პერსონალურ მონაცემთა დაცვის სამსახური

მსოფლიო პრაქტიკა

აპრილი/2023

მთავარი სიახლეები

სოციალური ქსელი “Facebook”-ი თავის მომხმარებლებს პერსონალური მონაცემების უნებართვოდ გავრცელების გამო 725 მილიონ აშშ დოლარს გადაუხდის

ევროპის მონაცემთა დაცვის საბჭომ (“EDPB”) მონაცემთა სუბიექტის წვდომის უფლებასთან დაკავშირებით სახელმძღვანელო გაიდლაინის განახლებული რედაქცია გამოაქვეყნა

ევროკავშირის მართლმსაჯულების სასამართლომ სამოქალაქო სამართალწარმოებაში “GDPR”-ის გამოყენების შესახებ წინასწარი გადაწყვეტილება გამოიტანა

ევროპის მონაცემთა დაცვის საბჭომ (“EDPB”) მონაცემთა სუბიექტის წვდომის უფლებასთან დაკავშირებით სახელმძღვანელო გაიდლაინის განახლებული რედაქცია გამოაქვეყნა

ევროკავშირის მართლმსაჯულების სასამართლომ სამოქალაქო სამართალწარმოებაში “GDPR”-ის გამოყენების შესახებ წინასწარი გადაწყვეტილება გამოიტანა

12.04.2023

2023 წლის 2 მარტს, ევროკავშირის მართლმსაჯულების სასამართლომ (CJEU) მიიღო გადაწყვეტილება, რომელიც ევროკავშირის წევრ ქვეყნებში სამოქალაქო სამართალწარმოებისას „მონაცემთა დაცვის ზოგადი რეგულაციის“ (GDPR) დებულებების გამოყენებას შეეხება.

ფოტო: curia.europa.eu

საქმის გარემოებები

დავის მონაწილე ორივე მხარის მიმართ შვედეთის კანონმდებლობა ვრცელდებოდა. საქმის გარემოებების მიხედვით, მოსარჩელემ მოპასუხეს საოფისე ნაგებობა აუშენა. აღნიშნულ სამშენებლო ობიექტზე მომუშავე პირები მათი სამუშაო ადგილზე ყოფნას თანამშრომელთა ელექტრონული რეესტრის საშუალებით აღრიცხავდნენ. შვედეთის საგადასახადო კანონმდებლობის მიხედვით, ნებისმიერ პირს, რომელიც სამშენებლო საქმიანობას ახორციელებდა, გარკვეულ შემთხვევებში თანამშრომელთა ელექტრონული რეესტრის წარმოების ვალდებულება გააჩნდა. რეესტრი ხელს უწყობდა არადეკლარირებული სამუშაოს იდენტიფიცირებას და მასში უნდა ასახულიყო ნებისმიერი ინფორმაცია, რომელიც შესაბამის ეკონომიკურ საქმიანობაში ჩართული პირების იდენტიფიცირებისთვის იყო საჭირო. აღნიშნული მოიცავდა პირის შესახებ ისეთ მონაცემს, როგორიცაა: ვინაობა, ეროვნული საგადასახადო საიდენტიფიკაციო ნომერი, სამუშაო საათების დაწყებისა და დასრულების დრო და სხვა.

მოსარჩელემ შესრულებული სამუშაოს დავალიანების ანაზღაურების მოთხოვნის თაობაზე სარჩელი პირველ ინსტანციაში შეიტანა. მოპასუხე ამტკიცებდა, რომ ასანაზღაურებელი საათების რაოდენობა უფრო ცოტა იყო, ვიდრე მოსარჩელემ მიუთითა. აღნიშნულის დასადასტურებლად კი, მოპასუხემ განსახილველი პერიოდის თანამშრომელთა არარედაქტირებული რეესტრის წარდგენა მოითხოვა. შვედეთის კანონმდებლობის მიხედვით, თუკი შესაძლებელია, დოკუმენტი მიჩნეულ იქნეს მტკიცებულებად, შესაბამისი მხარე ვალდებულია, იგი სამოქალაქო სამართალწარმოებაში წარადგინოს.

თუმცა, მოსარჩელის განმარტებით, ზემოთ მითითებული პროცედურა არღვევდა “GDPR”-ის მე-5 მუხლის პირველი პუნქტის “ხ” ქვეპუნქტით გათვალისწინებული მიზნის შეზღუდვის პრინციპს. მოსარჩელის პირად საქმეში შედიოდა პერსონალური მონაცემები, რომელთა შეგროვების მიზანს შვედეთის საგადასახადო ორგანოების მიერ კომპანიის საქმიანობის მონიტორინგი წარმოადგენდა. მოსარჩელე ამტკიცებდა, რომ

სასამართლოსთვის ამ მონაცემების არარედაქტირებული ფორმით გამჟღავნება ამ მიზანთან შეუთავსებელი იყო. მას შემდეგ, რაც მოსარჩელეს დაევალა პირველი ინსტანციის სასამართლოსთვის დოკუმენტაციის არარედაქტირებული, პირველადი ვერსიის წარდგენა, უზენაესმა სასამართლომ მისი კანონიერების საკითხის გადასაწყვეტად CJEU-ს კითხვებით მიმართა.

შვედეთის უზენაესმა სასამართლომ CJEU-ს წინაშე ორი საკითხი დააყენა:

1. მესამე პირების პერსონალური მონაცემები, რომელთა შეგროვება თავდაპირველად საგადასახადო მიზნებისთვის განხორციელდა, შეიძლება თუ არა, დამუშავების შეცვლილი მიზნით, სამოქალაქო სამართალწარმოების კონტექსტში მტკიცებულებად იქნას გამოყენებული, GDPR-ის მე-6 მუხლის მე-3 და მე-4 პუნქტების შესაბამისად?
2. GDPR-ის მე-5 და მე-6 მუხლების განმარტება ხომ არ გულისხმობს, რომ სამოქალაქო სამართალწარმოების დროს პერსონალური მონაცემების შემცველი დოკუმენტის წარმოდგენის შეფასებისას, ეროვნული სასამართლო ვალდებულია, გაითვალისწინოს მონაცემთა სუბიექტების ინტერესები? ასეთ შემთხვევაში ევროკავშირის კანონმდებლობა და კერძოდ, GDPR-ი შეფასების რაიმე კონკრეტულ მოთხოვნებს ხომ არ განსაზღვრავს?

CJEU-ს შეფასება

1 სამოქალაქო სამართალწარმოების კონტექსტში შეცვლილი მიზნით მტკიცებულებების გამოყენების შესაბამისობა GDPR-ის მე-6 მუხლთან:

CJEU-მ პირველ რიგში განმარტა, რომ GDPR-ის მე-2 მუხლის პირველი პუნქტის მატერიალური მოქმედების ფარგლები ვრცელდება კერძო პირების მიერ განხორციელებული დამუშავების ოპერაციებზე, ასევე საჯარო ხელისუფლების, მათ შორის, სასამართლო ორგანოების მიერ განხორციელებული დამუშავების ოპერაციებზე. გარდა ამისა, CJEU-მ აღნიშნა, რომ საგადასახადო მიზნებისთვის როგორც თანამშრომელთა ელექტრონული რეესტრის შექმნა და წარმოება, ასევე სასამართლო პროცესის კონტექსტში აღნიშნული დოკუმენტის წარდგენა, არის პერსონალური მონაცემების დამუშავება, GDPR-ის მე-4 მუხლის მე-2 პუნქტიდან გამომდინარე. ამგვარად, GDPR-ის გამოყენების ფარგლები ვრცელდება წინამდებარე საქმეზე. შესაბამისად, სასამართლოს მიერ მოთხოვნილი დოკუმენტების მტკიცებულების სახით წარდგენა მოითხოვდა GDPR-ის მე-6 მუხლით გათვალისწინებულ სამართლებრივ საფუძველს.

განსახილველ შემთხვევაში, სასამართლომ GDPR-ის მე-6 მუხლის პირველი პუნქტის “e” ქვეპუნქტი გამოსაყენებლად მიიჩნია. აღნიშნული ნორმის მიხედვით, პერსონალური მონაცემების დამუშავება კანონიერია, თუ ეს აუცილებელია საზოგადოებრივი ინტერესების სფეროში შემავალი ამოცანების შესასრულებლად

(წინამდებარე საქმეში, სასამართლოების უფლებამოსილებების განსახორციელებლად) და GDPR-ის მე-6 მუხლის მე-3 პუნქტის შესაბამისად, სამართლებრივი საფუძველი განსაზღვრულია შესაბამისი წევრი სახელმწიფოს კანონმდებლობით. CJEU-მ განმარტა, რომ ეს უკანასკნელი მოთხოვნა ასევე შესრულდა, რადგან შვედეთის კანონმდებლობა ითვალისწინებდა სასამართლოებისთვის მტკიცებულებების წარდგენის ვალდებულებას.

CJEU-მ დაადგინა მიზნის ცვლილება (ფისკალურიდან სამოქალაქო სამართალწარმოების მიზნებისთვის დამუშავებაზე) და მიიჩნია, რომ მონაცემთა დამუშავების შემდგომი მოთხოვნები უნდა განსაზღვრულიყო GDPR-ის მე-6 მუხლის მე-4 პუნქტის დებულებების საფუძველზე. ასევე, CJEU-მ აღნიშნა, რომ შიდა სასამართლომ უნდა გადაწყვიტოს, დაკმაყოფილდა თუ არა GDPR-ის მე-6 მუხლის მე-4 პუნქტის მოთხოვნები 23-ე მუხლის პირველ პუნქტთან ერთობლიობაში. აღნიშნული მოითხოვდა სასამართლოს მიერ გადაწყვეტილების მიღებას საქმის კონკრეტული გარემოებების გათვალისწინებით.

CJEU-ს პასუხი პირველ შეკითხვაზე:

GDPR-ის მე-6 მუხლის მე-3 და მე-4 პუნქტები ვრცელდება სამოქალაქო სამართალწარმოების კონტექსტშიც.

❷ მონაცემთა სუბიექტთა ინტერესების გათვალისწინება:

მეორე კითხვის ნაწილში, CJEU-მ განიხილა ეროვნული სასამართლოს ვალდებულების ბუნება მონაცემთა სუბიექტთა ინტერესების კონტექსტში. პირველ რიგში, CJEU-მ მიუთითა მონაცემთა დაცვის პრინციპების დაკმაყოფილების, მონაცემთა სუბიექტის უფლებების დაცვისა და GDPR-ის მე-6 მუხლის მიხედვით მონაცემთა დამუშავების საფუძვლის არსებობის შესახებ ზოგად მოთხოვნებზე.

CJEU-ს მიდგომა მე-2 კითხვაზე პასუხის გაცემისას ეფუძნებოდა შემდეგ მსჯელობას:

- ეროვნულმა სასამართლოებმა უნდა უზრუნველყონ პერსონალური მონაცემების დაცვა და პირადი ცხოვრების პატივისცემა. თუმცა, მონაცემთა დაცვის უფლება არ არის აბსოლუტური ხასიათის. საჭიროა ბალანსის დაცვა სხვა ისეთ ფუნდამენტურ უფლებებთან მიმართებით, მაგალითად, როგორიცაა ეფექტიანი სასამართლო დაცვის უფლება, რასაც ხელს უწყობს სამოქალაქო სამართალწარმოების პროცესებში მესამე პირების პერსონალური მონაცემების შემცველი დოკუმენტის წარმოება;
- GDPR-ის მე-5 მუხლის პირველი პუნქტის “c” ქვეპუნქტით განსაზღვრული „მონაცემთა მინიმიზაციის“ პრინციპის თანახმად, პერსონალური მონაცემი უნდა იყოს ადეკვატური, შესაბამისი და შეზღუდული იმ მიზნებით, რისთვისაც იგი მუშავდება;

სხვადასხვა ინტერესის გათვალისწინება არის ცალკეული ღონისძიების აუცილებლობისა და პროპორციულობის შესწავლის ნაწილი, რაც გათვალისწინებულია GDPR-ის მე-6 მუხლის მე-3 და მე-4 პუნქტებით. შედეგად, ეროვნულმა სასამართლოებმა, რომლებიც პერსონალური მონაცემების შემცველი დოკუმენტების წარმოდგენას ითხოვენ, უნდა განსაზღვრონ, არის თუ არა აღნიშნული ღონისძიება ადეკვატური და ხომ არ შეიძლება მისი მიღწევა ნაკლებად შემზღუდავი საშუალებებით.

CJEU-ს პასუხი მეორე შეკითხვაზე:

GDPR-ის მე-5 და მე-6 მუხლების თანახმად, ეროვნული სასამართლოს მიერ პერსონალური მონაცემების შემცველი დოკუმენტის წარმოდგენის შესახებ გადაწყვეტილების მიღებისას, იგი ვალდებულია, გაითვალისწინოს დაკავშირებული მონაცემთა სუბიექტების ინტერესი და დააბალანსოს იგი თითოეული საქმის გარემოებისა და საქმისწარმოების ტიპის გათვალისწინებით. სასამართლომ ასევე უნდა გაითვალისწინოს პროპორციულობის პრინციპის, კერძოდ, მონაცემთა მინიმიზაციის პრინციპიდან გამომდინარე GDPR-ის მე-5 მუხლის პირველი პუნქტის "c" ქვეპუნქტის, მოთხოვნები.

ევროკავშირის მართლმსაჯულების სასამართლოს ("CJEU") გენერალურმა ადვოკატმა მონაცემთა სუბიექტის მიერ მონაცემებზე წვდომის უფლებასთან დაკავშირებით მოსაზრება გამოაქვეყნა

20.04.2023

ფოტო: european-union.europa.eu

2023 წლის 20 აპრილს, ევროკავშირის მართლმსაჯულების სასამართლოს (CJEU) გენერალურმა ადვოკატმა (AG) საქმეში: FT v. DW (C-307/22), მონაცემთა სუბიექტის მიერ მონაცემებზე წვდომის უფლებასთან დაკავშირებით მოსაზრება გამოაქვეყნა. ფაქტობრივი გარემოებების თანახმად, სტომატოლოგიური კლინიკის პაციენტმა, რომელსაც ჰქონდა ეჭვი მის მიმართ ჩატარებულ არასწორ მკურნალობაზე, ექიმისგან მოითხოვა მის ხელთ არსებული ყველა სამედიცინო ჩანაწერის ასლების უფასოდ გადაცემა. ექიმის თქმით, თუ პაციენტი შესაბამის საფასურს არ გადაიხდიდა, მისი მოთხოვნა ვერ დაკმაყოფილდებოდა.

2020 წლის 30 მარტს, ადგილობრივმა სასამართლომ პაციენტის სარჩელი დააკმაყოფილა. სასამართლომ განმარტა, რომ მონაცემებზე წვდომის უფლება GDPR-ის მე-15(3) მუხლის შესაბამისად, არ გამორიცხავს პაციენტის მხრიდან იმ ინფორმაციის მოთხოვნის უფლებას,

რომელიც სამედიცინო პასუხისმგებლობის დადგენას შეეხება.

აღნიშნულის შემდგომ, სტომატოლოგმა დაიწყო სამართლებრივი დავა გერმანიის ფედერალურ სასამართლოში, რომელმაც 2022 წლის 29 მარტის გადაწყვეტილებით შეაჩერა პროცესი და კითხვებით მიმართა ევროკავშირის მართლმსაჯულების სასამართლოს (CJEU) წინასწარი განჩინების გამოტანის თხოვნით.

- → პირველი კითხვა შეეხებოდა GDPR-ის მე-12(5) და მე-15(3) მუხლების ინტერპრეტაციას. კერძოდ, აქვს თუ არა დამმუშავებელს ვალდებულება, მონაცემთა სუბიექტს უფასოდ წარუდგინოს პერსონალური მონაცემების ასლები მაშინ, როდესაც აღნიშნული მოთხოვნის საფუძველი არ წარმოადგენს პერსონალური მონაცემების დაცვას?
- → შემდეგი კითხვა მიემართებოდა ეროვნული კანონმდებლობის შესაბამისად ინფორმაციის მისაღებად თანხების გადახდის ვალდებულებას და ასევე, უნდა გადაეცეს თუ არა პაციენტს მის შესახებ არსებული მასალების სრული ასლები.

✅ პირველი კითხვის საპასუხოდ, გენერალური ადვოკატის განცხადებით, GDPR-ის მე-12(5) და მე-15(3) მუხლები იმგვარად უნდა იქნას განმარტებული, რომ მონაცემთა დამმუშავებელს დაევალოს მონაცემთა სუბიექტისთვის მისი პერსონალური მონაცემების ასლების გადაცემა მაშინაც კი, როდესაც იგი არ ითხოვს ასლებს, GDPR-ის 63-ე პუნქტით გათვალისწინებული მიზნების შესაბამისად. მისი თქმით, ინფორმაციის მოთხოვნის საფუძველს შეიძლება არ წარმოადგენდეს პერსონალური მონაცემების დაცვა.

გენერალური ადვოკატი მოსაზრებას GDPR-ის მე-12(5) და მე-15(3) მუხლების ფართო ინტერპრეტაციაზე დაყრდნობით ასაბუთებს. იგი აღნიშნავს, რომ 63-ე პუნქტის ფორმულირება მე-15 მუხლთან მიმართებით არ არის სრულად გასაგები. კონკრეტულად, აღნიშნული პუნქტიდან არ იკვეთება, რომ მონაცემებზე წვდომის უფლება მხოლოდ მასში ასახული მიზნებით უნდა იქნას გარანტირებული.

ადვოკატის განმარტებით, ეროვნული კანონმდებლობის გათვალისწინებით პაციენტისთვის ხარჯების ანაზღაურების ვალდებულება შეიძლება, დასაშვები იყოს მხოლოდ კონკრეტულ შემთხვევებში GDPR-ის 23-ე მუხლის საფუძველზე, თუკი ასანაზღაურებელი ხარჯები შემოიფარგლება მხოლოდ გაწეული ფაქტობრივი ხარჯებით.

დამატებით, გენერალური ადვოკატი აცხადებს, რომ ექიმსა და პაციენტს შორის ურთიერთობის კონტექსტში, GDPR-ის მე-15(3) მუხლი ვერ განიმარტება იმგვარად, რომ მონაცემთა სუბიექტს მის შესახებ არსებული სამედიცინო მასალების სრული ასლების მოსაპოვებლად მიენიჭოს ზოგადი უფლება. თუმცა, მონაცემთა დამმუშავებელი ვალდებულია, მონაცემთა სუბიექტს მიაწოდოს დოკუმენტების სრული ან ნაწილობრივი ასლები გასაგები ფორმით. თავის მხრივ მონაცემთა სუბიექტს შესაძლებლობა აქვს, დაადგინოს წარდგენილი მონაცემების სისრულე და სიზუსტე.

ევროპის მონაცემთა დაცვის საბჭომ (“EDPB”) მონაცემთა სუბიექტის წვდომის უფლებასთან დაკავშირებით სახელმძღვანელო გაიდლაინის განახლებული რედაქცია გამოაქვეყნა

17.04.2023

ფოტო: www.edps.europa.eu

ევროპის მონაცემთა დაცვის საბჭომ (“EDPB”) მონაცემთა სუბიექტის წვდომის უფლების შესახებ 2022 წლის სახელმძღვანელო გაიდლაინის გადამუშავებული ვერსია გამოაქვეყნა.

დღესდღეობით პერსონალური მონაცემები საჯარო და კერძო პირების მიერ მათი საქმიანობის მიზნებისთვის და სხვადასხვა საშუალებით მუშავდება. ფიზიკური პირები შეიძლება, არახელსაყრელ მდგომარეობაში აღმოჩნდნენ, იმის გათვალისწინებით, რომ მათთვის, ხშირად, უცნობია, თუ როგორ მუშავდება მათი პერსონალური მონაცემები და რომელი ტექნოლოგიის გამოყენებით. აღნიშნული გარემოების გათვალისწინებით და პერსონალური მონაცემების დაცვის მიზნით, „მონაცემთა დაცვის ზოგადი რეგულაციის“ (“GDPR”) მეშვეობით შეიქმნა რეგულირების თანმიმდევრული და მტკიცე სამართლებრივი ჩარჩო, მათ შორის, მონაცემთა სუბიექტის უფლებების რეალიზაციასთან დაკავშირებით.

პერსონალურ მონაცემებზე წვდომის უფლება არის მონაცემთა სუბიექტის ერთ-ერთი უფლება, რომელიც, სხვა ისეთ უფლებებთან ერთად, როგორიცაა: მონაცემთა გასწორებისა და წაშლის უფლება, მონაცემთა დაბლოკვის უფლება, მონაცემთა პორტირების (გადატანის) უფლება, მონაცემთა დამუშავების შეწყვეტის მოთხოვნის უფლება ან ავტომატიზირებული ინდივიდუალური გადაწყვეტილების მიღებაზე, მათ შორის, პროფილირების გზით, უარის თქმის უფლება — გათვალისწინებულია “GDPR”-ის III თავში. მონაცემთა სუბიექტის წვდომის უფლება გათვალისწინებულია, როგორც ევროკავშირის ფუნდამენტური უფლებების ქარტიაში, ასევე “GDPR”-ის მე-15 მუხლში, რომელიც ზუსტად აყალიბებს პერსონალურ მონაცემებსა და სხვა დაკავშირებულ ინფორმაციაზე წვდომის უფლებას.

“GDPR”-ის მიხედვით, წვდომის უფლება სამი კომპონენტისგან შედგება:

1. დასტური მასზედ, მუშავდება თუ არა პირის პერსონალური მონაცემი;

2. მის პერსონალურ მონაცემზე წვდომა;

3. დამუშავების შესახებ ისეთ ინფორმაციაზე წვდომა, როგორიცაა: მიზანი, მონაცემის კატეგორია, მონაცემის მიმღებთა კატეგორია (“data recipients”), მესამე ქვეყანაში მონაცემთა გადაცემის შემთხვევაში სათანადო დაცვის გარანტიები.

მონაცემთა სუბიექტს, ასევე, უფლება აქვს, მიიღოს დამუშავებული პერსონალური მონაცემების ასლი. აღნიშნული წარმოადგენს არათუ მონაცემთა სუბიექტის დამატებით უფლებას, არამედ

წვდომის უზრუნველყოფის საშუალებას. ამრიგად, წვდომის უფლება შეიძლება, გაგებული იყოს როგორც მონაცემთა სუბიექტის შესაძლებლობა, ჰკითხოს დამმუშავებელს, მუშავდება თუ არა მისი პერსონალური მონაცემები. მოთხოვნის საფუძველზე დამმუშავებელი ვალდებულია, მიაწოდოს მონაცემთა სუბიექტს "GDPR"-ის მე-15 მუხლის შესაბამისი ინფორმაცია. წვდომის უფლება ხორციელდება, როგორც პერსონალურ მონაცემთა დაცვის მომწესრიგებელი კანონის, ისე ფიზიკური პირების ძირითადი უფლებებისა და თავისუფლებების, კერძოდ, მათი უფლების ფარგლებში.

მისი პრაქტიკული მიზანია ფიზიკური პირების მიერ საკუთარი პერსონალური მონაცემების კონტროლის შესაძლებლობა. აღნიშნულის პრაქტიკაში ეფექტიანი განხორციელების მიზნით, "GDPR"-ი წვდომის უფლების რეალიზაციას სხვადასხვა გარანტიის შექმნით უზრუნველყოფს, რაც მონაცემთა სუბიექტს საშუალებას აძლევს, მარტივად, გონივრული ინტერვალის დაცვით და ზედმეტი შეფერხებისა თუ ხარჯების გარეშე ისარგებლოს აღნიშნული უფლებით. აღსანიშნავია, რომ იგი თავიდანვე წარმოადგენდა მონაცემთა დაცვის ევროპული საკანონმდებლო სისტემის ელემენტს.

"EDPB"-ის სახელმძღვანელო დოკუმენტში განხილულია წვდომის უფლების მიზნები, ფარგლები, მისი ძირითადი პრინციპები, წვდომის უფლების შესახებ მოთხოვნათა შეფასების გარკვეული ასპექტები, დამმუშავებლის მიერ წვდომის უზრუნველყოფის საკითხი, ასევე, უფლების შეზღუდვის წინაპირობები.

- **"EDPB"-ის ზოგადი მოსაზრებები მონაცემთა სუბიექტის მოთხოვნის შეფასების შესახებ**

მოთხოვნის შინაარსის გაანალიზებისას, დამმუშავებელმა უნდა შეაფასოს, ეხება თუ არა მოთხოვნა, განმცხადებელი პირის პერსონალურ მონაცემებს, ასევე, მიესადაგება თუ არა იგი "GDPR"-ის მე-15 მუხლს და არის თუ არა სხვა, უფრო კონკრეტული, დებულებები, რომლებიც არეგულირებს წვდომის უფლებას ცალკეულ სექტორში. დამმუშავებელმა, ასევე, უნდა შეაფასოს, თუ რამდენად შეეხება დამუშავებული ინფორმაცია მონაცემთა სუბიექტს. აღსანიშნავია, რომ არ არსებობს რაიმე მოთხოვნა წვდომის უფლების შესახებ განცხადების ფორმატთან დაკავშირებით. მონაცემთა სუბიექტს ინფორმაცია უნდა მიეწოდოს შესაბამისი და მარტივი საკომუნიკაციო არხების მეშვეობით. თუმცა, მონაცემთა სუბიექტს უფლება აქვს, არ გამოიყენოს დამმუშავებლის მიერ უზრუნველყოფილი საკომუნიკაციო არხი და ამის ნაცვლად, გაგზავნოს მოთხოვნა დამმუშავებლის ოფიციალურ საკონტაქტო პირთან. ამასთანავე, დამმუშავებელი არ არის ვალდებული, რეაგირება მოახდინოს ისეთ მოთხოვნებზე, რომლებიც არამიზნობრივად ან აშკარად არასწორ მისამართებზე იგზავნება. მაშინ, როდესაც დამმუშავებელს არ შეუძლია იმ მონაცემთა იდენტიფიცირება, რომელიც მონაცემთა სუბიექტს შეეხება, იგი ვალდებულია, აცნობოს მას აღნიშნულის შესახებ და მონაცემთა სუბიექტის მიერ იდენტიფიკაციის მიზნით დამატებითი ინფორმაციის მიწოდებამდე, უარი განაცხადოს წვდომის უფლების შესახებ მოთხოვნის დაკმაყოფილებაზე. უფრო

მეტიც, თუ დამმუშავებელს მონაცემთა სუბიექტის იდენტიფიცირებასთან დაკავშირებით აქვს გონივრული ეჭვი, მას უფლება აქვს, მოითხოვოს ის დამატებითი ინფორმაცია, რომლის მეშვეობით შესაძლებელი იქნება მისი იდენტიფიცირება. დამატებითი ინფორმაციის მოთხოვნა დამუშავებული მონაცემისა და შესაძლო ზიანის პროპორციული უნდა იყოს, რათა არ მოხდეს იმაზე მეტი ინფორმაციის დამუშავება, ვიდრე ეს კონკრეტული მიზნისთვის საჭიროა.

• წვდომის უფლების ფარგლები

მონაცემთა სუბიექტის წვდომის უფლების ფარგლებს განსაზღვრავს პერსონალური მონაცემების ცნების შინაარსი, "GDPR"-ის მე-4(1) მუხლის შესაბამისად. ვინაობის, საცხოვრებელი მისამართის, ტელეფონის ნომრისა და სხვა ინფორმაციის გარდა, ამ განსაზღვრებაში მოიაზრება მონაცემთა ფართო სპექტრი: სამედიცინო დასკვნები, შესყიდვების ისტორია, კრედიტუნარიანობის ინდიკატორები, აქტივობების ჩანაწერები ("activity logs"), საძიებო აქტივობები ("search logs") და ა. შ. ამასთანავე, ფსევდონიმიზაციის შემთხვევაშიც, პერსონალური მონაცემები, განსხვავებით ანონიმიზაციისგან, კვლავ პერსონალურ მონაცემად მიიჩნევა. იმის გათვალისწინებით, რომ წვდომის უფლება მიემართება მომთხოვნი პირის პერსონალურ მონაცემებს, იგი შეიძლება მოიცავდეს სხვა პირებთან დაკავშირებულ მონაცემსაც, მაგალითად, კომუნიკაციის ისტორია, რომელიც მოიცავს შემომავალ და გამავალ შეტყობინებებს.

პერსონალურ მონაცემებზე წვდომის უზრუნველყოფის გარდა, დამმუშავებელმა მონაცემთა სუბიექტს უნდა მიაწოდოს დამატებითი ინფორმაცია დამუშავებისა და მისი უფლებების შესახებ. ასეთი ინფორმაცია შეიძლება, ეფუძნებოდეს მონაცემთა დამუშავების ჩანაწერებსა ("GDPR"-ის 30-ე მუხლი) და კონფიდენციალურობის შეტყობინებაში ("GDPR"-ის მე-13 და მე-14 მუხლები) შეტანილ მონაცემებს. თუმცა, აღნიშნული ინფორმაცია შეიძლება, განახლდეს მოთხოვნისთანავე ან იყოს მორგებული დამუშავების იმ ოპერაციების ასახვაზე, რომელიც განმცხადებელ პირთან მიმართებით ხორციელდება.

• წვდომის უზრუნველყოფა

წვდომის უზრუნველყოფის გზები შეიძლება, განსხვავდებოდეს მონაცემთა მოცულობისა და დამუშავების სირთულის მიხედვით. თუკი განმცხადებელს არ აქვს დაკონკრეტებული, მოთხოვნა მიემართება მონაცემთა სუბიექტის ყველა პერსონალურ მონაცემს. თუკი დამმუშავებელი მონაცემთა დიდ მოცულობას ამუშავებს, მას უფლება აქვს, მოსთხოვოს მონაცემთა სუბიექტს იმის დაკონკრეტება, თუ რომელ პერსონალურ მონაცემს მიემართება მისი მოთხოვნა. დამმუშავებელი ვალდებულია, მოიძიოს პერსონალური მონაცემები, როგორც მთლიან IT სისტემაში, ასევე მის მიღმა, ძიების სხვადასხვა კრიტერიუმის საფუძველზე, რომელიც ასახავს ინფორმაციის „სტრუქტურულ გზას", მაგალითად, სახელი და მომხმარებლის ნომერი. სუბიექტს მონაცემთა დამუშავების შესახებ ინფორმაცია უნდა წარედგინოს ლაკონური, გამჭვირვალე, გასაგები და ადვილად ხელმისაწვდომი ფორმით, მკაფიო და მარტივი ენით.

აღნიშნული ყოველ ინდივიდუალურ შემთხვევაში დამოკიდებულია მონაცემთა დამუშავების სხვადასხვა გარემოებაზე, აგრეთვე, მონაცემთა სუბიექტის უნარზე, გაითავისოს და გაიაზროს კომუნიკაცია (მაგალითად, იმის გათვალისწინებით, რომ მონაცემთა სუბიექტი არის ბავშვი ან სპეციალური საჭიროების მქონე პირი). თუ მონაცემები შედგება გარკვეული კოდებისგან ან მოცემულია „დაუმუშავებელი“, პირველადი სახით, საჭიროა მათი განმარტება, რათა აღქმადი იყოს მონაცემთა სუბიექტისთვის.

წვდომის უზრუნველყოფის მთავარი საშუალება სუბიექტისთვის მონაცემთა ასლის მიწოდებაა, მაგრამ სხვა მეთოდებიც (როგორიცაა ინფორმაციის ზეპირად მიწოდება და ადგილზევე დათვალიერება) ასევე შეიძლება იყოს უზრუნველყოფილი, სუბიექტის მოთხოვნის შესაბამისად. მონაცემები შეიძლება, გაიგზავნოს ელექტრონული ფოსტით, იმ პირობით, თუკი გამოყენებული იქნება წვდომის უზრუნველსაყოფად ყველა საჭირო გარანტია, მაგალითად, მონაცემთა ხასიათის, თვითმომსახურების ინსტრუმენტების გათვალისწინებით. ზოგჯერ, დიდი მოცულობის მონაცემთა წვდომის შემთხვევაში, შესაძლებელია, მონაცემთა სუბიექტს გაუჭირდეს მათი გაგება, მით უფრო მაშინ, როდესაც ინფორმაცია ელექტრონულ ფორმატშია მოცემული. ასეთ შემთხვევაში ყველაზე მიღებული პრაქტიკაა „ეტაპობრივი მიდგომა“ (“layered approach”). რამდენიმე ეტაპად მონაცემის მიწოდებამ შესაძლებელია, უფრო გაამარტივოს მისი აღქმა, თუმცა დამმუშავებელს უნდა შეეძლოს ამგვარი მიდგომის გონივრულობის დასაბუთება. მონაცემთა ასლი და დამატებითი ინფორმაცია უნდა იყოს მოწოდებული კონსოლიდირებული სახით, მაგალითად, წერილობითი ტექსტის მეშვეობით, რომელიც შემდგომ შეიძლება ელექტრონული ფორმითაც იყოს გამოყენებული, რათა მონაცემთა სუბიექტმა ადვილად შეძლოს მისი გადმოწერა-შენახვა. მონაცემების მიწოდება შესაძლებელია ტრანსკრიფციით ან კრებულის სახით, თუ მასში მოცემულია სრული ინფორმაცია, მისი შინაარსის უცვლელად. წვდომის უფლების შესახებ მოთხოვნა უნდა დაკმაყოფილდეს უმოკლეს ვადაში, თუმცა გარკვეულ შემთხვევებში, შესაძლოა, ამას ერთი თვეც კი დასჭირდეს. საჭიროების შემთხვევაში, მოთხოვნის დაკმაყოფილების პერიოდი შესაძლოა გაგრძელდეს ორ თვემდე, რაც დამოკიდებულია მოთხოვნის სირთულესა და მონაცემთა მოცულობაზე. გარდა ამისა, აუცილებელია, მონაცემთა სუბიექტს ეცნობოს მოთხოვნის დაკმაყოფილების გაჭიანურების მიზეზი. დამმუშავებელმა უნდა უზრუნველყოს ყველა საჭირო ღონისძიება, რათა რაც შეიძლება მალე განიხილოს მოთხოვნა და მოარგოს იგი დამუშავების ცალკეულ გარემოებას. როდესაც მონაცემები ინახება მხოლოდ მოკლე ვადით, წვდომა უნდა იყოს უზრუნველყოფილი მოთხოვნის განხილვის პროცესში, თუმცა მონაცემების წაშლის გარეშე.

წვდომის შესახებ მოთხოვნის შეფასება უნდა მოხდეს, მოთხოვნის მიღების მომენტში არსებული გარემოებების გათვალისწინებით. დამმუშავებელმა მონაცემთა სუბიექტს უნდა მიაწოდოს, ის ინფორმაციაც, რომელიც შესაძლოა, არასწორად ან არაკანონიერად ჰქონდეს

დამუშავებული. თუმცა, ცხადია, თუ მონაცემები წაშლილია, დამმუშავებელი ვერ შეძლებს მონაცემთა სუბიექტისთვის მის გაზიარებას.

- **წვდომის უფლების შეზღუდვა**

"GDPR"-ი წვდომის უფლებაზე გარკვეული შეზღუდვების დაწესების შესაძლებლობას იძლევა.

მე-15(4) მუხლის თანახმად, ასლის მიღების უფლებამ სხვათა უფლებებსა და თავისუფლებებზე უარყოფითი გავლენა არ უნდა იქონიოს. თუმცა, მე-15(4) მუხლის რეალიზაციამ არ უნდა გამოიწვიოს მონაცემთა სუბიექტის მოთხოვნაზე საერთოდ უარის თქმა.

"GDPR"-ის მე-12(5) მუხლი მონაცემთა დამმუშავებელს მონაცემთა სუბიექტის მოთხოვნის შესრულებაზე უარის თქმის ან გონივრული საფასურის დაწესების შესაძლებლობას აძლევს, თუ მოთხოვნა ცალსახად დაუსაბუთებელი ან გადაჭარბებულად მოცულობითია. ამასთანავე, აღნიშნული ცნებები ვიწროდ უნდა განიმარტოს. მოთხოვნის გადაჭარბებულად შეფასება იმ სექტორის სპეციფიკაზეა დამოკიდებული, რომელშიც მონაცემთა დამმუშავებელი ოპერირებს. მონაცემთა დამმუშავებელს უნდა შეეძლოს მოთხოვნის აშკარად უსაფუძვლო ან გადაჭარბებული ხასიათის დასაბუთება.

წვდომის უფლების შეზღუდვა შესაძლოა, წევრი სახელმწიფოების ეროვნული კანონმდებლობითაც იყოს გათვალისწინებული.

საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ("CNIL") სკუტერების გამქირავებელ კომპანიას 125,000 ევროს ოდენობით ჯარიმა დაუწესა

28.03.2021

2023 წლის 16 მარტს, "CNIL"-მა კომპანია "CITYSCOOT"-ს 125,000 ევროს ოდენობის ჯარიმა დააკისრა. კომპანიამ დაარღვია მომხმარებელთა პირადი ცხოვრების ხელშეუხებლობა, მათი გეოლოკაციის შესახებ მონაცემების თითქმის მუდმივ რეჟიმში მიღების გამო.

ფოტო: cityscoot.eu

საქმის გარემოებები

კომპანია "CITYSCOOT"-ის საქმიანობას სკუტერების მოკლე ვადით გაქირავება წარმოადგენდა. შემოწმების ფარგლებში, "CNIL"-მა დაადგინა, რომ კერძო პირის მიერ სკუტერის დაქირავებისას, კომპანია სატრანსპორტო საშუალების გეოლოკაციასთან დაკავშირებით ყოველ 30 წამში აგროვებდა მონაცემებს. გარდა ამისა, კომპანია გადაადგილების ჩანაწერსაც აწარმოებდა.

ზემოაღნიშნული დასკვნების საფუძველზე, “CNIL”-ის მიერ “CITYSCOOT“-ის დაჯარიმების გადაწყვეტილება მიღებულ იქნა ესპანეთისა და იტალიის მონაცემთა დაცვის საზედამხედველო ორგანოებთან თანამშრომლობით, რადგან “CITYSCOOT”-ი აღნიშნულ ქვეყნებშიც ოპერირებს.

ჯარიმის ოდენობის განსაზღვრისას გათვალისწინებულ იქნა კომპანიის წლიური ფინანსური ბრუნვა, მომხმარებელთა რაოდენობა (რომელიც 2022 წლის მონაცემის თანახმად, დაახლოებით 250 000-ს შეადგენდა) და გამოვლენილი დარღვევების სიმძიმე. ამასთანავე ყურადღება გამახვილდა კომპანიის მიერ დარღვევების აღმოფხვრისთვის განხორციელებულ ღონისძიებებზე.

გამოვლენილი დარღვევები

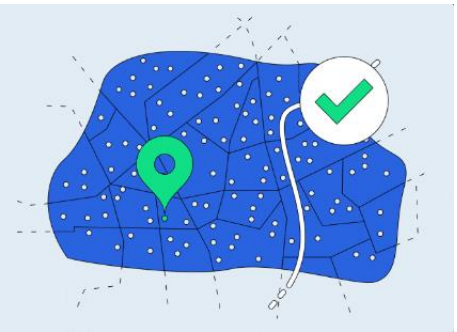
❶ მონაცემთა მინიმიზაციის ვალდებულების შეუსრულებლობა (GDPR-ის მე-5 მუხლის პირველი პუნქტის “c” ქვეპუნქტი):

კომპანია სკუტერების გეოლოკაციის შესახებ მონაცემებს სხვადასხვა მიზნით აგროვებდა:

- ✓ საგზაო მოძრაობის სამართალდარღვევათა შესახებ მონაცემების დამუშავება;
- ✓ მომხმარებელთა საჩივრების დამუშავება;
- ✓ საჭიროებისამებრ მომხმარებლის მხარდაჭერა;
- ✓ პრეტენზიებისა მართვა და ქურდობების პრევენცია.

კომპანიის მიერ დასახელებული დამუშავების მიზნების გაანალიზების შედეგად, “CNIL”-მა მიიჩნია, რომ მონაცემთა დამუშავების არცერთი დასახელებული მიზეზი ამართლებდა გეოლოკაციის მონაცემების ამგვარად დეტალურ შეგროვებას. მონაცემთა შეგროვებით მჟღავნდებოდა მომხმარებელთა გადაადგილების, ხშირად, მათ მიერ ნანახი ადგილების ან თუნდაც მოძრაობის პროცესში ყველა გაჩერების შესახებ მონაცემი.

კომპანიას იდენტური სერვისის მომხმარებლებისთვის მიწოდება თითქმის მუდმივ რეჟიმში, მათი გეოლოკაციის დადგენის გარეშე შეეძლო. შესაბამისად, “CITYSCOOT”-მა დაარღვია მონაცემთა მინიმიზაციის პრინციპი, რომლის მიხედვით მონაცემები უნდა იყოს ადეკვატური, შესაბამისი და დამუშავდეს მხოლოდ იმ მოცულობით, რაც აუცილებელია მონაცემთა შეგროვებისა და გამოყენების მიზნებისთვის.



ფოტო: cityscoot.eu

❷ უფლებამოსილი პირის მიერ განხორციელებული გადამუშავების ოპერაციებისთვის სახელშეკრულებო ჩარჩოს უზრუნველყოფის ვალდებულების

შეუსრულებლობა (GDPR-ის 28-ე მუხლის მე-3 პუნქტი):

“CNIL”-მა აღნიშნა, რომ “CITYSCOOT”-ის მიერ უფლებამოსილ პირებთან დადებული სამი ხელშეკრულება “GDPR”-ის მოთხოვნებს არ აკმაყოფილებდა. მსგავსი ხელშეკრულებები უნდა შეიცავდეს დებულებებს ისეთ საკითხებზე, როგორიცაა: მონაცემთა შეგროვება; უსაფრთხოების ზომები; ხელშეკრულების შეწყვეტის შემთხვევაში, თუ რა ბედი ეწევა მონაცემებს და სხვა.

❸ მომხმარებლის ინფორმირების ვალდებულების დარღვევა („საფრანგეთის მონაცემთა დაცვის აქტის“ 82-ე მუხლი):

მობილურ აპლიკაციაში ანგარიშის შექმნისას, ასევე, სისტემაში შესვლისას (“logging in”) და ვებგვერდზე დავიწყებული პაროლის აღდგენის პროცედურისთვის “CITYSCOOT”-ი იყენებდა “GOOGLE”-ის მექანიზმს (“reCAPTCHA”). აღნიშნული მექანიზმი ტექნიკური და პროგრამული უზრუნველყოფის ინფორმაციის შეგროვებით (როგორიცაა მოწყობილობისა და აპლიკაციის მონაცემები) მუშაობდა.

მიუხედავად იმისა, რომ შეგროვებული მონაცემები “GOOGLE”-ს შემდგომი ანალიზის მიზნით გადაეცემოდა, კომპანიას აღნიშნულის თაობაზე მომხმარებლებისთვის არ უცნობებია. გარდა ამისა, კომპანიამ არ მოიპოვა მომხმარებელთა წინასწარი თანხმობა „საფრანგეთის მონაცემთა დაცვის აქტის“ 82-ე მუხლის მოთხოვნათა დაცვით. თუმცა, კომპანიამ პროცედურის მომდინარეობისას განაცხადა, რომ აღნიშნული მექანიზმის გამოყენებას შეწყვეტდა.

ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ (“DPC”) მონაცემთა დამუშავებასთან დაკავშირებული საქმიანობის აღრიცხვის შესახებ მითითებები გამოაქვეყნა

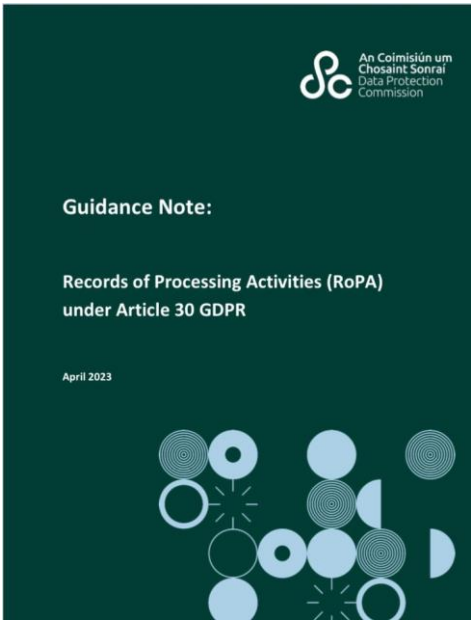
19.04.2023

2023 წლის 19 აპრილს ირლანდიის მონაცემთა დაცვის კომისრის მოადგილემ (“DPC”) სოციალურ ქსელ “LinkedIn”-ის მეშვეობით გამოაქვეყნა სახელმძღვანელო მონაცემთა დამუშავებასთან დაკავშირებული საქმიანობის აღრიცხვის შესახებ (RoPA).

მონაცემთა დაცვის ზოგადი რეგულაციის (“GDPR”) 30-ე მუხლის მიხედვით, მონაცემთა დამმუშავებელი ვალდებულია, აღრიცხოს და შეინახოს მისი უფლებამოსილების ფარგლებში დამუშავებასთან დაკავშირებული აქტივობები, ხოლო მონაცემთა დაცვის კომისრის მოთხოვნის შემთხვევაში — უზრუნველყოს მათი მიწოდება. უფრო მეტიც, კომისრის მოადგილის მიერ გამოქვეყნებულ სახელმძღვანელოში აღნიშნულია, რომ მონაცემთა დამუშავებასთან დაკავშირებული საქმიანობის აღრიცხვა წარმოადგენს შესაბამისობის დემონსტრირების ერთგვარ ღონისძიებას, რა დროსაც მონაცემთა დამმუშავებლები მოქმედებენ ანგარიშვალდებულების პრინციპის დაცვით, რომელიც განმტკიცებულია GDPR-ის მე-5(2) მუხლით.

სახელმძღვანელოს მიზანია, დაეხმაროს მონაცემთა დამმუშავებელს დაიცვას “GDPR”-ით გათვალისწინებული მონაცემთა დამუშავებასთან დაკავშირებული საქმიანობის აღრიცხვის პროცედურები.

სახელმძღვანელო შეიცავს საქმიანობის აღრიცხვის სანიმუშო პრაქტიკის მაგალითებს, დამუშავების აქტივობების დაჯგუფების ხერხებსა და პროცედურის სხვადასხვა გამონაკლისებს.*



ფოტო: www.linkedin.com

სოციალური ქსელი "Facebook"-ი თავის მომხმარებლებს პერსონალური მონაცემების უნებართვოდ გავრცელების გამო 725 მილიონ აშშ დოლარს გადაუხდის

ფოტო: bbc.com

სამართლებრივი დავა პერსონალური მონაცემების უნებართვოდ გავრცელების გამო 2019 წელს დაიწყო, რის შედეგად 2023 წლის მარტში, კალიფორნიის შტატის ფედერალურმა მოსამართლემ სოციალურ ქსელ "Facebook"-ს დაზარალებული მომხმარებლებისათვის მიყენებული ზიანის ანაზღაურების ვალდებულება დააკისრა.

2018 წელს, "Facebook"-მა 87 მილიონი მონაცემთა სუბიექტის პირად ინფორმაციაზე წვდომა, მათი თანხმობის გარეშე, გადასცა ანალიტიკურ ფირმას. კომპანია პერსონალურ მონაცემებზე დაყრდნობით სწავლობდა მომხმარებლების ფსიქოლოგიურ ქცევას, რის შემდგომაც იგი ზეგავლენას ახდენდა მათი, როგორც ამომრჩევლის არჩევანზე.

უპირველესად, ინფორმაცია გამჟღავნდა ფსიქოლოგიის პროფესორისგან, რომელმაც სოციალური ქსელის მილიონობით მომხმარებლის მონაცემები დაამუშავა და აპლიკაციის საშუალებით თითოეულ

* სახელმძღვანელოს გასაცნობად იხილეთ ბმული.

მათგანს „პიროვნების ტესტს“ სთავაზობდა. მოპოვებული ინფორმაცია კი გადაეცემოდა ანალიტიკურ კომპანიას, რომელიც სხვადასხვა მეთოდით ახდენდა ამომრჩევლის არჩევანზე ზეგავლენას.

საბოლოო ჯამში, “Meta”-მ აღნიშნული არ აღიარა, მაგრამ განაცხადა, რომ მიღწეულ იქნა მომხმარებლებთან გარკვეული შეთანხმება იმდენად, რამდენადაც აღნიშნული საზოგადოებისა და კორპორაციის აქციონერების ინტერესებში შედიოდა. შესაბამისად, “Facebook”-ის იმ მომხმარებლებს, რომლებმაც სოციალური ქსელის ანგარიში 2007 წლის 24 მაისიდან 2022 წლის 22 დეკემბრამდე შექმნეს, შესაძლებლობა აქვთ, პლატფორმის დედა-კომპანია “Meta”-ს 725 მილიონიანი ფონდიდან კუთვნილი წილის მისაღებად მიმართონ.

აღსანიშნავია, რომ “Meta” შესაბამის ანაზღაურებას მხოლოდ აშშ-ის მოქალაქეებს გადასცემს. ამასთანავე, უცნობია მისაღები თანხის ოდენობა, მაგრამ იგი განისაზღვრება იმის მიხედვით, თუ რა ხნის განმავლობაში სარგებლობდნენ მომხმარებლები “Facebook”-ის აქტიური ანგარიშით.

(+ 995 32) 242 1000
office@pdps.ge
www.pdps.ge