მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”) ფინანსურ მონაცემებზე წვდომის და საგადახდო მომსახურების შესახებ განცხადება გამოაქვეყნა

ნიდერლანდების სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა წაშლის უფლების დარღვევისთვის დააჯარიმა

ტელეკომუნიკაციის საბჭომ ევროკავშირის ციფრული პოლიტიკის მომავლის (“The Future of EU Digital Policy”) შესახებ სარეკომენდაციო დოკუმენტი შეიმუშავა

2024 წლის 21 მაისს, ტელეკომუნიკაციების საბჭომ (“The Telecoms Council”)[1] ერთხმად მიიღო სარეკომენდაციო ხასიათის დოკუმენტი, რომელშიც ასახულია საბჭოს დასკვნები ევროკავშირის ციფრული პოლიტიკის მომავლის შესახებ.[2]

ივნისი 2024

2024 წლის 21 მაისს, ტელეკომუნიკაციების საბჭომ (“The Telecoms Council”)[1] ერთხმად მიიღო სარეკომენდაციო ხასიათის დოკუმენტი, რომელშიც ასახულია საბჭოს დასკვნები ევროკავშირის ციფრული პოლიტიკის მომავლის შესახებ.[2]

აღსანიშნავია, რომ უკანასკნელი წლების განმავლობაში ევროკავშირის ფარგლებში ციფრული პოლიტიკის შესახებ არაერთი რეგულაცია იქნა მიღებული, მათ შორისაა, ხელოვნური ინტელექტისა[3] და მონაცემთა შესახებ[4] აქტები. ასევე, შეიქმნა ევროპის მონაცემთა ინოვაციის საბჭო, ევროპის ხელოვნური ინტელექტის საბჭო, რომელთა მიზანია ეროვნული კომპეტენტური ორგანოების კოორდინაცია ციფრული პოლიტიკის შემუშავების პროცესში. თანამედროვე ტენდენციების გათვალისწინებით, ევროკავშირის ერთიან ციფრულ ბაზარზე ფრაგმენტაციის ასარიდებლად, ევროკომისია და წევრი სახელმწიფოები აძლიერებენ კოორდინირებულ ურთიერთთანამშრომლობას.

რაც შეეხება უშუალოდ ტელეკომუნიკაციების საბჭოს მიერ შემუშავებულ სარეკომენდაციო დოკუმენტს, მასში ხაზგასმულია, რომ ევროპის ერთიანი ციფრული ბაზრის (“Digital Single Market”) გარდაქმნა და განვითარება მნიშვნელოვანია საზოგადოების ცხოვრების ხარისხის გაუმჯობესების, ეკონომიკური ზრდისა და მდგრადობის უზრუნველყოფის მიზნით.

სარეკომენდაციო დოკუმენტში წარმოდგენილია შემდეგი ძირითადი საკითხები:

- ციფრული მმართველობა და მისი მომწესრიგებელი წესები;
- „დიჯიტალიზაციის“ სოციალური ეფექტი;
- ციფრული და თანამედროვე ტექნოლოგიები;
- ციფრული ინფრასტრუქტურა;
- მონაცემთა დაცვის სტრატეგია;
- ციფრული უნარები;
- ციფრული გარდაქმნა;
- ევროკავშირის ციფრული პოლიტიკა.
-

სარეკომენდაციო დასკვნაში აღნიშნულია, რომ ინოვაციურ ტექნოლოგიებთან მიმართებით, გასათვალისწინებელია ერთიანი სტრატეგიული მიდგომები. საბჭოს რეკომენდაცია, ასევე, შეეხება მეწარმეობისა და კაპიტალის ბაზრის განვითარების ხელშეწყობის აუცილებლობას, რა მიზნითაც მნიშვნელოვანია, სათანადო გარანტიების შექმნა ციფრულ ტექნოლოგიებთან დაკავშირებული იმგვარი რისკების ასარიდებლად, როგორიცაა: დისკრიმინაცია, დეზინფორმაცია, კიბერძალადობა, პერსონალურ მონაცემთა მითვისება, მონაცემთა უსაფრთხოების დარღვევა და სხვა. ციფრული ტრანსფორმაციის პროცესში განსაკუთრებული როლი ენიჭება ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ განსაზღვრულ დებულებებს, რომელიც განსაზღვრავს რიგ ვალდებულებებს ონლაინ პლატფორმების საძიებო სისტემებთან მიმართებით.

სარეკომენდაციო დოკუმენტში ხაზგასმულია სოციალური რისკების დაძლევის მნიშვნელობა, განსაკუთრებით არასრულწლოვანთა უფლებების დასაცავად. ამასთან, სასურველია, შეიქმნას სადისკუსიო პლატფორმები და გაძლიერდეს ურთიერთთანამშრომლობა ევროკავშირის ფარგლებში სანდო და უსაფრთხო ონლაინ გარემოს შესაქმნელად.

წევრი სახელმწიფოებისა და ევროპული კომისიის მიზანია, კოორდინირებული ურთიერთთანამშრომლობით დაამკვიდრონ ერთიანი სტანდარტები ევროკავშირისა და ეროვნული კანონმდებლობის დონეზე, რისთვისაც მნიშვნელოვანია ციფრული, კიბერუსაფრთხოებისა და მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე ევროკავშირის შესაბამის ინსტიტუციებთან თანამშრომლობა:

„ქსელური და საინფორმაციო უსაფრთხოების ევროპული სააგენტო“ (“ENISA”); „ევროპული კიბერ უსაფრთხოების კომპეტენციის ცენტრი“ (“ECCC”); „მონაცემთა დაცვის ევროპული საბჭო“ (“EDPB”); „ელექტრონული კომუნიკაციების სფეროში ევროპული მარეგულირებელი ორგანო“ (“BEREC”).

ევროკავშირის ვალდებულება — უზრუნველყოს უსაფრთხო, დაცული, ინკლუზიური, ხელმისაწვდომი და მდგრადი ციფრული გარდაქმნა (“Digital Transformation”) ეფუძნება კონკურენტუნარიანობის პრინციპსა და ორიენტირებულია ადამიანის უფლებათა დაცვაზე. ევროკავშირი გამოხატავს სურვილს, ჰქონდეს წამყვანი როლი ციფრული გარდაქმნისა და მმართველობის პროცესში, რაც განავითარებს კვლევისა და ინოვაციის მიმართულებებს, ციფრულ შესაძლებლობებსა და ინფრასტრუქტურას.

ნიდერლანდების სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა წაშლის უფლების დარღვევისთვის დააჯარიმა

ნიდერლანდების სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა წაშლის უფლების დარღვევისთვის 6000 ევროს ოდენობით დააჯარიმა.[1]

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი წარმოადგენდა დასაქმების სააგენტოს, რომელიც სამუშაოს მაძიებლებს ეხმარებოდა ვაკანსიის პოვნაში. სააგენტო აღრიცხავდა და ვებგვერდზე რეგისტრირებული დამსაქმებლებისთვის საჯაროდ აქვეყნებდა: ფიზიკური პირის სახელსა და გვარს, მისამართს, ელექტრონულ ფოსტასა და ტელეფონის ნომერს, დაბადების თარიღს და ბიოგრაფიულ რეზიუმეს. რამდენიმე ვაკანსიის მოძიების შემდეგ სააგენტო უკავშირდებოდა ფიზიკურ პირს და დასაქმების რამდენიმე ალტერნატივას სთავაზობდა. სამუშაოს მაძიებლის თანხმობის შემთხვევაში და მისი მოთხოვნიდან 1 თვის ვადაში სააგენტო ვალდებული, იყო წაეშალა მონაცემები.

საქმის ფაქტობრივი გარემოებების თანახმად, ნიდერლანდების სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანოს მიმართა რამდენიმე ფიზიკურმა პირმა, რომლებიც აღნიშნავდნენ, რომ დასაქმების შემდეგ სააგენტო კვლავ აგრძელებდა მათი პერსონალური მონაცემების დამუშავებას, ვებგვერდიდან არ შლიდა თავდაპირველად მიწოდებულ მონაცემებს და არ აახლებდა საჯაროდ ხელმისაწვდომ ინფორმაციას

[1] საბჭო აერთიანებს ევროკავშირის წევრი სახელმწიფოების ციფრულ პოლიტიკაზე პასუხისმგებელ უწყებათა მინისტრებს.
[2] სრული ვერსია იხ. წინამდებარე ბმულზე: <https://data.consilium.europa.eu/doc/document/ST-9957-2024-INIT/en/pdf>.
[3] AI Act, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>, [5.06.2024].

მონაცემთა დაცვის საზედამხედველო ორგანომ იმსჯელა სააგენტოს მოქმედებების ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-17 მუხლის პირველ პუნქტთან და მე-12 მუხლის მე-3 პუნქტთან შესაბამისობის შესახებ და დაადგინა, რომ 650 მოთხოვნიდან მხოლოდ სამ შემთხვევაში გამოიკვეთა მონაცემთა წაშლის უფლების დარღვევა, რაც არ ათავისუფლებდა სააგენტოს პასუხისმგებლობისგან. საზედამხედველო ორგანომ გაითვალისწინა, რომ დარღვევა სააგენტოში დასაქმებული პირის შეცდომით იყო გამოწვეული, ხოლო სააგენტო სრულად აცნობიერებდა დაკისრებულ ვალდებულებებს.

ამდენად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს ჯარიმა მხოლოდ 6 000 ევროს ოდენობით განესაზღვრა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 58-ე მუხლის მე-2 პუნქტის (i) ქვეპუნქტის და 83-ე მუხლის მე-4 პუნქტის საფუძველზე.

მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”) ფინანსურ მონაცემებზე წვდომის და საგადახდო მომსახურების შესახებ განცხადება გამოაქვეყნა

2024 წლის 23 მაისს, მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”) ფინანსურ მონაცემებზე წვდომის და საგადახდო მომსახურების უზრუნველყოფის შესახებ განცხადება[1] გამოაქვეყნა, რომელიც შეეხება ევროკომისიის მიერ 2023 წელს, საფინანსო სფეროში თაღლითობის წინააღმდეგ ბრძოლის მიზნით წარდგენილი საკანონმდებლო ინიციატივების მხარდაჭერას:

- ფინანსურ მონაცემებზე წვდომა (Financial Data Access / FIDA);
- საგადახდო მომსახურების წესი (Payment Service Regulation / PSR);
- საგადახდო მომსახურების დირექტივა (Payment Service Directive / PSD3).

მონაცემთა დაცვის ევროპული საბჭოს მოსაზრება მიზნად ისახავს ზემოთ აღნიშნულ ინიციატივებთან დაკავშირებით მომხმარებელთა უფლებების დაცვის, ელექტრონული გადახდების კონკურენტული გარემოს და მონაცემთა გაზიარების წესების გაუმჯობესების მნიშვნელობის შესახებ სახელმძღვანელო რეკომენდაციების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებისათვის გაზიარებას.

განცხადებაში აღნიშნულია რეკომენდაციების ზოგადი შინაარსი:

1. გადარიცხვების მონიტორინგის მიზნით, მნიშვნელოვანია, რომ არსებობდეს პერსონალური მონაცემების კანონიერი დამუშავებისა და თაღლითობის წინააღმდეგ ბრძოლისთვის, უფლებამოსილი სუბიექტის მიერ მონაცემებზე წვდომის მოპოვების წინასწარ განსაზღვრული, მკაფიო წესები;

[1] AP (The Netherlands) - z2019-28837 <https://gdprhub.eu/index.php?title=AP_(The_Netherlands)_-_z2019-28837> [17.06.2024].

- საგადახდო მომსახურების გამწევი სუბიექტების ვალდებულებები მონაცემთა დამუშავების გამჭვირვალობის უზრუნველყოფისა და მინიმიზაციის ჭრილში;
- ფინანსურ მონაცემებზე წვდომის და საგადახდო მომსახურების გაწევისას მონაცემთა სუბიექტის თანხმობის განმარტება და მისი საჭიროება;
- ფინანსურ მონაცემებზე წვდომის და საგადახდო მომსახურების გაწევისთვის თანხმობის მოპოვების პირობები;
- საგადახდო მომსახურების გაწევისას განსაკუთრებული კატეგორიის მონაცემების დამუშავების წესი და პირობები;
- აღნიშნული ინიციატივის საფუძველზე, მნიშვნელობა საგადახდო მომსახურების სფეროში მონაცემთა დაცვის ეროვნულ საზედამხედველო ორგანოთა თანამშრომლობის აუცილებლობა.

მონაცემთა დაცვის ევროპული საბჭოს ზემოაღნიშნული რეკომენდაციები მიზნად ისახავს საფინანსო სფეროში თაღლითობის წინააღმდეგ ბრძოლის მიზნით წარდგენილ საკანონმდებლო ინიციატივებთან მიმართებით, პერსონალურ მონაცემთა დაცვის დამატებითი სამართლებრივი გარანტიების შემუშავებასა და ინტეგრირებას.

საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNIL”) ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების წესების თაობაზე რეკომენდაცია გამოაქვეყნა

2024 წლის 13 ივნისს, საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNIL”) გამოაქვეყნა რეკომენდაცია,[1] რომელიც ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავებას შეეხება. დოკუმენტში განხილულია მონაცემთა დაცვის საზედამხედველო ორგანოს წინასწარი ინფორმირების საკითხი ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების შემთხვევაში. რეკომენდაციის მიზანია, ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავებისას, მონაცემთა სუბიექტების უფლებების ჯეროვანი დაცვა.

“CNIL”-მა ყურადღება გაამახვილა პერსონალურ მონაცემთა დაცვის აქტზე, რომლის ითვალისწინებს ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების წესებს. კერძოდ, 65-ე მუხლის თანახმად, ჯანმრთელობის შესახებ პერსონალური მონაცემების დამუშავებისთვის საზედამხედველო ორგანოსგან წინასწარი ნებართვის მოპოვება არ არის საჭირო, თუ:

1] EDPB Statement 2/2024 on the financial data access and payments package.

- მონაცემთა სუბიექტმა განაცხადა მკაფიო თანხმობა ერთი ან რამდენიმე მიზნით მისი პერსონალური მონაცემის დამუშავების შესახებ;

- მონაცემთა სუბიექტს არ აქვს თანხმობის გაცემის შესაძლებლობა და მონაცემების დამუშავება აუცილებელია მისი ან სხვა ფიზიკური პირის არსებითი ინტერესების დასაცავად;

- მონაცემების დამუშავება აუცილებელია სამედიცინო დიაგნოზის დასმის, მკურნალობისა და ჯანდაცვის მიზნებისთვის.

“CNIL”-მა აღნიშნა, რომ ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავების პროცესის არსებითი ცვლილების შემთხვევაში, აუცილებელია ახალი მიდგომის გათვალისწინება. კერძოდ, „არსებით ცვლილებებში“ მოიაზრება მონაცემთა დამუშავების ახალი მიზნის არსებობა ან დამატებით, სხვა განსაკუთრებული კატეგორიის მონაცემების დამუშავება, რაც გამოქვეყნებული დოკუმენტის თანახმად, საჭიროებს მონაცემთა სუბიექტისგან ახალი თანხმობის მოპოვებას და მონაცემთა დაცვის საზედამხედველო ორგანოსგან ნებართვის მიღებას. იმ შემთხვევაში, თუ მონაცემების დამუშავება ხორციელდება “CNIL”-ის ნებართვის შემდგომ და მიმდინარე მონაცემთა დამუშავების პროცესი სცდება დამუშავების ფარგლებს, აუცილებელია ავტორიზაციის ხელახალი მოპოვება.

ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების კონტექსტში არსებით ცვლილებებად მოიაზრება:

- დამუშავებისთვის პასუხისმგებელი პირის ვინაობის შეცვლა ან თანადამუშავებაზე პასუხისმგებელი პირის დამატება;
- ჯანმრთელობის შესახებ მონაცემთა მიმღებ ახალ პირთა არსებობა;
- დამუშავების ახალი მიზანი;
- ახალი კატეგორიის სენსიტიური მონაცემების დამუშავება;
- მონაცემთა დამუშავება ახალი წყაროდან;
- ახალი მონაცემების დაკავშირება მონაცემთა წყაროსთან;
- დაინტერესებულ პირთა ოდენობის არსებითი ზრდა;
- თავდაპირველ მიზანთან მიმართებით მონაცემთა სუბიექტების უფლებების შეზღუდვა;
- მონაცემთა დამუშავებისა და შენახვის ვადების არსებითი გახანგრძლივება;
- ტექნიკური და ორგანიზაციული ზომების მოდიფიკაცია, რომლებიც ასუსტებს მონაცემთა უსაფრთხოებას.

[1] DataGuidance, France: CNIL provides recommendation on new health data processing procedures, 13 June 2024, <https://www.dataguidance.com/news/france-cnil-provides-recommendation-new-health-data>, [17.06.2024].

ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) დამუშავებისთვის პასუხისმგებელი პირი ინფორმაციის მიუწოდებლობის გამო დააჯარიმა

2024 წლის 22 მაისს, ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) გამოაქვეყნა გადაწყვეტილება, რომელიც დამუშავებისთვის პასუხისმგებელი პირის მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ დებულებების დარღვევას შეეხება.[1]

ფაქტობრივი გარემოებები:

2024 წლის 22 აპრილს, ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთი დამუშავებისთვის პასუხისმგებელი პირის შემოწმების ფარგლებში, მის წინააღმდეგ მონაცემთა სუბიექტის საჩივართან დაკავშირებით ინფორმაციის წარდგენა ორჯერ მოსთხოვა, თუმცა, აღნიშნულის მიუხედავად, საზედამხედველო ორგანოს ინფორმაცია არ გაუზიარა.

საზედამხედველო ორგანოს გადაწყვეტილება:

“GDPR”-ის 58-ე მუხლის პირველი პუნქტის “e” ქვეპუნქტის თანახმად, მონაცემთა დაცვის საზედამხედველო ორგანო უფლებამოსილია, საკითხის შესწავლის ფარგლებში დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოს შესაბამისი ინფორმაციის წარდგენა. ხოლო, აღნიშნული მოთხოვნის შეუსრულებლობა გამოიწვევს “GDPR”-ის 83-ე მუხლის მე-5 პუნქტის “e” ქვეპუნქტით განსაზღვრული სანქციის შეფარდებას.

აღნიშნულის გათვალისწინებით, საზედამხედველო ორგანომ მიზანშეწონილად მიიჩნია დამუშავებისთვის პასუხისმგებელი პირისათვის 160 000 ევროს ოდენობით სანქციის დაწესება. ჯარიმის განსაზღვრისას, საზედამხედველო ორგანომ მხედველობაში მიიღო დარღვევის სიმძიმე.

ადმინისტრაციული სამართალწარმოების შესახებ ესპანეთის სამეფოს კანონმდებლობის თანახმად, ჯარიმის მოცულობის შემცირების საფუძველს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ დარღვევის აღიარება, შესაბამისი პასუხისმგებლობის აღება და ჯარიმის ნებაყოფლობითი გადახდა წარმოადგენს, რის გამოც დამუშავებისთვის პასუხისმგებელი პირის მიმართ დადგენილი ჯარიმის ოდენობა 96 000 ევრომდე შემცირდა. ამავდროულად, საქმის შესწავლის მიზნით, ესპანეთის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს ზემოაღნიშნული ინფორმაციის წარდგენა 10 სამუშაო დღის ვადაში დაავალა.

[1] GDPRHub, AEPD (Spain), 22.05.2024: <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202405119>, [3.06.2024].

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ინტერნეტსივრცეში პერსონალურ მონაცემთა დაცვის თაობაზე ინსტრუქცია გამოაქვეყნა

2024 წლის 30 მაისს, იტალიის მონაცემთა დაცვის საზედამხედველო ორგანომ ("Garante per la protezione dei dati personali") გამოსცა ინსტრუქცია[1], რომელიც ვებგვერდებიდან მონაცემთა ავტომატური მოპოვებისას ("Web Scraping") პერსონალური მონაცემების დაცვას შეეხება. დოკუმენტში წარმოდგენილია წესები მესამე პირების მხრიდან მონაცემთა შეგროვების სტანდარტებთან დაკავშირებით, განსაკუთრებით კი ისეთ შემთხვევაში, როდესაც ხელოვნური ინტელექტის ("AI") სისტემები გამოიყენება.

იტალიის მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ შემუშავებულ ინსტრუქციაში ასახულია 2023 წლის დეკემბერში განხორციელებული ინსპექტირების შედეგები ვებგვერდიდან შეგროვებული პერსონალური მონაცემები ლეგიტიმური მიზეზების შეფასებების შესახებ. იტალიის საზედამხედველო ორგანო მიიჩნევს, რომ მნიშვნელოვანია, სწორად შეფასდეს პერსონალურ მონაცემთა დამუშავების პროცესები, რათა საჭიროებისამებრ შემუშავდეს ვებგვერდიდან მონაცემთა ავტომატური მოპოვების ("Web Scraping") შეჩერების ან მინიმიზაციის მექანიზმები.

შესაბამისად, იტალიის მონაცემთა დაცვის ორგანომ გასცა შემდეგი რეკომენდაციები:

- ვებგვერდის მომსახურების პირობებს ("Terms of Service") დაემატოს პუნქტები მონაცემების „სკრაპინგის" ("Web Scraping") წინააღმდეგ;
- ვებგვერდებზე შეიქმნას ე. წ. „რეზერვირებული სივრცე" ("Reserved Areas"), რომელიც მხოლოდ მომხმარებელთა დარეგისტრირების შემთხვევაში გახდება ხელმისაწვდომი;
- განხორციელდეს ვებგვერდებზე ინტერნეტტრაფიკის მონიტორინგის შემავალი და გამავალი მონაცემების ნებისმიერი უჩვეულო მოძრაობის იდენტიფიცირებისთვის;
- ვებგვერდებსა და პლატფორმებზე დაიბლოკოს ან შეიზღუდოს მონაცემებზე წვდომა ტექნოლოგიების გამოყენებით.
-

აღსანიშნავია, რომ იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ გამოქვეყნებული ინსტრუქცია სარეკომენდაციო ხასიათისაა. მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა შეიმუშაონ შესაბამისი ღონისძიებები „ვებსკრაპინგის" თავიდან ასარიდებლად ან შესამცირებლად. აღნიშნულ პროცესში გასათვალისწინებელია პერსონალურ მონაცემთა დამუშავების პროცესი, მოცულობა, კონტექსტი და მიზანი.

[1] Provvedimento del 20 maggio 2024 [10020316], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10020316; https://www.dataguidance.com/news/italy-garante-releases-instructions-defend-personal.

ჩეხეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა უკანონო დამუშავებისა და ინფორმირების ვალდებულების დარღვევისთვის დააჯარიმა

ჩეხეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა უკანონო დამუშავებისთვისა და ინფორმირების ვალდებულების დარღვევისთვის 13.9 მილიონი ევროს ოდენობით დააჯარიმა.[1]

საქმის ფაქტობრივი გარემოებების თანახმად, დამუშავებისთვის პასუხისმგებელი პირი წარმოადგენს წამყვან საექსპერტო დაწესებულებას, რომელიც საზოგადოებას პერსონალური მონაცემების და პირადი ცხოვრების ხელშეუხებლობის დაცვის მიზნით, შესაბამის მომსახურებას სთავაზობს. საქმის ფაქტობრივი გარემოებებით ასევე დადგინდა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტების პერსონალურ მონაცემებს ამუშავებდა ანტივირუსული პროგრამის მეშვეობით და დამუშავების შედეგებს შვილობილ კომპანიას გადასცემდა. აღნიშნულის შესახებ დამუშავებისთვის პასუხისმგებელი პირის მომხმარებლები არ იყვნენ ინფორმირებულნი.

აღსანიშნავია, რომ დამუშავებისთვის პასუხისმგებელი პირის შვილობილ კომპანიას 100 მილიონი მომხმარებლის ინტერნეტაქტივობის ისტორია ღია და იდენტიფიცირებადი ფორმით გადაეცა. ჩეხეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს განმარტებით, ინტერნეტაქტივობის ისტორია, თუნდაც არასრული ფორმით, წარმოადგენს პერსონალურ მონაცემს, რადგან იგი შესაძლებელია, უკავშირდებოდეს იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, მონაცემთა უკანონო დამუშავებისთვისა და მონაცემთა სუბიექტების ინფორმირების ვალდებულების დარღვევისათვის, დაეკისრა პასუხისმგებლობა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 და მე-13 მუხლის პირველი პუნქტის საფუძველზე.

[1] Czech SA imposed fine of 13.9 million EUR for infringement of Art. 6 and Art. 13 of GDPR, <edpb.europa.eu/news> [03.06.2024].

მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”) საერთაშორისო საჰაერო სატრანსპორტო საშუალების მგზავრთა სახის ამომცნობი სისტემის გამოყენების თაობაზე მოსაზრება გამოაქვეყნა

2024 წლის 23 მაისს, მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”) მოსაზრება გამოაქვეყნა,[1] რომელიც აეროპორტის ოპერატორებისა და ავიაკომპანიების მიერ მგზავრთა სახის ამომცნობი ტექნოლოგიების გამოყენებას შეეხება, რომლის მიზანია აეროპორტებში მგზავრთა დიდი ნაკადის მართვა მათი ავთენტიფიკაციისა და იდენტიფიკაციის უზრუნველყოფის საშუალებით. “EDPB” აღნიშნავს, რომ ბიომეტრიული მონაცემების, განსაკუთრებით კი სახის ამომცნობი სისტემის გამოყენება, მაღალ რისკს წარმოშობს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დაცვის თვალსაზრისით. ამგვარი მონაცემების დამუშავება, „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-9 მუხლის შესაბამისად, განსაკუთრებულ დაცვას საჭიროებს. სახის ამომცნობი ტექნოლოგიების გამოყენებამდე, მიზანშეწონილია, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა შეაფასონ მათი ზეგავლენა მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებზე. ამავდროულად, განიხილონ, შეიძლება თუ არა კონკრეტული მიზნის მიღწევა ნაკლებად მზღუდავი, სხვა საშუალებით.

დოკუმენტის მთავარი მიზანია პერსონალური მონაცემების დამუშავების თავსებადობის “GDPR”-ის მე-5 (1)(e), 25-ე და 32-ე მუხლებთან შესაბამისობის შეფასება შემდეგ კონკრეტულ შემთხვევებში: უსაფრთხოების საკონტროლო პუნქტი; ბარგის ჩასაბარებელი სივრცე; ჩასხდომის ეტაპი და მგზავრთა მიერ მოსასვენებელი სივრცე (“lounge”).

დოკუმენტის პირველ ნაწილში განხილულია ბიომეტრიული მონაცემების შენახვის საკითხები. “EDPB” ადგენს, რომ პერსონალური მონაცემების დამუშავების მიზნით განხორციელებული ღონისძიებები უნდა შეესაბამებოდეს აუცილებლობის პრინციპს, ხოლო დამუშავებისთვის პასუხისმგებელმა პირმა უნდა წარმოაჩინოს, რომ არ არსებობს ნაკლებად მზღუდავი საშუალება აღნიშნული მიზნის მისაღწევად. მონაცემთა დამუშავების სიმძიმე შესაძლებელია, დაბალანსდეს მგზავრთა მიერ კონტროლის მექანიზმითა და დამუშავების მიზნის მიღწევის შემდგომ, მათი პერსონალური მონაცემების წაშლის შესახებ ინფორმირებით.

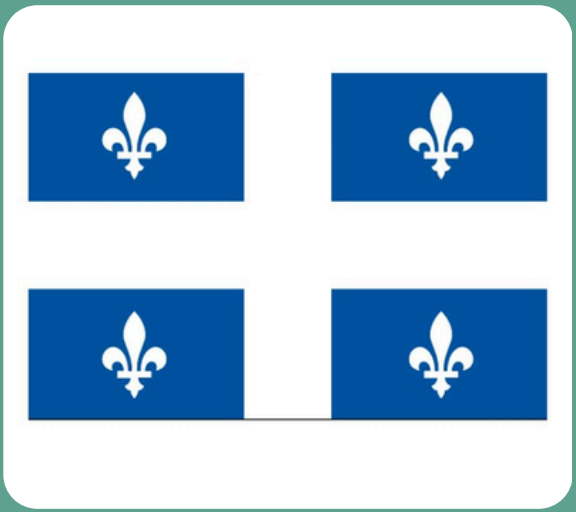
გამოქვეყნებული დოკუმენტის მეორე ნაწილი აეროპორტში პერსონალური მონაცემების დაშიფრული ფორმით შენახვის აუცილებლობას შეეხება. მონაცემთა დაცვის ევროპული საბჭოს მოსაზრებით, მონაცემების შენახვისას უნდა იქნას დაკმაყოფილებული აუცილებლობის პრინციპი. ამ შემთხვევაშიც, დამუშავებისთვის პასუხისმგებელ პირს უნდა შეეძლოს დაასაბუთოს, რომ ნაკლებად მზღუდავი საშუალება არ არსებობს კონკრეტული მიზნის მისაღწევად. დამატებით, დამუშავებისთვის პასუხისმგებელი პირი უნდა დარწმუნდეს, რომ მიიღო პერსონალურ მონაცემთა უსაფრთხოების უზრუნველსაყოფად შესაბამისი ზომები. მონაცემთა შენახვის ხანგრძლივობასთან მიმართებით “EDPB”-მ განმარტა, რომ “GDPR”-ის მე-5 (1)(e) მუხლის გათვალისწინებით, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა დაასაბუთოს შენახვის ვადის მართლზომიერება, მათ შორის, უნდა განისაზღვროს მონაცემთა შენახვის მინიმალური პერიოდი.

დოკუმენტის მესამე ნაწილში წარმოდგენილია აეროპორტის მონაცემთა ბაზაში საიდენტიფიკაციო და ბიომეტრიული მონაცემების შენახვის საკითხები. მოცემულ შემთხვევაში, აუცილებელია მონაცემთა ბაზის უსაფრთხოების უზრუნველყოფა, რადგან მისი დარღვევა გამოიწვევს მგზავრთა პერსონალურ მონაცემებზე არაავტორიზებულ პირთა წვდომას. აღნიშნულთან დაკავშირებით “EDPB” მიიჩნევს, რომ მგზავრთა ნაკადის ეფექტიანი მართვა შესაძლებელია ნაკლებად მზღუდავი საშუალებით, რომელიც მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებზე დიდ ზეგავლენას არ იქონიებს.

დოკუმენტის მეოთხე ნაწილში განხილულია ავიაკომპანიისა და მომსახურების მიმწოდებლის კონტროლის ფარგლებში პერსონალური მონაცემების სერვერზე შენახვის საკითხები. ასეთ შემთხვევაში არსებობს სხვა პირთა მიერ მგზავრთა პერსონალურ მონაცემებზე წვდომის შესაძლებლობა. შესაბამისად, “EDPB” მიუთითებს, რომ აუცილებელია პერსონალური მონაცემების გონივრული ვადით შენახვა, ასევე, აუცილებლობისა და პროპორციულობის პრინციპების გათვალისწინება. მონაცემთა დაცვის ევროპული საბჭოს მოსაზრებით, მგზავრთა ნაკადის ეფექტიანი მართვა შესაძლებელია ნაკლებად მზღუდავი საშუალებებით, რომლებსაც მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებზე არ ექნება დიდი ზეგავლენა.

დასკვნის სახით, შეიძლება ითქვას, რომ მონაცემთა დაცვის ევროპული საბჭოს მიერ მგზავრთა მიმართ სახის ამომცნობი მექანიზმების გამოყენების თაობაზე შემუშავებული მოსაზრების გათვალისწინება მნიშვნელოვანია მგზავრთა პერსონალური მონაცემების კანონიერი დამუშავების პროცესში მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დასაცავად.

[1] EDPB, Opinion 11/2024 on the use of facial recognition to streamline airport passengers’ flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, Adopted on 23 May 2024, <https://www.edpb.europa.eu/system/files/2024-05/edpb_opinion_202411_facialrecognitionairports_en.pdf>, [5.06.2024].



კანადის კვებეკის პროვინციაში „მონაცემთა დეპერსონალიზაციის აქტი“ მიიღეს

2024 წლის 15 მაისს, კანადის კვებეკის პროვინციაში „მონაცემთა დეპერსონალიზაციის აქტი“ მიიღეს, რომელიც 30 მაისიდან ამოქმედდა.[1] რეგულაცია კერძო და საჯარო სექტორში მონაცემთა დეპერსონალიზაციის ძირითად მიზნებს, პირობებსა და წესს განსაზღვრავს. იგი ადგენს კრიტერიუმებს, რომლის საფუძველზეც მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა შეაფასონ პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული რისკები და საფრთხეები.

„მონაცემთა დეპერსონალიზაციის აქტი“ სამი ნაწილისა და 10 მუხლისგან შედგება:

- პირველი ნაწილი — მიზანი და ტერმინთა განმარტება:
- აქტის მიზანია, საკანონმდებლო დონეზე განისაზღვროს მონაცემთა დეპერსონალიზაციის წესი და კრიტერიუმები, რომლებსაც გამოიყენებს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ყოველ კონკრეტულ შემთხვევაში.

- მეორე ნაწილი — მონაცემთა დეპერსონალიზაციის წესი:
- მონაცემთა დეპერსონალიზაციის პროცესის დაწყებამდე დამუშავებისთვის პასუხისმგებელმა პირმა უნდა განსაზღვროს მონაცემთა დეპერსონალიზაციის მიზანი. დარწმუნდეს, რომ მიზანი შეესაბამება მონაცემთა დაცვის ეროვნული კანონმდებლობის მოთხოვნებს. მონაცემთა დეპერსონალიზაცია უნდა განხორციელდეს ორგანიზაციის ხელმძღვანელი პირის ან კვალიფიციური სპეციალისტის მონაწილეობით. აქტში დეტალურადაა განხილული მონაცემთა დეპერსონალიზაციის პროცედურა, განხორციელებული შესაბამისი მოქმედებების აღრიცხვისა და რეგისტრაციის წესი.

- მესამე ნაწილი — დასკვნითი დებულებები განსაზღვრავს კანონის ამოქმედების საკითხს.

„მონაცემთა დეპერსონალიზაციის აქტის“ მიზანია კვებეკის პროვინციაში მონაცემთა დამუშავებისა და უსაფრთხოების წესების გაძლიერება, ასევე, მონაცემთა დეპერსონალიზაციის საკითხისთვის, დამუშავებისთვის პასუხისმგებელი პირების მიერ მონაცემთა დამუშავების პროცესების ეროვნულ კანონმდებლობასთან შესაბამისობის უზრუნველყოფა, რომელიც მოიცავს ფედერალურ დონეზე „პერსონალურ მონაცემთა დაცვისა და ელექტრონული დოკუმენტირების“, ხოლო სამხარეო დონეზე — „კერძო სექტორში მონაცემთა დაცვისა“ და „პერსონალური ინფორმაციის დაცვის მოდერნიზებულ“ აქტებს.

[1] Quebec’s Regulation on Anonymization Comes into Force, <publicationsduquebec.gouv.qc.ca> [05.06.2024].

“ChatGPT”-ის საკითხებზე მომუშავე ჯგუფმა “GDPR”-თან მის შესაბამისობაზე იმსჯელა

“ChatGPT”-ის[1] ფუნქციონირებასთან დაკავშირებული საკითხების განმხილველმა „ევროპის მონაცემთა დაცვის საბჭოს“ (“EDPS”) სამუშაო ჯგუფმა ხელოვნური ინტელექტის მონაცემთა დაცვის სტანდარტებთან შესაბამისობის შესახებ ანგარიში გამოაქვეყნა.[2] ანგარიშში წარმოდგენილია სამართლებრივი შეფასება, რომელიც ევროკავშირში “ChatGPT”-ის ფუნქციონირების პროცესში წამოჭრილ სამართლებრივ საკითხებს შეეხება. გასათვალისწინებელია, რომ “ChatGPT”-ის შესწავლა კვლავ მიმდინარეობს.

“GDPR”-ის თანახმად, პერსონალური მონაცემების დასამუშავებლად აუცილებელია შესაბამისი სამართლებრივი საფუძვლის არსებობა. ამ თვალსაზრისით “ChatGPT”-ს გააჩნია შეზღუდული არჩევანი და პერსონალური მონაცემის დამუშავების საფუძვლად იყენებს მხოლოდ ლეგიტიმურ ინტერესსა და მონაცემთა სუბიექტის თანხმობას. სამუშაო ჯგუფმა ყურადღება გაამახვილა პირადი ცხოვრების ხელშეუხებლობასთან დაკავშირებული რისკების შემცირების საჭიროებაზე. ამ მიმართულებით, პერსონალური მონაცემების დამუშავების პროცესში მნიშვნელოვანია გამჭვირვალობისა და სამართლიანობის პრინციპების გათვალისწინება. “GDPR”-თან შესაბამისობის თვალსაზრისით, შეშფოთებას იწვევს ინტერნეტ წყაროების მეშვეობით ინფორმაციის ამოღებისა (“web scraping”) და განსაკუთრებული კატეგორიის პერსონალური მონაცემების მოპოვება.

სამუშაო ჯგუფის შეფასებით, აუცილებელია, მონაცემთა დამუშავების პროცესის ყველა ეტაპზე შესაბამისი სამართლებრივი საფუძვლის არსებობა. ამავდროულად, მიზანშეწონილია, მიღებული იქნას შესაბამისი ზომები პირადი ცხოვრების ხელშეუხებლობის უფლებაზე ზეგავლენის შესამცირებლად. ასევე, გამჭვირვალობის პრინციპის დაცვის მიზნით, აუცილებელია პლატფორმის მომხმარებელთა ინფორმირება. ანგარიშში დამატებით აღნიშნულია, რომ მონაცემთა სუბიექტების მიერ უფლებებით სარგებლობის ხელშესაწყობად აუცილებელია ეფექტიანი მექანიზმების შემუშავება.

ანგარიშის დასკვნით ნაწილში აღნიშნულია, რომ ევროკავშირის მონაცემთა დაცვის რეგულაციებთან შესაბამისობა გარკვეულ გამოწვევად რჩება განსაკუთრებით ისეთი კომპანიისთვის, როგორიცაა “OpenAI”. ამისათვის, არსებითად მნიშვნელოვანია მისი მუდმივი მონიტორინგი ევროკავშირის პერსონალური მონაცემების დამუშავების სტანდარტებთან შესაბამისობის უზრუნველსაყოფად.

[1] “OpenAI”-ის სისტემური ნაწილი.
[2] Report of the work undertaken by the ChatGPT Taskforce, EDPB, 23 May 2024, <https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf>, [10.06.2024].

პროგრამა “Microsoft 365” შესაძლოა, არასრულწლოვან მონაცემთა სუბიექტთა უფლებებს არღვევდეს

დღესდღეობით, აქტუალური მნიშვნელობა შეიძინა პროგრამა “Microsoft 365”-ის საშუალებით არასრულწლოვანთა პერსონალურ მონაცემთა დამუშავების შესაბამისობამ ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციასთან“. პრობლემა წამოიჭრა მაშინ, როდესაც სკოლის მოსწავლეებს, როგორც მონაცემთა სუბიექტებს, გაუჩნდათ კითხვები და ინტერესი პროგრამის ფუნქციონირების მიმართ, კერძოდ, თუ ვის მიერ და რა ფორმით მუშავდებოდა მოსწავლეთა პერსონალური მონაცემები. დაინტერესებულ პირებს “Microsoft”-ის ოფიციალური განცხადებით განემარტათ, რომ სწორედ ზოგადსაგანმანათლებლო დაწესებულება წარმოადგენდა მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს და არა თავად კომპანია “Microsoft”-ი. ის ფაქტი, რომ ზოგადსაგანმანათლებლო დაწესებულებები აღნიშნულ პროგრამას სისტემურ და ფუნქციურ დონეზე ვერ მართავდნენ, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს შეფასებისა და განხილვის საგანი გახდა.

პროგრამა “Microsoft 365”-ის მიერ არასრულწლოვან მონაცემთა სუბიექტთა უფლებების შესაძლო დარღვევის საკითხზე, ავსტრიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოში რამდენიმე საჩივრის წარდგენის შემდეგ,[1] გამოიკვეთა ის პრობლემები, რომელთა გადასაჭრელად საზედამხედველო ორგანოს უნდა შეეფასებინა პროგრამის მართვის უფლების მქონე პირთა სტატუსი და უფლება-მოვალეობები.

ავსტრიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსთვის წარდგენილი საჩივრების თანახმად, ძირითადი პრობლემები უკავშირდება ისეთ საკითხებს, როგორიცაა:

1. ზოგადსაგანმანათლებლო დაწესებულებების მიერ პროგრამა “Microsoft 365”-ის გამოყენების პირობების კონტროლის და შეცვლის შეუძლებლობა. სკოლები აღნიშნულ პროგრამას, როგორც მოცემულობას ისე იღებენ და ეთანხმებიან იმ პირობებს, რომლებსაც ადგენს ან ცვლის კომპანია “Microsoft”;
2. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ განსაზღვრულ მონაცემთა სუბიექტთა უფლებების გაუთვალისწინებლობა. კერძოდ, პროგრამის მმართველი გუნდი აღნიშნულ პასუხისმგებლობას და შესაძლო რისკებს აკისრებს ზოგადსაგანმანათლებლო დაწესებულებებს, რომლებიც პროგრამის საშუალებით სასწავლო პროცესს წარმართავენ. რეალურად კი, სკოლები მოკლებულნი არიან შესაძლებლობას, ტექნიკურად გამართონ პროგრამა ისე, რომ უზრუნველყონ მონაცემთა დამუშავების გამჭვირვალობა და მონაცემთა სუბიექტთა ინფორმირება;
3. პროგრამის ფუნქციონირების სისტემური შეუთავსებლობა მონაცემთა დამუშავების მიზნებსა და საფუძვლებთან. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-4 მუხლის მე-7 პუნქტთან მიმართებით, აღნიშნული შეიძლება, იყოს დროსა და სივრცეში რეგულაციის მოთხოვნებთან აცდენილი პროცესი;

- არასრულწლოვნის პერსონალური მონაცემების უკანონო გამჟღავნების პრობლემა, სხვადასხვა შინაარსის მასალებზე არაუფლებამოსილ პირთა მიერ წვდომის მოპოვების რისკები. ამ შემთხვევაში, იგულისხმება გამჭვირვალობის პრინციპის დაუცველობა და მისი გაუთვალისწინებლობა.
- „მზა ჩანაწერების“ ფუნქციის არასაკმარისობა, რომელიც არასრულწლოვანთა მონაცემების დამუშავების განუსაზღვრელ მასშტაბს იღებს. ამ თვალსაზრისით აღსანიშნავია კომპანია “Microsoft”-ის მიერ ისეთი მოქმედებების განხორციელების შესაძლებლობა, რომლის შესახებ სკოლები და მოსწავლეები არ არიან ინფორმირებულნი, მაგალითად, პროფაილინგი და სხვა.
- პროგრამაში ატვირთული მასალებისა და დამუშავებული მონაცემების კონფიდენციალობის დაცვის პრობლემა. პროგრამული სისტემა ვერ უზრუნველყოფს მასში არსებული მონაცემების კონფიდენციალობის დაცვას, რისკების კონტროლსა და მონაცემთა სუბიექტისთვის შეტყობინებას.

ამდენად, ავსტრიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო უახლოეს პერიოდში განიხილავს ზემოაღნიშნულ საკითხებს, რაც განსაკუთრებულ და ყოველდღიურ გავლენას ახდენს არასრულწლოვნებზე, რომელთა მონაცემები პროგრამა “Microsoft 365”-ის მეშვეობით მუშავდება.

[1] Microsoft Violates Children’s Privacy – but Blames Your Local School, Data Subject Rights, <https://noyb.eu/en/microsoft-violates-childrens-privacy-blames-your-local-school> [10.06.2024].

ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) ბილბაოს კომერციული ბანკი (“BBVA”) მონაცემთა დამუშავების პრინციპის დარღვევისთვის 200 000 ევროს ოდენობით დააჯარიმა

2024 წლის 12 ივნისს, ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) გამოქვეყნა გადაწყვეტილება[1], რომელიც შეეხება კომერციულ ბანკ „ბილბაოს“ (“Banco Bilbao Vizcaya Argentaria”) მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ (“GDPR”) გათვალისწინებული მონაცემთა დამუშავების სიზუსტის პრინციპის დარღვევას.[2]

განმცხადებელი, რომელიც „ბილბაოს“ ბენეფიციარია, აღნიშნავდა, რომ ბანკმა მისი გადახდისუნარიანობის შესახებ პერსონალური მონაცემი საკრედიტო საინფორმაციო სერვისების კომპანიას გადასცა. აღნიშნული განხორციელდა მონაცემთა სუბიექტის წინასწარი გაფრთხილების შესახებ დადგენილი წესის დარღვევით, ვინაიდან შეტყობინება არასწორ მისამართზე გაიგზავნა.

“GDPR”-ის 5(1)(დ) მუხლით გათვალისწინებული მონაცემთა დამუშავების სიზუსტის პრინციპი მიხედვით, აუცილებელია, რომ შეგროვებული მონაცემები იყოს ზუსტი, ხოლო საჭიროების შემთხვევაში, იგი უნდა განახლდეს. ასევე, სავალდებულოა გონივრული ზომის მიღება არაზუსტი პერსონალური მონაცემების დაუყოვნებლივ წაშლის ან შესწორების მიზნით. ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს განმარტებით, კომერციულმა ბანკმა სერიოზული ზიანი მიაყენა მონაცემთა სუბიექტს, რადგან მან ვერ მიიღო შეტყობინება გადახდისუნარიანობის საქმესთან დაკავშირებით.

აქედან გამომდინარე, მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ ბანკმა დაარღვია “GDPR”-ის 5(1)(დ) მუხლით გათვალისწინებული სიზუსტის პრინციპი, რისთვისაც მას დაეკისრა ჯარიმა 200 000 ევროს ოდენობით. აღსანიშნავია, რომ მოგვიანებით საზედამხედველო ორგანოს მიერ ჯარიმის ოდენობა 120 000 ევრომდე შემცირდა.

[1] № PS-00088-2024, <https://www.aepd.es/documento/ps-00088-2024.pdf>.
[2] <https://www.dataguidance.com/news/spain-aepd-fines-bbva-200000-violation-principle>. “GDPR”-ის 5(1) (დ) მუხლის თანახმად, „პერსონალური მონაცემი უნდა იყოს ზუსტი და საჭიროებისამებრ განახლდეს. აუცილებელია ყველა გონივრული ზომის მიღება არაზუსტი პერსონალური მონაცემების დაუყოვნებლივ წასაშლელად ან შესასწორებლად, მათი დამუშავების მიზნების გათვალისწინებით“.

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს მისი თანამშრომლის პერსონალური მონაცემების უკანონო დამუშავებისთვის პასუხისმგებლობა დააკისრა

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს — იტალიის იუსტიციის სამინისტროს, თანამშრომლის პერსონალური მონაცემების უკანონო დამუშავებისთვის პასუხისმგებლობა დააკისრა.[1] ფაქტობრივი გარემოებების თანახმად, იუსტიციის სამინისტროში დასაქმებული პირი დარეგისტრირებული იყო ე. წ. „გაცნობის აპლიკაციაზე“, სადაც იგი ათავსებდა საკუთარ ფოტოებს, ასევე, მითითებული ჰქონდა საკუთარი საკონტაქტო ინფორმაცია და ფსევდონიმი. მონაცემთა სუბიექტის თანამშრომლებმა აღნიშნულის შესახებ აცნობეს ხელმძღვანელობას, რის საფუძველზე სამინისტროში დასაქმებული პირის მიმართ დაიწყო დისციპლინური წარმოება. დადგინდა, რომ სამსახურებრივი უფლებამოსილების შესრულებისას, მონაცემთა სუბიექტს არ ჩაუდენია დისციპლინური გადაცდომა.

აღნიშნულის გათვალისწინებით, სამინისტროში დასაქმებულმა პირმა მიმართა იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს და მიუთითა, რომ დამსაქმებელმა უკანონოდ დაამუშავა მის სექსუალურ ცხოვრებასთან და ორიენტაციასთან დაკავშირებული პერსონალური მონაცემები. სამინისტროს თანახმად, დასაქმებული პირის პერსონალურ მონაცემთა დამუშავება კანონიერი იყო იტალიის შრომის კანონმდებლობის მიხედვით, რომელიც დამსაქმებელს შესაძლებლობას ანიჭებს, შეამოწმოს საჯარო დაწესებულებების თანამშრომლის საქმიანობა. დამუშავებისთვის პასუხისმგებელი პირი აღნიშნავდა, რომ მონაცემთა სუბიექტმა თავად გახადა ხელმისაწვდომი ის ინფორმაცია, რომელიც შემდგომ სამინისტროს მიერ იქნა დამუშავებული.

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს შეფასებით, შრომის კანონმდებლობა მხოლოდ იმ შემთხვევაში განსაზღვრავს დასაქმებულის პირადი ცხოვრების შესახებ ინფორმაციის შესწავლას, თუკი აღნიშნული უკავშირებდა მის მიერ შესრულებულ სამუშაოს. მოცემულ შემთხვევაში მონაცემთა სუბიექტის სექსუალური ცხოვრების შესახებ ინფორმაციის დამუშავება არ იყო დაკავშირებული დასაქმებულის მიერ სამუშაოს შესრულებასთან. შესაბამისად, საზედამხედველო ორგანომ აღნიშნა, მიუხედავად იმისა, რომ მონაცემთა სუბიექტმა აპლიკაციაში თავად განათავსა ფოტოები, საკონტაქტო ინფორმაცია და ფსევდონიმი, დამუშავებისთვის პასუხისმგებელ პირს მაინც სჭირდებოდა სამართლებრივი საფუძველი აღნიშნულ მონაცემთა დასამუშავებლად, რომელიც, საზედამხედველო ორგანოს შეფასებით, სამინისტროს არ გააჩნდა.

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის პირველი პუნქტის „ა“, ასევე, მე-6, მე-9 და 88-ე მუხლები.

მეორე მხრივ, აღსანიშნავია, რომ საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირი სამართალდარღვევისთვის გააფრთხილა რეგულაციის 58-ე მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტის შესაბამისად. თუმცა ჯარიმა არ დააკისრა, სამინისტროს მიერ დისციპლინური წარმოების შესაბამისი წესებისა და კონფიდენციალობის სრული დაცვით განხორციელებისა და საზედამხედველო ორგანოსთან თანამშრომლობის გამო.

კომპანია “Google”-მა მომხმარებელთა ადგილმდებარეობის ისტორიის წაშლა დაიწყო

2024 წლის 10 ივნისს, “Google”-მა განაცხადა, რომ პერსონალური მონაცემების შენახვის შეზღუდვის ვალდებულების გათვალისწინებით, კომპანია გეგმავს მომხმარებელთა ადგილმდებარეობის შესახებ ყველა ინფორმაციის წაშლას,[1] რაც, ცხადია, მომხმარებელთა სურვილის არსებობის შემთხვევაში, ასევე, არ გამორიცხავს „ადგილმდებარეობის ისტორიის“ (“location data”) შენახვის შესაძლებლობას. აღსანიშნავია, რომ პერსონალური მონაცემები შეინახება მხოლოდ მომხმარებელთა პირად მოწყობილობაზე და არა “Google”-ის სერვერზე. საგულისხმოა, რომ მონაცემთა სუბიექტებს პირველ დეკემბრამდე აქვთ ვადა, მათი პერსონალური მონაცემების შესანახად. წინააღმდეგ შემთხვევაში, ინფორმაცია სამუდამოდ წაიშლება.

გარდა აღნიშნულისა, “Google”-ი შეამცირებს ადგილმდებარეობის ისტორიის შენახვის ხანგრძლივობასაც. კერძოდ, ინფორმაცია, ნაცვლად 18 თვისა, შენახვიდან 3 თვის შემდეგ წაიშლება. კომპანიას არ დაუსახელებია განხორციელებული ცვლილებების მიზეზები, თუმცა ხაზგასმით აღინიშნა მონაცემთა სუბიექტთა ნება, წაშლილიყო მათი გეოლოკაციის ისტორია. მომხმარებლების ადგილმდებარეობის შესახებ ინფორმაციის დაცვის გათვალისწინებით, “Google Maps”-ი არ მიჰყიდის სარეკლამო აგენტებს ან მესამე მხარეებს მომხმარებელთა პერსონალურ მონაცემებს.

აღსანიშნავია, რომ “Google”-ის მიერ მონაცემთა სუბიექტების პირადი ცხოვრების ხელშეუხებლობის დაცვის სტანდარტების გაძლიერება განაპირობა სამართალდამცავი მიზნებისთვის მომხმარებელთა მონაცემების გადაცემის გახშირებულმა მოთხოვნამ. აღნიშნული კი გულისხმობდა მონაცემთა სუბიექტებზე ზედამხედველობის განხორციელებას, რის შედეგადაც “Google”-ი იძულებული იყო, გაემჟღავნებინა მომხმარებელთა პერსონალური ინფორმაცია.

[1] Google to Delete Users’ Location Data, <https://gdprbuzz.com/news/google-to-delete-users-location-data/> [19.06.2024].

[1] Garante per la protezione dei dati personali (Italy) – 10021491, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_10021491> [19.06.2024].

(+ 995 32) 242
1000 o ce@pdps.ge
w w w.pdps.ge