სახელმძღვანელო რეკომენდაცია **05/2020** თანხმობის შესახებ, **2016/679** რეგულაციის მიხედვით

ვერსია 1.1

მიღებულია: 2020 წლის 4 მაისს

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

ვერსიების შესახებ

ვერსია 1.1	2020 წლის 13 მაისი	ფორმატთან დაკავშირებული შესწორებები
ვერსია 1.0	2020 წლის 4 მაისი	სახელმძღვანელო პრინციპების მიღება

სარჩევი

ევროპის მონაცემთა დაცვის საბჭო,

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

ითვალისწინებს რა ევროპის ეკონომიკური ზონის შესახებ (EEA) შეთანხმებას, კერძოდ, მის XI დანართსა და 37-ე პროტოკოლს, რომელიც შესწორებულია EEA ერთობლივი კომიტეტის 2018 წლის 6 ივლისის N154/2018 გადაწყვეტილებით;[1]

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

ითვალისწინებს რა, 29-ე მუხლის სამუშაო ჯგუფის სახელმძღვანელო პრინციპებს თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით, WP259 rev.01,

ამტკიცებს ქვემოთ წარმოდგენილ სახელმძღვანელო პრინციპებს

წინასიტყვაობა

2018 წლის 10 აპრილს, 29-ე მუხლის სამუშაო ჯგუფმა მიიღო სახელმძღვანელო პრინციპები თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით (WP259.01), რომელსაც მხარი დაუჭირა ევროპის მონაცემთა დაცვის საბჭომ (შემდგომში, EDPB) მის პირველ პლენარულ შეხვედრაზე. წინამდებარე დოკუმენტი აღნიშნული სახელმძღვანელოების უმნიშვნელოდ განახლებულ ვერსიას წარმოადგენს. თანხმობის შესახებ WP29-ის სახელმძღვანელო პრინციპებზე ნებისმიერი მითითება (WP259 rev.01) განმარტებული უნდა იქნას, როგორც ამ სახელმძღვანელო პრინციპებზე მითითება.

EDPB-ის დაკვირვებით, არსებობდა დამატებითი განმარტებების საჭიროება, განსაკუთრებით, ორ საკითხთან დაკავშირებით:

1. მონაცემთა სუბიექტის მიერ გაცემული თანხმობის ნამდვილობა (ლეგიტიმურობა), ე.წ. “cookie walls” ინტერაქციის დროს.

[1] „წევრ სახელმწიფოებზე“ გაკეთებული მითითება წინამდებარე დოკუმენტში გაგებული უნდა იქნას, როგორც „თავისუფალი ეკონომიკური ზონის წევრ სახელმწიფოებზე“ მითითება.

2. მე-16 მაგალითი სქროლინგის და თანხმობის შესახებ.

ამ ორი საკითხის შესახებ არსებული აბზაცები გადაიხედა და განახლდა, ხოლო დოკუმენტის დანარჩენი ნაწილი უცვლელი დარჩა, თუ არ ჩავთვლით რედაქტირების შედეგად შეტანილ ცვლილებებს. კერძოდ, გადაიხედა და განახლდა:

- სექცია, რომელიც ეხება ხელშეკრულების შესრულების ან მომსახურების მიწოდების დამოკიდებულებას თანხმობაზე (38-ე-41-ე პუნქტები)
- სექცია მონაცემთა სუბიექტის სურვილის მკაფიო გამოხატულების შესახებ (86-ე პუნქტი).

1. შესავალი

1. წინამდებარე სახელმძღვანელო პრინციპები ამომწურავად აანალიზებს თანხმობის ცნებას 2016/679 რეგულაციაში (მონაცემთა დაცვის ზოგადი რეგულაცია, შემდგომში, GDPR). თანხმობის კონცეფციამ, რომელიც დღეს-დღეობით გამოიყენება მონაცემთა დაცვის დირექტივაში (შემდგომში: დირექტივა 95/46/EC) და ციფრულ სფეროში მონაცემთა დაცვის დირექტივაში (e-Privacy Directive), ევოლუცია განიცადა. GDPR-ი შეიცავს დამატებით განმარტებებსა და სპეციფიკაციებს ნამდვილი (ლეგიტიმური) თანხმობის მოპოვებისა და დემონსტრირების მოთხოვნებთან დაკავშირებით. წინამდებარე სახელმძღვანელო პრინციპები ყურადღებას ამახვილებს ამ ცვლილებებზე, უზრუნველყოფს პრაქტიკულ ინსტრუქციებს GDPR-თან შესაბამისობის უზრუნველსაყოფად და ემყარება 29-ე სამუშაო ჯგუფის დასკვნას 15/2011 თანხმობის შესახებ. დამუშავებისთვის პასუხისმგებელ პირს ეკისრება ვალდებულება, განახორციელოს ინოვაციური ცვლილებები და მოიძიოს ახლებური გადაწყვეტები, რომლებიც კანონის პარამეტრებში ჯდება და აუმჯობესებს პერსონალური მონაცემებისა და მონაცემთა სუბიექტების ინტერესების დაცვას.

2. თანხმობა პერსონალური მონაცემების დამუშავების ექვსი კანონიერი საფუძვლიდან ერთ-ერთია. ეს საფუძვლები ჩამოთვლილია GDPR-ის მე-6 მუხლში.[2] იმ აქტივობების ინიციირებისას, რომლებიც პერსონალური

[2] GDPR-ის მეორე მუხლში წარმოდგენილია შესაძლო გამონაკლისების ჩამონათვალი, მონაცემთა სპეციალური კატეგორიების დამუშავების აკრძალვასთან დაკავშირებით. ერთ-ერთი გამონაკლისი მოიცავს სიტუაციას, როდესაც მონაცემთა სუბიექტი ამ მონაცემების გამოყენების მკაფიო თანხმობას იძლევა.

მონაცემების დამუშავებას მოიცავს, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ყოველთვის გარკვეული დრო დაუთმოს იმაზე ფიქრს, თუ რა წარმოადგენს გათვალისწინებული დამუშავების შესაბამის კანონიერ საფუძველს.

3. ზოგადად, თანხმობა შესაბამისი კანონიერი საფუძველია იმ შემთხვევაში, თუ მონაცემთა სუბიექტს სთავაზობენ კონტროლს და რეალურ არჩევანს შეთავაზებული პირობების მიღებასა და უარყოფას შორის ან მას უარის თქმა შეუძლია საკუთარი თავისათვის ზიანის მიყენების გარეშე. როდესაც დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტისგან ითხოვს თანხმობას, იგი ვალდებულია, შეაფასოს, თუ რამდენად აკმაყოფილებს ნამდვილი (ლეგიტიმური) თანხმობის მოპოვების ყველა მოთხოვნას. თანხმობა, რომელიც მოპოვებულია GDPR-თან სრულ შესაბამისობაში, წარმოადგენს ინსტრუმენტს, რომელიც მონაცემთა სუბიექტს აძლევს საშუალებას, აკონტროლოს, დამუშავდება თუ არა პერსონალური მონაცემები მის შესახებ. წინააღმდეგ შემთხვევაში, მონაცემთა სუბიექტის კონტროლი ხდება ილუზორული და თანხმობა ვერ იქნება დამუშავების ლეგიტიმური საფუძველი. შედეგად, დამუშავების აქტივობა იქნება უკანონო.[3]

4. 29-ე მუხლის სამუშაო ჯგუფის (WP29) არსებული დასკვნები თანხმობის შესახებ[4] კვლავ რელევანტურია იმდენად, რამდენადაც ისინი შეესაბამება ახალ სამართლებრივ ჩარჩოს, რადგან GDPR-ი ახდენს WP29-ის არსებული ინსტრუქციებისა და ზოგადი კარგი პრაქტიკის კოდიფიცირებას, ხოლო GDPR-ის მიხედვით, თანხმობის ძირითადი ელემენტები იგივე რჩება. ამრიგად, წინამდებარე დოკუმენტში EDPB ახდენს თანხმობასთან დაკავშირებული (95/46/EC დირექტივის მიხედვით) კონკრეტული თემების შესახებ 29-ე მუხლის სამუშაო ჯგუფის დასკვნების განვრცობას და შევსებას და არ ჩაანაცვლებს მათ.

5. როგორც WP29-მ აღნიშნა 15/2011 დასკვნაში თანხმობის განმარტების შესახებ, ადამიანებისათვის მონაცემთა დამუშავების ოპერაციაზე დათანხმების შეთავაზება უნდა დაექვემდებაროს მკაცრ მოთხოვნებს, ვინაიდან იგი ეხება მონაცემთა სუბიექტების ფუნდამენტურ უფლებებს, ხოლო დამუშავებისთვის პასუხისმგებელი პირის სურვილია, განახორციელოს დამუშავების ოპერაცია,

[3] ასევე, იხ. 29-ე მუხლის სამუშაო ჯგუფის დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP 187), გვ.გვ. 6-8, და/ან დასკვნა 06/2014, რომელიც ეხება მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური ინტერესების ცნებას, 95/46/EC დირექტივის (WP 2017) მე-7 მუხლის ჭრილში, გვ.გვ. 9, 10, 13 და 14.

[4] განსაკუთრებით, 29-ე მუხლის სამუშაო ჯგუფის დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP 187).

რომელიც მონაცემთა სუბიექტის თანხმობის გარეშე უკანონო იქნება.[5] თანხმობის უაღრესად მნიშვნელოვან როლს ხაზს უსვამს ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-7 და მე-8 მუხლები. ამას გარდა, თანხმობის მოპოვება არ უარყოფს და არ აკნინებს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებებს, დაიცვას GDPR-ით გათვალისწინებული დამუშავების პრინციპები, განსაკუთრებით, GDPR-ის მე-5 მუხლი, რომელიც ეხება სამართლიანობას, აუცილებლობასა და პროპორციულობას და ასევე, მონაცემთა ხარისხს. მაშინაც კი, თუ პერსონალური მონაცემების დამუშავება მონაცემთა სუბიექტის თანხმობას ეფუძნება, აღნიშნული არ ახდენს იმ მონაცემების შეგროვების ლეგიტიმიზაციას, რომელიც არ არის აუცილებელი დამუშავების გაცხადებული მიზნისთვის და იმ დამუშავების ლეგიტიმიზაციას, რომელიც სხვაგვარად ფუნდამენტურად უსამართლო იქნებოდა.[6]

6. ამავდროულად, EDPB-სათვის ცნობილია ელექტრონულ სივრცეში მონაცემთა დაცვის შესახებ დირექტივის (2002/58/EC) გადახედვის თაობაზე. თანხმობის ცნება აღნიშნული დირექტივის პროექტის თანახმად დაკავშირებულია GDPR-ში წარმოდგენილი თანხმობის ცნებასთან.[7] ელექტრონულ სივრცეში მონაცემთა დაცვის ინსტრუმენტის თანახმად, ონლაინ მარკეტინგის მიზნით გაგზავნილი შეტყობინებებისა თუ მარკეტინგული ზარებისთვის, და ონლაინ მონიტორინგის მეთოდების განხორციელებისთვის, მათ შორის, “cookie walls” ან აპლიკაციების ან სხვა კომპიუტერული პროგრამების გამოყენების გზით, სავარაუდოდ, ორგანიზაციებს დასჭირდებათ თანხმობა. EDPB-ს შემუშავებული აქვს რეკომენდაციები და ინსტრუქციები ევროპელი კანონმდებლებისთვის, ელექტრონულ სივრცეში მონაცემთა დაცვის რეგულაციის პროექტთან დაკავშირებით.[8]

7. რაც შეეხება ელექტრონულ სივრცეში მონაცემთა დაცვის არსებულ დირექტივას, EDPB აღნიშნავს, რომ გაუქმებულ 95/46/EC დირექტივაზე მითითებები გაგებული უნდა იქნას, როგორც GDPR-ზე მითითებები.[9] აღნიშნული, აგრეთვე, ეხება თანხმობაზე მითითებებს მოქმედ 2002/58/EC დირექტივაში, რადგან ელექტრონულ სივრცეში მონაცემთა დაცვის რეგულაცია (ePrivacy Regulation) 2018 წლის 25 მაისი მდგომარეობით, არ არის ძალაში შესული. GDPR-ის 95-ე

[5] დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP 187), გვ.8.

[6] ასევე, იხ. დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP 187) და GDPR-ის მე-5 მუხლი.

[7] e-Privacy რეგულაციის პროექტის მე-9 მუხლის თანახმად, გამოიყენება GDPR-ის 4(11) მუხლში და მე-7 მუხლში წარმოდგენილი თანხმობის განმარტება და პირობები.

[8] იხ. EDPB-ის განცხადება ელექტრონულ სივრცეში მონაცემთა დაცვის შესახებ - 25/05/2018 და EDPB-ის განცხადება 3/2019 ელექტრონულ სივრცეში მონაცემთა დაცვის რეგულაციის შესახებ.

[9] იხ. GDPR-ის 94-ე მუხლი.

მუხლის თანახმად, რეგულაცია არ ადგენს დამატებით ვალდებულებებს საჯარო საკომუნიკაციო ქსელებში საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციის მომსახურების ევროკავშირში მიწოდებასთან დაკავშირებით მონაცემთა დამუშავებისას, ვინაიდან e-Privacy დირექტივა ამავე მიზნებით სპეციფიურ ვალდებულებებს ითვალისწინებს. EDPB აღნიშნავს, რომ GDPR-ით გათვალისიწნებული თანხმობის მოთხოვნა „დამატებით ვალდებულებად“ არ უნდა იქნას განხილული, არამედ, იგი წარმოადგენს ლეგიტიმური დამუშავების წინაპირობას. ამრიგად, GDPR-ით დადგენილი პირობები ნამდვილი (ლეგიტიმური) თანხმობის მოპოვებასთან დაკავშირებით ვრცელდება იმ სიტუაციებზეც, რომლებიც e-Privacy დირექტივის მოქმედების სფეროში შედის.

2. თანხმობა GDPR-ის 4(11) მუხლში

8. GDPR-ის 4(11) მუხლი თანხმობას განსაზღვრავს, როგორც: *„მონაცემთა სუბიექტის სურვილის ნებაყოფლობით, კონკრეტულ, ინფორმირებულ, მკაფიო გამოხატულებას, რომელიც გადმოცემულია განცხადებით ან ნათლად და აქტიურად გამოხატული ქმედებით და რომლის საშუალებითაც ის აცხადებს თანხმობას მასთან დაკავშირებული პერსონალური მონაცემების დამუშავებაზე.“*

9. თანხმობის საბაზისო კონცეფცია არის იგივე, რასაც 95/46/EC დირექტივა ითვალისწინებს, ხოლო თანხმობა არის ერთ-ერთი კანონიერი საფუძველი, რომელსაც პერსონალური მონაცემების დამუშავება უნდა დაეფუძნოს, GDPR-ის მე-6 მუხლის შესაბამისად.[10] გარდა 4(11) მუხლში წარმოდგენილი შესწორებული განმარტებისა, GDPR-ი, აგრეთვე, უზრუნველყოფს დამატებით

[10] 95/46/EC დირექტივაში თანხმობა განმარტებულია შემდეგნაირად: *„ნებისმიერი თავისუფლად გამოხატული კონკრეტული და ინფორმირებული გამოხატულება მისი [მონაცემთა სუბიექტის] სურვილებისა, რომლითაც მონაცემთა სუბიექტი აღნიშნავს მის თანხმობას მასთან დაკავშირებული პერსონალური მონაცემების დამუშავებაზე.“* თანხმობა უნდა იყოს *„მკაფიოდ გამოხატული“* იმისათვის, რომ პერსონალური მონაცემების დამუშავება იყოს ლეგიტიმური (95/46/EC დირექტივის 7(a) მუხლი). იხ. WP29-ის დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP 187), სადაც წარმოდგენილია მაგალითები თანხმობის, როგორც კანონიერი საფუძვლის მიზანშეწონილობასთან დაკავშირებით. ამ დასკვნაში, WP29-მ წარმოადგინა ინსტრუქციები, თუ როგორ გავარჩიოთ ერთმანეთისგან ერთის მხრივ, შემთხვევები, როდესაც თანხმობა სათანადო კანონიერი საფუძველია და მეორეს მხრივ, შემთხვევები, როდესაც ლეგიტიმური ინტერესის საფუძველზე მითითება (უარის თქმის შესაძლებლობასთან ერთად) საკმარისია ან მიზანშეწონილია სახელშეკრულებო ურთიერთობის არსებობა. ასევე, იხ. WP29 დასკვნა 06/2014, პუნქტი III.1.2., გვ. 14 და სხვა. მკაფიო თანხმობა ერთ-ერთი გამონაკლისია სპეციალური კატეგორიის მონაცემთა დამუშავების აკრძალვასთან დაკავშირებით: იხ. GDPR-ის მე-9 მუხლი.

ინსტრუქციებს მე-7 მუხლში და პრეამბულის 32-ე, 33-ე, 42-ე და 43-ე პუნქტებში იმის თაობაზე, თუ როგორ უნდა მოქმედებდეს დამუშავებისთვის პასუხისმგებელი პირი, რათა შეასრულოს თანხმობის მოთხოვნის ძირითადი ელემენტები.

10. და ბოლოს, თანხმობის უკან გახმობის შესახებ კონკრეტული დებულებებისა და პრეამბულაში კონკრეტული პუნქტების გათვალისწინება ადასტურებს, რომ თანხმობა უნდა წარმოადგენდეს შექცევად გადაწყვეტილებას, ხოლო მონაცემთა სუბიექტს უნდა ჰქონდეს გარკვეული კონტროლი.

3. ნამდვილი (ლეგიტიმური) თანხმობის ელემენტები

11. GDPR-ის 4(11) მუხლის თანახმად, მონაცემთა სუბიექტის თანხმობა ნიშნავს ნებისმიერ:

    - ნებაყოფლობით
    - კონკრეტულ
    - ინფორმირებულ
    - და მკაფიო გამოხატულებას მონაცემთა სუბიექტის სურვილებისა, რომელიც გადმოცემულია განცხადებით ან ნათლად და აქტიურად გამოხატული ქმედებით და რომლის საშუალებითაც იგი აცხადებს თანხმობას მასთან დაკავშირებული პერსონალური მონაცემების დამუშავებაზე.

12. ქვემოთ წარმოდგენილ სექციაში, გაანალიზებულია, თუ რა დოზით მოითხოვს 4(11) მუხლის ფორმულირება **დამუშავებისთვის პასუხისმგებელი პირებისგან** მათი თანხმობის მოთხოვნების/ფორმების შეცვლას, რათა უზრუნველყოფილი იქნას GDPR-თან შესაბამისობა.[11]

[11] 95/46 დირექტივის მიხედვით, თანხმობის საფუძველზე მიმდინარე დამუშავების აქტივობებთან დაკავშირებით ინსტრუქციებისთვის, იხ. წინამდებარე დოკუმენტის მე-7 თავი და GDPR-ის პრეამბულის 171-ე პუნქტი.

3.1 თავისუფალი / ნებაყოფლობითი[12]

13. „თავისუფლების“ ელემენტი გულისხმობს რეალურ არჩევანს და კონტროლს მონაცემთა სუბიექტების შემთხვევაში. ზოგადი წესის სახით, GDPR-ი ადგენს, რომ თუ მონაცემთა სუბიექტს არ აქვს რეალური არჩევანი, თავს იძულებულად თვლის, განაცხადოს თანხმობა ან მასზე უარყოფითი გავლენა ექნება თანხმობის გაუცემლობას, მაშინ, თანხმობა არ არის ნამდვილი (ლეგიტიმური).[13] თუ თანხმობა შეფუთულია, როგორც წესებისა და პირობების შემადგენელი ნაწილი, რომელიც არ ექვემდებარება მოლაპარაკებას, მაშინ ითვლება, რომ თანხმობა არ არის ნებაყოფლობითი. შესაბამისად, თანხმობა არ ჩაითვლება ნებაყოფლობითად, თუ მონაცემთა სუბიექტს არ შეუძლია უარი თქვას თანხმობის გაცემაზე ან უკან გაიხმოს იგი ისე, რომ ზიანი არ მიადგეს.[14] GDPR-ში აგრეთვე გათვალისწინებულია დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის დისბალანსის ცნება.

14. თანხმობის ნებაყოფლობითობის შეფასებისას საჭიროა იმ სპეციფიური სიტუაციის გათვალისწინება, რომელიც თანხმობას აკავშირებს ხელშეკრულებებთან ან მომსახურების მიწოდებასთან, 7(4) მუხლში აღწერილი შემთხვევის შესაბამისად. 7(4) მუხლი ფორმულირებულია იმგვარად, რომ იგი არ არის ამომწურავი, კერძოდ, იგი შეიცავს სიტყვებს „მათ შორის“, რაც ნიშნავს იმას, რომ შესაძლოა არსებობდეს კიდევ სხვა არაერთი სიტუაცია, რომელზეც აღნიშნული დებულება ვრცელდება. ზოგადად, მონაცემთა სუბიექტზე არასათანადო ზეწოლის ან გავლენის ნებისმიერი შემთხვევა (რომელიც, შესაძლოა, სხვადასხვაგვარად გამოიხატოს), რომელიც მონაცემთა სუბიექტს ხელს უშლის თავისუფალი ნების განხორციელებისგან, თანხმობას არალეგიტიმურს უნდა ხდიდეს.

---

[12] რამდენიმე დასკვნაში, 29-ე მუხლის სამუშაო ჯგუფი შეეხო თანხმობის ლიმიტების საკითხს, ისეთ სიტუაციებში, როდესაც შეუძლებელია ნებაყოფლობითი თანხმობის გაცემა. ეს დოკუმენტებია: 15/2011 დასკვნა, რომელიც ეხება თანხმობის განმარტებას (WP 187), სამუშაო დოკუმენტი ჯანმრთელობის შესახებ ელექტრონულ ჩანაწერებში ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების შესახებ (WP 131), დასკვნა 8/2001 პერსონალური მონაცემების დასაქმების კონტექსტში დამუშავების შესახებ (WP48) და მეორე დასკვნა 4/2009 მსოფლიო ანტი-დოპინგური სააგენტოს (WADA) მიერ პერსონალური მონაცემების დამუშავების შესახებ (პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური ინფორმაციის საერთაშორისო სტანდარტი, WADA კოდექსის შესაბამის დებულებებთან დაკავშირებით და პირადი ცხოვრების ხელშეუხებლობის სხვა საკითხებზე, სპორტში აკრძალული ნივთიერებების გამოყენებასთან ბრძოლის კონტექსტში, WADA- სა და (ეროვნული) ანტი-დოპინგური ორგანიზაციების მიერ (WP 162).

[13] იხ. დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP187), გვ.12

[14] იხ. GDPR-ის პრეამბულის 42-ე და 43-ე პუნქტები და WP29-ის დასკვნა 15/2011 თანხმობის განმარტების შესახებ, მიღებულია 2011 წლის 13 ივლისს (WP 187), გვ.12.

15. მაგალითი 1: ფოტოების რედაქტირებისთვის განკუთვნილი მობილური აპლიკაცია მომხმარებლებს სთხოვს მათი GPS ლოკალიზაციის გააქტიურებას, იმისათვის, რომ სერვისით სარგებლობა შეძლონ. აპლიკაცია მომხმარებლებს, ასევე, განუმარტავს, რომ იგი შეაგროვებს მონაცემებს მომხმარებელთა ქცევაზე მორგებული რეკლამის მიზნებისთვის. გეოლოკალიზაცია და ქცევაზე მორგებული რეკლამა ფოტორედაქტირების სერვისის მიწოდებისთვის აუცილებლობას არ წარმოადგენს და ძირითადი სერვისი მიწოდების ფარგლებს სცდება. ვინაიდან მომხმარებლებს აპლიკაციის გამოყენება არ შეუძლიათ იმ შემთხვევაში, თუ აღნიშნული მიზნებისთვის არ გასცემენ თანხმობას, თანხმობა ვერ ჩაითვლება ნებაყოფლობით გაცემულად.

3.1.1 ძალაუფლების დისბალანსი

16. პრეამბულის 43-ე პუნქტი[15] მკაფიოდ მიუთითებს, რომ ნაკლებად სავარაუდოა, რომ სახელმწიფო უწყებებმა შეძლონ, დაეყრდნონ თანხმობას დამუშავებისთვის, რადგან როდესაც დამუშავებისთვის პასუხისმგებელი პირი სახელმწიფო უწყებაა, ხშირად მკაფიო ძალაუფლების დისბალანსი არსებობს დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის ურთიერთობაში. აგრეთვე, ნათელია, რომ უმეტეს შემთხვევებში, მონაცემთა სუბიექტს არ ექნება რეალისტური ალტერნატივები ამ ტიპის დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დამუშავებაზე (დამუშავების პირობებზე) არ დათანხმების შემთხვევაში. EDPB მიიჩნევს, რომ არსებობს დამუშავების სხვა კანონიერი საფუძვლები, რომლებიც არსებითად, უფრო მეტად მიესადაგება სახელმწიფო უწყებების მიერ მონაცემთა დამუშავების შემთხვევებს.[16]

17. აღნიშნული ზოგადი საკითხების მნიშვნელობის დაკნინების გარეშე, სახელმწიფო უწყებების მიერ თანხმობის, როგორც მონაცემთა დამუშავების კანონიერი საფუძვლის გამოყენება სრულად არ არის გამორიცხული GDPR-ით

[15] GDPR-ის პრეამბულის 43-ე პუნქტში მითითებულია: „თანხმობის ნებაყოფლობითობის უზრუნველსაყოფად, თანხმობა არ უნდა ჩაითვალოს ვალიდურ სამართლებრივ საფუძვლად იმ შემთხვევაში, როცა ცხადია უთანასწორობა დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის, განსაკუთრებით, როცა დამუშავებისთვის პასუხისმგებელი პირი სახელმწიფო უწყებაა და შესაბამისად, ნაკლებად სავარაუდოა, რომ თანხმობა იმ სიტუაციის ყველა კონკრეტული გარემოების გათვალისწინებით ნებაყოფლობით იყო გაცემული. (...)“.

[16] იხ. GDPR-ის მე-6 მუხლი, განსაკუთრებით, პუნქტები 1c და 1e.

დადგენილი სამართლებრივი ჩარჩოთი. ქვემოთ წარმოდგენილი მაგალითები ასახავს თანხმობის გამოყენების მიზანშეწონილობას გარკვეულ გარემოებებში.

18. მაგალითი 2: ადგილობრივი მუნიციპალიტეტი გეგმავს, ჩაატაროს გზების შეკეთების სამუშაოები. ვინაიდან აღნიშნული სამუშაოები დიდი ხნით შეაფერხებს სატრანსპორტო საშუალებების გადაადგილებას, მუნიციპალიტეტი მოქალაქეებს სთავაზობს, დარეგისტრირდნენ და იმეილის საშუალებით მიიღონ სიახლეები სამუშაოების მიმდინარეობისა და მოსალოდნელი შეფერხებების შესახებ. მუნიციპალიტეტი მკაფიოდ განმარტავს, რომ მოქალაქეებს არ მოეთხოვებათ დარეგისტრირება და (მხოლოდ და მხოლოდ) ამ მიზნისთვის, ელ-ფოსტის მისამართების გამოყენებაზე სთხოვს თანხმობას. თანხმობაზე უარი სამომავლოდ, მოქალაქეებს არ შეუშლის ხელს მუნიციპალიტეტისგან ძირითადი სერვისების მიღებაში ან რომელიმე უფლების განხორციელებაში. შესაბამისად, მათ აქვთ შესაძლებლობა, ნებაყოფლობით გასცენ თანხმობა ან უარი თქვან თანხმობის გაცემაზე, მონაცემთა აღნიშნული მიზნით გამოყენებასთან დაკავშირებით. გზებზე ჩატარებული სამუშაოების შესახებ ინფორმაცია, აგრეთვე, ხელმისაწვდომი იქნება მუნიციპალიტეტის ვებსაიტზე.

19. მაგალითი 3: პირს, რომელიც ფლობს მიწას, ესაჭიროება გარკვეული ნებართვები როგორც ადგილობრივი მუნიციპალიტეტისგან, ისე იმ პროვინციის მმართველობისგან, სადაც ეს მუნიციპალიტეტი მდებარეობს. ორივე საჯარო ორგანო საჭიროებს ერთსა და იმავე ინფორმაციას ნებართვის გასაცემად, თუმცა, მათ ერთმანეთის მონაცემთა ბაზებზე ხელი არ მიუწვდებათ. შესაბამისად, ორივე ორგანომ ერთი და იგივე ინფორმაცია ითხოვა, ხოლო მიწის მფლობელმა ეს მონაცემები ორივე ორგანოს გაუგზავნა. მუნიციპალიტეტი და პროვინციის მმართველობა მიწის მფლობელს სთხოვს თანხმობას ფაილების გასაერთიანებლად, რათა თავიდან იქნას აცილებული პროცედურებისა და კორესპონდენციის დუბლირება. ორივე ორგანომ მოქალაქეს განუმარტა, რომ ფაილების გაერთიანება არ წარმოადგენს სავალდებულო მოთხოვნას, ხოლო თუ მიწის მფლობელი უარს იტყვის მონაცემთა გაერთიანებაზე, ნებართვის შესახებ განცხადებებს სახელმწიფო ორგანოები ცალ-ცალკე შეისწავლიან. ამრიგად, მიწის მფლობელს სახელმწიფო ორგანოებმა მისცეს ნებაყოფლობითი თანხმობის გაცემის შესაძლებლობა, ფაილების გაერთიანების მიზნებისთვის.

20. <u>მაგალითი 4:</u> საჯარო სკოლამ მოსწავლეებს სთხოვა თანხმობა მათი ფოტოების ბეჭდურ სტუდენტურ ჟურნალში გამოქვეყნებისთვის. ამ შემთხვევაში, თანხმობა ნამდვილ არჩევანს წარმოადგენს, თუ ფოტოების გამოყენებაზე უარის თქმის შემთხვევაში, სტუდენტებს არ შეუწყდებათ საგანმანათლებლო ან სხვა სერვისებს და არ მიადგებათ რაიმე ზიანი.[17]

21. ძალაუფლების დისბალანსს ვხვდებით **დასაქმების** კონტექსტშიც.[18] იმის გათვალისწინებით, რომ დამსაქმებელსა და დასაქმებულს შორის ურთიერთობა გარკვეულ დამოკიდებულებას წარმოშობს, ნაკლებად სავარაუდოა, რომ მონაცემთა სუბიექტი შეძლებს, დამსაქმებელს უარი უთხრას საკუთარი მონაცემების დამუშავებაზე ისე, რომ არ განიცადოს უარის დამაზიანებელი შედეგების შიში ან რეალური საფრთხე. ნაკლებად სავარაუდოა, რომ დასაქმებული თავისუფალი ნების საფუძველზე შეძლებს, რომ უპასუხოს დამსაქმებლის მოთხოვნას თანხმობის შესახებ, მაგალითად, მონიტორინგის სისტემების გააქტიურებასთან (მაგ., ვიდეომონიტორინგი სამუშაო ადგილას) ან შეფასების ფორმების შევსებასთან დაკავშირებით, ისე, რომ თავი არ იგრძნოს იძულებულად, დაეთანხმოს დამსაქმებელს.[19] შესაბამისად, EDPB თვლის, რომ დამსაქმებლების მიერ ამჟამინდელი ან მომავალი დასაქმებულების პერსონალური მონაცემების დამუშავება, მათი თანხმობის საფუძველზე, პრობლემურია, რადგან ნაკლებად სავარაუდოა, რომ ეს თანხმობა იქნება ნებაყოფლობითი. დასაქმების კონტექსტში მონაცემთა ამგვარი დამუშავება დიდწილად ვერ და არ დაეფუძნება დასაქმებულის თანხმობას (მუხლი 6(1)(a)), დამსაქმებელსა და დასაქმებულს შორის არსებული ურთიერთობის ხასიათიდან გამომდინარე.[20]

[17] წინამდებარე მაგალითის მიზნებისთვის, საჯარო სკოლა ნიშნავს სახელმწიფოს მიერ დაფინანსებულ სკოლას ან ნებისმიერ საგანმანათლებლო დაწესებულებას, რომელიც ეროვნული კანონმდებლობის თანახმად, წარმოადგენს საჯარო დაწესებულებას ან ორგანოს.

[18] ასევე, იხ. GDPR-ის 88-ე მუხლი, სადაც ხაზგასმულია დასაქმებულთა სპეციფიური ინტერესების დაცვის საჭიროება და უზრუნველყოფილია წევრი სახელმწიფოს სამართალში გამონაკლისების დაშვების შესაძლებლობა. ასევე, იხ. პრეამბულის 155-ე პუნქტი.

[19] იხ. დასკვნა 15.2011 თანხმობის განმარტების შესახებ (WP 187), გვ.გვ. 12-14, დასკვნა 8/2001 პერსონალური მონაცემების დამუშავების შესახებ, დასაქმების კონტექსტში (WP 48), თავი 10, სამუშაო დოკუმენტი სამუშაო ადგილზე ელექტრონული კომუნიკაციების მოსმენის შესახებ (WP 55), პუნქტი 4.2 და დასკვნა 2/2017 სამსახურში მონაცემთა დამუშავების შესახებ (WP 249), პ.6.3.

[20] იხ. დასკვნა 2/2017 სამსახურში მონაცემთა დამუშავების შესახებ, გვ.გვ. 6-7.

22. ამავდროულად, ეს არ ნიშნავს, რომ დამსაქმებლები ვერასოდეს დაეყრდნობიან თანხმობას, როგორც დამუშავების კანონიერ საფუძველს. ზოგიერთ სიტუაციაში, დამსაქმებელი შეძლებს, მოახდინოს დემონსტრირება იმისა, რომ თანხმობა ნებაყოფლობით არის გაცემული. დამსაქმებელსა და დასაქმებულებს შორის ძალაუფლების დისბალანსის გათვალისწინებით, დასაქმებულებს თავისუფალი ნების საფუძველზე თანხმობის გაცემა მხოლოდ გამონაკლის ვითარებებში შეუძლიათ, როდესაც თანხმობის გაცემას ან არ გაცემას არ ექნება რაიმე უარყოფითი შედეგები.[21]

23. მაგალითი 5: გადამღები ჯგუფი აპირებს, ოფისის გარკვეულ ნაწილში გადაიღოს ფილმი. იმ თანამშრომლებს, რომლებიც ოფისის აღნიშნულ ნაწილში სხედან, დამსაქმებელი სთხოვს თანხმობას, რადგან ისინი შესაძლოა კადრში გამოჩნდნენ. თანამშრომლებს, რომელთაც კადრში გამოჩენა არ სურთ, არ დაუწესდებათ რაიმე სანქცია, არამედ, მათ გადაღების პერიოდში, შენობის სხვა მხარეს ეკვივალენტურ ადგილებს შესთავაზებენ.

24. ძალაუფლების დისბალანსი მოქმედებს არა მხოლოდ სახელმწიფო ორგანოებისა და დამსაქმებლების შემთხვევაში, არამედ, სხვა სიტუაციებშიც. WP29-მ რამდენიმე დასკვნაში ხაზი გაუსვა იმას, რომ თანხმობა ლეგიტიმურია მხოლოდ იმ შემთხვევაში, თუ მონაცემთა სუბიექტს რეალური არჩევანის გაკეთების შესაძლებლობა აქვს და არ არსებობს მოტყუების, ზეწოლის, იძულების ან მნიშვნელოვანი უარყოფითი შედეგების რისკი (მაგ., მნიშვნელოვანი დამატებითი ხარჯები), თუ მონაცემთა სუბიექტი უარს იტყვის თანხმობის გაცემაზე. თანხმობა არ ითვლება ნებაყოფლობითად იმ შემთხვევაში, თუ არსებობს იძულების, ზეწოლის ან თავისუფალი ნების განხორციელების შემაფერხებელი რაიმე ელემენტი.

3.1.2 ხელშეკრულების შესრულების ან მომსახურების მიწოდების დამოკიდებულება თანხმობაზე

25. GDPR-ის 7(4) მუხლი მნიშვნელოვან როლს ასრულებს იმის შეფასებაში, თუ რამდენად ნებაყოფლობითია თანხმობა.[22]

[21] ასევე, იხ. დასკვნა 2/2017 სამსახურში მონაცემთა დამუშავების შესახებ (WP249), p.6.2.

[22] GDPR-ის 7(4) მუხლი: *„თანხმობის ნებაყოფლობითობის შეფასებისას მხედველობაში მათ შორის ის, განსაკუთრებული ყურადღება უნდა დაეთმოს თუ რამდენად იყო დამოკიდებული ხელშეკრულების შესრულება ან მომსახურების მიწოდება იმგვარი მონაცემების დამუშავებაზე, რომლებიც არ იყო*

26. GDPR-ის 7(4) მუხლის თანახმად, inter alia, თანხმობის წესებსა და პირობებზე დათანხმებაზე „მიბმით“ ან ხელშეკრულების დებულების ან მომსახურების „მიბმა“ პერსონალური მონაცემების დამუშავებაზე თანხმობასთან, რაც არ წარმოადგენს აუცილებლობას ხელშეკრულების შესრულებისთვის ან მომსახურების მიწოდებისთვის, უაღრესად არასასურველად ითვლება. იმ შემთხვევაში, თუ თანხმობა გაიცემა ასეთ სიტუაციაში, მიჩნეულია, რომ თანხმობა არ არის ნებაყოფლობითი (პრეამბულა, პუნქტი 43). 7(4) მუხლის მიზანია, უზრუნველყოს, რომ არ მოხდეს პერსონალური მონაცემების დამუშავების მიზეზის შენიღბვა ან მიბმა ხელშეკრულების დებულებასთან ან მომსახურებასთან, რომლისთვისაც პერსონალური მონაცემები არ არის აუცილებელი. შედეგად, GDPR-ი უზრუნველყოფს, რომ პერსონალური მონაცემების დამუშავება, რისთვისაც თანხმობას ითხოვენ, არ გახდეს პირდაპირ ან ირიბად ხელშეკრულების რომელიმე მხარის მიერ ხელშეკრულების შეუსრულებლობაზე თქმის საფუძველი. დაუშვებელია პერსონალური მონაცემების დამუშავების ორი კანონიერი საფუძვლის, ე.ი., თანხმობის და ხელშეკრულების შერწყმა და მათ შორის ზღვრის წაშლა.

27. პერსონალური მონაცემების გამოყენებაზე დათანხმების იძულება, იმაზე დამატებით, რაც მკაცრად არის აუცილებელი, ზღუდავს მონაცემთა სუბიექტის არჩევანს და ნებაყოფლობითი თანხმობის განხორციელებას უშლის ხელს. მონაცემთა დაცვის კანონმდებლობის მიზანია, ფუნდამენტური უფლებების დაცვა. შესაბამისად, ფიზიკური პირის მიერ საკუთარი პერსონალური მონაცემების კონტროლი უაღრესად მნიშვნელოვანია და არსებობს მყარი მოსაზრება, რომ თანხმობა პერსონალური მონაცემების დამუშავებაზე, რომელიც არ არის საჭირო, ვერ იქნება მიჩნეული ხელშეკრულების ან მომსახურების განხორციელების სავალდებულო ელემენტად.

28. ამრიგად, როდესაც თანხმობის მოთხოვნა დაკავშირებულია დამუშავებისთვის პასუხისმგებელი პირის მიერ ხელშეკრულების შესრულებასთან, მონაცემთა სუბიექტს, რომელსაც არ სურს საკუთარი პერსონალური მონაცემები გახადოს დამუშავებისთვის ხელმისაწვდომი, ემუქრება საფრთხე, რომ მას მოთხოვნის მომსახურებაზე უარს ეტყვიან.

აუცილებელი ამ ხელშეკრულების შესასრულებლად ან მომსახურების მისაწოდებლად.“ ასევე, იხ. GDPR-ის პრეამბულის 43-ე პუნქტი, რომლის მიხედვითაც: *„[...] თანხმობა არ ითვლება ნებაყოფლობითად, თუ არ არსებობს თანხმობის პერსონალური მონაცემების დამუშავების ცალკეულ ოპერაციებზე გაცემის შესაძლებლობა, მიუხედავად კონკრეტულ შემთხვევაში არსებული მიზანშეწონილობისა, ან თუ ხელშეკრულების შესრულება, მათ შორის მომსახურების მიწოდება, დამოკიდებულია თანხმობაზე, მიუხედავად იმისა, რომ ამგვარი თანხმობა არ არის აუცილებელი ხელშეკრულების შესასრულებლად.“*

29. იმის შესაფასებლად, თუ რამდენად აქვს ადგილი თანხმობის „მიბმას“ ან დაკავშირებას [ხელშეკრულების დებულებასთან ან მომსახურებასთან], მნიშვნელოვანია განისაზღვროს, თუ რა არის ხელშეკრულების მოქმედების სფერო და რომელი მონაცემებია აუცილებელი ხელშეკრულების შესრულებისთვის.

30. WP29-ის 06/2014 დასკვნის თანახმად, ტერმინი „ხელშეკრულების შესრულებისთვის აუცილებელი“ მკაცრად უნდა იქნას ინტერპრეტირებული. დამუშავება აუცილებელი უნდა იყოს ხელშეკრულების შესრულებისთვის, თითოეულ ინდივიდუალურ მონაცემთა სუბიექტთან მიმართებით. აღნიშნული შესაძლოა მოიცავდეს, მაგალითად, მონაცემთა სუბიექტის მისამართის დამუშავებას, რათა ონლაინ შესყიდული საქონლის მიწოდება განხორციელდეს ან საკრედიტო ბარათის მონაცემების დამუშავებას, რათა განხორციელდეს გადახდა. დასაქმების კონტექსტში, აღნიშნული საფუძველი შესაძლოა, მაგალითად, სახელფასო ინფორმაციის და საბანკო რეკვიზიტების დამუშავების შესაძლებლობას იძლეოდეს, ანაზღაურების გადახდის მიზნით.[23] საჭიროა, არსებობდეს პირდაპირი და ობიექტური კავშირი მონაცემების დამუშავებას და ხელშეკრულების მიზნის განხორციელებას შორის.

31. თუ დამუშავებისთვის პასუხისმგებელი პირი ესწრაფვის იმ პერსონალური მონაცემების დამუშავებას, რომელიც რეალურად საჭიროა ხელშეკრულების შესასრულებლად, მაშინ თანხმობა არ წარმოადგენს შესაბამის კანონიერ საფუძველს.[24]

32. 7(4) მუხლი რელევანტურია მხოლოდ იმ შემთხვევაში, თუ მოთხოვნილი მონაცემები **არ** წარმოადგენს აუცილებლობას ხელშეკრულების შესრულებისთვის, (მათ შორის, სერვისის მიწოდებისთვის), ხოლო ამ ხელშეკრულების შესრულება დამოკიდებულია თანხმობის საფუძველზე მონაცემების მოპოვებაზე. მეორეს მხრივ, თუ დამუშავება **წარმოადგენს** აუცილებლობას ხელშეკრულების შესასრულებლად [მათ შორის, მომსახურების მიწოდებისთვის], მაშინ, არ მოქმედებს 7(4) მუხლი.

33. <u>მაგალითი 6:</u> ბანკი მომხმარებლებს სთხოვს თანხმობას, რათა მესამე მხარეებს მისცეს საშუალება, მათ მიერ განხორციელებული გადახდის დეტალები

[23] დამატებითი ინფორმაციისა და მაგალითებისთვის, იხ. დასკვნა 06/2014 მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური ინტერესის შესახებ, 95/46/EC დირექტივის მე-7 მუხლის შესაბამისად, მიღებულია WP24-ის მიერ, 2014 წლის 9 აპრილს, გვ.გვ.16-17. [WP 2017].

[24] ამ შემთხვევაში, დამუშავების შესაბამისი კანონიერი საფუძველია 6(1)(b) მუხლი (ხელშეკრულება).

პირდაპირი მარკეტინგის მიზნებისთვის გამოიყენოს. დამუშავების აღნიშნული აქტივობა არ წარმოადგენს აუცილებლობას მომხმარებელთან გაფორმებული ხელშეკრულების შესასრულებლად და ბანკის ჩვეულებრივი მომსახურების მიწოდებისთვის. თუ მომხმარებლის მიერ უარის თქმის შემთხვევაში ბანკი მას აღარ მიაწვდის საბანკო მომსახურებას, დაუხურავს საბანკო ანგარიშს ან გაზრდის საბანკო მომსახურების გადასახადს, მომხმარებლის თანხმობა ნებაყოფლობითად ვერ ჩაითვლება.

34. ის ფაქტი, რომ კანონმდებელი განსაკუთრებით ხაზს უსვამს ხელშეკრულების შესრულების ან მომსახურების მიწოდების თანხმობაზე დამოკიდებულების საკითხს, სხვა საკითხებთან ერთად, როგორც ნებაყოფლობითობის არ არსებობის მიმანიშნებელი, აჩვენებს, რომ შემთხვევები, სადაც ხელშეკრულების შესრულება ან მომსახურების მიწოდება დამოკიდებულია თანხმობაზე, ყურადღებით უნდა იქნას შესწავლილი. 7(4) მუხლში წარმოდგენილი ტერმინი „განსაკუთრებული ყურადღება“ მიუთითებს, რომ განსაკუთრებული სიფრთხილეა საჭირო დამუშავებისთვის პასუხისმგებელი პირის მხრიდან, როდესაც ხელშეკრულება (რაც შესაძლებელია, რომ მოიცავდეს მომსახურების მიწოდებას) ითხოვს პერსონალური მონაცემების დამუშავების თანხმობას, რომელიც მიბმულია ხელშეკრულების შესრულებაზე.

35. ვინაიდან 7(4) მუხლი არ ადგენს აბსოლუტურ პირობებს, უაღრესად შეზღუდული სივრცე არსებობს ისეთი შემთხვევებისთვის, როდესაც აღნიშნული დამოკიდებულება თანხმობას არალეგიტიმურად არ აქცევს. ამავდროულად, პრეამბულის 43-ე პუნქტში სიტყვა „ითვლება“ მკაფიოდ აღნიშნავს, რომ ასეთი შემთხვევები უაღრესად საგამონაკლისოა.

36. ნებისმიერ შემთხვევაში, 7(4) მუხლის თანახმად, მტკიცების ტვირთი დამუშავებისთვის პასუხისმგებელ პირს ეკისრება.[25] ეს კონკრეტული წესი ასახავს ანგარიშვალდებულების ზოგად პრინციპს, რომელიც GDPR-ის მთელს ტექსტს გასდევს. ამავდროულად, როდესაც მოქმედებს 7(4) მუხლი, უფრო რთულია დამუშავებისთვის პასუხისმგებელი პირისთვის დაადასტუროს, რომ თანხმობა მონაცემთა სუბიექტმა ნებაყოფლობით გასცა.[26]

[25] ასევე, იხ. GDPR-ის 7(1) მუხლი, რომლის თანახმადაც დამუშავებისთვის პასუხისმგებელმა პირმა უნდა დაადასტუროს, რომ მონაცემთა სუბიექტის თანხმობა იყო ნებაყოფლობითი.

[26] გარკვეულწილად, ამ პუნქტის შემოღება წარმოადგენს WP29-ის სახელმძღვანელო მითითების კოდიფიცირებას. როგორც ეს 15/2011 დასკვნაშია მითითებული, როდესაც მონაცემთა სუბიექტი დამოკიდებულია დამუშავებისთვის პასუხისმგებელ პირზე - მათ შორის არსებული ურთიერთობის

37. დამუშავებისთვის პასუხისმგებელ პირს შეუძლია დაამტკიცოს, რომ მისი ორგანიზაცია მონაცემთა სუბიექტს რეალურ არჩევანს სთავაზობს, თუ მონაცემთა სუბიექტს აქვს შესაძლებლობა, აირჩიოს, ერთის მხრივ, მომსახურება, რომელიც მოიცავს დამატებითი მიზნებისთვის პერსონალური მონაცემების გამოყენებაზე თანხმობას ან მეორეს მხრივ, ეკვივალენტური სერვისი, რომელსაც იგივე დამუშავებისთვის პასუხისმგებელი პირი უზრუნველყოფს და არ მოიცავს მონაცემთა გამოყენებაზე თანხმობას. თუ არსებობს დამუშავებისთვის პასუხისმგებელი პირის მიერ ხელშეკრულების შესრულების ან ხელშეკრულებით გათვალისწინებული მომსახურების მიწოდების შესაძლებლობა ისე, რომ მონაცემთა სუბიექტი არ დაეთანხმოს სხვა ან დამატებითი მონაცემების გამოყენებას, ეს ნიშნავს, რომ ხელშეკრულების შესრულება და მომსახურების მიწოდება აღარ არის დამოკიდებული თანხმობაზე. ამავდროულად, ორივე სერვისი ჭეშმარიტად ეკვივალენტური უნდა იყოს.

38. EDPB თვლის, რომ თანხმობა ნებაყოფლობითად ვერ ჩაითვლება, თუ დამუშავებისთვის პასუხისმგებელი პირი აცხადებს, რომ მონაცემთა სუბიექტს აქვს შესაძლებლობა, აირჩიოს სერვისი, რომელიც მოიცავს დამატებითი მიზნებისთვის პერსონალური მონაცემების გამოყენებას ან ეკვივალენტური სერვისი, რომელსაც სხვა დამუშავებისთვის პასუხისმგებელი პირი უზრუნველყოფს. ასეთ შემთხვევაში, არჩევანის თავისუფლება დამოკიდებული იქნება იმაზე, თუ რას აკეთებენ ბაზარზე არსებული სხვა მოთამაშეები და ინდივიდუალური მონაცემთა სუბიექტისათვის რეალურად ეკვივალენტურია თუ არა სხვა დამუშავებისთვის პასუხისმგებელი პირის მომსახურება. აღნიშნული, აგრეთვე, გულისხმობს დამუშავებისთვის პასუხისმგებელი პირების ვალდებულებას, მონიტორინგი გაუწიონ ბაზარზე მიმდინარე მოვლენებს, რათა უზრუნველყონ თანხმობის უწყვეტი ლეგიტიმურობა, მონაცემთა დამუშავებასთან დაკავშირებული აქტივობებისთვის, ვინაიდან კონკურენტმა, შესაძლოა, მოგვიანებით ცვლილებები შეიტანოს მომსახურებაში. ამრიგად, აღნიშნული არგუმენტის გამოყენება ნიშნავს იმას, რომ თანხმობა, რომელიც დამოკიდებულია მესამე მხარის მიერ შეთავაზებულ ალტერნატიულ ვარიანტზე, ვერ უზრუნველყოფს GDPR-თან შესაბამისობას, რაც ნიშნავს იმას, რომ მომსახურების მიმწოდებელი მონაცემთა სუბიექტს ვერ შეუზღუდავს

ხასიათიდან ან განსაკუთრებული გარემოებებიდან გამომდინარე - მაშინ, შესაძლოა არსებობდეს მყარი ვარაუდი, რომ თანხმობის ნებაყოფლობითობა ასეთ კონტექსტებში შეზღუდულია (მაგ., შრომითი ურთიერთობა ან თუ მონაცემთა შეგროვებას ახორციელებს სახელმწიფო ორგანო). 7(4) მუხლის ამოქმედების პირობებში, უფრო რთული იქნება დამუშავებისთვის პასუხისმგებელი პირისთვის დაადასტუროს, რომ თანხმობა იყო ნებაყოფლობითი. იხ. 29-ე სამუშაო ჯგუფის დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP 187), გვ.გვ. 12-17.

მომსახურებაზე წვდომას იმის გამო, რომ მონაცემთა სუბიექტი უარს ამბობს თანხმობის გაცემაზე.

39. იმისათვის, რომ თანხმობა ნებაყოფლობითად ჩაითვალოს, სერვისებსა და ფუნქციონალობებზე წვდომა არ უნდა იყოს დამოკიდებული მომხმარებლის თანხმობაზე ინფორმაციის შენახვის მიმართ ან მომხმარებლის ტერმინალურ მოწყობილობაში შენახულ ინფორმაციაზე წვდომის მიმართ (ე.წ. "cookie walls").[27]

40. <u>მაგალითი 6a:</u> ვებსაიტის პროვაიდერმა განათავსა ტექსტური ფაილი, რომელიც ბლოკავს შინაარსის ხილვადობას. ჩანს მხოლოდ ე.წ. "cookie" ფაილებზე დათანხმების მოთხოვნა და ინფორმაცია იმის შესახებ, თუ რომელი ფაილია მომართული და რა მიზნებით მოხდება მონაცემების დამუშავება. შეუძლებელია შინაარსზე წვდომა „cookie-ფაილებზე დათანხმების" ღილაკზე დაწკაპუნების გარეშე. ვინაიდან მონაცემთა სუბიექტს დამუშავებისთვის პასუხისმგებელი პირი არ სთავაზობს რეალურ არჩევანს, თანხმობა არ არის ნებაყოფლობითი.

41. აღნიშნული არ წარმოადგენს ლეგიტიმურ (ნამდვილ) თანხმობას, რადგან მომსახურების მიწოდება დამოკიდებულია მონაცემთა სუბიექტის მიერ „cookie-ფაილებზე დათანხმების" ღილაკზე დაწკაპუნებაზე. მონაცემთა სუბიექტს არ აქვს რეალური არჩევანი.

3.1.3 თანხმობის მოთხოვნათა დეტალურობა

42. მომსახურება, შესაძლოა, მოიცავდეს დამუშავების მრავლობით ოპერაციას, ერთზე მეტი მიზნისთვის. ასეთ შემთხვევაში, მონაცემთა სუბიექტებს უნდა შეეძლოთ, თავად აირჩიონ, თუ რომელ მიზანს დაეთანხმებიან. ისინი არ უნდა იყვნენ ვალდებულები, დაეთანხმონ დამუშავების მიზნების მთელ წყებას. ასეთ შემთხვევებში, GDPR-ის თანახმად მიზანშეწონილია რამდენიმე თანხმობის მოთხოვნა, მომსახურების შეთავაზების დასაწყებად.

43. პრეამბულის 43-ე პუნქტის თანახმად, თანხმობა არ ჩაითვლება ნებაყოფლობითად, თუ თანხმობის მოპოვების პროცესი/პროცედურა მონაცემთა

[27] როგორც ზემოთ განიმარტა, GDPR-ით ლეგიტიმური თანხმობის მოპოვებასთან დაკავშირებით დადგენილი პირობები იმ სიტუაციებზეც ვრცელდება, რომლებიც ელექტრონულ სივრცეში მონაცემთა დაცვის დირექტივის მოქმედების სფეროში ხვდებიან.

სუბიექტებს არ აძლევს თანხმობის პერსონალური მონაცემების დამუშავების ცალკეულ ოპერაციებზე გაცემის შესაძლებლობას (მაგ., დაეთანხმონ დამუშავების ზოგიერთ ოპერაციას და არ დაეთანხმონ დანარჩენებს), მიუხედავად კონკრეტულ შემთხვევაში არსებული მიზანშეწონილობისა. პრეამბულის 32-ე პუნქტის თანახმად, „თანხმობა უნდა შეეხებოდეს დამუშავების ყველა აქტივობას, რომლებიც *ხორციელდება იმავე მიზნით ან მიზნებით. თუ მონაცემთა დამუშავება ხორციელდება რამდენიმე მიზნით, თანხმობა უნდა გაიცეს თითოეულთან მიმართებაში.“*

44. თუ დამუშავებისთვის პასუხისმგებელმა პირმა მოახდინა დამუშავების რამდენიმე მიზნის გაერთიანება და არ მოითხოვა ცალ-ცალკე თანხმობა თითოეული მიზნისთვის, მაშინ თანხმობა არ იქნება ნებაყოფლობითი. თანხმობის ამგვარი დეტალურობა მჭიდროდ არის დაკავშირებული იმასთან, რომ თანხმობა უნდა იყოს კონკრეტული, როგორც ეს განხილულია 3.2 სექციაში (ქვემოთ). როდესაც მონაცემთა დამუშავება რამდენიმე მიზნისთვის ხორციელდება, ლეგიტიმური თანხმობის პირობებთან შესაბამისობა მოითხოვს დეტალურობას, ე.ი., ამ მიზნების დაყოფას და თითოეული მათგანისთვის შესაბამისი თანხმობის მოპოვებას.

45. მაგალითი 7: თანხმობის ერთი და იგივე მოთხოვნის ფარგლებში, საცალო მოვაჭრე მომხმარებლებს სთხოვს თანხმობას, რათა მათი მონაცემები გამოიყენოს მარკეტინგული იმეილების დაგზავნის მიზნით და ამასთან, მათი საკონტაქტო ინფორმაცია გაუზიაროს სხვა კომპანიებს, რომლებიც ერთი და იგივე ჯგუფის შემადგენლობაში შედიან. აღნიშნული თანხმობა არ არის დეტალური, რადგან დამუშავებისთვის პასუხისმგებელი პირი ამ ორი სხვადასხვა მიზნისთვის არ ითხოვს ცალ-ცალკე თანხმობას. შესაბამისად, თანხმობა ვერ იქნება ლეგიტიმური. ამ შემთხვევაში, ცალკე თანხმობა უნდა იქნას მიღებული მომხმარებელთა საკონტაქტო ინფორმაციის კომერციული პარტნიორებისთვის გაგზავნისთვის. ამგვარი კონკრეტული თანხმობა ლეგიტიმურად ჩაითვლება თითოეული პარტნიორის შემთხვევაში (ასევე, იხ. სექცია 3.3.1), რომელთა ვინაობის შესახებ ინფორმაციაც მიეწოდება მონაცემთა სუბიექტს, მისი თანხმობის მოპოვების დროს, იმ შემთხვევაში, თუ მონაცემები იგზავნება იგივე მიზნისთვის (მოცემულ მაგალითში: მარკეტინგის მიზნისთვის).

3.1.4 ზიანი

46. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მოახდინოს იმის დემონსტრირება, რომ შესაძლებელია თანხმობაზე უარის თქმა ან თანხმობის უკან გახმობა ისე, რომ მონაცემთა სუბიექტს არ მიადგეს ზიანი (პრეამბულა, პუნქტი 42). მაგალითად, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა დაამტკიცოს, რომ თანხმობის უკან გახმობა არ გამოიწვევს მონაცემთა სუბიექტზე რაიმე ხარჯების დაკისრებას და შესაბამისად, ის, ვინც თანხმობას უკან გაიხმობს, არ აღმოჩნდება არახელსაყრელ მდგომარეობაში.

47. ზიანის სხვა მაგალითებია: მოტყუება, ზეწოლა, იძულება ან მნიშვნელოვანი უარყოფითი შედეგები, თუ მონაცემთა სუბიექტი უარს იტყვის თანხმობის გაცემაზე. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეძლოს დამტკიცება იმისა, რომ მონაცემთა სუბიექტს თავისუფალი და რეალური არჩევანი ჰქონდა თანხმობის გაცემა-არ გაცემასთან დაკავშირებით და თანხმობის უკან გახმობა მონაცემთა სუბიექტს არ აყენებდა ზიანს.

48. თუ დამუშავებისთვის პასუხისმგებელი პირი შეძლებს, დაადასტუროს, რომ მომსახურება მოიცავს თანხმობის უკან გახმობის შესაძლებლობას, ყოველგვარი უარყოფითი შედეგების გარეშე, მაგ., მომსახურების მიწოდების გაუარესების გარეშე, რაც მომხმარებელს ზიანს აყენებს, ამ შემთხვევაში, იგი შეძლებს, დაადასტუროს, რომ თანხმობა იყო ნებაყოფლობითი. GDPR-ი არ გამორიცხავს ყველა წამახალისებელ საშუალებას, თუმცა, დამუშავებისთვის პასუხისმგებელ პირს დაეკისრება ტვირთი აჩვენოს, რომ ნებისმიერ გარემოებაში, თანხმობა იყო ნებაყოფლობითი.

49. <u>მაგალითი 8:</u> ცხოვრების წესის შესახებ მობილური აპლიკაციის ჩამოტვირთვისას, აპლიკაცია ითხოვს თანხმობას ტელეფონის აქსელერომეტრზე, რაც არ არის აუცილებელი იმისათვის, რომ აპლიკაციამ იმუშაოს, თუმცა, წვდომა სასარგებლო იქნება დამუშავებისთვის პასუხისმგებელი პირისთვის, რომელსაც სურს მეტი ინფორმაციის მიღება მომხმარებელთა მოძრაობისა და ფიზიკური აქტივობის დონის შესახებ. მოგვიანებით ერთ-ერთმა მომხმარებელმა გააუქმა გაცემული თანხმობა და აღმოაჩინა, რომ შედეგად, აპლიკაცია ლიმიტირებულად მუშაობს. ეს წარმოადგენს ზიანის მაგალითს, რომელზეც მიუთითებს პრეამბულის 42-ე მუხლი, რაც ნიშნავს იმას, რომ თანხმობის მოპოვება არ მომხდარა ლეგიტიმურად (შესაბამისად, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა

წაშალოს ყველა პერსონალური მონაცემები მომხმარებელთა გადაადგილებების შესახებ, რომელიც ამ გზით შეგროვდა).

50. <u>მაგალითი 9:</u> მონაცემთა სუბიექტმა გამოიწერა ტანსაცმლის მაღაზიის ონლაინ საინფორმაციო ბიულეტენი, საიდანაც იღებს ინფორმაციას ფასდაკლებების შესახებ. ტანსაცმლის მაღაზიამ მონაცემთა სუბიექტს სთხოვა შოფინგთან დაკავშირებული პრიორიტეტების შესახებ მონაცემების შესაგროვებლად, რათა შემდგომ მომხმარებლებს გაუგზავნოს მათ პრიორიტეტებზე მორგებული (პერსონალიზებული) შეთავაზებები ან კითხვარი, რომლის შევსებაც არ არის სავალდებულო. თანხმობის გაუქმების შემთხვევაში, მონაცემთა სუბიექტი კვლავ გააგრძელებს არა-პერსონალიზებული ფასდაკლებების მიღებას. აღნიშნული არ წარმოადგენს ზიანს, არამედ, თანხმობის გაუქმებით, მომხმარებელმა დაკარგა დასაშვები წამახალისებელი საშუალება.

51. <u>მაგალითი 10:</u> მოდის ჟურნალი მკითხველებს სთავაზობს, შეიძინონ მაკიაჟის ახალი პროდუქტები მანამ, სანამ ეს პროდუქტები ოფიციალურად გაიყიდება.

52. აღნიშნული პროდუქტები მალე ოფიციალურადაც გაიყიდება, თუმცა, ჟურნალი მკითხველებს მათი უფრო ადრე მოსინჯვის შესაძლებლობას სთავაზობს. ამ სარგებლის მისაღებად, მკითხველებმა ჟურნალს უნდა გაუზიარონ თავიანთი საფოსტო მისამართი და მეილინგ-ლისტში გაწევრიანდნენ. საფოსტო მისამართი პროდუქტის მიწოდებისთვის არის აუცილებელი, ხოლო მეილინგ-ლისტს ჟურნალი გამოიყენებს მთელი წლის მანძილზე კომერციული შეთავაზებების გასაგზავნად, ისეთი პროდუქტების შესახებ, როგორიცაა, კოსმეტიკური საშუალებები და მაისურები.

53. კომპანია განმარტავს, რომ მეილინგ ლისტის მონაცემებს გამოიყენებს მხოლოდ პროდუქტების და ბეჭდური რეკლამის გასაგზავნად და ამ მონაცემებს სხვა ორგანიზაციას არ გაუზიარებს.

54. თუ ჟურნალის მკითხველი უარს განაცხადებს აღნიშნული მიზნისთვის საკუთარი მისამართის გამჟღავნებაზე, მას რაიმე ზიანი არ მიადგება, რადგან პროდუქტები მათთვის კვლავ იქნება ხელმისაწვდომი.

3.2 კონკრეტული

55. 6(1)(a) მუხლი ადასტურებს, რომ მონაცემთა სუბიექტის თანხმობა გაცემული უნდა იქნას „ერთი ან რამდენიმე კონკრეტული“ მიზნისთვის, ხოლო მონაცემთა სუბიექტს უნდა შეეძლოს, თავად გადაწყვიტოს, გასცეს თუ არა თანხმობა თითოეულ ამ მიზანთან მიმართებით.[28] თანხმობის „კონკრეტულობის“ შესახებ მოთხოვნის მიზანია, მომხმარებელს მისცეს კონტროლის შესაძლებლობა და მონაცემთა სუბიექტისათვის უზრუნველყოს გამჭვირვალობა. ეს მოთხოვნა GDPR-ის მიერ არ შეცვლილა და იგი კვლავ მჭიდროდ არის დაკავშირებული „ინფორმირებული“ თანხმობის მოთხოვნასთან. ამავდროულად, იგი განმარტებული უნდა იქნას „თანხმობის მოთხოვნათა დეტალურობის“ მოთხოვნასთან შესაბამისობაში, იმისათვის, რომ თანხმობა იყოს „ნებაყოფლობითი“.[29] მოკლედ რომ შევაჯამოთ, „კონკრეტულობის“ ელემენტთან შესაბამისობისთვის, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს:

   i. მიზნის კონკრეტულობა, რაც „მცოცავი მიზნისგან“ [function creep - როდესაც მონაცემთა გამოყენება ხდება თავდაპირველად გაცხადებული მიზნისგან განსხვავებული მიზნით] დაცვის საშუალებაა;

   ii. თანხმობის მოთხოვნათა დეტალურობა; და

   iii. დამუშავების აქტივობებისთვის თანხმობის მოპოვებასთან დაკავშირებული ინფორმაციის მკაფიო გამიჯვნა სხვა საკითხების შესახებ ინფორმაციისგან.

56. **Ad. (i):** GDPR-ის 5(1)(b) მუხლის თანახმად, ლეგიტიმური თანხმობის მოპოვებას ყოველთვის წინ უსწრებს კონკრეტული, მკაფიო და ლეგიტიმური მიზნის განსაზღვრა, დაგეგმილი დამუშავებისთვის.[30] კონკრეტული თანხმობის

[28] „მიზნების“ განსაზღვრის შესახებ დამატებითი ინსტრუქციები იხილეთ 3/2013 დასკვნაში, რომელიც ეხება მიზნის შეზღუდვას (WP 203).

[29] GDPR-ის პრეამბულის 43-ე პუნქტის თანახმად, საჭიროა არსებობდეს პერსონალური მონაცემების დამუშავების ცალკეულ ოპერაციებზე თანხმობის გაცემის შესაძლებლობა. დეტალური თანხმობის შესაძლებლობა კი უზრუნველყოფილი უნდა იქნას იმისათვის, რომ მონაცემთა სუბიექტებმა შეძლონ, სხვადასხვა მიზნებს დაეთანხმონ ინდივიდუალურად.

[30] იხ. WP29-ის დასკვნა 3/2013 მიზნის შეზღუდვის შესახებ (WP 203), გვ.16. „ამ მიზეზების გამო, მიზანი, რომელიც ზოგადი და ბუნდოვანია, მაგალითად, „მომხმარებელთა გამოცდილების გაუმჯობესება“,

საჭიროება, 5(1)(b) მუხლით გათვალისწინებული მიზნის შეზღუდვის ცნებასთან ერთად, ერთგვარი დამცავი მექანიზმია იმ მიზნების ეტაპობრივი გაფართოებისგან ან გაუფერულებისგან, რომლისთვისაც ხდება მონაცემების დამუშავება, მას შემდეგ, რაც მონაცემთა სუბიექტი თანხმობას განაცხადებს მონაცემთა შეგროვების თავდაპირველ მიზანთან მიმართებით. ამ ფენომენს, აგრეთვე, ეწოდება „მცოცავი მიზანი“ [function creep]. იგი გარკვეულ რისკს წარმოშობს მონაცემთა სუბიექტებისთვის, რადგან შესაძლოა გამოიწვიოს დამუშავებისთვის პასუხისმგებელი პირის ან მესამე მხარეების მიერ პერსონალური მონაცემების მოულოდნელი გამოყენება და მონაცემთა სუბიექტის მიერ საკუთარ მონაცემებზე კონტროლის დაკარგვა.

57. თუ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ეყრდნობა 6(1)(a) მუხლს, მონაცემთა სუბიექტებმა თანხმობა დამუშავების კონკრეტული მიზნისთვის უნდა გასცენ.[31] *მიზნის შეზღუდვის* კონცეფციის, 5(1)(b) მუხლისა და პრეამბულის 32-ე პუნქტის მიხედვით, თანხმობა შესაძლოა მოიცავდეს სხვადასხვა ოპერაციებს იმ პირობით, თუ ეს ოპერაციები ერთსა და იმავე მიზანს ემსახურება. ბუნებრივია, კონკრეტული თანხმობის მოპოვება შესაძლებელია მხოლოდ იმ შემთხვევაში, თუ მონაცემთა სუბიექტები კონკრეტულად არიან ინფორმირებულები იმის შესახებ, თუ რა მიზნებით აპირებს დამუშავებისთვის პასუხისმგებელი პირი მათთან დაკავშირებული მონაცემების გამოყენებას.

58. იმ დებულებების მიუხედავად, რომელიც ეხება მიზნების თავსებადობას, თანხმობა უნდა იყოს კონკრეტული მიზნისადმი სპეციფიური. მონაცემთა სუბიექტები თანხმობას გასცემენ იმ დათქმით, რომ ისინი ინარჩუნებენ საკუთარ მონაცემებზე კონტროლს, ხოლო მონაცემების დამუშავება მოხდება მხოლოდ დასახელებული მიზნებისთვის. თუ დამუშავებისთვის პასუხისმგებელი პირი მონაცემებს ამუშავებს თანხმობის საფუძველზე და სურს, რომ სხვა მიზნისთვისაც დაამუშაოს ეს მონაცემები, მაშინ მან დამატებითი თანხმობა უნდა მოიპოვოს ამ სხვა მიზანთან მიმართებით, გარდა იმ შემთხვევისა, თუ არსებობს სხვა კანონიერი საფუძველი, რომელიც უკეთ ასახავს სიტუაციას.

59. <u>მაგალითი 11:</u> საკაბელო ტელევიზია გამომწერთა პერსონალურ მონაცემებს აგროვებს, მათი თანხმობის საფუძველზე, რათა მათ წარუდგინოს პერსონალური რჩევები ახალ ფილმებთან დაკავშირებით, იმის მიხედვით, თუ რა ფილმებს

„მარკეტინგული მიზნებისთვის“, „IT უსაფრთხოების მიზნებისთვის“ ან „სამომავლო კვლევისთვის“ - დამატებითი დეტალების გარეშე - როგორც წესი, ვერ აკმაყოფილებს „კონკრეტულობის“ კრიტერიუმს.“

[31] აღნიშნული შეესაბამება WP29-ის დასკვნას 15/2011 თანხმობის განმარტების შესახებ (WP 198), მაგალითად, გვ. 17.

უყურებენ მომხმარებლები. გარკვეული ხნის შემდეგ, საკაბელო ტელევიზია გადაწყვეტს, მესამე მხარეებს მისცეს საშუალება, გამომწერებს გაუგზავნოს (ან ეკრანზე განათავსოს) მიზნობრივი რეკლამები, რომელიც დაფუძნებული იქნება იგივე მონაცემებზე.

60. Ad. (ii): თანხმობის მექანიზმები არა მხოლოდ დეტალური უნდა იყოს იმისათვის, რომ შესრულდეს „ნებაყოფლობითი თანხმობის“ მოთხოვნა, არამედ, აგრეთვე, „კონკრეტულობის“ ელემენტსაც უნდა აკმაყოფილებდეს. ეს ნიშნავს იმას, რომ დამუშავებისთვის პასუხისმგებელი პირი, რომელსაც სურს თანხმობის მიღება რამდენიმე სხვადასხვა მიზნისთვის, ვალდებულია, თითოეულ მიზანთან დაკავშირებით უზრუნველყოს ცალკე დათანხმების შესაძლებლობა, რათა მომხმარებლებმა კონკრეტულ მიზნებთან მიმართებით გასცენ კონკრეტული თანხმობა.

61. **Ad. (iii):** და ბოლოს, დამუშავებისთვის პასუხისმგებელმა პირმა, თანხმობის თითოეულ მოთხოვნასთან ერთად, მონაცემთა სუბიექტი უნდა უზრუნველყოს კონკრეტული ინფორმაციით, რათა ისინი იყვნენ ინფორმირებულები თითოეული არჩევანის შედეგის შესახებ. ამრიგად, მონაცემთა სუბიექტი შეძლებს, გასცეს კონკრეტული თანხმობა. აღნიშნული საკითხი გარკვეულწილად მოიცავს მოთხოვნას, რომლის მიხედვითაც დამუშავებისთვის პასუხისმგებელმა პირმა უნდა წარმოადგინოს მკაფიო ინფორმაცია, რაც 3.3 პუნქტში არის განხილული (იხ. ქვემოთ).

3.3 ინფორმირებული

62. GDPR-ი ამყარებს მოთხოვნას, რომ თანხმობა უნდა იყოს ინფორმირებული. GDPR-ის მე-5 მუხლის თანახმად, გამჭვირვალობის მოთხოვნა ერთ-ერთი ფუნდამენტური პრინციპია და იგი მჭიდროდ არის დაკავშირებული სამართლიანობის და კანონიერების პრინციპებთან. მონაცემთა სუბიექტებისათვის ინფორმაციის მიწოდება მათი თანხმობის მიღებამდე მნიშვნელოვანია იმისათვის, რომ მათ ჰქონდეთ ინფორმირებული გადაწყვეტილებების მიღების შესაძლებლობა, გაიაზრონ, თუ რას ეთანხმებიან და მაგალითად, განახორციელონ თანხმობის უკან გახმობის უფლება. თუ დამუშავებისთვის პასუხისმგებელი პირი არ უზრუნველყოფს მისაწვდომ ინფორმაციას, მომხმარებლის კონტროლი გახდება ილუზორული, ხოლო თანხმობა დამუშავების არალეგიტიმური საფუძველი იქნება.

63. ინფორმირებული თანხმობის მოთხოვნების შეუსრულებლობის შედეგი არის ის, რომ თანხმობა იქნება არალეგიტიმური და დამუშავებისთვის პასუხისმგებელი პირი დაარღვევს GDPR-ის მე-6 მუხლს.

3.3.1 მინიმალური შინაარსთან დაკავშირებული მოთხოვნები, „ინფორმირებული“ თანხმობის ჭრილში

64. იმისათვის, რომ თანხმობა იყოს ინფორმირებული, აუცილებელია მონაცემთა სუბიექტის ინფორმირება გარკვეული ელემენტების შესახებ, რომელიც არჩევანის გასაკეთებლად აუცილებლობას წარმოადგენს. შესაბამისად, EDPB თვლის, რომ როგორც მინიმუმ, ქვემოთ წარმოდგენილი ინფორმაციაა საჭირო ლეგიტიმური თანხმობის მისაღებად:

i. დამუშავებისთვის პასუხისმგებელი პირის ვინაობა,[32]

ii. დამუშავების თითოეული ოპერაციის მიზანი, რომლისთვისაც დამუშავებისთვის პასუხისმგებელი პირი ითხოვს თანხმობას,[33]

iii. რა ტიპის მონაცემების შეგროვება და გამოყენება მოხდება,[34]

iv. თანხმობის უკან გახმობის უფლების არსებობა,[35]

v. ინფორმაცია მონაცემების ავტომატური გადაწყვეტილების მიღებისთვის გამოყენების შესახებ, 22(2)(c) მუხლის შესაბამისად,[36] საჭიროების მიხედვით, და

vi. ის შესაძლო რისკები, რომელიც დაკავშირებულია მონაცემთა გადაცემის შემთხვევებთან, შესაბამისობის შესახებ

[32] ასევე, იხ. GDPR-ის პრეამბულა, 42-ე პუნქტი: „[...] იმისთვის, რომ თანხმობა ინფორმირებული იყოს, მონაცემთა სუბიექტისთვის, ცნობილი უნდა იყოს, სულ მცირე, დამუშავებისთვის პასუხისმგებელი პირის ვინაობა და მონაცემთა დამუშავების მიზანი. [...].“

[33] კვლავ, იხ. პრეამბულის 42-ე პუნქტი

[34] ასევე, იხ. WP29-ის დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP 187), გვ.გვ. 19-20.

[35] იხ. GDPR-ის 7(3) მუხლი.

[36] ასევე, იხ. WP29-ის სახელმძღვანელო პრინციპები ავტომატური ინდივიდუალური გადაწყვეტილების მიღების და პროფილირების შესახებ, 2016/679 (WP251) რეგულაციის მიზნებისთვის, პუნქტი IV.B, გვ.20 და შემდგომი გვერდები.

გადაწყვეტილებისა და 46-ე მუხლით გათვალისწინებული დაცვის სათანადო გარანტიების არ არსებობის პირობებში.[37]

65. რაც შეეხება (i) და (iii) პუნქტებს, EDPB აღნიშნავს, რომ იმ შემთხვევაში, როდესაც მოთხოვნილ თანხმობას დაეყრდნობა რამდენიმე (ერთობლივი) დამუშავებისთვის პასუხისმგებელი პირი ან თუ მონაცემები გადაეცემა სხვა დამუშავებისთვის პასუხისმგებელ პირს ან დამუშავდება სხვა დამუშავებისთვის პასუხისმგებელი პირის მიერ, რომელსაც სურს, რომ დაეყრდნოს თავდაპირველ თანხმობას, უნდა მიეთითოს ყველა ამ ორგანიზაციის დასახელება. დამუშავებაზე უფლებამოსილი პირების დასახელება არ არის საჭირო თანხმობასთან დაკავშირებული მოთხოვნების კონტექსტში, თუმცა, GDPR-ის მე-13 და მე-14 მუხლებთან შესაბამისობისთვის, საჭიროა, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა წარმოადგინონ მონაცემთა მიმღებების ან მიმღებთა კატეგორიების სრული სია, დამუშავებაზე უფლებამოსილი პირების ჩათვლით. დასკვნის სახით, EDPB აღნიშნავს, რომ ინდივიდუალური შემთხვევის გარემოებებისა და კონტექსტის მიხედვით, შესაძლოა, საჭირო იტოს დამატებითი ინფორმაცია, რათა მონაცემთა სუბიექტი რეალურად იყოს ინფორმირებული დამუშავების მოცემული ოპერაციების შესახებ.

3.3.2 როგორ უნდა მოხდეს ინფორმაციის მიწოდება

66. GDPR-ი არ ადგენს ინფორმაციის მიწოდების ფორმას, ინფორმირებული თანხმობის მოთხოვნის შესასრულებლად. ეს ნიშნავს იმას, რომ ვალიდური (სარწმუნო) ინფორმაციის წარდგენა შესაძლებელია სხვადასხვა ფორმით, როგორიცაა, წერილობითი ან ზეპირი განცხადებები ან აუდიო თუ ვიდეო გზავნილები. ამავდროულად, GDPR-ი აწესებს რამდენიმე მოთხოვნას ინფორმირებულ თანხმობასთან დაკავშირებით, ძირითადად, 7(2) მუხლსა და პრეამბულის 32-ე პუნქტში. აღნიშნული განაპირობებს უფრო მაღალ სტანდარტს ინფორმაციის მკაფიოობასა და მისაწვდომობასთან დაკავშირებით.

67. თანხმობის მოთხოვნისას, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოფს მკაფიო და მარტივი ენის გამოყენება ყველა შემთხვევაში. ეს ნიშნავს, რომ გზავნილი ადვილად გასაგები უნდა იყოს საშუალო ადამიანისთვის და არა მხოლოდ იურისტებისთვის. დაუშვებელია კონფიდენციალურობის

[37] 49(1)(a) მუხლის თანახმად, კონკრეტული ინფორმაციაა საჭირო იმ დაცვის გარანტიების არ არსებობის შესახებ, რომლებიც 46-ე მუხლში არის აღწერილი, როდესაც დამუშავებისთვის პასუხისმგებელ პირს სურს, მიიღოს მკაფიო თანხმობა. აგრეთვე, იხ. WP29-ის მოსაზრება 15/2011 თანხმობის განმარტების შესახებ (WP 187), გვ.19.

ვრცელი პოლიტიკის გამოყენება, რომლის გაგებაც რთულია ან რომელიც სამართლებრივი ჟარგონებით არის დატვირთული. თანხმობა უნდა იყოს მკაფიო და სხვა საკითხებისგან გარჩევადი და გასაგები და ადვილად მისაწვდომი ფორმით უნდა იყოს უზრუნველყოფილი. აღნიშნული მოთხოვნა, არსებითად, ნიშნავს იმას, რომ თანხმობის შესახებ ინფორმირებული გადაწყვეტილებების მისაღებად საჭირო ინფორმაცია არ უნდა იქნას დამალული ზოგად წესებსა და პირობებში.[38]

68. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, უზრუნველყოს თანხმობის გაცემა იმ ინფორმაციის საფუძველზე, რომელიც მონაცემთა სუბიექტს საშუალებას აძლევს, ადვილად მოახდინოს იდენტიფიცირება, თუ ვინ არის დამუშავებისთვის პასუხისმგებელი პირი და გაიაზროს, თუ რას ეთანხმება იგი. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მკაფიოდ აღწეროს მონაცემთა შეგროვების მიზანი, რისთვისაც ითხოვს თანხმობას.[39]

69. სხვა კონკრეტული მითითებები მისაწვდომობასთან დაკავშირებით წარმოდგენილია WP29-ის სახელმძღვანელო ინსტრუქციებში გამჭვირვალობის შესახებ. თუ თანხმობის გაცემა ხდება ელექტრონული საშუალებით, მოთხოვნა უნდა იყოს მკაფიო და ლაკონიური. მრავალშრიანი და დეტალური ინფორმაცია მიზანშეწონილია ერთის მხრივ, ზუსტი და სრული და მეორეს მხრივ, გასაგები ინფორმაციის შესახებ ორმაგი ვალდებულების შესასრულებლად.

70. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, შეაფასოს, თუ რა სახის აუდიტორია ჰყავს მას, რომელიც ორგანიზაციას აწვდის პერსონალურ მონაცემებს. მაგალითად, თუ მიზნობრივი აუდიტორია მოიცავს არასრულწლოვან მონაცემთა სუბიექტებს, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს, რომ ინფორმაცია გასაგებია არასრულწლოვნებისთვის.[40] აუდიტორიის იდენტიფიცირების შემდგომ, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა განსაზღვროს, თუ რა სახის ინფორმაცია უნდა უზრუნველყოს მან და შემდგომ, როგორ წარუდგენს ამ ინფორმაციას მონაცემთა სუბიექტს.

71. 7(2) მუხლი ეხება თანხმობის წინასწარ ფორმულირებულ წერილობით დეკლარაციებს, რომლებიც, აგრეთვე, სხვა საკითხებსაც მოიცავს. როდესაც თანხმობის მოთხოვნა ხდება (ფიზიკური) ხელშეკრულების ფარგლებში,

[38] უნდა მიეთითოს თანხმობის განაცხადი, როგორც ასეთი. ფორმულირება, როგორიცაა „მე ვიცი, რომ ...“ არ აკმაყოფილებს მკაფიო ენის მოთხოვნას.

[39] იხ. GDPR-ის 4(11) და 7(2) მუხლები.

[40] ასევე, იხ. პრეამბულის 58-ე პუნქტი ბავშვებისთვის გასაგები ინფორმაციის შესახებ.

თანხმობის მოთხოვნა მკაფიოდ უნდა იყოს დიფერენცირებული სხვა საკითხებისგან. თუ ფიზიკური ხელშეკრულება ეხება ბევრ სხვა ასპექტს, რომელიც პერსონალური მონაცემების გამოყენების მიმართ თანხმობის საკითხთან არ არის დაკავშირებული, თანხმობის საკითხი მკაფიოდ უნდა გამოიყოს სხვა საკითხებისგან ან ცალკე დოკუმენტში იქნას წარმოდგენილი. მსგავსად აღნიშნულისა, თუ თანხმობის მოთხოვნა ხდება ელექტრონული საშუალებებით, ეს მოთხოვნა უნდა იყოს ცალკე მდგომი და სხვა საკითხებისგან განცალკევებული. პრეამბულის 32-ე პუნქტის თანახმად, დაუშვებელია ამ მოთხოვნის აბზაცის სახით გათვალისწინება წესებსა და პირობებში.[41] მცირე ზომის ეკრანების შემთხვევაში ან ისეთ სიტუაციებში, სადაც ინფორმაციისთვის გამოყოფილი სივრცე არის შეზღუდული, შესაძლებელია ინფორმაციის წარდგენა მრავალშრიანი ფორმით, საჭიროების შესაბამისად, რათა თავიდან იქნას აცილებული მომხმარებლის გამოცდილების ან პროდუქტის დიზაინის ზედმეტად გადატვირთვა.

72. დამუშავებისთვის პასუხისმგებელი პირი, რომელიც ეყრდნობა მონაცემთა სუბიექტის თანხმობას, აგრეთვე, ვალდებულია შეასრულოს ინფორმაციასთან დაკავშირებული სხვა მოვალეობები, რომელთაც მე-13 და მე-14 მუხლები ითვალისწინებს, რათა უზრუნველყოს GDPR-თან შესაბამისობა. პრაქტიკაში, ინფორმაციასთან დაკავშირებული ვალდებულებების შესრულება და ინფორმირებული თანხმობის მოთხოვნასთან შესაბამისობა ხშირად განაპირობებს ინტეგრირებულ მიდგომას. ამავდროულად, წინამდებარე სექცია შემუშავებულია იმის გათვალისწინებით, რომ ლეგიტიმური „ინფორმირებული“ თანხმობა შეიძლება არსებობდეს მაშინაც კი, თუ თანხმობის მოპოვების პროცესში დამუშავებისთვის პასუხისმგებელი პირი მე-13 და/ან მე-14 მუხლით გათვალისწინებულ ყველა ელემენტზე არ მიუთითებს (ეს საკითხები, რა თქმა უნდა, სხვა ადგილებში უნდა იქნას მითითებული, მაგალითად, კომპანიის კონფიდენციალურობის განაცხადი). WP29-მ გამოსცა ცალკე სახელმძღვანელო პრინციპები, რომლებიც ეხება გამჭვირვალობის მოთხოვნას.

73. <u>მაგალითი 12:</u> კომპანია X არის დამუშავებისთვის პასუხისმგებელი პირი, რომელმაც მიიღო საჩივრები იმასთან დაკავშირებით, რომ მონაცემთა სუბიექტებისთვის ბუნდოვანია, თუ მონაცემთა გამოყენების რა მიზნებთან მიმართებით სთხოვენ მათ თანხმობას. კომპანიამ გადაწყვიტა, გადაემოწმებინა,

[41] ასევე, იხ. პრეამბულის 42-ე პუნქტი და 93/13/EC დირექტივა, კერძოდ, მე-5 მუხლი (მარტივი, გასაგები ენა, ხოლო ეჭვის შემთხვევაში, ინტერპრეტაცია უნდა განხორციელდეს მომხმარებლის სასარგებლოდ) და მე-6 მუხლი (უსამართლო პირობების არალეგიტიმურობა, ხელშეკრულება არსებობას აგრძელებს ამ პირობების გარეშე მხოლოდ იმ შემთხვევაში, თუ იგი კვლავ კეთილგონივრულია. წინააღმდეგ შემთხვევაში, მთლიანი ხელშეკრულება არის ძალადაკარგული).

თუ რამდენად გასაგებია თანხმობის მოთხოვნაში წარმოდგენილი ინფორმაცია მონაცემთა სუბიექტებისთვის. X-მა ორგანიზება გაუწია მომხმარებელთა სხვადასხვა კატეგორიების ფოკუს-ჯგუფებს და მათ წარუდგინა განახლებული ინფორმაცია თანხმობის შესახებ, რათა გავრცელებამდე ინფორმაცია გაეტესტა აღნიშნულ აუდიტორიასთან. ფოკუს-ჯგუფების წევრები შეირჩნენ დამოუკიდებლობის პრინციპის პატივისცემით და იმ სტანდარტების საფუძველზე, რომელიც უზრუნველყოფს წარმომადგენლობით და მიუკერძოებელ შედეგს. პანელმა მიიღო კითხვარი და მიუთითა, თუ როგორ გაიგო წარმოდგენილი ინფორმაცია და როგორ შეაფასებდნენ ისინი ამ ინფორმაციის გასაგებობას და რელევანტურობას. დამუშავებისთვის პასუხისმგებელი პირი აგრძელებს ტესტირებას მანამ, სანამ ფოკუს-ჯგუფები არ განაცხადებენ, რომ ინფორმაცია არის გასაგები. X-მა ტესტირების შედეგების შესახებ მოამზადა ანგარიში, რომელსაც მომავალში გამოიყენებს საცნობაროდ. ამ მაგალითში წარმოდგენილია, თუ როგორ შეძლო კომპანია X-მა დემონსტრირება იმისა, რომ მონაცემთა სუბიექტები იღებენ მკაფიო ინფორმაციას მანამ, სანამ დაეთანხმებიან პერსონალური მონაცემების დამუშავებას X-ის მიერ.

74. <u>მაგალითი 13:</u> კომპანია ახორციელებს მონაცემების დამუშავებას თანხმობის საფუძველზე. კომპანია იყენებს კონფიდენციალურობის მრავალშრიან პოლიტიკას, რომელიც მოიცავს თანხმობის მოთხოვნას. კომპანია მონაცემთა სუბიექტებს სრულად აწვდის საბაზისო მონაცემებს დამუშავებისთვის პასუხისმგებელი პირის და დამუშავების გათვალისწინებული აქტივობების შესახებ.[42] ამავდროულად, კონფიდენციალურობის პოლიტიკის პირველ საინფორმაციო შრეში კომპანია არ უთითებს, თუ როგორ უნდა დაუკავშირდეს მონაცემთა სუბიექტი მონაცემთა დაცვის ოფიცერს. მე-6 მუხლის შესაბამისად, დამუშავების კანონიერი საფუძვლის მიზნებისთვის, აღნიშნულმა დამუშავებისთვის პასუხისმგებელმა პირმა მოიპოვა ლეგიტიმური „ინფორმირებული“ თანხმობა, იმის მიუხედავად, რომ მონაცემთა დაცვის ოფიცრის საკონტაქტო ინფორმაციას არ აწვდის მონაცემთა სუბიექტს კონფიდენციალურობის პოლიტიკის პირველ საინფორმაციო შრეში, GDPR-ის 13(1)(b) ან 14(1)(b) მუხლების შესაბამისად.

[42] გაითვალისწინეთ, რომ იმ შემთხვევაში, როდესაც დამუშავებისთვის პასუხისმგებელი პირის ვინაობა ან დამუშავების მიზანი კონფიდენციალურობის პოლიტიკის პირველ საინფორმაციო შრეში არ ჩანს (და შემდგომ შრეებშია გათვალისწინებული), დამუშავებისთვის პასუხისმგებელი პირისთვის რთული იქნება, დაადასტუროს, რომ მონაცემთა სუბიექტმა გასცა ინფორმირებული თანხმობა, გარდა იმ შემთხვევისა, თუ დამუშავებისთვის პასუხისმგებელ პირს შეუძლია აჩვენოს, რომ მონაცემთა სუბიექტი თანხმობის გამოხატვამდე გაეცნო ამ ინფორმაციას.

3.4 მონაცემთა სუბიექტის სურვილის მკაფიო გამოხატულება

75. GDPR-ში მკაფიოდ არის აღნიშნული, რომ თანხმობა გადმოცემული უნდა იყოს მონაცემთა სუბიექტის განცხადებით ან აქტიურად გამოხატული მკაფიო ქმედებით, რაც ნიშნავს იმას, რომ თანხმობის გაცემა ყოველთვის უნდა განხორციელდეს აქტიური ქმედების (მოძრაობის) ან განცხადების საშუალებით. ნათელი უნდა იყოს, რომ მონაცემთა სუბიექტი დაეთანხმა კონკრეტულ დამუშავებას.

76. 95/46/EC დირექტივის 2(h) მუხლის თანახმად, თანხმობა არის მონაცემთა სუბიექტის სურვილების გამოხატულება, „რომლითაც მონაცემთა სუბიექტი აღნიშნავს მის თანხმობას მასთან დაკავშირებული პერსონალური მონაცემების დამუშავებაზე.“ GDPR-ის 4(11) მუხლი ეფუძნება ამ განსაზღვრებას და განმარტავს, რომ ლეგიტიმური თანხმობა საჭიროებს *მკაფიო* გამოხატულებას *განცხადების ან აქტიურად გამოხატული მკაფიო ქმედების* გზით, WP29-ის მიერ გამოცემული წინა ინსტრუქციების შესაბამისად.

77. *„აქტიურად გამოხატული მკაფიო ქმედება“* ნიშნავს, რომ მონაცემთა სუბიექტი კონკრეტულ დამუშავებას დაეთანხმა მიზანმიმართული ქმედების განხორციელებით.[43] პრეამბულის 32-ე პუნქტი ადგენს დამატებით ინსტრუქციებს ამასთან დაკავშირებით. თანხმობის მოპოვება შესაძლებელია წერილობითი ან (ჩაწერილი) ზეპირი განცხადებით, მათ შორის, ელექტრონული საშუალებით.

[43] იხ. კომისიის ადმინისტრაციის სამუშაო დოკუმენტი, „ზემოქმედების შეფასება“, დანართი 2, გვ.20 და აგრეთვე, გვ.გვ.105-106: „როგორც WP29-ის დასკვნაშია მითითებული, აუცილებელია განიმარტოს, რომ ლეგიტიმური თანხმობა გულისხმობს იმ მექანიზმების გამოყენებას, რომელიც არ ტოვებს ეჭვს, რომ მონაცემთა სუბიექტის განზრახვა იყო დათანხმება. ამავდროულად, ციფრული გარემოს კონტექსტში, მკაფიოდ უნდა ჩანდეს, რომ ავტომატური პარამეტრების გამოყენება, რომელიც მონაცემთა სუბიექტმა უნდა შეცვალოს იმისათვის, რომ უარი თქვას დამუშავებაზე („თანხმობა დუმილის საფუძველზე“), როგორც ასეთი, არ წარმოადგენს მკაფიო თანხმობას. არამედ, აღნიშნული ფიზიკურ პირს მისცემს მეტ შესაძლებლობას, აკონტროლოს საკუთარი მონაცემები იმ შემთხვევაში, როდესაც დამუშავება ეყრდნობა მის თანხმობას. აღნიშნულს ვერ ექნება მნიშვნელოვანი გავლენა დამუშავებისთვის პასუხისმგებელ პირებზე, რადგან იგი მხოლოდ განმარტავს და უფრო მკაფიოდ წარმოაჩენს მოქმედი დირექტივის შესაძლო შედეგებს, მონაცემთა სუბიექტისგან ლეგიტიმური (ნამდვილი) და რეალური თანხმობის პირობებთან დაკავშირებით. კერძოდ, „ცალსახა“ თანხმობა - რომელიც ანაცვლებს „მკაფიოს“ - განმარტავს თანხმობის მოდალობებს და ხარისხს და იგი მიზნად არ ისახავს იმ შემთხვევებისა და სიტუაციების გაფართოვებას, სადაც (ცალსახა) თანხმობა გამოყენებული უნდა იქნას, როგორც დამუშავების საფუძველი. შესაბამისად, ამ ღონისძიებას დამუშავებისთვის პასუხისმგებელ პირებზე არ ექნება მნიშვნელოვანი გავლენა.“

78. „წერილობითი განცხადების“ კრიტერიუმის დაკმაყოფილების პირდაპირი გზა არის, როდესაც მონაცემთა სუბიექტი წერილით ან იმეილით მიმართავს დამუშავებისთვის პასუხისმგებელ პირს და ზუსტად განმარტავს, თუ რას ეთანხმება. თუმცა, ასეთი რამ, ხშირად არარეალისტურია. GDPR-თან შესაბამისობაში მყოფ წერილობით განცხადებებს, შესაძლოა, ჰქონდეს სხვადასხვა ფორმა და მოცულობა.

79. არსებული (ეროვნული) სახელშეკრულებო კანონმდებლობის დაკნინების გარეშე, თანხმობის მოპოვება შესაძლებელია ჩაწერილი ზეპირი განცხადებით, თუმცა, სათანადოდ უნდა იქნას გათვალისწინებული მონაცემთა სუბიექტისათვის თანხმობის გამოხატვამდე ხელმისაწვდომი ინფორმაცია. წინასწარ მონიშნული თანხმობის გრაფა არალეგიტიმურია GDPR-ის თანახმად. მონაცემთა სუბიექტის დუმილი ან უმოქმედობა, აგრეთვე, უბრალოდ მომსახურების მიღების გაგრძელება ვერ იქნება მიჩნეული, როგორც არჩევანის აქტიური გამოხატულება.

80. <u>მაგალითი 14:</u> პროგრამის ინსტალაციისას, აპლიკაცია მონაცემთა სუბიექტს სთხოვს თანხმობას ხარვეზის შესახებ არა-ანონიმიზებული შეტყობინებების გამოყენებაზე, პროგრამის გასაუმჯობესებლად. თანხმობის მოთხოვნას თან ახლავს კონფიდენციალურობის მრავალშრიანი პოლიტიკა, რომელიც უზრუნველყოფს საჭირო ინფორმაციას. არჩევანის აღმნიშვნელი გრაფის აქტიურად მონიშვნით (გრაფაში მითითებულია „თანახმა ვარ“), მომხმარებელი ადასტურებს თავის ნამდვილ თანხმობას დამუშავების მიმართ, „აქტიურად გამოხატული მკაფიო ქმედების“ განხორციელებით.

81. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს, რომ თანხმობის მოპოვება შეუძლებელია იგივე მოქმედებით, რა მოქმედებითაც მონაცემთა სუბიექტი ეთანხმება ხელშეკრულებას ან მომსახურების მიღების წესებსა და პირობებს. ბლანკეტური თანხმობა ზოგადი წესებისა და პირობების მიმართ ვერ იქნება მიჩნეული აქტიურად გამოხატულ მკაფიო ქმედებად, რომელიც გამოხატავს პერსონალური მონაცემების გამოყენებაზე თანხმობას. GDPR-ი დამუშავებისთვის პასუხისმგებელ პირებს არ აძლევს საშუალებას, რომ მონაცემთა სუბიექტებს შესთავაზოს წინასწარ მონიშნული გრაფები ან დამუშავებაზე უარის თქმის (opt-out) კონსტრუქციები, რომელიც მონაცემთა

სუბიექტის მხრიდან საჭიროებს ინტერვენციას, დათანხმების თავიდან ასაცილებლად (მაგ., „უარის გრაფები“).[44]

82. როდესაც თანხმობის მოთხოვნა ხდება ელექტრონული საშუალებით, ამგვარი მოთხოვნა ხელს არ უნდა უშლიდეს იმ მომსახურების გამოყენებას, რომლისთვისაც თანხმობას იძლევა მონაცემთა სუბიექტი.[45] აქტიურად გამოხატული ქმედება, რომლის საშუალებითაც მონაცემთა სუბიექტი გამოხატავს თანხმობას, საჭიროა იმ შემთხვევაში, როდესაც ნაკლებად შემზღუდავი ან ხელის შემშლელი საშუალებები გამოიწვევს ბუნდოვანებას. ამრიგად, შესაძლოა აუცილებელი იყოს, რომ თანხმობის მოთხოვნა გარკვეულწილად აფერხებდეს მომხმარებლის გამოცდილებას, იმისათვის, რომ მოთხოვნა იყოს ეფექტური.

83. ამავდროულად, GDPR-ის მოთხოვნების ფარგლებში, დამუშავებისთვის პასუხისმგებელ პირებს აქვთ თავისუფლება, შეიმუშაონ თანხმობის მიღების იმგვარი პროცესი, რომელიც შეესაბამება მათი ორგანიზაციის საჭიროებებს. ამ მხრივ, ფიზიკური ქმედებები, შესაძლოა, კვალიფიცირებული იქნას, როგორც აქტიურად გამოხატული მკაფიო ქმედება, GDPR-ის შესაბამისად.

84. დამუშავებისთვის პასუხისმგებელი პირების მიერ შემუშავებული თანხმობის მექანიზმები მონაცემთა სუბიექტებისთვის უნდა იყოს ნათელი. დამუშავებისთვის პასუხისმგებელმა პირებმა თავიდან უნდა აიცილონ ბუნდოვანება და უნდა უზრუნველყონ, რომ ქმედება, რომელიც გამოხატავს თანხმობას, იყოს სხვა ქმედებებისგან გარჩევადი. შესაბამისად, მხოლოდ ვებსაიტის ჩვეულებრივი გამოყენების გაგრძელება არ წარმოადგენს ქმედებას, რომლის საფუძველზეც შესაძლებელია დადგინდეს მონაცემთა სუბიექტის სურვილი, გამოხატოს თავისი თანხმობა დამუშავების შემოთავაზებული ოპერაციის მიმართ.

85. <u>მაგალითი 15:</u> ეკრანზე ღილაკის გაწევა (swiping), ჭკვიანი კამერის წინ ხელის ქნევა, სმარტფონის საათის ისრის მიმართულებით შემობრუნება ან რვიანის მოხაზვა შესაძლოა წარმოადგენდეს თანხმობის აღმნიშვნელ ქმედებას იმ პირობით, რომ მონაცემთა სუბიექტს მიეწოდა მკაფიო ინფორმაცია და ნათელია, რომ აღნიშნული ქმედება (მოძრაობა) ასახავს კონკრეტულ მოთხოვნაზე თანხმობას (მაგ., თუ ღილაკს მარცხნივ გაწევთ, თქვენ დაეთანხმებით X ინფორმაციის Y მიზნისთვის გამოყენებას. გაიმეორეთ მოძრაობა, რათა დაადასტუროთ.“). დამუშავებისთვის

[44] ასევე, იხ. მუხლი 7(2). ასევე, იხ. სამუშაო დოკუმენტი 02/2013 “cookie” ფაილებისთვის თანხმობის მოპოვების შესახებ (WP 208), გვ.გვ. 3-6.

[45] GDPR-ის პრეამბულა, 32-ე პუნქტი.

პასუხისმგებელმა პირმა უნდა შეძლოს დემონსტრირება, რომ თანხმობა ამ გზით იქნა მოპოვებული, ხოლო თანხმობის უკან გახმობა უნდა იყოს ისეთივე ადვილი, როგორც თანხმობის გაცემა.

86. <u>მაგალითი 16:</u> პრეამბულის 32-ე პუნქტის თანახმად, ქმედებები, როგორიცაა სკროლინგი ან სვაიფინგი ვებგვერდზე ან მომხმარებლის მსგავსი აქტივობა ვერც ერთ შემთხვევაში ვერ დააკმაყოფილებს მკაფიო და აქტიურად გამოხატული ქმედების მოთხოვნას: ამგვარი ქმედებები, შესაძლოა, მომხმარებლის სხვა ქმედებისგან ან ინტერაქციისგან ძნელი გასარჩევი იყოს. შესაბამისად, შეუძლებელი იქნება იმის დადგენა, რომ მონაცემთა სუბიექტმა გასცა მკაფიო თანხმობა. ამას გარდა, ასეთ შემთხვევაში, რთული იქნება მომხმარებლისათვის ისეთი საშუალების უზრუნველყოფა, რომლითაც თანხმობის უკან გახმობა იქნება ისეთივე ადვილი, როგორც თანხმობის გაცემა.

87. ციფრულ კონტექსტში, არაერთ მომსახურებას ფუნქციონირებისთვის ესაჭიროება პერსონალური მონაცემები. შესაბამისად, მონაცემთა სუბიექტები თანხმობის რამდენიმე მოთხოვნას იღებენ, რომელთაც მათ ყოველდღიურად პასუხი უნდა გასცენ დაწკაპუნებით თუ ღილაკის გაწევით (სვაიფინგით). აღნიშნული ზოგჯერ მომხმარებლებში იწვევს „დაწკაპუნებით გადაღლას“: თანხმობის მექანიზმების ეფექტურობა იკლებს იმის გამო, რომ მომხმარებელი ძალიან ხშირად ხვდება მათ.

88. შედეგად, წარმოიქმნება სიტუაციები, როდესაც თანხმობის შესახებ კითხვებს მომხმარებლები აღარ კითხულობენ. ეს განსაკუთრებულ რისკს უქმნის მონაცემთა სუბიექტებს, რადგან როგორც წესი, თანხმობის მოთხოვნა ხდება ისეთ ქმედებებთან დაკავშირებით, რომლებიც არსებითად უკანონოა მათი თანხმობის გარეშე. GDPR-ი დამუშავებისთვის პასუხისმგებელ პირებს აკისრებს ვალდებულებას, შეიმუშაონ ამ საკითხის მოგვარების გზები.

89. ონლაინ კონტექსტში ხშირად საუბრობენ მაგალითზე, რომელიც ეხება ინტერნეტ მომხმარებლებისგან თანხმობის მოპოვებას მათი ბრაუზერის პარამეტრების საშუალებით. ასეთი პარამეტრები GDPR-ში წარმოდგენილი ლეგიტიმური თანხმობის პირობების შესაბამისად უნდა შემუშავდეს. მაგალითად, ის, რომ თანხმობა გაცემული უნდა იქნას თითოეულ გათვალისწინებულ მიზანთან დაკავშირებით, ხოლო მონაცემთა სუბიექტისათვის მისაწოდებელი ინფორმაცია უნდა შეიცავდეს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების ვინაობას.

90. ნებისმიერ შემთხვევაში, თანხმობის მოპოვება უნდა მოხდეს მანამ, სანამ დამუშავებისთვის პასუხისმგებელი პირი დაიწყებს იმ პერსონალური მონაცემების დამუშავებას, რისთვისაც საჭიროა თანხმობა. WP29 საკუთარ დასკვნებში მუდმივად აცხადებს, რომ თანხმობა დამუშავების აქტივობამდე უნდა იქნას გაცემული.[46] მართალია, GDPR-ი 4(11) მუხლში პირდაპირ არ ადგენს, რომ თანხმობა დამუშავების აქტივობამდე უნდა იქნას გაცემული, აღნიშნული ცალსახად არის ნაგულისხმევი. აღნიშნულ ინტერპრეტაციას ამყარებს 6(1) მუხლის დასაწყისი და სიტყვა „განაცხადებს“. მე-6 მუხლიდან და პრეამბულის მე-40 პუნქტიდან ლოგიკურად მომდინარეობს, რომ დამუშავების დაწყებამდე წარმოდგენილი უნდა იქნას დამუშავების კანონიერი და ლეგიტიმური საფუძველი. შესაბამისად, თანხმობა მონაცემთა სუბიექტმა უნდა გასცეს დამუშავების აქტივობის დაწყებამდე. არსებითად, საკმარისია მონაცემთა სუბიექტისათვის თანხმობის ერთხელ თხოვნა. ამავდროულად, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა მოიპოვონ ახალი და კონკრეტული თანხმობა იმ შემთხვევაში, თუ მონაცემთა დამუშავების მიზნები შეიცვლება თანხმობის მოპოვების შემდგომ, ან თუ დამატებითი მიზანია გათვალისწინებული.

4. მკაფიო თანხმობის მოპოვება

91. მკაფიო თანხმობა საჭიროა გარკვეულ სიტუაციებში, როდესაც წარმოიშობა მონაცემთა დაცვის სერიოზული საფრთხეები და საჭიროა ხდება პერსონალურ მონაცემებზე მაღალი დონის ინდივიდუალური კონტროლი. GDPR-ის თანახმად, მკაფიო თანხმობა გარკვეულ როლს ასრულებს განსაკუთრებული კატეგორიების მონაცემთა დამუშავებაში (მუხლი 9), დაცვის სათანადო გარანტიების არ არსებობის პირობებში მონაცემების მესამე ქვეყნებისთვის ან საერთაშორისო ორგანიზაციებისათვის გადაცემაში (მუხლი 49)[47] და ავტომატური ინდივიდუალური გადაწყვეტილების მიღებაში, პროფილირების ჩათვლით (მუხლი 48).[48]

[46] WP29-ს აღნიშნულ პოზიციაზეა მას შემდეგ, რაც მან მიიღო 15/2011 დასკვნა თანხმობის განმარტების შესახებ (WP 187), გვ.გვ. 30-31.

[47] GDPR-ის 49(1)(a) მუხლის თანახმად, მკაფიო თანხმობას შეუძლია, გააუქმოს მონაცემთა დაცვის ადეკვატური კანონის არ მქონე ქვეყნებისთვის მონაცემთა გადაცემაზე დაწესებული აკრძალვა. ამასთან, აღსანიშნავია სამუშაო დოკუმენტი 95/46/EC დირექტივის 26(1) მუხლის საერთო ინტერპრეტაციის შესახებ, 1995 წლის 24 ოქტომბერი (WP 114), გვ.11, სადაც WP29 მიუთითებს, რომ მონაცემთა პერიოდულ ან მიმდინარე გადაცემაზე თანხმობა არ არის მიზანშეწონილი.

[48] 22-ე მუხლი შეიცავს დებულებებს, რომლებიც მონაცემთა სუბიექტებს იცავს გადაწყვეტილებების მხოლოდ ავტომატური დამუშავების საფუძველზე მიღებისგან (პროფილირების ჩათვლით). ამ საფუძველზე გადაწყვეტილებების მიღება დასაშვებია გარკვეულ სამართლებრივ პირობებში.

92. GDPR-ის თანახმად, „განცხადება ან აქტიურად გამოხატული მკაფიო ქმედება“ წარმოადგენს „ჩვეულებრივი“ თანხმობის წინაპირობას. „ჩვეულებრივი“ თანხმობის მოთხოვნა GDPR-ში უფრო მაღალ სტანდარტს აღწევს, ვიდრე თანხმობის მოთხოვნა 95/46/EC დირექტივაში. შესაბამისად, საჭიროა განიმარტოს, თუ რა დამატებითი ძალისხმევა უნდა განახორციელოს დამუშავებისთვის პასუხისმგებელმა პირმა, რათა მონაცემთა სუბიექტისგან მიიღოს *მკაფიო* თანხმობა, GDPR-ის მოთხოვნის შესაბამისად.

93. ტერმინი *მკაფიო* მიუთითებს მონაცემთა სუბიექტის მიერ თანხმობის გამოხატვის ფორმას. ეს ნიშნავს იმას, რომ მონაცემთა სუბიექტმა მკაფიოდ უნდა განაცხადოს თანხმობის შესახებ. საჭიროების შემთხვევაში, დამუშავებისთვის პასუხისმგებელმა პირმა, შესაძლოა, უზრუნველყოს წერილობითი განცხადების ხელმოწერა მონაცემთა სუბიექტის მიერ, რათა აღმოიფხვრას ყველა შესაძლო ეჭვი და უზრუნველყოს შესაბამისი მტკიცებულება.[49]

94. ამავდროულად, ამგვარი ხელმოწერილი განცხადება არ წარმოადგენს მკაფიო თანხმობის მოპოვების ერთადერთ გზას და შეუძლებელია იმის თქმა, რომ GDPR-ი წერილობით და ხელმოწერილ განცხადებებს ითხოვს ყველა იმ გარემოებაში, რომელიც საჭიროებს ლეგიტიმურ მკაფიო თანხმობას. მაგალითად, ციფრულ ან ონლაინ კონტექსტში, შესაძლებელია, რომ მონაცემთა სუბიექტმა საჭირო განცხადება გააკეთოს ელექტრონული ფორმის შევსებით, იმეილის გაგზავნით ან მის მიერ ხელმოწერილი სკანირებული დოკუმენტის ატვირთვის გზით ან ელექტრონული ხელმოწერის გამოყენებით. თეორიაში, ზეპირი განცხადება შეიძლება იყოს საკმარისად მკაფიო და ლეგიტიმური. ამავდროულად, შესაძლოა რთული იყოს დამუშავებისთვის პასუხისმგებელი პირისთვის იმის დამტკიცება, რომ განცხადების ჩაწერის დროს ლეგიტიმური თანხმობის ყველა პირობა იყო დაკმაყოფილებული.

95. ორგანიზაციას შეუძლია, მკაფიო თანხმობა მოიპოვოს სატელეფონო საუბრის საშუალებითაც, იმ პირობით, თუ არჩევანის შესახებ ინფორმაცია არის

თანხმობა მნიშვნელოვან როლს ასრულებს დაცვის აღნიშნულ მექანიზმში, რადგან GDPR-ის 22(2)(c) მუხლი მკაფიოდ ადგენს, რომ დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია მონაცემთა სუბიექტის მკაფიო თანხმობით განახორციელოს ავტომატური გადაწყვეტილების მიღება, პროფილირების ჩათვლით, რომელიც მნიშვნელოვან გავლენას ახდენს ფიზიკურ პირზე. WP29-მ მოამზადა ცალკე სახელმძღვანელო პრინციპები ამ საკითხზე: WP29 სახელმძღვანელო პრინციპები ავტომატური გადაწყვეტილების მიღების და პროფილირების შესახებ, 2016/679 რეგულაციის მიზნებისთვის, 2017 წლის 3 ოქტომბერი (WP 251).

[49] ასევე, იხ. WP29 დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP 187), გვ. 25.

სამართლიანი, გასაგები და მკაფიო და იგი მონაცემთა სუბიექტს სთხოვს კონკრეტულ დასტურს (მაგ., ღილაკზე დაჭერა ან ზეპირი დასტური).

96. <u>მაგალითი 17:</u> მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს შეუძლია საკუთარი ვებგვერდის ვიზიტორისგან მოიპოვოს მკაფიო თანხმობა, თუ მას შესთავაზებს ეკრანს მკაფიო თანხმობით, რომელზეც წარმოდგენილი იქნება „კი“ და „არა“ მოსანიშნი გრაფები. ამავდროულად, ტექსტი მკაფიოდ უნდა მიუთითებდეს თანხმობაზე, მაგალითად: „მე ჩემი მონაცემების დამუშავებას ვეთანხმები“ და არა „ჩემთვის ნათელია, რომ მოხდება ჩემი მონაცემების დამუშავება“. ცხადია, რომ სავალდებულოა ინფორმირებული თანხმობის აღნიშნული პირობებისა და ლეგიტიმური თანხმობის მოპოვების სხვა პირობების დაკმაყოფილება.

97. <u>მაგალითი 18:</u> კოსმეტიკური ქირურგიის კლინიკა პაციენტს სთხოვს მკაფიო თანხმობას მისი სამედიცინო ჩანაწერების ექსპერტისთვის გადასაცემად, რომელიც შემდგომ წარმოადგენს დასკვნას პაციენტის მდგომარეობის შესახებ. სამედიცინო ჩანაწერები ციფრული ფაილის ფორმატშია. აღნიშნული ინფორმაციის სპეციფიური ხასიათის გათვალისწინებით, კლინიკა მონაცემთა სუბიექტს სთხოვს ელექტრონულ ხელმოწერას, ლეგიტიმური და მკაფიო თანხმობის მოსაპოვებლად და იმისათვის, რომ მოახდინოს მკაფიო თანხმობის მოპოვების დემონსტრირება.[50]

98. თანხმობის ვერიფიცირების ორეტაპიანი პროცესი ხელს შეუწყობს მკაფიო თანხმობის ლეგიტიმურობის უზრუნველყოფას. მაგალითად, მონაცემთა სუბიექტი ელ-ფოსტით იღებს შეტყობინებას, რომ დამუშავებისთვის პასუხისმგებელი პირი აპირებს, სამედიცინო მონაცემების შემცველი ჩანაწერის დამუშავებას. დამუშავებისთვის პასუხისმგებელი პირი იმეილში განმარტავს, რომ იგი ითხოვს თანხმობას კონკრეტული მონაცემების კონკრეტული მიზნით გამოყენებაზე. მონაცემთა სუბიექტს, რომელიც ეთანხმება ამ მონაცემების გამოყენებას, დამუშავებისთვის პასუხისმგებელი პირი სთხოვს, იმეილს გასცეს პასუხი შემდეგი სიტყვებით: „თანახმა ვარ.“ პასუხის გაგზავნის შემდეგ, მონაცემთა სუბიექტი მიიღებს ვერიფიკაციის ბმულს, რომელსაც უნდა

[50] აღნიშნული მაგალითი არ აკნინებს ევროკავშირის რეგულაციას No.910/2014, რომელიც მიღებულია ევროპარლამენტისა და საბჭოს მიერ, 2014 წლის 23 ივლისს, ელექტრონული იდენტიფიცირებისა და ნდობის სერვისების შესახებ, შიდა ბაზარზე ელექტრონული ტრანზაქციების ჭრილში.

დააწკაპუნოს ან SMS შეტყობინებას ვერიფიკაციის კოდით, რათა დაადასტუროს თანხმობა.

99. 9(2) მუხლი მონაცემთა განსაკუთრებული კატეგორიების დამუშავებაზე ზოგად აკრძალვასთან დაკავშირებით, გამონაკლისის სახით არ ითვალისწინებს „აუცილებელია ხელშეკრულების შესრულებისთვის“. შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირები და მხარე სახელმწიფოები, რომლებიც ამგვარი სიტუაციის წინაშე იმყოფებიან, მათ უნდა გადახედონ სპეციფიურ გამონაკლისებს, რომლებიც წარმოდგენილია 9(2) მუხლის (b) - (j) ქვეპუნქტებში. იმ შემთხვევაში, თუ მოცემულ სიტუაციაზე არ ვრცელდება არც ერთი აღნიშნული გამონაკლისი, GDPR-ით გათვალისწინებული ლეგიტიმური თანხმობის პირობების შესაბამისად მკაფიო თანხმობის მოპოვება რჩება ერთადერთი შესაძლო კანონიერი გამონაკლისი ამგვარი მონაცემების დასამუშავებლად.

100. <u>მაგალითი 18:</u> ავიაკომპანია Holiday Airways მგზავრებს, რომელთაც დამხმარის გარეშე მგზავრობა არ შეუძლიათ (მაგალითად, შეზღუდული შესაძლებლობის გამო), დახმარების სერვისს სთავაზობს. ერთ-ერთმა მომხმარებელმა შეიძინა ამსტერდამი-ბუდაპეშტის ბილეთი და ითხოვა დახმარება თვითმფრინავში ასასვლელად. Holiday Airways-მა მომხმარებელს სთხოვა, წარმოედგინა ინფორმაცია მისი ჯანმრთელობის მდგომარეობის შესახებ, იმისათვის, რომ ავიახაზებს ამ ინფორმაციის საფუძველზე სათანადო სერვისები დაეგეგმა (ეს სერვისები, შესაძლოა, მოიცავდეს, მაგალითად: ეტლით მომსახურებას გასასვლელთან ან დამხმარეს, რომელიც მასთან ერთად იმგზავრებს ამსტერდამიდან ბუდაპეშტამდე). ავიაკომპანიამ მკაფიო თანხმობა ითხოვა მომხმარებლის ჯანმრთელობის მონაცემების დამუშავებაზე, მის მიერ მოთხოვნილი დახმარების უზრუნველყოფის მიზნით. თანხმობის საფუძველზე დამუშავებული მონაცემები აუცილებელი უნდა იყოს მოთხოვნილი მომსახურების გასაწევად. ამასთან, ფრენები ბუდაპეშტში, როგორც წესი, სამგზავრო დახმარების გარეშე ხორციელდება. ამ შემთხვევაში, არ მოქმედებს 7(4) მუხლი, ვინაიდან მონაცემები აუცილებელია მოთხოვნილი მომსახურების გასაწევად.

101. <u>მაგალითი 20:</u> წარმატებული კომპანია მომხმარებლებისთვის უზრუნველყოფს მათზე მორგებულ სათვალეებს თხილამურებზე სრიალისთვის, სნოუბორდისთვის და სხვა სახის სპორტული აქტივობებისთვის, რომლებიც ღია ცის ქვეშ ხორციელდება. იდეა მდგომარეობს იმაში, რომ ადამიანებმა აღნიშნული

სათვალეების ტარება შეძლონ საკუთარი მხედველობის სათვალეების გარეშე. კომპანია შეკვეთებს იღებს ცენტრალურ ოფისში, ხოლო პროდუქტებს აგზავნის მთელი ევროკავშირის მასშტაბით.

102. იმისათვის, რომ კომპანიამ შეძლოს ახლომხედველ მომხმარებლებზე მორგებული პროდუქტის მიწოდება, დამუშავებისთვის პასუხისმგებელი პირი მომხმარებლებს სთხოვს თანხმობას მათი მხედველობის შესახებ ინფორმაციის გამოყენებაზე. მომხმარებლები ონლაინ შეკვეთის განთავსებისას კომპანიას აწვდიან ჯანმრთელობის შესახებ საჭირო მონაცემებს, როგორიცაა, სათვალის რეცეპტი. ამ მონაცემების გარეშე, შეუძლებელია თითოეულ მომხმარებელზე მორგებული სათვალის მიწოდება. კომპანია მომხმარებლებს, აგრეთვე, სთავაზობს სათვალეებს მხედველობის სტანდარტული კორექციით. მომხმარებლებს, რომელთაც არ სურთ საკუთარი ჯანმრთელობის შესახებ მონაცემების გაზიარება, შეუძლიათ სტანდარტული ვერსიები აირჩიონ. შესაბამისად, იმისათვის, რომ თანხმობა ნებაყოფლობითად ჩაითვალოს, იგი უნდა იყოს მკაფიო (მე-9 მუხლის შესაბამისად).

5. ლეგიტიმური თანხმობის მოპოვების დამატებითი პირობები

103. GDPR-ის თანახმად, დამუშავებისთვის პასუხისმგებელ პირებს მოეთხოვებათ დამატებითი ძალისხმევის გაწევა, რათა მათ შეძლონ ლეგიტიმური თანხმობის მოპოვება, შენარჩუნება და დემონსტრირება. GDPR-ის მე-7 მუხლი ადგენს ლეგიტიმური თანხმობის ამ დამატებით პირობებს და შეიცავს კონკრეტულ დებულებებს თანხმობის ჩანაწერების წარმოებისა და თანხმობის უკან ადვილად გახმობის შესახებ. მე-7 მუხლი, აგრეთვე, ვრცელდება GDPR-ის სხვა მუხლებში მითითებულ თანხმობაზე - მაგალითად, მე-8 და მე-9 მუხლებში. სახელმძღვანელო ინსტრუქციები ლეგიტიმური თანხმობის დემონსტრირების დამატებითი მოთხოვნებისა და თანხმობის უკან გახმობის შესახებ წარმოდგენილია ქვემოთ.

5.1 თანხმობის დემონსტრირება

104. 7(1) მუხლში GDPR-ი მკაფიოდ ადგენს დამუშავებისთვის პასუხისმგებელი პირის ცალსახა ვალდებულებას, <u>მოახდინოს მონაცემთა სუბიექტის თანხმობის დემონსტრირება.</u> 7(1) მუხლის შესაბამისად, მტკიცების ტვირთი ეკისრება დამუშავებისთვის პასუხისმგებელ პირს.

105. პრეამბულის 42-ე პუნქტის თანახმად: *„როცა დამუშავება ხდება მონაცემთა სუბიექტის თანხმობის საფუძველზე, დამუშავებისთვის პასუხისმგებელ პირს უნდა შეეძლოს მონაცემთა სუბიექტის მიერ დამუშავების ოპერაციაზე მიცემული თანხმობის დემონსტრირება“.*

106. დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია, ამ დებულებასთან შესაბამისობისთვის შეიმუშაოს იმგვარი მეთოდები, რომლებიც თანხვედრაში იქნება მის ყოველდღიურ ოპერაციებთან. ამავდროულად, დამუშავებისთვის პასუხისმგებელი პირის მიერ ლეგიტიმური თანხმობის მოპოვების დემონსტრირების ვალდებულება, როგორც ასეთი, არ უნდა იწვევდეს დამატებითი მონაცემების დამუშავებას გადაჭარბებული ოდენობით. ეს ნიშნავს, რომ დამუშავებისთვის პასუხისმგებელ პირებს უნდა ჰქონდეთ საკმარისი მონაცემები, რათა დაადასტურონ კავშირი დამუშავებასთან (აჩვენონ, რომ თანხმობა მოპოვებული იქნა), თუმცა, მათ არ უნდა შეაგროვონ საჭიროზე მეტი ინფორმაცია.

107. დამუშავებისთვის პასუხისმგებელ პირზეა დამოკიდებული იმის დადასტურება, რომ მონაცემთა სუბიექტისგან ლეგიტიმური თანხმობა იქნა მოპოვებული. GDPR-ი ზუსტად არ განსაზღვრავს, თუ როგორ უნდა განხორციელდეს ეს. ამავდროულად, დამუშავებისთვის პასუხისმგებელ პირს უნდა შეეძლოს დამტკიცება, რომ მონაცემთა სუბიექტმა მოცემულ შემთხვევაში გასცა თანხმობა. თანხმობის დემონსტრირების ვალდებულება იმოქმედებს იმ ვადით, რა ვადითაც გაგრძელდება მონაცემთა დამუშავების მოცემული აქტივობა. დამუშავების აქტივობის დასრულების შემდეგ, თანხმობის დამადასტურებელი მტკიცებულება არ უნდა იქნას შენახული იმაზე მეტად, ვიდრე ეს მკაცრად აუცილებელია სამართლებრივი ვალდებულების შესასრულებლად ან სამართლებრივი პრეტენზიების დადგენის, განხორციელებისა და დაცვისთვის, 17(3) მუხლის (b) და (e) პუნქტების შესაბამისად.

108. მაგალითად, დამუშავებისთვის პასუხისმგებელ პირს უფლება აქვს, აწარმოოს მიღებული თანხმობის განცხადებების ჩანაწერი, რათა მან შეძლოს ჩვენება, თუ როგორ და როდის მოხდა თანხმობის მოპოვება და წარმოადგინოს, თუ რა ინფორმაცია მიაწოდა მონაცემთა სუბიექტს იმ მომენტში. დამუშავებისთვის პასუხისმგებელმა პირმა, აგრეთვე, უნდა შეძლოს ჩვენება იმისა, რომ მონაცემთა სუბიექტი იყო ინფორმირებული, ხოლო დამუშავებისთვის პასუხისმგებელი პირის სამუშაო პროცესები აკმაყოფილებს ლეგიტიმური თანხმობის ყველა რელევანტურ კრიტერიუმს. აღნიშნული ვალდებულება მოქმედებს იმის გათვალისწინებით, რომ GDPR-ის თანახმად, დამუშავებისთვის პასუხისმგებელი პირები ანგარიშვალდებულები არიან მონაცემთა სუბიექტებისგან ლეგიტიმური

თანხმობის მოპოვების კუთხით და თანხმობის იმ მექანიზმებთან დაკავშირებით, რომლებიც მათ დანერგეს. მაგალითად, ონლაინ კონტექსტში, დამუშავებისთვის პასუხისმგებელ პირს შეუძლია, შეინახოს ინფორმაცია იმ სესიის შესახებ, სადაც თანხმობა იქნა გამოხატული, სესიის მიმდინარეობისას, თანხმობასთან დაკავშირებული სამუშაო პროცესების დოკუმენტაციასთან ერთად, და იმ ინფორმაციის ასლი, რომელიც იმ მომენტში წარედგინა მონაცემთა სუბიექტს. საკმარისი არ არის მხოლოდ შესაბამისი ვებსაიტის სწორ კონფიგურაციაზე მითითება.

109. <u>მაგალითი 21:</u> საავადმყოფომ შექმნა სამეცნიერო კვლევის პროგრამა, სახელწოდებით „პროექტი X“, რომლის განხორციელებაც საჭიროებს რეალური პაციენტების სტომატოლოგიურ ჩანაწერებს. მონაწილეების რეკრუტირება ხდება სატელეფონო ზარების განხორციელებით, ხოლო პაციენტები ნებაყოფლობით ეთანხმებიან იმ კანდიდატთა სიაში გათვალისწინებას, რომელსაც საავადმყოფო აღნიშნული მიზნით დაუკავშირდება. დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტებს სთხოვს მკაფიო თანხმობას მათი სტომატოლოგიური ჩანაწერების გამოყენებაზე. თანხმობის მოპოვება ხდება სატელეფონო ზარის დროს, მონაცემთა სუბიექტის ზეპირი განცხადების ჩაწერის გზით, ხოლო ზეპირ განცხადებაში მონაცემთა სუბიექტი ადასტურებს, რომ იგი ეთანხმება საკუთარი მონაცემების „პროექტი X“-ის მიზნებისთვის გამოყენებას.

110. თანხმობის მოქმედებასთან დაკავშირებით, GDPR-ი არ ითვალისწინებს რაიმე კონკრეტულ ვადებს. თანხმობის მოქმედების ვადა დამოკიდებულია თავდაპირველი თანხმობის კონტექსტზე, მოქმედების ფარგლებზე და მონაცემთა სუბიექტის მოლოდინებზე. თუ დამუშავებასთან დაკავშირებული ოპერაციები მნიშვნელოვნად შეიცვლება ან განვითარდება, მაშინ თავდაპირველი თანხმობა აღარ იქნება ნამდვილი (ლეგიტიმური). ამ შემთხვევაში, საჭიროა ახალი თანხმობის მოპოვება.

111. EDPB რეკომენდაციის თანახმად, საუკეთესო პრაქტიკას წარმოადგენს სათანადო პერიოდულობით თანხმობის განახლება. ყველა ინფორმაციის მიწოდება მონაცემთა სუბიექტს ეხმარება, იყოს კარგად ინფორმირებული იმის შესახებ, თუ როგორ მოხდება მათი მონაცემების გამოყენება და როგორ განახორციელებენ ისინი თავიანთ უფლებებს.[51]

[51] იხ. 29-ე მუხლის სამუშაო ჯგუფის სახელმძღვანელო პრინციპები გამჭვირვალობის შესახებ, 2016/679 რეგულაციის თანახმად, WP 260 rev.01 - აღიარებულია EDPB-ის მიერ.

5.2 თანხმობის უკან გახმობა

112. თანხმობის უკან გახმობას GDPR-ში განსაკუთრებული ადგილი ეთმობა. დებულებები და პრეამბულის პუნქტები თანხმობის უკან გახმობის შესახებ შესაძლოა მიჩნეული იქნას, როგორც WP29-ის დასკვნებში ამ საკითხის არსებული ინტერპრეტაციის კოდიფიცირება.[52]

113. GDPR-ის 7(3) მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს, რომ მონაცემთა სუბიექტმა თანხმობის უკან გახმობა შეძლოს ისევე ადვილად, როგორც გაცემა. GDPR-ი არ ადგენს, რომ თანხმობის გაცემა და უკან გახმობა ყოველთვის ერთი და იგივე მოქმედების საშუალებით უნდა განხორციელდეს.

114. ამავდროულად, როდესაც თანხმობის მოპოვება ხდება ელექტრონული საშუალებით, მაუსის ერთი დაწკაპუნებით, ღილაკის გაწევით ან ღილაკზე დაჭერით, მონაცემთა სუბიექტებისთვის, პრაქტიკაში, თანხმობის უკან გახმობაც ასეთივე ადვილი უნდა იყოს. როდესაც თანხმობის მოპოვება ხდება მომსახურებისადმი სპეციფიური მომხმარებლის ინტერფეისის საშუალებით (მაგ., ვებსაიტით, აპლიკაციით, რეგისტრირებული პროფილით, საგანთა ინტერნეტში ჩართული მოწყობილობის ინტერფეისით ან იმეილით), მაშინ ეჭვგარეშეა, რომ მონაცემთა სუბიექტმა უნდა შეძლოს თანხმობის უკან გახმობა იგივე ელექტრონული ინტერფეისის საშუალებით, რადგან სხვა ინტერფეისზე გადასვლა მხოლოდ და მხოლოდ თანხმობის უკან გახმობის მიზნით, ზედმეტ ძალისხმევას მოითხოვს. ამას გარდა, მონაცემთა სუბიექტს უნდა შეეძლოს საკუთარი თანხმობის უკან გახმობა ისე, რომ მას არ მიადგეს რაიმე ზიანი. ეს ნიშნავს, მათ შორის, იმას, რომ დამუშავებისთვის პასუხისმგებელმა პირმა თანხმობის უკან გახმობა უნდა გახადოს უფასო ან თანხმობის უკან გახმობა არ უნდა იწვევდეს მომსახურების დონის შემცირებას.[53]

[52] WP29 აღნიშნულ საკითხს განიხილავს თანხმობის შესახებ დასკვნაში (იხ. დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP 187), გვ.გვ. 13, 20, 27 da 32-33) და, მათ შორის, დასკვნა ადგილმდებარეობის აღმნიშვნელი მონაცემების გამოყენების შესახებ. (იხ. დასკვნა 5/2005 ადგილმდებარეობის აღმნიშვნელი მონაცემების გამოყენების შესახებ, დამატებითი ღირებულების მქონე სერვისების უზრუნველყოფის მიზნით (WP 115, გვ.7).

[53] ასევე, იხ. დასკვნა WP29 4/2010 FEDMA-ს ევროპული ქცევის კოდექსის შესახებ, პირდაპირი მარკეტინგის მიზნებისთვის პერსონალური მონაცემების გამოყენებასთან დაკავშირებით (WP 174) და დასკვნა ადგილმდებარეობის აღმნიშვნელი მონაცემების გამოყენების შესახებ, დამატებითი ღირებულების მომსახურების უზრუნველყოფის მიზნით (WP 115).

115. <u>მაგალითი 22:</u> მუსიკის ფესტივალის ბილეთები იყიდება ონლაინ მოვაჭრის საშუალებით. თითოეულ გაყიდულ ბილეთთან დაკავშირებით, აგენტი ითხოვს თანხმობას საკონტაქტო მონაცემების მარკეტინგული მიზნებისთვის გამოსაყენებლად. ამ მიზნით თანხმობის გამოსახატავად, მომხმარებლები ირჩევენ პასუხს: „კი“ ან „არა“. დამუშავებისთვის პასუხისმგებელი პირი მომხმარებლებს აწვდის ინფორმაციას, რომ მათ აქვთ თანხმობის უკან გახმობის შესაძლებლობა. ამ მიზნით, მათ შეუძლიათ დაუკავშირდნენ ქოლცენტრს, სამუშაო დღეებში, დილის 8 საათიდან საღამოს 5 საათამდე, ხოლო ზარის განხორციელება უფასოა. მოცემულ მაგალითში, დამუშავებისთვის პასუხისმგებელი პირი არ ასრულებს GDPR-ის 7(3) მუხლით დადგენილ მოთხოვნას. თანხმობის უკან გახმობა საჭიროებს სატელეფონო ზარის განხორციელებას სამუშაო საათებში, რაც უფრო მეტ ძალისხმევას მოითხოვს, ვიდრე მაუსით ერთი დაწკაპუნება, რაც ონლაინ მოვაჭრისთვის თანხმობის მისაცემად იყო საჭირო, ხოლო ონლაინ მოვაჭრე მუშაობს დღეში 24 საათი, კვირაში 7 დღე.

116. თანხმობის უკან მარტივად გახმობის მოთხოვნა წარმოადგენს GDPR-ით გათვალისწინებული ლეგიტიმური (ნამდვილი) თანხმობის განუყოფელ ასპექტს. თუ უკან გახმობის უფლება ვერ აკმაყოფილებს GDPR-ის მოთხოვნებს, ეს ნიშნავს, რომ დამუშავებისთვის პასუხისმგებელი პირის თანხმობის მექანიზმი არ არის GDPR-თან შესაბამისობაში. როგორც ეს მითითებულია 3.1 სექციაში, ინფორმირებული თანხმობის პირობასთან დაკავშირებით, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტს განუმარტოს თანხმობის უკან გახმობის უფლება მანამ, სანამ მონაცემთა სუბიექტი გასცემს თანხმობას, GDPR-ის 7(3) მუხლის შესაბამისად. ამას გარდა, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გამჭვირვალობის ვალდებულების ფარგლებში, უზრუნველყოს მონაცემთა სუბიექტების ინფორმირება მათი უფლებების განხორციელების გზებზე.[54]

117. როგორც წესი, თუ ხდება თანხმობის უკან გახმობა, მონაცემთა დამუშავების ყველა ოპერაცია, რომელიც თანხმობას ეფუძნებოდა და თანხმობის უკან გახმობამდე განხორციელდა - GDPR-თან შესაბამისად - ინარჩუნებს ლეგიტიმურობას; ამავდროულად, დამუშავებისთვის პასუხისმგებელი პირი

[54] GDPR-ის პრეამბულის 39-ე პუნქტი, რომელიც მიუთითებს ამავე რეგულაციის მე-13 და მე-14 მუხლებზე, აცხადებს, რომ *„ფიზიკურ პირებს უნდა გააცნონ პერსონალური მონაცემების დამუშავებასთან დაკავშირებული რისკები, წესები, დაცვის მექანიზმები და უფლებები და მათი უფლებების რეალიზების გზები.“*

ვალდებულია, შეწყვიტოს დამუშავების შესაბამისი აქტივობები. თუ აღარ არსებობს მონაცემთა დამუშავების (მაგ., შემდგომი შენახვა) სხვა საფუძველი, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემები უნდა წაშალოს.[55]

118. როგორც წინამდებარე გაიდლაინებში იქნა აღნიშნული, უაღრესად მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა შეაფასოს მიზეზები, რისთვისაც რეალურად ხდება მონაცემების დამუშავება და კანონიერი საფუძვლები, რომელსაც ეყრდნობა იგი, მანამ, სანამ განახორციელებს მონაცემთა შეგროვებას. ხშირად, კომპანიებს პერსონალური მონაცემები სხვადასხვა მიზნებისთვის ესაჭიროებათ, ხოლო დამუშავება ერთზე მეტ კანონიერ საფუძველს ეყრდნობა, მაგ., მომხმარებელთა შესახებ მონაცემები, შესაძლოა, ეფუძნებოდეს ხელშეკრულებას ან თანხმობას. ამრიგად, თანხმობის უკან გახმობა არ ნიშნავს, რომ დამუშავებისთვის პასუხისმგებელმა პირმა უნდა წაშალოს მონაცემები, რომელთა დამუშავებაც ხდება მონაცემთა სუბიექტთან გაფორმებული ხელშეკრულების შესრულების მიზნისთვის. ამრიგად, დამუშავებისთვის პასუხისმგებელმა პირებმა თავიდანვე მკაფიოდ უნდა განსაზღვრონ, თუ რომელი მიზანი ვრცელდება მონაცემთა თითოეულ ელემენტზე და რომელ კანონიერი საფუძველს ეყრდნობა თითოეული ელემენტის დამუშავება.

119. თანხმობის უკან გახმობის შემდეგ დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, წაშალოს მონაცემები, რომლებიც დამუშავდა თანხმობის საფუძველზე, იმ შემთხვევაში, თუ მონაცემთა შენახვის გასაგრძელებლად არ არსებობს რაიმე სხვა საფუძველი.[56] გარდა ამ სიტუაციისა, რომელსაც 17(1)(b) მუხლი მოიცავს, ინდივიდუალურ მონაცემთა სუბიექტს უფლება აქვს, მოითხოვოს მის შესახებ მონაცემების წაშლა, რომელიც მუშავდება სხვა კანონიერ საფუძველზე დაყრდნობით, მაგ., 6(1)(b) მუხლის საფუძველზე.[57] დამუშავებისთვის პასუხისმგებელი პირები ვალდებულები არიან, შეაფასონ, თუ რამდენად მიზანშეწონილია მონაცემთა უწყვეტი დამუშავება, მონაცემთა სუბიექტის მიერ წაშლის მოთხოვნის არ არსებობის პირობებშიც.[58]

120. როდესაც მონაცემთა სუბიექტს უკან მიაქვს თავისი თანხმობა, ხოლო დამუშავებისთვის პასუხისმგებელ პირს სურვილი აქვს, გააგრძელოს

[55] იხ. GDPR-ის მე-17 მუხლის (1)(b) და (3) პუნქტები.

[56] ამ შემთხვევაში, სხვა მიზანს, რომელსაც ეყრდნობა დამუშავება, თავისი სამართლებრივი საფუძველი უნდა ჰქონდეს. ეს არ ნიშნავს, რომ დამუშავებისთვის პასუხისმგებელ პირს შეუძლია თანხმობა სხვა კანონიერი საფუძვლით ჩაანაცვლოს, იხ. სექცია 6 ქვემოთ.

[57] იხ. GDPR-ის მე-17 მუხლი, მათ შორის, გამონაკლისები, რომლებიც შეიძლება მოქმედებდეს, და პრეამბულის 56-ე პუნქტი.

[58] იხ. GDPR-ის 5(1)(e) მუხლი.

პერსონალური მონაცემების დამუშავება სხვა კანონიერ საფუძველზე დაყრდნობით, დაუშვებელია (უკან გამოხმობილი) თანხმობიდან ჩუმად სხვა კანონიერ საფუძველზე გადასვლა. დამუშავების კანონიერი საფუძვლის ცვლილების შესახებ დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს უნდა შეატყობინოს მე-13 და მე-14 მუხლებით გათვალისწინებული მოთხოვნების შესაბამისად და გამჭვირვალობის ზოგადი პრინციპის საფუძველზე.

6. თანხმობის მიმართება რეგულაციის მე-6 მუხლით გათვალისწინებულ სხვა კანონიერ საფუძვლებთან

121. მე-6 მუხლი ადგენს პერსონალური მონაცემების კანონიერად დამუშავების პირობებს და აღწერს ექვს კანონიერ საფუძველს, რომელსაც შესაძლებელია, რომ დამუშავებისთვის პასუხისმგებელი პირი დაეყრდნოს. აღნიშნული ექვსი საფუძვლიდან რომელიმეს გამოყენება უნდა დადგინდეს დამუშავების აქტივობის დაწყებამდე და კონკრეტულ მიზანთან მიმართებით.[59]

122. მნიშვნელოვანია აღინიშნოს, რომ თუ დამუშავებისთვის პასუხისმგებელი პირი აირჩევს, რომ დაეყრდნოს თანხმობას დამუშავების რომელიმე ნაწილთან მიმართებით, იგი მზად უნდა იყოს, პატივი სცეს ამ არჩევანს და შეწყვიტოს დამუშავების ეს ნაწილი, თუ ფიზიკური პირი უკან წაიღებს თანხმობას. შეტყობინების გაგზავნა, რომ მონაცემების დამუშავება მოხდება თანხმობის საფუძველზე მაშინ, როდესაც რეალურად დამუშავებისთვის პასუხისმგებელი პირი ეყრდნობა სხვა საფუძველს, წარმოადგენს ფუნდამენტურ უსამართლობას ფიზიკური პირების მიმართ.

123. სხვა სიტყვებით რომ ვთქვათ, დამუშავებისთვის პასუხისმგებელი პირი თანხმობას ვერ ჩაანაცვლებს დამუშავების სხვა საფუძვლით. მაგალითად, დაუშვებელია დამუშავების საფუძვლად ლეგიტიმური ინტერესის რეტროსპექტიული გამოყენება მას შემდეგ, რაც დამუშავებისთვის პასუხისმგებელი პირი წააწყდება გარკვეულ პრობლემებს თანხმობის ლეგიტიმურობასთან დაკავშირებით. ვინაიდან დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაამჟღავნოს კანონიერი საფუძველი, რომელსაც იგი ეყრდნობა პერსონალური მონაცემების შეგროვების

[59] 13(1)(c) და/ან 14(1)(c) მუხლების თანახმად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, აღნიშნულის შესახებ მონაცემთა სუბიექტს შეატყობინოს.

მომენტისთვის, დამუშავებისთვის პასუხისმგებელმა პირმა შეგროვებამდე წინასწარ უნდა გადაწყვიტოს, თუ რა წარმოადგენს შესაბამის კანონიერ საფუძველს.

7. სფეროები, რომელთაც GDPR-ი განსაკუთრებულ ყურადღებას უთმობს

7.1 არასრულწლოვნები (მუხლი 8)

124. ამჟამინდელ დირექტივასთან შედარებით, GDPR-ი ქმნის დაცვის დამატებით შრეს მოწყვლადი ფიზიკური პირების, განსაკუთრებით, ბავშვების მონაცემების დამუშავებასთან დაკავშირებით. მე-8 მუხლი ითვალისწინებს დამატებით ვალდებულებებს, რათა საინფორმაციო საზოგადოების მომსახურებასთან მიმართებით, უზრუნველყოფილი იქნას გაძლიერებული დაცვა ბავშვების შემთხვევაში. გაძლიერებული დაცვის მიზეზები პრეამბულის 38-ე პუნქტშია მითითებული: *„[...] მათთვის შესაძლოა ნაკლებად იყოს ცნობილი ის რისკები, შედეგები, დაცვის მექანიზმები და მათი უფლებები, რომლებიც უკავშირდება პერსონალური მონაცემების დამუშავებას.“* პრეამბულის 38-ე პუნქტი, აგრეთვე, უთითებს: *„კერძოდ, ამგვარი განსაკუთრებული დაცვა უნდა შეეხოს არასრულწლოვნების პერსონალური მონაცემების გამოყენებას მარკეტინგის მიზნებისთვის ან პიროვნების ან მომხმარებლის პროფილის შექმნას და არასრულწლოვნებთან დაკავშირებული პერსონალური მონაცემების შეგროვებას ისეთი მომსახურების გამოყენებისას, რომლის შეთავაზებაც არასრულწლოვანისათვის პირდაპირ ხდება მშობლის უფლების მქონე პირის თანხმობა არ არის საჭირო არასრულწლოვნებისთვის პრევენციული ან საკონსულტაციო მომსახურების პირდაპირ შეთავაზების შემთხვევაში.“* სიტყვის „კერძოდ“ გამოყენება მიანიშნებს, რომ სპეციფიური დაცვა არ შემოიფარგლება მხოლოდ მარკეტინგითა და პროფილირებით, არამედ, მოიცავს ზოგადად, „ბავშვებთან დაკავშირებით პერსონალური მონაცემების შეგროვებას.“

125. 8(1) მუხლის თანახმად, იმ შემთხვევებში, სადაც გამოიყენება თანხმობა, საინფორმაციო საზოგადოების მომსახურების პირდაპირ ბავშვისათვის შეთავაზებასთან დაკავშირებით, არასრულწლოვნის პერსონალური მონაცემების დამუშავება კანონიერია, თუ არასრულწლოვანს მიღწეული აქვს 16 წლის ასაკისთვის. თუ არასრულწლოვანს არ მიუღწევია 16 წლისთვის, ამგვარი დამუშავება კანონიერია მხოლოდ იმ შემთხვევაში და იმდენად, რამდენადაც დამუშავებაზე თანხმობა გაცემულია ან დამუშავება ნებადართულია ბავშვზე

მშობლის უფლების მქონე პირის მიერ.[60] რაც შეეხება ლეგიტიმური თანხმობის ასაკობრივ ზღვარს, GDPR-ი ითვალისწინებს გარკვეულ მოქნილობას. კერძოდ, მხარე სახელმწიფოებს შეუძლიათ, კანონით დაადგინონ უფრო დაბალი ასაკი, თუმცა, ეს ასაკი არ უნდა იყოს 13 წელზე ნაკლები.

126. როგორც ინფორმირებული თანხმობის შესახებ 3.1 სექციაშია აღნიშნული, ინფორმაცია გასაგები უნდა იყოს იმ აუდიტორიისთვის, რომელსაც დამუშავებისთვის პასუხისმგებელი პირი მიმართავს, ხოლო განსაკუთრებული ყურადღება უნდა მიექცეს არასრულწლოვნის მდგომარეობას. იმისათვის, რომ „ინფორმირებული თანხმობა“ იქნას მოპოვებული ბავშვისგან, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მას განუმარტოს ბავშვისათვის მკაფიო და მარტივ ენაზე, თუ როგორ აპირებს იგი შეგროვებული მონაცემების დამუშავებას.[61] თუ თანხმობა უნდა გასცეს მშობელმა, მაშინ სავარაუდოდ საჭირო იქნება ის ინფორმაცია, რომელიც ზრდასრულებს საშუალებას აძლევს მიიღონ ინფორმირებული გადაწყვეტილება.

127. ზემოაღნიშნულიდან ნათელია, რომ მე-8 მუხლი ვრცელდება მხოლოდ იმ შემთხვევაში, როდესაც დაკმაყოფილებულია ქვემოთ წარმოდგენილი პირობები:

[60] ისე, რომ არ მიადგეს ზიანი მხარე სახელმწიფოში მოქმედი ეროვნული კანონმდებლობის შესაძლებლობას, გადაუხვიოს ასაკობრივი ზღვარიდან, იხ. მუხლი 8(1).

[61] GDPR-ის პრეამბულის 58-ე პუნქტი განამტკიცებს ამ ვალდებულებას და აცხადებს, რომ საჭიროების შესაბამისად, დმამუშავებელმა უნდა უზრუნველყოს, რომ მიწოდებული ინფორმაცია არასრულწოვნებისთვის არის გასაგები.

- დამუშავება დაკავშირებულია საინფორმაციო საზოგადოების მომსახურების პირდაპირ ბავშვისათვის შეთავაზებასთან.[62] [63]

- დამუშავება ეფუძნება თანხმობას.

7.1.1 საინფორმაციო საზოგადოების მომსახურება

128. ტერმინის „საინფორმაციო საზოგადოების მომსახურების“ მოქმედების ფარგლების დასადგენად, GDPR-ის 4(25) მუხლი მიუთითებს 2015/1535 დირექტივაზე.

129. აღნიშნული განმარტების მოქმედების სფეროს შეფასებისას, EDPB აგრეთვე, მიუთითებს ECJ-ის პრეცედენტულ სამართალზე.[64] ECJ-მ დაადგინა, რომ საინფორმაციო საზოგადოების მომსახურება მოიცავს ხელშეკრულებებს და სხვა სერვისებს, რომელთა შესრულება ან გადაცემა ხდება ონლაინ. როდესაც მომსახურებას აქვს ეკონომიკური თვალსაზრისით ორი

[62] GDPR-ის 4(25) მუხლის თანახმად, საინფორმაციო საზოგადოების მომსახურება ნიშნავს მომსახურებას, რომელსაც განმარტავს 2015/1535 დირექტივის 1(1) მუხლის (b) პუნქტი: *„b) 'მომსახურება' აღნიშნავს საინფორმაციო საზოგადოების ნებისმიერ მომსახურებას, ე.ი., ნებისმიერ მომსახურებას, რომელიც უზრუნველყოფილია ანაზღაურების სანაცვლოდ, დისტანციურად, ელექტრონული საშუალებებით და მომსახურების მიმღების ინდივიდუალური მოთხოვნის საფუძველზე. ამ განმარტების მიზნებისთვის: (i) 'დისტანციურად' აღნიშნავს მომსახურების მიწოდებას ისე, რომ მხარეები ერთდროულად არ იმყოფებიან ერთსა და იმავე ადგილას; (ii) 'ელექტრონული საშუალებით' ნიშნავს, რომ მომსახურების თავდაპირველად გაგზავნა და დანიშნულების ადგილას მიღება ხდება მონაცემთა დამუშავების (მათ შორის, ციფრული კომპრესიის) და შენახვისთვის განკუთვნილი ელექტრონული მოწყობილობის საშუალებით, და მომსახურების სრულად გადაცემა, გამოხატვა და მიღება ხდება კაბელით, რადიოთი, ოპტიკური საშუალებებით ან სხვა ელექტრომაგნეტური საშუალებებით; (iii) „მომსახურების მიმღების ინდივიდუალური მოთხოვნის საფუძველზე“ ნიშნავს, რომ მომსახურების მიწოდება ხორციელდება ინდივიდუალური მოთხოვნის საფუძველზე მონაცემების გადაცემით“.* აღნიშნული განმარტებით მოცული მომსახურებების ჩამონათვალი წარმოდგენილია დირექტივის I დანართში. აგრეთვე, იხ. 2000/31 დირექტივის პრეამბულა, მე-18 პუნქტი.

[63] გაეროს ბავშვის დაცვის კონვენციის 1-ლი მუხლის თანახმად, „[...] ბავშვად ითვლება ყოველი ადამიანი სანამ 18 წლის ასაკს მიაღწევდეს, თუ კანონით, რომელიც ამ ბავშვისადმი გამოიყენება, ის უფრო ადრე არ აღწევს სრულწლოვანებას“, იხ. გაეროს გენერალური ასამბლეის 1989 წლის 20 ნოემბრის 44/25 რეზოლუცია (კონვენცია ბავშვის უფლებების შესახებ).

[64] იხ. მართლმსაჯულების ევროპული სასამართლო, 2010 წლის 2 დეკემბერი, საქმე C-108/09, (Ker-Optika), პუნქტები 22 და 28. „კომპოზიტურ სერვისებთან“ დაკავშირებით, EDPB, აგრეთვე, მიუთითებს C-434/15 საქმეზე (Asociacion Profesional Elite Taxi v Uber Systems Spain SL), პუნქტი 40, რომლის თანახმადაც საინფორმაციო საზოგადოების მომსახურება, რომელიც განუყოფელი ნაწილია იმ ზოგადი მომსახურებისა, რომლის ძირითად კომპონენტს არ წარმოადგენს საინფორმაციო საზოგადოების მომსახურება (ამ შემთხვევაში, სატრანსპორტო მომსახურება), არ უნდა იქნას კვალიფიცირებული, როგორც „საინფორმაციო საზოგადოების მომსახურება“.

ურთიერთდამოკიდებული კომპონენტი, საიდანაც ერთ-ერთი ონლაინ კომპონენტია, როგორიცაა, შეთავაზება ან შეთავაზების მიღება ხელშეკრულების გაფორმების კონტექსტში ან პროდუქტებისა თუ სერვისების შესახებ ინფორმაცია, მათ შორის, მარკეტინგული აქტივობები, ეს კომპონენტი განისაზღვრება, როგორც საინფორმაციო საზოგადოების მომსახურება, ხოლო მეორე კომპონენტი კი არის ფიზიკური მიწოდება და დისტრიბუცია პროდუქტების, რომლებსაც არ მოიცავს საინფორმაციო საზოგადოების მომსახურების ცნება. მომსახურების ონლაინ მიწოდება ხვდება ტერმინის „საინფორმაციო საზოგადოების მომსახურება“ ფარგლებში, რომელსაც ითვალისწინებს GDPR-ის მე-8 მუხლი.

7.1.2 პირდაპირ არასრულწლოვნისთვის შეთავაზება

130. სიტყვების *„პირდაპირ არასრულწლოვნისთვის შეთავაზება“* გამოყენება მიუთითებს, რომ მე-8 მუხლი ვრცელდება არა ყველა საინფორმაციო საზოგადოების მომსახურებაზე, არამედ, ზოგიერთ მათგანზე. ამ მხრივ, თუ საინფორმაციო საზოგადოების მომსახურების მიმწოდებელი მკაფიოდ განუმარტავს პოტენციურ მომხმარებლებს, რომ იგი მომსახურებას სთავაზობს მხოლოდ 18 ასაკს მიღწეულ პირებს, ხოლო საწინააღმდეგოზე არ მეტყველებს სხვა მტკიცებულება (მაგ., საიტის შინაარსი ან მარკეტინგული გეგმები), მაშინ არ ჩაითვლება, რომ მომსახურების შეთავაზება ხდება „პირდაპირ არასრულწლოვნისთვის“ და არ გავრცელდება მე-8 მუხლი.

7.1.3 ასაკი

131. GDPR-ი მიუთითებს, რომ *„წევრი სახელმწიფო უფლებამოსილია, კანონმდებლობით დააწესოს უფრო დაბალი ასაკი, მაგრამ არანაკლებ 13 წლისა.“* დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, იყოს ინფორმირებული ეროვნულ დონეზე მოქმედი სხვადასხვა კანონების შესახებ და გაითვალისწინოს, თუ საზოგადოების რომელი ჯგუფი წარმოადგენს მისი მომსახურების სამიზნეს. კერძოდ, აღსანიშნავია, რომ დამუშავებისთვის პასუხისმგებელი პირი, რომელიც უზრუნველყოფს საერთაშორისო (საზღვართშორის) სერვისს, ყოველთვის ვერ დაეყრდნობა მხოლოდ იმ წევრი სახელმწიფოს კანონთან შესაბამისობას, სადაც მას აქვს ძირითადი დაწესებულება, არამედ, საჭირო იქნება, რომ უზრუნველყოს იმ თითოეული წევრი სახელმწიფოს ეროვნულ კანონებთან შესაბამისობა, სადაც იგი ახორციელებს საინფორმაციო საზოგადოების (ერთი ან რამდენიმე) მომსახურების შეთავაზებას. აღნიშნული დამოკიდებულია იმაზე, თუ რომელ ადგილს აირჩევს წევრი სახელმწიფო ამოსავალ წერტილად საკუთარ ეროვნულ კანონმდებლობაში - ადგილს, სადაც მდებარეობს დამუშავებისთვის პასუხისმგებელი პირის ძირითადი დაწესებულება თუ ადგილს, სადაც

ცხოვრობს მონაცემთა სუბიექტი. ამ არჩევანის გაკეთებისას, პირველ რიგში, წევრმა სახელმწიფომ უნდა გაითვალისწინოს არასრულწლოვნის საუკეთესო ინტერესები. სამუშაო ჯგუფი წევრ სახელმწიფოებს ურჩევს, ამ საკითხთან დაკავშირებით მოიძიონ ჰარმონიზებული გადაწყვეტა.

132. როდესაც არასრულწლოვნებისთვის ხდება საინფორმაციო საზოგადოების მომსახურების მიწოდება თანხმობის საფუძველზე, დამუშავებისთვის პასუხისმგებელი პირის მიმართ არსებობს მოლოდინი, რომ იგი განახორციელებს გონივრულ ძალისხმევას, რათა დარწმუნდეს, რომ მომხმარებელი ციფრული ტექნოლოგიების სფეროში თანხმობის მინიმალურ ასაკს მიღწეული პირია, ხოლო აღნიშნული ზომები უნდა იყოს დამუშავების აქტივობების ხასიათისა და მასთან დაკავშირებული რისკების პროპორციული.

133. იმ შემთხვევაში, თუ მომხმარებელი აცხადებს, რომ იგი ციფრული ტექნოლოგიების სფეროში თანხმობის მინიმალურ ასაკს მიღწეული პირია, მაშინ დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია, განახორციელოს შესაბამისი ზომები, რათა დარწმუნდეს ამ განცხადების სისწორეში. ამავდროულად, GDPR-ი პირდაპირ არ ითვალისწინებს ასაკის შესამოწმებლად გონივრული ძალისხმევის გაწევის საჭიროებას, არამედ, აღნიშნული ირიბი მოთხოვნაა, ვინაიდან თუ ლეგიტიმური თანხმობის ასაკს მიუღწეველი ბავშვი გასცემს თანხმობას საკუთარი სახელით, მაშინ, მონაცემების დამუშავება იქნება უკანონო.

134. თუ მომხმარებელი განაცხადებს, რომ იგი ციფრული ტექნოლოგიების სფეროში თანხმობის მინიმალურ ასაკს მიუღწეველი პირია, მაშინ დამუშავებისთვის პასუხისმგებელ პირს ეს განცხადება შეუძლია მიიღოს დამატებითი შემოწმების გარეშე. ამავდროულად, დამუშავებისთვის პასუხისმგებელმა პირმა შესაბამისი ნებართვა უნდა მოიპოვოს მშობლისგან და უნდა დარწმუნდეს, რომ პირი, რომელიც იძლევა ნებართვას, მშობლის უფლების მქონე პირია.

135. ასაკის შემოწმება არ უნდა იწვევდეს მონაცემთა გადაჭარბებით დამუშავებას. ასაკის შესამოწმებლად არჩეული მექანიზმი უნდა მოიცავდეს დაგეგმილ დამუშავებასთან დაკავშირებული რისკის შეფასებას. ზოგიერთ სიტუაციებში, სადაც რისკი დაბალია, შესაძლოა, მიზანშეწონილი იყოს ახალი გამომწერების მიმართ მოთხოვნის დაწესება, რომლის თანახმადაც მათ უნდა გაამჟღავნონ დაბადების თარიღი ან შეავსონ ფორმა, სადაც მიუთითებენ რომ ისინი (არ) არიან არასრულწლოვნები.[65] ეჭვების წარმოშობის შემთხვევაში, დამუშავებისთვის

[65] ეს ერთ-ერთი მაგალითია და არ წარმოადგენს საშუალებას, რომელიც უზრუნველყოფს ყველა სიტუაციის გადაჭრას.

პასუხისმგებელი პირი ვალდებულია, გადახედოს ასაკის შემოწმების მექანიზმებს მოცემულ შემთხვევაში და გაითვალისწინოს, თუ რამდენად საჭიროა ალტერნატიული შემოწმება.[66]

7.1.4 ბავშვის თანხმობა და მშობლის უფლება

136. მშობლის უფლების მქონე პირის ნებართვასთან დაკავშირებით, GDPR-ი არ აკონკრეტებს პრაქტიკულ საშუალებებს მშობლის თანხმობის მოსაპოვებლად ან იმის დასადგენად, რომ გარკვეულ პირს აქვს ამ მოქმედების განხორციელების უფლებამოსილება.[67] შესაბამისად, EDPB-ის რეკომენდაცია გულისხმობს პროპორციული მიდგომის დანერგვას, GDPR-ის 8(2) და 5(1)(c) მუხლების შესაბამისად (მონაცემთა მინიმიზაცია). პროპორციული მიდგომა, შესაძლოა, მოიცავდეს შეზღუდული მოცულობის ინფორმაციის მოპოვებას, როგორიცაა, პაციენტის ან მეურვის საკონტაქტო მონაცემები.

137. ის, თუ რა წარმოადგენს გონივრულ მიდგომას, როდესაც დამუშავებისთვის პასუხისმგებელი პირი ამოწმებს მომხმარებლის სრულწლოვანებას (თანხმობის გასაცემად) და იმას, თუ რამდენად აქვს მშობლის უფლება პირს, რომელიც გასცემს თანხმობას არასრულწლოვნის სახელით, დამოკიდებულია დამუშავების დამახასიათებელ რისკებზე და ხელმისაწვდომ ტექნოლოგიაზე. დაბალი რისკის შემცველ შემთხვევებში, შესაძლოა საკმარისი იყოს მშობლის უფლების ელ-ფოსტის საშუალებით შემოწმება. მეორეს მხრივ, მაღალი რისკის შემცველ შემთხვევებში მიზანშეწონილია უფრო მეტი დამადასტურებელი მტკიცებულების მოთხოვნა, რათა დამუშავებისთვის პასუხისმგებელმა პირმა შეძლოს ინფორმაციის შემოწმება და შენახვა, GDPR-ის 7(1) მუხლის შესაბამისად.[68] სანდო მესამე მხარის ვერიფიკაციის მომსახურება, შესაძლოა, უზრუნველყოფდეს პრობლემის იმგვარ გადაწყვეტას, რაც ამცირებს იმ პერსონალური მონაცემების მოცულობას, რომელიც დამუშავებისთვის პასუხისმგებელმა პირმა უნდა დაამუშაოს.

---

[66] იხ. WP29 დასკვნა 5/2009 სოციალური ქსელების მომსახურების შესახებ (WP 163).

[67] WP29 აღნიშნავს, რომ ზოგჯერ, მშობლის უფლების მქონე პირი არ წარმოადგენს ბავშვის ბიოლოგიურ მშობელს, ხოლო მშობლის უფლება, შესაძლოა, ჰქონდეს რამდენიმე მხარეს, როგორც იურიდიულ, ისე ფიზიკურ პირებს.

[68] მაგალითად, შესაძლებელია, მშობელს ან მეურვეს ეთხოვოს 0,01 ევროს გადახდა დამუშავებისთვის პასუხისმგებელი პირისთვის, საბანკო გადარიცხვის საშუალებით, ხოლო ტრანზაქციის დანიშნულების ველში მიეთითება, რომ ბანკის ანგარიშის მფლობელი არის მშობლის უფლების მქონე, მომხმარებელთან მიმართებით. საჭიროების შემთხვევაში, უზრუნველყოფილი უნდა იქნას ვერიფიკაციის ალტერნატიული მეთოდი, იმ პირთა დისკრიმინაციული მოპყრობის გამოსარიცხად, რომელთაც არ აქვთ საბანკო ანგარიში.

138. <u>მაგალითი 23:</u> ონლაინ თამაშების პლატფორმას სურს, რომ არასრულწლოვანმა მომხმარებლებმა პლატფორმის სერვისების მიღება შეძლონ მხოლოდ მშობლის ან მეურვის თანხმობის საფუძველზე. დამუშავებისთვის პასუხისმგებელი პირი მისდევს შემდეგ ნაბიჯებს:

139. ნაბიჯი 1: დამუშავებისთვის პასუხისმგებელი პირი მომხმარებელს უსვამს კითხვას, არის თუ არა იგი 16 წელს მიღწეული პირი (ამ შემთხვევაში, ონლაინ ტექნოლოგიების სფეროში მოქმედი მინიმალური ასაკი). თუ მომხმარებელი განაცხადებს, რომ მას აღნიშნული მინიმალური ასაკისთვის არ მიუღწევია:

140. ნაბიჯი 2: დამუშავებისთვის პასუხისმგებელი პირი არასრულწლოვანს ატყობინებს, რომ არასრულწლოვნისთვის მომსახურების მიწოდებამდე საჭიროა, რომ დამუშავებაზე თანხმობა ან ნებართვა გასცეს მშობელმა ან მეურვემ. დამუშავებისთვის პასუხისმგებელი პირი მომხმარებელს სთხოვს, წარმოადგინოს მშობლის ან მეურვის ელ-ფოსტის მისამართი.

141. ნაბიჯი 3: პლატფორმა უკავშირდება მშობელს ან მეურვეს და მოიპოვებს მის თანხმობას დამუშავებაზე, ელ-ფოსტის საშუალებით. პლატფორმა დგამს გონივრულ ნაბიჯებს, რათა დაადასტუროს, რომ ზრდასრულს მართლაც აქვს მშობლის უფლება.

142. ნაბიჯი 4: საჩივრების შემთხვევაში, პლატფორმა დამატებით ნაბიჯებს დგამს, რათა შეამოწმოს გამომწერის ასაკი.

143. თუ პლატფორმა თანხმობასთან დაკავშირებულ სხვა მოთხოვნებს აკმაყოფილებს, თუ აღნიშნულ ნაბიჯებს გადადგამს, იგი შეძლებს, შეასრულოს GDPR-ის მე-8 მუხლით გათვალისწინებული დამატებითი კრიტერიუმები.

144. ამ მაგალითიდან ჩანს, თუ როგორ შეუძლია დამუშავებისთვის პასუხისმგებელ პირს იმის ჩვენება, რომ მან განახორციელა გონივრული ძალისხმევა ლეგიტიმური თანხმობის მოსაპოვებლად, იმ სერვისებთან დაკავშირებით, რომელთა მიწოდებაც ხდება ბავშვისათვის. 8(2) მუხლი კონკრეტულად ადგენს, რომ: *„არსებული ტექნოლოგიების გათვალისწინებით, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მიიღოს გონივრული ზომები, რათა დაადგინოს, არის თუ არა თანხმობა გაცემული ან ნებადართული მშობლის უფლების მქონე პირის მიერ.“*

145. დამუშავებისთვის პასუხისმგებელმა პირმა ყოველ ინდივიდუალურ შემთხვევაში თავად უნდა დაადგინოს, თუ რომელი ზომებია მიზანშეწონილი. ზოგადად, დამუშავებისთვის პასუხისმგებელმა პირმა თავიდან უნდა აიცილოს ვერიფიკაციის იმგვარი გზები, რომლებიც თავის თავში მოიცავენ პერსონალური მონაცემების გადაჭარბებულ შეგროვებას.

146. EDPB ითვალისწინებს, რომ ზოგ შემთხვევაში, ვერიფიკაცია გამოწვევებთან არის დაკავშირებული (მაგ., როდესაც ბავშვს, რომელიც თავად გამოხატავს თანხმობას, არ შეუქმნია „იდენტობის ანაბეჭდი“ ან იმ შემთხვევაში, როდესაც მშობლის უფლების შემოწმება არ არის ადვილი). აღნიშნულის გათვალისწინება შესაძლებელია, როდესაც დამუშავებისთვის პასუხისმგებელი პირი იღებს გადაწყვეტილებას, თუ რომელი ძალისხმევაა გონივრული. ამავდროულად, დამუშავებისთვის პასუხისმგებელი პირის მიმართ არსებობს მოლოდინი, რომ იგი უნდა უზრუნველყოფდეს საკუთარი პროცესებისა და ხელმისაწვდომი ტექნოლოგიების მუდმივად გადახედვას.

147. რაც შეეხება მონაცემთა სუბიექტის ავტონომიას, დაეთანხმოს საკუთარი პერსონალური მონაცემების დამუშავებას და სრულად აკონტროლოს დამუშავება, შესაძლებელია მშობლის უფლების მქონე პირის მიერ ბავშვის პერსონალური მონაცემების დამუშავებაზე გაცემული თანხმობის ან ნებართვის დადასტურება, შეცვლა/მოდიფიცირება ან უკან გახმობა მას შემდეგ, რაც მონაცემთა სუბიექტი მიაღწევს ციფრული ტექნოლოგიების სფეროში თანხმობის მინიმალურ ასაკს.

148. პრაქტიკაში, აღნიშნული ნიშნავს იმას, რომ თუ ბავშვი არ განახორციელებს რაიმე ქმედებას, მშობლის უფლების მქონე პირის მიერ გაცემული თანხმობა ან ნებართვა პერსონალური მონაცემების დამუშავებაზე, ბავშვის მიერ ციფრული ტექნოლოგიების სფეროში თანხმობის ასაკის მიღწევამდე, დამუშავების ლეგიტიმურ საფუძვლად დარჩება.

149. ციფრული ტექნოლოგიების სფეროში თანხმობის მინიმალური ასაკის მიღწევის შემდეგ, ბავშვს ენიჭება შესაძლებლობა, თავად უკან გაიხმოს თანხმობა, 7(3) მუხლის შესაბამისად. სამართლიანობის და ანგარიშვალდებულების პრინციპების შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ბავშვს მიაწოდოს ინფორმაცია ამ შესაძლებლობის შესახებ.[69]

[69] ამასთან, მონაცემთა სუბიექტები ინფორმირებულები უნდა იყვნენ დავიწყების უფლების შესახებ, რომელსაც მე-17 მუხლი ითვალისწინებს. აღნიშნული უფლება განსაკუთრებით რელევანტურია იმ

150. მნიშვნელოვანია აღინიშნოს, რომ პრეამბულის 38-ე პუნქტის თანახმად, მშობლის ან მეურვის თანხმობა არ მოითხოვება პრევენციული ან საკონსულტაციო სერვისების კონტექსტში, რომლის შეთავაზებაც ხდება პირდაპირ ბავშვისთვის. მაგალითად, ბავშვის დაცვის სერვისების ონლაინ სივრცეში უზრუნველყოფა ბავშვისთვის, ონლაინ ჩატის საშუალებით, არ მოითხოვს წინასწარ ნებართვას მშობლის მხრიდან.

151. და ბოლოს, GDPR-ის თანახმად, მშობლის ნებართვასთან დაკავშირებულმა წესებმა არ უნდა მოახდინოს გავლენა „წევრი სახელმწიფოების სახელშეკრულებო სამართლის იმ ნორმებზე, რომლებიც ეხება ხელშეკრულების ნამდვილობას, მის შედგენას და შედეგებს არასრულწლოვანთან მიმართებით.“ ამრიგად, არასრულწლოვნების შესახებ მონაცემების გამოყენებაზე ლეგიტიმურ თანხმობასთან დაკავშირებული მოთხოვნები სამართლებრივი ჩარჩოს შემადგენელი ნაწილია, რომელიც ეროვნულ დონეზე მოქმედი სახელშეკრულებო სამართლისგან განყენებულად უნდა იქნას აღქმული. შესაბამისად, წინამდებარე სახელმძღვანელო დოკუმენტი არ შეეხება იმას, თუ რამდენად კანონიერია არასრულწლოვნის მიერ ონლაინ ხელშეკრულების დადება. ორივე სამართლებრივი რეჟიმი, შესაძლოა, მოქმედებდეს ერთდროულად, ხოლო GDPR-ის მოქმედების სფერო არ მოიცავს სახელშეკრულებო სამართლის ეროვნული დებულებების ჰარმონიზებას.

7.2 სამეცნიერო კვლევა

152. სამეცნიერო კვლევასთან დაკავშირებული მიზნების განმარტებას მნიშვნელოვანი გავლენა აქვს მონაცემთა დამუშავების აქტივობების ფარგლებზე, რომელთა განხორციელებაც შეუძლია დამუშავებისთვის პასუხისმგებელ პირს. ტერმინი „სამეცნიერო კვლევა“ არ არის განმარტებული GDPR-ში. პრეამბულის 159-ე პუნქტის თანახმად, „(...) ამ რეგულაციის მიზნებიდან გამომდინარე, პერსონალური მონაცემების სამეცნიერო კვლევებისთვის დამუშავება უნდა განისაზღვროს ფართოდ (...)“; ამავდროულად, EDPB მიიჩნევს, რომ აღნიშნული ცნება არ უნდა გაფართოვდეს მისი საერთო მნიშვნელობის მიღმა და თვლის, რომ „სამეცნიერო კვლევა“ ამ კონტექსტში გულისხმობს კვლევით პროექტს, რომელიც შემუშავებულია სექტორთან დაკავშირებული შესაბამისი მეთოდოლოგიური და ეთიკური სტანდარტების თანახმად, კარგ პრაქტიკასთან შესაბამისობაში.

თანხმობასთან მიმართებით, რომელიც გაიცა მონაცემთა სუბიექტის არასრულწლოვნებისას, იხ. პრეამბულის 63-ე პუნქტი.

153. როდესაც თანხმობა წარმოადგენს კვლევის ჩატარების საფუძველს, GDPR-ის შესაბამისად, პერსონალური მონაცემების გამოყენებაზე თანხმობა უნდა განირჩეს თანხმობის სხვა მოთხოვნებისგან, რომლებიც დაკავშირებულია ეთიკურ სტანდარტთან ან პროცედურულ ვალდებულებასთან. როდესაც დამუშავება ეფუძნება არა თანხმობას, არამედ სხვა სამართლებრივ საფუძველს, ამგვარი პროცედურული ვალდებულების მაგალითი წარმოდგენილი იქნება კლინიკური ცდების შესახებ რეგულაციაში. მონაცემთა დაცვის სამართლის კონტექსტში, თანხმობის ეს უკანასკნელი ფორმა შესაძლოა მიჩნეული იქნას, როგორც დაცვის დამატებითი გარანტია.[70] ამავდროულად, GDPR-ის თანახმად, კვლევითი მიზნებისთვის მონაცემების დამუშავებასთან დაკავშირებით, მე-6 მუხლის გამოყენება მხოლოდ თანხმობით არ შემოიფარგლება. იმდენად, რამდენადაც ადგილზეა სათანადო დაცვის გარანტიები, როგორიცაა, 89(1) მუხლით გათვალისწინებული მოთხოვნები, ხოლო დამუშავება არის სამართლიანი, კანონიერი, გამჭვირვალე და შეესაბამება მონაცემთა მინიმიზაციის სტანდარტებსა და ინდივიდუალურ უფლებებს, სხვა კანონიერი საფუძვლები, როგორებიცაა 6(1) მუხლის (e) და (f) პუნქტები, შესაძლოა ხელმისაწვდომი იყოს.[71] აღნიშნული, აგრეთვე, ვრცელდება მონაცემთა განსაკუთრებულ კატეგორიებზე, 9(2)(j) მუხლით გათვალისწინებული გამონაკლისის შესაბამისად.[72]

154. პრეამბულის 33-ე პუნქტი, ერთი შეხედვით, გარკვეულ მოქნილობას ითვალისწინებს თანხმობის დეტალურობასა და კონკრეტულობასთან დაკავშირებით, სამეცნიერო კვლევის კონტექსტში. პრეამბულის 33-ე პუნქტის თანახმად: *„მონაცემთა შეგროვების მომენტში ხშირად შეუძლებელია პერსონალური მონაცემების დამუშავების მიზნის სრულად განსაზღვრა სამეცნიერო კვლევის მიზნებისათვის. შესაბამისად, მონაცემთა სუბიექტებს უნდა ჰქონდეთ საშუალება, დაეთანხმონ სამეცნიერო კვლევის განხორციელებას გარკვეულ სფეროში, სამეცნიერო კვლევის აღიარებული ეთიკური სტანდარტების დაცვის გათვალისწინებით. მონაცემთა სუბიექტებს უნდა ჰქონდეთ შესაძლებლობა, რომ დაეთანხმონ კვლევის მხოლოდ გარკვეულ სფეროებს ან კვლევითი პროექტების ნაწილებს, რამდენადაც დამუშავების მიზანი ამის საშუალებას იძლევა.“*

[70] ასევე, იხ. GDPR-ის 161-ე პუნქტი.

[71] შესაძლებელია, რომ 6(1)(c) მუხლი, აგრეთვე, გავრცელდეს დამუშავების ოპერაციების იმ ნაწილებზე, რომლებიც კონკრეტულად არის კანონით გათვალისწინებული, როგორიცაა, სანდო და მყარი მონაცემების შეგროვება წევრი სახელმწიფოს მიერ დამტკიცებული პროტოკოლის შესაბამისად, კლინიკური ცდების შესახებ რეგულაციის ფარგლებში.

[72] სამედიცინო პროდუქტების სპეციფიური ტესტირება/გამოცდა, შესაძლოა, განხორციელდეს ევროკავშირის ან ეროვნული სამართლის საფუძველზე, 9(2)(i) მუხლის შესაბამისად.

155. პირველ რიგში, უნდა აღინიშნოს, რომ პრეამბულის 33-ე პუნქტი არ ითვალისწინებს ვალდებულებებს კონკრეტული თანხმობის მოთხოვნასთან დაკავშირებით. ეს ნიშნავს, რომ არსებითად, სამეცნიერო კვლევითი პროექტები თანხმობის საფუძველზე პერსონალურ მონაცემებს შესაძლებელია მოიცავდეს მხოლოდ იმ შემთხვევაში, თუ მათ აქვთ კარგად აღწერილი მიზანი. თუ სამეცნიერო კვლევითი პროექტის ფარგლებში შეუძლებელია მონაცემთა დაცვის მიზნების თავიდანვე დაკონკრეტება, 33-ე პუნქტის თანახმად, გამონაკლისის სახით დაშვებულია მიზნის უფრო ზოგადი ფორმულირებით აღწერა.

156. იმ მკაცრი პირობების გათვალისწინებით, რომელთაც GDPR-ის მე-9 მუხლი ადგენს მონაცემთა განსაკუთრებული კატეგორიების დამუშავებასთან დაკავშირებით, EDPB აღნიშნავს, რომ განსაკუთრებული კატეგორიების მონაცემთა მკაფიო თანხმობის საფუძველზე დამუშავების დროს, 33-ე პუნქტით გათვალისწინებული მოქნილი მიდგომის გამოყენება დაექვემდებარება უფრო მკაცრ ინტერპრეტაციას და მოითხოვს კონტროლის მაღალ დონეს.

157. მთლიანობაში, დაუშვებელია GDPR-ის განმარტება იმგვარად, რაც დამუშავებისთვის პასუხისმგებელ პირებს საშუალებას მისცემს, გვერდი აუარონ იმ მიზნების დაკონკრეტების ძირითად პრინციპს, რომლისთვისაც დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტს სთხოვს თანხმობას.

158. თუ შეუძლებელია კვლევის მიზნის სრულად დაკონკრეტება, დამუშავებისთვის პასუხისმგებელმა პირმა სხვა გზებს უნდა მიმართოს იმისათვის, რომ მაქსიმალურად შესრულდეს თანხმობასთან დაკავშირებული მოთხოვნები - მაგალითად, მონაცემთა სუბიექტებს მისცეს შესაძლებლობა, დაეთანხმონ უფრო ზოგადად ფორმულირებულ კვლევის მიზანს და კვლევითი პროექტის კონკრეტულ ეტაპებს, რომელთა შესახებაც თავიდანვე ცნობილია. კვლევის მიმდინარეობასთან ერთად, შესაძლებელია მომდევნო ნაბიჯებზე თანხმობის მოპოვება მანამ, სანამ მომდევნო ეტაპი დაიწყება. ამავდროულად, ამგვარი თანხმობა უნდა იყოს სამეცნიერო კვლევის ეთიკურ სტანდარტებთან შესაბამისობაში.

159. ამას გარდა, დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია, ასეთ შემთხვევებში გამოიყენოს დამატებითი დაცვის გარანტიები. მაგალითად, 89(1) მუხლი ხაზს უსვამს სამეცნიერო ან ისტორიული თუ სტატისტიკური მიზნებისთვის მონაცემთა დამუშავების აქტივობებში დაცვის გარანტიების საჭიროებას. ეს მიზნები *„უნდა განხორციელდეს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის სათანადო გარანტიებით“.* დაცვის შესაძლო გარანტიების სახით დასახელებულია მონაცემთა მინიმიზაცია,

ანონიმიზაცია და მონაცემთა უსაფრთხოება.[73] როგორც კი შესაძლებელი გახდება კვლევის მიზნის მიღწევა პერსონალური მონაცემების დამუშავების გარეშე, რეკომენდებულია მონაცემთა ანონიმიზაცია.

160. გამჭვირვალობა დაცვის დამატებითი გარანტიაა იმ შემთხვევაში, როდესაც კვლევის გარემოებები კონკრეტული თანხმობის შესაძლებლობას არ იძლევა. მიზნის არ-დაკონკრეტება შესაძლებელია დაბალანსდეს დამუშავებისთვის პასუხისმგებელი პირის მიერ მიზნის შემუშავების შესახებ ინფორმაციის რეგულარული მიწოდებით, კვლევითი პროექტის პროგრესირებასთან ერთად, რათა გარკვეული დროის შემდგომ, თანხმობა გახდეს მაქსიმალურად კონკრეტული. აღნიშნულ პროცესში, მონაცემთა სუბიექტს როგორც მინიმუმ, საბაზისო წარმოდგენა ექნება არსებულ სიტუაციაზე, რაც მას მისცემს საშუალებას, შეაფასოს, მაგალითად, გამოიყენოს თუ არა თანხმობის უკან გახმობის უფლება, 7(3) მუხლის შესაბამისად.[74]

161. ამას გარდა, კომპლექსური კვლევითი გეგმის ხელმისაწვდომობა, რომელსაც მონაცემთა სუბიექტები გაეცნობიან დათანხმებამდე, დააბალანსებს მიზნის არ-დაკონკრეტებას. კვლევითი გეგმა მაქსიმალურად მკაფიოდ უნდა აკონკრეტებდეს კვლევით კითხვებსა და გათვალისწინებულ სამუშაო მეთოდებს.[75] კვლევითი გეგმა, აგრეთვე, ხელს შეუწყობს 7(1) მუხლთან შესაბამისობას, რადგან დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა აჩვენონ, თუ რა ინფორმაცია იყო ხელმისაწვდომი მონაცემთა

[73] მაგ., იხ. პრეამბულის 156-ე პუნქტი. პერსონალური მონაცემების დამუშავება სამეცნიერო მიზნებისთვის, აგრეთვე, უნდა აკმაყოფილებდეს შესაბამის კანონმდებლობას, როგორიცაა, კანონმდებლობა კლინიკური ცდების შესახებ, იხ. პრეამბულის 156-ე პუნქტი, რომელიც მიუთითებს ევროპარლამენტისა და საბჭოს 2014 წლის 16 აპრილის No. 536/2014 რეგულაციაზე კლინიკური ცდების შესახებ იმ სამედიცინო პროდუქტებთან დაკავშირებით, რომლებიც გამოიყენება ადამიანების მიერ. ასევე, იხ. WP29 დასკვნა 15/2011 თანხმობის განმარტების შესახებ (WP 187), გვ.7: „ამას გარდა, თანხმობის მოპოვება არ აუქმებს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებებს, რომლებიც მათ მე-6 მუხლის თანახმად ეკისრებათ სამართლიანობასთან, აუცილებლობასთან და პროპორციულობასთან, ისევე როგორც მონაცემთა ხარისხთან დაკავშირებით. მაგალითად, მაშინაც კი, თუ პერსონალური მონაცემების დამუშავება ეფუძნება მომხმარებლის თანხმობას, აღნიშნული არ ახდენს იმ მონაცემების შეგროვების ლეგიტიმიზაციას, რომლებიც გადაჭარბებულია კონკრეტულ მიზანთან მიმართებით.“ [...] არსებითად, თანხმობა არ უნდა იქნას აღქმული, როგორც გამონაკლისი მონაცემთა დაცვის სხვა პრინციპებიდან, არამედ, როგორც დაცვის გარანტია. იგი, ძირითადად, კანონიერების საფუძველია და არ გულისხმობს სხვა პრინციპების მოქმედების შეწყვეტას.“

[74] შესაძლოა, აგრეთვე რელევანტური იყოს გამჭვირვალობის სხვა ზომები. როდესაც დამუშავებისთვის პასუხისმგებელი პირი ახორციელებს დამუშავებას სამეცნიერო მიზნებისთვის, თუ შეუძლებელია თავიდანვე სრული ინფორმაციის მიწოდება, დამუშავებისთვის პასუხისმგებელ პირს შეუძლია, მონაცემთა სუბიექტებისთვის გამოყოს სპეციალური საკონტაქტო პირი, რომელიც პასუხს გასცემს მათ კითხვებს.

[75] ამგვარ შესაძლებლობას ითვალისწინებს ფინეთის პერსონალურ მონაცემთა აქტის 14(1) მუხლი (Henkilötietolaki, 523/1999).

სუბიექტებისთვის, თანხმობის გაცემის დროს, რათა შეძლონ დემონსტრირება იმისა, რომ თანხმობა იყო ლეგიტიმური.

162. მნიშვნელოვანია გავიხსენოთ, რომ იმ შემთხვევაში, როდესაც დამუშავების კანონიერ საფუძველს წარმოადგენს თანხმობა, მონაცემთა სუბიექტს თანხმობის უკან გახმობა უნდა შეეძლოს. EDPB აღნიშნავს, რომ თანხმობის უკან გახმობამ, შესაძლოა, დააზიანოს სამეცნიერო კვლევის გარკვეული კატეგორიები, რომლებიც მოითხოვენ მონაცემებს, რომელთა დაკავშირებაც შესაძლებელია ფიზიკურ პირებთან; ამავდროულად, GDPR-ი მკაფიოდ ადგენს, რომ თანხმობის უკან გახმობა შესაძლებელია, ხოლო დამუშავებისთვის პასუხისმგებელმა პირმა რეაგირება უნდა მოახდინოს აღნიშნულზე - ეს მოთხოვნა არ ითვალისწინებს რაიმე გამონაკლისს სამეცნიერო კვლევისთვის. თუ დამუშავებისთვის პასუხისმგებელი პირი მიიღებს თანხმობის უკან გახმობის მოთხოვნას, მან არსებითად, დაუყოვნებლივ უნდა უნდა წაშალოს პერსონალური მონაცემები, თუ სურს, რომ გააგრძელოს მონაცემების გამოყენება კვლევის მიზნებისთვის.[76]

7.3 მონაცემთა სუბიექტის უფლებები

163. თუ მონაცემთა დამუშავების აქტივობა ეფუძნება მონაცემთა სუბიექტის თანხმობას, აღნიშნული გავლენას მოახდენს ამ ფიზიკური პირის უფლებებზე. მონაცემთა სუბიექტებს ენიჭებათ პერსონალურ მონაცემთა პორტირების (გადატანის) უფლება (მუხლი 20), როდესაც დამუშავება თანხმობას ეფუძნება. ამავდროულად, დამუშავების შეწყვეტის მოთხოვნის უფლება (მუხლი 21) არ მოქმედებს, როდესაც დამუშავება თანხმობას ეფუძნება, თუმცა, თანხმობის ნებისმიერ დროს უკან გახმობის უფლება უზრუნველყოფს იგივე შედეგის დადგომას.

164. GDPR-ის მე-16 და მე-20 მუხლების თანახმად (როდესაც მონაცემთა დამუშავება თანხმობას ეფუძნება), მონაცემთა სუბიექტს ენიჭება მონაცემების წაშლის მოთხოვნის უფლება, თანხმობის უკან გახმობის შემთხვევაში, და მონაცემთა დაბლოკვის, გასწორების და მონაცემებზე წვდომის მოთხოვნის უფლებები.[77]

[76] ასევე, იხ. WP29-ის დასკვნა 05/2014 „ანონიმიზაციის ტექნიკების“ შესახებ (WP2016).

[77] როდესაც მონაცემთა დამუშავების გარკვეული აქტივობები GDPR-ის მე-18 მუხლის თანახმად არის შეზღუდული, მონაცემთა სუბიექტის თანხმობაა საჭირო ამ შეზღუდვების გასაუქმებლად.

8. 95/46/EC დირექტივის თანახმად მოპოვებული თანხმობა

165. დამუშავებისთვის პასუხისმგებელ პირებს, რომლებიც ამჟამად მონაცემებს ამუშავებენ თანხმობის საფუძველზე, ეროვნულ დონეზე მოქმედი მონაცემთა დაცვის კანონმდებლობის შესაბამისად, ავტომატურად მოეთხოვებათ, სრულად განაახლონ მონაცემთა სუბიექტებთან თანხმობის საფუძველზე არსებული ყველა ურთიერთობა, GDPR-თან შესაბამისობისთვის სამზადისში. მონაცემთა სუბიექტისგან მოპოვებული თანხმობა კვლავ ლეგიტიმურად რჩება იმდენად, რამდენადაც იგი შეესაბამება GDPR-ით დადგენილ პირობებს.

166. მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა დეტალურად გადახედონ არსებულ სამუშაო პროცესებსა და ჩანაწერებს, 2018 წლის 28 მაისამდე, რათა დარწმუნდნენ, რომ არსებული თანხმობები აკმაყოფილებს GDPR-ის სტანდარტს (იხ. პრეამბულის 171-ე პუნქტი[78]). პრაქტიკაში, GDPR-ი უფრო მაღალ სტანდარტს ადგენს თანხმობის მექანიზმთა იმპლემენტაციის კუთხით და ითვალისწინებს რამდენიმე ახალ მოთხოვნას, რომელიც დამუშავებისთვის პასუხისმგებელი პირისგან მოითხოვს არა მხოლოდ კონფიდენციალურობის პოლიტიკის გადამუშავებას, არამედ, თანხმობის მექანიზმებში ცვლილების შეტანას.[79]

167. მაგალითად, ვინაიდან GDPR-ის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მოახდინოს დემონსტრირება, რომ მან მოიპოვა ლეგიტიმური (ნამდვილი) თანხმობა, ნავარაუდევი თანხმობები, რომელთა დამადასტურებელი მტკიცებულებაც არ არის შენახული, ავტომატურად ჩაითვლება, რომ ვერ აკმაყოფილებს GDPR-ის თანხმობის სტანდარტს და საჭირო იქნება მათი განახლება. მსგავსად აღნიშნულისა, ვინაიდან GDPR-ი ითხოვს *„განცხადებას ან აქტიურად გამოხატულ მკაფიო ქმედებას“*, ყველა ნავარაუდევი თანხმობა, რომელიც ეფუძნება მონაცემთა სუბიექტის ქმედების ნაგულისხმევ

[78] GDPR-ის პრეამბულის 171-ე პუნქტის თანახმად: „ამ რეგულაციით უქმდება 95/46/EC დირექტივა. დამუშავება, რომელიც მიმდინარეობს ამ რეგულაციის ძალაში შესვლის მომენტში, უნდა მოვიდეს შესაბამისობაში მოცემულ რეგულაციასთან რეგულაციის ძალაში შესვლიდან ორი წლის განმავლობაში. თუ დამუშავება ეფუძნება თანხმობას 95/46/EC დირექტივის შესაბამისად, აღარ არის აუცილებელი მონაცემთა სუბიექტის მიერ თანხმობის ხელახლა გამოხატვა, თუ თანხმობის გამოხატვის შეესაბამება ამ რეგულაციის პირობებს, რათა დამუშავებისთვის პასუხისმგებელმა პირმა შეძლოს დამუშავების გაგრძელება რეგულაციის ძალაში შესვლის თარიღიდან. კომისიის მიერ მიღებული გადაწვეტილებები და საზედამხედველო ორგანოების მიერ გაცემული ნებართვები, რომლებიც ეფუძნება 95/46/EC დირექტივას, რჩება ძალაში ჩასწორებამდე, ჩანაცვლებამდე ან გაუქმებამდე.“

[79] როგორც შესავალში იქნა მითითებული, GDPR უფრო დეტალურად აკონკრეტებს და განამარტავს მოთხოვნებს, რომლებიც დაკავშირებულია ლეგიტიმური (ნამდვილი) თანხმობის მოპოვებასთან და დემონსტრირებასთან. არაერთი ახალი მოთხოვნა ეყრდნობა 15/2011 დასკვნას თანხმობის შესახებ.

ფორმას (მაგ., წინასწარ მონიშნული თანხმობის გრაფა), აგრეთვე, ვერ დააკმაყოფილებს GDPR-ის თანხმობის სტანდარტს.

168. ამას გარდა, იმისათვის, რომ დამუშავებისთვის პასუხისმგებელმა პირმა შეძლოს თანხმობის მოპოვების დემონსტრირება ან უფრო დეტალურად წარმოადგინოს მონაცემთა სუბიექტის სურვილების, ოპერაციული და საინფორმაციო ტექნოლოგიების სისტემები შესაძლოა საჭიროებდეს გადახედვას. ამასთან, ხელმისაწვდომი უნდა იყოს მონაცემთა სუბიექტის მიერ თანხმობის ადვილად უკან გახმობის მექანიზმები და მონაცემთა სუბიექტები ინფორმირებულები უნდა იყვნენ, თუ როგორ მოახდინონ თანხმობის უკან გახმობა. თუ თანხმობის მოპოვების და მართვის არსებული პროცედურები ვერ აკმაყოფილებს GDPR-ის სტანდარტებს, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მოიპოვოს ახალი თანხმობა, რომელიც რეგულაციასთან შესაბამისობაში იქნება.

169. მეორეს მხრივ, იმის გათვალისწინებით, რომ ყოველთვის არ არის აუცილებელი მე-13 და მე-14 მუხლებში დასახელებული ყველა ელემენტი იყოს წარმოდგენილი, როგორც ინფორმირებული თანხმობის პირობა, GDPR-ით გათვალისწინებული განვრცობილი ვალდებულებები ინფორმირებასთან დაკავშირებით სულაც არ ეწინააღმდეგება GDPR-ის ძალაში შესვლამდე გამოხატული თანხმობის უწყვეტობას. 95/46/EC დირექტივის თანახმად, არ მოქმედებდა მონაცემთა დამუშავების საფუძვლის შესახებ მონაცემთა სუბიექტის ინფორმირების მოთხოვნა.

170. თუ დამუშავებისთვის პასუხისმგებელი პირი დაადგენს, რომ ძველი კანონმდებლობის საფუძველზე წარსულში მოპოვებული თანხმობა ვერ აკმაყოფილებს GDPR-ის თანხმობის სტანდარტს, მაშინ იგი ვალდებულია, განახორციელოს ქმედება ამ სტანდარტებთან შესაბამისობისთვის - მაგ., განაახლოს თანხმობა GDPR-თან შესაბამისი გზით. GDPR-ის თანახმად, დაუშვებელია ერთი კანონიერი საფუძვლის მეორით ჩანაცვლება. თუ დამუშავებისთვის პასუხისმგებელი პირი ვერ შეძლებს თანხმობის GDPR-თან შესაბამისობაში განახლებას და ვერ უზრუნველყოფს - ერთ კონკრეტულ სიტუაციაში - GDPR-თან შესაბამისობაზე გადასვლას (ტრანზიციას) მონაცემების სხვა კანონიერ საფუძველზე დამუშავებით, ისე, რომ ამავდროულად უზრუნველყოს უწყვეტი დამუშავების სამართლიანობა და ანგარიშვალდებულება, დამუშავებასთან დაკავშირებული აქტივობები უნდა შეწყდეს. ნებისმიერ შემთხვევაში, საჭიროა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დაიცვას კანონიერი, სამართლიანი და გამჭვირვალე დამუშავების პრინციპები.