მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება ბანკის კლიენტების პერსონალურ მონაცემთა „მეტასთვის“ გადაცემის შესახებ

მართლმსაჯულების ევროპული სასამართლოს გადაწყვეტილებით კომპანია „მეტას“ მარკეტინგული მიზნებისათვის პერსონალური მონაცემების გამოყენების მინიმიზაცია დაევალა

ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მომხმარებელთა პაროლების შენახვის წესების დარღვევის გამო კომპანია „მეტას“ დაჯარიმების შესახებ

საზედამხედველო ორგანომ კომპანია „მეტა“ 91 მილიონი ევროს ოდენობით დააჯარიმა. [1]

საქმის ფაქტობრივი გარემოებები:

ინსპექტირების დაწყების საფუძველი თავად კომპანია „მეტას“ მიერ საზედამხედველო ორგანოსადმი მიმართვა გახდა.

ოქტომბერი 2024

საქმის ფაქტობრივი გარემოებები:

ინსპექტირების დაწყების საფუძველი თავად კომპანია „მეტას“ მიერ საზედამხედველო ორგანოსადმი მიმართვა გახდა. კომპანიამ საზედამხედველო ორგანოს შიდა სისტემებში უნებლიედ, წინასწარი შეცნობის გარეშე, სოციალური მედია პლატფორმის მომხმარებელთა პაროლების პერსონალურ მონაცემთა დაცვის ზომების გატარების გარეშე,[2] ჩვეულებრივი ტექსტის გამოყენებით (კრიპტოგრაფიული დაცვის ან დაშიფვრის გარეშე) შენახვის შესახებ აცნობა.

საზედამხედველო ორგანომ ინსპექტირების პროცესში შეაფასა კომპანია „მეტას“ მიერ გატარებული მონაცემთა უსაფრთხოების ზომების შესაბამისობა „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებთან, აგრეთვე, იმ რისკებთან, რომელთანაც ასოცირდება კონკრეტული ტიპის მონაცემის (ამ შემთხვევაში, პლატფორმის მომხმარებელთა პაროლების) დამუშავება.

„მონაცემთა დაცვის ძირითადი რეგულაციის“ დარღვევა:

ძირითადი რეგულაცია მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს ავალდებულებს, რომ მონაცემთა დამუშავების კონტექსტიდან გამომდინარე, დანერგონ მომხმარებელთა კონფიდენციალურობის დარღვევის რისკების შესაბამისი დაცვის ღონისძიებები. აღნიშნული უზრუნველყოფს მონაცემთა უსაფრთხოების რისკების შემცირებას.

საქმის ფაქტობრივი გარემოებების შესწავლის შედეგად, საზედამხედველო ორგანომ გამოავლინა ძირითადი რეგულაციის შემდეგი დარღვევები:

- ძირითადი რეგულაციის 33-ე მუხლის პირველი პუნქტის დარღვევა, ვინაიდან კომპანიამ არ აცნობა მონაცემთა დაცვის საზედამცედველო ორგანოს მონაცემთა უსაფრთხოების ინციდენტის შესახებ. უსაფრთხოების ინციდენტი ეხებოდა მომხმარებელთა პატოლების დაცვას, სათანადო ღონისძიებების გარეშე და მარტივი ტექსტის ფორმით (“plain text format”) შენახვას;
- 33-ე მუხლის მეხუთე პუნქტის დარღვევა, ვინაიდან კომპანიამ ვერ უზრუნველყო მონაცემთა უსაფრთხოების ინციდენტის დოკუმენტირება;
- მე-5 მუხლის პირველი (f) პუნქტის დარღვევა[3], რადგან კომპანიამ არ გამოიყენა შესაბამისი ტექნიკური და ორგანიზაციული ზომები არაავტორიზებული დამუშავებისგან მომხმარებელთა პაროლების დასაცავად;
- 32-ე მუხლის პირველი პუნქტის დარღვევა, ვინაიდან კომპანიამ არ გამოიყენა რისკთან შესაბამისი ტექნიკური და ორგანიზაციული ზომები, მაგალითად, მომხმარებელთა პაროლების უსაფრთხოებისთვის პაროლების კონფიდენციალურობის მუდმივად განახლებადი დაცვის ღონისძიებების დანერგვა (“ongoing confidentiality of user passwords”.)

გადაწყვეტილების გამოქვეყნებამდე, 2024 წლის ივნისში ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მის მიერ მიღებული პირველადი გადაწყვეტილება სამუშაო ვერსიის სახით (”draft decision”), „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-60 მუხლით გათვალისწინებული წესებისა და პროცედურების დაცვით, გაუზიარა ევროკავშირის წევრი ქვეყნების კოლეგა საზედამხედველო ორგანოებს, რომელთაც გადაწყვეტილებასთან დაკავშირებით საწინააღმდეგო პოზიცია არ გამოუთქვამთ.

საზედამხედველო ორგანოს ძირითადი მიგნებები:

საზედამხედველო ორგანოს გადაწყვეტილების თანახმად, მომხმარებელთა პაროლები არ უნდა იქნეს შენახული მარტივი ტექსტური ფორმით „plaintext”[4], ვინაიდან წინამდებარე მონაცემებზე წვდომის და მისი არამართლზომიერი გამოყენების შედეგად, მონაცემთა სუბიექტების უფლებების შელახვის რისკები მაღალია.

საყურადღებოა, რომ ამგვარი სახის მონაცემი (მომხმარებლის პაროლები) განსაკუთრებული სიფრთხილით უნდა დამუშავდეს, ვინაიდან მათი არამართლზომიერი გამოყენება უკავშირდება მონაცემთა სუბიექტების პირადი სოციალური მედიის ანგარიშებზე არაავტორიზებული წვდომის რისკს.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილებით, კომპანია „მეტას“ სამართალდარღვევებისათვის დაეკისრა ჯარიმა 91 მილიონი ევროს ოდენობით.

შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება ბანკის კლიენტების პერსონალურ მონაცემთა „მეტასთვის“ გადაცემის შესახებ

2021 წლის 8 ივნისს, შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ, შვედური ბანკისგან მიიღო შეტყობინება მონაცემთა უსაფრთხოების ინციდენტისთაობაზე.[1] ბანკმა საზედამხედველო ორგანოს მიაწოდა ინფორმაცია მის ვებგვერდზე და აპლიკაციაში ინტეგრირებული „Facebook“-ის პიქსელის (ამჟამად კომპანია „მეტას“ პიქსელის) შესახებ, რომელიც გამოიყენებოდა მარკეტინგის მიზნებისათვის. მისი მეშვეობით კომპანია „მეტასთან“ უნებლიედ, მონაცემთა უსაფრთხოების არასაკმარისი ზომების გატარების მიზეზით, ხორციელდებოდა ბანკის კლიენტების პერსონალური მონაცემების გადაცემა. ბანკის მიერ საზედამხედველო ორგანოსთვის მიწოდებული ინფორმაციით, 2019 წლის 15 ნოემბრიდან 2021 წლის 2 ივნისამდე, პიქსელის საშუალებით კომპანია „მეტას“ უნებლიედ გადაეცა დაახლოებით მილიონი მომხმარებლის პერსონალური მონაცემები.

საზედამხედველო ორგანოს ძირითადი მიგნებები

საზედამხედველო ორგანოს მიერ საქმის ფაქტობრივ გარემოებათა შესწავლის საფუძველზე დადგინდა, რომ უსაფრთხოების ინციდენტის, კერძოდ, პერსონალურ მონაცემთა შემთხვევით გადაცემის საფუძველი გახდა ბანკის მიერ კომპანია „მეტას“ პიქსელში ახალი ფუნქციების შეცდომით გააქტიურება. შესაბამისად, პიქსელის არასწორ პარამეტრებზე დაყენებამ გამოიწვია ბანკის კლიენტების ინფორმაციის კომპანია „მეტასთვის“ გადაცემა, მათ შორის: სასესხო ვალდებულების, საბანკო ანგარიშების ნომრებისა და სოციალური მომსახურების მისაღებად საჭირო და პიროვნების მაიდენტიფიცირებელი მონაცემების შესახებ.

აღსანიშნავია, რომ უსაფრთხოების ინციდენტის შესახებ ინფორმაციის მიღების შემდგომ, ბანკმა გააუქმა პიქსელი და შეწყვიტა მისი გამოყენება. შვედური ბანკის განცხადებით, კომპანია „მეტამ“ წაშალა პიქსელის მეშვეობით შეგროვებული პერსონალური მონაცემები, აგრეთვე, დაადასტურა, რომ მან არ გამოიყენა შეცდომით მიღებული ინფორმაცია უსაფრთხოების ინციდენტის აღმოჩენის შემდგომ. ამასთან, ბანკმა დაუყოვნებლივ გადახედა პერსონალურ მონაცემთა დამუშავების შიდა პროცედურას.[2]

საზედამხედველო ორგანოს გადაწყვეტილება

შვედეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს შეფასებით, ბანკმა დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ გათვალისწინებული მოთხოვნები. კერძოდ, ბანკმა ვერ უზრუნველყო მის ვებგვერდსა და აპლიკაციაში უსაფრთხოების სათანადო ტექნიკური და ორგანიზაციული ღონისძიების მიღება. შესაბამისად, სამართალდარღვევისათვის დამუშავებისთვის პასუხისმგებელ პირს დაეკისრა ადმინისტრაციული ჯარიმა 1 300 000 ევროს ოდენობით.

ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება პოლიტიკური პარტიის მიერ მონაცემთა სუბიექტების მონაცემების უკანონო დამუშავების შესახებ

ნორვეგიის ერთ-ერთი მუნიციპალიტეტის სააღმზრდელო დაწესებულებებში მყოფი ბავშვების მშობლებმა ელექტრონულ ფოსტაზე მიიღეს პოლიტიკური პარტიის შეტყობინება, რომელიც პოლიტიკური რეკლამის შინაარსს შეიცავდა. საკითხის შესწავლის მიზნით, მონაცემთა სუბიექტებმა მიმართეს საზედამხედველო ორგანოს.

საქმის ფაქტობრივი გარემოებების თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა თავდაპირველად აღნიშნა, რომ მონაცემთა დამუშავების პროცესს ახორციელებდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6(1)(e) მუხლის საფუძველზე. რეგულაციის აღნიშნული ქვეპუნქტი ითვალისწინებს მონაცემთა დამუშავებას საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად ან მინიჭებული ოფიციალური უფლებამოსილების განსახორციელებლად. თუმცა მოგვიანებით, დამუშავებისთვის პასუხისმგებელმა პირმა დააკონკრეტა და დამუშავების საფუძვლად მე-6(1)(f) მუხლი მიუთითა, რომლის თანახმად დამუშავება კანონიერია, თუ მონაცემთა დამუშავება აუცილებელია მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ან მესამე პირის კანონიერი ინტერესების დასაცავად. გარდა იმ შემთხვევისა, როდესაც აღნიშნულ ინტერესებს აღემატება იმ მონაცემთა სუბიექტის ინტერესები ან ფუნდამენტური უფლებები და თავისუფლებები, რომელიც მოითხოვს მონაცემთა დაცვას.

ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელ პირს არ ჰქონდა დამუშავების კანონიერი საფუძველი და მის მიერ განხორციელებული მოქმედებების დაირღვა მონაცემთა სუბიექტებისთვის ინფორმაციის მიწოდების ვალდებულება (ძირითადი რეგულაციის მე-14 მუხლი). კერძოდ, დამუშავებისთვის პასუხისმგებელმა პირმა მართალია, კანონიერად მიიღო მონაცემები მუნიციპალიტეტის ადმინისტრაციისგან (ამომრჩეველთა სიების დაზუსტების მიზნით), თუმცა მას აღნიშნული მონაცემების სხვა მიზნით დამუშავების (პოლიტიკური რეკლამის გაგზავნის) საფუძველი არ ჰქონდა განსაზღვრული. შესაბამისად, მონაცემთა სუბიექტები არ იყვნენ ინფორმირებულნი დამუშავების პროცესების შესახებ. ამასთანავე, მონაცემთა სხვაგვარი მიზნით დამუშავების თაობაზე დამუშავებისთვის პასუხისმგებელ პირს არ ჰქონდა მუნიციპალიტეტთან დადებული რაიმე სახის ხელშეკრულება, რაც ძირითადი რეგულაციის 28-ე მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს კონკრეტული მოქმედების განხორციელების უფლებამოსილებას მიანიჭებდა.

ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს მისცა შენიშვნა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6(1)(f) და მე-14 მუხლების დარღვევისთვის.

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება ორგანოს გადაწყვეტილება მონაცემთა დამუშავების კანონიერების შესახებ

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“ICO”) აზარტული ონლაინ თამაშების კომპანიის მიერ მონაცემთა დამუშავების კანონიერების შესახებ გადაწყვეტილება მიიღო[1].

ფაქტობრივი გარემოებები:
აზარტული ონლაინ თამაშების კომპანიის ვებგვერდი იყენებდა ე.წ. „თრექინგის“ ტექნოლოგიას, მარკეტის მიზნებისთვის პერსონალური მონაცემების შესაგროვებლად. მას შემდეგ, რაც ინფორმაცია გავრცელდა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ დიდი რაოდენობით მონაცემების მონაცემთა სუბიექტების თანხმობის გარეშე მესამე პირებისთვის გადაცემის შესახებ, გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ საკითხის შესწავლა დაიწყო.
როგორც აღმოჩნდა, კომპანიის ვებგვერდზე შესვლისთანავე, მომხმარებლების მოწყობილობებზე „მზა ჩანაწერები“ ბანერის მეშვეობით ავტომატურად, შესაბამისი თანხმობის გაცემამდე, თავსდებოდა. შესაბამისად, მომხმარებელთა პერსონალური მონაცემები მუშავდებოდა და გადაეცემოდა მესამე პირებს, მონაცემთა სუბიექტების ცოდნისა და ნებართვის გარეშე, ავტომატურად, ვებგვერდზე ვიზიტის გზით.
2023 წლის 2 მარტს, გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მიუთითა მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა დამუშავების უკანონო პრაქტიკის აღმოფხვრაზე. აღნიშნულის საპასუხოდ, კომპანიამ მეორე დღესვე მიიღო შესაბამისი ზომები.

გადაწყვეტილების დასაბუთება:
2023 წლის 17 მარტს, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა განმარტა, რომ პერსონალური მონაცემები მონაცემთა სუბიექტთა თანხმობით დამუშავდა, რაც წარმოადგენს დამუშავების კანონიერ საფუძველს. აქედან გამომდინარე, გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ 2023 წლის 10 იანვრიდან 3 მარტამდე მონაცემთა დამუშავების პროცესები ხორციელდებოდა უკანონოდ, რადგან მომხმარებელთა მონაცემები, მონაცემთა სუბიექტების ცოდნისა და თანხმობის გარეშე, ვებგვერდის „მზა ჩანაწერების“ მეშვეობით დამუშავდ და გაზიარდა.
პერსონალურ მონაცემთა უკანონო გამჟღავნება მესამე პირებისთვის საზოგადოებრივად მნიშვნელოვან საკითხს წარმოადგენს, განსაკუთრებით კომერციული თვალსაზრისით.

მიღებული გადაწყვეტილება:
გაერთიანებული სამეფოს „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“UK GDPR”) 58(2)(ბ) მუხლის შესაბამისად, საზედამხედველო ორგანომ აზარტული ონლაინ თამაშების კომპანიას რეგულაციის 5(1)(ა), 6(1)(ბ) და 7(1) მუხლების დარღვევისთვის შენიშვნა გამოუცხადა.

ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა უსაფრთხოების დარღვევის შესახებ

ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთ საგანმანათლებლო დაწესებულებაში მონაცემთა უსაფრთხოების დარღვევის შესახებ გადაწყვეტილება მიიღო.[1]

ფაქტობრივი გარემოებები:
2018 წლიდან აგდერის უნივერსიტეტი სასწავლო პროცესში აქტიურად იყენებდა საკომუნიკაციო პლატფორმებს: “MS Teams”-სა და “Sharepoint”-ს. მოგვიანებით, უნივერსიტეტის თანამშრომელმა შეიტყო, რომ “MS Teams”-ის საქაღალდე ყველა თანამშრომელსა და სტუდენტს ანიჭებდა პერსონალურ მონაცემების შემცველ დოკუმენტებზე წვდომას. მაგალითისთვის, 4 დოკუმენტი მიემართებოდა 4 851 თანამშრომლისა და 10 419 გარეშე პირის (2014 წლამდე) მონაცემებს, ხელმისაწვდომი იყო მათ შორის იმგვარი მონაცემები, როგორიცაა: სახელები, პირადი ნომრები, თანამშრომლის ნომრები, თანამდებობიდან გათავისუფლების თარიღები და ორგანიზაციული ერთეულები. უფრო მეტიც, დოკუმენტი შეიცავდა 568 სტუდენტის საგამოცდო ნაშრომსა და 64 უკრაინელი ლტოლვილის პირად მონაცემებს.

თანამშრომლის მიერ აღნიშნულის თაობაზე უნივერსიტეტის ინფორმირების შემდეგ, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირმა დაუყოვნებლივ შეცვალა “MS Teams”-ის საქაღალდეების წვდომის პარამეტრები. განახლებული პარამეტრების მიხედვით, საქაღალდეზე წვდომა შესაძლებელი გახდა მხოლოდ საქაღალდის მფლობელის დადასტურების შემთხვევაში.

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) 33-ე მუხლის შესაბამისად, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შესახებ შეატყობინა ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (“Datilsynet”). ძირითადი რეგულაციის 34-ე მუხლის შესაბამისად, მან აღნიშნული, ასევე, შეატყობინა შესაბამის მონაცემთა სუბიექტებს. გარდა ამისა, უნივერსიტეტმა თავის ვებგვერდზე გამოაქვეყნა მონაცემთა უსაფრთხოების დარღვევის შესახებ დეტალური ინფორმაცია. იქიდან გამომდინარე, რომ „ლოგირების“ შესახებ ჩანაწერები მხოლოდ გასულ 6 თვეს მოიცავდა, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა ვერ დაადასტურა ჩამოტვირთეს თუ არა გაზიარებული მონაცემები თანამშრომლებმა ან სტუდენტებმა.

გადაწყვეტილების დასაბუთება:

- ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ საკითხთან მიმართებით დაირღვა კონფიდენციალობის უფლება, ვინაიდან პერსონალური მონაცემები ხელმისაწვდომი გახდა უნივერსიტეტის დაახლოებით *1 200* თანამშრომლისთვის და *12 000* სტუდენტისთვის.
- გარდა ამისა, დამუშავებისთვის პასუხისმგებელ პირს არ ჰქონდა კანონთან შესაბამისი „ლოგირების“ მექანიზმი, რამაც შეუძლებელი გახადა იმის შეფასება, თუ რამდენ ადამიანს ჰქონდა წვდომა მონაცემებზე.
- ამავდროულად, უნივერსიტეტმა ვერ განახორციელა, მათ შორის, თანამშრომლების ტრენინგი პროგრამის *(“MS Teams”)* გამოყენებასთან დაკავშირებით შესაბამისი შიდა პროცედურები.
- ასევე, არასწორად განისაზღვრა პროგრამის თავდაპირველი პარამეტრი. შესაბამისად, არ მოწმდებოდნენ ის თანამშრომლები, რომელთაც წვდომა ჰქონდათ *“MS Teams”*-ის საქაღალდეებზე.
- მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა ვერ უზრუნველყო უსაფრთხოების შესაბამისი ზომები ძირითადი რეგულაციის *24*-ე და *32*-ე მუხლის მიხედვით, რამაც გამოიწვია მონაცემთა უსაფრთხოების დარღვევა.

მიღებული გადაწყვეტილება:

ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ აღნიშნა, რომ მართალია, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა განაახლა “MS Teams”-ის პარამეტრები, თუმცა დარღვევის სიმძიმიდან (კერძოდ, იმ პირების რაოდენობა, ვისაც პოტენციურად მიუწვდებოდა ხელი მონაცემებზე) გამომდინარე, აუცილებლად მიიჩნია საზედამხედველო ორგანოს რეაგირება.
პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) 24-ე და 32-ე მუხლის დარღვევა, შედეგად, აგდერის უნივერსიტეტს დაეკისრა ჯარიმა 12 700 ევროს ოდენობით.

მართლმსაჯულების ევროპული სასამართლოს გადაწყვეტილებით კომპანია „მეტას“ მარკეტინგული მიზნებისათვის პერსონალური მონაცემების გამოყენების მინიმიზაცია დაევალა

მართლმსაჯულების ევროპულმა სასამართლომ გამოაქვეყნა გადაწყვეტილება პერსონალურ მონაცემთა დაცვის ერთ-ერთი აქტივისტის, ავსტრიის მოქალაქის — მაქსიმილიან შრემსის მიერ კომპანია “მეტას” წინააღმდეგ შეტანილი საჩივრის თაობაზე.[1]

სასამართლოს მიერ განხილული ძირითადი საკითხები: [2]

·პერსონალური მონაცემების გამოყენების შეზღუდვის დაწესება ონლაინ მარკეტინგის მიზნებისათვის;

·საჯაროდ ხელმისაწვდომი პერსონალური მონაცემების გამოყენების მინიმიზაცია და პერსონალური მონაცემების გამოყენების დაშვება მხოლოდ იმ მიზნებით, რა მიზნითაც წინამდებარე მონაცემები გასაჯაროვდა.

მონაცემების მარკეტინგული მიზნებით გამოყენების მინიმიზაცია:

საქმის ფაქტობრივი გარემოებების თანახმად, კომპანია „მეტას“ პლატფორმა ინახავს და მარკეტინგული მიზნებით იყენებს 2004 წლიდან მის მიერ შეგროვებულ მონაცემებს, რაც მოიცავს პლატფორმის მომხმარებლების მიერ სოციალურ მედიაში განთავსებულ,[1] აგრეთვე, სხვა მომხმარებლების მიერ ერთმანეთის შესახებ პლატფორმაზე განთავსებულ ინფორმაციას, ასევე, ონლაინ აპლიკაციების მიერ ავტომატურად შეგროვებულ მონაცემთა მომხმარებელთა შესახებ.

მონაცემთა განუსაზღვრელი რაოდენობით, კონკრეტული მიზნის გარეშე შეგროვების პრაქტიკის თავიდან ასარიდებლად, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ მონაცემთა დამუშავების მინიმიზაციის პრინციპის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს ავალდებულებს, დაამუშავონ მხოლოდ ის მონაცემები, რაც აუცილებელია დამუშავების მიზნის მისაღწევად.

„მეტამ” მონაცემთა დამუშავების მინიმიზაციის პრინციპი არ გაითვალისწინა, ამასთანავე, არ განსაზღვრა მონაცემთა წაშლის კონკრეტული ვადები,[2] აგრეთვე, მონაცემთა ტიპის გათვალისწინებით, არ შეზღუდა მონაცემთა დამუშავების ოპერაციები ისე, რომ მათი მიზნიდან გამომდინარე, დამუშავებულიყო მონაცემთა მინიმალური რაოდენობა და ტიპი.

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები ვალდებულნი არიან დაიცვან მონაცემთა მინიმიზაციის პრინციპი მონაცემთა დამუშავების საფუძვლის მიუხედავად. იმ შემთხვევაშიც კი, თუ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა სუბიექტისაგან მოპოვებული აქვს თანხმობა პერსონალიზებული სარეკლამო შეტყობინებების მიღების თაობაზე, დაუშვებელია მათი მონაცემების განუსაზღვრელი ვადით დამუშავება.

მართლმსაჯულების ევროპული სასამართლოს გადაწყვეტილებით, მონაცემთა მინიმიზაციის პრინციპის რეგულირების საკითხი ეროვნული სასამართლოების დისკრეციას წარმოადგენს.

საჯაროდ ხელმისაწვდომი პერსონალური მონაცემების გამოყენება:

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-9 (1)(ე) მუხლის საფუძველზე, მონაცემთა სუბიექტის მიერ გასაჯაროებული ინფორმაცია, შესაძლოა გამოიყენოს ორგანიზაციამ, ვინაიდან ასეთ შემთხვევაში, იგი თანახმაა მონაცემების დამუშავებაზე.

საქმის ფაქტობრივი გარემოებები:

ავსტრიის ეროვნულმა სასამართლომ განიხილა მაქსიმილიან შრემსსა და კომპანია „მეტას“ შორის არსებული დავა. მოსარჩელემ საქმე 2014 წელს შეიტანა ავსტრიის სასამართლოში „მონაცემთა დაცვის ძირითადი რეგულაციის“ დარღვევებზე[3] დაყრდნობით, მათ შორის, მონაცემთა სარეკლამო მიზნებით დამუშავების გამო. 2021 წელს ავსტრიულმა სასამართლომ საქმის ფაქტობრივი გარემოებების შესაბამისად, რიგ საკითხებზე მართლმსაჯულების ევროპულ სასამართლოს მიმართა. ხოლო ევროპულმა მართლმსაჯულების სასამართლომ საქმის განხილვა 2024 წლამდე შეაჩერა, ვინაიდან ერთ-ერთი სხვა საქმე (C-252/21 Bundeskartellamt) წინამდებარე საქმის მსგავს საკითხებს ეხებოდა.

აღსანიშნავია, რომ 2024 წლის 8 თებერვალს მართლმსაჯულების სასამართლომ განიხილა მაქსიმილიან შრემსსა და კომპანია „მეტას“ შორის არსებული დავის შემდეგი ორი საკითხი:

-პირველი საკითხი მონაცემთა მინიმიზაციის პრინციპის ინტერპრეტაციას ეხებოდა. კონკრეტულად, აქვთ თუ არა სოციალური მედიის პლატფორმებს უფლება მარკეტინგული მიზნებით, მონაცემთა შეერთების და მათი შეერთბული ფორმით დამუშავების ისე, რომ დამუშავება მოიცავდეს როგორც მონაცემთა სუბიექტის მიერ, ასევე მონაცემთა სუბიექტის შესახებ სხვა პირთა მიერ პლატფორმაზე ატვირთული ინფორმაციის დამუშავებას, აგრეთვე, აპლიკაციის მიერ ავტომატური მონიტორინგის შედეგად მიღებული ინფორმაციის დამუშავებას.

-მეორე განსახილველი საკითხი კონკრეტულ სიტუაციას ასახავდა. კერძოდ, ღონისძიების მსვლელობისას, საჯარო გამომსვლელის მიერ[1] მისი სექსუალური ორიენტაციის შესახებ გაჟღერების შემდგომ, დასაშვებია თუ არა ამ პიროვნების შესახებ არსებული ყველა ინფორმაციის გაერთიანების (მათ შორის, ინფორმაციის სექსუალური ორიენტაციის შესახებ) საფუძველზე, პიროვნების შესახებ ინფორმაციის შეგროვება და დამუშავება მარკეტინგის მიზნებისათვის.

სასამართლოს გადაწყვეტილებით, მიუხედავად იმისა, რომ პლატფორმის გარეთ შრემსმა თავად გაასაჯაროვა ინფორმაცია მისი სექსუალური ორიენტაციის შესახებ, დაუშვებელი იყო პლატფორმის მეშვეობით საჯარო ინფორმაციის გამოყენება მონაცემთა სუბიექტისათვის მარკეტინგული მიზნით გარკვეული პროდუქტის ან მომსახურების შესათავაზებლად.[2]

განსხვავებით სასამართლოს გადაწყვეტილებისაგან, კომპანია „მეტას“ პოზიციის თანახმად, ყველა საჯარო ინფორმაცია ექცევა საჯარო ინფორმაციის ცნების ქვეშ და შესაძლოა მისი დამუშავება შეზღუდვების გარეშე, ნებისმიერი ფორმით, განუსაზღვრელი დროის განმავლობაში.

მონაცემთა მინიმიზაცია:

ზოგიერთ შემთხვევაში მონაცემთა წაშლის ვადა განსაზღვრულია ან ნათელია თუმცა, როდესაც მონაცემები მარკეტინგის მიზნებისათვის მუშავდება, მონაცემთა მინიმიზაციის საკითხი უფრო ბუნდოვანია, რის აღმოსაფხვრელადაც რეკომენდებულია კომპანიებმა შეიმუშავონ მონაცემთა პერიოდული წაშლის სისტემა.

მართლმსაჯულების სასამართლომ წინამდებარე გადაწყვეტილების პირველი შემაჯამებელი დოკუმენტი უკვე გამოსცა, თუმცა მისი სრული ტექსტი ჯერ არ არის გამოქვეყნებული.

მართლმსაჯულების ევროპული სასამართლოს მთავარი მიგნებები:

—მონაცემთა სუბიექტის მიერ ინფორმაციის გასაჯაროების მიუხედავად, პლატფორმებს არ აქვთ უფლება, მარკეტინგული მიზნებით გამოიყენონ საჯარო ინფორმაცია, რათა შესთავაზონ მონაცემთა სუბიექტს პროდუქტი ან მომსახურეობა.

—როდესაც მონაცემები მარკეტინგის მიზნებისათვის მუშავდება, რეკომენდებულია, კომპანიებმა შეიმუშავონ მონაცემთა პერიოდული წაშლის სისტემა.

[1]მართლმსაჯულების სასამართლოს გადაწყვეტილება “მეტას” ვალდებულებაზე მონაცემთა მინიმიზაციის კუთხით https://noyb.eu/en/cjeu-meta-must-minimise-use-personal-data-ads [08.10.2024]
[2] სექსუალური ორიენტაციის შესახებ პერსონალური მონაცემების შეგროვების გამო აქტივისმა კომპანია „მეტას“ წინააღმდეგ დავა მოიგო https://abcnews.go.com/Business/wireStory/austrian-activist-schrems-wins-privacy-case-meta-personal-114492941 [08.10.2024]

“LinkedIn”-მა ჰონგ-კონგში ხელოვნური ინტელექტის სწავლების მიზნით პერსონალურ მონაცემთა დამუშავება შეაჩერა

“LinkedIn”-მა ხელოვნური ინტელექტის ინტეგრირება 2023 წლიდან დაიწყო და დღეისთვის უკვე ფუნქციონირებს ხელოვნურ ინტელექტზე დამოკიდებული რამდენიმე მომსახურება, მაგალითად, ე.წ. “AI-Generated Recruiter Messages” სერვისი, რომელიც დამსაქმებლებს და დასაქმების მსურველ კანდიდატებს თავიანთ მიზნებსა და ინტერესებზე მორგებული შეტყობინებების გაგზავნის შესაძლებლობას ანიჭებს. კერძოდ, „პირადი პროფილის შექმნის“ (“Profile Writing Suggestions”) სერვისის სარგებლობის პროცესში “LinkedIn” იყენებს მომხმარებელთა პერსონალურ მონაცემებს. გენერირებადი ხელოვნური ინტელექტი კომპანიებს ეხმარება მომსახურების გაუმჯობესებაში, ხოლო მომხმარებლებს უმარტივებს შეთავაზებულ სერვისზე ხელმისაწვდომობას. ამდენად, “LinkedIn” დასაქმებაზე ორიენტირებული სერვისების წარმართვისას, საჭიროებს ხელოვნური ინტელექტის სწავლების მიზნით პერსონალურ მონაცემთა დამუშავებას.

2024 წლის 18 სექტემბერს “LinkedIn”-მა განაახლა კონფიდენციალობის პოლიტიკა, რომლის თანახმად, ხელოვნური ინტელექტის სწავლების მიზნით, კომპანიამ შეიძლება გამოიყენოს მისი მომხმარებლის პერსონალური მონაცემები. აღნიშნული გულისხმობს ყველა იმ მომხმარებლის მონაცემთა დამუშავებას, რომლებსაც დამუშავებაზე არ აქვთ აშკარად გამოხატული თანხმობა. ამასთანავე, კომპანიას გააჩნია პარამეტრი, რომლის გაუქმებით, მომხმარებელს შეუძლია მონაცემთა ამგვარ დამუშავებაზე უარის გაცხადება, თუმცა, როგორც ჰონგ-კონგის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო აღნიშნავს, მომხმარებლები არ არიან დამუშავების პროცესზე საკმარისად ინფორმირებულნი. მათ არ გააჩნიათ საკუთარი მონაცემების დამუშავების პროცესების მართვისა და კონტროლის შესაძლებლობა, შედეგად მომხმარებელთა უმეტესობამ არც იცის აღნიშნული პარამეტრის არსებობის შესახებ.

ჰონგ-კონგის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს განმარტებით, მონაცემების დამუშავება ხორციელდება მომხმარებელთა აშკარად გამოხატული თანხმობის გარეშე. აღნიშნულის თაობაზე საზედამხედველო ორგანომ ოფიციალური შეტყობინებით მიმართა “LinkedIn”-ს, რომლის საპასუხოდ კომპანიამ ჰონგ-კონგში მყოფი მომხმარებლების პერსონალურ მონაცემთა ამ მიზნით დამუშავება დროებით შეაჩერა. აღსანიშნავია, რომ მონაცემთა დამუშავება დროებით შეჩერდა ევროპის ეკონომიკურ ზონაში მყოფ ქვეყნებში, გაერთიანებულ სამეფოში, შვეიცარიასა და ჰონგ-კონგში. ჰონგ-კონგის საზედამხედველო ორგანო მიესალმა ამ ცვლილებას. მან ასევე მოუწოდა “LinkedIn”-ის მომხმარებლებს, რომ ხელახლა გაცნობოდნენ პლატფორმაზე მიმდინარე კონფიდენციალობის პოლიტიკის ცვლილებებს და ხელოვნურ ინტელექტზე დამოკიდებული სერვისებით სარგებლობისას, არ გამოეყენებინათ მათი პერსონალური მონაცემები.

საგულისხმოა, რომ “LinkedIn”-ის მიერ ხელოვნური ინტელექტის სწავლების მიზნით პერსონალური მონაცემების დამუშავების შეჩერების სურვილის შემთხვევაში, მომხმარებელს შეუძლია, რომ პლატფორმის პარამეტრების მეშვეობით, სექციაში „მონაცემთა კონფიდენციალობა“ (“Data privacy”) მოახდინოს დეაქტივაცია ფუნქციისა: „მონაცემები გენერირებადი ხელოვნური ინტელექტის გაუმჯობესებისთვის“ (“Data for generative AI improvement”).

გამოყენებული წყაროები:
LinkedIn and Generative AI (GAI) FAQs, <https://www.linkedin.com/help/linkedin/answer/a5538339?hcppcid=search> [23.10.2024].

*Updates to LinkedIn's Terms of Service, <**https://www.linkedin.com/blog/member/trust-and-safety/updates-to-our-terms-of-service-2024**> [23.10.2024].*

LinkedIn suspends collecting Hong Kong users’ data for GenAI: privacy watchdog, <https://www.scmp.com/news/hong-kong/society/article/3282452/linkedin-suspends-collecting-hong-kong-users-data-genai-privacy-watchdog> [23.10.2024].

LinkedIn users alert: your data helps train AI models, <https://www.thestandard.com.hk/section-news/section/15/266700/LinkedIn-users-alert:-your-data-helps-train-AI-models> [23.10.2024].

LinkedIn suspends collecting Hong Kong users’ data for GenAI: privacy watchdog, <https://www.scmp.com/news/hong-kong/society/article/3282452/linkedin-suspends-collecting-hong-kong-users-data-genai-privacy-watchdog> [23.10.2024].

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