პერსონალურ მონაცემთა
დაცვის სამსახური

მსოფლიო პრაქტიკა

იანვარი / 2024

მთავარი სიახლეები

მონაცემთა დაცვის ევროპულმა საბჭომ, (“EDPB”) მონაცემთა დაცვის ოფიცრის თაობაზე, კვლევის შედეგები გამოაქვეყნა

საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNIL”) დასაქმებულთა მონიტორინგთან დაკავშირებით კომპანია — “AMAZON FRANCE LOGISTIQUE” 32 მილიონი ევროს ოდენობით დააჯარიმა

მართლმსაჯულების ევროპულმა სასამართლომ (“CJEU”) იმსჯელა განსაკუთრებული კატეგორიის მონაცემის დამუშავების შესახებ

ადამიანის უფლებათა ევროპულმა სასამართლომ (“ECtHR”) საქმეზე: "Tena arregui v. Spain" იმსჯელა

მონაცემთა დაცვის ევროპულმა საბჭომ, (“EDPB”) მონაცემთა დაცვის ოფიცრის თაობაზე, კვლევის შედეგები გამოაქვეყნა

16.01.2024

ფოტო: edpb.europa.eu

მონაცემთა დაცვის ევროპული საბჭოს გადაწყვეტილებით (“EDPB”), შეიქმნა „კოორდინირებული აღსრულების ჩარჩო“ (“Coordinated Enforcement Framework” (“CEF”)), რომლის ძირითადი მიზანია მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის თანამშრომლობის ხელშეწყობა. აღნიშნული ჩარჩოს ფარგლებში, პრიორიტეტულ თემად მიჩნეული იქნა მონაცემთა დაცვის ოფიცერთან (“DPO”) დაკავშირებული საკითხების შესწავლა. 2023 წლის განმავლობაში, მონაცემთა დაცვის ოცდახუთმა საზედამხედველო ორგანომ კოორდინირებულად მოიკვლია “DPO”-ს შესახებ თემატიკა, რომლის ფარგლებშიც შემუშავდა მონაცემთა დამმუშავებლებისა და უფლებამოსილი პირების მიერ შესავსები კითხვარი.

2024 წლის 16 იანვარს, “EDPB”-მ გამოაქვეყნა საზედამხედველო ორგანოების მიერ ჩატარებული ერთობლივი კვლევის შედეგები.[1] დოკუმენტში განხილულია ოფიცრების შესახებ არსებული გამოწვევები და წარმოდგენილია შესაბამისი რეკომენდაციები.

კვლევის ფარგლებში წარმოდგენილი შეფასებები და რეკომენდაციები

1. ოფიცრის დანიშვნის/განსაზღვრის საკითხი

კვლევის პროცესში გამოიკვეთა შემთხვევები, როდესაც კონკრეტულ ორგანიზაციაში, “GDPR”-ის 37(1)-ე მუხლით დადგენილი ვალდებულების მიუხედავად, “DPO” არ არის დანიშნული. მაგალითად, იმ მიზეზთა გამო, რომ მონაცემთა დამმუშავებელი მიიჩნევდა, რომ 37(1)-ე მუხლი მათზე არ ვრცელდებოდა.

💡 რეკომენდაცია

მონაცემთა დაცვის საზედამხედველო ორგანოებმა უნდა აამაღლონ ორგანიზაციებში ცნობიერება “DPO”-ს დანიშვნის ვალდებულებასთან დაკავშირებით.

2. არასაკმარისი რესურსები

საკითხის მოკვლევის პროცესში გამოვლინდა ოფიცრების საჭიროებები ხელმისაწვდომ რესურსებთან დაკავშირებით. “GDPR”-ის 38(2)-ე მუხლის თანახმად, მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა ხელი უნდა შეუწყონ ოფიცერს მისი ფუნქციების

[1] European Data Protection Board (EDPB), Designation and Position of Data Protection Officers, Adopted on 16 January 2024: <https://edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf>, [24.01.2024].

შესრულებაში და უზრუნველყონ აუცილებელი და სათანადო რესურსებით. ზოგიერთ შემთხვევაში, ორგანიზაციის მოცულობის და სტრუქტურის გათვალისწინებით, შესაძლოა, საჭირო იყოს ოფიცერთა გუნდის შექმნა.

კვლევაში მონაწილე ზოგიერთმა საზედამხედველო ორგანომ აღნიშნა, რომ ოფიცრებს არ ჰქონდათ საკმარისი რესურსი. ასევე, ხაზი გაესვა, რომ "DPO"-ებს არ ჰყავდათ მოადგილე, რაც ქმნიდა პრობლემას სამუშაოს შესრულების ეფექტიანობისა და უწყვეტობის თვალსაზრისით (მაგალითად, ოფიცრის შვებულებაში გასვლა, თანამდებობის დატოვება და სხვა).

ამასთან, ყურადღება გამახვილდა "DPO"-ების ერთობლივად სხვადასხვა უწყებაში მუშაობაზე, რა დროსაც ვერ ხერხდებოდა ფუნქციების სათანადოდ შესრულება, სათანადო რესურსების გათვალისწინებით. მსგავსი პრობლემა წამოიჭრა ორგანიზაციის ფარგლებში დანიშნულ ოფიცერთან მიმართებითაც, რომელსაც ასევე დაკისრებული აქვს სხვა ამოცანები.

გასათვალისწინებელია, "GDPR" არ ადგენს ვალდებულებას, რომ: "DPO"-ს ჰყავდეს მოადგილე; "DPO" არ მუშაობდეს ნახევარ განაკვეთზე; ერთმა "DPO"-მ არ შეასრულოს სხვადასხვა მოვალეობა. თუმცა, ყველა შემთხვევაში, აუცილებელია, რომ ოფიცერს ჰქონდეს საკმარისი რესურსი დაკისრებული ვალდებულებების შესასრულებლად.

რეკომენდაციები:

- ✓ მონაცემთა დაცვის საზედამხედველო ორგანოებმა გადადგან შესაბამისი ნაბიჯები ორგანიზაციების ხელმძღვანელობის წახალისების თვალსაზრისით, რათა "DPO"-ებსა და მათ გუნდზე მეტი რესურსი იქნეს გათვალისწინებული;
- ✓ მონაცემთა დამმუშავებლებმა და უფლებამოსილმა პირებმა, განახორციელონ შესაბამისი ანალიზი ოფიცრების საჭიროებებთან დაკავშირებით;
- ✓ მონაცემთა დამმუშავებლებმა და უფლებამოსილმა პირებმა უზრუნველყონ ფუნქციების შესასრულებლად "DPO"-ების სათანადო რესურსებით აღჭურვა;
- ✓ მონაცემთა დაცვის საზედამხედველო ორგანოებმა შეიმუშაონ სახელმძღვანელოები და დამატებითი სასწავლო მასალა, რათა დაეხმარონ მონაცემთა დაცვის ოფიცრებს კომპლექსური საკითხების მართვასა და დროის რესურსების ეფექტიანად განაწილებაში.

3. ოფიცრის არასათანადო ექსპერტული ცოდნა

კვლევის პროცესში გამოიკვეთა, რომ "DPO"-ებს არ აქვთ სათანადო ექსპერტული ცოდნა.

"GDPR"-ის პრეამბულის 97-ე პუნქტის თანახმად, ოფიცრებს, მონაცემთა დამუშავების ოპერაციების ბუნების

გათვალისწინებით, სათანადო ექსპერტული ცოდნა მოეთხოვებათ.

რეკომენდაციები:

- ✓ მონაცემთა დაცვის საზედამხედველო ორგანოებმა შეიმუშაონ სახელმძღვანელო ოფიცრის თემატიკაზე და ჩაატარონ სასწავლო ტრენინგები;
- ✓ მონაცემთა დამმუშავებლებმა და უფლებამოსილმა პირებმა უზრუნველყონ მონაცემთა დაცვის ოფიცრების გადამზადება თანამედროვე სტანდარტების შესაბამისად;
- ✓ გაძლიერდეს დაინტერესებულ პირებთან თანამშრომლობა.

4. ოფიცრის არასათანადო ფუნქციებით აღჭურვა

"GDPR"-ის 30-ე მუხლი ითვალისწინებს დავალებათა ნუსხას, რომელიც უნდა შეასრულოს მონაცემთა დაცვის ოფიცერმა. კვლევის შედეგების თანახმად, აღნიშნული ამოცანები ყოველთვის სათანადოდ არ არის დაკისრებული.

რეკომენდაციები:

- ✓ მონაცემთა დაცვის საზედამხედველო ორგანოებმა გადადგან შესაბამისი ქმედითი ნაბიჯები, რათა მონაცემთა დამმუშავებლებმა და უფლებამოსილმა პირებმა უზრუნველყონ ოფიცრებზე ფუნქციებისა და მოვალეობების სათანადო გადანაწილება;
- ✓ მონაცემთა დამმუშავებლები დარწმუნდნენ, რომ "DPO"-ები აღჭურვილნი არიან სათანადო ფუნქციებით;
- ✓ მონაცემთა დამმუშავებლებმა "DPO"-ებთან ერთობლივი მუშაობით გადაანაწილონ ფუნქციები.

ფოტო: flaticon.com

5. ორგანიზაციის ფარგლებში ოფიცრის სისტემური ჩართულობის ნაკლებობა

კვლევამ გამოავლინა, რომ არსებობს გარკვეული ხარვეზები და არათანმიმდევრულობა მონაცემთა დაცვის ოფიცრის ფუნქციებთან მიმართებით. რამდენიმე საზედამხედველო ორგანომ აღნიშნა, რომ "DPO"-ებს არ ჰქონდათ საკმარისი ინფორმაცია მონაცემთა დაცვის საკითხების თაობაზე.

რეკომენდაციები:

- ✓ მონაცემთა დაცვის ოფიცერს საკუთარი ფუნქციის განხორციელებისას უნდა ჰქონდეს სათანადო მხარდაჭერა;
- ✓ მონაცემთა დაცვის საზედამხედველო ორგანოებმა სხვადასხვა აქტივობის ორგანიზებით გააძლიერონ "DPO"-ების დამოუკიდებლობის ხარისხი;
- ✓ მონაცემთა დამმუშავებლებმა და უფლებამოსილმა პირებმა მონაცემთა დაცვის ოფიცრები შესაბამისად ჩართონ სხვადასხვა ორგანიზაციულ საკითხში.

6. ოფიცრის ინტერესთა კონფლიქტი და არასათანადო დამოუკიდებლობა

კვლევის შედეგებზე დაყრდნობით, გარკვეულ შემთხვევებში, გამოიკვეთა საჭიროებები "DPO"-ების მიმართ ინტერესთა კონფლიქტის არსებობისა და მათი დამოუკიდებლობის თვალსაზრისით. გარდა ამისა, "GDPR"-ის 38(3) მუხლით დადგენილი მოთხოვნების მიუხედავად, "DPO"-ები იღებდნენ მითითებებს თავიანთი მოვალეობებისა და ამოცანების შესრულებასთან დაკავშირებით.

რეკომენდაციები:

- ✓ "DPO"-ების როლის გათვალისწინებით, ინტერესთა კონფლიქტის თაობაზე შემუშავდეს სახელმძღვანელო;
- ✓ ოფიცერთა დამოუკიდებლობის თემატიკაზე განხორციელდეს ცნობიერების ამაღლების კამპანიები;
- ✓ ორგანიზაციებმა და ოფიცრებმა წერილობით განსაზღვრონ "DPO"-ების მოვალეობები და სხვა რელევანტური საკითხები.

7. ოფიცრის ანგარიშვალდებულება ორგანიზაციის უმაღლესი ხელმძღვანელობის წინაშე

"GDPR"-ის 38 (3)-ე მუხლი ადგენს მონაცემთა დაცვის ოფიცრის ანგარიშვალდებულებას უმაღლესი ხელმძღვანელობის წინაშე. პრაქტიკაში გამოიკვეთა შემთხვევები, როდესაც ამგვარი მოთხოვნა არ არის დაკმაყოფილებული. კერძოდ, მონაცემთა დაცვის ოფიცრებს არ აქვთ პირდაპირი კავშირი უმაღლეს მენეჯმენტთან.

რეკომენდაციები:

- ✓ უმაღლესი მენეჯმენტის წინაშე ანგარიშვალდებულების კონტექსტში მიზანშეწონილია, შემუშავდეს კონკრეტული სახელმძღვანელო, რაც მონაცემთა დამმუშავებლებს და უფლებამოსილ პირებს დაეხმარებათ შესაბამისი სტანდარტების დანერგვაში;
- ✓ მონაცემთა დაცვის საზედამხედველო ორგანოები დაეხმარონ ორგანიზაციებს, რათა შეიმუშაონ უწყებრივი სტანდარტები და მონაცემთა დაცვის შიდა პოლიტიკა იმისათვის, რომ უზრუნველყოფილი იქნას მონაცემთა დაცვის ოფიცრის ანგარიშვალდებულება უმაღლესი ხელმძღვანელობის წინაშე;
- ✓ მიზანშეწონილია, მონაცემთა დაცვის საზედამხედველო ორგანოებმა ან/და „მონაცემთა დაცვის ევროპულმა საბჭომ" მიიღონ საუკეთესო პრაქტიკაზე დაფუძნებული რეკომენდაციები "DPO"-ების ანგარიშვალდებულების უზრუნველსაყოფად;
- ✓ სასურველია, მონაცემთა დაცვის საზედამხედველო ორგანოებმა განახორციელონ მეტი აქტივობა მონაცემთა დაცვის ოფიცრების უმაღლეს მენეჯმენტთან პირდაპირი კავშირის ხელშეწყობის თვალსაზრისით, რაც "DPO"-ების დამოუკიდებლობის მნიშვნელოვან გარანტს წარმოადგენს.

კვლევის ფარგლებში წარმოდგენილი შეფასებები და რეკომენდაციები ხაზს

უსვამს მონაცემთა დაცვის ოფიცრის როლის გაძლიერებისა და ხელშეწყობის მნიშვნელობას. ოფიცერზე დაკისრებული ფუნქციების ეფექტიანად, მონაცემთა დაცვის მოთხოვნების შესაბამისად განსახორციელებლად, აუცილებელია მათი სათანადო რესურსებით უზრუნველყოფა. ამ მიმართულებით საჭიროა „კოორდინირებული აღსრულების ჩარჩოს“ (“CEF”) ფარგლებში თანამშრომლობა და ასევე, შესაბამისი სახელმძღვანელოების შექმნა.

ადამიანის უფლებათა ევროპულმა სასამართლომ (“ECtHR”) საქმეზე: "Tena arregui v. Spain" იმსჯელა

11.01.2024

ფოტო: coe.int

საქმე “Tena Arregui v. Spain”[2] შეეხება მომჩივნის პირადი ცხოვრების პატივისცემისა და მიმოწერის კონფიდენციალურობის უფლების დაცვას „ადამიანის უფლებათა ევროპული კონვენციის“ (“ECHR”) მე-8 მუხლის მიხედვით. მომჩივანი — პ. ესპანეთის პოლიტიკური პარტიის — “Unión, Progreso y Democracia” (“UPyD”) წევრი იყო და საქმე შიდაპარტიული დავების დროს, მისი პირადი ელექტრონული ფოსტის მონიტორინგსა და გამჟღავნებას შეეხებოდა.

ფაქტობრივი გარემოებები:

2015 წლის აპრილის დასაწყისში, პოლიტიკური პარტიის — “UPyD”-ის ლიდერებმა მისი ერთ-ერთი წევრი — პ. გააძევეს იმ ვარაუდით, რომ იგი ჩართული იყო ოპოზიციურ პარტია “Ciudadanos”-თან მოლაპარაკებებში. “UPyD”-ის ლიდერებმა რამდენიმე თვის ხანგრძლივობით დაიქირავეს კერძო კომპანია, რათა მონიტორინგი განეხორციელებინათ გაძევებული წევრის მიერ გაგზავნილი და მიღებული ელექტრონული ფოსტის კორესპონდენციებზე. მონიტორინგის შედეგად აღმოჩნდა, რომ მომჩივანს წერილები გაგზავნილი ჰქონდა განსხვავებული აზრის მქონე პარტიის წევრებთან, რომლებშიც კოალიციის ჩამოყალიბების მიზნით ახალი პოლიტიკური პარტიის შექმნის საკითხი იყო განხილული. მონიტორინგის განმახორციელებელი კომპანიის მიერ აღმოჩენილი ელექტრონული წერილების შესახებ ინფორმაცია ცნობილი გახდა პრესისთვის.

[2] საჩივრის ნომერი № 42541/18, https://hudoc.echr.coe.int/?i=001-229933.

საჩივარი:

ელექტრონული ფოსტის გამჟღავნების საპასუხოდ, მომჩივანმა მიმართა “UPyD”-ის დავების განსახილველ ორგანოს. საჩივარს პარტიის ის სხვა წევრები შეუერთდნენ, რომელთა კორესპონდენციებიც ასევე იქნა განხილული და მოთხოვნილი იქნა დისციპლინური სამართალწარმოება “UPyD”-ის ლიდერების წინააღმდეგ. თუმცა, დავის განმხილველმა ორგანომ არ დააკმაყოფილა საჩივარი და დაადასტურა, რომ მიყურადება აუცილებელი და პროპორციული იყო შექმნილი განსაკუთრებული გარემოების გათვალისწინებით, რომელიც პარტიას არჩევნებამდე შეექმნა.

შემდგომში, მომჩივანმა საჩივრით მიმართა სამართალდამცავ ორგანოებს სისხლისსამართლებრივი დევნის განხორციელების მიზნით - საქმე “UPyD”-ის ორგანიზაციული მენეჯერის წინააღმდეგ საიდუმლოების უკანონო გამჟღავნების გამო, ესპანეთის კონსტიტუციის მე-18 მუხლის მიხედვით მისი პირადი ცხოვრების ხელშეუხებლობის უფლების დარღვევის მოტივით.

ეროვნული სასამართლოების გადაწყვეტილებები:

მოსამართლემ, ფაქტობრივი გარემოებების შესწავლისა და მტკიცებულებების მოძიების შემდგომ, სისხლის სამართლის საქმის აღძვრის გადაწყვეტილება მიიღო. თუმცა, მადრიდის “Audiencia Provincial” სასამართლომ გააუქმა აღნიშნული გადაწყვეტილება და საქმის დროებით შეწყვეტის ბრძანება გასცა. მადრიდის სასამართლომ საქმის დროებით შეწყვეტის გადაწყვეტილება განმარტა იმით, რომ მონიტორინგი მიზნად ისახავდა პარტიაში არსებული დარღვევების გამოვლენას და ბრალდებული არ მოქმედებდა სხვა განზრახვით, გარდა პარტიასთან დაკავშირებული გადაცდომის გამოვლენისა. მან დაასკვნა, რომ ფაქტი არ იყო საკმარისად დასაბუთებული.

მომჩივანმა მოითხოვა ზემოაღნიშნული გადაწყვეტილების ბათილად ცნობა, მაგრამ მადრიდის “Audiencia Provincial” სასამართლომ არ დააკმაყოფილა მისი მოთხოვნა. მომჩივანმა საკონსტიტუციო სასამართლოს მიმართა, ამტკიცებდა რა მისი ეფექტიანი სამართლებრივი დაცვისა და კონფიდენციალურობის მიმოწერის უფლების დარღვევას.

2018 წლის მარტში, საკონსტიტუციო სასამართლომ არ დააკმაყოფილა საჩივარი, მხარი დაუჭირა მადრიდის “Audiencia Provincial” სასამართლოს გადაწყვეტილებას. საკონსტიტუციო სასამართლომ განაცხადა, რომ გადაწყვეტილება საქმის შეწყვეტის შესახებ იყო ადეკვატურად დასაბუთებული და მომჩივნის უფლებები დაცული იყო სხვა სამართლებრივი საშუალებებით.

ევროპული სასამართლოს გადაწყვეტილება:

სასამართლომ დაადგინა, რომ კონვენციის მე-8 მუხლის მიხედვით, ელექტრონული ფოსტა განიხილება „პირადი ცხოვრების“ და „კორესპონდენციის“ ცნებების ფარგლებში მაშინაც კი, როდესაც იგი პროფესიული ხასიათისაა ან სამუშაო ადგილიდან არის გაგზავნილი[3]. მან აღნიშნა, რომ მიუხედავად იმისა, რომ მე-8 მუხლი, უპირველეს ყოვლისა, აღკვეთს საჯარო ხელისუფლების თვითნებურ ჩარევას, იგი ასევე აკისრებს სახელმწიფოებს პოზიტიური ვალდებულებებს აღნიშნული უფლებების ეფექტიანი დაცვის უზრუნველყოფის მიზნით.

სასამართლომ ხაზი გაუსვა ინდივიდუალურ და საზოგადოების ინტერესებს შორის სამართლიანი ბალანსის მნიშვნელობას და აღიარა, რომ სახელმწიფოს პოზიტიური ვალდებულებები მოიცავს საკანონმდებლო ჩარჩოსაც, რომელმაც უნდა უზრუნველყოს პირადი ცხოვრების დაცვა სხვადასხვა კონტექსტში. სასამართლომ აღიარა პოლიტიკური პარტიების ავტონომია, მაგრამ ხაზგასმით აღნიშნა, რომ აღნიშნული არ უნდა იძლეოდეს პოლიტიკური პარტიის წევრების მიმოწერის მონიტორინგის შეუზღუდავ შესაძლებლობას.

მოცემულ შემთხვევაში, პოლიტიკური პარტიის გაძევებული წევრის სხვა პარტიის წარმომადგენლებთან მოლაპარაკებების დამადასტურებელი ელექტრონული ფოსტის მონიტორინგი, სასამართლომ ფიზიკური პირის პირადი ცხოვრების უფლებაში სერიოზულ ჩარევად შეაფასა. თუმცა, მან ასევე აღნიშნა, რომ ადგილობრივი ხელისუფლების ორგანოებმა ამ შემთხვევაში საკუთარი პოზიტიური ვალდებულებები შეასრულეს. სასამართლომ აღნიშნა შემთხვევის განსხვავება დამსაქმებელ-თანამშრომლის ურთიერთობებისგან და ხაზგასმით თქვა, რომ პოლიტიკურმა პარტიებმა კორესპონდენციის მონიტორინგის დროს უნდა უზრუნველყონ შესაბამისი უსაფრთხოების ზომები.

სასამართლომ განიხილა შიდა ხელისუფლების არგუმენტები სისხლის სამართლის პროცესის შეწყვეტის შესახებ. მან დაადგინა, რომ გადაწყვეტილება არ იყო თვითნებური ან არაგონივრული და რომ მომჩივანს ჰქონდა შესაძლებლობა, გაესაჩივრებინა იგი ეროვნულ სასამართლოში.

შედეგად, ევროპულმა სასამართლომ დაასკვნა, რომ ესპანეთის შიდა საკანონმდებლო ბაზა

[3] იხ. *Copland v. the United Kingdom*, no. 62617/00, § 41, ECHR 2007-I.

ითვალისწინებდა ადეკვატურ დაცვას პიროვნების პირადი ცხოვრებისა და მიმოწერის უფლებისთვის და არ არსებობდა კონვენციის მე-8 მუხლის დარღვევა.

მართლმსაჯულების ევროპულმა სასამართლომ ("CJEU") იმსჯელა განსაკუთრებული კატეგორიის მონაცემის დამუშავების შესახებ

8.01.2024

ფოტო: en.wikipedia.org

მართლმსაჯულების ევროპულმა სასამართლომ ("CJEU"), "*ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts*" (C-667/21) საქმესთან დაკავშირებით განსაკუთრებული კატეგორიის მონაცემების დამუშავების შესახებ განმარტებები გააკეთა.[4] საქმე შეეხებოდა დასაქმებულთა მონაცემების დამუშავების საკითხს და „მონაცემთა დაცვის ძირითადი რეგულაციის" ("GDPR") შესაბამისად კომპენსაციის მიღების უფლებას.

"MDK Nordrhein" წარმოადგენდა ჯანმრთელობის დაზღვევის სახელმწიფო ორგანოს, რომელიც პასუხისმგებელია შრომისუუნარობის შესახებ საექსპერტო დასკვნების შემუშავებაზე, მათ შორის, საკუთარი დასაქმებულების შესახებ. აღნიშნული ვალდებულების შესრულება ევალება სამსახურის სპეციალურ ორგანიზაციულ ერთეულს და თანამშრომლების მხოლოდ შეზღუდულ რაოდენობას აქვს წვდომა პირთა „სოციალურ მონაცემებზე" და ელექტრონულ არქივებზე, რომელთა შორისაა IT დეპარტამენტის ზოგიერთი თანამშრომელი.

განმცხადებელი, რომელიც წლების განმავლობაში "MDK Nordrhein"-ის IT განყოფილებაში მუშაობდა, გახდა შრომისუუნარო, რის გამოც დასჭირდა ექსპერტის დასკვნის მომზადება. სპეციალიზებულმა განყოფილებამ მისი ჯანმრთელობის შესახებ ინფორმაცია შეაგროვა, მათ შორის, განმცხადებლის მკურნალი ექიმისგან, ხოლო შემდგომში კი მოითხოვა სამედიცინო ექსპერტიზის ასლები IT დეპარტამენტის კოლეგებისგან.

იქიდან გამომდინარე, რომ განმცხადებელმა თავისი სამედიცინო მონაცემების დამუშავება უკანონოდ

[4] იხ. ელექტრონული ბმული: https://www.dataguidance.com/news/eu-cjeu-issues-judgment-sensitive-data-processing-and. [24.01.2024].

მიიჩნია, მოითხოვა დამსაქმებლისგან ზიანის ანაზღაურება 20 000 ევროს ოდენობით.

განმცხადებელმა დიუსელდორფის შრომითი დავების განმხილველ სასამართლოს მიმართა პერსონალური მონაცემების უკანონო დამუშავების გამო კომპენსაცია მოთხოვნის დაკმაყოფილების მიზნით. მას მიაჩნდა, რომ ექსპერტიზა სხვა ორგანიზაციის მიერ უნდა განხორციელებულიყო, რათა მის ყოფილ კოლეგებს სამედიცინო მონაცემებზე წვდომა არ ჰქონოდათ. ამასთან, მიიჩნევდა, არადამაკმაყოფილებელი იყო უსაფრთხოების ზომები სამედიცინო დასკვნების არქივთან მიმართებით.

ფოტო: flaticon.com

აღნიშნულ საკითხთან დაკავშირებით, CJEU-მ ხაზი გაუსვა, რომ განსაკუთრებული კატეგორიის მონაცემების დასამუშავებლად უნდა არსებობდეს „GDPR“-ის მე-6 და მე-9 მუხლებით განსაზღვრული შესაბამისი სამართლებრივი საფუძველი. სასამართლომ, ასევე, განმარტა, რომ განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების შეზღუდვები, GDPR-ის 9.2(თ) მუხლის თანახმად, არ ვრცელდება იმ შემთხვევაში, თუ დამუშავება აუცილებელია პრევენციული მედიცინის ან შრომითი უსაფრთხოების მიზნებიდან გამომდინარე — კერძოდ, დასაქმებულის სამუშაო შესაძლებლობების შესაფასებლად, სამედიცინო დიაგნოზის დასასმელად, ჯანდაცვის ან სოციალური დაცვის უზრუნველსაყოფად, ჯანდაცვისა და სოციალური უზრუნველყოფის სფეროსა და შესაბამისი მომსახურების სამართავად და ა. შ.

CJEU-მ დაადგინა, რომ “GDPR”-ის მე-9 მუხლის მე-2 პუნქტის „თ“ ქვეპუნქტით გათვალისწინებული განსაკუთრებული კატეგორიის მონაცემის დამუშავების აკრძალვის გამონაკლისის ჩამონათვალი უნდა განიმარტოს შემდეგნაირად: აკრძალვის გამონაკლისი გამოიყენება იმ შემთხვევებში, როდესაც სამედიცინო მომსახურების ორგანო ამუშავებს მონაცემებს მისი ერთ-ერთი თანამშრომლის ჯანმრთელობის შესახებ, არა როგორც დამსაქმებელი, არამედ როგორც სამედიცინო მომსახურების მიმწოდებელი ორგანო. ბუნებრივია, იმ პირობით, რომ დამუშავება აკმაყოფილებდეს “GDPR”-ის 9(2)(თ) მუხლით დადგენილ მოთხოვნებს; მათ შორის, აუცილებელია, რომ მონაცემები მუშავდებოდეს იმ პირის მიერ ან მისი ზედამხედველობით, რომელსაც აქვს პროფესიული საიდუმლოს შენახვის

ვალდებულება ევროკავშირის ან წევრი სახელმწიფოს კანონის ან კომპეტენტური ეროვნული უწყების მიერ დადგენილი წესების თანახმად; ან სხვა პირის მიერ, რომელსაც აქვს კონფიდენციალობის ვალდებულება ევროკავშირის ან წევრი სახელმწიფოს კანონის ან კომპეტენტური ეროვნული უწყებების მიერ დადგენილი წესების თანახმად. CJEU-მ ასევე განმარტა, რომ GDPR-ის 9 (3) მუხლი თავისთავად არ ავალდებულებს დამმუშავებელს, დააწესოს კონკრეტული შეზღუდვები კოლეგების ჯანმრთელობის მონაცემებზე წვდომის შესახებ.

✅ CJEU-მ, ასევე, განმარტა, რომ GDPR-ის 9 (2) „თ“ ქვეპუნქტის თანახმად, ჯანმრთელობის შესახებ მონაცემების დამუშავება უნდა შეესაბამებოდეს არა მხოლოდ ამავე მუხლით დადგენილ მოთხოვნებს, არამედ მონაცემთა დამუშავების კანონიერების ერთ-ერთ საფუძველს, რომელიც განსაზღვრულია GDPR-ის მე-6 მუხლის პირველი პუნქტით.[5]

✅ რაც შეეხება კომპენსაციის საკითხს, CJEU-ს მოსაზრებით, GDPR-ის 82(1) მუხლი იმგვარად უნდა განიმარტოს, რომ იგი ასრულებდეს კომპენსატორულ ფუნქციას, იქიდან გამომდინარე, რომ მოთხოვნილი ფინანსური კომპენსაცია სრულად აანაზღაურებს GDPR-ის დარღვევის შედეგად რეალურად მიყენებულ ზიანს.

საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNIL”) დასაქმებულთა მონიტორინგთან დაკავშირებით კომპანია — “AMAZON FRANCE LOGISTIQUE” 32 მილიონი ევროს ოდენობით დააჯარიმა

23.01.2024

2023 წლის 27 დეკემბერს, “CNIL”-მა თანამშრომლების საქმიანობისა და სამუშაო პროცესის მონიტორინგის ზედმეტად ინტრუზიული სისტემის შექმნისთვის კომპანია - “AMAZON FRANCE LOGISTIQUE” 32 მილიონი ევროს ოდენობით დააჯარიმა. კომპანია ასევე დაჯარიმდა ვიდეომეთვალყურეობის დროს მონაცემთა უსაფრთხოების ვალდებულების დარღვევის გამო.

ფოტო: en.wikipedia.org

📌 საქმის გარემოებები

კომპანია - “AMAZON FRANCE LOGISTIQUE” საფრანგეთში მართავს “AMAZON”-ის ჯგუფის დიდ საწყობებს, რომლებშიც იგი იღებს/ინახავს ნივთებს და შემდეგ, მომხმარებლებისთვის მიწოდების მიზნით, ამზადებს ამანათებს. საწყობის

[5] “GDPR”-ის მე-6 მუხლის პირველი პუნქტი.

თითოეულ თანამშრომელს, საკუთარი საქმიანობის წარმართვის მიზნით, ეძლევა სკანერი, რათა შეძლოს დაკისრებული ამოცანების შესრულების რეალურ დროში დოკუმენტირება (მაგალითად, თაროებზე საქონლის შენახვა, მათი აღება, გადატანა ან შეფუთვა და ა.შ.).

თანამშრომლების მიერ დასკანერებით ხორციელდებოდა მონაცემთა ჩაწერა. ისინი ინახებოდა და გამოიყენებოდა ისეთი ინდიკატორების გამოსათვლელად, რომლებიც იძლეოდა ინფორმაციას თითოეული თანამშრომლის მიერ შესრულებული სამუშაოს ხარისხის, პროდუქტიულობისა და უმოქმედობის პერიოდების შესახებ.

კომპანიის ზემოაღნიშნული პრაქტიკის თაობაზე პრესაში გამოქვეყნებული სტატიების საფუძველზე "CNIL"-მა რამდენიმე შემოწმება ჩაატარა. საზედამხედველო ორგანომ ასევე მიიღო კომპანიის თანამშრომლების რამდენიმე საჩივარი.

📌 სკანერების გამოყენებით თანამშრომელთა მონიტორინგთან დაკავშირებით გამოვლენილი სამართალდარღვევები

! *საწყობის მარაგისა და შეკვეთის მართვასთან დაკავშირებული დარღვევები*

საწყობებში მარაგებისა და შეკვეთების რეალურ დროში მართვის მიზნით, კომპანია იყენებდა პერსონალის აქტივობისა და შესრულებული სამუშაოს შეფასების ინდიკატორებს, რომლებიც სკანერების საშუალებით გროვდებოდა.

1 მონაცემთა მინიმიზაციის პრინციპის დარღვევა[6]

მარაგებისა და შეკვეთების მართვის პროცესი იყოფოდა რამდენიმე ამოცანად (საქონლის მიღება, ინვენტარის შენახვა, შეკვეთების მომზადება და გაგზავნა) და დამოკიდებული იყო თითოეული თანამშრომლის მენეჯმენტზე, რათა, საჭიროების შემთხვევაში, მომხდარიყო დავალებების შესრულების დროს მათთვის დახმარების გაწევა ან სხვა ამოცანების დაკისრება.

თუმცა, "CNIL"-მა მიიჩნია, რომ თანამშრომლისთვის დახმარების გაწევა ან რეალურ დროში მათი სხვა დავალებებზე გადანაწილება არ მოითხოვდა წვდომას ბოლო თვის განმავლობაში თანამშრომლის მიერ შესრულებული სამუშაოს ხარისხისა და პროდუქტიულობის მაჩვენებლების ყველა დეტალის შესახებ სკანერების მეშვეობით შეგროვებულ ინფორმაციაზე. "CNIL"-მა აღნიშნა, რომ ხელმძღვანელებს შეეძლოთ, დაყრდნობოდნენ რეალურ დროში მიწოდებულ მონაცემებს, რათა გამოევლინათ თანამშრომლის წინაშე არსებული ნებისმიერი სირთულე ან მოეხდინათ იმ თანამშრომელთა იდენტიფიცირება, რომლებიც გადაყვანილნი იქნებოდნენ კონკრეტულ დავალებებზე. სწორედ ამიტომ, "CNIL"-მა მიიჩნია, რომ რეალურ დროში მიღებული მონაცემებთან ერთად შეგროვებული

[6] მონაცემთა დაცვის ძირითადი რეგულაციის ("GDPR") მე-5 მუხლის პირველი პუნქტის "c" ქვეპუნქტი.

ინფორმაციის მიღება, მაგალითად, ყოველკვირეულად, საკმარისი იქნებოდა.

ფოტო: freepik.com

2 მონაცემთა დამუშავების კანონიერების დარღვევა[7]

"CNIL"-მა დაადგინა, რომ არაკანონიერი იყო კომპანიის მიერ შემდეგი სამი მაჩვენებლის დამუშავება:

- ☑ ინდიკატორი — *"Stow Machine Gun"*, რომელიც მიუთითებდა შეცდომის შესახებ, როდესაც თანამშრომელი ნივთს „ძალიან სწრაფად" ასკანერებდა (ანუ, წინა ნივთის სკანირებიდან 1,25 წამზე ნაკლებ დროში);
- ☑ ინდიკატორი — *"idle time"*, რომელიც მიუთითებდა სკანერის ათი წუთით ან მეტი დროით უმოქმედობაზე;
- ☑ ინდიკატორი — *"latency under ten minutes"*, რომელიც აჩვენებდა სკანერის შეფერხების პერიოდებზე ერთიდან ათ წუთამდე.

"CNIL"-მა მიუთითა, რომ ზემოაღნიშნული სამი ინდიკატორის დამუშავება არ შეიძლება დაფუძნებული ყოფილიყო ლეგიტიმურ ინტერესზე, რადგან აღნიშნულმა გამოიწვია თანამშრომელთა გადაჭარბებული მონიტორინგი.

ერთი მხრივ, *"Stow Machine Gun"* ინდიკატორის დამუშავება გულისხმობდა, რომ თანამშრომლის მიერ შესრულებული ნებისმიერი ოპერაციის (კერძოდ, შენახვა) მუდმივი მონიტორინგი ხორციელდებოდა და შეცდომა დაკავშირებული შეიძლება ყოფილიყო თანამშრომლის მიერ პროცესის სწრაფად დასრულებასთან.

მეორე მხრივ, *"idle time"* და *"latency under ten minutes"* ინდიკატორების მეშვეობით შესაძლებელი იყო მუდმივი მონიტორინგი ნებისმიერ დროს, როდესაც თანამშრომლის მიერ სკანერის გამოყენება ჩერდებოდა უშუალოდ დავალების შესრულების პერიოდში, თუნდაც ძალიან მოკლე დროით (ათ წუთზე ნაკლები ან ათ წუთზე მეტი ვადით).

"CNIL"-მა აღნიშნა, რომ კომპანიას თავისი მიზნების მიღწევისთვის (საწყობებში ხარისხისა და უსაფრთხოების უზრუნველყოფა) უკვე ჰქონდა რეალურ დროში წვდომა, როგორც ინდივიდუალურ, ისევე აგრეგირებულ უამრავ ინდიკატორზე. საზედამხედველო ორგანომ ასევე აღნიშნა, რომ *"idle time"* და *"latency under ten minutes"* ინდიკატორების დამუშავება ნიშნავდა, რომ თანამშრომელს, ნებისმიერ დროს, პოტენციურად მოეთხოვებოდა სკანერის გამოყენების თუნდაც მცირე ხნით შეწყვეტის დასაბუთება. აღნიშნულის გათვალისწინებით, "CNIL"-მა დაასკვნა, რომ მონაცემთა დამუშავება გადაჭარბებულ ჩარევას იწვევდა.

[7] "GDPR"-ის მე-6 მუხლი.

! *სამუშაო გრაფიკთან და თანამშრომელთა შეფასებასთან დაკავშირებული დარღვევები*

კომპანია თავის საწყობებში სამუშაოების დასაგეგმად და ყოველკვირეულად თანამშრომელთა შესაფასებლად/გადასამ-ზადებლად იყენებდა თანამშრომლების აქტივობისა და სამუშაოს შესრულების შესახებ მონაცემებს, ასევე, სკანერების მეშვეობით შეგროვებულ ინდიკატორებს.

ფოტო: freepik.com

1 მონაცემთა მინიმიზაციის პრინციპის დარღვევა[8]

"CNIL"-მა მიიჩნია, რომ საწყობების სამუშაო განრიგის დაგეგმვა, თანამშრომელთა შეფასება და მათი გადამზადება, არ საჭიროებდა ბოლო თვის განმავლობაში თანამშრომლის მიერ სკანერის გამოყენების თითოეულ მონაცემსა და სტატისტიკურ ინდიკატორებზე კომპანიის მხრიდან წვდომას.

"CNIL"-მა აღნიშნა, რომ სტატისტიკა ერთ თანამშრომელზე, მაგალითად, ერთი კვირის განმავლობაში, საკმარისი იყო თანამშრომლის მიერ დავალების შესრულების ხარისხის შესაფასებლად და შესაბამისი ჯგუფების დასაკომ-პლექტებლად. ანალოგიურად, ასეთი სტატისტიკა თანამშრომლის მიერ სამუშაოს შესრულების შესახებ ინფორმაციული იყო და საკმარისი იყო ტრენინგის საჭიროებების შესაფასებლად/გამოსავლენად ან თანამშრომლის პროგრესის მონიტორინგისთვის.

ზემოაღნიშნულის გათვალისწინებით, "CNIL"-მა დაადგინა, რომ თანამშრომელთა ფაქტობრივი მუშაობის მონიტორინგის, ასევე, მათი შეფასების ან სწავლების მიზანი არ ამართლებდა სკანერის ათ წუთზე მეტი დროის უმოქმედობის დაფიქსირებას.

2 ინფორმაციის მიწოდების ვალდებულებისა და გამჭვირვალობის დარღვევა[9]

"CNIL"-მა დაადგინა, რომ 2020 წლის აპრილამდე კომპანიის დროებითი თანამშრომლები არ იყვნენ სათანადოდ ინფორმირებულნი, რადგან კომპანიამ სკანერების გამოყენებით მათი პირადი მონაცემების შეგროვებამდე არ უზრუნველყო კონფიდენციალურობის პოლიტიკის მიწოდება.

📌 ვიდეომეთვალყურეობასთან დაკავშირებით გამოვლენილი დარღვევები

[8] "GDPR"-ის მე-5 მუხლის პირველი პუნქტის "c" ქვეპუნქტი.

[9] "GDPR"-ის მე-12 და მე-13 მუხლები.

1 ინფორმაციის მიწოდების ვალდებულებისა და გამჭვირვალობის დარღვევა[10]

“CNIL”-მა აღნიშნა, რომ არც თანამშრომლები და არც გარე ვიზიტორები იყვნენ სათანადოდ ინფორმირებულნი ვიდეოთვალთვალის სისტემების შესახებ, ვინაიდან GDPR-ის მე-13 მუხლით მოთხოვნილი ზოგიერთი ინფორმაცია არ იყო განთავსებული საინფორმაციო დაფებსა თუ ინფორმაციის საშუალებებსა და დოკუმენტაციაში.

ფოტო: freepik.com

2 პერსონალური მონაცემების უსაფრთხოების ვალდებულების დარღვევა[11]

“CNIL”-მა აღნიშნა, რომ ვიდეოთვალთვალის პროგრამულ უზრუნველყოფაზე წვდომის დროს არ იყო დაცული უსაფრთხოების გარანტიები, ვინაიდან წვდომის პაროლი არ იყო საკმარისად ძლიერი და ანგარიშზე წვდომა რამდენიმე მომხმარებელს ჰქონდა. უსაფრთხოების აღნიშნული ხარვეზები ართულებდა ვიდეო სურათებზე წვდომასა და თითოეული პირის იდენტიფიცირებას, რომელიც ახორციელებდა პროგრამულ უზრუნველყოფასთან დაკავშირებულ მოქმედებებს.

ფოტო: immoweek.fr

📌 “CNIL”-ის ძირითადი დასკვნები

“CNIL”-მა მიიჩნია, რომ თანამშრომელთა საქმიანობისა და სამუშაო პროცესის მონიტორინგის სისტემა ითვალისწინებდა ზედმეტ ჩარევას, განსაკუთრებით შემდეგი გარემოებების გამო:

- ☑ კომპანიამ დანერგა ინდიკატორები, რომლითაც მოწმდებოდა თანამშრომელთა მიერ სკანერების გამოყენების შეჩერების დრო. “CNIL”-მა დაადგინა, რომ არაკანონიერი იყო სამუშაო პროცესის ნებისმიერი წყვეტის გაზომვის ისეთი ზუსტი სისტემის შექმნა, რომელიც თანამშრომლების მხრიდან პოტენციურად მოითხოვდა ყოველი შესვენების ან სამუშაოს სხვაგვარი შეჩერების გამართლებას;
- ☑ “CNIL”-მა დაადგინა, რომ ნივთების სკანირების სიჩქარის გაზომვის სისტემა გადაჭარბებული იყო. იმ

[10] “GDPR”-ის მე-12 და მე-13 მუხლები.

[11] “GDPR”-ის 32-ე მუხლი.

პრინციპზე დაყრდნობით, რომ ნივთების ძალიან სწრაფად სკანირება ზრდიდა შეცდომის რისკს, ინდიკატორი ზომავდა, განხორციელდა თუ არა ნივთის დასკანერება წინა ნივთის სკანირებიდან 1,25 წამზე ნაკლებ დროში;

- ☑ "CNIL"-მა, ასევე გადაჭარბებულად მიიჩნია თითოეული თანამშრომლისა და დროებით დასაქმებული პირის შესახებ სისტემის მიერ შეგროვებული ყველა მონაცემისა და სტატისტიკური ინდიკატორის 31 დღის განმავლობაში შენახვა.

"CNIL"-ს ეჭვქვეშ არ დაუყენებია ის ფაქტი, რომ ძალიან მძიმე შეზღუდვები, რომლებიც თან ახლდა "Amazon"-ის საქმიანობას და მიზნები, რომლებიც კომპანიამ თავად დააწესა, შესაძლოა, ამართლებდა სკანერის სისტემას, რომელიც კომპანიის ბიზნესის მართვისთვის შეიქმნა. თუმცა, საზედამხედველო ორგანომ მიიჩნია, რომ ყველა ამ მონაცემისა და შედეგად მიღებული სტატისტიკური მაჩვენებლების თაობაზე ინფორმაციის შენახვა მთლიანობაში არაპროპორციული იყო.

შედეგად, კომპანიას ჯარიმის სახით 32 მილიონი ევრო დაეკისრა. ჯარიმის ოდენობის გამოთვლისას "CNIL"-მა გაითვალისწინა ის ფაქტი, რომ თანამშრომლების მონაცემების დამუშავება სკანერების გამოყენებით განსხვავდებოდა აქტივობების მონიტორინგის ტრადიციული მეთოდებისგან, მათი განხორციელების მასშტაბით და იწვევდა თანამშრომლების მუშაობის ზუსტ და დეტალურ მონიტორინგს.

აღნიშნული სისტემები, თანამშრომლების მიერ სკანერების მეშვეობით, თითოეული დავალების შესრულების პროცესზე ზუსტ მეთვალყურეობას ახორციელებდა და მათ მუდმივი ზეწოლის ქვეშ აქცევდა. "CNIL"-მა, ასევე, გაითვალისწინა დასაქმებულთა დიდი რაოდენობა (რამდენიმე ათასი) და მიიჩნია, რომ კომპიუტერული მონიტორინგის საშუალებით თანამშრომლებზე დაწესებული შეზღუდვები პირდაპირ უწყობდა ხელს კომპანიის ეკონომიკურ მოგებას და ანიჭებდა მას კონკურენტულ უპირატესობას ონლაინ გაყიდვების ბაზარზე მოქმედ სხვა კომპანიებთან შედარებით.[12]

[12] იხ. ელექტრონული ბმული: <https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million>.

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