო ქაღალდის ფორმებს კლინიკების მიმღებ განყოფილებებში, იმისათვის რომ ხელი შეუწყოს პერსონალურ მონაცემებზე წვდომის შესახებ მოთხოვნების წარდგენას როგორც ონლაინ, ისე პირისპირ ფორმატში. აღნიშნული მოდალობების მიუხედავად, ჯანდაცვის პროვაიდერი, აგრეთვე, იღებს სხვა საშუალებების გამოყენებით წარდგენილ მოთხოვნებს (მაგ., წერილის ან ელ-ფოსტის საშუალებით) და მას გამოყოფილი ჰყავს საკონტაქტო პირი (რომელთან დაკავშირებაც შესაძლებელია ელ-ფოსტით და იმეილით), რომელიც მონაცემთა სუბიექტებს თავიანთი უფლებების განხორციელებაში ეხმარება.

გამონაკლისები ინფორმაციის უზრუნველყოფის ვალდებულებიდან

გამონაკლისები მე-13 მუხლით დადგენილი ვალდებულებებიდან

56. მე-13 მუხლით დადგენილ ვალდებულებებთან დაკავშირებით გამონაკლისი დაშვებულია მხოლოდ იმ შემთხვევაში, როდესაც პერსონალური მონაცემების შეგროვება ხდება პირდაპირ მონაცემთა სუბიექტისგან და „იმ შემთხვევაში და იმდენად, რამდენადაც [მე-13 მუხლის 1-ლი, მე-2 და მე-3 პუნქტებით გათვალისწინებულ] ინფორმაციას უკვე ფლობს მონაცემთა სუბიექტი.“[53] ანგარიშვალდებულების პრინციპის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მოახდინოს დემონსტრირება იმისა, თუ რა ინფორმაცია (და დოკუმენტი) აქვს უკვე მონაცემთა სუბიექტს, როგორ და როდის მიიღო მან ეს ინფორმაცია და რომ მას შემდეგ, ამ ინფორმაციაში არ შესულა ისეთი ცვლილებები, რომელიც მას მოძველებულად აქცევს. ამას გარდა,

[53] მუხლი 13.4

ფრაზის „იმდენად, რამდენადაც“ გამოყენება 13.4 მუხლში ნათელს ხდის, რომ მაშინაც კი, თუ მონაცემთა სუბიექტს მე-13 მუხლით გათვალისწინებული ინფორმაციიდან გარკვეული კატეგორიების ინფორმაცია უკვე მიეწოდა, დამუშავებისთვის პასუხისმგებელ პირს კვლავ ეკისრება ვალდებულება, შეავსოს ეს ინფორმაცია, რათა მონაცემთა სუბიექტს სრულად ჰქონდეს 13.1 და 13.2 პუნქტებში ჩამოთვლილი ინფორმაციები. ქვემოთ წარმოდგენილია საუკეთესო პრაქტიკის მაგალითი, რომელიც ეხება 13.4 მუხლით გათვალისწინებული გამონაკლისის შეზღუდულად გამოყენებას.

მაგალითი

მომხმარებელი დარეგისტრირდა ელ-ფოსტის მომსახურების მისაღებად და დარეგისტრირების მომენტში მიიღო მე-13 მუხლის 1-ლი და მე-2 პუნქტებით გათვალისწინებულ ყველა ინფორმაცია. 6 თვის შემდეგ, მონაცემთა სუბიექტი ელ-ფოსტის სერვისის პროვაიდერის საშუალებით ააქტიურებს მყისიერი შეტყობინებების მიღების ფუნქციას და ამ მიზნით, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს აწვდის თავისი მობილური ტელეფონის ნომერს. პროვაიდერი მონაცემთა სუბიექტს აწვდის მე-13 მუხლის 1-ლი და მე-2 პუნქტებით გათვალისწინებულ ინფორმაციას ტელეფონის ნომრის დამუშავების შესახებ (მაგ., დამუშავების მიზნები და სამართლებრივი საფუძვლები, მიმღებები, შენახვის პერიოდი), თუმცა, სხვა ინფორმაციას, რომელიც მან მომხმარებელს 6 თვის წინ მიაწოდა, ხელმეორედ აღარ აწვდის, რადგან ეს ინფორმაცია მას შემდეგ არ შეცვლილა (ე.ი., დამუშავებისთვის პასუხისმგებელი პირის და მონაცემთა დაცვის ოფიცრის ვინაობა და საკონტაქტო ინფორმაცია, ინფორმაცია მონაცემთა სუბიექტის უფლებების შესახებ და შესაბამის ზედამხედველ ორგანოში გასაჩივრების უფლება). ამავდროულად, საუკეთესო პრაქტიკიდან გამომდინარე, მონაცემთა სუბიექტს უნდა მიეწოდოს ინფორმაცია სრულად, თუმცა, მონაცემთა სუბიექტმა უნდა შეძლოს, ადვილად გაარჩიოს, თუ მიღებული ინფორმაციიდან რომელია ახალი ინფორმაცია. მყისიერი შეტყობინებების სერვისის მიზნებისთვის ახალი დამუშავება, შესაძლოა, მონაცემთა სუბიექტზე ახდენდეს იმგვარ გავლენას, რაც მას უბიძგებს იმ უფლების გამოყენებისკენ, რომლის შესახებაც მას შესაძლებელია, რომ აღარ ახსოვს, რადგან ექვსი თვის წინ მიაწოდეს ინფორმაცია. ამ ინფორმაციის კიდევ ერთხელ მიწოდება ხელს უწყობს მონაცემთა სუბიექტის კარგად ინფორმირებას იმის შესახებ, თუ როგორ ხდება მისი პერსონალური მონაცემების გამოყენება და რა უფლებები აქვს მას.

გამონაკლისები მე-14 მუხლით დადგენილი ვალდებულებებიდან

57. მე-14 მუხლი ითვალისწინებს უფრო ფართო გამონაკლისებს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირზე დაკისრებული ინფორმირების ვალდებულებიდან, იმ შემთხვევებში, როდესაც მონაცემების მოპოვება არ ხდება მონაცემთა სუბიექტისგან. აღნიშნული გამონაკლისები, როგორც წესი, ვიწროდ უნდა იქნას განმარტებული და გამოყენებული. გარდა იმ შემთხვევებისა, როდესაც მონაცემთა სუბიექტს უკვე აქვს მოცემული ინფორმაცია (მუხლი 14.5(a)), მე-14 მუხლის მე-5 პუნქტი შემდეგ გამონაკლისებს ითვალისწინებს:

- მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდება შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ/გაუმართლებელ ძალისხმევასთან, კერძოდ, საჯარო ინტერესის ფარგლებში მონაცემთა არქივირების, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებით დამუშავების შემთხვევაში, ან იმ შემთხვევებში, როცა მე-14 მუხლის პირველ პუნქტით განსაზღვრული ვალდებულების შესრულება შეუძლებელია ან მნიშვნელოვნად დააზიანებს მონაცემთა დამუშავების მიზნების მიღწევას;
- მონაცემთა შეგროვება ან გაცემა გათვალისწინებულია ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით, რომელიც ვრცელდება დამუშავებისთვის პასუხისმგებელ პირზე და განსაზღვრავს მონაცემთა სუბიექტის კანონიერი ინტერესების დაცვის სათანადო ზომებს; ან
- მონაცემთა კონფიდენციალობა უნდა იყოს დაცული ევროკავშირის ან წევრი სახელმწიფოს პროფესიული საიდუმლოების მარეგულირებელი სამართლებრივი ნორმების შესაბამისად, რაც ასევე მოიცავს კანონით გათვალისწინებულ ვალდებულებას საიდუმლოების დაცვის შესახებ.

„ინფორმაციის მიწოდება შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ/გაუმართლებელ ძალისხმევასთან“

58. 14.5(b) მუხლი 3 სხვადასხვა სიტუაციებს ითვალისწინებს, როდესაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი განთავისუფლებულია მე-14 მუხლის 1-ლი, მე-2 და მე-4 პუნქტებით დადგენილი ვალდებულებებისგან:

(i) მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდება შეუძლებელია (კერძოდ, დაარქივების, სამეცნიერო/ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის);
(ii) დაკავშირებულია არაპროპორციულად დიდ/გაუმართლებელ ძალისხმევასთან (კერძოდ, დაარქივების, სამეცნიერო/ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის);

(iii) როცა მე-14 მუხლის პირველ პუნქტით განსაზღვრული ვალდებულების შესრულება შეუძლებელია ან მნიშვნელოვნად დააზიანებს მონაცემთა დამუშავების მიზნების მიღწევას.

„შეუძლებელია“

59. 14.5(b) მუხლის თანახმად ინფორმაციის მიწოდების „შეუძლებლობა“ ასახავს სიტუაციას „ან ყველაფერი, ან არაფერი“ (all or nothing), რადგან რაღაც ან არის შეუძლებელი ან არ არის. არ არსებობს შეუძლებლობის დონეები. ამრიგად, თუ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი აპირებს, რომ ამ გამონაკლისს დაეყრდნოს, მან უნდა შეძლოს იმ ფაქტორების დემონსტრირება, რომლებიც რეალურად უშლის მას ხელს მცემული ინფორმაციის მონაცემთა სუბიექტისათვის მიწოდებაში. იმ შემთხვევაში, თუ გარკვეული პერიოდის შემდეგ, ფაქტორები, რომლებიც „შეუძლებლობას“ იწვევდა, აღარ იარსებებს და შესაძლებელი გახდება ამ ინფორმაციის მონაცემთა სუბიექტისათვის მიწოდება, მაშინ, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი დაუყოვნებლივ ასე უნდა მოიქცეს. პრაქტიკაში, იშვიათად შეძლებს დამუშავებისთვის პასუხისმგებელი პირი მოახდინოს იმის დემონსტრირება, რომ რეალურად შეუძლებელია ინფორმაციის მონაცემთა სუბიექტებისათვის მიწოდება. ქვემოთ წარმოდგენილი მაგალითი ადასტურებს ამას.

მაგალითი

მონაცემთა სუბიექტი რეგისტრირდება ონლაინ გამოწერის ფასიან სერვისზე, რომელიც მომსახურებისთვის თანხის გადახდას ითვალისწინებს ეტაპობრივად, მომსახურების მიღების შემდგომ. რეგისტრაციის შემდეგ, დამმუშავებელი აგროვებს მონაცემთა სუბიექტის საკრედიტო ისტორიის შესახებ მონაცემებს საკრედიტო საინფორმაციო ბიუროსგან, რათა გადაწყვიტოს, უზრუნველყოს მომსახურება. დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტს ინფორმაცია აღნიშნული მონაცემების შეგროვების შესახებ უნდა მიაწოდოს შეგროვებიდან სამი დღის ვადაში, 14.3(a) მუხლის შესაბამისად. ამავდროულად, მონაცემთა სუბიექტის მისამართი და ტელეფონის ნომერი არ არის საჯაროდ ხელმისაწვდომი (უფრო მეტიც, მონაცემთა სუბიექტი საზღვარგარეთ ცხოვრობს). მონაცემთა სუბიექტს არ დაუტოვებია ელ-ფოსტის მისამართი სერვისზე დარეგისტრირების დროს ან ელ-ფოსტის საშუალებით მიუწვდომელია. დამუშავებისთვის პასუხისმგებელი პირისთვის შეუძლებელია მონაცემთა სუბიექტთან პირდაპირ დაკავშირება. ამ შემთხვევაში, დამუშავებისთვის პასუხისმგებელმა პირმა ინფორმაცია საკრედიტო ისტორიის შესახებ მონაცემების შეგროვების თაობაზე საკუთარ ვებგვერდზე უნდა განათავსოს, ხოლო ამ ინფორმაციას მონაცემთა სუბიექტები დარეგისტრირებამდე

გაეცნობიან. შედეგად, მე-14 მუხლით გათვალისწინებული ინფორმაციის მიწოდება შეუძლებელი აღარ იქნება.

„შეუძლებელია მონაცემთა წყაროს შესახებ ინფორმაციის მიწოდება“

60. პრეამბულის 61-ე პუნქტის თანახმად, „თუკი რამდენიმე წყაროს არსებობის გამო შეუძლებელია მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდება პერსონალური მონაცემების წყაროს შესახებ, მან უნდა მიიღოს ზოგადი ინფორმაცია“. მონაცემთა სუბიექტებისათვის მათი პერსონალური მონაცემების წყაროს შესახებ ინფორმაციის მიწოდების მოთხოვნა არ მოქმედებს მხოლოდ იმ შემთხვევაში, თუ ეს შეუძლებელია იმის გამო, რომ ერთსა და იმავე მონაცემთა სუბიექტთან დაკავშირებული სხვადასხვა პერსონალური მონაცემები ვერ მიეწერება ერთ კონკრეტულ წყაროს. მაგალითად, მხოლოდ ის ფაქტი, რომ მონაცემთა ბაზა შედგება სხვადასხვა მონაცემთა სუბიექტის პერსონალური მონაცემებისგან, რომელიც მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმაშექმნა ერთზე მეტი წყაროს გამოყენებით, ვერ იქნება საკმარისი ამ მოთხოვნის გასაუქმებლად, თუ შესაძლებელია (თუმცა, შრომატევადია ან გარკვეულ ტვირთს აკისრებს დამუშავებისთვის პასუხისმგებელ პირს იმ წყაროს იდენტიფიცირება, საიდანაც მომდინარეობს ინდივიდუალური მონაცემთა სუბიექტების პერსონალური მონაცემები. თუ გავითვალისწინებთ მოთხოვნებს, რომლებიც ეხება მონაცემთა მეტად დაფარვის პრიორიტეტს, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას („Privacy by Design“) („Privacy by Default“),[54] გამჭვირვალობის მექანიზმები მონაცემთა დამუშავების სისტემებში უნდა დაინერგოს თავიდანვე, რათა შესაძლებელი იყოს ორგანიზაციაში მიღებული პერსონალური მონაცემების ყველა წყაროს იდენტიფიცირება და დაკავშირება თავიანთ წყაროსთან, მონაცემთა დამუშავების ცხოვრების ციკლის ნებისმიერ მომენტში (იხ. პუნქტი 43).

„არაპროპორციულად დიდი ძალისხმევა“

61. 14.5(b) მუხლი „შეუძლებელთან“ ერთად, აგრეთვე, ითვალისწინებს *„არაპროპორციულად დიდი ძალისხმევის“ პირობას, „კერძოდ, საჯარო ინტერესის ფარგლებში მონაცემთა არქივირების, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებით დამუშავების შემთხვევაში, იმ შემთხვევაში, რაც ექვემდებარება 81(1) მუხლით გათვალისწინებული მექანიზმებით დაცვას.“* 62-ე პუნქტი, აგრეთვე, მიუთითებს აღნიშნულ მიზნებზე, როგორც შემთხვევებზე, როდესაც მონაცემთა სუბიექტისათვის

[54] მუხლი 25

ინფორმაციის მიწოდება მოიცავს არაპროპორციულ ძალისხმევას და აცხადებს, რომ ამ დროს, უნდა გათვალისწინებულ იქნეს მონაცემთა სუბიექტების რაოდენობა, მონაცემების ხანდაზმულობა და დაცვის სათანადო გარანტიის არსებობა. ვინაიდან გამონაკლისის ჭრილში, პრეამბულის 62-ე პუნქტი და 14.5(b) მუხლი განსაკუთრებით ხაზს უსვამს მონაცემთა დამუშავებას არქივირების, კვლევის და სტატისტიკური მიზნებისთვის, WP29-ის პოზიცია მდგომარეობს იმაში, რომ აღნიშნული გამონაკლისი რუტინულად არ უნდა იქნას გამოყენებული მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ, რომლებიც პერსონალური მონაცემების დამუშავებას არ ახორციელებენ საჯარო ინტერესის ფარგლებში არქივირების, სამეცნიერო ან ისტორიული კვლევის მიზნებისთვის ან სტატისტიკური მიზნებისთვის. WP29 ხაზს უსვამს იმ ფაქტს, რომ იმ შემთხვევაში, თუ დამუშავება აღნიშნულ მიზნებს ემსახურება, 89.1 მუხლით დადგენილი პირობები მაინც უნდა შესრულდეს და ინფორმაციის მიწოდება უნდა მოიცავდეს არაპროპორციულად დიდ/გაუმართლებელ ძალისხმევას.

62. იმის განსაზღვრისას, თუ რა წარმოადგენს „შეუძლებლობას“ ან „არაპროპორციულად დიდ/გაუმართლებელ ძალისხმევას“ 14.5(b) მუხლის ჭრილში, მნიშვნელოვანია იმის გათვალისწინება, რომ მსგავს გამონაკლისებს არ შეიცავს მე-13 მუხლი (როდესაც მონაცემთა შეგროვება ხდება მონაცემთა სუბიექტისგან). ერთადერთი განსხვავება მე-13 და მე-14 მუხლით გათვალისწინებულ სიტუაციებს შორის არის ის, რომ მე-14 მუხლის შემთხვევაში, პერსონალური მონაცემების შეგროვება არ ხდება მონაცემთა სუბიექტისგან. შესაბამისად, „შეუძლებლობა“ და „არაპროპორციულად დიდი/გაუმართლებელი ძალისხმევა“, როგორც წესი, წარმოიშვება იმ გარემოებებში, რომელიც არა არის დაკავშირებული პერსონალური მონაცემების მონაცემთა სუბიექტისგან შეგროვებასთან. სხვა სიტყვებით რომ ვთქვათ, „შეუძლებლობა“ და „არაპროპორციულად დიდი/გაუმართლებელი ძალისხმევა“ პირდაპირ უნდა იყოს დაკავშირებული იმ ფაქტთან, რომ პერსონალური მონაცემების მოპოვების წყარო არ არის მონაცემთა სუბიექტი.

მაგალითი

ერთ-ერთ მსხვილ საავადმყოფოში პაციენტებს სტაციონალური და ამბულატორიული მკურნალობისთვის მოეთხოვებათ პაციენტთა საინფორმაციო ფორმის შევსება, რომელშიც ერთ-ერთი პუნქტი ითვალისწინებს ორი ახლო ნათესავის შესახებ ინფორმაციის მითითებას (მონაცემთა სუბიექტები). იმის გათვალისწინებით, რომ საავადმყოფოს ყოველდღიურად დიდი ოდენობით პაციენტები აკითხავენ, საავადმყოფოს მხრიდან არაპროპორციულად დიდ ძალისხმევასთანაა დაკავშირებული

ყველა იმ პირისათვის, რომლის შესახებ მონაცემებსაც პაციენტები ფორმაში უთითებენ, მე-14 მუხლით დადგენილი ინფორმაციის მიწოდება.

63. ფაქტორები, რომელზეც პრეამბულის 62-ე პუნქტი მიუთითებს (მონაცემთა სუბიექტების რაოდენობა, მონაცემების ხანდაზმულობა და დაცვის სათანადო გარანტიის არსებობა) შესაძლოა, მიუთითებდეს იმ საკითხებზე, რომელიც განაპირობებს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ არაპროპორციულად დიდი ძალისხმევის გამოყენებას იმისათვის, რომ მონაცემთა სუბიექტს მიაწოდოს მე-14 მუხლით დადგენილი ინფორმაცია.

მაგალითი

ისტორიის მკვლევარები ახორციელებენ კვლევას გენეოლოგიის სფეროში, გვარების საფუძველზე. ისინი ირიბად მოიპოვებენ 20,000 მონცემთა სუბიექტის შესახებ მონაცემთა ფართომასშტაბიან ნაკრებს. ამავდროულად, ამ მონაცემთა ნაკრების შეგროვება განხორციელდა 50 წლის წინ, მას შემდეგ იგი არ განახლებულა და არ შეიცავს რაიმე საკონტაქტო მონაცემებს. მონაცემთა ნაკრების მოცულობისა და მონაცემთა ხანდაზმულობის გათვალისწინებით, მკვლევარებს დასჭირდებათ არაპროპორციულად დიდი ძალისხმევის გაწევა, რათა ინდივიდუალურად მოახდინონ მონაცემთა სუბიექტებთან დაკავშირება, იმისათვის, რომ მათ მიაწოდონ მე-14 მუხლით გათვალისწინებული ინფორმაცია.

64. თუ მონაცემთა სუბიექტი აცხადებს, რომ იგი სარგებლობს 14.5(b) მუხლით გათვალისწინებული გამონაკლისით, ვინაიდან ინფორმაციის მიწოდება დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან, მან უნდა უზრუნველყოს ბალანსი და მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდებისთვის საჭირო ძალისხმევა შეადაროს იმას, თუ რა ზეგავლენა ექნება მონაცემთა სუბიექტზე ამ ინფორმაციის არ ქონას. აღნიშნული შედარება დამუშავებისთვის პასუხისმგებელი პირისმიერ დოკუმენტირებული უნდა იქნას, ანგარიშვალდებულების მოვალეობის შესაბამისად. ამ შემთხვევაში, 14.5(b) პუნქტი მიუთითებს, რომ დამუშავებისთვის პასუხისმგებელმა პირმა სათანადო ზომები უნდა მიიღოს, რათა დაიცვას მონაცემთა სუბიექტის უფლებები, თავისუფლებები და ლეგიტიმური ინტერესები. აღნიშნული ვრცელდება ისეთ შემთხვევებზე, როდესაც დამუშავებისთვის პასუხისმგებელი პირი დაადგენს, რომ ინფორმაციის მიწოდება შეუძლებელია, ან დამუშავების მიზნების მიღწევას სავარაუდოდ შეუძლებელს გახდის ან მნიშვნელოვნად შეაფერხებს. ერთ-ერთი მიზანშეწონილი ღონისძიება, 14.5(b) მუხლის თანახმად, არის ის, რომ დამუშავებისთვის პასუხისმგებელმა პირმაინფორმაცია ყოველთვის

საჯაროდ ხელმისაწვდომი უნდა გახადოს. დამმუშავებელს აღნიშნულის განხორციელება სხვადასხვანაირად შეუძლია, მაგალითად, თუ ინფორმაციას განათავსებს საკუთარ ვებგვერდზე, ან რეკლამის სახით პროაქტიულად გამოაქვეყნებს გაზეთში ან განათავსებს პოსტერებს თავის ტერიტორიაზე. ინფორმაციის საჯარო ხელმისაწვდომობის უზრუნველყოფის გარდა, სხვა შესაფერისი ზომები დამოკიდებული იქნება დამუშავების გარემოებებზე, თუმცა, შესაძლოა მოიცავდეს: მონაცემთა დაცვის ზეგავლენის შეფასების განხორციელებას; ფსევდონომიზაციის ტექნიკების გამოყენებას მონაცემების მიმართ; შეგროვებული მონაცემებისა და შენახვის პერიოდის მინიმუმამდე შემცირებას; ტექნიკური და ორგანიზაციული ღონისძიებების განხორციელებას, მაღალი დონის უსაფრთხოების უზრუნველყოფის მიზნით; ამას გარდა, შესაძლოა არსებობდეს სიტუაციები, როდესაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ამუშავებს პერსონალურ მონაცემებს, რომლებიც არ მოითხოვს მონაცემთა სუბიექტის იდენტიფიკაციას (მაგ., ფსევდონიმიზებული მონაცემების შემთხვევაში). ასეთ დროს, შესაძლოა, აგრეთვე, გავრცელდეს 11.1 მუხლი, რადგან ამ მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი არ არის ვალდებული შეინახოს, მოიპოვოს ან დაამუშაოს დამატებითი ინფორმაცია, რათა მოახდინოს მონაცემთა სუბიექტის იდენტიფიცირება, მხოლოდ და მხოლოდ GDPR-ის მოთხოვნებთან შესაბამისობის მიზნებისთვის.

„მნიშვნელოვნად დააზიანებს მიზნების მიღწევას“

65. ბოლო სიტუაცია, რომელსაც ითვალისწინებს 14.5(b) მუხლი, ეხება იმ შემთხვევას, როდესაც დამუშავებისთვის პასუხისმგებელი პირისმიერ ინფორმაციის მონაცემთა სუბიექტისათვის მიწოდება, 14.1 მუხლის თანახმად, სავარაუდოდ, შეუძლებელს გახდის ან მნიშვნელოვნად დააზიანებს დამუშავების მიზნების მიღწევას. ამ გამონაკლისით სარგებლობისთვის, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მოახდინოს დემონსტრირება იმისა, რომ 14.1 მუხლით გათვალისწინებული ინფორმაციის მიწოდება, ცალკე აღებული, მონაცემთა დამუშავების მიზნებს აუქმებს. აღსანიშნავია, რომ 14.4(b) მუხლის ამ ასპექტზე მითითება მოიაზრებს იმას, რომ დამუშავება აკმაყოფილებს მე-5 მუხლით დადგენილ ყველა პრინციპს და რაც ყველაზე მნიშვნელოვანია, ნებისმიერ გარემოებაში, პერსონალური მონაცემების დამუშავება არის სამართლიანი და აქვს სამართლებრივი საფუძველი.

მაგალითი

A ბანკი ვალდებულია, ფულის გათეთრებასთან ბრძოლის კანონმდებლობის თანახმად, განახორციელოს ყველა იმ საეჭვო ქმედების შესაბამისი სამართალდამცავი ორგანოებისათვის შეტყობინება, რომელიც დაკავშირებულია აღნიშნული ბანკში არსებულ ანგარიშებთან. A ბანკმა მიიღო

ინფორმაცია B ბანკისგან (სხვა წევრ-სახელმწიფოში), რომ ერთ-ერთმა ანგარიშის მფლობელმა მას მიმართა თხოვნით, A ბანკში თანხის გადარიცხვის შესახებ, ხოლო ეს გადარიცხვა გარკვეულ ეჭვებს წარმოშობდა. A ბანკმა ანგარიშის მფლობელის შესახებ აღნიშნული მონაცემები და ინფორმაცია საეჭვო აქტივობების შესახებ მიაწოდა შესაბამის სამართალდამცავ ორგანოებს. ფულის გათეთრებასთან ბრძოლის კანონმდებლობის თანახმად, სისხლის სამართლის დანაშაულს წარმოადგენს ბანკის მიერ ანგარიშის მფლობელის გაფრთხილება იმის თაობაზე, რომ იგი შესაძლოა დაექვემდებაროს მარეგულირებლის მიერ გამოძიებას. ამ შემთხვევაში, მოქმედებს 14.5(b) მუხლი, რადგან მონაცემთა სუბიექტის (A ბანკში ანგარიშის მფლობელი) მე-14 მუხლით გათვალისწინებული ინფორმაციის მიწოდება, B ბანკისგან მიღებული პერსონალური მონაცემების დამუშავების შესახებ, მნიშვნელოვან საფრთხეს შეუქმნის კანონმდებლობით დადგენილ მიზნებს, რაც მათ შორის, მოიცავს ანგარიშის მფლობელის გაფრთხილების პრევენციას. ამავდროულად, A ბანკში ანგარიშების ყველა მფლობელს ბანკმა უნდა მიაწოდოს ზოგადი ინფორმაცია ბანკში ანგარიშის გახსნის დროს, რომ მათი პერსონალური მონაცემები, შესაძლოა, დამუშავდეს ფულის გათეთრებასთან ბრძოლის მიზნებისთვის.

„მონაცემთა შეგროვება ან გაცემა ცალსახად არის დადგენილი კანონით“

66. 14.5(c) მუხლის თანახმად, 14.1, 14.2 და 14.4 მუხლებით გათვალისწინებული მოთხოვნები აღარ მოქმედებს, თუ პერსონალური მონაცემების შეგროვება ან გაცემა *„ცალსახად გათვალისწინებულია ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით, რომელიც ვრცელდება* დამუშავებისთვის პასუხისმგებელ პირებზე.“ თუმცა, ამ გამონაკლისით სარგებლობისთვის, აუცილებელია, რომ კანონი ითვალისწინებდეს *„დაცვის შესაფერის ზომებს, მონაცემთა სუბიექტის ლეგიტიმური ინტერესების დასაცავად.“* ეს კანონი პირდაპირ უნდა ეხებოდეს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს და მონაცემთა შეგროვება ან გაცემა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისთვის სავალდებულო უნდა იყოს. შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს უნდა შეეძლოს დემონსტრირება, რომ მოცემული კანონი ვრცელდება მასზე და კანონის თანახმად იგი ვალდებულია, შეაგროვოს ან გასცეს მოცემული პერსონალური მონაცემები. ევროკავშირზე ან წევრ სახელმწიფოზეა დამოკიდებული, კანონის ფორმულირება მოახდინოს იმგვარად, რომ იგი ითვალისწინებდეს *„შესაფერის ზომებს, მონაცემთა სუბიექტის ლეგიტიმური ინტერესების დასაცავად“*; თუმცა, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს (და შეძლოს დემონსტრირება), რომ მის მიერ პერსონალური მონაცემების შეგროვება და გაცემა ამ ზომებთან შესაბამისობაშია. ამას გარდა, დამუშავებისთვის პასუხისმგებელმა პირმა

მონაცემთა სუბიექტს მკაფიოდ უნდა განუმარტოს, რომ იგი პერსონალური მონაცემების შეგროვებას და გაცემას ახორციელებს მოცემული კანონის შესაბამისად, გარდა იმ შემთხვევისა, თუ მოქმედებს სამართლებრივი აკრძალვა, რომელიც მონაცემთა სუბიექტს აღნიშნულის შესაძლებლობას უზღუდავს. GDPR-ის პრეამბულის 41-ე პუნქტის ეს სტრიქონი, რომლის თანახმადაც სამართლებრივი საფუძველი ან საკანონმდებლო ზომა უნდა იყოს მკაფიო და ზუსტი, ხოლო მისი გამოყენება განჭვრეტადი უნდა იყოს იმ პირებისთვის, ვის მიმართაც ეს ზომა გამოიყენება, მართლმსაჯულების ევროპული სასამართლოს და ადამიანის უფლებათა ევროპული სასამართლოს პრეცედენტული სამართლის შესაბამისად. ამავდროულად, 14.5(c) მუხლი არ მოქმედებს, თუ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემები *პირდაპირ მონაცემთა სუბიექტისგან* მოიპოვოს, რა დროსაც გამოიყენება მე-13 მუხლი. ამ შემთხვევაში, GDPR-ით დაშვებული ერთადერთი გამონაკლისი, რომელიც დამუშავებისთვის პასუხისმგებელ პირს ათავისუფლებს მონაცემთა სუბიექტის ინფორმაციით უზრუნველყოფის ვალდებულებისგან, არის 13.4 მუხლით გათვალისწინებული გამონაკლისი (ე.ი., იმ შემთხვევაში და იმდენად, რამდენადაც მონაცემთა სუბიექტს უკვე აქვს ეს ინფორმაცია). ამავდროულად, როგორც 68-ე პუნქტშია მითითებული, ეროვნულ დონეზე, წევრ სახელმწიფოებს, 23-ე მუხლის თანახმად, გააჩნიათ უფლებამოსილება, კანონმდებლობით დაადგინონ სპეციფიური შეზღუდვები გამჭვირვალობის უფლებაზე, მე-12 მუხლის შესაბამისად და ინფორმაციის მიღების უფლებაზე, მე-13 და მე-14 მუხლების შესაბამისად.

მაგალითი

საგადასახადო ორგანო ეროვნული კანონმდებლობის თანახმად ვალდებულია, დამსაქმებლებისგან მოიპოვოს დასაქმებულთა ხელფასების შესახებ დეტალური მონაცემები. პერსონალური მონაცემების მოპოვება არ ხდება მონაცემთა სუბიექტებისგან. შესაბამისად, საგადასახადო ორგანო ექვემდებარება მე-14 მუხლის მოთხოვნებს. ვინაიდან საგადასახადო ორგანოს მიერ დამსაქმებლებისგან დასაქმებულების პერსონალური მონაცემების მოპოვება კანონით ცალსახად არის გათვალისწინებული, მე-14 მუხლით გათვალისწინებული მოთხოვნები ინფორმაციის მიწოდებასთან დაკავშირებით, ამ შემთხვევაში, არ ვრცელდება საგადასახადო ორგანოზე.

„კონფიდენციალურობა, რომელიც საიდუმლოების დაცვის ვალდებულებიდან მომდინარეობს“

67. 14.5(d) მუხლი ითვალისწინებს გამონაკლისს მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდების მოთხოვნასთან დაკავშირებით, იმ შემთხვევაში, თუ

„მონაცემთა კონფიდენციალობა უნდა იყოს დაცული ევროკავშირის ან წევრი სახელმწიფოს პროფესიული საიდუმლოების მარეგულირებელი სამართლებრივი ნორმების შესაბამისად, რაც ასევე მოიცავს კანონით გათვალისწინებულ ვალდებულებას საიდუმლოების დაცვის შესახებ.“ თუ დამუშავებისთვის პასუხისმგებელ პირს სურს, რომ ამ გამონაკლისით ისარგებლოს, მან უნდა შეძლოს დემონსტრირება იმისა, რომ სათანადოდ მოახდინა გამონაკლისის იდენტიფიცირება და უნდა დაასაბუთოს, თუ რომ დამუშავებისთვის პასუხისმგებელი პირი ექვემდებარება პროფესიული საიდუმლოების დაცვის ვალდებულებას და ამ ვალდებულების თანახმად აკრძალული აქვს მონაცემთა სუბიექტისათვის 14.1, 14.2 და 14.4 მუხლებით გათვალისწინებული ინფორმაციის მიწოდება.

მაგალითი

სამედიცინო სფეროში მომუშავე პრაქტიკოსს (მონაცემთადამუშავებისთვის პასუხისმგებელი პირი ეკისრება პროფესიული საიდუმლოების დაცვის ვალდებულება პაციენტთა სამედიცინო ინფორმაციასთან მიმართებით. პაციენტი (ვისთან მიმართებითაც მოქმედებს პროფესიული საიდუმლოების დაცვის ვალდებულება) პრაქტიკოსს აწვდის ინფორმაციას საკუთარი ჯანმრთელობის შესახებ, გენეტიკურ დაავადებასთან დაკავშირებით, რომელიც, აგრეთვე, აღენიშნება მის რამდენიმე ახლო ნათესავს. პაციენტი პრაქტიკოსს, აგრეთვე, აწვდის გარკვეულ პერსონალურ მონაცემებს მისი ნათესავების (მონაცემთა სუბიექტების) შესახებ, რომელთაც იგივე დაავადება აღენიშნებათ. პრაქტიკოსს არ მოეთხოვება აღნიშნული ნათესავებისათვის მე-14 მუხლით გათვალისწინებული ინფორმაციის მიწოდება, ვინაიდან ამ შემთხვევაში, მოქმედებს 14.5(d) მუხლით გათვალისწინებული გამონაკლისი. თუ სამედიცინო პრაქტიკოსი ნათესავებს მიაწვდის მე-14 მუხლით გათვალისწინებულ ინფორმაციას, დაირღვევა პროფესიული საიდუმლოს დაცვის ვალდებულება, რომელიც მოქმედებს პაციენტის მიმართ.

შეზღუდვები მონაცემთა სუბიექტის უფლებებზე

68. 23-ე მუხლის თანახმად, შესაძლებელია, რომ მონაცემთა სუბიექტის უფლებები გამჭვირვალობასთან დაკავშირებით და მონაცემთა სუბიექტის მატერიალური უფლებები დამატებით შეიზღუდოს წევრი სახელმწიფოების (ან ევროკავშირის)

მიერ მიღებული კანონმდებლობით,[55] იმ შემთხვევაში, თუ შესაბამისი ზომები პატივს სცემს ფუნდამენტური უფლებებისა და თავისუფლებების არსს და აუცილებელია და პროპორციულია 23.1 მუხლის (a)-(j) ქვეპუნქტებით დადგენილი ერთი ან რამდენიმე ინტერესის დასაცავად. თუ ეროვნულ დონეზე მოქმედი ამგვარი ზომები აკნინებს მონაცემთა სუბიექტის კონკრეტულ უფლებებს ან ზოგადად, გამჭვირვალობასთან დაკავშირებულ ვალდებულებებს, რომელთა დაცვაც სხვა შემთხვევაში, GDPR-ის თანახმად სავალდებულო იქნებოდა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისთვის, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეძლოს დემონსტრირება იმისა, თუ როგორ ვრცელდება მასზე ეროვნულ დონეზე მოქმედი დებულება. 23.2(h) მუხლის თანახმად, საკანონმდებლო ზომა უნდა შეიცავდეს დებულებას, რომელიც ადგენს მონაცემთა სუბიექტის უფლებას, იყოს ინფორმირებული მის უფლებებზე დაწესებული შეზღუდვის შესახებ, გარდა იმ შემთხვევისა, თუ მონაცემთა სუბიექტის ინფორმირება ზიანს მიაყენებს შეზღუდვის მიზანს. აღნიშნულის შესაბამისად და სამართლიანობის პრინციპის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა, აგრეთვე, უნდა მოახდინოს მონაცემთა სუბიექტების ინფორმირება მასზედ, რომ იგი იყენებს (ან გამოიყენებს, თუ მონაცემთა სუბიექტი განახორციელებს შესაბამის უფლებას) მონაცემთა სუბიექტის უფლებების განხორციელებასთან ან გამჭვირვალობის ვალდებულებასთან დაკავშირებით კანონმდებლობით გათვალისწინებულ შეზღუდვას, გარდა იმ შემთხვევისა, თუ აღნიშნული [ინფორმირება] ზიანს მიაყენებს საკანონმდებლო შეზღუდვის არსს. როგორც ასეთი, გამჭვირვალობა მოითხოვს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ წინასწარ ადეკვატური ინფორმაციის მიწოდებას მონაცემთა სუბიექტებისთვის, მათი უფლებებისა და ამ უფლებებთან დაკავშირებული კონკრეტული გამონაკლისების შესახებ, რომელიც შესაძლოა გამოიყენოს დამუშავებისთვის პასუხისმგებელმა პირმა, რათა მონაცემთა სუბიექტისათვის მოულოდნელი არ იყოს კონკრეტული უფლების სავარაუდო შეზღუდვა მაშინ, როდესაც ისინი მოგვიანებით შეეცდებიან ამ უფლების დამუშავებისთვის პასუხისმგებელი პირის წინააღმდეგ განხორციელებას. რაც შეეხება ფსევდონიმიზაციას და მონაცემთა მინიმიზაციას და იმდენად, რამდენადაც დამუშავებისთვის პასუხისმგებელმა პირებმა შესაძლოა მიმართონ GDPR-ის მე-11 მუხლს, WP29-მ თავის დასკვნაში 3/2017[56] დაადასტურა, რომ GDPR-ის მე-11 მუხლი განმარტებული უნდა იქნას იმგვარად, რაც განამტკიცებს მონაცემთა რეალურ მინიმიზაციას ისე, რომ ამან ხელი არ შეუშალოს მონაცემთა

[55] მე-12-22-ე მუხლების და 34-ე მუხლის შესაბამისად და აგრეთვე, მე-5 მუხლის თანახმად, იმ შემთხვევაში, თუ კანონმდებლობა შეიცავს დებულებებს, რომლებიც შეესაბამება მე-12 და 22-ე მუხლებით გათვალისწინებულ უფლებებს და ვალდებულებებს.

[56] დასკვნა 03/2017 პერსონალური მონაცემების დამუშავების შესახებ, თანამშრომლობითი ინტელექტუალური ტრანსპორტირების სისტემების კონტექსტში (C-ITS) - იხ. პუნქტი 4.2

სუბიექტის უფლებების განხორციელებას, ხოლო მონაცემთა სუბიექტის უფლებების განხორციელება შესაძლებელი უნდა იყოს დამატებითი ინფორმაციის დახმარებით, რომელსაც წარმოადგენს მონაცემთა სუბიექტი.

69. ამას გარდა, 85-ე მუხლი წევრ სახელმწიფოებს ავალდებულებს, კანონმდებლობის საფუძველზე, უზრუნველყონ მონაცემთა დაცვის დაბალანსება გამოხატვისა და ინფორმაციის თავისუფლებასთან. აღნიშნული, სხვა საკითხებთან ერთად, მოითხოვს, რომ წევრმა სახელმწიფოებმა უზრუნველყონ გამონაკლისები ან გადახვევის შესაძლებლობა GDPR-ის გარკვეული მუხლებიდან (მათ შორის, 12-14 მუხლებით გათვალისწინებული გამჭვირვალობის ვალდებულებებისგან), როდესაც დამუშავება ხორციელდება ჟურნალისტური, აკადემიური, არტისტული ან ლიტერატურული გამოხატვის მიზნებისთვის, თუ ისინი [გამონაკლისები და გადახვევის შესაძლებლობები] საჭიროა ამ ორი უფლების დასაბალანსებლად.

გამჭვირვალობა და მონაცემთა უსაფრთხოების დარღვევა

70. WP29-მ ცალკე სახელმძღვანელო პრინციპები შეიმუშავა მონაცემთა უსაფრთხოების დარღვევის შესახებ[57], თუმცა, წინამდებარე სახელმძღვანელო პრინციპების მიზნებისთვის, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებები მონაცემთა უსაფრთხოების დარღვევის შემთხვევებზე მონაცემთა სუბიექტის ინფორმირებასთან დაკავშირებით სრულად უნდა ითვალისწინებდეს მე-12 მუხლით დადგენილ მოთხოვნებს გამჭვირვალობის შესახებ.[58] მონაცემთა დარღვევის შემთხვევების შესახებ მონაცემთა სუბიექტის ინფორმირება უნდა აკმაყოფილებდეს იმავე მოთხოვნებს, რომლებიც ზემოთ არის აღწერილი (კერძოდ, მკაფიო და მარტივი ენის გამოყენების შესახებ) და რომლებიც ვრცელდება მონაცემთა სუბიექტთან ნებისმიერი სხვა სახის კომუნიკაციაზე მათი უფლებების შესახებ ან მე-13 და მე-14 მუხლის თანახმად ინფორმაციის მიწოდებასთან დაკავშირებით.

[57] სახელმძღვანელო პრინციპები პერსონალური მონაცემების დარღვევის შესახებ შეტყობინების თაობაზე, 2016/679 რეგულაციის თანახმად, WP 250

[58] აღნიშნული ნათელია 12.1 მუხლის თანახმად, რომელიც კონკრეტულად მიუთითებს „მონაცემთა სუბიექტთან მე-15-22-ე მუხლებითა **<u>და 34-ე მუხლით</u>** განსაზღვრულ კომუნიკაციაზე მონაცემთა დამუშავებასთან დაკავშირებით [ხაზგასმა დამატებულია].

დანართი

ინფორმაცია, რომელიც მონაცემთა სუბიექტს უნდა მიაწოდოს დამუშავებისთვის პასუხისმგებელმა პირმა მე-13 და მე-14 მუხლების თანახმად

საჭირო ინფორმაციის ტიპი	**მუხლი (თუ პერსონალური მონაცემების შეგროვება ხდება პირდაპირ მონაცემთა სუბიექტისგან)**	**მუხლი (თუ პერსონალური მონაცემების შეგროვება არ ხდება მონაცემთა სუბიექტისგან)**	**WP-29-ის კომენტარები ინფორმაციის მიწოდების მოთხოვნასთან დაკავშირებით**
დამუშავებისთვის პასუხისმგებელი პირის და მისი წარმომადგენლის (ასეთის არსებობის შემთხვევაში) ვინაობა და საკონტაქტო ინფორმაცია[59]	მუხლი 13.1(a)	მუხლი 14.1(a)	ეს ინფორმაცია უნდა იძლეოდეს დამუშავებისთვის პასუხისმგებელი პირის ადვილად იდენტიფიცირების შესაძლებლობას და სასურველია, რომ ითვალისწინებდეს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთან კომუნიკაციის სხვადასხვა ფორმებს (მაგ., ტელეფონის ნომერი, ელ-ფოსტა, საფოსტო მისამართი და ა.შ.).

[59] განმარტებულია GDPR-ის 4.17-ე მუხლში (და მითითებულია პრეამბულის მე-80 პუნქტში); 'წარმომადგენელი' ნიშნავს ევროკავშირში დაფუძნებულ ფიზიკურ ან იურიდიულ პირს, რომელიც დანიშნულია დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ წერილობითი დოკუმენტის საფუძველზე, 27-ე მუხლის შესაბამისად და რომელიც წარმოადგენს დამმუშავებელს ან უფლებამოსილ პირს ამ რეგულაციით განსაზღვრული ვალდებულებების შესრულებისას. ეს ვალდებულება მოქმედებს, როდესაც 3.2 მუხლის შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი ან დამუშავებაზე უფლებამოსილი პირი არ არის დაფუძნებული ევროკავშირში, მაგრამ ამუშავებს იმ მონაცემთა სუბიექტების პერსონალურ მონაცემებს, რომლებიც ევროკავშირში არიან, ხოლო დამუშავება დაკავშირებულია საქონლის ან სერვისების შეთავაზებასთან, ან ევროკავშირში მონაცემთა სუბიექტების ქცევის მონიტორინგთან.

პერსონალურ მონაცემთა დაცვის ოფიცრის (ასეთის არსებობის შემთხვევაში) საკონტაქტო ინფორმაცია	მუხლი 13.1(b)	მუხლი 14.1(b)	იხ. WP29 სახელმძღვანელო პრინციპები მონაცემთა დაცვის ოფიცრების შესახებ[60]
მონაცემთა დამუშავების მიზნები და სამართლებრივი საფუძველი	მუხლი 13.1(c)	მუხლი 14.1(c)	უნდა მიეთითოს არა მხოლოდ დამუშავების მიზნები, არამედ, შესაბამისი სამართლებრივი საფუძველი, მე-6 მუხლის თანახმად. პერსონალური მონაცემების სპეციალური კატეგორიების შემთხვევაში, უნდა მიეთითოს მე-9 მუხლის შესაბამისი პუნქტი (და საჭიროების შემთხვევაში, ევროკავშირის ან წევრი სახელმწიფოს შესაბამისი კანონმდებლობა, რომლის საფუძველზეც ხდება მონაცემების დამუშავება). თუ დამუშავება ხდება მე-10 მუხლის შესაბამისად, კერძოდ, პერსონალური მონაცემები ეხება ნასამართლობას და დანაშაულებს ან შესაბამის უსაფრთხოების ზომებს, 6.1 მუხლის თანახმად, უნდა მიეთითოს ევროკავშირის ან წევრი სახელმწიფოს კანონი, რომლის საფუძველზეც ხორციელდება დამუშავება.
თუ მონაცემები მუშავდება მე-6 მუხლის, პირველი პუნქტის, „ვ“ ქვეპუნქტის შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირის ან მესამე პირის	მუხლი 13.1(d)	მუხლი 14.2(b)	საჭიროა კონკრეტული ინტერესის იდენტიფიცირება, მონაცემთა სუბიექტის სასარგებლოდ. საუკეთესო პრაქტიკის მიხედვით, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს, ასევე, უნდა მიაწოდოს ინფორმაცია *დაბალანსების ტესტიდან,*

[60] Guidlines on Data Protection Officers, WP243 rev.01, ბოლო გადახედვისა და მიღების თარიღი: 2017 წლის 5 აპრილი.

მიერ განსაზღვრული კანონიერი ინტერესების შესახებ			რომელიც უნდა განხორციელდეს იმისათვის, რომ დამუშავებისთვის პასუხისმგებელმა პირმაშეძლოს, გამოიყენოს 6.1(f) მუხლი, როგორც დამუშავების კანონიერი საფუძველი, მონაცემთა სუბიექტის პერსონალური მონაცემების შეგროვებამდე. ინფორმაციული გადაღლის თავიდან ასაცილებლად, აღნიშნულის გათვალისწინება შესაძლებელია კონფიდენციალობის მრავალშრიან განაცხადში / შეტყობინებაში (იხ. პ.35). ნებისმიერ შემთხვევაში, WP29-ის პოზიცია მდგომარეობს იმაში, რომ მონაცემთა სუბიექტისათვის მიწოდებული ინფორმაცია ნათელს უნდა ხდიდეს, რომ მას შეუძლია დაბალანსების ტესტის შესახებ ინფორმაციის მოპოვება, მოთხოვნის საფუძველზე. ეს აუცილებელია ეფექტური გამჭვირვალობისთვის, თუ მონაცემთა სუბიექტებს აქვთ ეჭვი იმასთან დაკავშირებით, ჩატარდა თუ არა დაბალანსების ტესტი სამართლიანად ან სურთ საჩივრის შეტანა საზედამხედველო ორგანოში.
შესაბამისი პერსონალური მონაცემების კატეგორიები	არ მოითხოვება	მუხლი 14.1(d)	ეს ინფორმაცია საჭიროა მე-14 მუხლით გათვალისწინებულ შემთხვევაში, რადგან პერსონალური მონაცემების მოპოვება არ მომხდარა მონაცემთა სუბიექტისგან. შესაბამისად, იგი არ არის ინფორმირებული, თუ რა კატეგორიების პერსონალური მონაცემები მოიპოვა დამუშავებისთვის პასუხისმგებელმა პირმა.

პერსონალური მონაცემების მიმღები[61] (ან მიმღებთა კატეგორიები)	მუხლი 13.1(e)	მუხლი 14.1(e)	ტერმინი „მიმღები“ განმარტებულია 4.9 მუხლში: „ფიზიკურ ან იურიდიულ პირს, საჯარო უწყებას, დაწესებულებას ან სხვა უწყებას, რომელსაც გადაეცემა პერსონალური მონაცემები ***მიუხედავად იმისა, წარმოადგენს თუ არა ის მესამე მხარეს.***“ [ხაზგასმა დამატებულია]. როგორც ასეთი, არ არის აუცილებელი, რომ მიმღები იყოს მესამე მხარე. შესაბამისად, ტერმინი „მიმღები“ მოიცავს დამუშავებისთვის პასუხისმგებელ პირებსერთობლივ დამუშავებისთვის პასუხისმგებელ პირებს და უფლებამოსილ პირებს, ვისაც გადაეცემა ან მიეწოდება მონაცემები, ხოლო დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტს მიაწოდოს ასეთი მიმღებების შესახებ ინფორმაცია, მესამე მხარების შესახებ ინფორმაციაზე დამატებით. დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს უნდა მიაწოდოს რეალური (კონკრეტული) მიმღებების ან მიმღებთა კატეგორიების შესახებ ინფორმაცია. სამართლიანობის პრინციპის შესაბამისად, დამმუშავებლებმა მონაცემთა სუბიექტს უნდა მიაწოდონ მნიშვნელოვანი მიმღებების შესახებ ინფორმაცია. პრაქტიკაში,

[61] განმარტებულია GDPR-ის 4.9-ე მუხლში და მითითებულია პრეამბულის 31-ე პუნქტში.

			ეს ნიშნავს კონკრეტულ მიმღებებს, რათა მონაცემთა სუბიექტმა ზუსტად იცოდეს, თუ ვის აქვს მისი პერსონალური მონაცემები. თუ დამუშავებისთვის პასუხისმგებელი პირი სგადაწყვეტს, მონაცემთა სუბიექტს მიაწოდოს ინფორმაცია მიმღებთა კატეგორიების შესახებ, ინფორმაცია უნდა იყოს მაქსიმალურად კონკრეტული და უნდა მიეთითოს მიმღების ტიპი (ე.ი., მიეთითოს აქტივობები, რომელსაც იგი ახორციელებს), შესაბამისი ინდუსტრია, სექტორი და ქვე-სექტორი და მიმღების ადგილმდებარეობა.
მესამე ქვეყნებისთვის გადაცემის დეტალები, გადაცემის ფაქტი და მონაცემთა დაცვის შესაბამისი გარანტიების დეტალები[62] (მათ შორის, კომისიის შესაბამისობის გადაწყვეტილების არსებობა ან არ არსებობა[63]) და ინფორმაცია, მონაცემების ასლის მოპოვების გზებისა და მათი განთავსების წყაროს შესახებ	მუხლი 13.1(f)	მუხლი 14.1(f)	უნდა მიეთითოს GDPR-ის შესაბამისი მუხლი, რომელიც ითვალისწინებს ამგვარ გადაცემას და შესაბამის მექანიზმს (მაგ., შესაბამისობის გადაწყვეტილება 45-ე მუხლის თანახმად / სავალდებულო ძალის მქონე კორპორატიული წესები 47-ე მუხლის თანახმად / მონაცემთა დაცვის სტანდარტული დებულებები 46.2 მუხლის თანახმად / გამონაკლისები და დაცვის საშუალებები 49-ე მუხლის თანახმად და ა.შ.). ასევე, უნდა მიეთითოს ინფორმაცია, თუ სად და როგორ არის შესაბამისი დოკუმენტის მიღება შესაძლებელი - მაგ., გამოყენებული მექანიზმის ბმულის მიწოდება. სამართლიანობის პრინციპის თანახმად, მესამე ქვეყნისათვის

[62] 46.2 და 46.3 მუხლების შესაბამისად.

[63] 45-ე მუხლის შესაბამისად.

			მონაცემთა გადაცემის შესახებ ინფორმაცია უნდა იყოს მაქსიმალურად მნიშვნელოვანი მონაცემთა სუბიექტისთვის; ეს, როგორც წესი, ნიშნავს, რომ მესამე ქვეყნები უნდა მიეთითოს.
მონაცემთა შენახვის ვადა, ან თუ ვადის განსაზღვრა შეუძლებელია, მონაცემთა შენახვის ვადის განსაზღვრის კრიტერიუმები	მუხლი 13.2(a)	მუხლი 14.2(a)	ეს დაკავშირებულია მონაცემთა მინიმიზაციის მოთხოვნასთან, 5.1(c) მუხლის შესაბამისად და შენახვაზე დაწესებულ შეზღუდვასთან, 5.1(e) მუხლის შესაბამისად. შენახვის პერიოდი (ან კრიტერიუმები მის დასადგენად), შესაძლოა, განისაზღვროს ისეთი ფაქტორებით, როგორიცაა, სკაანონმდებლო მოთხოვნები ან ინდუსტრიაში მოქმედი გაიდლაინები, თუმცა, ფორმულირებული უნდა იყოს იმგვარად, რომ მონაცემთა სუბიექტს ჰქონდეს შესაძლებლობა, საკუთარი მდგომარეობის საფუძველზე, შეაფასოს, თუ რა იქნება შეფასების ვადა, კონკრეტული მონაცემების/მიზნების გათვალისწინებით. არ არის საკმარისი, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა ზოგადად მიუთითოს, რომ პერსონალური მონაცემების შენახვა მოხდება საჭირო ვადით, დამუშავების ლეგიტიმური მიზნებისთვის. თუ საჭიროა, შენახვის სხვადასხვა პერიოდები უნდა დადგინდეს პერსონალური მონაცემების სხვადასხვა კატეგორიებისათვის და/ან დამუშავების სხვადასხვა მიზნებისთვის, მათ შორის, თუ საჭიროა, დაარქივების პერიოდები.

მონაცემთა სუბიექტის უფლება, მოითხოვოს: • მონაცემებზე წვდომა • მონაცემების გასწორება • წაშლა • დაბლოკვა • დამუშავების შეწყვეტა • მონაცემთა გადატანა.	მუხლი 13.2(b)	მუხლი 14.2(c)	ეს ინფორმაცია უნდა იყოს დამუშავების გარემოებების შესაბამისი და მოიცავდეს მოკლე ინფორმაციას იმის შესახებ, თუ რას ითვალისწინებს უფლება, მონაცემთა სუბიექტს რა ნაბიჯების გადადგმა შეუძლია მის განსახორციელებლად და რა შეზღუდვები მოქმედებს უფლებასთან დაკავშირებით (იხ. პ.68). კერძოდ, დამუშავების შეწყვეტის მოთხოვნის უფლება ცალსახად უნდა განემარტოს მონაცემთა სუბიექტს, როგორც მინიმუმ, პირველი კომუნიკაციის დროს და მკაფიოდ უნდა წარედგინოს მას, ნებისმიერი სხვა ინფორმაციისგან განცალკევებით.[64] რაც შეეხება გადატანის უფლებას, იხ. WP29-ის სახელმძღვანელო პრინციპები მონაცემთა გადატანის უფლებაზე.[65]
თუ დამუშავება ეფუძნება თანხმობას (ან ცალსახა თანხმობას), თანხმობის ნებისმიერ დროს უკან გახმობის უფლება	მუხლი 13.2(c)	მუხლი 14.2(d)	ეს ინფორმაცია უნდა მოიცავდეს თანხმობის უკან გახმობის გზას, იმის გათვალისწინებით, რომ მონაცემთა სუბიექტისათვის თანხმობის უკან გახმობა უნდა იყოს ისეთივე ადვილი, როგორც მისი მიცემა.[66]
საზედამხედველო ორგანოში საჩივრის წარდგენის უფლება	მუხლი 13.2(d)	მუხლი 14.2(e)	ეს ინფორმაცია უნდა განმარტავდეს, რომ 77-ე მუხლის თანახმად, მონაცემთა სუბიექტს უფლება აქვს, საზედამხედველო ორგანოს მიმართოს საჩივრით, კერძოდ, წევრ სახელმწიფოში ან მის საცხოვრებელ ადგილას, სამუშაო ადგილას ან GDPR-ის სავარაუდო დარღვევის ადგილას.

[64] მუხლი 21.4 და პრეამბულის პუნქტი 70 (რომელიც ვრცელდება პირდაპირი მარკეტინგის შემთხვევებზე).

[65] სახელმძღვანელო პრინციპები მონაცემთა პორტატულობის შესახებ, WP 242 rev.01, ბოლო გადახედვის და მიღების თარიღ: 2017 წლის 5 აპრილი.

[66] მუხლი 7.3

მონაცემთა სუბიექტისგან მის შესახებ მონაცემების მოთხოვნა წარმოადგენს კანონისმიერ თუ სახელშეკრულებო მოთხოვნას, ან ხელშეკრულების დასადებად აუცილებელ პირობას, აგრეთვე მონაცემთა სუბიექტისთვის სავალდებულოა თუ ნებაყოფლობითი მონაცემთა მიწოდება და ინფორმაციის მიწოდებაზე უარის თქმის მოსალოდნელი შედეგები	მუხლი 13.2(e)	არ მოითხოვება	მაგალითად, დასაქმების კონტექსტში, შესაძლოა, კონტრაქტით იყოს გათვალისწინებული გარკვეული ინფორმაციის მიწოდება ამჟამინდელი ან სამომავლო დამსაქმებლისთვის. ონლაინ ფორმებში მკაფიოდ უნდა იყოს მითითებული, თუ რომელი ველის შევსებაა სავალდებულო, რომლის არა და რა შედეგებს გამოიწვევს სავალდებულო ველის არ შევსება.
მონაცემთა შეგროვების წყარო და ასეთის არსებობის შემთხვევაში , მითითება რომ აღნიშნული წარმოადგენს საჯაროდ ხელმისაწვდომ წყაროს	არ მოითხოვება	მუხლი 14.2(f)	წარმოდგენილი უნდა იქნას მონაცემთა კონკრეტული წყარო, გარდა იმ შემთხვევისა, თუ ეს შეუძლებელია - იხ. დამატებითი ინფორმაცია, მე-60 პუნქტში. თუ კონკრეტული წყარო არ არის დასახელებული, მაშინ წარმოდგენილი ინფორმაცია უნდა მოიცავდეს: წყაროების ხასიათს (ე.ი., საჯარო/კერძო) და ორგანიზაციის/ინდუსტრიის/სექტორის ტიპს.
გადაწყვეტილების ავტომატიზებულად მიღების, მათ შორის, „პროფილირების“, და საჭიროების შემთხვევაში, მნიშვნელოვანი/არსებითი ინფორმაცია გამოყენებული	მუხლი 13.2(f)	მუხლი 14.2(g)	იხ. WP29-ის საახელმძღვანელო პრინციპები ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღების ან პროფილირების შესახებ.[67]

[67] სახელმძღვანელო პრინციპები 2016/679 რეგულაციის მიზნებისთვის, ავტომატიზებული ინდივიდუალური გადაწყვეტილების მიღების და პროფილირების შესახებ, WP 251

ლოგიკის/კრიტერიუმების, საჭიროების და მონაცემთა სუბიექტისთვის შესაძლო შედეგების შესახებ			