მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

„ევროპის მონაცემთა დაცვის საბჭომ“ „ბლოკჩეინ“ ტექნოლოგიის საშუალებით პერსონალურ მონაცემთა დამუშავების შესახებ სახელმძღვანელო რეკომენდაცია გამოაქვეყნა

პოლონეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება კომერციული ბანკის დაჯარიმების შესახებ

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება იურიდიული კომპანიის 60 000 ფუნტის ოდენობით დაჯარიმების შესახებ

საზედამხედველო ორგანოს მიერ გამოვლენილი დარღვევა შეეხებოდა პერსონალურ მონაცემთა დაცვისთვის არასათანადო ტექნიკური და ორგანიზაციული უსაფრთხოების ზომების მიღებასა და ინციდენტის შესახებ საზედამხედველო ორგანოსათვის დადგენილ ვადაში შეტყობინების ვალდებულების დარღვევას.

ico.

მაისი 2025

საქმის ფაქტობრივი გარემოებები:

2022 წლის ივნისში იურიდიული კომპანია “DPP Law”-ზე კიბერთავდასხმა განხორციელდა, რის შედეგადაც ერთი კვირის განმავლობაში არაუფლებამოსილ პირებს კომპანიის IT სისტემებზე ჰქონდათ წვდომა , მათ შორის იმ ადმინისტრატორის ანგარიშზე, რომელიც საქმის მართვის ძველ სისტემაზე წვდომისთვის გამოიყენებოდა. შედეგად, კიბერთავდამსხმელებმა მიითვისეს 32 GB მოცულობის მონაცემი, რომელიც მოიცავდა კომპანიის კლიენტებთან დაკავშირებულ სასამართლო დოკუმენტებს, ფაილებს, ფოტოებსა და ვიდეოებს, რომელთაგან ზოგიერთი სექსუალურ დანაშაულებსა და ბავშვთა სექსუალური ძალადობის შემცველ მასალას წარმოადგენდა.

ინციდენტის შესახებ იურიდიულმა კომპანიამ დანაშაულის ეროვნულ სააგენტოსგან (“National Crime Agency”) 2022 წლის ივლისში შეიტყო. მომხდარი თავდასხმიდან 43 დღეში მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა აღნიშნულის თაობაზე გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიაწოდა ინფორმაცია.

საზედამხედველო ორგანოს გადაწყვეტილების დასაბუთება:
საზედამხედველო ორგანომ დაადგინა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია გაერთიანებული სამეფოს „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“UK GDPR”) 5(1)(f) მუხლით გათვალისწინებული კეთილსინდისიერებისა და კონფიდენციალურობის პრინციპი და 32(1) მუხლით გათვალისწინებული ტექნიკური და უსაფრთხოების ზომების განხორციელების ვალდებულება.

შესწავლის შედეგად გამოიკვეთა დამუშავებისთვის პასუხისმგებელი პირის ქსელის უსაფრთხოების კრიტიკული ხარვეზები, რამაც თავდამსხმელებს კიბერშეტევის განხორციელების საშუალება მისცა. დამუშავებისთვის პასუხისმგებელმა პირმა ვერ შეძლო შესაბამისი ზომების მიღება ელექტრონულად შენახული პერსონალური ინფორმაციის უსაფრთხოების უზრუნველსაყოფად. შესაბამისი უსაფრთხოების სტანდარტების არარსებობამ კიბერთავდამსხმელებს საშუალება მისცა, იშვიათად გამოყენებული ანგარიშის მეშვეობით, რომელსაც არ ჰქონდა მრავალსაფეხურიანი ავთენტიფიკაცია (“MFA”), მიეღოთ წვდომა კომპანიის ქსელზე და მოეპოვებინათ დიდი რაოდენობით მონაცემები.

საზედამხედველო ორგანოს განმარტებით, არსებული რისკები აუდიტის შედეგად იდენტიფიცირებული უნდა ყოფილიყო. ასევე აღმოჩნდა, რომ გამოყენებული საქმის მართვის სისტემა მოძველებული იყო, ვინაიდან სისტემის მხარდაჭერაც 2019 წელს დასრულდა.

იურიდიული კომპანია ფუნქციონირებდა სამართლებრივი დახმარების მიმართულებით. იურიდიული კომპანიის საქმიანობის ბუნებიდან გამომდინარე, ის პასუხისმგებელია სხვადასხვა კატეგორიის, მათ შორის განსაკუთრებული კატეგორიის პერსონალურ მონაცემებზე. თავდამსხმელების მიერ მოპარული ინფორმაცია შეეხებოდა იდენტიფიცირებადი პირების, კერძოდ, კომპანიის კლიენტების შესახებ პირად მონაცემებს, შესაბამისად, კომპანია კანონის თანახმად პასუხისმგებელი იყო მის სათანადო დაცვაზე.

საზედამხედველო ორგანომ დაადგინა, რომ იურიდიული კომპანიის მიერ დაირღვა გაერთიანებული სამეფოს „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“UK GDPR”) 33(1) მუხლით გათვალისწინებული პერსონალური მონაცემების დარღვევის შესახებ საზედამხედველო ორგანოსთვის 72 საათის განმავლობაში შეტყობინების ვალდებულება.
გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ უარყოფითად შეაფასა ინციდენტის შესახებ შეტყობინების დაგვიანება. კერძოდ, ინციდენტის შესახებ დამუშავებისთვის პასუხისმგებელმა პირმა 43 დღის შემდეგ ეროვნული კრიმინალური სააგენტოსგან შეიტყო. პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადასტურა, რომ დამუშავებისთვის პასუხისმგებელი პირი ცდილობდა სისტემის ხელახლა ამოქმედებას, თუმცა ამავდროულად აღნიშნა, რომ ინციდენტის დროს მონაცემთა სუბიექტებისთვის შექმნილი რისკები სათანადოდ არ იყო შეფასებული და გათვალისწინებული.

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება:
გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა გაერთიანებული სამეფოს „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“UK GDPR”) 5(1)(f) მუხლის - კეთილსინდისიერებისა და კონფიდენციალურობის პრინციპის, 32(1) მუხლის - მონაცემთა დამუშავების უსაფრთხოებისა და 33(1) მუხლის - საზედამხედველო ორგანოსთვის შეტყობინების ვალდებულების დარღვევა. ჯარიმის ოდენობის განსაზღვრაზე გავლენა იქონია, პერსონალური მონაცემების შინაარსმა, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ქმედების დაუდევრობის ხასიათმა. ამასთან, საზედამხედველო ორგანომ საჭიროდ მიიჩნია დაკისრებულ სახდელს ჰქონოდა შემაკავებელი ხასიათი. ზემოთ აღნიშნულის გათვალისწინებით, საზედამხედველო ორგანომ ჯარიმის ოდენობა 60 000 ფუნტის (69,781 ევრო) ოდენობით განსაზღვრა.

„ევროპის მონაცემთა დაცვის საბჭომ“ „ბლოკჩეინ“ ტექნოლოგიის საშუალებით პერსონალურ მონაცემთა დამუშავების შესახებ სახელმძღვანელო რეკომენდაცია გამოაქვეყნა

2025 წლის აპრილის პლენარულ სხდომაზე, „ევროპის მონაცემთა დაცვის საბჭომ“ (EDPB) „ბლოკჩეინ“ ტექნოლოგიის გამოყენებით პერსონალური მონაცემების დამუშავების შესახებ სახელმძღვანელო რეკომენდაცია გამოაქვეყნა.

„ბლოკჩეინი“ ერთგვარი ციფრული ჩანაწერების წიგნია, რომელიც კონკრეტული დროის მონაკვეთში ტრანზაქციების დადასტურებისა და ციფრული აქტივების (მაგალითად, კრიპტოვალუტა) ადრესატის დადგენის საშუალებას იძლევა. ტექნოლოგია უზრუნველყოფს მონაცემების უსაფრთხო დამუშავებასა და გადაცემას, ინარჩუნებს მათ სისწორესა და მიკვლევადობას.[1] ციფრული სისტემა, რომელიც დიდი მოცულობის ინფორმაციას უსაფრთხოდ და გამჭვირვალედ ინახავს, სარგებლობს იმ უპირატესობით, რომ ერთხელ ჩაწერილი მონაცემის შეცვლა პრაქტიკულად შეუძლებელია და ტრანზაქცია ყველა მონაწილისათვის არის ხელმისაწვდომი.[2] მოცემული ტექნოლოგია ყველაზე ხშირად კრიპტოვალუტისათვის გამოიყენება, მაგრამ შესაძლებელია მისი დანრეგვა ნებისმიერ სფეროში, სადაც ინფორმაციის უსაფრთხოდ შენახვა და გაზიარებაა საჭირო.

„ბლოკჩეინის“ გამოყენების ზრდის საპასუხოდ, საბჭო მნიშვნელოვნად მიიჩნევს მონაცემთა დაცვის ძირითად რეგულაციასთან შესაბამისობის მიღწევაში დაეხმაროს ორგანიზაციებს, რომლებიც აღნიშნულ ტექნოლოგიას იყენებენ. სახელმძღვანელო რეკომენდაციაში განხილულია „ბლოკჩეინ“ ტექნოლოგიის ტექნიკური მახასიათებლებსი და პერსონალურ მონაცემთა დამუშავებაზე მათ გავლენა. ასევე, ხაზგასმულია, რომ მნიშვნელოვანია ტექნიკური და ორგანიზაციული ზომების მიღება მონაცემთა დამუშავების ადრეული ეტაპიდანვე, ისე, რომ „ბლოკჩეინთან“ დაკავშირებულ მონაცემთა დამუშავების პროცესში ჩართულ პირთა პასუხისმგებლობისა და ვალდებულების საკითხი განისაზღვროს მონაცემთა დამუშავების დაწყებამდე, პროექტის შემუშავების ეტაპზე.

სახელმძღვანელო რეკომენდაციის თანახმად, „მონაცემთა დაცვაზე ზეგავლენის შეფასება“ (DPIA) საჭიროა განხორციელდეს იმ შემთხვევაში, როდესაც „ბლოკჩეინის“ ტექნოლოგიების გამოყენებით მონაცემთა დამუშავებამ შესაძლოა წარმოშვას მაღალი რისკი მონაცემთა სუბიექტების უფლებებისა და თავისუფლებებისთვის.

სახელმძღვანელო რეკომენდაცია მონაცემთა მინიმიზაციის, დამუშავებისა და შენახვის მეთოდების თაობაზე ინფორმაციას და მაგალითებს შეიცავს. ამასთან, საყურადღებოა რომ „ბლოკჩეინ“ ტექნოლოგიაში პერსონალური მონაცემების შენახვა დაუშვებელია, თუ აღნიშნული ეწინააღმდეგება მონაცემთა დამუშავების პრინციპებს. რეკომენდაციაში ასევე ყურადღება არის გამახვილებული მონაცემთა სუბიექტების უფლებების მნიშვნელობაზე არის განსაკუთრებით გამჭვირვალობის, მონაცემების შესწორებისა და წაშლის უფლებების მიმართულებით.
სახელმძღვანელო რეკომენდაცია საჯარო კონსულტაციებისთვის ხელმისაწვდომია 2025 წლის 9 ივნისამდე.

პოლონეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება კომერციული ბანკის დაჯარიმების შესახებ

პოლონეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ კომერციული ბანკის „Toyota Bank Polska S.A.“ ინსპექტირების შედეგად დადგინდა, რომ ბანკმა ვერ უზრუნველყო მონაცემთა დაცვის ოფიცრის სრული დამოუკიდებლობა.[1] ასევე, ბანკის მიერ შედგენილი დოკუმენტაცია არ შეიცავდა ინფორმაციას საქმიანობის პროცესში განხორციელებული „პროფაილინგის“ თაობაზე. კერძოდ:

- მონაცემთა დაცვასთან დაკავშირებული ინფორმაციის აღრიცხვის დოკუმენტი “Records of Processing Activities”- “ROPA”;
- მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტი, ”Data Protection Impact Assessment “ – “DPIA”.

მონაცემთა დაცვის ოფიცრის არასწორი პოზიციონირება ორგანიზაციის მასშტაბით:
საზედამხედველო ორგანომ კანონმდებლობის მოთხოვნათა დარღვევად მიიჩნია ის ფაქტი, რომ ორგანიზაციის მონაცემთა დაცვის ოფიცერი უშუალოდ არ იყო ანგარიშვალდებული ბანკის მენეჯმენტის და მმართველი რგოლის წინაშე. ოფიცერი ინფორმაციული ტექნოლოგიების აუდიტორისა და უსაფრთხოების სპეციალისტის ფუნქციებს ითავსებდა მონაცემთა უსაფრთხოების დეპარტამენტში და ანგარიშვალდებული იყო ამავე დეპარტამენტის ხელმძღვანელის წინაშე.[3] საზედამხედველო ორგანომ გადაწყვეტილების მიღებისას მხედველობაში მიიღო ის გარემოება, რომ მონაცემთა უსაფრთხოების დეპარტამენტის ხელმძღვანელის ფუნქცია-მოვალეობებში მონაცემთა დამუშავების მოქმედებების მართვაც შედიოდა.

„პროფაილინგის“ შესახებ ინფორმაციის აღრიცხვის საკითხი:
ბანკი მომხმარებელთა გადახდისუნარიანობის დასადგენად მონაცემთა სუბიექტების დიდი რაოდენობით ინფორმაციას ამუშავებდა, მათ შორის, „პროფაილინგის“ გზით. ამავე მიზნით მუშავდებოდა მომხმარებელთა საკრედიტო ქულის (“Credit Score“) შესახებ მონაცემები.
მონაცემთა დაცვასთან დაკავშირებული ინფორმაციის აღრიცხვის დოკუმენტში (“ROPA”), მონაცემთა დამუშავების მოქმედების სრული ინფორმაცია არ იყო მითითებული, მათ შორის, „პროფაილინგის“ შესახებ. ასევე, ბანკს „პროფაილინგის“ პროცესში მონაცემთა დაცვაზე ზეგავლენა (“DPIA”) არ ჰქონდა შეფასებული. საზედამხედველო ორგანოს გადაწყვეტილებაში ხაზგასმულია მონაცემთა მასშტაბური დამუშავების დოკუმენტირებისა და მონაცემთა დამუშავების რისკების შეფასების მნიშვნელობაზე. მიზანშეწონილია, რომ მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტში (“DPIA”) „პროფაილინგის“ ფარგლების შესახებ, მათ შორის მისი კონტექსტისა და მიზნების თაობაზე, ასახული ინფორმაცია სრულყოფილად და გამჭვირვალედ იყოს აღრიცხული.

საზედამხედველო ორგანოს გადაწყვეტილება
შედეგად, საზედამხედველო ორგანომ ბანკს დააკისრა ადმინისტრაციული სახდელი - ჯარიმა:

- 60,000 ევროს ოდენობით - GDPR-ის 38(3) მუხლის დარღვევისთვის;
- 72,000 ევროს ოდენობით - GDPR-ის 30(1) და 35(1.7) მუხლების დარღვევისთვის.

აღსანიშნავია, რომ ბანკზე დაკისრებული ადმინისტრაციული ჯარიმის საერთო რაოდენობამ 132 000 ევრო შეადგინა.

ევროკავშირის მონაცემთა დაცვის ზედამხედველმა (“EDPS”) ევროპის საინვესტიციო ბანკის (“EIB”) მიერ პერსონალურ მონაცემთა გადაცემის მოთხოვნა უარყო

„ევროკავშირის მონაცემთა დაცვის ზედამხედველმა“ (“EDPS”) უარყო ევროპის საინვესტიციო ბანკის (“EIB”) მოთხოვნა პერსონალური მონაცემების, მათ შორის მომხმარებელთა საკონტაქტო ინფორმაციის, ინდოეთსა და ევროკავშირის სხვა არაწევრ ქვეყნებში გადაცემის შესახებ.[1] გადაწყვეტილება 2024 წლის თებერვალში იქნა მიღებული და ზედამხედველის საქმიანობის 2025 წლის ანგარიშში გამოქვეყნდა. „ევროკავშირის მონაცემთა დაცვის ზედამხედველმა“ მონაცემთა უსაფრთხოების უზრუნველსაყოფად არასაკმარისი გარანტიების არსებობაზე გაამახვილა ყურადღება და ხაზი გაუსვა, რომ აღნიშნული სახელმწიფოები ვერ უზრუნველყოფდნენ მონაცემთა დაცვის ისეთ გარანტიებს, რომელიც ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციასთან“ იქნებოდა შესაბამისი.

აღსანიშნავია, რომ ინდოეთის პერსონალურ მონაცემთა დაცვის ციფრული აქტი (“DPDP”), რომელიც 2023 წლის აგვისტოში იქნა მიღებული, დღემდე არ ამოქმედებულა. „ევროკავშირის მონაცემთა დაცვის ზედამხედველმა“ ხაზგასმით აღნიშნა, რომ პერსონალურ მონაცემთა დაცვის ციფრული აქტი ამჟამად, არ გვთავაზობს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ საკანონმდებლო ჩარჩოთი განმტკიცებულ მონაცემთა სათანადო დაცვის გარანტიებს.

„ევროკავშირის მონაცემთა დაცვის ზედამხედველის“ განმარტებით, ინდოეთში მონაცემთა დაცვის კანონის არარსებობა სახელმწიფოში შესაბამისი საკანონმდებლო გარანტიების გაუთვალისწინებლობას გულისხმობდა, კერძოდ, გადაცემული პერსონალური მონაცემები სათანადოდ არ იქნება დამუშავებული და დაცული.

ზედამხედველმა რეკომენდაცია გასცა, რომ არსებულ შემთხვევაში ევროპის საინვესტიციო ბანკი (“EIB”) მონაცემთა გადაცემისთვის შეზღუდული გამოყენების გამონაკლისს დაეყრდნოს, რომელიც ცნობილია, როგორც „გადახვევა“ (“derogation”). აღნიშნული გამონაკლისი კონკრეტული საზოგადოებრივი ინტერესების გათვალისწინებით, იძლევა მონაცემთა გაზიარების საშუალებას, მაშინაც კი, როდესაც მიმღები ქვეყანა ევროკავშირის შესაბამის მონაცემთა დაცვის სტანდარტებს არ აკმაყოფილებს. ამავდროულად, „გადახვევა“ მხოლოდ გამონაკლისი შემთხვევებისთვის არის განკუთვნილი და არა რეგულარული მონაცემთა გაცვლისთვის.

აღსანიშნავია, რომ სტანდარტული სახელშეკრულებო პუნქტების (“SCC”) გამოყენება კვლავ რჩება მონაცემთა ევროკავშირიდან ინდოეთში გადაცემის სათანადო მექანიზმად. პერსონალურ მონაცემთა დაცვის ციფრული აქტის (“DPDP”) ძალაში შესვლისა და პრაქტიკული გამოყენების შესახებ სიცხადის ნაკლებობა, განსაკუთრებით მისი გამონაკლისები, ზემოაღნიშნულ პოზიციას უფრო მეტად დასაბუთებულს და ნათელს ხდის. აღნიშნულ საკითხთან დაკავშირებით ინდოეთის ელექტრონიკისა და ინფორმაციული ტექნოლოგიების სამინისტროს (“MeitY”) საპასუხო განცხადება არ გაუკეთებია.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ სამშენებლო ასოციაცია მოვალეთა პერსონალური მონაცემების შემცველი სიის საჯარო გამოქვეყნებისთვის დააჯარიმა

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ, მონაცემთა სუბიექტის მიმართვის საფუძველზე, სამშენებლო ასოციაციის მიერ მოვალეთა პერსონალური მონაცემების შემცველი სიის ბეჭდური ფორმით საჯარო გამოქვეყნების ფაქტი შეისწავლა.

სამშენებლო ასოციაციამ, როგორც დამუშავებისთვის პასუხისმგებელმა პირმა, შენობის შესასვლელში ყველასთვის ხელმისაწვდომ ადგილას - განცხადებებისთვის გამოყოფილ შემინულ სივრცეში, ასოციაციის წევრთა სამუშაო შეხვედრის დეტალები გამოაქვეყნა, რომელსაც თან დაერთო ასოციაციის 12 მოვალის პერსონალური მონაცემების შემცველი სია. აღნიშნულ სიაში მოხსენიებულმა ერთ-ერთმა მოვალემ, შემდგომში მონაცემთა სუბიექტმა, მისი მონაცემების დამუშავების კანონიერების საკითხის შესწავლის მიზნით, საზედამხედველო ორგანოს განცხადებით მიმართა.

დამუშავებისთვის პასუხისმგებელმა პირმა საზედამხედველო ორგანოსთან არ ითანამშრომლა და მისთვის წარდგენილ შეკითხვებს არ უპასუხა.

საზედამხედველო ორგანოს მიერ საქმის შესწავლის შემდეგ დადგინდა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა მოვალეთა პერსონალური მონაცემების შემცველი სიის ბეჭდური ფორმით საჯარო გამოქვეყნებით ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის პირველი პუნქტის „ვ“ ქვეპუნქტი დაარღვია, 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 (უსაფრთხოება და კონფიდენციალურობა). მოვალეთა პერსონალური ინფორმაციის შემცველი სიის საჯარო გამოქვეყნება კი, არღვევდა ძირითადი რეგულაციის წინამდებარე პრინციპს.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ სამშენებლო ასოციაცია *1 000* ევროს ოდენობით დააჯარიმა და გადაწყვეტილების მიღებიდან *1* თვის განმავლობაში ასოციაციის მოქმედებების ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციასთან“ შესაბამისობაში მოყვანა დაავალა.

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