პერსონალურ მონაცემთა
დაცვის სამსახური

მსოფლიო პრაქტიკა

თებერვალი / 2023

მთავარი სიახლეები

ციფრული სერვისებით სარგებლობისას ბავშვის ასაკის დადასტურების მეთოდების მნიშვნელობა

ნიდერლანდების სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ როტერდამის პოლიციას 50 000 ევროს ოდენობით ჯარიმა დააკისრა

“ICO”-მ დაადგინა, თუ რა შემთხვევაშია შინაური ცხოველის სახელი პიროვნების პერსონალური მონაცემი

ჰოლანდიის საზედამხედველო ორგანომ “Tesla”-ს მანქანებში ძარცვისა და ვანდალიზმისგან დაცვის სისტემის მიერ მონაცემთა დამუშავების კანონიერება შეისწავლა

ნიდერლანდების სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ როტერდამის პოლიციას 50 000 ევროს ოდენობით ჯარიმა დააკისრა

08.02.2023

ფოტო: gdprhub.eu

ნიდერლანდების სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ როტერდამის პოლიციას კამერით აღჭურვილი ავტომობილების გამოყენებისთვის 50 000 ევროს ოდენობით ჯარიმა დააკისრა. კამერით აღჭურვილი ავტომობილების გამოყენების მიზანს კორონავირუსთან დაკავშირებულ ღონისძიებებთან შესაბამისობის მონიტორინგი წარმოადგენდა. თუმცა, მონაცემთა დამუშავებამდე პოლიციამ პირადი ცხოვრების ხელშეუხებლობის თანმდევი რისკები არ შეაფასა. ფაქტობრივი გარემოებების მიხედვით, ავტომობილები მოძრაობისას აგროვებდნენ და ინახავდნენ ადამიანების დეტალურ ფოტოსურათებს.

საზედამხედველო ორგანოს მიერ ჩატარებული შემოწმების შედეგად, ასევე, გამოვლინდა, რომ საკმაოდ ბევრი ფოტოსურათი საჭიროების გარეშე შეგროვდა. მიუხედავად ამისა, საზედამხედველო ორგანომ ამ დარღვევისთვის პოლიციას ჯარიმა ვერ დააკისრა.

საზოგადოების მონიტორინგი

COVID-19-ის პანდემიის კონტექსტში, 2020 წელს, ხუთი კვირის განმავლობაში, როტერდამის მუნიციპალიტეტი და პოლიცია იყენებდა ორ ავტომობილს, რომელიც აღჭურვილი იყო 360 გრადუსიანი კამერებით. მათი საშუალებით ხორციელდებოდა საზოგადოების მიერ 1,5 მეტრიანი დისტანციის დაცვის მონიტორინგი. გარდა ამისა, 50 კმ/სთ-ში მოძრაობისას კამერებით შესაძლებელი იყო უშუალოდ ავტომობილების სიახლოვეს მყოფ ინდივიდთა იდენტიფიცირებისათვის საჭირო, საკმაოდ მკაფიო და დეტალური ფოტოსურათების გადაღება.

შეგროვებული ფოტოსურათების დათვალიერება, შენახვა და პოლიციის სხვა ლოკაციებზე გადაგზავნა საკონტროლო ცენტრიდან ხორციელდებოდა. სამართლებრივი თვალსაზრისით, ეს სურათები პოლიციის მიერ დამუშავებულ მონაცემებად მიიჩნეოდა, შესაბამისად, პასუხისმგებელი თავად იყო.

2020 წლის მაისში, საზედამხედველო ორგანომ კამერით აღჭურვილი ავტომობილების გამოყენებასთან დაკავშირებით ახსნა-განმარტება მოითხოვა, რის შემდეგაც მანქანებით სარგებლობა შეჩერდა. თუმცა მათი კვლავ გამოყენების თაობაზე ინფორმაციის მიღების შემდეგ, საზედამხედველო ორგანომ შემოწმება დაიწყო.

საზედამხედველო ორგანოს დასკვნების მიხედვით, კამერით აღჭურვილი ავტომობილების გამოყენება კანონს არღვევდა. საზედამხედველო ორგანომ დაადგინა, რომ არსებობდა განსხვავებული მოსაზრებები ასეთი ავტომობილების

გამოყენების სამართლებრივ საფუძვლებთან დაკავშირებით.

ფოტო: freepik.com

რისკების წინასწარ შეფასებასთან დაკავშირებული ხარვეზები

ფოტოსურათების გადაღებამდე, პოლიციამ წინასწარ არ ჩაატარა იმის შეფასება, თუ რა შესაძლო რისკები მოჰყვებოდა კამერით აღჭურვილი ავტომობილების გამოყენებას პირადი ცხოვრების ხელშეუხებლობის თვალსაზრისით. ამ ტიპის ანალიზი ცნობილია „მონაცემთა დაცვის ზეგავლენის შეფასების“ სახელწოდებით.

პოლიციას უნდა სცოდნოდა, რომ ამგვარი ავტომობილების გამოყენება პირადი ცხოვრების ხელშეუხებლობისთვის მნიშვნელოვან რისკს ქმნიდა, შესაბამისად, „მონაცემთა დაცვის ზეგავლენის შეფასება“ უნდა ჩატარებულიყო. ამასთან, აღსანიშნავია, რომ კამერებით სარგებლობით პოლიცია ახალ ტექნოლოგიას იყენებდა.

უფრო მეტიც, პოლიცია პერსონალური მონაცემების შეგროვებას საჯარო სივრცეში პირთა ფართო ჯგუფებისგანაც კი აპირებდა. მათ კი, სავარაუდოდ, ფოტოსურათების შეგროვების ფაქტის, მათი გამოყენების გზების შესახებ ინფორმაცია არ ექნებოდათ.

აღნიშნული ქმედებებით დაირღვა „პოლიციის მონაცემთა აქტი“, რომელიც პოლიციის მიერ პირადი ცხოვრების ხელშეუხებლობის დაცვის ძირითად წესებს ითვალისწინებს. პოლიციამ აღნიშნული დარღვევა აღიარა, შესაბამისად, მას 50 000 ევროს ოდენობით ჯარიმა დაეკისრა.

არაპროპორციული დამუშავება

აღსანიშნავია, რომ მაშინაც კი, როდესაც არ ფიქსირდებოდა კორონავირუსის წინააღმდეგ დაწესებული ისეთი ღონისძიებების დარღვევა, როგორიცაა — ჯგუფური შეკრებების აკრძალვა, რამდენიმე დღის განმავლობაში, კამერით აღჭურვილი ავტომობილები მაინც იღებდნენ პირთა იდენტიფიცირებად ფოტოსურათებს. უფრო მეტიც, ფოტოგადაღება გარდა დანიშნულების წერტილებისა, სხვა ადგილებშიც — ერთი ლოკაციიდან მეორეში გადაადგილების დროსაც კი განხორციელდა.

პოლიციამ შეაგროვა და შეინახა საკმაოდ ბევრი ფოტოსურათი, მიუხედავად იმისა, რომ აღნიშნული არ იყო აუცილებელი მისი საქმიანობის განსახორციელებლად. პოლიციამ ამ ნაწილშიც აღიარა მონაცემთა აქტის დარღვევა. მიუხედავად იმისა, რომ საზედამხედველო ორგანო ზედამხედველობს „პოლიციის მონაცემთა აქტის“ დაცვასა და მასთან შესაბამისობას, აღნიშნული დარღვევისთვის მას ჯარიმის დაკისრება არ შეეძლო.

კანონიერება

კამერით აღჭურვილი ავტომობილების გამოყენება პოლიციის აქტის მე-3 ნაწილის საფუძველზე განხორციელდა. როგორც ეს

საზედამხედველო ორგანოს გადაწყვეტილებაში აღინიშნა, არსებობს განსხვავებული შეხედულებები იმის თაობაზე, თუ რამდენად გამართლებულია კანონმდებლობის საფუძველზე კამერით აღჭურვილი ავტომობილების უფრო ხანგრძლივი პერიოდით გამოყენება. სწორედ ამიტომ, ამჟამად, საზედამხედველო ორგანო მუშაობს აღნიშნული დებულების სტანდარტის განმარტებაზე.

ჰოლანდიის საზედამხედველო ორგანომ “Tesla”-ს მანქანებში ძარცვისა და ვანდალიზმისგან დაცვის სისტემის მიერ მონაცემთა დამუშავების კანონიერება შეისწავლა

23.02.2023

ჰოლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ 2023 წლის 22 თებერვალს გამოაქვეყნა განცხადება “Tesla Inc.”-ის მიერ მანქანაში ჩაშენებული კამერების გამოყენების შესახებ. კერძოდ, საზედამხედველო ორგანომ აღნიშნა, რომ “Tesla”-მ შეცვალა ჩაშენებული უსაფრთხოების კამერების კონფიდენციალურობის პარამეტრები. შედეგად სისტემა მეტად ორიენტირებულია მონაცემთა დაცვაზე, რასაც წინ უძღვოდა ჰოლანდიის საზედამხედველო ორგანოს მიერ საკითხის შესწავლა. საზედამხედველო ორგანოს განმარტებით, “Tesla”-ს ე. წ. „საგუშაგო-რეჟიმი“ (“Sentry-Mode”), რომელიც მიზნად ისახავს ქურდობისა ან/და ვანდალიზმისგან დაცვას, 4 კამერით უწყვეტ რეჟიმში იღებდა ყველაფერს მანქანის ირგვლივ და ინახავდა 1 საათის ხანგრძლივობის ვიდეოჩანაწერს.

ფოტო: autoriteitpersoonsgegevens.nl

“Tesla”-ს მიერ პროგრამული უზრუნველყოფის განახლების შემდეგ, ე. წ. „საგუშაგო-რეჟიმის“ კამერები გამორთულია. იგი მომხმარებლის მიერ მისი ჩართვის შედეგად აქტიურდება და ინახავს მხოლოდ 10 წუთის ხანგრძლივობის ვიდეოჩანაწერს.

გარდა ამისა, ე. წ. „საგუშაგო-რეჟიმი“ მოქმედებებს ავტომობილთან მხოლოდ ფიზიკურად შეხების შემთხვევაში, შესაბამისად, კამერა არ იღებს ყველა „საეჭვო“ მოქმედებას. ამასთან, იგი უგზავნის შეტყობინებას მანქანის მფლობელს ან მესაკუთრეს.

ფოტო: frpfreeet.com

მანქანას, ასევე, შეუძლია ფოტოების გადაღება კამერით, თუმცა მხოლოდ მაშინ, როდესაც მომხმარებელი თავად გააქტიურებს აღნიშნულ ფუნქციას. ავტომობილის კამერებით გადაღებული ფოტოები მანქანის ეკრანზე აისახება. ასევე,

ავტომობილის ფარები იძლევა სპეციალურ გამაფრთხილებელ ნიშანს, რითაც იგი აცნობებს გარშემო მყოფ პირებს ფოტო ან ვიდეო გადაღების შესახებ. გადაღებული ფოტოები ინახება მხოლოდ ავტომობილის მიერ და არ ეგზავნება "Tesla"-ს.

ჰოლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ "Tesla"-ს არ დააკისრა პასუხისმგებლობა, ვინაიდან საკითხის შესწავლით დადგინდა, რომ მონაცემთა დამმუშავებელი არა "Tesla", არამედ ცალკეული ავტომობილის მფლობელი ან მესაკუთრეა.

საზედამხედველო ორგანოს განმარტებით, მანქანაში ჩაშენებული კამერების გამოყენებაზე ვრცელდება კერძო საკუთრების ვიდეო მეთვალყურეობასთან დაკავშირებული წესი. აღნიშნული გულისხმობს საჯარო სივრცეების გადაღების აკრძალვას, გარდა გამონაკლისი შემთხვევებისა, როდესაც პირი უფლებამოსილია კონკრეტული ლეგიტიმური მიზნის მისაღწევად (მაგალითად, უსაფრთხოებასთან დაკავშირებული სერიოზული საფრთხის არსებობის შემთხვევაში, ძარცვისგან თავდაცვა), საჯარო სივრცე ავტომობილში ჩაშენებული კამერებით გადაიღოს. ასეთ შემთხვევაში საზედამხედველო ორგანო დამმუშავებლის ვალდებულებად კამერების სწორად განთავსებასა და მესამე პირთა პირადი ცხოვრების დაცვას საზღვრავს.

"ICO"-მ დაადგინა, თუ რა შემთხვევაშია შინაური ცხოველის სახელი პიროვნების პერსონალური მონაცემი

17.02.2013

[დიდი ბრიტანეთის ინფორმაციის კომისიონერის ოფისმა ("ICO") იმსჯელა შინაური ცხოველის სახელის პერსონალურ მონაცემად მიჩნევის თაობაზე.]

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის ზოგადი რეგულაციის ("UK GDPR") თანახმად, პერსონალური მონაცემია ნებისმიერი ინფორმაცია, რომელიც ეხება ცოცხალ ინდივიდს, რომელიც იდენტიფიცირებულია ან იდენტიფიცირებადია აღნიშნული ინფორმაციის გამოყენებით. პერსონალურ მონაცემთა განმსაზღვრელი ამომწურავი განმარტება არ არსებობს და შესაბამისად, თითოეულ შემთხვევაში უნდა დადგინდეს, კონკრეტული მონაცემი ხდის თუ არა პირის ვინაობას იდენტიფიცირებულს ან იდენტიფიცირებადს. "ICO"-ს მიერ განხილული შემთხვევა წარმოაჩენს იმას, თუ რამდენად ფართედ შეიძლება, განიმარტოს პერსონალური მონაცემის ცნება. კერძოდ, "ICO"-მ მიიღო გადაწყვეტილება, რომლის თანახმად, ძაღლის სახელმა შეიძლება, გამოიწვიოს პიროვნების იდენტიფიცირება და შესაბამისად, იყოს პერსონალური მონაცემი.

საქმის ფაქტობრივი გარემოებები

განმცხადებელმა მოითხოვა ინფორმაცია ეივონისა და სომერსეტის რაიონული პოლიციის მიერ ელექტრონული მუსიკის თანხლებით მიმდინარე უკანონო თავყრილობის დაშლის დროს, პოლიციის

ძაღლის მიერ საზოგადოების წევრის სერიოზულად დაშავების ინციდენტზე.

ფოტო: istockphoto.com

“ICO”-ს მიერ განსახილველი საკითხი

“ICO”-ს უნდა ემსჯელა „ინფორმაციის თავისუფლების აქტითა“ (“FOIA”) და “UK GDPR”-ით დადგენილი უფლებების ურთიერთბალანსზე. ეივონისა და სომერსეტის რაიონულმა პოლიციამ მოთხოვნა შემდეგი ინფორმაციის გაცემაზე მიიღო:

- კონკრეტული ძაღლის სახელი, რომელმაც გამოიწვია დაზიანება;
- ძაღლის მეპატრონის სახელი;
- ძაღლის შესახებ საპოლიციო ჩანაწერები, შენიშვნები, ვარჯიშის ჩანაწერები და ა. შ.

ეივონისა და სომერსეტის რაიონულმა პოლიციამ უარი განაცხადა აღნიშნული ინფორმაციის გაცემაზე და მიუთითა „ინფორმაციის თავისუფლების აქტით“ დადგენილ გამონაკლისებზე, აგრეთვე, პერსონალურ მონაცემთა დაცვის ვალდებულებაზე, იმ მოტივით, რომ ინციდენტში მონაწილე ძაღლის სახელის გამჟღავნება ირიბად იდენტიფიცირებადს გახდიდა ძაღლის მესაკუთრეს. რაიონული პოლიციის განმარტებით, აღნიშნული ინფორმაცია “UK GDPR”-ის მე-3 მუხლის მე-2 პუნქტით გათვალისწინებული „პერსონალური მონაცემის“ დეფინიციას შეესაბამებოდა.

ფოტო: ico.org.uk

საზედამხედველო ორგანოს უნდა განესაზღვრა, ერთი მხრივ, წარმოადგენდა თუ არა ძაღლის სახელი პერსონალურ მონაცემს, ხოლო მეორე მხრივ — ყურადღება გაემახვილებინა კანონმდებლობით დადგენილი პერსონალური მონაცემების შინაარსზე; კერძოდ, აღნიშნული ინფორმაცია ეხება თუ არა პიროვნებას და რამდენად იწვევს იგი მის პირდაპირ ან ირიბად იდენტიფიცირებას.

“ICO”-ს გადაწყვეტილება

“ICO”-მ განმარტა, რომ მოთხოვნილი ინფორმაცია შეეხებოდა აღნიშნული ძაღლის პატრონს და რომ ინფორმაციის გაცემით შესაძლებელი იქნებოდა მისი ირიბად იდენტიფიცირება. საზედამხედველო ორგანომ დამატებით აღნიშნა, რომ გადაწყვეტილების მიღებისას უნდა შეფასდეს ყველა ის საშუალება, რომელიც ინდივიდის იდენტიფიცირებისათვის გონივრულია ან დიდი ალბათობით იქნება გამოყენებული. მოცემულ შემთხვევაში, რაიონულმა პოლიციამ განაცხადა, რომ ძაღლის სახელის ინტერნეტ ძიების შედეგად, შესაძლებელია მისი მეპატრონის სახელის დადგენა, რაც ასევე დაადასტურა “ICO”-მ.

დასკვნა

იქიდან გამომდინარე, რომ მხოლოდ ძაღლის სახელის გამოყენებით იყო შესაძლებელი მისი მეპატრონის — „ცოცხალი ინდივიდის“, იდენტიფიცირება, “ICO”-მ მართებულად მიიჩნია რაიონული პოლიციის გადაწყვეტილება ძაღლის სახელის პერსონალურ მონაცემად მიჩნევის თაობაზე.

საზედამხედველო ორგანომ ასევე განმარტა, რომ მაშინაც კი, თუ ძაღლის სახელი არ იქნებოდა საჯარო დომეინში ძებნადი, პოლიციის თანამშრომლებს ძაღლის სახელის მარტოოდენ გაჟღერებითაც ექნებოდათ შესაძლებლობა, განესაზღვრათ, თუ ვინ იყო ცხოველის მეპატრონე. ამასთანავე, აღინიშნა, რომ ძაღლთან დაკავშირებული სხვა ინფორმაცია (წვრთნის შესახებ, მისი საპოლიციო ჩანაწერები) არ იძლეოდა ცხოველის მეპატრონის იდენტიფიცირების შესაძლებლობას და შესაბამისად, არ წარმოადგენდა პერსონალურ მონაცემს.

მოცემულ შემთხვევაში “ICO”-ს შეხედულება კონკრეტულ ფაქტებს ემყარებოდა. მას არ დაუდგენია, რომ შინაური ცხოველის სახელი ავტომატურად პერსონალური მონაცემია. გადაწყვეტილებაში აღნიშნულია, რომ ინფორმაციის პერსონალურ მონაცემად დადგენა არ საჭიროებს პიროვნების მხოლოდ პირდაპირ იდენტიფიცირებას; ინფორმაციის პერსონალურ მონაცემად მიჩნევის საფუძველს შეიძლება, პირის ირიბი იდენტიფიკაციაც წარმოადგენდეს. შესაბამისად, თუ ინფორმაცია არა მხოლოდ შეეხება ინდივიდს, არამედ შესაძლებელს ხდის მის იდენტიფიცირებას, არსებობს იმის ალბათობა, რომ იგი პერსონალური მონაცემია.

“ICO”-ს განმარტებით, პერსონალური მონაცემის შინაარსი ყოველთვის უნდა განისაზღვროს კონკრეტული გარემოებების საფუძველზე. განსახილველ შემთხვევაში ცხოველის სახელი იყო უნიკალური და ასევე იყო ცნობილი, რომ ძაღლის მეპატრონე ეივონისა და სომერსეტის რაიონულ პოლიციაში მუშაობდა. შესაბამისად, ძაღლის სახელის გამჟღავნება მეპატრონის ვინაობას ხდიდა არაპირდაპირ იდენტიფიცირებადს.

ციფრული სერვისებით სარგებლობისას ბავშვის ასაკის დადასტურების მეთოდების მნიშვნელობა

15.02.2023

ბავშვები ინტერნეტის ერთ-ერთი ყველაზე მოწყვლადი მომხმარებლები არიან და მათი დაცვა ციფრულ სამყაროში უდიდესი გამოწვევაა. ციფრული საშუალებების გამოყენებისას ბავშვის ასაკის დადასტურების სხვადასხვა მეთოდი არსებობს. [ევროპარლამენტის ვებგვერდზე გამოქვეყნებული კვლევა სწორედ ამ საკითხს შეისწავლის სუპრანაციონალურ დონეზე.]

European Parliament

ფოტო: www.centre.europarl.europa.eu

ერთ-ერთი კვლევის[1] თანახმად, ციფრულ სერვისებს არ აქვთ შესაბამისი ასაკის ვერიფიკაციის ან მშობლის თანხმობის გაცემის აპრობირებული მეთოდები. აღნიშნული კი გასულ წელს გახდა „ინსტაგრამის“ რეკორდული თანხით დაჯარიმების საფუძველი.

ინტერნეტ სივრცეში ასაკის ვერიფიკაციის ძირითადი მეთოდებია:

- *თვითგანაცხადი* (“Self-declaration”) — აღნიშნული მეთოდი არასრულწლოვნებისთვის საკმაოდ მარტივად არის დაძლევადი. მაგალითად, მას შეუძლია, მიუთითოს მცდარი დაბადების წელი.
- *საკრედიტო ბარათი* — მომხმარებლებს მოეთხოვებათ, რომ საცდელად განახორციელონ ტრანზაქცია, გადახდა მინიმალური თანხის ოდენობით. აღნიშნული მეთოდი, უმეტესწილად, გამოიყენება ელექტრონული ვაჭრობის ვებგვერდებისა და აპლიკაციების მიერ, რომლებიც ზრდასრულებისთვის განკუთვნილი ნივთებით ვაჭრობაზე არიან ორიენტირებულნი. თუმცა, აღსანიშნავია, რომ ამ შემთხვევაში, საკრედიტო ბარათისთვის დადგენილი მინიმალური ასაკი განსხვავდება ქვეყნების მიხედვით.
- *ბიომეტრული მონაცემი* — ხელოვნური ინტელექტის გამოყენებით ბიომეტრული მონაცემების დამუშავება სულ უფრო აქტუალური ხდება. მაგალითად, სახის ამომცნობი აპლიკაციები სულ უფროდაუფრო დიდ გავრცელებას ჰპოვებს. სახის ამომცნობი სისტემის გამოყენებით შეიძლება, დადგინდეს, არის თუ არა პირი სრულწლოვანი. ამ შემთხვევაშიც შესაძლოა, არასრულწლოვანმა გამოიყენოს სხვა, სრულწლოვანი პირის გამოსახულება იმისათვის, რომ მიიღოს კანონით აკრძალული დაშვება. ამასთან, პერსონალური მონაცემების დაცვის თვალსაზრისით, აღსანიშნავია, რომ სახის იდენტიფიცირება და ბიომეტრული მონაცემების გამოყენება წარმოადგენს განსაკუთრებული კატეგორიის პერსონალურ მონაცემს, რომელიც მომეტებულ დაცვას საჭიროებს.
- *მშობლის თანხმობა* — არსებობს რიგი აპლიკაციები და მომსახურებათა კატეგორიები, რომლებიც მოითხოვს მშობლის დასტურს, რათა არასრულწლოვანმა შეძლოს ციფრული სერვისის მიღების მიზნით რეგისტრაცია. მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობის მეთოდად შეიძლება, განისაზღვროს პირადობის დამადასტურებელი დოკუმენტების შემოწმება.
- *გარანტია* — აღნიშნული მეთოდიც მოიაზრებს მომხმარებლის მიერ ბავშვის ასაკის დადასტურებას. თუმცა, აღსანიშნავია, რომ პირი, ვინც ასაკს ადასტურებს, არ წარმოადგენს არასრულწლოვნის მშობელს ან კანონიერ წარმომადგენელს.
- *ციფრული ID* — აღნიშნული გულისხმობს ციფრულ სერვისებზე წვდომის მიღებამდე, არასრულწლოვანი პირის ასაკის იდენტიფიცირებისთვის სახელმწიფოს მიერ სხვადასხვა ცალკეული მეთოდების შემუშავებას.

[1] *Hof S., Ouburg S.,* 'We Take Your Word For It' — A Review of Methods of Age Verification and Parental Consent in Digital Services, EDPLR, Vol. 8(1), 2022.

მაგალითად, ჩინეთი, კანადა და ავსტრალია იყენებენ ამ მეთოდს. ასევე, არსებობს მოსაზრება, რომ ევროკავშირის მასშტაბით შეიქმნას „ევროპული ციფრული საიდენტიფიკაციო საფულე“ (“European Digital Identity Wallet”).

- *ასაკის დადასტურება სპეციალური აპლიკაციის გამოყენებით* — საფრანგეთში გარკვეული ტიპის ინფორმაციაზე წვდომის მოსაპოვებლად, მომხმარებლებს მალე დაუწესდებათ ვალდებულება, გადმოწერონ სახელმწიფოს მიერ ლიცენზირებული ციფრული სერტიფიცირების აპლიკაცია.

ფოტო: www.freepik.com

ცალკეულ გამოწვევებთან გასამკლავებლად, ევროკავშირის დონეზე უკვე განხორციელდა რიგი აქტივობები. უპირველეს ყოვლისა, აღსანიშნავია, მონაცემთა დაცვის ზოგადი რეგულაცია (“GDPR”), რომელიც მოითხოვს ასაკის დადასტურების მექანიზმების გამოყენებას და მშობლის თანხმობას. ევროკავშირის დონეზე შემუშავებული სისტემის მეშვეობით — “EU eID Proposal” კომისია მიზნად ისახავს ასაკის დადასტურების მეთოდების გაძლიერებას. აგრეთვე, არსებობს ევროკავშირის მიერ თანადაფინანსებული პროექტი “euCONSENT”, რომელიც ასევე გამიზნულია ასაკის დადასტურების ერთიანი სისტემის შემუშავებისკენ.

ევროკავშირის მონაცემთა დაცვის ზედამხედველმა (“EDPS”) მგზავრების შესახებ ინფორმაციის წინასწარი შეგროვებისა და გადაცემის (“API”) რეგულაციების თაობაზე მოსაზრება გამოაქვეყნა

08.02.2023

ფოტო: edps.europa.eu

2023 წლის 8 თებერვალს, ევროკავშირის მონაცემთა დაცვის ზედამხედველმა (“EDPS”) „მგზავრების შესახებ ინფორმაციის წინასწარი შეგროვებისა და გადაცემის“ (“API”) რეგულაციებთან დაკავშირებით, ევროპული კომისიის მიერ შეთავაზებული ორი საკანონმდებლო წინადადების საპასუხოდ, მოსაზრება გამოაქვეყნა. მგზავრების შესახებ ინფორმაციაში იგულისხმება სამოგზაურო დოკუმენტებში ასახული პერსონალური მონაცემები (პასპორტი ან პირადობის დამადასტურებელი მოწმობა), რომლებიც რეგისტრაციის პროცესში გროვდება.

ევროპული კომისიის მიერ შემუშავებული საკანონმდებლო წინადადებების მიზანს წარმოადგენდა:

- ეფექტიანი სასაზღვრო კონტროლის უზრუნველყოფა და არალეგალურ მიგრაციასთან ბრძოლა;
- ტერორისტული და მძიმე დანაშაულების პრევენცია, გამოვლენა, გამოძიება და დამნაშავეთა დასჯა.

"EDPS"-ის მოსაზრებაში ყურადღებაა გამახვილებული სამართალდამცავი მიზნებისთვის ევროკავშირის წევრ სახელმწიფოთა შორის მგზავრების შესახებ ინფორმაციის გადაცემის აუცილებლობასა და პროპორციულობაზე. კერძოდ, შეფასებულია ევროპული კომისიის მიერ წარდგენილი წინადადებების შესაბამისობა „მგზავრის პირადი მონაცემების შესახებ" ("PNR") დირექტივასა და ევროკავშირის მართლმსაჯულების სასამართლოს ("CJEU") გადაწყვეტილებასთან.

ფოტო: flaticon.com

"PNR" დირექტივა ადგენს მგზავრთა მონაცემების შეგროვებასთან დაკავშირებით წესებს, რომელთა მიზანია ტერორიზმთან და საერთაშორისო დანაშაულთან ბრძოლა. აღნიშნული დირექტივის თაობაზე "CJEU"-ის მიერ მიღებული გადაწყვეტილების თანახმად, მძიმე დანაშაულისა და ტერორიზმთან ბრძოლის მიზნებისთვის, ევროკავშირის წევრ სახელმწიფოებს შეუძლიათ, დაამუშაონ ევროკავშირის ფარგლებში პირთა მოგზაურობასთან დაკავშირებული მონაცემები. განსხვავებით "PNR" მონაცემებისგან, "API" მონაცემები არ წარმოადგენს პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა დაცვის უფლებაში უხეშ ჩარევას. თუმცა, ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის თანახმად, მათ შორის, თავისუფალი გადაადგილების უფლების გათვალისწინებით, "API" მონაცემების დამუშავება უნდა შეიზღუდოს მკაცრი საჭიროებით. ამ თვალსაზრისით მნიშვნელოვანია, რომ ევროკავშირის კანონმდებლობა იყოს ნათელი და გასაგები.

შემუშავებულ დოკუმენტში "EDPS"-ის ზედამხედველი მოუწოდებს კანონმდებლებს გაითვალისწინონ შემდეგი რეკომენდაციები:

- "CJEU"-ს გადაწყვეტილების შესაბამისად, შემუშავდეს ჰარმონიზებული კრიტერიუმები და მეთოდოლოგია, რათა განისაზღვროს პირთა "API" მონაცემების შეგროვების საფუძველი;
- გაძლიერდეს უსაფრთხოების ზომები მონაცემთა დაცვის დამატებითი გარანტიების გამოყენებით, მაგალითად, როგორიცაა ფსევდონიმიზაცია ან მონაცემების დაშიფვრა;
- წაიშალოს პერსონალური მონაცემები, თუკი ტექნიკური მიზეზებით ვეღარ ხორციელდება კომპეტენტური ორგანოსთვის მათი გადაცემა.

მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”) 3 სახელმძღვანელო დოკუმენტი გამოაქვეყნა

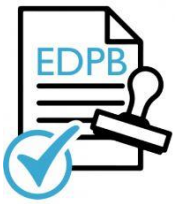
24.02.2023

ფოტო: edpb.europa.eu

2023 წლის 24 თებერვალს, მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”), პერსონალურ მონაცემთა დაცვის აქტუალური საკითხების შესახებ საჯარო კონსულტაციების ჩატარების შედეგად, 3 სახელმძღვანელო დოკუმენტი გამოაქვეყნა:

👉 სახელმძღვანელო “GDPR”-ის მე-3 მუხლისა და მე-5 თავის („დებულებები საერთაშორისო გადაცემის შესახებ“) გამოყენების თაობაზე: სახელმძღვანელოში განმარტებულია “GDPR”-ის მე-3 მუხლსა და მონაცემთა საერთაშორისო გადაცემის შესახებ მე-5 თავს შორის ურთიერთმიმართება ტერიტორიული დაფარვის თვალსაზრისით. დოკუმენტი მონაცემთა დამმუშავებლებსა და უფლებამოსილ პირებს ეხმარება: დაადგინონ დამუშავების ოპერაცია მოიცავს თუ არა საერთაშორისო გადაცემას; ასევე, განსაზღვრონ „საერთაშორისო გადაცემის“ ცნების ერთიანი გაგება. საჯარო კონსულტაციების გამართვის შემდეგ, სახელმძღვანელო განახლდა და მასში დამატებითი განმარტებები აისახა, კერძოდ, დამმუშავებლის პასუხისმგებლობის შესახებ, როდესაც მონაცემთა გადამცემი არის უფლებამოსილი პირი. ამასთან, მონაცემთა პირდაპირი შეგროვების ასპექტების განსამარტავად, დოკუმენტი ითვალისწინებს რიგ პრაქტიკულ მაგალითებს.

👉 სახელმძღვანელო სერტიფიცირების, როგორც მონაცემთა გადაცემის ინსტრუმენტის შესახებ: სახელმძღვანელოს ძირითადი მიზანია მონაცემთა გადაცემის ინსტრუმენტის პრაქტიკული გამოყენების თაობაზე დამატებითი განმარტების ჩამოყალიბება. დოკუმენტი შედგება 4 ნაწილისგან, რომელთაგან თითოეული შეეხება სერტიფიცირების, როგორც გადაცემის საშუალებების სპეციფიკურ მახასიათებლებს. სახელმძღვანელო ავსებს სერტიფიცირების შესახებ 1/2018 გაიდლაინებს, რომელშიც წარმოდგენილია შედარებით ზოგადი მითითებები. საჯარო კონსულტაციების შედეგად დოკუმენტი განახლდა და მასში აისახა შესაბამისი კომენტარები.



ფოტო: edpb.europa.eu

👉 სახელმძღვანელო სოციალური მედიის პლატფორმების მანიპულაციურ დიზაინთან დაკავშირებით: დოკუმენტში წარმოდგენილია პრაქტიკული რეკომენდაციები სოციალური მედიის პლატფორმების შემქმნელებისა და მომხმარებელთათვის, კერძოდ, თუ როგორ უნდა შეაფასონ და თავიდან აირიდონ სოციალური მედიის ინტერფეისში მანიპულაციური დიზაინის მქონე შაბლონები, რომლებიც არღვევს “GDPR”-ის

მოთხოვნებს. ასევე, მოცემულია: შეცდომაში შემყვანი დიზაინის კონკრეტული მაგალითები; სხვადასხვა შემთხვევებთან დაკავშირებით საუკეთესო პრაქტიკა; მომხმარებლის ინტერფეისების შემქმნელებისთვის რეკომენდაციები, რომელთა მიზანია "GDPR"-ის ეფექტიანი განხორციელება. აღსანიშნავია, რომ საჯარო კონსულტაციების შედეგად მიღებული დოკუმენტის საბოლოო ვერსიაში განახლდა კონკრეტული წინადადებების ფორმულირება და ცალკეული განმარტებები.

ხელოვნური ინტელექტი: იტალიის მონაცემთა დაცვის საზედამხედველო ორგანო ჩათბოტ "Replika"-ს დროებით შეზღუდვას უწესებს, რადგან იგი მაღალი რისკის შემცველია ბავშვებისთვის და ემოციურად დაუცველი პირებისთვის

03.02.2023

ფოტო: chatlayer.ai

ხელოვნური ინტელექტის მქონე ჩათბოტი, რომელიც ტექსტური და ვიდეო ინტერფეისების გამოყენებით „ვირტუალურ მეგობარს" ქმნის, იტალიის მონაცემთა დაცვის საზედამხედველო ორგანო — "Garante"-ს გადაწყვეტილებით, უკვე ვეღარ შეძლებს იტალიელი მომხმარებლების პერსონალური მონაცემების დამუშავებას. მონაცემთა დამუშავების თაობაზე დროებითი შეზღუდვა იტალიის მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ აშშ-ში დაფუძნებული კომპანიის — "Luka Inc."-ის მიმართ დაწესდა, რომელიც არის აპლიკაციის შემქმნელი და მმართველი.

ბოლოდროინდელმა ცნობებმა და საზედამხედველო ორგანოს მიერ ჩათბოტ "Replika"-ზე ჩატარებულმა შემოწმებებმა ცხადყო, რომ აპლიკაცია არსებითი რისკების შემცველია, უპირველეს ყოვლისა, ბავშვებისთვის. „ვირტუალურ მეგობარს" შეუძლია, გააუმჯობესოს მომხმარებლების ემოციური მდგომარეობა, დაეხმაროს საკუთარი აზრების შეცნობაში, სტრესის მართვაში, შფოთვითი აშლილობასთან გამკლავებაში. აღნიშნული მახასიათებლები იწვევს პიროვნების განწყობასთან ურთიერთქმედებას და შეიძლება, შეიცავდეს გარკვეულ რისკებს იმ პირებისთვის, რომლებიც ჯერ კიდევ არ არიან ზრდასრულ ასაკში ან არიან ემოციურად დაუცველნი. აპლიკაციაში, რეალურად, არ არსებობს ასაკის ვერიფიკაციის რაიმე მექანიზმი. ანგარიშის შექმნის ეტაპზე პლატფორმა ითხოვს მხოლოდ მომხმარებლის სახელის, ელექტრონული ფოსტისა და სქესის მითითებას. ხოლო მაშინ, როდესაც ბავშვი აფიქსირებს, რომ იგი არასრულწლოვანია, აპლიკაციას არ გააჩნია მექანიზმი, რომელიც შეზღუდავს მის გამოყენებას. ჩათბოტის მიერ გენერირებული პასუხები მომხმარებლების კითხვებზე კი, ხშირ შემთხვევაში, წინააღმდეგობაში მოდის იმ

მთავარ პრინციპებთან, რომლებიც ჩათბოტს გააჩნია. როგორც ეს კვლევის შედეგად დადგინდა, მომხმარებლები გამოხატავენ უკმაყოფილებას, რადგან, ხშირად, პლატფორმა უხამსი პასუხებით შემოიფარგლება.

იტალიის მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ ჩათბოტი “Replika” არღვევს ევროკავშირის მონაცემთა დაცვის ზოგად რეგულაციას (“GDPR”): იგი არ შეესაბამება გამჭვირვალობის მოთხოვნებს და უკანონოდ ამუშავებს პერსონალურ მონაცემებს. აღნიშნული გამომდინარეობს იქიდან, რომ იტალიური კანონმდებლობის თანახმად, ბავშვებს არ შეუძლიათ, იყვნენ ხელშეკრულების მხარეები.

აშშ-ში დაფუძნებულ დეველოპერს — “Luka Inc.”-ს დაევალა, შეწყვიტოს იტალიელი მომხმარებლების მონაცემების დამუშავება და 20 დღის განმავლობაში აცნობოს იტალიის მონაცემთა დაცვის საზედამხედველო ორგანოს მიღებული გადაწყვეტილების შესასრულებლად განხორციელებული ღონისძიებების შესახებ; წინააღმდეგ შემთხვევაში, საზედამხედველო ორგანო კომპანიას განუსაზღვრავს ჯარიმას 20 მილიონ ევრომდე ოდენობით, რაც კომპანიის მთლიანი წლიური ბრუნვის 4%-ს შეადგენს.

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