მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

ნიდერლანდების სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება კომპანია “Netflix”-ის დაჯარიმების შესახებ

რუმინეთის საზედამხედველო ორგანოს გადაწყვეტილება საზოგადოებრივი სატრანსპორტო კომპანიის მიერ პერსონალურ მონაცემთა დამუშავების

გადაწყვეტილება ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მონაცემთა უსაფრთხოების დარღვევასთან დაკავშირებით

მონაცემთა უსაფრთხოების დარღვევა გავრცელდა უნივერსიტეტის ექვსი თანამშრომლის სამსახურებრივ ელექტრონული ფოსტის ანგარიშებზე. არაავტორიზებულმა პირებმა ანგარიშები გამოიყენეს უკანონოდ და არამართლზომიერად, თაღლითობის ჩადენის მიზნით. დანაშაულებრივი ქმედების შედეგად მატერიალური ზიანი განიცადა მონაცემთა ერთმა სუბიექტმა.

თებერვალი 2025

2024 წლის 6 დეკემბერს, ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ გამოაქვეყნა გადაწყვეტილება მონაცემთა უსაფრთხოების დარღვევის შესახებ. საზედამხედველო ორგანომ აღნიშნული საქმის შესწავლა 2019 წლის ივლისში, საკუთარი ინიციატივის საფუძველზე დაიწყო, რასაც წინ უსწრებდა 2018 წლის ნოემბერში ერთ-ერთი უნივერსიტეტის (“Maynooth University”) მიმართვა საზედამხედველო ორგანოსადმი პერსონალურ მონაცემთა უსაფრთხოების დარღვევასთან, კერძოდ, კიბერთაღლითობის გავრცელებულ ფორმასთან, „ფიშინგთან“ დაკავშირებით.

საქმის ფაქტობრივი გარემოებები:
მონაცემთა უსაფრთხოების დარღვევა გავრცელდა უნივერსიტეტის ექვსი თანამშრომლის სამსახურებრივ ელექტრონული ფოსტის ანგარიშებზე. არაავტორიზებულმა პირებმა ანგარიშები გამოიყენეს უკანონოდ და არამართლზომიერად, თაღლითობის ჩადენის მიზნით. დანაშაულებრივი ქმედების შედეგად მატერიალური ზიანი განიცადა მონაცემთა ერთმა სუბიექტმა.

საზედამხედველო ორგანოს გადაწყვეტილება:
საზედამხედველო ორგანომ შეაფასა უნივერსიტეტის მიერ პერსონალურ მონაცემთა დამუშავებისას მონაცემთა უსაფრთხოების უზრუნველსაყოფად გატარებული ტექნიკური და ორგანიზაციული ზომები. შესწავლილ იქნა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა უსაფრთხოების დარღვევის შესახებ დროული შეტყობინების ვალდებულების საკითხიც.

საზედამხედველო ორგანოს გადაწყვეტილების თანახმად, დადგინდა შემდეგი დარღვევები:

- ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 32-ე და 5(1)(ფ) მუხლების დარღვევა, პერსონალურ მონაცემთა დამუშავებისას სათანადო ტექნიკური და ორგანიზაციული ზომების გაუტარებლობის შესახებ მონაცემთა უსაფრთხოების უზრუნველსაყოფად;
- ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 33(1) მუხლის დარღვევა, საზედამხედველო ორგანოსათვის მონაცემთა უსაფრთხოების ხელყოფის შესახებ 72 საათის განმავლობაში შეუტყობინებლობა.

საზედამხედველო ორგანომ აღნიშნულ დარღვევებთან დაკავშირებით უნივერსიტეტს შენიშვნა გამოუცხადა, აგრეთვე, დააკისრა ადმინისტრაციული ჯარიმა 40 000 ევროს ოდენობით და დაავალა მონაცემთა დამუშავების მოქმედებების „მონაცემთა დაცვის ძირითად რეგულაციასთან“ შესაბამისობაში მოყვანა. საზედამხედველო ორგანომ ხაზგასმით აღნიშნა ინფორმაციის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებთან შესაბამისად დამუშავების საჭიროება და მონაცემთა შესაბამისი უსაფრთხოების წესების გათვალისწინებისა და სათანადო ტექნიკური და ორგანიზაციული ღონისძიებების გატარების ვალდებულება. ამავდროულად აღინიშნა, რომ ინციდენტის შესახებ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა საზედამხედველო ორგანოს უნდა შეატყობინოს დაუყოვნებლივ, მონაცემთა უსაფრთხოების დარღვევის შესახებ შესაბამისი ინფორმაციის მიღების შემდგომ.

რუმინეთის საზედამხედველო ორგანოს გადაწყვეტილება საზოგადოებრივი სატრანსპორტო კომპანიის მიერ პერსონალურ მონაცემთა დამუშავების კანონიერების შესახებ

რუმინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ საზოგადოებრივი სატრანსპორტო კომპანია “Cluj-Napoca“ აუდიო- და ვიდეო მონიტორინგის გზით დასაქმებულთა პერსონალური მონაცემების უკანონო დამუშავებისთვის 4 000 ევროს ოდენობით დააჯარიმა.

საქმის ფაქტობრივი გარემოებები:
რუმინეთის პერსონალურ მონაცემთა საზედამხედველო ორგანომ, მიღებული შეტყობინების საფუძველზე, სატრანსპორტო კომპანიის მიერ პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლა დაიწყო. საკითხის შესწავლისას დადგინდა, რომ კომპანიის ოპერატორი წლების განმავლობაში უკანონოდ ამუშავებდა მძღოლების პერსონალურ მონაცემებს - გამოსახულებასა და ხმას. მონაცემთა დამუშავება სატრანსპორტო კომპანიის მძღოლის კაბინაში დამონტაჟებული აუდიო- და ვიდეო სათვალთვალო სისტემის მეშვეობით ხორციელდებოდა. აღსანიშნავია, რომ ზოგიერთ შემთხვევაში, კომპანია აუდიო- და ვიდეომონიტორინგის გზით შეგროვებულ ინფორმაციას დასაქმებულებისათვის დისციპლინური პასუხისმგებლობის დაკისრებისათვის იყენებდა.

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილების დასაბუთება:
რუმინეთის პერსონალურ მონაცემთა საზედამხედველო ორგანომ დაადგინა, რომ კომპანიის მიერ დასაქმებულთა პერსონალური მონაცემების დამუშავების პროცესი ეწინააღმდეგებოდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ (“GDPR”) გათვალისწინებულ მონაცემთა დამუშავების კანონიერების, სამართლიანობის, მიზნით შეზღუდვისა და მონაცემთა მინიმიზაციის პრინციპებს.

ამავდროულად, საზედამხედველო ორგანომ აღნიშნა, რომ სატრანსპორტო საშუალებაში აუდიო- და ვიდეოჩამწერი მოწყობილობით, მძღოლების პერსონალური მონაცემების შეგროვების გარდა, სხვა მონაცემთა სუბიექტების — მგზავრების პერსონალური მონაცემებიც მუშავდებოდა. აღნიშნული მათი პერსონალური მონაცემების უკანონო დამუშავებად შეფასდა, ვიანიდან მძღოლთა აუდიო- და ვიდეომონიტორინგის ფარგლებში, მგზავრთა გამოსახულებისა და ხმის ჩაწერაც ხორციელდებოდა.

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება:
რუმინეთის პერსონალურ მონაცემთა საზედამხედველო ორგანომ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-5 მუხლი პირველი ნაწილის ა, ბ, გ, ქვეპუნქტების, ამავე მუხლის მე-2 ნაწილისა და მე-6 მუხლის დარღვევა დაადგინა. აღნიშნულიდან გამომდინარე, სატრანსპორტო კომპანია 4 000 ევროს ოდენობით დაჯარიმდა.

დამატებით, საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა დამუშავების არსებული პრაქტიკის შეფასება დაავალა. ასევე, ხაზგასმით აღინიშნა მძღოლების სალონში აუდიო და ვიდეო სათვალთვალო კამერების გამოყენების მონაცემთა დამუშავების საერთაშორისო და ეროვნული კანონმდებლობის სამართლებრივ პრინციპებთან შესაბამისობის უზრუნველსაყოფად.

ნიდერლანდების სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება კომპანია “Netflix“-ის დაჯარიმების შესახებ

2024 წლის 18 დეკემბერს, ნიდერლანდების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ევროკავშირის „მონაცემთა დაცვის რეგულაციის“ (“GDPR”) დარღვევისათვის კომპანია “Netflix” 4,75 მილიონი ევროს ოდენობით დააჯარიმა.

საქმის ფაქტობრივი გარემოებები:
“Netflix” ამერიკული კომპანიაა, რომელიც სხვადასხვა სახის პერსონალურ მონაცემებს ამუშავებს, მათ შორის, მომხმარებელთა პირად ინფორმაციას, ელექტრონული ფოსტის მისამართებს, ტელეფონის ნომრებსა, მომხმარებელთა გადასახადებთან დაკავშირებულ მონაცემს.

ნიდერლანდების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ საქმის შესწავლა ორგანიზაცია “None of Your Business”-ის (“NOYB”) საჩივრის საფუძველზე დაიწყო. თავდაპირველად საჩივარი წარედგინა ავსტრიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს. თუმცა, ევროკავშირის „მონაცემთა დაცვის რეგულაციის“ მიხედვით კომპანიები, რომლებიც მონაცემებს ევროკავშირის წევრ სხვადასხვა ქვეყანაში ამუშავებენ, ექვემდებარებიან იმ სახელმწიფოს იურისდიქციას, სადაც კომპანია არის დაარსებული. შესაბამისად, საქმის შესწავლა ნიდერლანდების საზედამხედველო ორგანომ დაიწყო, ვინაიდან “Netflix”-ის ევროპის სათაო ოფისი ამსტერდამში მდებარეობს,.

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილების დასაბუთება:
ნიდერლანდების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ კომპანია “Netflix”-ის კონფიდენციალობის პოლიტიკა მონაცემთა დაცვის კანონმდებლობასთან შეუსაბამო იყო, ვინაიდან დამუშავებისთვის პასუხისმგებელ პირი მომხმარებლებს არ აწვდიდა მკაფიო და გასაგებ ინფორმაციას მონაცემთა შეგროვების, გამოყენების მიზნებისა და სამართლებრივი საფუძვლების შესახებ. ასევე, კონფიდენციალობის პოლიტიკა არ შეიცავდა სათანადო ინფორმაციას ევროკავშირის ფარგლებს გარეთ მონაცემთა გადაცემის შესახებ, მათ შორის პერსონალური მონაცემების უსაფრთხოების ზომებთან დაკავშირებით.

აღსანიშნავია, რომ “Netflix”-მა ვერ შეძლო დაეკონკრეტებინა, თუ რა კატეგორიის მონაცემი გადაეცემოდა მესამე მხარეს და რა საფუძვლით. “Netflix”-მა საზედამხედველო ორგანოს ასევე ვერ მიაწოდა დასაბუთებული ინფორმაცია მომხმარებელთა მონაცემების შენახვის ვადასთან დაკავშირებით. ამასთან, ბუნდოვანი იყო კომპანიის მიერ მონაცემთა შენახვის ვადის განსაზღვრის კრიტერიუმები.

დამატებით, კომპანიამ, მონაცემთა სუბიექტების მოთხოვნათა მიუხედავად, არ გასცა ინფორმაცია, იმ მონაცემების შესახებ, რომლებსაც იგი ამუშავებდა. აღნიშნულის გათვალისწინებით, დაირღვა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ განსაზღვრული, მონაცემთა სუბიექტის უფლებები.

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება:
ნიდერლანდების სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-5 მუხლის დარღვევა და კომპანია 4,75 მილიონი ევროს ოდენობით დააჯარიმა. ადმინისტრაციული ჯარიმის ოდენობის განსაზღვრისას, საზედამხედველო ორგანომ მხედველობაში მიიღო, როგორც დარღვევის სიმძიმე, ასევე კომპანიის წლიური შემოსავალი.

ნიდერლანდების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს თავმჯდომარემ, ალეიდ ვოლფსენმა ხაზგასმით აღნიშნა გამჭვირვალობის მნიშვნელობა ისეთი დიდი კომპანიების მიერ მონაცემთა დამუშავების პროცესში, როგორიცაა “Netflix”.

საზედამხედველო ორგანოს გადაწყვეტილების შესაბამისად, “Netflix”-მა გაანახლა კონფიდენციალობის პოლიტიკა და გააუმჯობესა მონაცემთა სუბიექტებისთვის ინფორმაციის მიწოდების არხები. მიუხედავად კომპანიის მიერ განხორციელებული ცვლილებებისა, დამუშავებისთვის პასუხისმგებელმა პირმა კანონით დადგენილი წესით გაასაჩივრა საზედამხედველო ორგანოს გადაწყვეტილება ჯარიმის ოდენობის შემცირების მოთხოვნით.

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს რეკომენდაცია საზოგადოებრივი ინტერესის მქონე საჯარო ინფორმაციის პროაქტიული გამოქვეყნების შესახებ

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ, 2024 წლის 16 დეკემბერს, გამოაქვეყნა რეკომენდაცია წყალმომარაგების კომპანიების მიმართ, რაც წყალმომარაგებასთან დაკავშირებული სამუშაოების შესახებ საზოგადოებრივი ინტერესის მქონე საჯარო ინფორმაციის პროაქტიული გამოქვეყნების დასაშვებობას გულისხმობს.

საზედამხედველო ორგანოს რეკომენდაცია დაეფუძნა მონაცემთა სუბიექტების არაერთ განცხადებას საზოგადოებრივი ინტერესის მქონე საჯარო ინფორმაციის გამჭვირვალობის თაობაზე. მოქმედი წესის თანახმად, აღნიშნული ინფორმაციის მიწოდება კომპანიებს ევალებათ მომხმარებლის მოთხოვნის ან გარემოსდაცვითი რეგულაციების შესაძლო დარღვევის თავიდან ასაცილებლად, თუმცა საზედამხედველო ორგანოს რეკომენდაციით მსგავსი ინფორმაციის ყოველთვიურად გამოქვეყნება მონაცემთა გამჭვირვალობის მაღალ ხარისხს დაამკვიდრებს და წყალმომარაგების კომპანიების მიმართ მოქალაქეთა ჭარბ მიმართვიანობას შეამცირებს.

საზედამხედველო ორგანოს რეკომენდაციას მხოლოდ ორი კომპანია გამოეხმაურა და უზრუნველყვეს ინფორმაციის პროაქტიული გამოქვეყნება, რაც მოიცავს მონაცემებს სამუშაოების დაწყების, შეჩერების დროისა და ტერიტორიული არეალების შესახებ, გარემოსდაცვითი ორგანოებისთვის საჯარო შეტყობინების შესახებ. კომპანიების უმრავლესობა აღნიშნავს, რომ მითითებული ინფორმაციის გამოქვეყნება დაუშვებელია პერსონალურ მონაცემთა დაცვის ეროვნული კანონმდებლობიდან გამომდინარე, თუმცა, საზედამხედველო ორგანოს მითითებით, საზოგადოებრივი ინტერესის მქონე საჯარო ინფორმაცია უპირობოდ, არ შეიძლება განხილულ იქნეს პირადი ხასიათის პერსონალურ მონაცემად.

გაერთიანებული სამეფოს საზედამხედველო ორგანოს მიერ გამოქვეყნებული რეკომენდაცია გამოხატავს საზოგადოებრივი ინტერესის მქონე საჯარო ინფორმაციის გამჭვირვალობის განსაკუთრებულ მნიშვნელობას, რათა მომხმარებელს არ სჭირდებოდეს სატელეფონო ზარი ან ორგანოსთვის პერსონალურად მიმართვის სხვა საკომუნიკაციო საშუალება საზოგადოებრივი ინტერესის მქონე ინფორმაციის გადასამოწმებლად.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება ორგანიზაციის ყოფილი თანამშრომლის პერსონალური მონაცემების დამუშავების კანონიერების შესახებ

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) ორგანიზაციის ყოფილი თანამშრომლის სამსახურებრივი ტელეფონიდან პერსონალური მონაცემების წაშლის კანონიერების თაობაზე გადაწყვეტილება მიიღო.

საქმის ფაქტობრივი გარემოებები:
მონაცემთა სუბიექტსა და მის დამსაქმებელთან დადებული შრომითი ხელშეკრულება 2021 წლის სექტემბერს შეწყდა. შესყიდვის შეთანხმების შესაბამისად, ხელშეკრულების შეწყვეტისთანავე, ყოფილ დასაქმებულ პირს შესაძლებლობა ჰქონდა, საკუთრებაში დაეტოვებინა სამსახურებრივი ტელეფონი.

ტელეფონის გამოყენებიდან რამდენიმე თვეში, მონაცემთა სუბიექტს ტელეფონზე წვდომა შეეზღუდა და მიიღო შეტყობინება, რომელშიც მითითებული იყო, რომ მისი ტელეფონი დამუშავებისთვის პასუხისმგებელი პირის მიერ დისტანციურად მოწმდებოდა. მონაცემთა სუბიექტი დაუკავშირდა დამუშავებისთვის პასუხისმგებელ პირს, რომელმაც უთხრა, რომ ტელეფონში არსებული ინფორმაცია უნდა წაეშალა და პარამეტრები ხელახლა ჩაეწერა (“Reset”). სხვა შემთხვევაში, იგი ტელეფონით სარგებლობას ვერ შეძლებდა. მონაცემთა სუბიექტს შეთავაზებული ფუნქციის გამოყენება არ სურდა, რადგან არ უნდოდა წაშლილიყო მისი პერსონალური ინფორმაცია.

2023 წლის 13 თებერვალს, მონაცემთა სუბიექტმა დამუშავებისთვის პასუხისმგებელი პირის წინააღმდეგ ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანოში საჩივარი შეიტანა. 2024 წლის 7 ოქტომბერს, “AEPD”-მ ადმინისტრაციული წესით დაიწყო დისციპლინური სამართალწარმოება დამსაქმებლის მიმართ, რომელიც აცხადებდა, რომ, შესყიდვის ხელშეკრულების თანახმად, მას ჰქონდა უფლება მონაცემთა სუბიექტისთვის დაევალებინა მის ტელეფონში შენახული ინფორმაციის წაშლა.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება:
საზედამხედველო ორგანოს შეფასებით, მიუხედავად იმისა, რომ ტელეფონის შესყიდვის თაობაზე ხელშეკრულება დამუშავებისთვის პასუხისმგებელ პირს ანიჭებდა უფლებას, წაეშალა სამსახურებრივ საქმიანობასთან დაკავშირებული ინფორმაცია, აღნიშნული არ ვრცელდებოდა პირადი სარგებლობის ფარგლებში შეგროვებულ მონაცემებზე. ფაქტობრივი გარემოებების თანახმად კი, მონაცემთა სუბიექტის მიერ ტელეფონით სარგებლობისთვის აუცილებელი იყო ტელეფონში არსებული მონაცემების წაშლა, რომელიც, მათ შორის, მოიცავდა პირადი სარგებლობის ფარგლებში შეგროვებულ ინფორმაციას.

ამდენად, *“AEPD”*-მ დააგდინა, რომ დამუშავებისთვის პასუხისმგებელ პირს, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ *(“GDPR”)* მე-*6* მუხლის („მონაცემთა დამუშავების კანონიერება“) პირველი პუნქტის შესაბამისად, არ ჰქონდა მონაცემთა სუბიექტისთვის ტელეფონში არსებული პირადი ინფორმაციის წაშლის მოთხოვნის უფლება.
ზემოაღნიშნულის გათვალისწინებით, ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს დააკისრა ჯარიმა *120 000* ევროს ოდენობით.

საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა უკანონო შენახვის შესახებ

მიმართვის საფუძველზე საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ *(“HDPA”)* მონაცემთა სუბიექტის ყოფილი ადვოკატის მიერ მონაცემთა უკანონო შენახვის შესახებ გადაწყვეტილება მიიღო.

მონაცემთა სუბიექტი, რომელმაც საზედამხედველო ორგანოს მისი ყოფილი ადვოკატის წინააღმდეგ მიმართა, აცხადებდა, რომ სამართალწარმოების დასრულების შემდეგ, ადვოკატმა არ დააბრუნა სუბიექტის პერსონალურ მონაცემთა შემცველი დოკუმენტები, რაც წარმოადგენდა მონაცემებზე წვდომის უფლების დარღვევას, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ *(“GDPR”)* მე-*15* მუხლის თანახმად.

საქმის ფაქტობრივი გარემოებები
2019 წელს მონაცემთა სუბიექტმა პირველად მიმართა მის ყოფილ ადვოკატს სამართლებრივ საკითხებთან დაკავშირებული დოკუმენტების გამოთხოვის მოთხოვნით. მიუხედავად მრავალი შეხსენებისა, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისგან მან პასუხი ვერ მიიღო.

საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ საკითხის შესწავლის ფარგლებში, მოითხოვა წერილობითი განმარტებები მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისგან იმის შესახებ, თუ როგორ დამუშავდა მონაცემთა სუბიექტის მოთხოვნა და რატომ უგულებელყვეს განმეორებითი შეტყობინებები. დამუშავებისთვის პასუხისმგებელმა პირმა განაცხადა, რომ შესაბამისი დოკუმენტები პროკურორის მიერ დაარქივდა.

საბერძნეთის პერსონალურ მონაცემთა დაცვის ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს შეახსენა ძირითადი რეგულაციის *31*-ე მუხლიდან გამომდინარე საზედამხედველო ორგანოსთან თანამშრომლობის ვალდებულება და კიდევ ერთხელ მოითხოვა მისგან განმარტებები, რასაც რეაგირება არ მოჰყოლია.

საკითხთან დაკავშირებით 2024 წელს დაინიშნა ზეპირი მოსმენა. მონაცემთა სუბიექტი ამტკიცებდა, რომ პერსონალურ მონაცემებზე წვდომის უფლება დაირღვა, რადგან მისმა ყოფილმა ადვოკატმა ვერ უზრუნველყო დოკუმენტების დაბრუნება. სუბიექტის განმარტებით, საჩივარი შეეხებოდა არა პერსონალური მონაცემების დარღვევას, არამედ დოკუმენტების უკანონოდ შენახვას. მეორე მხრივ, დამუშავებისთვის პასუხისმგებელი პირი ამტკიცებდა, რომ დოკუმენტები აღარ იყო ხელმისაწვდომი მათთვის, რადგან ოფისშიც არ ინახებოდა. აღნიშნული დოკუმენტები კი ხელმისაწვდომი იყო სხვადასხვა წყაროდან, ისეთი, როგორიცაა: საჯარო ჩანაწერები ან სასამართლო ფაილები, რის გამოც მონაცემთა სუბიექტის მოთხოვნა უსაფუძვლო იყო.

გადაწყვეტილების დასაბუთება
საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“HDPA”) დაადგინა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია ძირითადი რეგულაციის მე-15 მუხლი, რადგან მონაცემთა სუბიექტის მოთხოვნაზე რეაგირება არ მოახდინა და არ დააბრუნა დოკუმენტაცია. გარდა ამისა, აღსანიშნავია რომ მონაცემთა სუბიექტისთვის პერსონალურ ფაილზე წვდომის უფლება, ასევე, უზრუნველყოფილია საბერძნეთის ეროვნული კანონის, მე-5 მუხლით.
საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია ძირითადი რეგულაციის 31-ე მუხლი, როდესაც უარი განაცხადა საზედამხედველო ორგანოსთან თანამშრომლობაზე და არ მიაწოდა საჭირო განმარტებები “HDPA”-სთან თანამშრომლობაზე - არ მიაწოდა საჭირო განმარტებები, მიუხედავად ორგანოს არაერთი მოთხოვნისა.

მიღებული გადაწყვეტილება
საქმის ფაქტობრივი გარემოებების შეფასების შედეგად, საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს დააკისრა ორი ადმინისტრაციული ჯარიმა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 58(2)(i) მუხლის შესაბამისად: მონაცემთა სუბიექტის ხელმისაწვდომობის უფლებების დარღვევისთვის 700 ევროს, ხოლო საზედამხედველო ორგანოსთან თანამშრომლობის ვალდებულების შეუსრულებლობისთვის - 700 ევროს ოდენობით.

სლოვენიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება თანამშრომელთა ვიდეომონიტორინგის წესების დარღვევის გამო

საქმის ფაქტობრივი გარემოებები:

2023 წელს, სლოვენიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ კომპანია “FOVELLA”-ს მიერ პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლა დაიწყო.

მონაცემთა დამუშავების კანონიერების შესწავლის შედეგად, საზედამხედველო ორგანომ დაადგინა, რომ კომპანია ახორციელებდა თანამშრომელთა უკანონო მონიტორინგს. კერძოდ, მიმდინარეობდა იმ თანამშრომელთა მუდმივი ვიდეომონიტორინგი, რომლებიც კომპანიის ერთ-ერთ ობიექტზე, რესტორნის სამზარეულოში მუშაობდნენ. სამზარეულოში დამონტაჟებული ვიდეომონიტორინგის სისტემით დამუშავებული ვიდეომასალა პირდაპირ რეჟიმში კომპანიის ვებგვერდზე იყო ხელმისაწვდომი.

შესწავლის შედეგად დადგინდა, რომ ვიდეომონიტორინგის სისტემის საშუალებით პირდაპირ რეჟიმში ტრანსლირება კომპანიის ბიზნესმოდელის ნაწილი იყო. ინსპექტირების პროცესში საზედამხედველო ორგანომ ორი დარღვევა გამოავლინა:

სამუშაო სივრცეში ვიდეომონიტორინგის სისტემის უკანონოდ განთავსება:
თანამშრომლების მონიტორინგი შეიძლება განხორციელდეს მხოლოდ გამონაკლისის სახით (ultima ratio) და იმ შემთხვევაში, თუკი აღნიშნული აბსოლუტურად აუცილებელია ფიზიკურ პირთა ან ქონების უსაფრთხოების მიზნებისათვის.

მოცემულ შემთხვევაში, დამუშავებისთვის პასუხისმგებელმა პირმა ვერ შეძლო ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ ანგარიშვალდებულების პრინციპთან შესაბამისობის დემონსტრირება[3]. კომპანიამ რესტორნის სამზარეულოს მონიტორინგი განახორციელა აუცილებელი საჭიროების გარეშე. ამავდროულად, იგი ვიდეომონიტორინგის სისტემის გამოყენებით, რესტორნის სამუშაო პროცესის პირდაპირ რეჟიმში ტრანსლირებას ახდენდა კომპანიის ვებგვერდზე (https://dodopizza.si/ljubljana), რისთვისაც აუცილებელი საჭიროება არ არსებობდა. აღსანიშნავია, რომ სლოვენიის მონაცემთა დაცვის ეროვნული კანონმდებლობა კრძალავს თანამშრომელთა სამუშაო სივრცეში ვიდეომონიტორინგის სისტემის განთავსებას. ასეთ ვითარებაში ვიდეომონიტორინგი დასაშვებია მხოლოდ გამონაკლის შემთხვევაში, თუ დასახელებული მიზნების მიღწევა სხვა საშუალებით შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან.

მონაცემთა დამუშავებისთვის ლეგიტიმური ინტერესის არარსებობა:
საზედამხედველო ორგანომ შეაფასა პირდაპირ რეჟიმში ტრანსლირების პროცესი და აღნიშნა, რომ დამუშავებისთვის პასუხისმგებელ პირს არ გააჩნდა მონაცემთა დამუშავების ლეგიტიმური ინტერესი.

საზედამხედველო ორგანოს განცხადებით, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებაა, შეაფასოს მონაცემთა დამუშავების პროცესთან დაკავშირებული ყოველი მოქმედება, კონკრეტული კონტექსტისა და მონაცემთა სუბიექტების უფლებების დაცვის პოზიციიდან. მიუხედავად რესტორნის სურვილისა, რომ ვიდეომონიტორინგის გზით გაემყარებინა მომხმარებელთა ნდობა, პირდაპირი ტრანსლირება კომპანიის კონკრეტული მიზნის გათვალისწინებით არ შეფასდა პროპორციულ საშუალებად. კერძოდ, კომპანიის მიერ მომხმარებელთა ნდობის გამყარების ინტერესი არ აჭარბებს იმ თანამშრომელთა უფლებების დაცვის ინტერესს, რომლებიც კომპანიაში მუშაობდნენ და რომელთა სამუშაო პროცესის ტრანსლირება პირდაპირ რეჟიმში ხორციელდებოდა.

მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება

რესტორნის სამზარეულოში უკანონო ვიდეომონიტორინგის წარმოებისათვის და მისი კომპანიის ვებგვერდზე სამართლებრივი საფუძვლის გარეშე ტრანსლირებისათვის საზედამხედველო ორგანომ კომპანია 25 000 ევროს ოდენობით დააჯარიმა.

დამატებით, საზედამხედველო ორგანომ კომპანიას გამოუცხადა შენიშვნა თანამშრომელთა მონაცემების დამუშავების გამო, მათი წინასწარი ინფორმირების გარეშე.

ვინაიდან კომპანია საქმიანობას ახორციელებს ევროკავშირის სხვადასხვა ქვეყანაში, სლოვენიის მონაცემთა დაცვის საზედამხედველო ორგანომ წინამდებარე საქმის შესახებ ინფორმაცია კოლეგა საზედამხედველო ორგანოებს გაუზიარა.

აღსანიშნავია, რომ საზედამხედველო ორგანოს ინსპექტირების შედეგად მიღებული გადაწყვეტილება საბოლოოა და იგი არ ექვემდებარება გასაჩივრებას.

ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება აგდერის უნივერსიტეტის დაჯარიმების შესახებ

ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ აგდერის უნივერსიტეტი დააჯარიმა თანამშრომელთა მიერ ინფორმაციაზე წვდომის შეზღუდვის ვალდებულებისა და მონაცემთა უსაფრთხოების წესების დაუცველობისათვის.

დაჯარიმების საფუძველი:
2024 წლის თებერვალში, აგდერის უნივერსიტეტის თანამშრომელმა აღმოაჩინა, რომ სისტემატურად ირღვეოდა პერსონალურ მონაცემთა შემცველი დოკუმენტების შენახვის წესი. პერსონალურ მონაცემთა შემცველი დოკუმენტები “Microsoft Teams”-ის პლატფორმაზე (საქაღალდეებში) ინახებოდა და მასზე წვდომა განურჩევლად საჭიროებისა. ყველა თანამშრომელს ჰქონდა.[1] მონაცემთა უსაფრთხოების დარღვევა იყო დენადი ხასიათის, 2018 წლის აგვისტოდან მოყოლებული (როდესაც უნივერსიტეტის თანამშრომლებმა პროგრამა Microsoft Teams-ის გამოყენება დაიწყეს) 2024 წლის თებერვლამდე პერიოდს მოიცავდა.

საზედამხედველო ორგანოს მთავარი მიგნებები:
2018 წლის აგვისტოდან 2024 წლის თებერვლამდე, თანამშრომელთათვის “Microsoft Teams”-ის სისტემაში, კერძოდ, საქაღალდეებში, თანამშრომლების, სტუდენტების და გარეშე პირების პერსონალური მონაცემების შემცველი ინფორმაცია ღიად იყო ხელმისაწვდომი, და თანამშრომლებს მასზე წვდომა მარტივად, პროგრამა “Microsoft Teams”-ის საქაღალდეებში საძიებო ფუნქციის გამოყენებით ჰქონდათ.

ინფორმაციული უსაფრთხოების აღნიშნული დარღვევა შეეხო 16 000 მონაცემთა სუბიექტის პერსონალურ მონაცემებს, კერძოდ: სახელებს, საიდენტიფიკაციო ნომრებს, სხვადასხვა სტუდენტის საჭიროებაზე მორგებული (ადაპტირებული) გამოცდების შესახებ ინფორმაციას; ინფორმაციას დამატებით გამოცდაზე სტუდენტის გასვლის შესახებ და რა სპეციალური ღონისძიებები ან/და მოწყობილობები იქნა გამოყენებული გამოცდის პროცესში ზოგიერთი სტუდენტის განსაკუთრებული საჭიროებების დაკმაყოფილებისათვის.

მონაცემთა უსაფრთხოების დარღვევა შეეხოთ ასევე უნივერსიტეტთან ასოცირებული, ლტოლვილის სტატუსის მქონე პირების შესახებ ინფორმაციასაც, რაც მოიცავდა მათ საკონტაქტო ინფორმაციას, ასევე, მონაცემებს მათი განათლების და ნორვეგიაში ცხოვრების უფლების შესახებ.

მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება:
ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ დარღვევის გამო, კერძოდ, პერსონალურ მონაცემთა უსაფრთხოების ზომების დაუცველობისათვის, ნორვეგიის მონაცემთა დაცვის საზედამხედველო ორგანომ მიიღო გადაწყვეტილება აგდერის უნივერსიტეტის 12 700 ევროს ოდენობით დაჯარიმების შესახებ.

საზედამხედველო ორგანოს შეფასების თანახმად, უნივერსიტეტს ჰქონდა ვალდებულება დაეცვა პერსონალურ მონაცემთა შემცველი ინფორმაციის უსაფრთხოება, კერძოდ, უზრუნველეყო მისი დაცვა არაავტორიზებული წვდომისაგან. აღნიშნულ ინფორმაციაზე წვდომის განხორციელება შესაძლებელი უნდა ყოფილიყო მხოლოდ იმ თანამშრომლებისათვის, რომელთაც ეს აუცილებლად სჭირდებოდათ მათზე დაკისრეული სამუშაოს შესასრულებლად. თანამშრომლებს უნდა ჰქონოდათ წვდომა ინფორმაციაზე მხოლოდ იმ მოცულობით, რაც აუცილებელი იყო მათზე დაკისრებული კონკრეტული სამუშაოს შესრულებისთვის, მონაცემთა მინიმიზაციის პრინციპის გათვალისწინებით.

ევროპის მონაცემთა დაცვის საბჭოს („EDPB”) გზამკვლევის პროექტი „მონაცემთა დამუშავების ლეგიტიმურ ინტერესის შესახებ“

2024 წლის 7 ოქტომბერს „ევროპის მონაცემთა დაცვის საბჭომ“ გამოსცა რეკომენდაციის პროექტი[1] მონაცემთა დამუშავების ლეგიტიმურ ინტერესთან დაკავშირებით.
პროექტის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ მონაცემთა კანონიერების ფარგლებში, დასამუშავებლად აუცილებელია შესაბამისი სამართლებრივი საფუძველის არსებობა. ლეგიტიმური ინტერესი კი ერთ-ერთ სამართლებრივ საფუძველს წარმოადგენს. შესაბამისად, გზამკვლევის პროექტი ეხება დამუშავებისთვის პასუხისმგებელ პირების მიერ ლეგიტიმური ინტერესის საფუძველზე მონაცემთა დამუშავებას.

ინტერესის ლეგიტიმურობის შესახებ:
ლეგიტიმურად შესაძლოა მიჩნეულ იქნას მხოლოდ კანონიერი ინტერესი, რომელიც ჩამოყალიბებულია ნათლად და გარკვევით, არის რეალური და ამჟამინდელი, რეალურ დროში არსებული. მაგალითად, კომპანიას, რომელიც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირია და მონაცემთა სუბიექტს მომსახურებას უწევს შესაძლოა ჰქონდეს მონაცემთა სუბიექტის პერსონალური მონაცემების დამუშავების ლეგიტიმური ინტერესი.

მონაცემთა დამუშავების „აუცილებლობის“ სტანდარტი:
თუ მონაცემთა დამუშავების მიზნის მიღწევა შესაძლებელია სხვა უფრო ადეკვატური და ეფექტიანი ალტერნატივის მეშვეობით, დამუშავება ვერ მიიჩნევა აუცილებელ მეთოდად. დამუშავების აუცილებლობის სტანდარტი უნდა შეფასდეს მონაცემთა მინიმიზაციის პრინციპის გათვალისწინებით.

ინტერესთა ურთიერთბალანსი:
დაუშვებელია დამუშავებისთვის პასუხისმგებელი პირის იმგვარი ლეგიტიმური ინტერესით პერსონალური მონაცემების დამუშავება, რომელიც ხელყოფს მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებს. ლეგიტიმური ინტერესის განსაზღვრისას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია გაითვალისწინოს მონაცემთა სუბიექტის გონივრული მოლოდინები და უზრუნველყოს დამუშავების რისკთან შესაბამისი მონაცემთა უსაფრთხოების ზომების გატარება.

რეკომენდაცია მიმოიხილავს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ მონაცემთა დამუშავების ლეგიტიმური ინტერესის არსებობის შეფასების საკითხს. კერძოდ, რეკომენდაციებში წარმოდგენილია მონაცემთა დამუშავების სხვადასხვა კონტექსტი და მიზანი, როგორიცაა: თაღლითობის პრევენცია, პირდაპირი მარკეტინგი და ინფორმაციის უსაფრთხოება. დოკუმენტი, განიხილავს კავშირს მონაცემთა დამუშავების სამართლებრივ საფუძველსა და ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ გათვალისწინებულ მონაცემთა სუბიექტის უფლებებს შორის.

მონაცემთა ლეგიტიმური დამუშავების განმსაზღვრელი კრიტერიუმები:
რეკომენდაციებში წარმოდგენილია მონაცემთა დაცვის კანონიერად, ლეგიტიმური ინტერესის საფუძველზე დამუშავების კრიტერიუმების[2] ანალიზი.[3]იმისათვის, რომ მონაცემთა დამუშავების სამართლებრივ საფუძველად ლეგიტიმური ინტერესი ჩაითვალოს, ერთდროულად უნდა დაკმაყოფილდეს შემდეგი სამი ძირითადი პირობა:

1. პერსონალურ მონაცემთა დამუშავების ლეგიტიმური ინტერესის არსებობა;
2. მონაცემთა დამუშავების ინტერესის მკაფიოდ და გარკვევით ჩამოყალიბება;
3. დამუშავების ინტერესის რეალურ დროში არსებობა.

პირობა I. მონაცემთა დამუშავების ლეგიტიმური ინტერესის არსებობა:
უპირველეს ყოვლისა, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი უნდა დარწმუნდეს, რომ მისი ინტერესი „ლეგიტიმურია“. აქვე, უნდა აღინიშნოს, რომ არ არსებობს დამუშავების ლეგიტიმური ინტერესების ამოწურვადი ჩამონათვალი და „მონაცემთა დაცვის ძირითადი რეგულაცია“ ლეგიტიმური ინტერესის კონკრეტულ განმარტებას არ შეიცავს.

აგრეთვე, საგულისხმოა, რომ დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური „ინტერესი“ მონაცემთა დამუშავებისათვის განსხვავდება მონაცემთა დამუშავების „მიზნისაგან“.[4] დამუშავებისთვის პასუხისმგებელ პირს, შესაძლოა ჰქონდეს მის მიერ წარმოებული პროდუქტის ან მომსახურეობის რეკლამირების ინტერესი, რაც შესაძლოა, პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების გზით განხორციელდეს.

GDPR-ის, აგრეთვე, ევროპის მართლმსაჯულების სასამართლოს პრაქტიკის ანალიზზე დაყრდნობით, ლეგიტიმური ინტერესების მაგალითებია:

- ინტერნეტში არსებულ ინფორმაციაზე ხელმისაწვდომობა;
- საჯარო ვებგვერდებზე წვდომა;
- ქონებრივი ზიანის მიმყენებელი პირის მონაცემებზე წვდომა, ზიანის ანაზღაურების მიზნით.
- მაცხოვრებელთა უძრავი ქონების, ჯანმრთელობის და სიცოცხლის დაცვის ინტერესი;
- პროდუქტის გაუმჯობესების ინტერესი, მონაცემთა სუბიექტების კრედიტის გადახდის უნარიანობის შემოწმება, და სხვა.

პირობა II. კანონიერია, ჩამოყალიბებულია „ნათლად“ და „გარკვევით“:
ლეგიტიმურად მიიჩნევა ინტერესი, რომელიც კანონიერია, ჩამოყალიბებულია ნათლად და გარკვევით, არის რეალური და ამჟამინდელი (ახლანდელ დროში არსებული). მაგალითად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, როგორც მომსახურების გამწევს, უნდა გააჩნდეს მონაცემთა დამუშავების ლეგიტიმური ინტერესი.

„კანონიერების“ კრიტერიუმი მაგალითი:
კრიტერიუმი მაგალიბამესის საფუხელწოდებაელექტრო სიგარეტის მწარმოებელ ევროპულ კომპანიას სურს წარმოებული პროდუქციის რეკლამირება, რისთვისაც ესაჭიროება, ევროპაში მცხოვრებ მომხმარებლებთან სარეკლამო შეტყობინებების გაგზავნა. აღნიშნული მიზნის განსახორციელებლად, იგი ამუშავებს მომხმარებელთა პერსონალურ მონაცემებს. პირდაპირი მარკეტინგის მიზნებისათვის პერსონალურ მონაცემთა დამუშავების ინტერესი შესაძლოა, ზოგიერთ შემთხვევაში, მონაცემთა დამუშავების ლეგიტიმურ ინტერესად ჩაითვალოს, თუმცა აუცილებელია მონაცემთა დამუშავების კონტექსტის გათვალისწინება.

მოცემულ შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, შეამოწმოს მონაცემთა კონკრეტული მიზნით დამუშავების კანონიერება. იმის გათვალისწინებით, რომ ევროკავშირში აკრძალულია ელექტრო სიგარეტის რეკლამა, ევროპული თამბაქოს დირექტივის და მასთან ასოცირებული კანონმდებლობის საფუძველზე, კომპანიას ვერ ექნება ლეგიტიმური ინტერესი პერსონალურ მონაცემთა დამუშავებისათვის, მონაცემთა დამუშავების „კანონიერების ელემენტის“ არარსებობის გამო.

პირობა III. „ნათლად“ და „გარკვევით“ ჩამოყალიბების კრიტერიუმის მაგალითი:
ორგანიზაციას „სამეზობლოს მცველები“ წევრებმა გადაწყვიტეს, რომ სამეზობლოში განათავსონ ვიდეო მეთვალყურეობის სისტემა, საცხოვრებელ პერიმეტრზე პოტენციური კრიმინალური ქმედებების კონტროლის მიზნით.

მიუხედავად იმისა, რომ შესაძლოა ლეგიტიმურ ინტერესად იქნას მიჩნეული ქონების, ჯანმრთელობის და სიცოცხლის დაცვა, ამ კონკრეტულ შემთხვევაში, მეთვალყურეობის სისტემის დასაყენებლად ხსენებული მიზეზი მეტად ზოგადია და არ მიუთითებს კონკრეტული უსაფრთხოების პრობლემაზე, რის საპასუხოდაც პროპორციული იქნებოდა მეთვალყურეობის სისტემის განთავსება. შესაბამისად, ორგანიზაციის ინტერესი ვერ აკმაყოფილებს სამ საფეხურიანი შეფასების კრიტერიუმს.

პირობა III. „რეალურ დროში არსებული“ კრიტერიუმის მაგალითი:
გაზეთის მენეჯმენტს სურს შექმნას მონაცემთა ბაზა, რომელშიც გაერთიანდება ინფორმაცია იმ გამომწერთა შესახებ, რომელთაც შესაბამისი ვადის ამოწურვის შემდგომ, არ მოისურვეს გაზეთის ხელახალი გამოწერა. მონაცემთა ბაზის შექმნის საჭიროებას გაზეთის მენეჯმენტი იმ არგუმენტით ასაბუთებს, რომ მომავალში, ახალი გაზეთის გამოცემის შემთხვევაში, პრაქტიკული იქნება ძველი გამომწერების შესახებ ინფორმაციაზე წვდომა. საგულისხმოა, რომ ახალი გაზეთის ჩამოყალიბების იდეა მხოლოდ ჰიპოთეტური ფორმით არსებობს. მოცემულ შემთხვევაში, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ინტერესი ვერ იქნება აღქმული როგორც „რეალური და ამჟამინდელი“ ინტერესი, ვინაიდან ახალი გაზეთის შექმნის საკითხი მხოლოდ სავარაუდოა. აქედან გამომდინარე, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ინტერესი ლეგიტიმურად ვერ იქნება მიჩნეული.

რეკომენდაციის პრაქტიკული დანიშნულება:
რეკომენდაცია მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს დაეხმარება ლეგიტიმური ინტერესის საფუძველზე პერსონალური მონაცემების კანონიერად დამუშავებაში.

დამუშავებისთვის პასუხისმგებელი პირები, რეკომენდაციის საშუალებით, დეტალურად გაეცნობიან იმ პირობებსა და კრიტერიუმებს, რომელთა გათვალისწინება და დაკმაყოფილება აუცილებელია პერსონალურ მონაცემთა ლეგიტიმური ინტერესის საფუძველზე დასამუშავებლად.

ევროკომისია არამატერიალური ზიანის მიყენებისთვის დაჯარიმდა

საქმის ფაქტობრივი გარემოებები:
2022 წელს ევროკომისიის მასპინძლობით ევროკავშირის ინსტიტუციური მომავლის თემატიკაზე კონფერენცია გაიმართა. ღონისძიებაში მონაწილეობა დაინტერესებულ პირებს ევროკომისიის მიერ შემუშავებულ ვებგვერდზე რეგისტრაციის გზით შეეძლოთ. ვებგვერდზე რეგისტრირებულმა გერმანიის მოქალაქემ, მისი პერსონალური მონაცემების დამუშავების წესების დარღვევასთან დაკავშირებით, საჩივარი შეიტანა ევროკავშირის მართლმსაჯულების სასამართლოში ევროკომისიის წინაღმდეგ. კერძოდ, იგი მონაწილეობდა ე. წ. “GoGreen” ღონისძიებაში, რომელიც იყენებდა ევროკავშირის რეგისტრაციის პორტალს, სადაც მომჩივანი საკუთარი „ფეისბუქ“ ანგარიშით დარეგისტრირდა.[1] მომჩივნის განმარტებით, ვებგვერდზე რეგისტრაციის შემდეგ, მისი მონაცემები გადაეცა კომპანია “Amazon Web Services”-ის მონაცემთა ბაზას, რომელიც აკონტროლებდა სარეგისტრაციო ვებგვერდის მონაცემთა გადაცემის ქსელს.

სარეგისტრაციო ვებგვერდზე მომხმარებლის „ფეისბუქ“ ანგარიშით რეგისტრაციისას, მომხმარებლის მონაცემები “Amazon Web Services”-ის გარდა, გადაეცემოდა ასევე კომპანია “Meta“-ს. ორივე შემთხვევაში მომხმარებლის პერსონალური მონაცემი აშშ-ში არსებულ მონაცემთა ბაზებში გადაიცემოდა. აღნიშნული აჩენდა საფრთხეს, რომ მონაცემები უკანონოდ დამუშავდებოდა აშშ-ის სამართალდამცავი ორგანოების მიერ. აღსანიშნავია, რომ დავის წარმოჭრის ეტაპზე, ევროკომისიას ჯერ არ ჰქონდა შემუშავებული შესაბამისობის გადაწყვეტილება აშშ-ში მონაცემთა გადაცემის თაობაზე.

სასამართლოს გადაწყვეტილება:
ევროკავშირის მართლმსაჯულების სასამართლომ, ევროკომისიის სარეგისტრაციო ვებგვერდის ფუნქციონირებისას, კომპანია “Amazon Web Services”-ში მონაცემთა გადაცემა დარღვევად არ მიიჩნია და განმარტა, რომ მონაცემთა გადაცემა ხორციელდებოდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ განსაზღვრული პრინციპების შესაბამისად. სასამართლომ დაადგინა, რომ ვებგვერდზე რეგისტრირებული მომხმარებლის მონაცემები გადაიცემოდა რეგისტრაციის ადგილთან ყველაზე ახლოს მდებარე სერვერზე, მოცემულ შემთხვევაში, ევროკავშირის ტერიტორიაზე – ლუქსემბურგში. ვებგვერდზე ხელმეორე რეგისტრაციისას კი, თვითონ მომხმარებელმა შეცვალა მონაცემთა დამუშავების პარამეტრები, რომლის საფუძველზეც მონაცემები აშშ-ში განთავსებულ სერვერზე გადაიცა.
მიუხედავად ამისა, სასამართლომ დაადგინა დარღვევა ევროკომისიის ვებგვერდზე „ფეისბუქის“ საშუალებით რეგისტრაციის პროცედურაში, რის შედეგადაც მომხმარებლის საიდენტიფიკაციო მონაცემები აშშ-ში გადაიცემოდა. დარღვევის აღმოჩენის ეტაპზე ევროკავშირსა და აშშ-ს შორის არ არსებობდა შესაბამისობის გადაწყვეტილება. ამდენად, კომისიას არ ჰქონდა მიღებული მონაცემთა გადაცემაზე კონკრეტული ღონისძიებები, შედეგად კი ევროკომისიის ვებგვერდზე მონაცემთა მიმართ მოქმედებები “META” პლატფორმის მიერ იმართებოდა.

სასამართლომ განმარტა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 46-ე და 48-ე მუხლების დაცვის აუცილებლობა, რაც ევროკომისიამ არ გაითვალისწინა ვებგვერდის შემუშავების პროცესში.

სასამართლოს გადაწყვეტილებით ევროკომისიას დაევალა მოსარჩელისთვის არამატერიალური ზიანის ანაზღაურება 400 ევროს ოდენობით.

„მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB") მოსაზრება მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებისთვის პასუხისმგებელი პირის ქვე-დამმუშავებლის (“Sub-Processor”) ვალდებულებების შესახებ

2024 წლის 7 ოქტომბერს „მონაცემთა დაცვის ევროპულმა საბჭომ“ გამოაქვეყნა მოსაზრება[1] მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის და დამუშავებისთვის პასუხისმგებელი პირის ქვე-კონტრაქტორის ან ქვე-დამმუშავებლის (“Sub-Processor”) შესახებ.

საბჭოს მოსაზრება შეეხება მონაცემთა დამუშავებისთვის პასუხისმგებელ პირსა და მის თანა-დამმუშავებელთან, აგრეთვე ქვე-დამმუშავებელთან ურთიერთობების საკითხებს.

ქვე-კონტრაქტორი ან ქვე-დამმუშავებელი დამუშავებაზე უფლებამოსილი პირის დავალების მიხედვით მოქმედი პირია,[2] რომელიც პერსონალურ მონაცემებს ამუშავებს დამუშავებაზე უფლებამოსილი პირისათვის. ქვე-დამმუშავებელი შეიძლება იყოს იურიდიული პირი, მაგალითად, მცირე და საშუალო ბიზნესი, საჯარო დაწესებულება, სააგენტო ან სხვა ორგანო.

ქვე-დამმუშავებლის დანიშვნა:
ქვე-დამმუშავებლის დასანიშნად აუცილებელი წინაპირობაა წერილობითი თანხმობა, რომელიც გაიცემა მონაცემთა დამუშავებისთვის უფლებამოსილი პირის ან თანა-დამმუშავებლის მიერ. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეადგინოს ხელშეკრულება ქვე-დამმუშავებელთან, რომლითაც განისაზღვრება ქვე-დამმუშავებელის ვალდებულებები.

წინამდებარე ხელშეკრულება დამუშავებაზე უფლებამოსილ პირსა და ქვე-დამმუშავებელს შორის უნდა უზრუნველყოფდეს მონაცემთა სუბიექტების უფლებების დაცვის იგივე ხარისხს, რაც უზრუნველყოფილია მონაცემთა დამუშავებისთვის უფლებამოსილ პირსა და დამუშავებაზე პასუხისმგებელ პირს შორის არსებული ხელშეკრულებით.

საბჭოს მიერ მომზადებულ სარეკომენდაციო ხასიათის დოკუმენტში განხილულია სხვადასხვა შემთხვევა, როდესაც საჭიროა დამუშავებისთვის პასუხისმგებელი პირის გარკვეული უფლებებისა და მოვალეობების განმარტების საკითხი, აგრეთვე, მხარეთა შორის დასადები ხელშეკრულების ტექსტის შედგენის საკითხი.

საბჭოს მოსაზრება შეიცავს პრაქტიკულ ინფორმაციას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებების შესახებ.

საკონტაქტო ინფორმაციის შენახვის ვალდებულება:
მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, უნდა ჰქონდეს ყველა დამუშავებაზე უფლებამოსილი პირისა და ქვე-დამმუშავებელის შესახებ ინფორმაცია (მაგალითად, სახელი, მისამართი, საკონტაქტო პირის ვინაობა).
უსაფრთხოების გარანტიებთან შესაბამისობის შემოწმების ვალდებულება:
დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გადაამოწმოს დამუშავებაზე უფლებამოსილი პირის და ქვე-დამმუშავებლის მიერ მონაცემთა უსაფრთხოების დაცვის სათანადო გარანტიებთან შესაბამისობის საკითხი.

გადამოწმების ვალდებულება წარმოიშვება განუსაზღვრელად იმისა, აყენებს თუ არა დამუშავების პროცესი მონაცემთა სუბიექტების უფლებებს და თავისუფლებებს მაღალი რისკის ქვეშ.
მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი, როგორც გადაწყვეტილების მიმღები პირი:
დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მიაღწიოს შეთანხმებას ქვე-დამმუშავებელთან „უსაფრთხოების დაცვის სათანადო გარანტიების“ შესახებ, თუმცა, წინამდებარე საკითხებზე საბოლოო გადაწყვეტილებების მიღების ვალდებულება და მისგან მომდინარე პასუხისმგებლობები ქვე-დამმუშავებელთან თანამშრომლობის თვალსაზრისით, კვლავ მონაცემთა დამუშავებისთვის უფლებამოსილი პირის (და არა დამუშავებაზე პასუხისმგებელი პირის) ვალდებულების ნაწილში ექცევა.

საბჭოს მოსაზრებით, ევროპის „მონაცემთა დაცვის ძირითადი რეგულაცია“ არ ავალდებულებს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს სისტემატიურად მოითხოვოს ხელშეკრულებების ასლები, რათა შეამოწმოს, თუ რამდენად გაითვალისწინეს მასთან თანამშრომლობაში მყოფმა ქვე-დამმუშავებლებმა მონაცემთა დაცვის შესაბამისი კანონმდებლობის მიერ განსაზღვრული ვალდებულებები.

მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეაფასოს, სიტუაციიდან გამომდინარე, საჭიროა თუ არა ხელშეკრულებების ასლების მოთხოვნა და გაცნობა, რათა შეძლოს ევროპის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებთან შესაბამისობის უზრუნველყოფა უფლებამოსილი პირებისა და საზედამხედველო ორგანო(ები)სათვის.

ვალდებულებები მონაცემთა საერთაშორისო გადაცემასთან მიმართებით:
თუ ქვე-დამმუშავებელი პერსონალურ მონაცემებს ევროპის ეკონომიკური სივრცის გარეთ გადასცემს, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მოამზადოს შესაბამისი დოკუმენტი, სადაც გადაცემის შესახებ ყველა საკითხი დეტალურად იქნება გათვალისწინებული.

მონაცემთა გადაცემის შესახებ დოკუმენტში საჭიროა აღიწეროს მონაცემთა გადაცემის ფორმა, გადაცემის მონაცემთა სუბიექტების უფლებებზე ზეგავლენის შეფასება და მონაცემთა უსაფრთხოების უზრუნველსაყოფად განხორციელებული ზომების შესახებ ინფორმაცია.

ამავდროულად, მონაცემთა დაცვის საზედამხედველო ორგანოს მოთხოვნის საფუძველზე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ადაადასტუროს მონაცემთა დაცვის სათანადო გარანტიებთან შესაბამისობა.მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა აღნიშნული დოკუმენტი, მოთხოვნისამებრ, უნდა მიაწოდოს საზედამხედველო ორგანოს.

რუმინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება ადგილობრივი მუნიციპალიტეტის მიერ პერსონალური მონაცემების დამუშავების კანონიერების შესახებ

რუმინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ბუქარესტის ადგილობრივი მუნიციპალიტეტის მიერ პერსონალური მონაცემების დამუშავების კანონიერება შეაფასა. საქმის შესწავლის ფარგლებში, ყურადღება გამახვილდა დამუშავებისთვის პასუხისმგებელი პირის საზედამხედველო ორგანოსთან თანამშრომლობის მნიშვნელობაზე.

საქმის ფაქტობრივი გარემოებები:
მონაცემთა სუბიექტის საჩივრის საფუძველზე რუმინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ბუქარესტის ადგილობრივი მუნიციპალიტეტის მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მოთხოვნების სავარაუდო დარღვევის შესწავლა დაიწყო.

საჩივარი შეეხებოდა სუბსიდირების პროგრამის („საოჯახო მეურნეობაში ენერგეტიკული საჭიროებისა და ენერგოეფექტურობის უზრუნველყოფის მიზნით გასატარებელი ღონისძიებები“) ფარგლებში პერსონალური მონაცემების დამუშავებას. რეზიდენტები, პირადი ან ელექტრონული ფოსტის საშუალებით, წარადგენდნენ სათანადო დოკუმენტაციას და ამ გზით მონაწილეობდნენ აღნიშნულ პროგრამაში. ელექტრონულ პლატფორმაში პერსონალური მონაცემების უსაფრთხოება სათანადოდ არ იყო უზრუნველყოფილი.

საზედამხედველო ორგანოს გადაწყვეტილება:
საზედამხედველო ორგანოს მოთხოვნის მიუხედავად, საქმის შესწავლის ფარგლებში, დამუშავებისთვის პასუხისმგებელმა პირმა არ წარადგინა სათანადო ინფორმაცია. ძირითადი რეგულაციის 58-ე მუხლის პირველი პუნქტის “a” და “e” ქვეპუნქტების თანახმად, საზედამხედველო ორგანო უფლებამოსილია, მისი ფუნქციების განსახორციელებლად დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირებისგან მიიღოს ნებისმიერი ინფორმაცია და მოითხოვოს პერსონალურ მონაცემებზე წვდომა. ზემოაღნიშნული ნორმის საფუძველზე, საზედამხედველო ორგანომ ადგილობრივ მუნიციპალიტეტს გაფრთხილება გამოუცხადა. ამავდროულად, დამუშავებისთვის პასუხისმგებელ პირს ყველა საჭირო ინფორმაციის წარდგენა დაევალა.

აღსანიშნავია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა საზედამხედველო ორგანოს მიერ განსაზღვრულ ვადაში არ განახორციელა შესაბამისი ღონისძიებების იმპლემენტაცია. ასევე, არ წარადგინა მოთხოვნილი ინფორმაცია, რის გამოც, “GDPR”-ის 58-ე მუხლის პირველი პუნქტის “a” და “e” ქვეპუნქტების შესაბამისად, დაეკისრა ჯარიმა 2, 010.38 ევროს ოდენობით.
საქმის განხილვის ფარგლებში დადგინდა, რომ ადგილობრივი მუნიციპალიტეტი მონაცემთა უსაფრთხოების წესების დარღვევით ამუშავებდა პერსონალურ ინფორმაციას. შესაბამისად, საზედამხედველო ორგანომ, ძირითადი რეგულაციის 58-ე მუხლის მე-2 პუნქტის “d” ქვეპუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს, მონაცემთა დამუშავების პროცესის “GDPR”-თან შესაბამისობის უზრუნველყოფა დაავალა.

ევროპის მონაცემთა დაცვის საბჭოს მიერ პერსონალურ მონაცემთა ფსევდონიმიზაციის სახელმძღვანელო რეკომენდაციის გამოქვეყნების შესახებ

2025 წლის იანვრის პლენარულ სხდომაზე ევროპის მონაცემთა დაცვის საბჭომ (“EDPB”) შეიმუშავა რეკომენდაცია მონაცემთა ფსევდონიმიზაციის შესახებ, რომელიც ხელს შეუწყობს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირთა მონაცემთა დაცვის საკანონმდებლო მოთხოვნებთან შესაბამისობას. საბჭო ფსევდონიმიზაციას განმარტავს როგორც მონაცემთა დაცვის ეფექტიან საშუალებას. ფსევდონიმიზაცია მონაცემთა იმგვარი დამუშავებაა, რომლის დროსაც დამატებითი ინფორმაციის გამოყენების გარეშე შეუძლებელია მონაცემების კონკრეტულ სუბიექტთან დაკავშირება და ეს დამატებითი ინფორმაცია შენახულია ცალკე, ტექნიკური და ორგანიზაციული ზომების მეშვეობით, იმგვარად, რომ მონაცემების იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირთან დაკავშირება პრაქტიკულად შეუძლებელია. რეკომენდაციაში საბჭო მიმოიხილავს ფსევდონიმიზაციისა და ფსევდონიმიზირებულ მონაცემებს, მათი გამოყენების საკითხს და აღნიშნულის უპირატესობებს.

სახელმძღვანელო რეკომენდაციაში განმარტებულია რამდენიმე მნიშვნელოვანი სამართლებრივი საკითხი:

მონაცემთა ფსევდონიმიზაციის არსი: მონაცემი ფსევდონიმიზაციის პროცესის შემდგომ, დამატებით ინფორმაციასთან გაერთიანების გზით შესაძლოა დაუკავშირდეს იდენტიფიცირებად მონაცემთა სუბიექტს, შესაბამისად, ფსევდონიმიზირებული მონაცემი კვლავ პერსონალურ მონაცემად მიიჩნევა. იმ შემთხვევაში, თუ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს შეუძლია დააკავშიროს ფსევდონიმიზირებული მონაცემი მონაცემთა სუბიექტთან, აღნიშნული ინფორმაცია პერსონალურ მონაცემად უნდა კვალიფიცირდეს.
რისკის შემცირება: ფსევდონიმიზაციის პროცესი იძლევა მონაცემთა დამუშავებასთან ასოცირებული რისკების შემცირების შესაძლებლობას, რადგან აღნიშნული პროცესი ითვალისწინებს იმ პერსონალურ მონაცემთა განცალკევებით და უსაფრთხოდ შენახვას, რომლებიც იდენტიფიცირებად ან იდენტიფიცირებულ პირებთან შესაძლოა იქნას ასოცირებული.

ლეგიტიმური ინტერესი, როგორც მონაცემთა დამუშავების სამართლებრივი საფუძველი: რეკომენდაციის თანახმად, ფსევდონიმიზაცია ამარტივებს მონაცემთა დამუშავების საფუძვლად ლეგიტიმური ინტერესის გამოყენებას. ლეგიტიმური ინტერესის კრიტერიუმი არის პერსონალური მონაცემების დამუშავების ერთ-ერთი ყველაზე მნიშვნელოვანი სამართლებრივი საფუძველი.

თუმცა, ლეგიტიმური ინტერესის საფუძველზე მონაცემთა დამუშავებამდე საჭიროა მონაცემთა სუბიექტის უფლებათა დაცვასა და მონაცემთა დამუშავების ინტერესის დაბალანსება (ე.წ. „ბალანსის ტესტი “balancing exercise”). ვინაიდან ფსევდონიმიზაციის პროცესი ამცირებს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებებზე ნეგატიური ზემოქმედების რისკებს. ზემოთ აღნიშნული ბალანსის შეფასების პროცესში პრიორიტეტი შესაძლოა დამუშავებისთვის პასუხისმგებელი პირის ინტერესს მიენიჭოს.

რეკომენდაციაში განმარტებულია ფსევდონიმიზაციის, როგორც ორგანიზაციებისათვის დამხმარე საშუალების ფუნქცია, კერძოდ, მონაცემთა დაცვის პრინციპების[5] („ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლი), განხორციელებასთან დაკავშირებული ვალდებულებების შესრულებაში, ასევე, მონაცემთა მეტად დაფარვის პრიორიტეტის (ძირითადი რეგულაციის 25-ე მუხლი) და უსაფრთხოებს კუთხით (ძირითადი რეგულაციის 32-ე მუხლი). რეკომენდაცია შეიცავს ტექნიკური და ორგანიზაციული ზომებისა და გარანტიების ანალიზს, ფსევდონიმიზაციის გზით მონაცემთა სუბიექტების კონფიდენციალურობის უზრუნველსაყოფად.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება სახის ამომცნობი სისტემის გამოყენებით პერსონალური მონაცემების დამუშავების შესახებ

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) საფეხბურთო მოედანზე დაშვების მიზნით მოქალაქეთა სახის ამომცნობი სისტემის გამოყენების მართლზომიერების შესახებ გადაწყვეტილება მიიღო.

საქმის ფაქტობრივი გარემოებები:

2022 წლის 22 ნოემბერს, მონაცემთა სუბიექტმა ესპანური საფეხბურთო კლუბის მიერ მოედნის რამდენიმე შესასვლელში სახის ამომცნობი სისტემის დამონტაჟების საკითხზე პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს საჩივრით მიმართა. აღსანიშნავია, რომ ფეხბურთის მატჩზე დამსწრე გულშემატკივრებს საშუალება ჰქონდათ ონლაინ დარეგისტრირებულიყვნენ, რა პროცესშიც მათ უნდა გადაეღოთ საკუთარი ფოტოსურათი (“Selfie”), საიდენტიფიკაციო ბარათის ასლი და, აგრეთვე, დათანხმებოდნენ მონაცემთა დამუშავების წესებსა და პირობებს. დამუშავებისთვის პასუხისმგებელი პირის განმარტებით, სისტემის შექმნის უმთავრესი მიზანი იყო მომხმარებლებისთვის მოსახერხებელი მომსახურების მიწოდება და არა უსაფრთხოებისა და ვინაობის დადასტურების უზრუნველყოფა. აღსანიშნავია, რომ სახის ამომცნობი ტექნოლოგიის გამოყენება არ იყო სავალდებულო.

საფეხბურთო კლუბმა, როგორც დამუშავებისთვის პასუხისმგებელმა პირმა, განახორციელა მონაცემთა დაცვაზე ზეგავლენის შეფასება და დაადგინა, რომ სამართლებრივი საფუძვლის - თანხმობის არსებობის გათვალისწინებით, მონაცემთა დამუშავება, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის თვალსაზრისით, არ იყო რაიმე საფრთხის შემცველი. ამავდროულად, ზეგავლენის შეფასების შედეგად დადგინდა, რომ მონაცემები წინასწარ განსაზღვრული მიზნებით მუშავდებოდა.

მონაცემთა სუბიექტის მტკიცებით, ბიომეტრიული მონაცემების ფართომასშტაბიანი დამუშავება ეწინააღმდეგებოდა მონაცემთა დამუშავების პროპორციულობის პრინციპს. ამასთან, დამუშავებისთვის პასუხისმგებელმა პირმა ვერ უზრუნველყო მონაცემთა დაცვის სათანადო გარანტიები და მხოლოდ თანხმობა არ იყო მონაცემთა დამუშავებისთვის საკმარისი საფუძველი.

საზედამხედველო ორგანოს გადაწყვეტილება:

- თანხმობის საკითხი

საზედამხედველო ორგანომ თანხმობის გაცემის მართლზომიერებასთან დაკავშირებით ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-6 მუხლის პირველი პუნქტის “a” ქვეპუნქტის ფარგლებში იმსჯელა. “AEPD”-მ დაადასტურა, რომ სახის ამომცნობი ტექნოლოგიის გამოყენებით სისტემაზე რეგისტრაცია იყო ნებაყოფლობითი. ფეხბურთის გულშემატკივრებს სახის ამომცნობი ტექნოლოგიის გამოყენებაზე უარის თქმა ან თანხმობის გამოხმობა ნებისმიერ დროს შეეძლოთ. აგრეთვე, ონლაინ სისტემაზე რეგისტრაცია მოითხოვდა თანხმობის მრავალეტაპიან დადასტურებას. შესაბამისად, საზედამხედველო ორგანომ დაადგინა, რომ მონაცემთა სუბიექტის მიერ გაცხადებული თანხმობა აკმაყოფილებდა ინფორმირებულობისა და ნებაყოფლობითობის კრიტერიუმებს. აგრეთვე, აღინიშნა, რომ მონაცემთა სუბიექტები მონაცემთა დამუშავების მიზნების თაობაზე ინფორმირებულნი იყვნენ.

- განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების აუცილებლობა

საზედამხედველო ორგანომ, ძირითადი რეგულაციის მე-9 მუხლით („განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავება“) გათვალისწინებული მოთხოვნების შესაბამისად, ბიომეტრიული მონაცემების დამუშავების კანონიერება შეაფასა. “AEPD”-მ დაადგინა, რომ მუშავდებოდა იმაზე მეტი პერსონალური ინფორმაცია (მაგალითად, საიდენტიფიკაციო ბარათის ასლი, ფოტოსურათი, სახის ამომცნობი სისტემა), ვიდრე საჭირო იყო მონაცემთა დამუშავების მიზნის მისაღწევად. საზედამხედველო ორგანომ განმარტა, რომ მონაცემთა მინიმიზაციის პრინციპი დამუშავებისთვის პასუხისმგებელი პირისგან მონაცემთა სუბიექტის უფლებებში ჩარევის ნაკლებად მზღუდავი ალტერნატივის გამოყენებას მოითხოვს.

- მონაცემთა მინიმიზაციის პრინციპის სავარაუდო დარღვევა

საზედამხედველო ორგანოს შეფასებით, თანხმობის არსებობის მიუხედავად, განსაკუთრებული კატეგორიის, ბიომეტრიული მონაცემების დამუშავება უნდა იყოს მიზნის მიღწევის აუცილებელი საშუალება. სახის ამომცნობი ტექნოლოგიის ალტერნატივა შეიძლებოდა, ყოფილიყო სპეციალური კოდი (“QR code”) და ელექტრონული ბილეთი, რომელთა საშუალებითაც მიიღწეოდა მონაცემთა დამუშავების იგივე მიზანი (სტადიონზე მარტივად შესვლა). ამდენად, დადგინდა ძირითადი რეგულაციის მე-5 მუხლის პირველი პუნქტის “c” ქვეპუნქტის – მონაცემთა მინიმიზაციის პრინციპის დარღვევა, რის გამოც დამუშავებისთვის პასუხისმგებელ პირს სახის ამომცნობი სისტემის მონაცემთა დაცვაზე ზეგავლენის ხელახალი შეფასება დაევალა.

- დაკისრებული ადმინისტრაციული ჯარიმა

საზედამხედველო ორგანომ აღნიშნა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა სახის ამომცნობი ტექნოლოგიის დანერგვისას არ დაიცვა ძირითადი რეგულაციით გათვალისწინებული მოთხოვნები, რაც გამოიხატა განსაკუთრებული კატეგორიის პერსონალური მონაცემების ფართომასშტაბიან დამუშავებაში. შედეგად, საფეხბურთო კლუბს, მისი შემოსავლის გათვალისწინებით, დაეკისრა ჯარიმა 200 000 ევროს ოდენობით.

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