მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ არასრულწლოვანთა პერსონალური მონაცემების დამუშავების პროცესის შესწავლისას, პასუხისმგებელ და უფლებამოსილ პირებს შორის ხელშეკრულების არარსებობის ფაქტი გამოავლინა

ბავშვების ციფრული უსაფრთხოების შესახებ ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის (“OECD”) ანგარიში

ბიზნეს-სოციალურმა ქსელმა “LinkedIn”-მა მიზნობრივი რეკლამები შეზღუდა

ბიზნეს-სოციალური ქსელის — “LinkedIn”-ის გადაწყვეტილებით, 2024 წლიდან პლატფორმაზე აიკრძალა “LinkedIn Groups”-ის მონაცემების გამოყენებით სარეკლამო აგენტების მიერ მიზნობრივი რეკლამების განთავსება.[1] გადაწყვეტილებას საფუძვლად უდევს სამოქალაქო საზოგადოების სხვადასხვა ჯგუფის მიერ ევროკომისიაში წარდგენილი საჩივარი „ციფრული სერვისების შესახებ“ აქტის (“DSA“) შესაძლო დარღვევასთან დაკავშირებით

ივლისი 2024

აქტი მიმდინარე წლის თებერვალში შევიდა ძალაში და მისი მიზანია ელექტრონული შინაარსის (“Content”) მართვის მკაცრი რეგულაციების დაწესება, რაც მოიცავს ვალდებულებებს ალგორითმულ გამჭვირვალობასა და მიზნობრივ რეკლამებთან დაკავშირებით.

2010 წელს კომპანია “Microsoft”-ის საკუთრებაში არსებულმა ბიზნეს-სოციალურმა ქსელმა ერთგვაროვანი ინტერესების მქონე მომხმარებლებს შორის კავშირების გასამარტივებლად, შექმნა ე. წ. პლატფორმა “Groups”. მიუხედავად “Groups”-ის დამოუკიდებელ აპლიკაციად ჩამოყალიბების მცდელობისა, იგი 2018 წელს გაერთიანდა “LinkedIn“-ის მთავარ აპლიკაციაში. განსაკუთრებული კატეგორიის პერსონალური მონაცემების ბოროტად გამოყენების პოტენციური რისკის შესახებ ევროკომისიის მოთხოვნის პასუხად, “LinkedIn”-მა აკრძალა ე. წ. სარეკლამო აუდიტორიები ევროპაში “LinkedIn” ჯგუფის წევრობის მონაცემებზე დაყრდნობით.

შედეგად, “LinkedIn”-ის გადაწყვეტილებით, სრულად აღმოიფხვრა “LinkedIn Groups”-ის მონაცემების გამოყენებით მიზნობრივი რეკლამების განთავსების ფუნქცია, რათა დაცული ყოფილიყო „ციფრული სერვისების შესახებ“ აქტის (“DSA”) პრინციპებთან და მარეგულირებელ სტანდარტებთან შესაბამისობა. აღსანიშნავია, რომ ევროკომისია ზედამხედველობას გაუწევს “LinkedIn”-ის მიერ საჯარო ვალდებულებების და ხსენებული აქტის მოთხოვნათა დაცვას.

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ არასრულწლოვანთა პერსონალური მონაცემების დამუშავების პროცესის შესწავლისას, პასუხისმგებელ და უფლებამოსილ პირებს შორის ხელშეკრულების არარსებობის ფაქტი გამოავლინა

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელი პირი — ჰელსინკის ადმინისტრაცია,[1] დამუშავებაზე უფლებამოსილი პირის — ერთ-ერთი კომპანიის დახმარებით ამუშავებდა არასრულწლოვნების, კერძოდ, სკოლის მოსწავლეთა პერსონალურ მონაცემებს.

მონაცემები მუშავდებოდა ელექტრონული აპლიკაციის საშუალებით, რომლითაც მონაცემთა სუბიექტებს შესაძლებლობა ჰქონდათ, დაკავშირებოდნენ სკოლის ადმინისტრაციას ან ფსიქოლოგს.[2] ფაქტობრივი გარემოებების შესწავლის შედეგად დადგინდა, რომ აპლიკაციის შემუშავებიდან საქმის განხილვის დროისთვის დამუშავებისთვის პასუხისმგებელ და დამუშავებაზე უფლებამოსილ პირებს შორის ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) 28-ე მუხლით განსაზღვრული ხელშეკრულება არ იყო დადებული.[3]

დამუშავებისთვის პასუხისმგებელმა პირმა განმარტა, რომ იგი უკვე აღარ სარგებლობდა დამუშავებაზე უფლებამოსილი პირის — ერთ-ერთი კომპანიის მომსახურებით, თუმცა აპლიკაციის გამოყენების უზრუნველსაყოფად, იგი სხვა უფლებამოსილ პირს დაუკავშირდა. აღნიშნულის მიუხედავად, სხვა უფლებამოსილ პირთან გაფორმებული შეთანხმებაც არ შეიცავდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 28-ე მუხლით გათვალისწინებულ მოთხოვნებს.

რეგულაციის 28-ე მუხლის მე-3 პუნქტი განსაზღვრავს, რომ უფლებამოსილი პირის მიერ მონაცემების დამუშავების პროცესი წესრიგდება ხელშეკრულებით ან ევროკავშირის ან წევრი სახელმწიფოების კანონმდებლობით დადგენილი სხვა სამართლებრივი აქტით, რომელიც უფლებამოსილ პირს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის წინაშე აკისრებს გარკვეულ ვალდებულებებს და განსაზღვრავს მონაცემთა დამუშავების მიზანს, ხასიათს, ხანგრძლივობას, დასამუშავებელ მონაცემთა და მონაცემთა სუბიექტების კატეგორიებს, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის უფლებებსა და ვალდებულებებს.[4]
ზემოაღნიშნულის გათვალისწინებით, ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირი ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 28-ე მუხლის მე-3 პუნქტის დამრღვევად მიიჩნია, თუმცა არ დააკისრა ჯარიმა ფინეთის „მონაცემთა დაცვის შესახებ კანონის“ 24-ე მუხლის მე-2 პუნქტიდან გამომდინარე,[5] რომლის თანახმად, საჯარო ორგანოს ადმინისტრაციული ჯარიმა არ ეკისრება.

სკანდინავიის ქვეყნების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებმა ონლაინ თამაშებით სარგებლობისას ბავშვთა პერსონალურ მონაცემთა დაცვის შესახებ სახელმძღვანელო გამოაქვეყნეს

2024 წლის 30 მაისს, სკანდინავიის ქვეყნების (“Nordic DPAs”) პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებმა გამოაქვეყნეს სახელმძღვანელო,[1] რომელიც ონლაინ თამაშების პროცესში ბავშვთა პერსონალური მონაცემების დაცვის საკითხებს შეეხება. დოკუმენტის შემუშავების საფუძველი გახდა 2022 წლის 13-14 ოქტომბერს, ჰელსინკში გამართული სკანდინავიის ქვეყნების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოთა შეხვედრა, რომლის ფარგლებშიც მიღებულ იქნა „ჰელსინკის დეკლარაცია“ (“Helsinki Declaration”).

[1] Principles on Children & Online Gaming, <https://www.datatilsynet.dk/Media/638544622578121029/Principle%20on%20Children%20and%20Online%20Gaming%20june24.pdf>, [21.06.2024].

შეხვედრაზე პრიორიტეტულ საკითხად ბავშვების პერსონალური მონაცემების დაცვა დასახელდა. დანიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ყურადღება გაამახვილა ონლაინ თამაშებთან მიმართებით ბავშვთა პერსონალური მონაცემების დაცვის საჭიროებაზე. აღნიშნული მიზნით შეიქმნა სკანდინავიის ქვეყნების საზედამხედველო ორგანოების (“Nordic DPA”) სამუშაო ჯგუფი, რომლის მთავარ ორიენტირს ონლაინ თამაშებით სარგებლობისას ბავშვთა პერსონალურ მონაცემთა დაცვა წარმოადგენდა.

ონლაინ თამაშებით სარგებლობისას ბავშვთა პერსონალურ მონაცემთა დაცვის შესახებ სახელმძღვანელოში აღნიშნულია, რომ ონლაინ თამაშები ფართოდ ხელმისაწვდომია არასრულწლოვნებისთვის, რაც ქმნის გარკვეულ რისკებს მათი პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა დაცვის თვალსაზრისით. აღნიშნულის საპასუხოდ, დამუშავებისთვის პასუხისმგებელი პირი, რომელიც განსაზღვრავს მონაცემთა დამუშავების მიზნებს, ვალდებულია, გაითვალისწინოს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ დადგენილი სტანდარტები, ონლაინ თამაშების მომხმარებლების — მონაცემთა სუბიექტების უფლებების დასაცავად. ასევე, განსაკუთრებული სიფრთხილით უნდა დამუშავდეს ბავშვების პერსონალური მონაცემები. რეგულაციის პრეამბულის 38-ე პუნქტის თანახმად, „ბავშვები სარგებლობენ პერსონალური მონაცემების დაცვის განსაკუთრებული უფლებით, რადგან მათთვის შეიძლება ნაკლებად იყოს ცნობილი ის რისკები, შედეგები, დაცვის მექანიზმები და მათი უფლებები, რომლებიც უკავშირდება პერსონალური მონაცემების დამუშავებას“.

სახელმძღვანელოში განხილულია ონლაინ თამაშების კონტექსტში ბავშვების პერსონალური მონაცემების დამუშავების პროცესის ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებთან შესაბამისობა. დოკუმენტში განხილულია სამართლიანობის, გამჭვირვალობის, მონაცემთა მინიმიზაციისა და ანგარიშვალდებულების პრინციპები. სახელმძღვანელო დამუშავებისთვის პასუხისმგებელ პირებს მონაცემთა დამუშავების პროცესის კანონმდებლობასთან შესაბამისობის მოყვანაში დაეხმარებათ, რაც იქნება მონაცემთა სუბიექტის უფლებების დაცვის დამატებითი გარანტია.
საკითხი აქტუალურია საქართველოშიც, რის გათვალისწინებით, 2022 წლის პირველ ივნისს, საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურმა გამოაქვეყნა გზამკვლევი,[1] რომელიც ციფრულ გარემოში ბავშვის პერსონალური მონაცემების დაცვის საკითხებს შეეხება. დოკუმენტის მიზანია ციფრულ გარემოში ბავშვების უფლებებთან დაკავშირებით საუკეთესო საერთაშორისო სტანდარტების შესწავლა და მათი ეროვნულ კანონმდებლობასთან მისადაგება.

[1] პერსონალურ მონაცემთა დაცვის სამსახური, „ციფრულ გარემოში ბავშვის პერსონალურ მონაცემთა დაცვის გზამკვლევი“, 2022 წელი, <https://shorturl.at/BwMlk>, [21.06.2024].

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ სახელმძღვანელო დოკუმენტი გამოაქვეყნა

2024 წლის 18 ივნისს, ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ სახელმძღვანელო გამოაქვეყნა.[1] დოკუმენტში აღნიშნულია, რომ ოფიცერი აუცილებლად უნდა იყოს დამოუკიდებელი. იგი უნდა აღიჭურვოს სათანადო რესურსებითა და ძალაუფლებით. ამასთანავე, დაუშვებელია ოფიცრის დაჯარიმება და პოზიციიდან გათავისუფლება მის მიერ ფუნქციების ჯეროვანი განხორციელების გამო, რაც მიუთითებს მის დამოუკიდებელ ავტონომიასა და მისი დაცვის დამატებით სამართლებრივ გარანტიებზე.

სახელმძღვანელოში განხილულია პერსონალურ მონაცემთა დაცვის ოფიცრის ძირითადი უფლება-მოვალეობები:

·დაკისრებული ამოცანების შესასრულებლად ჰქონდეს წვდომა აუცილებელ და სათანადო რესურსებზე;
·ადრეული ეტაპიდან ჩართული იყოს პერსონალურ მონაცემთა დაცვასთან დაკავშირებული რიგი საკითხების გადაწყვეტაში;
·ჰქონდეს წვდომა ყველა შესაბამის ინფორმაციაზე, რომელიც აუცილებელია მისი უფლებამოსილების განსახორციელებლად;
·გასცეს კონსულტაცია პერსონალურ მონაცემთა დაცვის საკითხებზე;
·დაესწროს პერსონალურ მონაცემთა დაცვასთან დაკავშირებული გადაწყვეტილების მიღების პროცესს;
·მკაფიოდ და წერილობითი ფორმით ჰქონდეს განსაზღვრული ორგანიზაციაში დასაქმებულთა მოვალეობები;

·იყოს ანგარიშვალდებული უწყების ან ორგანიზაციის უმაღლესი მენეჯმენტის წინაშე; ამასთანავე, მოიწვიონ მათ შეხვედრებზე.

სახელმძღვანელოში, ასევე, ხაზგასმულია პერსონალურ მონაცემთა დაცვის ოფიცრის ინტერესთა კონფლიქტის აკრძალვის ვალდებულება. დაუშვებელია, რომ უწყებაში ან ორგანიზაციაში ოფიცერი იკავებდეს იმგვარ პოზიციას ან თანამდებობას, რომელიც მას შესაძლებლობას მისცემს, განსაზღვროს მონაცემთა დამუშავების მიზანი და საშუალება. შესაბამისად, იგი არ უნდა იყოს მონაცემთა დამუშავებისთვის პასუხისმგებელი ან/და მონაცემთა დამუშავებაზე უფლებამოსილი პირი. სახელმძღვანელოში აგრეთვე წარმოდგენილია „ევროპის მონაცემთა დაცვის ზედამხედველის“ (“EDPS”) შეფასება, რომლის თანახმად, ინტერესთა კონფლიქტი სახეზეა, როდესაც ოფიცრის მიერ სხვა მოვალეობების განხორციელება ნეგატიურად აისახება პერსონალური მონაცემების დაცვაზე.

აღსანიშნავია, რომ 2024 წელს პერსონალურ მონაცემთა დაცვის სამსახურმა შეიმუშავა რეკომენდაციები პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ[1], რომელიც მიზნად ისახავს, ოფიცრის ინსტიტუტის მომწესრიგებელი ნორმის — „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 33-ე მუხლის განმარტებას, მისი იმპლემენტაციის პროცესში საუკეთესო პრაქტიკის დამკვიდრების ხელშეწყობის მიზნით.

ბავშვების ციფრული უსაფრთხოების შესახებ ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის (“OECD”) ანგარიში

2024 წლის 21 ივნისს, ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციამ (“OECD”) გამოაქვეყნა ანგარიში, რომელიც ბავშვების ციფრული უსაფრთხოების საკითხებს შეეხება. დოკუმენტში აღნიშნულია, რომ ციფრული გარემო ბავშვების ცხოვრების განუყოფელი ნაწილია, რაც ქმნის მნიშვნელოვან რისკებს მათი პირადი ცხოვრების ხელშეუხებლობის თვალსაზრისით. თანამედროვე ტექნოლოგიების განვითარებასთან ერთად, მეტად გამოიკვეთა ბავშვების პერსონალურ მონაცემთა დაცვის მიზნით დაუყოვნებლივი ღონისძიებების განხორციელების საჭიროება. შესაბამისად, “OECD”-ის მიერ შემუშავებულ დოკუმენტში განხილულია ახალი პროდუქტის ან მომსახურების შექმნისას, ბავშვების ციფრულ გარემოში უსაფრთხოებასთან დაკავშირებული საკითხები.

ანგარიშში წარმოდგენილია პრაქტიკული მაგალითები ონლაინ სივრცეში ბავშვების ციფრული უსაფრთხოების საკითხზე. აღსანიშნავია, რომ სახელმწიფოებმა ბავშვების ციფრული უსაფრთხოების დასაცავად არაერთი კანონი მიიღეს, რამაც შესაძლებელია, წარმოშვას გარკვეული რისკები საერთაშორისო ნორმებთან მიმართებით. ამდენად, მნიშვნელოვანია ადამიანის უფლებებზე ორიენტირებული მიდგომის დანერგვა, დაინტერესებულ პირებს შორის მრავალმხრივი დიალოგების წარმართვა და საერთაშორისო თანამშრომლობა, რაც ხელს შეუწყობს ეფექტიანი ციფრული პოლიტიკის ჩამოყალიბებას, მონაცემთა სუბიექტთა უფლებების დაცვას.

ანგარიშში წარმოდგენილია ახალი პროდუქტის ან მომსახურების შექმნისას ბავშვების ციფრულ გარემოში უსაფრთხოებასთან დაკავშირებული ძირითადი ასპექტები:

·ასაკის დამადასტურებელი მექანიზმების დანერგვა, რომლის შესაბამისადაც მომსახურების მიმწოდებლებს არასრულწლოვანი მომხმარებლების იდენტიფიცირების შესაძლებლობა ექნებათ;

·ბავშვებზე მორგებული დიზაინის შემუშავება, რომელიც გულისხმობს არასრულწლოვანის საჭიროებების გათვალისწინებას და მათი უსაფრთხოების ხელშეწყობას;

[1] რეკომენდაციები პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ, 2024, <https://pdps.ge/ka/content/984/rekomendaciebi> [21.06.2024].

·ზიანის რისკის იდენტიფიცირება და პრევენცია — მომსახურების მიმწოდებლებმა, ტექნიკური უსაფრთხოების ზომების მიღებით, პროაქტიულად უნდა გამოავლინონ რისკები და განახორციელონ შესაბამისი ღონისძიებები მათ შესამცირებლად;

·ბავშვების პირადი ცხოვრების ხელშეუხებლობის დარღვევამ და მათი მონაცემების არასათანადო გამოყენებამ შეიძლება, პირდაპირი გავლენა იქონიოს მათ უსაფრთხოებაზე;

·ინფორმაციის მიწოდება ბავშვებზე მორგებული ფორმით — ბავშვებს უნდა მიეწოდოთ შესაბამისი ინფორმაცია ციფრულ სივრცესთან დაკავშირებული თანმდევი რისკებისა და უსაფრთხოების საშუალებების არსებობის შესახებ;

·საჩივრებისა და სამართლებრივი დაცვის ეფექტიანი საშუალებების ხელშეწყობა — გასაჩივრების ეფექტიანი არხების შემუშავება, ბავშვების უსაფრთხოებასთან უზრუნველსაყოფად მომსახურების მიმწოდებლების ანგარიშვალდებულების ნაწილია;

·გადაწყვეტილების მიღების პროცესში ბავშვების მოსაზრებების გათვალისწინება, ციფრული გარემოს ბავშვის საუკეთესო ინტერესებზე მორგების მიზნით;

·ბავშვების კეთილდღეობისა და უსაფრთხოების კულტურის ხელშეწყობა.

ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა დამუშავების შეწყვეტის უფლების შესახებ

ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ განიხილა განცხადება, რომელშიც მონაცემთა სუბიექტი აღნიშნავდა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა მასთან კომუნიკაციისას დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 21-ე მუხლის პირველი პუნქტით გათვალისწინებული მოთხოვნები მონაცემთა დამუშავების შეწყვეტის მოთხოვნის უფლების შესახებ.[1]

ფაქტობრივი გარემოებების თანახმად, დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტს მომსახურებას ხელშეკრულების საფუძველზე უწევდა და მოსალოდნელ გადახდებთან დაკავშირებით ყოველთვიურად უგზავნიდა ელექტრონულ ფოსტაზე ავტომატურ შეტყობინებებს. იქიდან გამომდინარე, რომ მონაცემთა სუბიექტი დროულად იხდიდა გადასახადებს და არ ჰქონია სურვილი მიეღო ავტომატური შეტყობინებები, მან მიმართა დამუშავებისთვის პასუხისმგებელ პირს დამუშავების შეწყვეტის მოთხოვნით, თუმცა მას უარი ეთქვა მოთხოვნის დაკმაყოფილებაზე.

დამუშავებისთვის პასუხისმგებელმა პირმა აღნიშნა, რომ მონაცემთა სუბიექტთან დადებული ხელშეკრულების საფუძველზე, მონაცემთა დამუშავების თავდაპირველი მიზნიდან გამომდინარე, ვალდებული იყო დაეცვა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის პირველი პუნქტის “ბ” და “ვ” ქვეპუნქტები. წინააღმდეგ შემთხვევაში ის დაარღვევდა ძირითადი რეგულაციის მოთხოვნებს. აღსანიშნავია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დაადასტურა მონაცემთა სუბიექტის მიერ თვიური გადასახადის დროულად დაფარვის ფაქტი, ხოლო ავტომატური შეტყობინებების გაგზავნის საჭიროება, მხოლოდ და მხოლოდ ძირითადი რეგულაციის მოთხოვნათა დაცვით განმარტა.

ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ საქმის ფაქტობრივი გარემოებები შეაფასა და დაადგინა, რომ მონაცემთა სუბიექტისთვის უწყვეტად ელექტრონულ ფოსტაზე მოსალოდნელ გადახდებთან დაკავშირებული ავტომატური შეტყობინებების გაგზავნა არ შეესაბამებოდა მასთან დადებული ხელშეკრულებით განსაზღვრულ თავდაპირველ მიზანს. პერსონალური მონაცემების დამუშავების შესახებ მონაცემთა სუბიექტის მიერ გამოთქმული უარის საპირწონედ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის პირველი პუნქტის “ბ” და “ვ” ქვეპუნქტების მითითება არ იყო საკმარისი საფუძველი იმისთვის, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს კვლავ გაეგრძელებინა ელექტრონულ ფოსტაზე ავტომატური შეტყობინებების გაგზავნა. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ ხსენებულ მუხლში მითითებულია, რომ მონაცემთა დამუშავება კანონიერია მხოლოდ იმ შემთხვევაში და იმ მოცულობით, თუკი ერთი მხრივ, მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის მიერ დადებული ხელშეკრულების შესასრულებლად ან სუბიექტის თხოვნით ხელშეკრულების გაფორმებამდე გარკვეული ზომების მისაღებად, ხოლო მეორე მხრივ — მონაცემთა დამუშავება აუცილებელია მონაცემთა დამუშავებისთვის პასუხისმგებელი ან მესამე პირის კანონიერი ინტერესების დასაცავად, გარდა იმ შემთხვევისა, როდესაც აღნიშნულ ინტერესებს აღემატება იმ მონაცემთა სუბიექტის ინტერესები ან ფუნდამენტური უფლებები და თავისუფლებები, რომლებიც მოითხოვს მონაცემთა დაცვას, განსაკუთრებით თუ მონაცემთა სუბიექტი ბავშვია.[2]

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ერთმანეთს შეუპირისპიროს ზოგადი და სპეციალური შემთხვევები, როდესაც საკითხი მონაცემთა სუბიექტის უფლების დაცვას შეეხება. მონაცემთა დაცვის საზედამხედველო ორგანოს განმარტებით, მონაცემთა დამუშავების შეწყვეტის უფლება უპირატესად უნდა შეფასდეს ზოგად მოთხოვნებთან მიმართებით. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 21-ე მუხლის პირველი პუნქტის თანახმად, მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, ინდივიდუალური გარემოებების გათვალისწინებით, მოითხოვოს რეგულაციის მე-6 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტის შესაბამისად მონაცემთა დამუშავების, აგრეთვე, პროფაილინგის შეწყვეტა. შესაბამისად, დამუშავებისთვის პასუხისმგებელმა პირმა აღარ უნდა დაამუშაოს მონაცემები, გარდა იმ შემთხვევისა, როდესაც მას გააჩნია მონაცემთა დამუშავების კანონიერი საფუძველი, რომელიც აღემატება მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებს ან ამგვარი დამუშავება აუცილებელია სამართლებრივი მოთხოვნის დადგენის, განხორციელების ან დაცვის მიზნით.[3] მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელი პირი სწორედ პროფაილინგის საშუალებით ამუშავებდა მომხმარებლის პერსონალურ მონაცემებს და თავდაპირველ მიზანთან შეუსაბამო, შემდგომი დამუშავებით დაირღვა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 21-ე მუხლის პირველი პუნქტი. შესაბამისად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს დაევალა, მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ გაცემული ინსტრუქციების საფუძველზე მონაცემთა დამუშავების შეწყვეტის მოთხოვნაზე რეაგირების წესის შემუშავება.

[1] ADA (Lithuania) - 2024-02-23, <https://gdprhub.eu/index.php?title=ADA_(Lithuania)_-_2024-02-23> [24.06.2024].
[2] General Data Protection Regulation (GDPR), <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [24.06.2024].
[3] General Data Protection Regulation (GDPR), <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [24.06.2024].

გერმანიის ფინანსური ზედამხედველობის ფედერალურმა ორგანომ ინციდენტის შეტყობინების წესის შესახებ სახელმძღვანელო შეიმუშავა

2024 წლის 18 ივნისს, გერმანიის ფინანსური ზედამხედველობის ფედერალურმა ორგანომ (“BaFin”) მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შეტყობინების შესახებ[1], „ციფრული ოპერატიული მდგრადობის აქტის“ (“Digital Operational Resilience Act”) შესაბამისად, სახელმძღვანელო გამოაქვეყნა. დოკუმენტში აღნიშნულია, რომ 2025 წლის იანვრიდან საინფორმაციო საკომუნიკაციო ტექნოლოგიების (“ICT”) მონაცემთა უსაფრთხოების მნიშვნელოვანი დარღვევები (ინციდენტები) უნდა ეცნობოს გერმანიის ფინანსური ზედამხედველობის ფედერალურ ორგანოს (“BaFin”). „ციფრული ოპერატიული მდგრადობის აქტი“ (“DORA”) განსაზღვრავს ფინანსურ სექტორში ინციდენტის მართვასთან დაკავშირებულ მოთხოვნებს და მნიშვნელოვანი ინციდენტებისა და კიბერსაფრთხეებისთვის, ამკვიდრებს ჰარმონიზებული ანგარიშგების სისტემას.

სახელმძღვანელო დოკუმენტში კლასიფიცირებულია საინფორმაციო საკომუნიკაციო ტექნოლოგიების ინციდენტთა სახეები და განმარტებულია ინციდენტის დეფინიცია. ამასთან, ინციდენტის შეტყობინების პირველადი ანგარიში უნდა შეიცავდეს შემდეგ ინფორმაციას:

- ინციდენტის აღწერა;
- თუ რაზე იქონია ზეგავლენა მონაცემთა უსაფრთხოების დარღვევამ;
- როგორ შეიძლება აისახოს ინციდენტის ზეგავლენა მომხმარებლებზე, კონტრაჰენტებსა ან/და ფინანსური ბაზრის სხვა მონაწილეებზე;
- განგრძობადი ინციდენტის შემთხვევაში, მისი ხანგრძლივობა;
- განზრახვით არის თუ არა ინციდენტი გამოწვეული;
- ინციდენტი ფინანსური ინსტიტუტის პერსპექტივიდან (ძალიან დაბალი, დაბალი, საშუალო, მაღალი ან ძალიან მაღალი მნიშვნელობის).

გერმანიის ფინანსური ზედამხედველობის ფედერალური ორგანო მოუწოდებს ორგანიზაციებსა და უწყებებს დაუყოვნებლივ დაიწყონ მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შეტყობინებასთან დაკავშირებული პროცედურების მოწესრიგება. გარდა ამისა, უზრუნველყონ, რომ მონაცემთა დაცვაზე პასუხისმგებელი პერსონალი აღჭურვილი იყოს ინციდენტის იდენტიფიცირებისა და აღმოფხვრის სათანადო მექანიზმებით განახლებული სტანდარტების, მოთხოვნების შესაბამისად.

[1] Germany: BaFin publishes guide on incident reporting under DORA,

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება ფორლის მუნიციპალიტეტის მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის (“GDPR”) მოთხოვნების დარღვევის შესახებ

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს 2024 წლის 20 ივნისის გადაწყვეტილებით[1] ფორლის მუნიციპალიტეტი დაჯარიმდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით (“GDPR”) დადგენილი მოთხოვნების დარღვევისთვის.
საქმის ფაქტობრივი გარემოებების თანახმად, ფორლის მუნიციპალიტეტმა შექმნა ელექტრონული აპლიკაცია, რომლის საშუალებით მოქალაქეებს ჰქონდათ შესაძლებლობა, გადაუდებელი სიტუაციის არარსებობის შემთხვევაში, მიემართათ ადგილობრივი პოლიციისთვის. აპლიკაცია ადგილობრივ პოლიციას რთავდა ნებას, დაეთვალიერებინა კონკრეტულ ტერიტორიაზე განთავსებული ვიდეოსამეთვალყურეო კამერების ჩანაწერები და განესაზღვრა პატრულის ჩართვის ან უპილოტო საჰაერო ხომალდის გამოყენების საჭიროება. აღსანიშნავია, აპლიკაცია არ იძლეოდა გეოგრაფიულ ადგილმდებარეობასთან დაკავშირებით ტელეფონის ნომრით მიდევნების საშუალებას.

პერსონალურ მონაცემთა დაცვის თვალსაზრისით აპლიკაციის გამოყენებასთან მიმართებით არსებობდა არაერთი კრიტიკული მოსაზრება მონაცემთა დაცვის ოფიცრისა და ექსპერტების მხრიდან, თუმცა, მიუხედავად ამისა, ონლაინ საინფორმაციო სისტემა საჯაროდ ხელმისაწვდომი გახდა.

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილებით, საქმის ფაქტობრივი გარემოებების შესწავლის შედეგად, მუნიციპალიტეტის მიერ შემდეგი პრინციპების დარღვევა დაადგინა: ანგარიშვალდებულება; ახალი პროდუქტის ან მომსახურების შექმნისას მონაცემთა დაცვის სტანდარტების გათვალისწინება და მონაცემთა დაცვა პირველად პარამეტრად (“Privacy by Design and by Default”). ამდენად, საზედამხედველო ორგანომ მიიჩნია, რომ დამუშავებისთვის პასუხისმგებელი პირის მიერ ტექნიკური და ორგანიზაციული უსაფრთხოების ზომები ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5(2) და 25-ე მუხლების შესაბამისად არ იყო უზრუნველყოფილი.

ასევე, საზედამხედველო ორგანომ აღნიშნა, რომ აპლიკაცია დაინტერესებულ პირებს არ აწვდიდა ინფორმაციას პერსონალური მონაცემების დამუშავების თაობაზე, რაც ეწინააღმდეგება “GDPR”-ის მე-5(1)(a), მე-12(1) და მე-13 მუხლებს. ასევე, მუნიციპალიტეტმა, დაარღვია რეგულაციის 28-ე მუხლის მე-3 პუნქტი, რადგან არასწორად განსაზღვრა თავისი სტატუსი პერსონალურ მონაცემთა დამუშავებასთან მიმართებით. ამასთანავე, მუნიციპალიტეტმა აპლიკაციის გამოყენებამდე არ განახორციელა მონაცემთა დაცვაზე ზეგავლენის შეფასება, რის გამოც მან დაარღვია “GDPR”-ის 35-ე მუხლის პირველი პუნქტი. აგრეთვე, აპლიკაციაზე არაავტორიზებული წვდომის გამო, ადგილი ჰქონდა “GDPR”-ის მე-5 (1)(f) მუხლის დარღვევას. აღნიშნულის გათვალისწინებით, ფორლის მუნიციპალიტეტს დაეკისრა ჯარიმა 15 000 ევროს ოდენობით.

დანიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება დამუშავებისთვის პასუხისმგებელი პირის დასაქმებულის შეცდომის შედეგად გამოწვეული მონაცემთა უსაფრთხოების დარღვევის შესახებ

დანიის მონაცემთა დაცვის საზედამხედველო ორგანომ შეისწავლა საქმე, რომელიც ეხებოდა დამუშავებისთვის პასუხისმგებელი პირის - კოპენჰაგენის მუნიციპალური ადმინისტრაციის თანამშრომლის შეცდომის შედეგად გამოწვეულ მონაცემთა უსაფრთხოების დარღვევის ფაქტს.[1]

აღსანიშნავია, რომ მონაცემთა უსაფრთხოების დარღვევის ფაქტი დამუშავებისთვის პასუხისმგებელმა პირმა ელექტრონული ფაილების გეგმური შემოწმების დროს გამოავლინა, როდესაც აღმოაჩინა, რომ ნაცვლად რამდენიმე თანამშრომლისა, რომლებსაც სამსახურებრივად ევალებოდათ ფაილური სისტემის ტექნიკური და ორგანიზაციული კონტროლი, მასზე წვდომა მუნიციპალიტეტის 37 500 თანამშრომელს ჰქონდა. ფაილები მოიცავდა 3 700 000 მონაცემთა სუბიექტის პერსონალურ ინფორმაციას: სოციალური კეთილდღეობის, ენობრივი საჭიროების, არასრულწლოვანთა სტომატოლოგიური და სამედიცინო მომსახურების შესახებ. მუნიციპალიტეტის შიდა მოკვლევით დადგინდა, რომ დამუშავებისთვის პასუხისმგებელი პირის თანამშრომელმა ელექტრონულ ფაილებზე შეცდომით ყველა თანამშრომელს მიანიჭა წვდომა. შესაბამისად, ორი თვის განმავლობაში, იქამდე, ვიდრე შეცდომას აღმოაჩენდნენ, პერსონალური ინფორმაცია ხელმისაწვდომი იყო ყველა თანამშრომლისთვის. დამუშავებისთვის პასუხისმგებელმა პირმა განმარტა, რომ დარღვევის აღმოჩენიდან მალევე შეისწავლა ელექტრონულ ფაილებზე აღნიშნული ორი თვის განმავლობაში განხორციელებული აქტივობის ისტორია და მიუთითა, რომ წვდომაზე არაუფლებამოსილი პირები, მართალია, არ გაეცნენ ინფორმაციას, თუმცა პოტენციური რისკი მაინც არსებობდა.

დამუშავებისთვის პასუხისმგებელმა პირმა აღნიშნა, ელექტრონულ ფაილებზე განთავსებული ინფორმაციის წასაკითხად საჭირო იყო სპეციალური პროგრამა, რომელიც თანამშრომლების უმეტესობას არ ჰქონდა. ასევე, მიუთითა, რომ გააძლიერებდნენ ინციდენტზე რეაგირების წესებს.

დანიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილებით, განსახილველ საქმეში პერსონალურ მონაცემებზე არაავტორიზებული წვდომა და მონაცემთა უსაფრთხოების დარღვევის საკითხი ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-4 მუხლის მე-12 პუნქტის ფარგლებში უნდა განხილულიყო. საზედამხედველო ორგანოს განმარტებით, ძირითადი რეგულაციის 32-ე მუხლის პირველი პუნქტი ადგენს, რომ უახლესი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ხასიათის, მოცულობის, კონტექსტისა და მიზნების, ასევე, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისათვის სავარაუდო რისკების გათვალისწინებით, მონაცემთა დამუშავებისთვის პასუხისმგებელმა და დამუშავებაზე უფლებამოსილმა პირებმა უნდა მიიღონ სავარაუდო რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები უსაფრთხოების უზრუნველსაყოფად.

[1] Datatilsynet (Denmark) - 2024-442-4149, <https://gdprhub.eu/index.php?title=Datatilsynet_(Denmark)_-_2024-442-4149> [01.07.2024]

მიუხედავად იმისა, რომ დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა უსაფრთხოების დარღვევის ფაქტზე რეაგირების საკმაოდ ეფექტიანი წესები ჰქონდა შემუშავებული, მაინც ვერ იქნა უზრუნველყოფილი თანამშრომლის შეცდომის შედეგად 3 700 000 ფიზიკური პირის პერსონალურ მონაცემთა ხელმისაწვდომობა არაავტორიზებული პირებისთვის. ასევე, დამუშავებისთვის პასუხისმგებელი პირის მიერ გეგმური შემოწმების ვადები იმდენად ფართო იყო, რომ ინციდენტის დროულად აღმოჩენას ხელს უშლიდა.

საზედამხედველო ორგანოს განმარტებით, ინციდენტზე რეაგირების წესების არსებობა არ ნიშნავს, რომ დამუშავებისთვის პასუხისმგებელმა პირმა შეასრულა ძირითადი რეგულაციის 32-ე მუხლით განსაზღვრული მოთხოვნები. მნიშვნელოვანია, რომ ავტორიზებული პირებისთვის ელექტრონულ ფაილებზე წვდომის ინსტრუქცია წინასწარ განისაზღვროს და თანამშრომლის მოქმედება დააზღვიოს სხვა თანამშრომელმა ან სისტემური უზრუნველყოფის მეშვეობით, უშუალოდ სისტემამ, რომელიც დააგენერირებს განხორციელებული აქტივობების შედეგებს. ამისთვის კი დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შექმნას პერსონალურ მონაცემთა ფაილური სისტემის ერთმანეთთან დაკავშირებული მექანიზმები, რომელიც თითოეულ ეტაპზე დარღვევათა ალბათობას შეამცირებს ან დააზღვევს რისკებს.

დანიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილებით, დამუშავებისთვის პასუხისმგებელ პირს გამოეცხადა საყვედური ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 32-ე მუხლის პირველი პუნქტის დარღვევისთვის.

საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს რეკომენდაცია (“CNIL”) ჯანმრთელობასთან დაკავშირებული მონაცემების ეროვნული სისტემის (“National Health Data System”) შესახებ

2024 წლის 24 ივნისს, საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNIL”) ჯანმრთელობასთან დაკავშირებული მონაცემების ეროვნული სისტემის (“SNDS”) შესახებ რეკომენდაციები[1] გამოსცა. აღნიშნული დოკუმენტი 2020 წელს გამოქვეყნებულ სახელმძღვანელოს დაეყრდნო, რომელიც მონაცემების ეროვნულ სისტემასა (“SNDS”) და საჯარო თუ კერძო სამედიცინო დაწესებულებებში რეგისტრაციის საკითხს შეეხება.

ჯანმრთელობასთან დაკავშირებული მონაცემების ეროვნული სისტემა (“SNDS”) წარმოადგენს ე. წ. „მონაცემთა ბაზას“, სადაც ფიზიკური პირების ჯანმრთელობასთან დაკავშირებული ინფორმაციაა განთავსებული. სისტემის მიზანია დაეხმაროს მკვლევრებსა და სამედიცინო სფეროში ჩართულ პირებს ჯანმრთელობის ტენდენციების შესწავლასა და საზოგადოებრივი ჯანდაცვის გაუმჯობესებაში.

რეკომენდაციებში ხაზგასმულია, რომ წერილებზე, დოკუმენტებზე, ნიმუშებსა და სამედიცინო ანგარიშებზე აღნიშნული ნომერი (“NIR”)[2] წარმოადგენს საჯარო იდენტიფიკატორს. თითოეული კომუნიკაცია უნდა იყოს უსაფრთხო, თანამედროვე ტექნოლოგიების შესაბამისი ავთენტიფიკაციის ზომებისა და დაშიფვრის მეთოდების გამოყენებით.

საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ აღნიშნა, რომ სარეგისტრაციო ნომერი (“NIR”) მხოლოდ ერთ ადგილას (“single source location”) ან პასუხისმგებელ მესამე პირთან უნდა ინახებოდეს დაშიფრული სახით, ხოლო ინფორმაციის გადაცემისას ჯანმრთელობის მონაცემებისგან განცალკევდეს. გარდა ამისა, მნიშვნელოვანია, რომ მესამე პირებს ცენტრების მიერ შენახულ მონაცემებზე, მათ შორის, ჯანმრთელობასთან დაკავშირებულ სხვა პერსონალურ ინფორმაციაზე, წვდომა არ გააჩნდეთ.

გამოქვეყნებული რეკომენდაცია ხაზს უსვამს განსაკუთრებული კატეგორიის მონაცემთა კანონიერად დამუშავების, სარეგისტრაციო ნომრების უსაფრთხოდ განთავსებისა და დაშიფვრის მნიშვნელობას. სახელმძღვანელოში განხილული ღონისძიებები ხელს შეუწყობს მონაცემთა უსაფრთხოების გაძლიერებასა და პირთა პირადი ცხოვრების ხელშეუხებლობის დაცვას.

ლუქსემბურგის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება დასაქმებულის სამუშაო სივრცის მიმდებარე ტერიტორიის ვიდეომონიტორინგთან დაკავშირებით

2024 წლის 13 ივნისს, ლუქსემბურგის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNPD”) გამოაქვეყნა გადაწყვეტილება დასაქმებული პირის ვიდეომონიტორინგის ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციასთან“ შესაბამისობაზე.[1]

საქმის ფაქტობრივი გარემოებების გათვალისწინებით, 2013 წელს, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ გაცემული ნებართვის საფუძველზე, მუნიციპალური შენობების გარეთ ვიდეოსამეთვალყურეო სისტემა დაამონტაჟა. 2020 წლის მარტში, მონაცემთა სუბიექტმა საჩივრით მიმართა “CNPD”-ს, რომლის საფუძველზეც განაცხადა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა ვიდეოჩანაწერები გამოიყენა როგორც სამსახურებრივი გადაცდომის მტკიცებულება და დასაქმებული პირი გაათავისუფლა დაკავებული პოზიციიდან.

[1] France: CNIL publishes recommendation on National Health Data System registry, <https://www.dataguidance.com/news/france-cnil-publishes-recommendation-national-health> [29.06.2024]

[2]სარეგისტრაციო ნომერი (“NIR”) წარმოადგენს უნიკალურ იდენტიფიკატორს, რომელიც ენიჭება ფიზიკურ პირებს ადმინისტრაციული მიზნებისთვის, ჯანმრთელობისა და სოციალური დაცვის კონტექსტში. იგი გამოიყენება სხვადასხვა დოკუმენტებსა და ჩანაწერებში პირთა იდენტიფიცირებისთვის.

საქმის შესწავლის ფარგლებში “CNPD”-მ დაადასტურა, რომ ვიდეოსამეთვალყურეო სისტემის განთავსების მიზანი დასაქმებულ პირთა უსაფრთხოების უზრუნველყოფა იყო. დამუშავებისთვის პასუხისმგებელი პირი აღნიშნავდა, რომ ლუქსემბურგის „დასაქმების შესახებ კანონის“ (“Employment Law”) თანახმად, გარდა მონაცემთა დაცვის სტანდარტებისა, პირის თანამდებობიდან გათავისუფლების ბრძანება დეტალურად უნდა ასახავდეს დასაქმებული პირის სავარაუდო გადაცდომის შესახებ ინფორმაციას. ამდენად, ვიდეოჩანაწერების საფუძველზე მოპოვებული ინფორმაცია აუცილებელი იყო სასამართლოსთვის დასაქმებული პირის გათავისუფლების მართლზომიერების დასასაბუთებლად.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 (1)(b) მუხლზე დაყრდნობით, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ განმარტა, რომ მონაცემები უნდა შეგროვდეს კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნის მისაღწევად და არ უნდა დამუშავდეს სხვა, ამ მიზანთან შეუთავსებელი მიზნით. ამასთანავე, “CNPD”-მ ყურადღება გაამახვილა „პერსონალური მონაცემების ვიდეომოწყობილობით დამუშავების შესახებ“ „მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB”) სახელმძღვანელო რეკომენდაციაზე,[2] რომლის თანახმად, ვიდეოსამეთვალყურეო სისტემის გამოყენებამდე მონაცემთა დამუშავების მიზანი უნდა დაზუსტდეს და განისაზღვროს რეგულაციის მე-5(1)(b) მუხლის მოთხოვნების გათვალისწინებით. აღნიშნულ რეკომენდაციაზე დაყრდნობით, “CNPD”-მ ასევე აღნიშნა, პერსონალური მონაცემების შემდგომი დამუშავების შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირი, უპირველესად, უნდა დარწმუნდეს, რომ დამუშავება თავსებადია თავდაპირველ მიზანთან, რაც, ასევე, უნდა შეფასდეს რეგულაციის მე-6(4) მუხლით დადგენილი მოთხოვნების ფარგლებში.

“CNDP”-მ ყურადღება გაამახვილა, რომ ვიდეომონიტორინგის განხორციელების მიზანი დასაქმებულთა და ინფრასტრუქტურით მოსარგებლე პირთა უსაფრთხოების უზრუნველყოფა იყო. ფაქტობრივი გარემოებების გათვალისწინებით, საზედამხედველო ორგანომ დაადგინა, რომ პერსონალური მონაცემები მუშავდებოდა თავდაპირველი ამოცანისგან განსხვავებული მიზნით, კერძოდ, მონაცემთა სუბიექტის თანამდებობიდან გათავისუფლების შესახებ მიღებული გადაწყვეტილების დასასაბუთებლად. საზედამხედველო ორგანომ აღნიშნა, რომ “GDPR”-ის მე-5(1)(b) და მე-6(4) მუხლების თანახმად, დამუშავებისთვის პასუხისმგებელ პირს პერსონალური მონაცემების დამუშავების უფლებამოსილება ექნებოდა მონაცემთა სუბიექტის თანხმობის არსებობის ან მონაცემთა შემდგომი დამუშავების თავდაპირველ მიზანთან თავსებადობის შემთხვევაში.

საქმის ფაქტობრივი გარემოების გათვალისწინებით, “CNPD”-მ დამუშავებისთვის პასუხისმგებელ პირს რეგულაციის მე-5(1)(b) მოთხოვნების დარღვევის გამო შენიშვნა გამოუცხადა.

შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება პერსონალურ მონაცემებზე არაავტორიზებული წვდომის შესახებ

შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“IMY”)დამუშავებისთვის პასუხისმგებელი პირის — კომერციული ბანკის (“Avanza Bank”) მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-5 (1)(f) და 32-ე მუხლების დარღვევა დაადგინა.[1]

საქმის ფაქტობრივი გარემოებების თანახმად, კომერციული ბანკი იყენებდა პლატფორმა “Meta”-ს ანალიტიკის ინსტრუმენტს (“Meta Pixel”), რათა განესაზღვრა ბანკის მიერ სოციალურ ქსელ “Facebook”-ზე შეთავაზებული რეკლამების ეფექტიანობა კონკრეტული გვერდების ვიზიტორთა სტუმრობის შესახებ ინფორმაციის მიღებით. მოწყობილობით უნდა შეგროვებულიყო ინფორმაცია მონაცემთა სუბიექტების ვებგვერდებზე ვიზიტის, “IP” მისამართისა და ვებგვერდებზე საძიებო სისტემის ისტორიის შესახებ. დადგინდა, რომ დამუშავებისთვის პასუხისმგებელი პირის მიერ, შემთხვევით, გააქტიურდა ორი ფუნქცია: „წინასწარი ავტომატური დაკავშირება“ (“Automatic Advanced Matching”, “AAM”) და „ავტომატური ღონისძიებები“ (“Automatic Events”, „AE”).

„წინასწარი ავტომატური დაკავშირების“ შემთხვევაში, გროვდებოდა ინფორმაცია მომხმარებლების სახელის, გვარისა და ელექტრონული ფოსტის მისამართის შესახებ. თუ მონაცემთა სუბიექტი შეავსებდა დამუშავებისთვის პასუხისმგებელი პირის ვებგვერდზე ან მობილურ მოწყობილობაში ხუთი სხვადასხვა ფორმიდან რომელიმე ერთს, მისი მონაცემები გადაეცემოდა “Meta”-ს არასისტემატიზებული ფორმით. თუკი მომხმარებელი ავტორიზაციას კონკრეტულ აპლიკაციაში გაივლიდა და დაეთანხმებოდა მარკეტინგული მიზნით არსებულ „მზა ჩანაწერებს“ (“cookies”), „წინასწარი ავტომატური დაკავშირების“ (“AAM”) გზით გროვდებოდა პერსონალური ინფორმაცია. კერძოდ, საიდენტიფიკაციო ნომერი, საკონტაქტო ინფორმაცია, სესხის რაოდენობა, დასაქმებულების შესახებ ინფორმაცია, დასაქმების სახე და ანგარიშის ნომერი. აღნიშნული ინფორმაციის საშუალებით “Meta Pixel”-ი არასისტემატიზებული ფორმით მიღებულ მონაცემებს აკავშირებდა ვებგვერდზე მონაცემთა სუბიექტების ქცევასთან.

„ავტომატური ღონისძიებების“ (“AE”) მეშვეობით იდენტიფიცირებადი იყო, თუ რომელი ღილაკი გააქტიურა მონაცემთა სუბიექტმა დამუშავებისთვის პასუხისმგებელი პირის ვებგვერდსა და მობილურ აპლიკაციაში. აღნიშნული ინფორმაცია გადაეცემოდა “Meta”-ს, სოციალურ ქსელ “Facebook”-ზე მარკეტინგული შეთავაზების მიზნით. „ავტომატური ღონისძიებების“ (“AE”) მეშვეობით, გროვდებოდა პერსონალური ინფორმაცია: სესხის რაოდენობა, ანგარიშის ნომერი, ელექტრონული ფოსტის მისამართი და სოციალური ბარათის ნომერი.

[1] GDPR Hub, Decision of Sweden DPA (IMY), <https://gdprhub.eu/index.php?title=IMY_(Sweden)_-_DI-2021-5544_Avanza_Bank>, [10.07.2024].

დამუშავებისთვის პასუხისმგებელმა პირმა დაადგინა, რომ 2019 წლის 15 ნოემბრიდან 2021 წლის 2 ივნისამდე პერიოდში, ზემოაღნიშნული ორი ფუნქციის შემთხვევით გააქტიურების შედეგად, დაახლოებით, მილიონამდე ფიზიკური პირის პერსონალური მონაცემები შეცდომით გადაეცა “Meta”-ს (“Facebook”).

2021 წლის 8 ივნისს, შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირისგან მონაცემთა უსაფრთხოების დარღვევის თაობაზე შეტყობინება მიიღო. დამუშავებისთვის პასუხისმგებელი პირი აცხადებდა, რომ მონაცემების გადაცემით მონაცემთა სუბიექტებს რაიმე სახის ზიანი არ მიადგათ, რამდენადაც “Meta”-მ გადაცემული მონაცემები პირადი მიზნით არ დაამუშავა. ამასთანავე, დამუშავებისთვის პასუხისმგებელი პირის მოთხოვნის საფუძველზე, მონაცემები წაიშალა.

საზედამხედველო ორგანოს გადაწყვეტილების თანახმად, ანალიტიკური ინსტრუმენტის ორი ფუნქციის შემთხვევითმა გააქტიურებამ გამოიწვია “Meta”-სთან პერსონალური მონაცემების არაავტორიზებული გადაცემა. საზედამხედველო ორგანოს განმარტებით, გადაცემული მონაცემები შეიცავდა მონაცემთა სუბიექტების დიდი რაოდენობის სენსიტიურ ინფორმაციას. მონაცემთა უმეტესობა გადაცემული იყო გასაგები ტექსტით, რაც წარმოშობდა მაღალ რისკებს მათი უფლებების დაცვის თვალსაზრისით. ყურადღება გამახვილდა ფაქტზე, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დროულად ვერ მიიღო ინფორმაცია ზემოაღნიშნული ფუნქციების გააქტიურების თაობაზე. მიუხედავად იმისა, რომ დამუშავებისთვის პასუხისმგებელ პირს პერსონალური მონაცემების დამუშავების შესახებ პროცედურა შემუშავებული ჰქონდა, პრაქტიკაში აღნიშნული სტანდარტი არ იქნა გათვალისწინებული. ასევე, საზედამხედველო ორგანომ ყურადღება გაამახვილა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა პერსონალური მონაცემების არაავტორიზებული გადაცემის შესახებ ინფორმაცია გარე წყაროებიდან მიიღო.

შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელ პირს, “GDPR”-ის მე-5 (1) (f) და 32-ე მუხლების თანახმად, ჰქონდა ვალდებულება, რომ შესაბამისი ტექნიკური და ორგანიზაციული ზომების მეშვეობით, უზრუნველეყო პერსონალური მონაცემები დაცვა არაავტორიზებული წვდომისა და დამუშავებისგან. ასევე, დამუშავებისთვის პასუხისმგებელ პირს უნდა ჰქონოდა უსაფრთხოების შესაბამისი პროგრამა, რომლის მეშვეობითაც, რეგულარული შემოწმების საფუძველზე, გამოვლინდებოდა პერსონალური მონაცემების არაავტორიზებული გადაცემის ფაქტები. ამდენად, საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია “GDPR”-ის მე-5 (1)(f) და 32-ე მუხლები. ყოველივე აღნიშნულის გათვალისწინებით, დამუშავებისთვის პასუხისმგებელ პირს დაეკისრა ჯარიმა 1 318 955. 55 ევროს ოდენობით.

ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (“VDAI”) რეკომენდაცია დასაქმებულთა ნასამართლობის შესახებ მონაცემების დამუშავების თაობაზე

2024 წლის 8 ივნისს, ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“VDAI”) დასაქმებულების ნასამართლობის შესახებ მონაცემების დამუშავების თაობაზე რეკომენდაცია შეიმუშავა.[1] დოკუმენტში განხილულია შემთხვევები, როდესაც დამსაქმებლებს დასაქმებულთა ნასამართლობის შესახებ ჩანაწერების დამუშავება შეუძლიათ.

დამსაქმებელი უფლებამოსილია დაამუშაოს დასაქმებულთა ნასამართლობის შესახებ ჩანაწერები, როდესაც მას აქვს ამის კანონიერი ვალდებულება ან/და როდესაც ისინი დამსაქმებლის ლეგიტიმური ინტერესებისთვის მუშავდება. საგულისხმოა, რომ აღნიშნულის შესახებ წინასწარ უნდა ეცნობოს მონაცემთა სუბიექტს.

რეკომენდაციაში ხაზგასმულია, რომ „კომერციული ბანკების შესახებ“ ლიეტუვის კანონის (“Banking Law of Lithuania”) 34-ე მუხლის თანახმად, თანამშრომელთა ნასამართლობის შესახებ ცნობების შეგროვება დასაშვებია იმ შემთხვევაში, როდესაც თანამშრომელთა ფუნქციები უკავშირდება ფულის გათეთრების საწინააღმდეგო (“AML”) ვალდებულებების შესრულებას, თუმცა დამსაქმებლებს აკისრიათ მტკიცების ტვირთი დამუშავების კანონიერების დასაბუთების თაობაზე. იმ შემთხვევაში, როდესაც ლეგიტიმური ინტერესის საფუძველზე მუშავდება დასაქმებულის ნასამართლობის შესახებ მონაცემები, დამსაქმებელი ვალდებულია, შეაფასოს ინტერესთა ბალანსი, აგრეთვე, კონსულტაციისთვის მიმართოს პერსონალურ მონაცემთა დაცვის ოფიცერს (“DPO”).

დამსაქმებელმა უნდა განსაზღვროს თანამდებობათა სია, რომელზეც დანიშნული პირები არ უნდა იყვნენ ნასამართლევი და მხოლოდ საჭიროებისამებრ დაამუშაოს მონაცემები. ამასთან, მნიშვნელოვანია, რომ დამსაქმებელმა უშუალოდ მონაცემთა სუბიექტისგან მიიღოს ნასამართლობის შესახებ ცნობები.

ლეგიტიმური ინტერესის შეფასებისას, დამსაქმებლებმა უნდა გაითვალისწინონ:

- თანამდებობის სპეციფიკური მოვალეობების თავისებურებები;
- დაკავებულ პოზიციასთან დაკავშირებული რისკები;
- ნასამართლობის არქონის მოთხოვნის დასაბუთება;
- დასაქმებულის უფლებებისა და თავისუფლებების შეფასება;
- სხვა მნიშვნელოვანი გარემოებები.

ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს რეკომენდაცია იძლევა მკაფიო მითითებებს დამსაქმებლებისთვის, რათა კანონიერად დამუშავდეს დასაქმებულთა ნასამართლობის შესახებ მონაცემი. რეკომენდაცია მიზნად ისახავს უზრუნველყოს ცნობების სათანადოდ და გამჭვირვალედ გამოყენება, რაც, ხელს შეუწყობს ორგანიზაციების სამართლებრივ შესაბამისობას პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან და ასევე, კონფიდენციალობის უფლების დაცვას შრომით ურთიერთობებში.

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა სუბიექტების საკონტაქტო მონაცემების გასაჯაროების შესახებ

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა სუბიექტების საკონტაქტო მონაცემების (ტელეფონის ნომრების) გასაჯაროების შესახებ გადაწყვეტილება მიიღო.[1]

საქმის ფაქტობრივი გარემოებების შესწავლის შედეგად დადგინდა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა (სატრანსპორტო კომპანიის ოპერატორი) მასთან დასაქმებული პირების (ავტოსატრანსპორტო საშუალების მძღოლების) ტელეფონის ნომრები კომპანიაში დასაქმებულ პირთა შორის სწრაფი კომუნიკაციისა და სამსახურებრივი მოვალეობების შესრულების მიზნით გაასაჯაროვა. ტელეფონის ნომრები განთავსდა კომპანიის შიდა ელექტრონულ სისტემაში და მასზე წვდომა მხოლოდ იმ მონაცემთა სუბიექტებს ჰქონდათ, რომელთა პერსონალური მონაცემებიც იქნა განთავსებული. ასევე, დამუშავებისთვის პასუხისმგებელი პირი მიუთითებდა, რომ ტელეფონის ნომრების გასაჯაროების უფლება დასაქმებულებთან დადებული ხელშეკრულებით იყო გათვალისწინებული.

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ განმარტა, რომ ეროვნული კანონმდებლობის თანახმად, სამუშაო ადგილას დასაქმებულთა პერსონალური მონაცემების დამუშავება დასაშვებია, თუ აღნიშნულს ითვალისწინებს სამსახურებრივი ფუნქციების შესრულება. თუმცა დამუშავებისთვის პასუხისმგებელი პირი, ამავდროულად, ვალდებულია, რომ დამუშავების პროცესები შეუსაბამოს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებს, განსახილველ შემთხვევაში კი მე-6 მუხლის პირველ პუნქტს (მონაცემთა დამუშავების კანონიერება).

საზედამხედველო ორგანომ მიიჩნია, რომ მონაცემთა სუბიექტების ტელეფონის ნომრების გაზიარება არ იყო აუცილებელი თითოეულის მიერ ნაკისრი სამსახურებრივი ვალდებულების შესრულების თვალსაზრისით, რადგან დამუშავებისთვის პასუხისმგებელ პირს შეეძლო, შედარებით ნაკლებად შემზღუდავი საშუალებით დაემუშავებინა იმ პირთა მონაცემები, რომლებიც საერთო სამუშაო განრიგით ასრულებდნენ სამსახურებრივ ფუნქციებს. აღნიშნული მოთხოვნა მიემართებოდა მხოლოდ სამსახურებრივ ნომრებს და არა პირად სატელეფონო ნომრებს, რაც დამუშავებისთვის პასუხისმგებელ პირს არ ჰქონდა გათვალისწინებული.

ამდენად, საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის პირველი პუნქტისა და „სამუშაო ადგილას პირადი ცხოვრების ხელშეუხებლობის დაცვის შესახებ“ ეროვნული აქტის მე-3 მუხლი. შედეგად, დამუშავებისთვის პასუხისმგებელ პირს გამოეცხადა შენიშვნა და დაევალა შიდა ელექტრონულ სისტემაში საჯაროდ განთავსებული ტელეფონის ნომრების წაშლა.

ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მასობრივი ინფორმაციის საშუალებებით საზოგადოების ინფორმირებისთვის მონაცემთა დამუშავების შესახებ

ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ განიხილა ფიზიკური პირის საჩივარი, რომელიც შეეხებოდა დამუშავებისთვის პასუხისმგებელი პირის — მედია ორგანიზაციის მიერ ფიზიკური პირის ჯანმრთელობასთან დაკავშირებული მონაცემების მასობრივი ინფორმაციის საშუალებებით გამოქვეყნებას.[1] დამუშავებისთვის პასუხისმგებელი პირი მიუთითებდა, რომ იგი მოქმედებდა გამოხატვის თავისუფლებისა და საზოგადოების ინფორმირების მიზნით, რაც შეესაბამებოდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ გათვალისწინებულ საგამონაკლისო წესს.

საქმის ფაქტობრივი გარემოებების შესწავლის შემდეგ დადგინდა, რომ დამუშავებისთვის პასუხისმგებელი პირი ჯანმრთელობასთან დაკავშირებულ მონაცემებს საჯარო ინტერესის ფარგლებში, მასობრივი ინფორმაციის საშუალებებით აქვეყნებდა და მას ჰქონდა საზოგადოების ინფორმირების მკაფიო მიზანი. საზედამხედველო ორგანომ განმარტა, რომ ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავების შეზღუდვის მოთხოვნა არ წარმოადგენს ერთადერთ საკმარის საშუალებას საჯარო ინტერესების დასაძლევად.

[1] Decision of DPA (Ireland), <gdprhub.eu> [12.07.2024].

საზედამხედველო ორგანომ იხელმძღვანელა ძირითადი რეგულაციის 85-ე მუხლს, რომელიც განსაზღვრავს მონაცემთა დამუშავებას გამოხატვისა და ინფორმაციის თავისუფლების ფარგლებში. კერძოდ, წევრი სახელმწიფოები უფლებამოსილნი არიან, დაადგინონ პერსონალური მონაცემების დაცვის უფლების შესაბამისობა გამოხატვისა და ინფორმაციის თავისუფლებასთან. ამასთანავე, აღინიშნა, რომ ირლანდიის ეროვნული კანონმდებლობა მასობრივი ინფორმაციის საშუალებებით საზოგადოების ინფორმირების მიზნით მონაცემთა დამუშავებას საგამონაკლისო წესით აწესრიგებს.

აღსანიშნავია, რომ საგამონაკლისო წესი ვრცელდება ძირითადი რეგულაციის მე-2 თავთან (პრინციპები), მე-3 (მონაცემთა სუბიექტის უფლებები), მე-4 (მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი და უფლებამოსილი პირი), მე-5 (მონაცემების მესამე სახელმწიფოსთვის და საერთაშორისო ორგანიზაციისთვის გადაცემა), მე-6 (დამოუკიდებელი საზედამხედველო ორგანო), მე-7 (თანამშრომლობა და თანამიმდევრულობა) და მე-9 თავებთან (მონაცემთა დამუშავების სპეციფიური სიტუაციები) მიმართებით, თუ ეს აუცილებელია პერსონალური მონაცემების დაცვის უფლების გამოხატვის თავისუფლებასთან შესაბამისობის უზრუნველყოფის მიზნით.

ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ შეწყვიტა საჩივრის განხილვა, რადგან დაადგინა, რომ დამუშავებისთვის პასუხისმგებელი პირი კანონიერად მოქმედებდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 85-ე მუხლის ფარგლებში.

ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება დამუშავებისთვის პასუხისმგებელი პირის მიერ სამართლიანობისა და გამჭვირვალობის პრინციპების დარღვევის შესახებ

2024 წლის 2 ივლისს, ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“VDAI”) გამოაქვეყნა გადაწყვეტილება[1] დამუშავებისთვის პასუხისმგებელი პირის მიერ სამართლიანობისა და გამჭვირვალობის პრინციპების დარღვევის შესახებ.
საქმის ფაქტობრივი გარემოებების თანახმად, 2021 და 2022 წლებში მონაცემთა სუბიექტებმა დამუშავებისთვის პასუხისმგებელი პირის — ონლაინ მაღაზიის წინააღმდეგ საჩივრით მიმართეს საფრანგეთისა და პოლონეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებს. იქიდან გამომდინარე, რომ დამუშავებისთვის პასუხისმგებელი პირის მთავარი ადგილსამყოფელი ლიეტუვა იყო, საჩივრები განსახილველად ლიეტუვის მონაცემთა დაცვის საზედამხედველო ორგანოს გადაეგზავნა.

მონაცემთა სუბიექტები აცხადებდნენ, რომ დამუშავებისთვის პასუხისმგებელმა პირმა არ გაითვალისწინა მათი მოთხოვნა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-17 და მე-15 მუხლებით დაცული უფლებების, კერძოდ, მონაცემთა წაშლისა და მონაცემებზე წვდომის უფლებების უზრუნველყოფის მიზნით. დამუშავებისთვის პასუხისმგებელი პირის მიერ წარმოდგენილი არგუმენტების თანახმად, მონაცემთა წაშლის შესახებ მონაცემთა სუბიექტების მოთხოვნა არ იქნა დაკმაყოფილებული, რადგან მათ არ მიუთითეს მოთხოვნის „კონკრეტული საფუძველი“, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-17 მუხლის პირველი პუნქტის შესაბამისად.

ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ, უპირველეს ყოვლისა, აღნიშნა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა არ შეასრულა მონაცემთა წაშლასთან დაკავშირებული მოთხოვნა. საზედამხედველო ორგანომ არ გაიზიარა დამუშავებისთვის პასუხისმგებელი პირის არგუმენტი და დაადგინა, რომ მხოლოდ წაშლის საფუძვლის მითითების არარსებობის გამო მონაცემთა წაშლაზე უარი, არ იყო გამართლებული. იმ შემთხვევაშიც კი, თუ დამუშავებისთვის პასუხისმგებელ პირს ექნებოდა უარის თქმის საფუძველი, აღნიშნული მიზეზის შესახებ ინფორმაცია უნდა მიეწოდებინა მონაცემთა სუბიექტებისთვის. ასევე, მას უნდა განემარტა, რომ მონაცემთა დამუშავება კვლავ გაგრძელდებოდა.

დამატებით, საზედამხედველო ორგანომ აღნიშნა, რომ დამუშავებისთვის პასუხისმგებელი პირი იყენებდა „ფარული დაბლოკვის“ (“Shadow Blocking”) პრაქტიკას. აღნიშნული გულისხმობს პლატფორმაში მომხმარებლის დაბლოკვას მისი ინფორმირების გარეშე. საზედამხედველო ორგანოს შეფასებით, ამგვარი პრაქტიკა არღვევდა სამართლიანობისა და გამჭვირვალობის პრინციპებს. შესაბამისად, საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა არ მიიღო სათანადო ტექნიკური და ორგანიზაციული ზომები ანგარიშვალდებულების პრინციპის უზრუნველსაყოფად. ასევე, მან ვერ დაასაბუთა, რომ მონაცემთა სუბიექტებისათვის უზრუნველყოფილი იყო საკუთარ პერსონალურ მონაცემებზე წვდომის უფლება.

საქმის ფაქტობრივი გარემოების გათვალისწინებით, ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის პირველი („ა“ ქვეპუნქტი) და მე-2 პუნქტების, მე-12 მუხლის პირველი და მე-4 პუნქტების დარღვევა, რისთვისაც დამუშავებისთვის პასუხისმგებელ პირს დაეკისრა ჯარიმა 2 385 276 ევროს ოდენობით.

[1] GDPR Hub, VDAI (Lithuania) - Vinted UAB, <https://gdprhub.eu/index.php?title=VDAI_(Lithuania)_-_Vinted_UAB>, [12.07.2024].

შვედეთის ადმინისტრაციული სასამართლოს გადაწყვეტილება მუსიკალური აპლიკაციის კომპანია “Spotify AB”-სთვის დაკისრებული ჯარიმის ოდენობის შემცირების შესახებ

შვედეთის ადმინისტრაციულმა სასამართლომ, განმცხადებლის მიმართვის საფუძველზე, განიხილა შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება, რომლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს — მუსიკალური აპლიკაციის კომპანია “Spotify AB”-ს დაეკისრა 5 მილიონი ევროს ოდენობით ჯარიმა, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-15 მუხლის დარღვევის გამო.[1] აღსანიშნავია, რომ სასამართლომ საზედამხედველო ორგანოს მიერ დაკისრებული ჯარიმა 3.5 მილიონ ევრომდე შეამცირა. სასამართლომ გაიზიარა საზედამხედველო ორგანოს განმარტებები დამუშავებისთვის პასუხისმგებელი პირის მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-15 მუხლის დარღვევის შესახებ, რომლის თანახმად, მონაცემთა სუბიექტს უფლება აქვს, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისგან მოითხოვოს დადასტურება, მუშავდება თუ არა მისი მონაცემები და მიიღოს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ განსაზღვრული ინფორმაცია. მოცემულ საქმეში, მუსიკალური აპლიკაციის მომხმარებლებს არ ჰქონდათ შესაბამისი ინფორმაცია საკუთარი მონაცემების დამუშავების შესახებ.

სასამართლომ აღნიშნა, რომ საზედამხედველო ორგანოს მიერ განსაზღვრული ჯარიმის ოდენობა დაეყრდნო კომპანიის მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-12 მუხლის პირველი პუნქტის და მე-15 მუხლით განსაზღვრულ მოთხოვნათა შეუსრულებლობას. ძირითადი რეგულაციის მე-12 მუხლი აწესრიგებს ინფორმაციის გამჭვირვალობას და მონაცემთა სუბიექტის უფლებების განხორციელების თავისებურებებს. აღნიშნული გულისხმობს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, მიიღოს სათანადო ღონისძიებები, რათა მონაცემთა სუბიექტს მიაწოდოს ძირითადი რეგულაციის მე-13 და მე-14 მუხლებით გათვალისწინებული ნებისმიერი ინფორმაცია და წარმართოს მასთან 15-22 მუხლებითა და 34-ე მუხლით განსაზღვრული კომუნიკაცია ამომწურავი, გამჭვირვალე, გასაგები და მარტივად ხელმისაწვდომი ფორმით.

შესაბამისად, შვედეთის ადმინისტრაციულმა სასამართლომ გაიზიარა საზედამხედველო ორგანოს გადაწყვეტილება ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ დარღვევის შესახებ, თუმცა საქმეში არსებული გარემოებების შესწავლის შედეგად, შეამცირა დაკისრებული ჯარიმის ოდენობა, რადგან მიიჩნია, რომ დარღვევა არ იყო ისეთი სიმძიმის, როგორც აღნიშნული საზედამხედველო ორგანომ შეაფასა.[2]

[1] Court reduces Spotify GDPR fine, <https://gdprbuzz.com/news/court-reduces-spotify-gdpr-fine-to-4-million-euros/> [22.07.2024].
[2] Sweden: IMY Fines Spotify SEK 58M for Failures regarding Data Subject Requests, <https://www.dataguidance.com/news/sweden-imy-fines-spotify-sek-58m-failures-regarding> [22.07.2024].

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება დამუშავებისთვის პასუხისმგებელი პირის მიერ პერსონალური მონაცემების არაკანონიერი დამუშავების შესახებ

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) ერთ-ერთი საფინანსო კომპანიის მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ (“GDPR”) განსაზღვრული მოთხოვნების დარღვევის შესახებ იმსჯელა და დამუშავებისთვის პასუხისმგებელი პირი 225 000 ევროს ოდენობით დააჯარიმა.[1]

საქმის ფაქტობრივი გარემოებების თანახმად, მონაცემთა სუბიექტმა დამუშავებისთვის პასუხისმგებელ პირს — საფინანსო კომპანიას საკრედიტო საინფორმაციო სისტემიდან მისი პერსონალური მონაცემების წაშლის მოთხოვნით მიმართა, რაზეც კომპანიამ უარი განაცხადა იმაზე მითითებით, რომ განმცხადებელს აღებული ჰქონდა დიდი ოდენობის სესხი. თავის მხრივ, მონაცემთა სუბიექტმა უარყო კომპანიისგან სესხის აღების ფაქტი. მეტიც, მისი განცხადებით, იგი ვინაობის მითვისების (“identity theft”) მსხვერპლი გახდა, რის გამოც საჩივრით მიმართა სამართალდამცავ ორგანოს.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ყურადღება გაამახვილა გარემოებაზე, რომ მომჩივანი არ იმყოფებოდა საფინანსო კომპანიასთან სასესხოსამართლებრივ ურთიერთობაში, თუმცა დამუშავებისთვის პასუხისმგებელი პირი საკრედიტო საინფორმაციო სისტემიდან მის პერსონალურ ინფორმაციას არ შლიდა. შესაბამისად, საზედამხედველო ორგანომ დაადგინა, რომ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს განმცხადებლის პერსონალური მონაცემების დამუშავების კანონიერი საფუძველი არ გააჩნდა. გარდა აღნიშნულისა, საფინანსო კომპანიამ დაარღვია რეგულაციის მე-17 მუხლი (მონაცემთა წაშლის უფლება) და 37-ე მუხლის მე-7 პუნქტი, რომლის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიაწოდოს მონაცემთა დაცვის ოფიცრის საკონტაქტო ინფორმაცია.

საქმის ფაქტობრივი გარემოების გათვალისწინებით, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს დააკისრა ჯარიმა 225 000 ევროს ოდენობით, რომელიც ნებაყოფლობითი წესით გადახდის გამო, 180 000 ევრომდე იქნა შემცირებული. გარდა აღნიშნულისა, ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ საფინანსო კომპანიას დაავალა:

- საკრედიტო საინფორმაციო სისტემიდან მონაცემთა სუბიექტის პერსონალური ინფორმაციის წაშლა;
- მონაცემთა სუბიექტების ვინაობის დამადასტურებელი პროცედურის გაუმჯობესება;
- მონაცემთა სუბიექტის მოთხოვნის საფუძველზე, პერსონალური მონაცემების დამუშავების შეწყვეტა და წაშლა.

[1] Data Guidance, Spain: AEPD fines ID FINANCE €225,000 for unlawful processing of personal data, <https://www.dataguidance.com/news/spain-aepd-fines-id-finance-225000-unlawful-processing>, [22.07.2024].

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