მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება საქმის განხილვის პროცესში დამუშავებისთვის პასუხისმგებელი პირის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსთან თანამშრომლობის ვალდებულების შესახებ

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (“AEPD”) გადაწყვეტილება[1] შეეხება დამუშავებისთვის პასუხისმგებელი პირის მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 58-ე მუხლის პირველი პუნქტის დარღვევას, რაც გამოიხატა საქმის განხილვის პროცესში საზედამხედველო ორგანოსთან თანამშრომლობისთვის თავის არიდებაში.

aepd agencia española protección datos

აგვისტო 2024

საქმის ფაქტობრივი გარემოებების თანახმად, მონაცემთა სუბიექტს სარეკლამო შეთავაზების მიზნით არაერთხელ დაუკავშირდა დამუშავებისთვის პასუხისმგებელი პირი, სატელეფონო კომპანია — “Vodafone España, S.A.U”. მონაცემთა სუბიექტის მტკიცებით, მას არ ჰქონდა გაცხადებული თანხმობა სატელეფონო შეტყობინებების მიღების შესახებ. ხოლო დამუშავებისთვის პასუხისმგებელი პირის განმარტებით, სატელეფონო სარეკლამო შეთავაზების უშუალო განმახორციელებლები იყვნენ მასთან სახელშეკრულებო ურთიერთობაში მყოფი პირები (შემდგომში — “Vodafone”-ის პარტნიორები), რომლებსაც ჰქონდათ ვალდებულება, დაეცვათ ხელშეკრულებით გათვალისწინებული მოთხოვნები პერსონალურ მონაცემთა დაცვის თაობაზე.

აღსანიშნავია, რომ საზედამხედველო ორგანომ განსახილველად არ მიიღო საჩივრის ის ნაწილი, რომლის თანახმად, ვერ დგინდებოდა დამუშავებისთვის პასუხისმგებელი პირის მიერ სატელეფონო ზარების განხორციელება. თუმცა, მან დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვა მესამე მხარეების, კერძოდ, “Vodafone”-ის პარტნიორების მიერ განხორციელებული მოქმედებების შესახებ დეტალური ინფორმაციის გაზიარება. მიუხედავად მოთხოვნისა, დამუშავებისთვის პასუხისმგებელმა პირმა საზედამხედველო ორგანოს არ გადასცა მოთხოვნილი ინფორმაცია. აღნიშნულის გათვალისწინებით, ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 58-ე მუხლის პირველი პუნქტის საფუძველზე დამუშავებისთვის პასუხისმგებელი პირის მიმართ საკითხის შესწავლა დაიწყო. სატელეფონო კომპანიის განმარტების თანახმად, მას არ ჰქონდა საქმის გარემოებების შესწავლის პროცესში ხელის შეშლის განზრახვა. ამასთანავე, სატელეფონო შეტყობინებებთან დაკავშირებით მან განაცხადა, რომ აღნიშნული განხორციელდა არა “Vodafone”-ის, არამედ იმ პირების სახელით, რომლებთანაც სახელშეკრულებო ურთიერთობაში რეალურად აღარ იმყოფებოდა. თავის მხრივ ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ სატელეფონო კომპანია — “Vodafone España, S.A.U” დააჯარიმა 200 000 ევროს ოდენობით და აღნიშნა, რომ დამუშავებისთვის პასუხისმგებელი პირმა ინფორმაციის საზედამხედველო ორგანოსთვის მიუწოდებლობით ხელი შეუშალა საკითხის შესწავლას, რის შედეგადაც დაირღვა რეგულაციის 58-ე მუხლის პირველი პუნქტი.

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავებისას მონაცემთა უსაფრთხოების დარღვევის შესახებ

საქმის ფაქტობრივი გარემოებების თანახმად, 2022 წელს, დამუშავებისთვის პასუხისმგებელი პირის — ადამიანის იმუნოდეფიციტის ვირუსების ტესტირებასთან დაკავშირებული ასოციაციის თანამშრომელმა, ასოციაციის მომსახურებით მოსარგებლე, 270 აქტიური სტატუსის მქონე მომხმარებელს ელექტრონული ფოსტის მეშვეობით შეტყობინება გაუგზავნა. აღსანიშნავია, რომ გაგზავნილ კორესპონდენციაში ელექტრონული ფოსტის მისამართების ჩამონათვალი საჯაროდ იყო ხელმისაწვდომი, რაც ქმნიდა ასოციაციის მომხმარებელთა სრული ან ნაწილობრივი იდენტიფიცირების რისკს.

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ საქმის ფაქტობრივი გარემოებების შესწავლის შედეგად დაადგინა, რომ დამუშავებისთვის პასუხისმგებელი პირი ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავების პროცესში არ იყენებდა მონაცემთა უსაფრთხოების დაცვისთვის აუცილებელ ტექნიკურ და ორგანიზაციულ საშუალებებს, რამაც მონაცემთა უსაფრთხოების დარღვევა გამოიწვია.[1]

საზედამხედველო ორგანოს განმარტების თანახმად, აღნიშნული პრობლემა დამუშავებისთვის პასუხისმგებელი პირის თანამშრომელთა დაბალი ცნობიერებით იყო გამოწვეული, რადგან თანამშრომელთა გარკვეული ნაწილი მონაცემთა უსაფრთხოების აღნიშნულ დარღვევას არ მიიჩნევდა პრობლემად და აღნიშნავდნენ, რომ მომხმარებლებისთვის გაგზავნილი ინფორმაცია არ შეიცავდა პერსონალურ მონაცემებს.

საზედამხედველო ორგანოს განმარტების თანახმად, მხოლოდ ის ფაქტი, რომ შეტყობინების ადრესატებს ერთმანეთის იდენტიფიცირება შეეძლოთ, უკვე საკმარის საფუძველს წარმოადგენდა სათანადო რეაგირებისთვის, რაც გამოიხატება მონაცემთა უსაფრთხოების დარღვევის შესახებ საზედამხედველო ორგანოსთვის შეტყობინებასა და სათანადო ღონისძიებების განხორციელებაში. აღსანიშნავია, რომ ასოციაციას არ ჰქონდა შესაბამის ტექნიკურ-ორგანიზაციულ ღონისძიებათა პოლიტიკა, რომელიც დააზღვევდა ამ სფეროში არსებულ შესაძლო რისკებს. ამასთანავე, ასოციაცია არ უზრუნველყოფდა პერსონალურ მონაცემთა დამუშავებისა და დაცვის საკითხზე მონაცემთა დამუშავებისთვის პასუხისმგებელი თანამშრომლების კვალიფიკაციის პერიოდულ ამაღლებას, ხოლო თანამშრომელთა გარკვეულ ნაწილს არ ჰქონდა გავლილი აღნიშნული მიმართულებით შესაბამისი სასწავლო ტრენინგები.

საზედამხედველო ორგანომ, შემთხვევის სერიოზულობიდან გამომდინარე, ჯარიმის ოდენობა თავდაპირველად 349 000 ევროს ოდენობით განსაზღვრა, თუმცა ჯარიმის დაკისრების ახალი სახელმძღვანელო პოლიტიკის გათვალისწინებით, შეამცირა 8 730 ევრომდე. აღნიშნული სახელმძღვანელო პოლიტიკა პერსონალური მონაცემების დამუშავებასთან დაკავშირებული ადმინისტრაციული სამართალდარღვევისთვის ჯარიმის დაკისრებისა და შესაბამისი ოდენობების განსაზღვრის ინსტრუქციას წარმოადგენს. ხოლო ჯარიმის ოდენობის განსაზღვრისთვის მხედველობაში მიიღება:

- დარღვევის სიმძიმე;
- ორგანიზაციის ფინანსური ბრუნვა;
- დარღვევის ჩადენის საწყისი ეტაპის დადგენა და განგრძობადი ხასიათი;
- პასუხისმგებლობის დამამძიმებელი და შემამსუბუქებელი გარემოებები;
- ჯარიმის უკვე განსაზღვრული ოდენობის ცვლილების საგამონაკლისო შემთხვევები.[2]

შესაბამისად, ჯარიმის ოდენობის გამოთვლისას, საზედამხედველო ორგანომ მხედველობაში მიიღო დამუშავებისთვის პასუხისმგებელი პირის ოთხდღიანი დაგვიანება მონაცემთა უსაფრთხოების დარღვევის შეტყობინების შესახებ, აგრეთვე, დარღვევის გამომწვევი მიზეზები და რეაგირების მიზნით განხორციელებული ღონისძიებები. იმის გათვალისწინებით, რომ ელექტრონული ფოსტით გაგზავნილი შეტყობინება აშკარად მიემართებოდა იმ პირებს, რომელთაც ასოციაციისგან უკვე მიღებული ჰქონდათ ან სურდათ ჯანმრთელობასთან დაკავშირებული მომსახურების მიღება, საზედამხედველო ორგანომ დაადგინა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის პირველი პუნქტის „ვ“ ქვეპუნქტის დარღვევა, რომლის თანახმად, პერსონალური მონაცემები უნდა დამუშავდეს იმგვარად, რომ სათანადო ტექნიკური ან ორგანიზაციული ზომების მეშვეობით უზრუნველყოფილი იყოს მათი უსაფრთხოება, მათ შორის, დაცული იყოს უკანონო და არაუფლებამოსილი პირების მიერ დამუშავების, შემთხვევით დაკარგვის, განადგურების ან დაზიანებისაგან.

[1] Decision of ICO (UK), <https://gdprhub.eu/index.php?title=ICO_(UK)_-_The_Central_Young_Men%E2%80%99s_Christian_Association> [24.07.2024].
[2] Information Commissioner's Office ("ICO"), Data Protection Fining Guidance, <https://ico.org.uk/about-the-ico/ourinformation/policies-and-procedures/dataprotection-fining-guidance/> [24.07.2024].

ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა შემდგომი დამუშავების მიზნისა და უსაფრთხოების დარღვევის შესახებ

ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (“APD”) გადაწყვეტილება[1] შეეხება მესამე მხარესთან ელექტრონული ფოსტის შეცდომით გაგზავნას, რომლის ფარგლებშიც საზედამხედველო ორგანომ მონაცემთა შემდგომ დამუშავებასა და მონაცემთა უსაფრთხოების დარღვევასთან დაკავშირებულ საკითხებზე იმსჯელა.

საქმის ფაქტობრივი გარემოებების გათვალისწინებით, დამუშავებისთვის პასუხისმგებელმა პირმა — სანოტარო ბიურომ მონაცემთა სუბიექტის პერსონალური მონაცემები: სახელი, მისამართი, დაბადების თარიღი და მათი მემკვიდრეების ეროვნული სარეგისტრაციო ნომერი, შემთხვევით არასწორ ადრესატთან გაგზავნა. მონაცემთა მიმღებმა აღნიშნული შეცდომის თაობაზე ყველა შესაბამის ადრესატს აცნობა, რის საფუძველზეც მონაცემთა სუბიექტმა ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს საჩივრით მიმართა.

საზედამხედველო ორგანომ, უპირველეს ყოვლისა, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-5 მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტზე დაყრდნობით აღნიშნა, რომ მონაცემები უნდა შეგროვდეს კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნისათვის და არ უნდა დამუშავდეს სხვა, ამ მიზანთან შეუთავსებელი მიზნით. მოცემულ საქმეში საზედამხედველო ორგანოს უნდა შეეფასებინა მესამე მხარესთან ელექტრონული ფოსტის გაგზავნის შესაბამისობა მონაცემთა თავდაპირველი დამუშავების მიზანთან.

მონაცემთა შემდგომი დამუშავება კანონიერია მხოლოდ სამართლებრივი საფუძვლის არსებობის შემთხვევაში. საქმის ფაქტობრივი გარემოებებიდან გამოიკვეთა, მესამე მხარე და ასევე, დამუშავებისთვის პასუხისმგებელი პირი აღნიშნავდნენ, რომ შეცდომით მოხდა პერსონალური მონაცემების გაგზავნა. შესაბამისად, მესამე მხარისათვის მონაცემების გადაცემა არ წარმოადგენდა დამუშავებისთვის პასუხისმგებელი პირის მიზანს.

ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს შეფასების თანახმად, მოცემულ შემთხვევაში პერსონალურ მონაცემთა დამუშავება „შეცდომად“ უნდა შეფასდეს და არა იმგვარ დამუშავებად, როდესაც დამუშავებისთვის პასუხისმგებელი პირი წინასწარ განსაზღვრავს სამართლებრივ საფუძველს. მონაცემთა „მთლიანობისა და კონფიდენციალობის“ დაცვის მიზნით, დამუშავებისთვის პასუხისმგებელ პირი ვალდებულია, მონაცემთა უსაფრთხოების უზრუნველსაყოფად დანერგოს შესაბამისი ორგანიზაციული და ტექნიკური ზომები. წინამდებარე საქმის ფაქტობრივი გარემოებების თანახმად, პერსონალურ მონაცემთა უკანონო გამჟღავნებამ გამოიწვია მონაცემთა კონფიდენციალობის დარღვევა. დამუშავებისთვის პასუხისმგებელმა პირმა ვერ მიიღო სათანადო ზომები მონაცემთა უსაფრთხოების დარღვევის თავიდან ასარიდებლად, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 (1)(f) და 32(1)(b)-ე მუხლების შესაბამისად.

აღსანიშნავია, რომ რეგულაციის 33-ე მუხლის პირველი პუნქტის მიხედვით, დამუშავებისთვის პასუხისმგებელი პირი, პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შემთხვევაში, ვალდებულია დაუყოვნებლივ და თუ შესაძლებელია დარღვევის შესახებ შეტყობიდან არაუგვიანეს 72 საათისა, აცნობოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს, გარდა იმგვარი შემთხვევისა, როდესაც ნაკლებსავარაუდოა, რომ დარღვევა საფრთხეს შეუქმნის ფიზიკურ პირთა უფლებებსა და თავისუფლებებს. ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ აღნიშნა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა მიიღო იმის დამადასტურებელი მტკიცებულება, რომ მესამე მხარემ გაზიარებული დოკუმენტაცია არ გახსნა და დაუყოვნებლივ წაშალა. ამდენად, მიჩნეულ იქნა, რომ მონაცემთა უსაფრთხოების დარღვევა საფრთხეს ვერ შეუქმნიდა მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებს. აღნიშნულის გათვალისწინებით, დამუშავებისთვის პასუხისმგებელ პირს საზედამხედველო ორგანოსთვის მონაცემთა უსაფრთხოების დარღვევის თაობაზე შეტყობინების ვალდებულება არ ჰქონდა.

საქმის ფაქტობრივი გარემოების შეფასების საფუძველზე, ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5(1)(a)(b)(f), მე-6 და 32-ე მუხლების დარღვევა და დამუშავებისთვის პასუხისმგებელი პირის მიმართ სანქციის სახით გაფრთხილება გამოიყენა.

სლოვენიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება კომპანიის დირექტორის პასუხისმგებლობის შესახებ

საქმის ფაქტობრივი გარემოებების თანახმად, მონაცემთა სუბიექტმა მიმართა სლოვენიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს, დამუშავებისთვის პასუხისმგებელი პირის წარმომადგენელი დირექტორის მიერ მონაცემთა სუბიექტის ვინაობის მაიდენტიფიცირებელი ფინანსური და ეკონომიკური მონაცემების უკანონო დამუშავების შესწავლის მიზნით.[1]

საქმის გარემოებათა შესწავლის შემდეგ დადგინდა, რომ დამუშავებისთვის პასუხისმგებელი პირი არ ასრულებდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის პირველი პუნქტის მოთხოვნებს (მონაცემთა დამუშავების კანონიერება), კერძოდ, კომპანიის დირექტორი მონაცემთა სუბიექტის პერსონალურ მონაცემებს თავის თანამშრომლებს მონაცემთა დამუშავების სამართლებრივი საფუძვლის გარეშე უზიარებდა. ხოლო მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ არ იქნა გათვალისწინებული შესაბამისი ტექნიკური და ორგანიზაციული ზომები, რის გამოც დაირღვა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 32-ე მუხლით განსაზღვრული მოთხოვნა.

აღსანიშნავია, რომ სლოვენიის „მონაცემთა დაცვის აქტი“ ერთმანეთისგან მიჯნავს მონაცემთა დამუშავების კონტექსტში დამუშავებისთვის პასუხისმგებელი პირის წარმომადგენელი დირექტორისა და უშუალოდ დამუშავებისთვის პასუხისმგებელი პირის პასუხისმგებლობას. საზედამხედველო ორგანოს მიერ შესწავლილი საქმის ფაქტობრივი გარემოებების თანახმად, დირექტორი მონაცემებს პირადი მიზნით ამუშავებდა და უზიარებდა თანამშრომლებს. თუმცა, მიუხედავად ამისა, იგი მაინც წარმოადგენდა დამუშავებისთვის პასუხისმგებელ პირს, რადგან მოქმედებდა მისი სახელით, მისგან მიღებული ინფორმაციის საფუძველზე და კომპანიის ორგანიზაციული მოწყობის ფარგლებში.

სლოვენიის „მონაცემთა დაცვის აქტის“ თანახმად, პირადი მიზნით მონაცემთა დამუშავების ფაქტის გამოკვეთის შემთხვევაში, პასუხისმგებლობა უშუალოდ კომპანიის დირექტორს, ინდივიდუალურად ეკისრება. თუმცა, მოცემული საქმის შესწავლის შედეგად, საზედამხედველო ორგანომ არა მხოლოდ დირექტორს, არამედ დამუშავებისთვის პასუხისმგებელ პირსაც მისცა შენიშვნა, რადგან დირექტორმა სამსახურებრივი უფლებამოსილების განხორციელებისას დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის პირველი პუნქტითა და 32-ე მუხლით განსაზღვრული მოთხოვნები.

ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება დამუშავებისთვის პასუხისმგებელი პირის მიერ საზედამხედველო ორგანოს მოთხოვნის შეუსრულებლობის შესახებ

ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს გამოუცხადა შენიშვნა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის პირველი პუნქტის „ა“ და „გ“ ქვეპუნქტების, ასევე, მე-12 მუხლის პირველი და მე-4 პუნქტების დარღვევის გამო[1] და დაავალა საკუთარ ვებგვერდზე გამოქვეყნებული მონაცემების ცვლილება ან წაშლა. დავალების შესრულების ვადის გასვლის შემდეგ, საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირის ვებგვერდის შემოწმების პროცესში აღმოაჩინა, რომ მიუხედავად უწყების მიერ განსაზღვრული მოთხოვნისა, ძირითადი რეგულაციის დარღვევით დამუშავებული პერსონალური მონაცემები ვებგვერდის მეშვეობით კვლავ ხელმისაწვდომი იყო. შესაბამისად, საზედამხედველო ორგანომ განაახლა საქმის შესწავლა.

აღნიშნულთან დაკავშირებით დამუშავებისთვის პასუხისმგებელმა პირმა განმარტა, რომ მას არ შეეძლო მონაცემების ცვლილება ან წაშლა, რადგან არ ჰქონდა წვდომა აღნიშნული ვებგვერდის არქივზე. ასევე, მან მიუთითა, რომ ვებგვერდის არქივზე წვდომა მხოლოდ წინა ადმინისტრატორს ჰქონდა.

საზედამხედველო ორგანომ მხედველობაში არ მიიღო დამუშავებისთვის პასუხისმგებელი პირის განმარტება და აღნიშნა, რომ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 24-ე მუხლის პირველი პუნქტის მიხედვით, პერსონალური მონაცემის დამუშავების ხასიათის, მოცულობის, კონტექსტისა და მიზნების, ასევე, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისათვის სავარაუდო რისკების გათვალისწინებით, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაატაროს შესაბამისი ტექნიკური და ორგანიზაციული ზომები, რათა უზრუნველყოს ძირითადი რეგულაციის შესაბამისად მონაცემთა დამუშავება. აღნიშნული ღონისძიებები, საჭიროების შემთხვევაში, უნდა გადაიხედოს და განახლდეს. ამდენად, დამუშავებისთვის პასუხისმგებელი პირის მიერ ვალდებულების შეუსრულებლობა, მოქმედების განხორციელების ფაქტობრივი შეუძლებლობის მიზეზით, არ ათავისუფლებს მას პასუხისმგებლობისგან.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის მე-2 პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს ევალება, რომ უზრუნველყოს პერსონალურ მონაცემთა დამუშავების პრინციპების დაცვა და შეეძლოს განხორციელებული მოქმედებების მონაცემთა დამუშავების პრინციპებთან შესაბამისობის დემონსტრირება. შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირს უნდა შეემუშავებინა ისეთი ორგანიზაციულ-ტექნიკური მექანიზმი, რომლითაც უზრუნველყოფდა საკუთარ ვებგვერდზე გამოქვეყნებული ინფორმაციის შეცვლის ან წაშლის შესაძლებლობას.

ზემოაღნიშნულიდან გამომდინარე, ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნები დაარღვია არა უბრალოდ დაუდევრობით, არამედ პერსონალურ მონაცემთა უკანონო დამუშავების პროცესების კვლავ გაგრძელებით. შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირს დაეკისრა ჯარიმა 1 000 ევროს ოდენობით.

[1] Decision of DPA (Latvia), <gdprhub.eu> [29.07.2024].

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება დამუშავებისთვის პასუხისმგებელი პირის აპლიკაციაში განთავსებული მონაცემების უსაფრთხოების შესახებ

დამუშავებისთვის პასუხისმგებელი პირი — ფინეთის გოლფის ასოციაცია, მომხმარებელთა მომსახურების გასაუმჯობესებლად იყენებდა მობილურ აპლიკაციას. აპლიკაციაში რეგისტრაციისას მომხმარებელი მიუთითებდა სხვადასხვა პერსონალურ მონაცემს: სახელს, გვარს, დაბადების თარიღს. რეგისტრაციის შემდეგ, მონაცემთა სუბიექტს ენიჭებოდა საიდენტიფიკაციო ნომერი, რომლის საშუალებითაც შეეძლო აპლიკაციით სარგებლობა.[1]

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ყურადღება გაამახვილა, რომ აპლიკაციაში ავთენტიფიკაციისთვის მომხმარებელს არ სჭირდებოდა პაროლი და მას მხოლოდ საიდენტიფიკაციო ნომრით შეეძლო საკუთარი ანგარიშის გააქტიურება. ხოლო საიდენტიფიკაციო ნომერი შედგებოდა იმ მონაცემებისგან, რომლებიც გენერირდებოდა მონაცემთა სუბიექტის საიდენტიფიკაციო ბარათიდან. საგულისხმოა, რომ აღნიშნული ბარათის მონაცემები ასოციაციის ვებგვერდზე საჯაროდ იყო ხელმისაწვდომი.
საზედამხედველო ორგანომ მიიჩნია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 25-ე მუხლის პირველი პუნქტი და 32-ე მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტი, რადგან აპლიკაციის გამართულად ფუნქციონირებისთვის, მას არ ჰქონდა განხორციელებული სათანადო ორგანიზაციული და ტექნიკური ზომები.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 25-ე მუხლის პირველი პუნქტის მოთხოვნა მიემართება უახლესი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ხასიათის, მასშტაბის, კონტექსტისა და მიზნების, ასევე, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისათვის სავარაუდო რისკების გათვალისწინებით, დამუშავების საშუალებების განსაზღვრისა და დამუშავების პროცესში, სათანადო ტექნიკური და ორგანიზაციული ზომების მიღებას, ხოლო 32-ე მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტის შინაარსი ტექნიკური და ორგანიზაციული ზომების უსაფრთხოების უზრუნველყოფასთან ერთად, დამუშავების სისტემებისა და სერვისების კონფიდენციალობის დაცვას, ხელშეუხებლობას, ხელმისაწვდომობასა და მოქნილობას გულისხმობს.

საზედამხედველო ორგანომ დაადგინა, რომ აპლიკაციაში ავთენტიფიკაციის მიზნით, სათანადო პაროლის არარსებობა ქმნის მონაცემთა სუბიექტების საიდენტიფიკაციო ნომრების მარტივად იდენტიფიცირების შესაძლებლობას, რის შედეგადაც შესაძლებელი იყო მომხმარებელთა ანგარიშებსა და პერსონალურ მონაცემებზე არაუფლებამოსილი წვდომა. შესაბამისად, საზედამხედველო ორგანომ მიიჩნია, რომ დამუშავებისთვის პასუხისმგებელი პირი ვერ უზრუნველყოფდა აპლიკაციაში განთავსებული პერსონალური მონაცემების უსაფრთხოების დაცვას.

საქმის ზემოაღნიშნული ფაქტობრივი გარემოებების შეფასების შედეგად, ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს მისცა შენიშვნა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 25-ე მუხლის პირველი პუნქტის და 32-ე მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტის დარღვევის გამო და დაავალა აპლიკაციის საშუალებით მონაცემთა დამუშავებასთან დაკავშირებული მოქმედებების ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებთან შესაბამისობაში მოყვანა.

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება დამუშავებისთვის პასუხისმგებელი პირის მიერ საჯარო მოსამსახურეთა კონკურსის შედეგების გამოქვეყნების შესახებ

დამუშავებისთვის პასუხისმგებელმა პირმა (იტალიის ერთ-ერთმა მუნიციპალიტეტმა) საჯარო მოსამსახურეთა შერჩევის მიზნით გამოაცხადა კონკურსი, რომლის შედეგები საჯაროდ გამოაქვეყნა საკუთარ ვებგვერდზე. ვებგვერდზე განთავსდა კანდიდატთა სია, რომლებმაც წარმატებით გაიარეს კონკურსი და პირთა სია, ვინც ვერ დააკმაყოფილა საკონკურსო მოთხოვნები.

განმცხადებელმა წარმატებით ვერ გაიარა კონკურსი და მოითხოვა ვებგვერდიდან მისი სახელისა და გვარის წაშლა. დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს განუმარტა, რომ მუნიციპალიტეტის ვებგვერდი იმართებოდა სხვა კომპანიის მიერ და მუნიციპალიტეტი დამოუკიდებლად ვერ შეძლებდა მონაცემების წაშლას. მონაცემთა სუბიექტს ასევე, განემარტა რომ კანდიდატთა სიის საჯარო გამოქვეყნების წესი განსაზღვრული იყო კანონით და კონკურსის შედეგებთან დაკავშირებული პერსონალური მონაცემები საჯაროდ უნდა ყოფილიყო გამოქვეყნებული 5 წლის განმავლობაში (კონკურსზე საბოლოო შედეგების მიღებიდან), მხოლოდ ამ დროის გასვლის შემდეგ იქნებოდა შესაძლებელი მონაცემთა წაშლა.

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ საქმის ფაქტობრივი გარემოებების შესწავლის შემდეგ, დადგინდა რომ მართალია, კონკურსის შედეგების საჯარო გამოქვეყნება კანონით იყო განსაზღვრული, თუმცა ეს არ გულისხმობდა, რომ კონკურსის ორგანიზატორს უნდა გამოექვეყნებინა იმ კანდიდატთა სია, რომლებიც არ შერჩეულან აღნიშნულ პოზიციებზე. ამ შემთხვევაში, საბოლოო შედეგების გამოქვეყნებაში იგულისხმებოდა კონკურსში გამარჯვებულ კანდიდატთა სია.

კონკურსში მონაწილე ყველა კანდიდატის სახელისა და გვარის გამოქვეყნება არ იყო შესაბამისობაში ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის პირველი პუნქტის „გ“ ქვეპუნქტის მოთხოვნასთან. აღსანიშნავია, რომ დამუშავებისთვის პასუხისმგებელი პირის სახელით, დამუშავებაზე უფლებამოსილი პირი (კომპანია, რომელიც მართავდა ვებგვერდს) ამ მონაცემებს შესაბამისი საფუძვლის გარეშე ამუშავებდა, რა დროსაც არღვევდა ძირითადი რეგულაციის მე-5 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტს და მე-6 მუხლის პირველ პუნქტს.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტის თანახმად, პერსონალური მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად და გამჭვირვალედ მონაცემთა სუბიექტთან მიმართებით. მე-6 მუხლის პირველ პუნქტის მიხედვით, მონაცემთა დამუშავება კანონიერია მხოლოდ იმ შემთხვევაში და იმ მოცულობით, თუ არსებობს ძირითადი რეგულაციით პირდაპირ განსაზღვრული მონაცემთა დამუშავების სულ მცირე ერთი საფუძველი მაინც. განსახილველ შემთხვევაში დაირღვა „გ“ ქვეპუნქტის მოთხოვნა, რომლითაც დადგენილია, რომ მონაცემთა დამუშავება კანონიერია თუ ეს აუცილებელია მონაცემთა დამმუშავებელზე დაკისრებული სამართლებრივი ვალდებულების შესასრულებლად.

საზედამხედველო ორგანომ განმარტა, რომ დამუშავებისთვის პასუხისმგებელი პირი ვერ მართავდა საკუთარ ვებგვერდს და მას ამისთვის სჭირდებოდა გარეშე კომპანიის დახმარება, რომელიც უნდა ჩათვლილიყო დამუშავებაზე უფლებამოსილ პირად, თუმცა მათ შორის არ იყო გაფორმებული ხელშეკრულება, რის გამოც დამუშავებაზე უფლებამოსილი პირი სამართლებრივი საფუძვლის გარეშე ამუშავებდა მონაცემებს.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 28-ე მუხლის მე-3 პუნქტის თანახმად, დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემების დამუშავების პროცესი რეგულირდება ხელშეკრულებით ან ევროკავშირის ან წევრი სახელმწიფოების კანონმდებლობით დადგენილი სამართლებრივი დოკუმენტით, რომელიც დამუშავებაზე უფლებამოსილ პირს დააკისრებს ვალდებულებებს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის წინაშე და განსაზღვრავს მონაცემთა დამუშავების საგანს და ხანგრძლივობას, დამუშავების ხასიათსა და მიზანს, მონაცემთა ტიპებსა და მონაცემთა სუბიექტების კატეგორიებს, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებებსა და უფლებებს.

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 28-ე მუხლის მე-3 პუნქტის დარღვევისთვის დააკისრა ჯარიმა 20 000 ევროს ოდენობით, ხოლო დამუშავებაზე უფლებამოსილი პირი ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტის და მე-6 მუხლის პირველი პუნქტის დარღვევის გამო 12 000 ევროს ოდენობით დააჯარიმა.

ინფორმაცია საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (“CNIL”) ახალი უფლებამოსილების შესახებ

2024 წლის 21 მაისს მიღებული კანონით ციფრული გარემოს შესახებ (№2024-449)[1], საფრანგეთის მონაცემთა დაცვის ორგანოს (“CNIL”) უფლებამოსილებების ფარგლები გაიზარდა. აღნიშნული კანონი “CNIL”-ს აღსრულების ახალი შესაძლებლობებით აღჭურავს და საშუალებას მისცემს გაზარდოს ინსპექტირებების ეფექტიანობა.

საკანონმდებლო ცვლილების შემდეგ, “CNIL” პასუხისმგებელია ზედამხედველობა გაუწიოს საფრანგეთში დაფუძნებულ ონლაინ პლატფორმებს, „ციფრული სერვისების შესახებ აქტის“ (“DSA”) დებულებების აღსრულების მიზნით. აღნიშნული მოიცავს რეკლამების გამჭვირვალობის ვალდებულებების დაცვას და მომხმარებლის პროფილზე მორგებული რეკლამის აკრძალვას, რომელიც იყენებს განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს, მათ შორის, პოლიტიკური შეხედულებებისა და ჯანმრთელობასთან დაკავშირებულ მონაცემებს. იმ შემთხვევაში, თუ პლატფორმები არ იქნება კანონმდებლობასთან შესაბამისობაში, შესაძლოა, დაეკისროთ ჯარიმები დიდი ოდენობით (შემოსავლის ექვს პროცენტამდე), ასევე, დამატებითი ჯარიმები, ინსპექტირების ხელის შეშლის შემთხვევაში.

გარდა ამისა, “CNIL”-ის ვალდებულებაა, აღასრულოს „ციფრული მართვის აქტის“ (“DGA”) დებულებები, რომლებიც დაკავშირებულია მონაცემთა ალტრუიზმთან. აღნიშნული კონცეფცია გულისხმობს მონაცემთა ნებაყოფლობით გაზიარებას საჯარო ინტერესების მიზნებისთვის, როგორიცაა ჯანდაცვა და კლიმატის ცვლილება. საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო, ასევე, განიხილავს საჩივრებს გამჭვირვალობის საკითხებთან დაკავშირებით ორგანიზაციებში.

აღნიშნული ცვლილებები აფართოებს საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს უფლებამოსილების ფარგლებს, რაც განპირობებულია მონაცემთა დაცვის სფეროს მზარდი განვითარებითა და ახალი ტექნოლოგიური სიახლეების ინტეგრირებით.

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება შეზღუდული შესაძლებლობების მქონე პირის ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემის უკანონო დამუშავების შესახებ

იტალიის მოქალაქემ განცხადებით მიმართა სახელმწიფო ჯანდაცვის ორგანოს შეზღუდული შესაძლებლობების მქონე პირის სტატუსის მინიჭების მოთხოვნით და შესაბამის საფუძვლად, ჯანმრთელობასთან დაკავშირებული მონაცემის მითითებით. მოქალაქის მოთხოვნა დაკმაყოფილდა და მას მიენიჭა შეზღუდული შესაძლებლობის მქონე პირის სტატუსი.

აღსანიშნავია, რომ იტალიის კანონმდებლობა ითვალისწინებს ახლო ნათესავის მოვლის მიზნით სამსახურიდან დროებით გათავისუფლებას. მონაცემთა სუბიექტის ახლო ნათესავმა საკუთარ დამსაქმებელს სთხოვა მონაცემთა სუბიექტის მოვლისთვის სამსახურიდან დროებით გათავისუფლება. დამსაქმებელმა ინფორმაციის გადასამოწმებლად სახელმწიფო ჯანდაცვის ორგანოსგან მოითხოვა განცხადებაში მითითებული მონაცემთა სუბიექტის, როგორც შეზღუდული შესაძლებლობის მქონე პირის სტატუსის გადამოწმება. სახელმწიფო ჯანდაცვის ორგანომ დამსაქმებელს მიაწოდა ინფორმაცია მონაცემთა სუბიექტის სტატუსის და მის ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემის შესახებ, რაც საფუძვლად დაედო აღნიშნული სტატუსის მინიჭებას.

მონაცემთა სუბიექტმა მიმართა იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს და მოითხოვა მის ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემის დამუშავების კანონიერების შესწავლა.[1]
დამუშავებისთვის პასუხისმგებელი პირის (სახელმწიფო ჯანდაცვის ორგანოს) განმარტებით, დამსაქმებლისთვის მონაცემთა სუბიექტის მონაცემების გადაცემა გამოწვეული იყო ადამიანური შეცდომით, რადგან უწყებაში მონაცემთა დამუშავებაზე პასუხისმგებელ თანამშრომელთა რაოდენობა აღნიშნულ პერიოდში მკვეთრად შემცირებული იყო და შესაბამისად, ვერ მოხერხდა უწყებაში შემოსული მოთხოვნის სათანადო შესწავლა და ინფორმაციის გაცემის მონიტორინგი.

იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მხედველობაში მიიღო აღნიშნული ფაქტი და განმარტა, რომ მხოლოდ ეს გარემოება არ იყო საკმარისი ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნათა დარღვევის საპასუხოდ. საზედამხედველო ორგანომ ყურადღება გაამახვილა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-9 მუხლის პირველ პუნქტზე, რომლის თანახმად, აკრძალულია ისეთი მონაცემების დამუშავება, რომლებიც ამჟღავნებს პირის ჯანმრთელობასთან დაკავშირებულ მონაცემებს. აღნიშნული წესისგან გამონაკლისს წარმოადგენს შემთხვევა, როდესაც მონაცემთა დამუშავება აუცილებელია სამედიცინო დიაგნოზის დასასმელად, ჯანდაცვის ან სოციალური დაცვის უზრუნველსაყოფად, ჯანდაცვისა და სოციალური უზრუნველყოფის სფეროსა და შესაბამისი მომსახურების სამართავად.

საზედამხედველო ორგანოს განმარტებით, სახელმწიფო ჯანდაცვის ორგანოს ჰქონდა მონაცემთა დამუშავების თავდაპირველი საფუძველი (მიზანი) - დაედგინა მონაცემთა სუბიექტის, როგორც შეზღუდული შესაძლებლობების მქონე პირის სტატუსი, მაგრამ დამუშავებისთვის პასუხისმგებელ პირს, დამსაქმებლისთვის ინფორმაციის გაცემისას ერთმანეთისგან უნდა გაემიჯნა შშმ პირის სტატუსის შესახებ ინფორმაცია და ჯანმრთელობასთან დაკავშირებული მონაცემი, რაც მას არ განუხორციელებია.

საზედამხედველო ორგანომ აღნიშნა, რომ დამსაქმებლის მოთხოვნა, რომ გაეგო იყო თუ არა მონაცემთა სუბიექტი ნამდვილად შეზღუდული შესაძლებლობის მქონე, არ გულისხმობდა მისთვის დამატებით, ამ პირის ჯანმრთელობასთან დაკავშირებული მონაცემების მიწოდებას. ამ მოქმედებით დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის პირველი პუნქტის „გ“ ქვეპუნქტის მოთხოვნა მონაცემთა მინიმიზაციის შესახებ. საგულისხმოა, რომ დამუშავებისთვის პასუხისმგებელი პირს არ ჰქონდა გათვალისწინებული შესაბამისი ორგანიზაციული და ტექნიკური მექანიზმები, რაც მნიშვნელოვანი იქნებოდა მონაცემთა დამუშავებისა და ინფორმაციის გაცემის პროცესში მონაცემთა სუბიექტის უფლებების დასაცავად. შესაბამისი მექანიზმების არარსებობამ განაპირობა ადამიანური შეცდომა, რომელიც საზედამხედველო ორგანოს აზრით არა გამამართლებელი, არამედ შემაშფოთებელი გარემოებაა ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავებისას.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 32-ე მუხლის პირველი პუნქტის საფუძველზე, 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. საზედამხედველო ორგანოს აზრით დამუშავებისთვის პასუხისმგებელი პირის მოქმედებები არ შეესაბამებოდა აღნიშნულ მოთხოვნას.
იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის პირველი პუნქტის „გ“ ქვეპუნქტის და 32-ე მუხლის პირველი პუნქტის დარღვევისთვის დააკისრა ჯარიმა 24 000 ევროს ოდენობით.

ინფორმაცია ევროპის მონაცემთა დაცვის ზედამხედველის მონაცემთა უსაფრთხო გადაცემის ახალი მოდელის შესახებ, ევროკავშირის დაწესებულებებსა და საერთაშორისო ორგანიზაციებს შორის

2024 წლის 31 ივლისს ევროპის მონაცემთა დაცვის ზედამხედველმა გამოაქვეყნა ადმინისტრაციული მოწყობის მოდელი პერსონალურ მონაცემთა გადაცემისათვის.[1] მოდელი ეხება საერთაშორისო ორგანიაციებისათვის მონაცემთა გადაცემას ევროკავშირის ორგანოებიდან და სააგენტოებიდან.

მონაცემთა გადაცემის მოდელი შემუშავდა ევროკავშირის იმ სააგენტოების დასახმარებლად, რომლებიც თავიანთი საქმიანობის პროცესში გადასცემენ მონაცემებს საერთაშორისო ორგანიზაციებს. მოდელი მიზნად ისახავს ევროკავშირის სააგენტოების დახმარებას მონაცემთა გადაცემის საკითხებში, რათა სააგენტოებმა ევროკავშირის მონაცემთა დაცვის კანონმდებლობასთან და „მონაცემთა დაცვის ძირითად რეგულაციასთან“[2] შესაბამისად გადასცენ მონაცემებს საერთაშორისო ორგანიზაციებს.

ევროპის მონაცემთა დაცვის ზედამხედველის მიერ გავრცელებული განცხადების თანახმად,[3] ევროკავშირის სააგენტოებმა, თავიანთი საქმიანობის სფეროდან გამომდინარე, შესაძლოა, საერთაშორისო ორგანიზაციებს მიაწოდონ ინფორმაცია ისეთი მნიშვნელოვანი მიზნების მისაღწევად, როგორიცაა მაგალითად, საკვებით დახმარება ან ადამიანის უფლებების შესახებ ადვოკატირება.

ევროპის მონაცემთა დაცვის ზედამხედველი მიიჩნევს რომ, მონაცემთა სუბიექტების პერსონალური მონაცემები დაცული უნდა იყოს ევროპული სტანდარტებისა და საუკეთესო პრაქტიკის შესაბამისად, როგორც ევროკავშირისა და ევროპული ეკონომიკური სივრცის შიგნით, ასევე მის გარეთ. ადმინისტრაციული მოწყობის მოდელი პერსონალურ მონაცემთა გადაცემისათვის დაეხმარება ევროპულ სააგენტოებს ეფექტურად განახორციელონ საერთაშორისო ორგანიზაციებისათვის, საჭიროებისამებრ, პერსონალური მონაცემების გადაცემისათვის.

წინამდებარე მოდელი დაფუძნებულია მონაცემთა დაცვის ძირითად პრინციპებზე და აწესებს დაცვის აუცილებელ მექანიზმებს, რათა უზრუნველყოს ევროკავშირის კანონმდებლობის მონაცემთა დაცვის შესაბამისი ხარისხი.
ევროპის მონაცემთა დაცვის ზედამხედველის გადაწყვეტილების დანართი[4] შეიცავს ინფორმაციას მოდელში განხილულ საკითხებზე:

- შესაბამის განმარტებებს;
- მონაცემთა დაცვის გარანტიებს, მათ შორის, მონაცემთა დამუშავების მიზნის შეზღუდვას, მონაცემთა მთლიანობას და კონფიდენციალურობას, მონაცემთა სიზუსტეს და სისრულეს, მონაცემთა შენახვის ვადას;
- მონაცემთა სუბიექტების უფლებები, მათ შორის, გამჭვირვალობას, ავტომატურ რეჟიმში გადაწყვეტილებების მიღებას;

- მონაცემთა დაცვის საზედამხედველო ორგანოებისაგან ინფორმაციის მიღების უფლებას;
- განსაკუთრებული კატეგორიის მონაცემების შესახებ ინფორმაციას;
- მონაცემთა სუბიექტების საჩივრებზე დროული რეაგირება;
- დამოუკიდებლობას და მიუკერძოებლობას.

ევროკავშირის სააგენტოები ვალდებულნი არიან მონაცემთა გადაცემისას, წინამდებარე მოდელის გამოყენების პარალელურად, მიიღონ დასტური მონაცემთა გადაცემაზე ევროპის მონაცემთა დაცვის ზედამხედველისაგან. მონაცემთა გადაცემის ახალი მოდელის გამოყენება ხელს შეუწყობს და გაამარტივებს მონაცემთა გადაცემის შესახებ ევროპის მონაცემთა დაცვის ზედამხედველის თანხმობის მიცემის პროცესს ევროკავშირის სააგენტოებისათვის.

ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შესახებ

მონაცემთა სუბიექტის მიმართვის საფუძველზე ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შესახებ გადაწყვეტილება მიიღო[1]. ბანკის თანამშრომელს, რომელიც წარსულში მონაცემთა სუბიექტთან დაახლოებული პირს წარმოადგენდა, განმცხადებლის პერსონალურ მონაცემებთან წელიწადნახევრის განმავლობაში ჰქონდა წვდომა.

მონაცემთა სუბიექტმა ორჯერ მიმართა დამუშავებისთვის პასუხისმგებელ პირს, ბანკის მიერ მონაცემთა კონფიდენციალობის დაცვის მოთხოვნით.

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის განმარტებით, ბანკის თანამშრომელმა დაამუშავა მონაცემთა სუბიექტის შესახებ ინფორმაცია მისი სამსახურეობრივი ვალდებულებების ფარგლებს მიღმა და დამუშავებისთვის პასუხისმგებელი პირის უშუალო მითითების გარეშე. გარდა ამისა, ბანკის მიერ გატარდა აუცილებელი და პროპორციული ზომები, რომლებიც შესაბამისობაში იყო ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) 32-ე მუხლთან. ასევე, განხორციელდა მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შესახებ პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსათვის შეტყობინების ვალდებულება “GDPR”-ის 33-ე მუხლის შესაბამისად.

ბელგიის პერსონალურ მონაცემთა დაცვის ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა სუბიექტის შეტყობინების შემდეგ განხორციელებული ზომები ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციასთან“ შესაბამისი იყო. გასათვალისწინებელია, რომ დამუშავებისთვის პასუხისმგებელი პირი მოქმედებდა პროაქტიულად, რათა მომავალში მსგავსი დარღვევები თავიდან აერიდებინა.

ამასთან, განმცხადებელი საჩივარში მიუთითებდა თვალთვალის (“Stalking”) შესახებ, რომელიც სისხლის სამართლის დანაშაულს წარმოადგენს. თუმცა, აღნიშნულ საკითხთან დაკავშირებით ბელგიის პერსონალურ მონაცემთა დაცვის ორგანოს უფლებამოსილების ფარგლები არ ვრცელდება. ყოველივე ზემოხსენებულიდან გამომდინარე, საჩივარი არ დაკმაყოფილდა, ხოლო თვალთვალის ნაწილში დაუშვებლად იქნა ცნობილი.

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს დასკვნა კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების (Privacy-enhancing Technologies - PETs) შესახებ

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების (“Privacy-enhancing Technologies – PETs”) შესახებ დასკვნა გამოაქვეყნა. დასახული მიზნის მისაღწევად საზედამხედველო ორგანოს ინიციატივით დაიწყო აქტიური თანამშრომლობა დამუშავებისთვის პასუხისმგებელ და უფლებამოსილ პირებთან მონაცემთა დამუშავების პროცესში არსებული გამოწვევების შესაფასებლად და კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების შესამუშავებლად. აღსანიშნავია, რომ განხორციელებული მოქმედებების მიუხედავად, ჯერ კიდევ დაბალია ინტერესი აღნიშნული ტექნოლოგიების მიმართ, რადგან მათი შემუშავება, შესაძლოა, დამატებით ფინანსურ ხარჯებთან იყოს დაკავშირებული.[1]

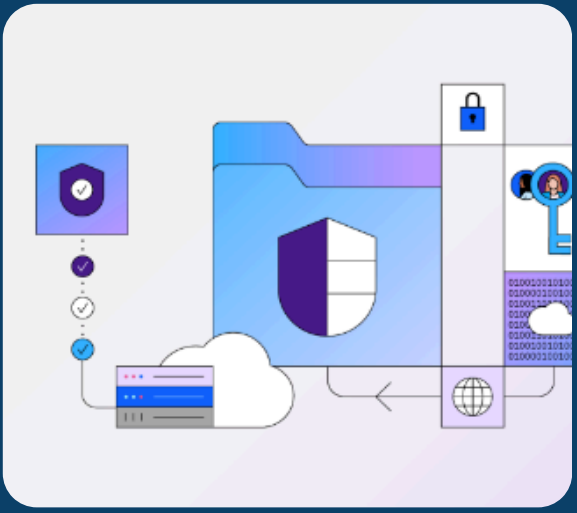
არსებული გამოწვევების საპასუხოდ, საზედამხედველო ორგანოს დასკვნა გამოკვეთს იმ უპირატესობებს, რომლებიც კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების გამოყენებით უზრუნველყოფს, ერთი მხრივ, მონაცემთა დაცვის კანონმდებლობის მოთხოვნათა დაცვას, ხოლო, მეორე მხრივ, მონაცემთა დამმუშავებლებისთვის მოსალოდნელი რისკების წინასწარ დაზღვევას.

დოკუმენტი მიემართება საჯარო და კერძო სექტორის ორგანიზაციებს, რომლებიც მონაცემთა გადაცემის პროცესში აქტიურად გამოიყენებენ აღნიშნულ ტექნოლოგიებს; ორგანიზაციებს, რომლებიც კონცენტრირებულნი არიან მსგავსი ტექნოლოგიების შემუშავებასა და მონაცემთა დამმუშავებლებისთვის მიწოდებაზე; მონაცემთა დაცვის ეროვნულ და უცხოეთის საზედამხედველო ორგანოებს.

კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების მიმართ ინტერესი გამოწვეულია თანამედროვე ტექნოლოგიური სიახლეებითა და მონაცემთა დამუშავების ავტომატური საშუალებების განვითარებით, სადაც განსაკუთრებულად მნიშვნელოვანია მონაცემთა სუბიექტების უფლებების დაცვის უზრუნველყოფა.

[1] Tackling barriers to privacy-enhancing technologies adoption - a PETs project report, <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tackling-barriers-to-privacy-enhancing-technologies-adoption/> [15.08.2024].

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.



ინფორმაცია უსაფრთხოების დარღვევიდან (ინციდენტიდან) გამომდინარე დამდგარი ზიანის ღირებულების “IBM”-ის 2024 წლის ანგარშის შესახებ

კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის სფეროში მოღვაწე მსოფლიოში უდიდესმა სამრეწველო კვლევითმა ორგანიზაციამ „IBM“-მა 2024 წელს გამოაქვეყნა ანგარიში უსაფრთხოების დარღვევების ღირებულების შესახებ.[1]

კვლევის მთავარი საკითხები:

- უსაფრთხოების დარღვევათა დიდი ნაწილი (46%) ეხებოდა პერსონალური მონაცემების ან ინტელექტუალური საკუთრების საკითხებს.
- უსაფრთხოების დარღვევათა გამო დამდგარი ზიანის საშუალო ღირებულება 4.8 მილიონ დოლარს შეადგენს. უსაფრთხოების დარღვევათა გამო დამდგარი ყველაზე დიდი ფინანსური ზიანი ამერიკის შეერთებულ შტატებში ფიქსირდება;
- კიბერუსაფრთხოების სფეროში დასაქმებული კადრების რაოდენობის სიმცირე კვლავ აქტუალურია, თუმცა ამ სფეროში დასაქმებულთა რაოდენობა გაზრდილია;
- ხუთიდან ერთი ორგანიზაცია, სხვადასხვა ფორმით იყენებს გენერირებადი ხელოვნური ინტელექტის უსაფრთხოების ინსტრუმენტებს;

- მონაცემთა უსაფრთხოების დარღვევათა 35% უკავშირდება „არათვალსაჩინო მონაცემებს“ (“shadow data“);
- სრული ფინანსური ზიანიდან 4.9 მილიონი დოლარის ზიანი დადგა შიდა თავდასხმების გამო (“malicious insider attack”). ამ ტიპის თავდასხმები უკავშირდება გენერირებადი ხელოვნური ინტელექტის გამოყენებას, ვინაიდან წინამდებარე ტექნოლოგია მარტივად წერს გამართულ ტექსტებს.
- გაზრდილია უსაფრთხოების დარღვევები, რომლებიც უკავშირდება ინტელექტუალური საკუთრების შესახებ მონაცემებს.
-
- რეკომენდაციები:

- არსებული მონაცემების დეტალურად დაგეგმვა და აღრიცხვა, რა გარემოში და რა საშუალებებით ინახება მონაცემები;

- პრევენციული სტრატეგიების შემუშავება ხელოვნური ინტელექტის და „ავტომატიზაციის“ (“automation”) გათვალისწინებით;

- გენერირებადი ხელოვნური ინტელექტის გამოყენებისას „უსაფრთხოების უპირატესობის“ პრინციპით ხელმძღვანელობა.

- ხელოვნური ინტელექტის გამოყენებამდე და დანერგვამდე, დაგეგმვის ეტაპზე ინფორმაციული უსაფრთხოების საკითხების გათვალისწინება;

- მეტი რესურსის მიმართვა კიბერუსაფრთხოების სფეროში სწავლების მიმართულებით.

საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა უსაფრთხოების დარღვევის შესახებ

საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“HDPA”), მონაცემთა სუბიექტის მიმართვის საფუძველზე, დამუშავებისთვის პასუხისმგებელი პირის (ალიმოსის მუნიციპალიტეტი) მიერ მონაცემთა უსაფრთხოების დარღვევის (ინციდენტი) შესახებ იმსჯელა.[1] საკითხის შესწავლის ფარგლებში შეფასდა როგორც დამუშავებისთვის პასუხისმგებელი პირის, ისე დამუშავებაზე უფლებამოსილი პირის ქმედებების მართლზომიერება.

[1] Cost of Data Breach Report by „IBM“, International Business Machines Corporation.) <https://www.ibm.com/reports/data-breach>, [15.08.2024].

ფაქტობრივი გარემოებების თანახმად, ვებგვერდის საშუალებით მოქალაქეთა პერსონალური ინფორმაციის შემცველ მასალებზე ნებისმიერ ინტერნეტმომხმარებელს ჰქონდა წვდომა. დამუშავებისთვის პასუხისმგებელი პირის განმარტებით, დამუშავებაზე უფლებამოსილმა პირმა ინტერნეტაპლიკაციის არასწორი ვერსია გააქტიურა.

საზედამხედველო ორგანომ აღნიშნა, რომ პერსონალური მონაცემების უსაფრთხოების დასაცავად არ იქნა სათანადო ზომები მიღებული, მაგალითად, არ ხორციელდებოდა სისტემატური მონიტორინგი. დამუშავებისთვის პასუხისმგებელმა და დამუშავებაზე უფლებამოსილმა პირებმა ინციდენტის შესახებ მონაცემთა სუბიექტის მიერ საზედამხედველო ორგანოსთვის მიმართვის შემდეგ შეიტყვეს. მიუხედავად იმისა, რომ ინციდენტი სამჯერ განხორციელდა, შესაბამისი ზომები არ იქნა მიღებული. ამდენად, “HDPA”-მ დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირების მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) 32-ე მუხლის დარღვევა დაადგინა. ასევე, დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია “GDPR”-ის მე-5(1)(f) მუხლი, რომლის შესაბამისადაც პერსონალური მონაცემები „უნდა დამუშავდეს იმგვარად, რომ სათანადო ტექნიკური ან ორგანიზაციული ზომების მეშვეობით უზრუნველყოფილი იყოს მათი უსაფრთხოება, მათ შორის, დაცული იყოს უკანონო და არაუფლებამოსილი პირების მიერ დამუშავების, შემთხვევით დაკარგვის, განადგურების ან დაზიანებისაგან.“

დამატებით, საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ და დამუშავებაზე უფლებამოსილ პირებს შორის გაფორმებული ხელშეკრულების “GDPR”-ის 28-ე მუხლთან შესაბამისობა შეაფასა და აღნიშნა, რომ დოკუმენტში დამუშავებაზე უფლებამოსილი პირის ვალდებულებების შესახებ დებულებები არ იყო ასახული. ფაქტობრივ გარემოებებზე დაყრდნობით, გამოიკვეთა, რომ ინციდენტის თაობაზე დამუშავებაზე უფლებამოსილმა პირმა დამუშავებისთვის პასუხისმგებელ პირს ინფორმაცია გვიან მიაწოდა. თავის მხრივ, დამუშავებისთვის პასუხისმგებელმა პირმა ინფორმაციის დროულად მისაღებად შესაბამისი ზომები არ მიიღო. შედეგად, დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირების მიერ “GDPR”-ის 28-ე მუხლის მე-3 პუნქტის დარღვევა დადგინდა.

“HDPA”-მ, ასევე, განიხილა მონაცემთა უსაფრთხოების დარღვევის თაობაზე მონაცემთა სუბიექტისთვის შეტყობინების საკითხი. აღინიშნა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა საწყის ეტაპზე საჭიროდ არ ჩათვალა მონაცემთა სუბიექტების ინფორმირება. მონაცემთა დაცვის ოფიცერმა, 2023 წლის ივლისში, დამუშავებისთვის პასუხისმგებელ პირს ურჩია მონაცემთა სუბიექტებისათვის ინფორმაციის მიწოდება, თუმცა, მიუხედავად ამისა, პირებს 2023 წლის ოქტომბერში მიეწოდათ არასრული ინფორმაცია. აღნიშნულიდან გამომდინარე, დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია “GDPR”-ის 33-ე მუხლის მე-4 პუნქტი და 34-ე მუხლის პირველი პუნქტი.

საქმის ფაქტობრივი გარემოების შეფასების საფუძველზე, საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს დააკისრა ჯარიმა 20 000 ევროს ოდენობით.

[1] GDPR Hub, HDPA (Greece) - Decision 18/2024, <https://gdprhub.eu/index.php?title=HDPA_(Greece)_-_Decision_18/2024>, [20.08.2024].

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება კომპანიის მიერ მომხმარებელთა მონაცემების შენახვის ვადის შესახებ

მონაცემთა სუბიექტის მიმართვის საფუძველზე ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მომხმარებელთა მონაცემების 3 წელზე მეტი ვადით დამუშავების შესახებ გადაწყვეტილება მიიღო[1]. ფინურმა სატელეკომუნიკაციო კომპანიამ არ დააკმაყოფილა მომხმარებლის პერსონალური მონაცემების წაშლის შესახებ მოთხოვნა, რადგან დამუშავებისთვის პასუხისმგებელი პირის განმარტებით, მონაცემები მუშავდებოდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) 17 (3) (ე) მუხლის შესაბამისად. ხანდაზმული სესხის შესახებ ფინეთის კანონის მე-4 ნაწილის[2] თანახმად, სასესხო ვალდებულების შესრულების ხანდაზმულობის ვადა სამ წელს შეადგენს, აქედან გამომდინარე, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს არ შეეძლო პერსონალური მონაცემების წაშლა, რადგან მონაცემთა სუბიექტთან სახელშეკრულებო ურთიერთობის დასრულებიდან სამი წელი ჯერ კიდევ არ იყო გასული.

დამუშავებისთვის პასუხისმგებელი პირის განცხადებით, როგორც წესი, კომპანიაში მომხმარებელთა მონაცემები სამ წელზე მეტი დროით არ ინახებოდა და ავტომატურად იშლებოდა ვადის გასვლის შემდეგ, რაც აღნიშნულ შემთხვევაში არ განხორციელებულა ტექნიკური ხარვეზის გამო. თუმცა, ორგანიზაციამ მოგვიანებით მონაცემთა სუბიექტის პერსონალური მონაცემები მექანიკურად წაშალა.

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა სუბიექტის პერსონალური მონაცემების შენახვის უფლება ჰქონდა სახელშეკრულებო ურთიერთობის დასრულებიდან სამი წლის განმავლობაში. თუ იგი მონაცემთა სუბიექტის პერსონალურ მონაცემებს წაშლიდა, ვერ შეძლებდა თავის დაცვას მომხმარებელთა ან სხვა კრედიტორების მხრიდან დავის ან პრეტენზიების შესაძლო შემთხვევებში.

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ სატელეკომუნიკაციო კომპანიის მხრიდან “GDPR”-ის მე-17 მუხლის მე-3 პუნქტის “ე” ქვეპუნქტის დარღვევა დაადგინა, რადგან მონაცემთა სუბიექტის მოთხოვნის მიუხედავად, არ წაშალა ის პერსონალური მონაცემები, რომლებიც მოთხოვნამდეც კი ავტომატურად უნდა წაშლილიყო სისტემებიდან. შედეგად, ფინეთის პერსონალურ მონაცემთა დაცვის ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს გამოუცხადა შენიშვნა GDPR-ის 58(2)(ბ) მუხლის შესაბამისად.

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება სკოლაში სახის ამომცნობი სისტემის დანერგვის შესახებ

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“ICO”) საგანმანათლებლო დაწესებულებაში სახის ამომცნობი სისტემის დანერგვის მართლზომიერების შესახებ გადაწყვეტილება[1] მიიღო.

საქმის ფაქტობრივი გარემოებების თანახმად, 11-დან 18 წლამდე მოსწავლეებისთვის უნაღდო ანგარიშსწორების მექანიზმის დანერგვის მიზნით სახის ამომცნობი სისტემა ამოქმედდა. დამუშავებისთვის პასუხისმგებელი პირი, გაერთიანებული სამეფოს „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“UK GDPR”) მე-9 მუხლის მე-2 პუნქტის შესაბამისად, პერსონალურ მონაცემებს ამუშავებდა მშობლებისა და მეურვეების თანხმობის საფუძველზე, რომელიც მოპოვებულ იქნა ავტომატურად და ძალაში იყო შესაბამისი პირების მიერ მის უარყოფამდე (“Opt-out Mechanism”).

საზედამხედველო ორგანომ, ძირითადი რეგულაციის მე-4 მუხლის მე-11 პუნქტზე მითითებით, განმარტა, რომ თანხმობა უნდა იყოს ნათლად გამოხატული. თანხმობის მოპოვება “Opt-out” პროცედურის გამოყენებით არ იყო მიზანშეწონილი, რამდენადაც არ იკვეთებოდა შესაბამისი პირების მკაფიო ნება.

ამასთან, “ICO”-მ აღნიშნა, რომ სისტემის დანერგვამდე დამუშავებისთვის პასუხისმგებელმა პირმა არ განახორციელა მონაცემთა დაცვაზე ზეგავლენის შეფასება, რასაც ითვალისწინებს “UK GDPR”-ის 35-ე მუხლი. “UK GDPR”-ის 35-ე მუხლის მე-4 პუნქტის თანახმად, “ICO”-ს გამოქვეყნებული აქვს იმ აქტივობათა ნუსხა, რომლებიც საჭიროებს პერსონალური მონაცემების დამუშავებამდე მონაცემთა დაცვაზე ზეგავლენის შეფასებას, მათ შორის, ახალი ტექნოლოგიების გამოყენებით ბავშვების პერსონალური მონაცემების დამუშავება.

საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს “UK GDPR”-ის 35-ე მუხლის პირველი პუნქტის დარღვევის გამო შენიშვნა გამოუცხადა და რეკომენდაციები წარუდგინა:

·პერსონალური მონაცემთა დამუშავების დაწყებამდე განხორციელდეს მონაცემთა დაცვაზე ზეგავლენის შეფასება და მისი შედეგები პროექტის გეგმაში აისახოს;
·რისკების შესამცირებლად მონაცემთა დამუშავების აუცილებლობა და პროპორციულობა ხშირად გადაიხედოს;
·სკოლაში გათვალისწინებულ იქნას “ICO”-ს მიერ შემუშავებული სახელმძღვანელო რეკომენდაციები;
·კონფიდენციალობის პოლიტიკა მოსწავლეებისათვის გასაგები ფორმით შემუშავდეს.

[1] GDPR hub, ICO (UK) - ICO - Chelmer Valley High School, <https://gdprhub.eu/index.php?title=ICO_(UK)_-_ICO_-_Chelmer_Valley_High_School>, [21.08.2024].

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანოს შენიშვნა საარჩევნო კომისიაზე კიბერთავდასხმის შესახებ

გაერთიანებული სამეფოს მონაცემთა საზედამხედველო ორგანომ საარჩევნო კომისიის მისამართით შენიშვნა გამოსცა,[1] საარჩევნო კომისიის სერვერებზე კიბერთავდასხმასთან დაკავშირებით. კიბერთავდასხმის შედეგად დამნაშავეებმა მოიპოვეს წვდომა სერვერებზე, სადაც განთავსებული იყო 40 მილიონი ადამიანის პერსონალური მონაცემები.

2021 წლის აგვისტოში, დამნაშავეებმა მოახერხეს საარჩევნო კომისიის სერვერზე (“Microsoft Exchange Server”) წვდომა და პროგრამული ხარვეზების შესახებ ინფორმაციაზე დაყრდნობით შეაღწიეს სერვერზე, რომლებიც სათანადოდ არ იყო დაცული.
2021 წლის ინციდენტიდან ერთი წლის შემდეგ, 2022 წლის ოქტომბერში თავდამსხმელებს საარჩევნო რეესტრში განთავსებულ პერსონალურ მონაცემებზე ჰქონდათ წვდომა, მათ შორის, ამომრჩეველთა სახელებზე, გვარებზე და მისამართებზე. ამასთან, სერვერებზე შეღწევის რამდენიმე შემთხვევა დაფიქსირდა, რის შესახებაც საარჩევნო კომისიას არ ჰქონდა ინფორმაცია.

გაერთიანებული სამეფოს საზედამხედველო ორგანოს მოკვლევის საფუძველზე დადგინდა, რომ საარჩევნო კომისიას არ ჰქონდა მიღებული სათანადო უსაფრთხოების ზომები პერსონალური მონაცემების დასაცავად. სერვერები არ იყო დაცული შესაბამისი უსაფრთხოების სისტემის განახლებებით (“Security Updates“). თავდასხმამდე რამდენიმე თვით ადრე, 2021 წლის აპრილში და მაისში გამოქვეყნდა პროგრამული ხარვეზების გასწორებისათვის საჭირო განახლების პროგრამები (“Security Patches“). ვინაიდან საარჩევნო კომისიის მიერ სერვერების დაცვის სისტემა დროულად არ განახლდა, თავდამსხმელებმა შეაღწიეს სერვერებზე.
თავდასხმის მომენტში, საარჩევნო კომისიას არ ჰქონდა გამართული წესები და პროცედურები მონაცემთა უსაფრთხოების მიმართულებით.

საარჩევნო კომისიამ მიიღო თავდასხმის შემდგომი გამოსასწორებელი ზომები, უსაფრთხოების გასაუმჯობესებლად, მათ შორის, ინფრასტუქტურის განახლების, პაროლების შესახებ წესების და პოლიტიკის დოკუმენტების, ისევე როგორც სისტემაში შესვლის დადასტურების (“Multi-factor Authentication“) მექანიზმების დანერგვის მიმართულებით.

[1]ICO reprimands the Electoral Commission after cyber-attack compromises servers <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/07/ico-reprimands-the-electoral-commission-after-cyber-attack-compromises-servers/> [21.08.2024].

რუმინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება პაციენტის მონაცემების დარღვევის შესახებ

მონაცემთა სუბიექტის მიმართვის საფუძველზე რუმინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ პაციენტის აუდიო და ვიდეოჩანაწერის დამზადება-გავრცელების შესახებ გადაწყვეტილება მიიღო[1].სამსახურებრივი ვალდებულების შესრულებისას ექიმმა პაციენტს მისი თანხმობის გარეშე პირადი ტელეფონით გადაუღო ვიდეო და სოციალურ ქსელ “Facebook“-ზე ატვირთა. აღნიშნულით გასაჯაროვდა მონაცემთა სუბიექტის პერსონალური მონაცემები, კერძოდ, გამოსახულება, ხმა, სახელი, გვარი და ჯანმრთელობის მდგომარეობა. მიუხედავად იმისა, რომ ექიმმა ვიდეოჩანაწერი იმავე დღეს წაშალა, “Facebook” პოსტი უამრავმა ადამიანმა ნახა, ასევე, გავრცელდა სხვადასხვა მედიასაშუალებასა და ვებგვერდზე.

რუმინეთის პერსონალურ მონაცემთა დაცვის ორგანომ შეაფასა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციისა“ (“GDPR”) და პაციენტის უფლებების შესახებ ეროვნული კანონმდებლობის შესაძლო დარღვევის საკითხი. „პაციენტის უფლებების დაცვის შესახებ“ (46/2023)[2] რუმინეთის კანონის მე-20 მუხლის მიხედვით, დაუშვებელია სამედიცინო განყოფილებაში პაციენტის თანხმობის გარეშე ფოტო ან/და ვიდეო გადაღება, გარდა იმ შემთხვევისა, როდესაც ეს აუცილებელია სამედიცინო დიაგნოსტიკისთვის, მკურნალობისთვის ან პაციენტების მხრიდან საჩივრებისა და პრეტენზიებისგან თავის დასაცავად.

“GDPR”-ის მე-5 მუხლის 1 პუნქტის „ა“ ქვეპუნქტის თანახმად, პერსონალური მონაცემები უნდა დამუშავდეს „კანონიერად, სამართლიანად და გამჭვირვალედ“. მონაცემთა დამუშავება მხოლოდ იმ შემთხვევაშია კანონიერი, თუ ხორციელდება “GDPR”-ის მე-6(1) მუხლით განსაზღვრული რომელიმე საფუძვლით. მოცემულ შემთხვევაში, მონაცემთა დამუშავებას (გადაღებას და განთავსებას) კანონიერი საფუძველი არ გააჩნდა.

ამასთან, “GDPR”-ის მე-9 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტის მიხედვით, განსაკუთრებული კატეგორიის მონაცემების დამუშავება დასაშვებია, თუ ცალსახაა მონაცემთა სუბიექტის თანხმობა. ჯანმრთელობასთან დაკავშირებული ინფორმაცია წარმოადგენს განსაკუთრებული კატეგორიის მონაცემს, რომელიც ექიმის მიერ გადაღებულ ვიდეოჩანაწერში იდენტიფიცირებადი იყო.
აღნიშნულიდან გამომდინარე, რუმინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-5, მე-6 (1) და მე-9 მუხლის დარღვევა, შედეგად, ექიმს დაეკისრა ჯარიმა 2 000 (ორი ათასი) ევროს ოდენობით.

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