მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება კომპანია "Sambla Group"-ის მიერ მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შესახებ

საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს რეკომენდაციები ხელოვნური ინტელექტის შესახებ

საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ „მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასების" სახელმძღვანელო რეკომენდაცია გამოაქვეყნა

საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ორგანიზაციებისა და დაწესებულებებისათვის ევროპის ეკონომიკური სივრცის გარეთ პერსონალურ მონაცემთა გადაცემის შემთხვევაში გამოსაყენებელი სახელმძღვანელო რეკომენდაცია გამოაქვეყნა, რომელშიც ყურადღება გამახვილებულია დამუშავების აღნიშნულ პროცესში მონაცემთა დაცვის შესაბამისი გარანტიების უზრუნველყოფაზე.

მარტი 2025

სახელმძღვანელო რეკომენდაციაში განხილულია შემდეგი საკითხები:

- პერსონალურ მონაცემთა საერთაშორისო გადაცემის მაკვალიფიცირებელი მოთხოვნები;
- მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასება;
- მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასებაზე პასუხისმგებელი პირი;
- მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასების ფარგლები, მათ შორის, მონაცემთა შემდგომ გადაცემებთან მიმართებით;
- გადაცემის „მონაცემთა დაცვის ძირითადი რეგულაციით“ გათვალისწინებულ პრინციპებთან შესაბამისობის საკითხი.

მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასების პროცესში, სახელმძღვანელო რეკომენდაციის თანახმად, მიზანშეწონილია შემდეგი ეტაპების გათვალისწინება:

- მონაცემთა გადაცემის შესახებ დეტალური ინფორმაციის მხედველობაში მიღება;
- „მონაცემთა გადაცემის საშუალების“ (“Transfer Tool”) იდენტიფიცირება (იგულისხმება იმგვარი საშუალებები, მაგალითად, როგორებიცაა: ხელშეკრულების სტანდარტული პირობები, სავალდებულო კორპორაციული წესები და სხვა);
- მონაცემთა მიმღები ქვეყნის კანონმდებლობისა და პრაქტიკის, ასევე, მონაცემთა უსაფრთხოების დაცვის დამატებითი საშუალებების და მონაცემთა გადაცემის საშუალების ეფექტიანობის შეფასება;
- შესაბამისი დამატებითი ზომებისა და პროცედურების განხორციელება;
- პერიოდულად მონაცემთა დაცვის გარანტიების შემოწმება, ასევე, ისეთი გარემოებების გათვალისწინება, რომელთაც შესაძლოა მოახდინონ მასზე ზეგავლენა.

პერსონალურ მონაცემთა დაცვის მაღალი ხარისხის გარანტია
პერსონალურ მონაცემთა საერთაშორისო, მათ შორის, ევროპის ეკონომიკური სივრცის გარეთ გადაცემის საკითხი აქტუალურობას ინარჩუნებს, როგორც მცირე, აგრეთვე, საშუალო ზომის ორგანიზაციებისა და დაწესებულებებისათვის. მზარდია პერსონალურ მონაცემთა მესამე ქვეყნებში გადაცემის შემთხვევებიც, სადაც ევროკავშირის კანონმდებლობა და „მონაცემთა დაცვის ძირითადი რეგულაცია“ ყოველთვის არ ვრცელდება.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ თანახმად, საერთაშორისო გადაცემის შემთხვევაშიც, საჭიროა შენარჩუნდეს მონაცემთა უსაფრთხოების დაცვის რეგულაციით განსაზღვრული სტანდარტი. ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკაში, კერძოდ, გადაწყვეტილებაში სახელწოდებით — “Schrems II” შეფასებულია იმ მონაცემთა გადამცემი ორგანიზაციების პასუხისმგებლობის საკითხი, რომლებიც პერსონალურ მონაცემებს ევროპის ეკონომიკური სივრცის გარეთ გადასცემენ, აგრეთვე, ხაზგასმულია მიმღებ სახელმწიფოში, პერსონალურ მონაცემთა უსაფრთხოების დაცვის მიმართულებით მონაცემთა მიმღები პირების პასუხისმგებლობაზე. მათი ვალდებულებაა დარწმუნდნენ, რომ მონაცემები, მათ შორის, მათი გადაცემის პროცესშიც, მუშავდება ევროპის ეკონომიკური სივრცის საკანონმდებლო ჩარჩოს მოთხოვნების შესაბამისად. ევროკავშირის მართლმსაჯულების სასამართლოს განმარტებით, მონაცემთა გადამცემი დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებაა მონაცემთა საერთაშორისო გადაცემის შეწყვეტა და შესაბამისი ხელშეკრულების მოშლა იმ შემთხვევაში, თუ იმპორტიორი არ/აღარ ასრულებს ნაკისრ ვალდებულებებს პერსონალურ მონაცემთა დაცვის შესახებ.

მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასების საკითხი

მონაცემთა გადამცემი დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებაა მონაცემთა საერთაშორისო გადაცემისას (მათ შორის, მესამე ქვეყნებში) შეამოწმოს მათი დაცვის ხარისხი და რამდენად არსებობს დამატებითი მექანიზმების გამოყენების საჭიროება აღნიშნულ საკითხთან მიმართებით. ეს პროცესი ცნობილია მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასების სახელწოდებით (“Data Transfer Impact Assessment – TIA”).

საფრანგეთის საზედამხედველო ორგანოს სახელმძღვანელო რეკომენდაცია მონაცემთა ექსპორტიორებისათვის მონაცემთა საერთაშორისო გადაცემის რისკის შეფასების პროცესში დასახმარებლად იქნა შემუშავებული. მასში „ევროპის მონაცემთა დაცვის საბჭოს“ (“EDPB”) „მონაცემთა საერთაშორისო გადაცემის ინსტრუმენტთა დამატებითი ზომების შესახებ“ სახელმძღვანელო რეკომენდაცია იქნა გათვალისწინებული.

მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასების საჭიროება
მონაცემთა გადამცემი ორგანიზაცია (დამუშავებისთვის პასუხისმგებელი პირი), რომელზეც ევროკავშირის „პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაცია“ ვრცელდება, ცალკეულ შემთხვევებში ვალდებულია, განახორციელოს მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასება. იგი შეფასებას მონაცემთა მიმღები ორგანიზაციის დახმარებით ახორციელებს. მაგალითად, ევროპის ეკონომიკური სივრცის გარეთ მონაცემთა გადაცემამდე, საჭიროა შეფასდეს მონაცემთა საერთაშორისო გადაცემის ზეგავლენა, თუ მონაცემთა გადაცემა ძირითადი რეგულაციის 46-ე მუხლით განსაზღვრული საშუალებით ხორციელდება (მაგალითად: ხელშეკრულების სტანდარტული პირობები, სავალდებულო კორპორაციული წესები და სხვა მსგავსი საშუალებით). მონაცემთა გადამცემი ორგანიზაცია აღნიშნული ვალდებულებისაგან შემდეგ ორ შემთხვევაში თავისუფლდება:

- თუ მიმღები ქვეყანა ექცევა ევროკომისიის მიერ შემუშავებულ მონაცემთა დაცვის სათანადო დაცვის გარანტიების ნუსხაში;

- მონაცემთა საერთაშორისო გადაცემა ეფუძნება ძირითადი რეგულაციის 49-ე მუხლით განსაზღვრულ ერთ-ერთ გამონაკლისს.

მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასების მიზანი
მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასების გადამცემი ორგანიზაციის მიერ მონაცემთა დაცვის ვალდებულებებთან შესაბამისობის კონკრეტული საშუალებით (მაგალითად: ხელშეკრულების სტანდარტული პირობები, სავალდებულო კორპორაციული წესები და სხვა) მიწევის შესაძლებლობის დასაბუთება. საჭიროა მხედველობაში იქნას მიღებული მესამე ქვეყნის კანონმდებლობა და მონაცემთა დაცვის სტანდარტები. განსაკუთრებული ყურადღებით უნდა შეფასდეს მესამე ქვეყანაში ადგილობრივ მთავრობათა მიერ გადაცემულ მონაცემებზე წვდომის საკითხი.
მონაცემთა საერთაშორისო გადაცემის ზეგავლენის შეფასების დოკუმენტი, ზოგიერთ შემთხვევაში, საჭიროა ამოწმებდეს შერჩეული დამატებითი უსაფრთხოების ზომების ადეკვატურობას, რათა ევროკავშირისა და მესამე ქვეყნის კანონმდებლობათა მოთხოვნების განსხვავებების შემთხვევაში, სათანადოდ იქნას უზრუნველყოფილი გადაცემულ მონაცემთა უსაფრთხოება.

სახელმძღვანელო რეკომენდაციის მიზანი და ფარგლები
სახელმძღვანელო რეკომენდაცია ითვალისწინებს საერთაშორისო გადაცემის ზეგავლენის შეფასებამდე განსახორციელებელი მოქმედებების შესახებ ინფორმაციას. იგი წარმოადგენს ერთგვარ გზამკვლევს, თუ როგორ უნდა იქნას გათვალისწინებული „მონაცემთა დაცვის ევროპული საბჭოს“ შესაბამისი რეკომენდაციები, აგრეთვე, აღნიშნულ თემატიკაზე დამატებითი სასარგებლო წყაროებსა და რესურსებს. საგულისხმოა, რომ მას მხოლოდ სარეკომენდაციო ხასიათი აქვს.

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება სოციალური პლატფორმების მიერ არასრულწლოვანთა პერსონალური მონაცემების დამუშავების კანონიერების შესახებ

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ სოციალური ქსელების (“TikTok”-ი, “Reddit”-ი, “Imgur”-ი) მიერ არასრულწლოვანთა პერსონალური მონაცემების დამუშავების კანონიერების შესწავლის მიზნით აღნიშნული პლატფორმების პოლიტიკის შესწავლა დაიწყო, რაც ციფრულ გარემოში არასრულწლოვანთა უსაფრთხოების უზრუნველყოფასა და მონაცემთა სხვადასხვა დამუშავების პროცესების გაერთიანებული სამეფოს „ბავშვის უფლებათა კოდექსთან“ შესაბამისობის დადგენას ემსახურება.

აღსანიშნავია, რომ სოციალური პლატფორმა “TikTok”-ის მიმართ საზედამხედველო ორგანო 13-დან 17 წლამდე ბავშვებისთვის შესათავაზებელი სოციალური პროდუქტების შინაარსის დამდგენი ალგორითმის შეფასებას, ხოლო “Reddit” და “Imgur”-ის შემთხვევაში - არასრულწლოვანთა მონაცემების ფართო მოცულობით გამოყენებისა და მონაცემთა სუბიექტის ასაკის უზრუნველყოფის მექანიზმის გამოკვლევას გეგმავს. საზედამხედველო ორგანომ მსგავსი ღონისძიებები გასულ წელსაც განახორციელა, რის საფუძველზეც მობილურ აპლიკაციებს “Sendit”-ის და “BeReal”-ს დაევალათ არასრულწლოვან მონაცემთა სუბიექტების ადგილმდებარეობის შესახებ მონაცემის („გეოლოკაციის“) დამუშავების წესების განახლება.

საზედამხედველო ორგანოს პოზიციით, სოციალური პლატფორმების მიერ ციფრული ტექნოლოგიებისა და ინოვაციების განვითარებასთან ერთად არ უნდა იქნეს უგულებელყოფილი ბავშვთა, როგორც მონაცემთა სუბიექტების, უფლებები და უნდა შემუშავდეს მექანიზმები, რომელთა საშუალებით შესაძლებელი იქნება ციფრულ გარემოში მათი უსაფრთხოების უზრუნველყოფა.

ისლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება სამედიცინო მომსახურების მიმწოდებელი კომპანიის მიერ პერსონალური მონაცემების დამუშავების კანონიერების შესახებ

ისლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ სამედიცინო მომსახურების მიმწოდებელი კომპანიის მიერ პერსონალური მონაცემების დამუშავების კანონიერება შეაფასა. საქმე შეეხებოდა სამედიცინო ჩანაწერების საერთო საინფორმაციო სისტემაზე წვდომის მართლზომიერებას.

ფაქტობრივი გარემოებები:
დამუშავებისთვის პასუხისმგებელი პირი (ჯანდაცვის ცენტრი[2]) მომსახურებას უწევდა რამდენიმე კომპანიას, რომელთაგან ერთ-ერთის მიმართ ისლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ სამედიცინო ჩანაწერების საერთო საინფორმაციო სისტემაში პერსონალური მონაცემების დამუშავების კანონიერების შესწავლა დაიწყო.

საქმის შესწავლის ფარგლებში გამოიკვეთა, რომ დამუშავებისთვის პასუხისმგებელ პირს ხელშეკრულება რამდენიმე ათეულ ორგანიზაციასთან ჰქონდა გაფორმებული, მათ შორის, ჯანდაცვის მომსახურების სხვა მიმწოდებლებთან, ისლანდიის საფეხბურთო გაერთიანებასთან და სატრანსპორტო ადმინისტრაციასთან. აღსანიშნავია, რომ ყველა მათგანს წვდომა ჰქონდა საერთო სამედიცინო ჩანაწერებზე, რომლებიც მოიცავდა დაახლოებით 450 000 მონაცემთა სუბიექტის პერსონალურ ინფორმაციას. ისლანდიის „სამედიცინო ჩანაწერების შესახებ“ აქტის თანახმად, ამგვარი შეთანხმებების გაფორმება საჭიროებს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსა და სოციალური დაცვის სამინისტროს მხრიდან წინასწარი ნებართვის მოპოვებას.

საქმის ფაქტობრივი გარემოებების შესწავლისას გამოიკვეთა, რომ დამუშავებისთვის პასუხისმგებელ პირს ამგვარი ნებართვა მოპოვებული ჰქონდა მხოლოდ ერთ კომპანიასთან გაფორმებულ შეთანხმებასთან მიმართებით. ნებართვის მოპოვების პროცესში, „სამედიცინო ჩანაწერების შესახებ“ ისლანდიის აქტისა და ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”-ი) მე-6(1)(e)[4] და მე-9(2)(h)[5] მუხლების შესაბამისად, საზედამხედველო ორგანომ იმსჯელა სამედიცინო ჩანაწერების საერთო საინფორმაციო სისტემის საჭიროებაზე და დაადგინა, რომ მონაცემთა დამუშავების მიზანს საზოგადოებრივი ინტერესების დაცვა და პაციენტთა უსაფრთხოების უზრუნველყოფა წარმოადგენდა. დამუშავებისთვის პასუხისმგებელი პირის მითითებით, სხვა შეთანხმებები სწორედ აღნიშნულ ხელშეკრულებას ეყრდნობოდა, შესაბამისად, დამატებითი ლიცენზირების გავლის საჭიროება აღარ არსებობდა.

საზედამხედველო ორგანოს გადაწყვეტილება:
პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მხოლოდ სამედიცინო კომპანიასთან გაფორმებულ შეთანხმებასთან მიმართებით გაცემული ნებართვა არ დააყენა ეჭვქვეშ, რამდენადაც სპეციალური ნებართვა ამ შემთხვევაში უკვე არსებობდა. თუმცა, სხვა შეთანხმებებთან მიმართებით გამოიკვეთა, რომ ეროვნული კანონმდებლობის შესაბამისად კომპეტენტური ორგანოების მხრიდან სათანადო ნებართვა არ იყო მოპოვებული.

საზედამხედველო ორგანოს შეფასებით, ხელშეკრულების მხარისთვის საერთო სამედიცინო ჩანაწერების საინფორმაციო სისტემაზე წვდომის მინიჭების შემთხვევაში, ამგვარი ნებართვა უნდა იქნეს მოპოვებული თითოეულ შეთანხმებასთან მიმართებით. აღნიშნულიდან გამომდინარე, დამუშავებისთვის პასუხისმგებელმა პირმა ვერ დაასაბუთა, რომ სამედიცინო ჩანაწერებზე წვდომა ნებადართული იყო “GDPR”-ის მე-6 მუხლის (მონაცემთა დამუშავების კანონიერება) პირველი და მე-2 პუნქტების შესაბამისად.

“GDPR”-ის 83(2)(a)-ე მუხლის[6] გათვალისწინებით, ერთი მხრივ, აღინიშნა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა ითანამშრომლა საზედამხედველო ორგანოსთან და დროულად მიიღო დარღვევის გამოსასწორებელი ზომები, კერძოდ, ხელშეკრულებების გაფორმების პროცესში გაიარა ლიცენზირების პროცედურა და, აგრეთვე, არაუფლებამოსილ პირებს პერსონალურ მონაცემებზე წვდომა შეუჩერა. თუმცა, მეორე მხრივ, საზედამხედველო ორგანომ, ძირითადი რეგულაციის 83(2)(a)-ე მუხლის შესაბამისად, დაადგინა, რომ დარღვევა თავისი შინაარსის გათვალისწინებით იყო მძიმე, რამდენადაც სამედიცინო ჩანაწერების საერთო საინფორმაციო სისტემაში პერსონალური მონაცემები მრავალი წლის განმავლობაში მუშავდებოდა.

აგრეთვე, საზედამხედველო ორგანოს განმარტებით, დამუშავებისთვის პასუხისმგებელმა პირმა დარღვევა ჩაიდინა განზრახ, რამდენადაც კანონი მკაფიოდ ადგენდა ნებართვის მოპოვების აუცილებლობას და აღნიშნულის თაობაზე არსებობდა წინასწარი ინფორმაცია. შესაბამისად, აღნიშნულმა ფაქტმა, ძირითადი რეგულაციის 83(2)(b)-ე მუხლის[7] მიხედვით, გავლენა იქონია დარღვევის სიმძიმეზე. ამასთანავე, აღნიშნულ პროცესში მუშავდებოდა ჯანმრთელობასთან დაკავშირებული პერსონალური ინფორმაცია, რომელიც “GDPR”-ის 83(2)(g)-ე მუხლის[8] შესაბამისად, წარმოადგენს განსაკუთრებული კატეგორიის პერსონალურ მონაცემს.

ზემოაღნიშნული გარემოებების გათვალისწინებით, ისლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს დააკისრა ჯარიმა 34 360 ევროს ოდენობით.

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება კომპანია “Sambla Group”-ის მიერ მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შესახებ

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ კომპანია “Sambla Group”-ის მიერ მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) ფაქტი შეისწავლა.

საქმის ფაქტობრივი გარემოებები:

დამუშავებისთვის პასუხისმგებელი პირი კომპანია — “Sambla Group” მომხმარებლებისთვის საკრედიტო შეთავაზებების მიწოდებას უზრუნველყოფს, რისთვისაც იყენებდა სარეგისტრაციო ბმულებს. გეგმური შემოწმების მიზნით, საზედამხედველო ორგანოს ინიციატივით, დაიწყო დამუშავებისთვის პასუხისმგებელი პირის ელექტრონული სისტემის ფუნქციონირების და სარეგისტრაციო ბმულების შესწავლა, რის საფუძველზეც დადგინდა, რომ მომხმარებელთა საკრედიტო განაცხადები ელექტრონული ბმულების საშუალებით მესამე პირებისთვის იყო ხელმისაწვდომი. კერძოდ, სარეგისტრაციო ბმულები ვერ უზრუნველყოფდა მასზე განთავსებული ინფორმაციის დაცულობას. მონაცემთა უსაფრთხოების მნიშვნელოვანმა დარღვევამ გამოიწვია მომხმარებლისთვის განკუთვნილი პირადი ანგარიშებისა და საკრედიტო განაცხადების გამჟღავნება არაუფლებამოსილი პირისთვის, რომლებმაც აღნიშნული ბმულების გამოყენებით მოიპოვეს წვდომა მომხმარებელთა პერსონალურ მონაცემებზე.

დამუშავებისთვის პასუხისმგებელმა პირმა განმარტა, რომ ინციდენტის აღმოჩენისთანავე სარეგისტრაციო ბმულების წაშლით შეზღუდა მესამე პირების წვდომა მომხმარებელთა ინფორმაციებზე. საზედამხედველო ორგანოს განმარტებით, აღნიშნული არ იყო საკმარისი ინციდენტზე შესაბამისი რეაგირებისთვის, რადგან დამუშავებისთვის პასუხისმგებელ პირს უნდა გამოეკვლია ის შედეგები, რომლებიც მონაცემთა უსაფრთხოების დარღვევამ გამოიწვია და აგრეთვე, უნდა მიეღო პრევენციული ზომები მომხმარებლებისთვის შესაბამისი შეტყობინების გაგზავნით.

სასამართლოს გადაწყვეტილება:
ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირი 950 000 ევროს ოდენობით დააჯარიმა და მონაცემთა უსაფრთხოების დარღვევის შესახებ ინფორმაციის მომხმარებლებისთვის შეტყობინება დაავალა.

საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს რეკომენდაციები ხელოვნური ინტელექტის შესახებ

საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ, ხელოვნური ინტელექტის გამოყენების პროცესის ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციასთან“ *(“GDPR”)* შესაბამისობის უზრუნველყოფის მიზნებისთვის ორი რეკომენდაცია გამოაქვეყნა*[1]*. რეკომენდაციებში აღნიშნულია, რომ ძირითადი რეგულაციით განსაზღვრული ვალდებულებები ხელოვნური ინტელექტის გამოყენებასთან დაკავშირებულ გამოწვევებს შეესაბამება და უზრუნველყოფს მონაცემთა სუბიექტების ინფორმირებას, ასევე მათთვის რეგულაციით მინიჭებული უფლებებით სარგებლობას.

აღსანიშნავია, რომ ხელოვნური ინტელექტის ზოგიერთი მოდელი ანონიმურია და, შესაბამისად, არ ექცევა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოქმედების ფარგლებში. თუმცა სხვა მოდელები, მაგალითად, „დიდი ენობრივი მოდელი“ *(“LLM”)*, შესაძლოა შეიცავდეს პირთა პერსონალურ მონაცემებს. ამასთან, „მონაცემთა დაცვის ევროპულმა საბჭომ“ *(“EDPB”) 2024* წლის დეკემბერში ხელოვნური ინტელექტის მოდელებთან დაკავშირებით ძირითადი რეგულაციის გამოყენების კრიტერიუმები განსაზღვრა.

“GDPR”-ის მიხედვით, პერსონალური მონაცემები დაცული უნდა იყოს, მათ შორის, ე. წ. ხელოვნური ინტელექტის „სწავლების მონაცემთა ნაკრებებში“ *(“training datasets”)*. მიუხედავად იმისა, რომ მოცემულ შემთხვევებზე მონაცემთა დაცვის ფუნდამენტური პრინციპები ვრცელდება, საგულისხმოა რომ ისინი ადაპტირებული უნდა იყოს ხელოვნური ინტელექტის სპეციფიკურ კონტექსტთან.

ორგანიზაციების მიერ პერსონალურ მონაცემების ხელოვნური ინტელექტის მოდელის შესაქმნელად დამუშავების დროს აუცილებელია მოხდეს მონაცემთა სუბიექტების ინფორმირება. ევროკავშირის კანონმდებლობა მონაცემთა დამუშავების პროცესის გამჭვირვალობის ვალდებულებას ითვალისწინებს, რაც მონაცემთა სუბიექტს თავისი პერსონალური მონაცემების დამუშავების თაობაზე ინფორმაციის მიღების უფლებას ანიჭებს.

დაინტერესებული მხარისათვის აღნიშნული ინფორმაციის მიწოდების ფორმა შესაძლოა ინდივიდუალური რისკებსა და საოპერაციო შეზღუდვებთან ადაპტირდეს. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ შესაბამისად, თუ ხელოვნურ ინტელექტს მონაცემთა სუბიექტების შესახებ ინფორმაციას მესამე პირი აწვდის და პროვაიდერს არ აქვს შესაძლებლობა ფიზიკურ პირებს უშუალოდ დაუკავშირდეს, დამუშავებისთვის პასუხისმგებელ პირებს შეუძლიათ ინფორმაცია საჯაროდ ხელმისაწვდომ ადგილას განათავსონ *(მაგალითად, ვებგვერდზე)*. როდესაც მონაცემთა შეგროვება რამდენიმე წყაროდან ხდება *(როგორც წესი, აღნიშნული ზოგადი დანიშნულების ხელოვნური ინტელექტის მოდელების ახასიათებს)* აუცილებელია მონაცემთა მოპოვების წყაროს კატეგორიებისა და ძირითადი წყაროების მითითება. მონაცემთა დამუშავების ევროპული რეგულაციები მონაცემთა სუბიექტის წვდომის, გასწორების, დაბლოკვის, გასაჩივრებისა და წაშლის უფლებებს განამტკიცებს. აღნიშნულის უზრუნველყოფა შესაძლებელია განსაკუთრებით გართულდეს ისეთ შემთხვევაში, როდესაც ხელოვნური ინტელექტის მიერ მონაცემთა დამუშავების პროცესში რთულია პირის იდენტიფიცირება.

საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს რეკომენდაციები ხელოვნური ინტელექტის შესახებ

მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შედეგად, შესაძლოა, მონაცემთა სუბიექტის პერსონალური მონაცემები ხელმისაწვდომი გახდეს მესამე პირთათვის. ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ინდივიდების, ორგანიზაციებისა და დაწესებულებებისათვის ინფორმაციის არასწორად მიღების შემთხვევათა მართვის მიზნით, სახელმძღვანელო რეკომენდაცია შეიმუშავა. ამასთან, მისი დახმარებით პერსონალურ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები პრაქტიკულ რჩევებს მიიღებენ პერსონალურ მონაცემთა შემცველი ინფორმაციის არასწორ ადრესატთან გაგზავნის შემთხვევებზე რეაგირების თაობაზე.

1. ფიზიკურ პირთათვის სახელმძღვანელო რეკომენდაცია სხვა პირისთვის განკუთვნილ პერსონალურ მონაცემთა შემცველი ინფორმაციის შეცდომით მიღების დროს გამოსაყენებლად.

იმ შემთხვევაში, თუ მონაცემთა დამუშავებაზე პასუხისმგებელი პირი (ფიზიკური პირი, კომპანია ან დაწესებულება) ამუშავებს მონაცემთა სუბიექტის პერსონალურ მონაცემებს და დამუშავების პროცესში შემთხვევით არასწორ ადრესატს გადასცემს მის პერსონალურ მონაცემებს, სახეზეა მონაცემთა უსაფრთხოების დარღვევა (ინციდენტი). მაგალითად, ამგვარი ინციდენტის შემთხვევებს წარმოადგენს: ბანკის მიერ ამონაწერის არასწორ მომხმარებელთან გაგზავნა ელექტრონული ფოსტის საშუალებით, დაწესებულების მიერ წერილის არასწორ მისამართზე გაგზავნა, ფოსტის მიერ ამანათის არასწორ მისამართზე მიტანა ან კლინიკის მიერ ჯანმრთელობის შესახებ ინფორმაციის შემცველი წერილის გაგზავნა სხვა პაციენტთან.

საზედამხედველო ორგანოს რეკომენდაციით, სხვა ადრესატისთვის გამიზნული პერსონალური მონაცემების მიღების შემთხვევაში, მიზანშეწონილია ინდივიდმა იმოქმედოს სწრაფად, რათა შეამციროს აღნიშნული შეცდომისაგან გამომდინარე რისკები, აგრეთვე:

- მოახდინოს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის იდენტიფიცირება (მაგალითად, ელექტრონული ფოსტის მისამართის ან საკონტაქტო ინფორმაციის საშუალებით) და აცნობოს მას შეცდომის შესახებ. შეცდომით გაგზავნილი ინფორმაციის მიმღები არ უნდა დაელოდოს გამოხმაურებას აღნიშნული უზუსტობის თაობაზე, არამედ საჭიროა, რომ იგი პირადი ინიციატივით დაუკავშირდეს დამუშავებისთვის პასუხისმგებელ პირს.
- მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის იდენტიფიცირების მიზნებისათვის, არ არის რეკომენდებული ინფორმაციის მესამე პირთან ან სოციალური მედიის საშუალებით გაზიარება.
- არ უნდა გახსნას შეტყობინების დანართები.

- იმ შემთხვევაში, თუ ეს შესაძლებელია, შეათანხმოს დამუშავებისთვის პასუხისმგებელ პირთან შეცდომაზე რეაგირების საკითხი. შესაძლოა, საკმარისი იყოს შეცდომით მიღებული ელექტრონული ფოსტის წაშლა ან დამუშავებისთვის პასუხისმგებელმა პირმა არასწორ მისამართზე გაგზავნილი წერილის ან ამანათის უკან დასაბრუნებლად გააგზავნოს კურიერი.
- იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელი პირის იდენტიფიცირება შეუძლებელია, ინფორმაციის მიმღები პირი აუცილებელია დაუკავშირდეს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს.
- რეკომენდებული არ არის იმ მონაცემთა სუბიექტთან დაკავშირება, ვისაც შეეხება პერსონალური მონაცემები, ვინაიდან, აღნიშნული წარმოადგენს პერსონალურ მონაცემთა დამუშავებას მონაცემთა სუბიექტის შესახებ. მონაცემთა მიმღები პირი უნდა დაუკავშირდეს არა მონაცემთა სუბიექტს, არამედ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს.

2. სახელმძღვანელო რეკომენდაცია დაწესებულებებისა და ორგანიზაციებისათვის:

ხშირ შემთხვევაში, დაწესებულებები ან კომპანიები შეცდომით იღებენ მონაცემთა სუბიექტების პერსონალური მონაცემების შემცველ ინფორმაციას. მაგალითად, ორგანიზაციის მიერ სხვისთვის გამიზნული წერილის ან ამანათის მიღების, მომხმარებლის მიერ ნაკლის მქონე პროდუქტის ფოტოსურათის ვებგვერდზე ატვირთვის მცდელობისას, შემთხვევით, სხვა ფოტოსურათის გაზიარების, მეილის ადრესატის მითითების შემთხვევაში დაშვებული შეცდომის, დოკუმენტების ან ელექტრონული მოწყობილობების ოფისის ან დაწესებულების ტერიტორიაზე გაუფრთხილებლობით დატოვების გზით.

იმ შემთხვევაში, როდესაც ინფორმაცია გამიზნულად თუ შემთხვევით აღმოჩნდება ორგანიზაციის ან დაწესებულების ხელთ, იგი ვალდებულია იმოქმედოს იმგვარად, რომ უნებლიედ არ დაამუშაოს სხვისთვის განკუთვნილი პერსონალური მონაცემების შემცველი ინფორმაცია. საჭიროა, მხედველობაში იქნას მიღებული მონაცემთა დამუშავების ფართო განმარტება, რაც გულისხმობს, რომ მონაცემთა დამუშავება ხორციელდება არა მხოლოდ აქტიური მოქმედების გზით, არამედ მათი შენახვის გზითაც.

საზედამხედველო ორგანოს რეკომენდაციის თანახმად, სხვისთვის გამიზნული პერსონალური მონაცემების მიღების შემთხვევაში, მიზანშეწონილია:

- გამომგზავნისათვის ელექტრონული ფოსტის შეტყობინებაზე დაუყოვნებლივ პასუხის გაცემა და შეცდომის შესახებ ინფორმაციის მიწოდება, ასევე, მეილის წაშლა, მისი დანართების ნახვის გარეშე;
- წერილის შინაარსის გაცნობისაგან თავის შეკავება;
- წერილის/ამანათის კანონიერი ადრესატისათვის გადაცემის მიზნით შენახვის დროს, საჭიროა მათი უსაფრთხო გარემოში შენახვა, სადაც მასზე შემთხვევითი წვდომა ან მისი განადგურება ვერ განხორციელდება.

თუ კანონიერი ადრესატის პოვნა შეუძლებელია, მიზანშეწონილია, რომ კომპანია ან დაწესებულება დაუკავშირდეს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს, რომელიც დამუშავებისთვის პასუხისმგებელ პირს გაუწევს რეკომენდაციას მონაცემთა დაცვასთან დაკავშირებული ვალდებულებების შესრულების თაობაზე.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (“AEPD”) გადაწვეტილება საფოსტო კომპანიის 200 000 ევროს ოდენობით დაჯარიმების შესახებ

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) საფოსტო კომპანია მონაცემთა უსაფრთხოების დარღვევასთან (ინციდენტი) დაკავშირებული პრევენციული ზომების განუხორციელებლობისთვის 200 000 ევროს ოდენობით დააჯარიმა.

საქმის ფაქტობრივი გარემოებები:
2022 წლის 22 სექტემბერს ქალაქ ლა პალმას ადგილობრივმა პოლიციამ ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს საჩივრით მიმართა. საჩივარი შეეხებოდა მიტოვებულ მიწის ნაკვეთზე 1 404 საფოსტო წერილის აღმოჩენის საკითხს. წერილები გაგზავნილი იყო 2022 წლის თებერვალსა და მარტში. აღსანიშნავია, რომ მათზე გამოსახული ლოგო მიწოდების ვალდებულების მქონე საფოსტო კომპანიის იდენტიფიცირებას ხდიდა შესაძლებელს.

2022 წლის 17 ნოემბერს ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მიიღო კიდევ ერთი შეტყობინება ბალეარის კუნძულების პოლიციისგან, რომელიც იუწყებოდა, რომ ლა პალმას ორ ლოკაციაზე დამატებით 5 354 წერილი იქნა აღმოჩენილი. პოლიციის მიერ მიწოდებული დოკუმენტაციის მიხედვით, წერილების უმრავლესობა დალუქული, თუმცა მათი ნაწილის მთლიანობა დარღვეული იყო.

2022 წლის 28 დეკემბერს ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ საკითხის შესწავლა დაიწყო და მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს – საფოსტო კომპანიას საჩივრების შესახებ აცნობა, რომელმაც შემდგომში მის მიერ განხორციელებული პრევენციული ზომების შესახებ ინფორმაცია წარადგინა. კერძოდ, საფოსტო კომპანიის განმარტებით, დადგენილ იქნა ინციდენტზე პასუხისმგებელი თანამშრომლების ვინაობა და მათ მიმართ დისციპლინური დევნა დაიწყო. ამასთან, კომპანიამ აღნიშნა, რომ აღმოჩენილი წერილები არ იყო გახსნილი, შესაბამისად, არ არსებობდა მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დარღვევის რისკი.

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილების დასაბუთების თანახმად, მიუხედავად იმისა, რომ მონაცემთა დამუშავებისათვის პასუხისმგებელმა პირმა დასაქმებულთა მიერ ხელმოწერილი კონფიდენციალობის დაცვის შესახებ შეთანხმება წარადგინა, თუმცა ინციდენტის პრევენციის ორგანიზაციული ზომების განხორციელებასთან დაკავშირებით შესაბამისი მტკიცებულებები არ წარუდგენია.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ დამსაქმებლები არ უზრუნველყოფდნენ დასაქმებულთათვის სამუშაოს სპეციფიკის შესახებ სათანადო ცნობების მიწოდებას, ისინი თანამშრომლებს მხოლოდ შრომითი ურთიერთობის საწყის ეტაპზე - ერთსაათიან ტრენინგს უტარებდნენ.

საზედამხედველო ორგანომ მიიჩნია, რომ საფოსტო კომპანიაში არ არსებობდა შესაბამისი სისტემა, რომლის მეშვეობითაც დადგინდებოდა მიაღწია თუ არა წერილებმა განსაზღვრულ მისამართზე. აღნიშნული სისტემა, საფოსტო სერვისის განმახორციელებელი კომპანიის საქმიანობიდან გამომდინარე, არსებითად საჭიროდ იქნა მიჩნეული.

ესპანეთის პერსონალურ მონაცემთა საზედამხედველო ორგანომ კომპანიის მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) 5(1)(f) და 32-ე მუხლების დარღვევა დაადგინა, რის საფუძველზეც 200 000 ევროს ოდენობით ჯარიმის გადახდა დააკისრა .

დამატებით, საზედამხედველო ორგანომ მონაცემთა დამუშავებისათვის პასუხისმგებელ პირს წერილების ადგილმდებარეობის კონტროლის (“tracking system”) შესაბამისი სისტემის დანერგვა, ასევე დასაქმებულთათვის თავიანთი საქმიანობის პროცესის ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მოთხოვნებთან შესაბამისობის მიზნით ტრენინგების გამართვა დაავალა.

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