პერსონალურ მონაცემთა დაცვის სამსახური

მსოფლიო პრაქტიკა

აგვისტო / 2023

მთავარი სიახლეები

„პირადი ცხოვრების ხელშეუხებლობის უფლების ჯგუფმა“ (“NOYB”) ავიაკომპანია “Ryanair”-ის წინააღმდეგ საჩივარი შეიტანა

ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანო კრძალავს “Yango” ტაქსის მიერ პერსონალური მონაცემების ფინეთიდან რუსეთში გადაცემას

სოციალური ქსელი “X” ბიომეტრული მონაცემებისა და დასაქმების ისტორიის შეგროვებას იწყებს

„გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ“ (“ICO”) დასაქმებულ პირთა ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების თაობაზე სახელმძღვანელო რეკომენდაცია გამოაქვეყნა

„პირადი ცხოვრების ხელშეუხებლობის უფლების ჯგუფმა“ (“NOYB”) ავიაკომპანია “Ryanair”-ის წინააღმდეგ საჩივარი შეიტანა

10.08.2023

ფოტო: flightglobal.com

„პირადი ცხოვრების ხელშეუხებლობის უფლების ჯგუფმა“ (“NOYB”), მომხმარებელთა პერსონალური მონაცემების სავარაუდო დარღვევის გამო, მსოფლიოს ყველაზე დიდი ავიაკომპანია “Ryanair”-ის წინააღმდეგ ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანოში საჩივარი შეიტანა.[1] „პირადი ცხოვრების ხელშეუხებლობის უფლების ჯგუფს“ ხელმძღვანელობს მაქს შრემსი[2] — პირადი ცხოვრების ხელშეუხებლობის ავსტრიელი აქტივისტი.

საჩივრის წარდგენის მიზეზს ტურისტული სააგენტოს მეშვეობით, ავიარეისის დაჯავშნის დროს ავიაკომპანიის მიერ პირთა იდენტიფიკაციის მიზნით, სახის ამომცნობი ტექნოლოგიის გამოყენება წარმოადგენდა. მოსარჩელე იყო ერთ-ერთი მომხმარებელი, რომელიც ესპანეთში არსებული ტურისტული კომპანიის დახმარებით ჯავშნიდა რეისს.

ავიაკომპანიის პოზიციის თანახმად, იდენტიფიკაციის პროცესი გამართლებული იყო უსაფრთხოების მოთხოვნების დაცვის უზრუნველსაყოფად. ასევე აღინიშნა, რომ ტურისტული სააგენტოები, ხშირ შემთხვევაში, არ აზიარებენ მომხმარებლების საკონტაქტო და გადახდასთან დაკავშირებულ ინფორმაციას და ამდენად, არსებობდა პირის ვინაობის გადამოწმების საჭიროება.

მგზავრებს, ერთი მხრივ, შეუძლიათ გამგზავრებამდე 2 საათით ადრე გამოცხადება ან ფორმის წინასწარ წარდგენა, რომელიც მოიცავს პასპორტს ან პირადობის დამადასტურებელ მოწმობას შესაბამის სურათთან ერთად. თუმცა, აღნიშნული პროცესი შეიძლება გაგრძელდეს 7 დღემდე. აღსანიშნავია, რომ ამ პროცედურის გავლა არ არის აუცილებელი, როდესაც დაჯავშნა პირდაპირ “Ryanair”-ის ვებგვერდისა ან

[1] GDPRbuzz, <https://gdprbuzz.com/news/privacy-group-challenges-ryanairs-use-of-facial-recognition/>, [10.08.2023].

[2] IAPP, < https://iapp.org/resources/article/max-schrems/>, [10.08.2023].

მობილური აპლიკაციის გამოყენებით ხორციელდება.

„პირადი ცხოვრების ხელშეუხებლობის უფლების ჯგუფი“ ამტკიცებს, რომ “Ryanair”-ი არღვევს მომხმარებლის მონაცემთა დაცვის უფლებებს, რათა მოიპოვოს უპირატესობა ალტერნატიული დაჯავშნის საშუალებებთან მიმართებით. დამატებით აღსანიშნავია, რომ იდენტობის დამადასტურებელი პროცედურა არ არის “GDPR”-თან შესაბამისობაში, რადგან ავიაკომპანია ვერ ასახელებს აღნიშნული „ინვაზიური“ პროცესის განსახორციელებლად შესაბამის მიზანს. მეორე მხრივ, ავიაკომპანია აცხადებს, რომ მისი ბიომეტრული და არაბიომეტრული პროცესები “GDPR”-ით დადგენილ მოთხოვნებს სრულად ითვალისწინებს.

„გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ“ (“ICO”) დასაქმებულ პირთა ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების თაობაზე სახელმძღვანელო რეკომენდაცია გამოაქვეყნა

31.08.2023

ფოტო: ico.org.uk

2023 წლის 31 აგვისტოს, „გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ“ (“ICO”) სახელმძღვანელო რეკომენდაცია გამოაქვეყნა, რომელიც დასაქმებული პირების ჯანმრთელობის შესახებ პერსონალური მონაცემების დამუშავებას შეეხება.[3]

დოკუმენტის მიზანია დასაქმებულ პირთა ჯანმრთელობასთან დაკავშირებული მონაცემის დამუშავებისას დამსაქმებლების დახმარება, რათა

[3] ICO, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/information-about-workers-health-1-0.pdf>, [10.08.2023].

გაიაზრონ მონაცემთა დაცვასთან დაკავშირებული ვალდებულებები “UK GDPR”-ის და „მონაცემთა დაცვის აქტის“ (“DPA 2018”) შესაბამისად. ჯანმრთელობის მდგომარეობის თაობაზე დასაქმებულების პერსონალური მონაცემის დამუშავების სენსიტიურობიდან გამომდინარე, “ICO”-მ მიზანშეწონილად მიიჩნია აღნიშნული მიმართულებით შესაბამისი განმარტებების გაკეთება.

სახელმძღვანელო შედგება ორი ძირითადი ნაწილისგან. პირველი ნაწილი მოიცავს მიმოხილვას დასაქმებული პირების ჯანმრთელობის შესახებ ინფორმაციის დამუშავებისას მონაცემთა დაცვის კანონმდებლობის გამოყენების თაობაზე. აღნიშნულის ფარგლებში ყურადღება გამახვილებულია მონაცემთა დაცვის პრინციპებსა და საფუძვლებზე. მეორე ნაწილში განხილულია ჯანმრთელობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების შესახებ ზოგადი პრაქტიკა. ამ თვალსაზრისით, წარმოდგენილია კანონმდებლობით გათვალისწინებული მოთხოვნები, ასევე, პრაქტიკული რჩევები. ამასთანავე, დოკუმენტში წარმოდგენილია დამსაქმებლების მიერ გასათვალისწინებელი პუნქტები (“Checklists”), რათა ჯეროვნად იქნას დასაქმებულის პერსონალური მონაცემები დაცული.

“UK GDPR”-ით მოწესრიგებულია პერსონალური ინფორმაციის შეგროვებასა და გამოყენებასთან დაკავშირებული პრინციპები, მათ შორის, ჯანმრთელობის მდგომარეობის შესახებ. “UK GDPR”-ის მე-4 მუხლის მიხედვით, პერსონალური მონაცემები განიმარტება როგორც ინფორმაცია, რომელიც უკავშირდება ინდივიდის ფიზიკურ ან მენტალურ ჯანმრთელობას, აგრეთვე, ჯანდაცვის მომსახურებას, რომლის მეშვეობით იდენტიფიცირებადია პირის ჯანმრთელობის სტატუსი.

საზედამხედველო ორგანოს აღნიშვნით, ჯანმრთელობასთან დაკავშირებული ინფორმაციის კანონიერი დამუშავების მიზნით, “UK GDPR”-ის მე-6 მუხლის შესაბამისად უნდა განისაზღვროს დამუშავების საფუძველი. ვინაიდან ჯანმრთელობის შესახებ ინფორმაცია არის განსაკუთრებული კატეგორიის მონაცემი, იგი საჭიროებს ეფექტიან დაცვას.

“ICO”-ს მიერ შემუშავებულ სახელმძღვანელოში წარმოდგენილია სხვადასხვა გარემოება, როდესაც დამსაქმებელი ამუშავებს დასაქმებულის ჯანმრთელობის თაობაზე პერსონალურ მონაცემს; აღნიშნული შეიძლება უკავშირდებოდეს:

- ჯანმრთელობასთან დაკავშირებული პრობლემების

ხაზგასასმელად კითხვარის შევსებას;

- ავადმყოფობის არარსებობის თაობაზე ფორმის წარდგენას;
- შეზღუდული ქმედუნარიანობის ან შრომისუუნაროობის შესახებ ინფორმაციას;
- დასაქმებულის მხედველობის ტესტის შედეგებს;
- ალკოჰოლისა და ნარკოტიკული საშუალებების მოხმარების დასადგენად ტესტის შედეგებს;
- ვაქცინაციისა და იმუნიზაციის სტატუსისა და ისტორიის შესახებ ჩანაწერებს;
- სამუშაოსთვის შესაფერის ფიზიკურ ფორმაში ყოფნის შედეგებს.

სახელმძღვანელოში დასაქმებულების ჯანმრთელობასთან დაკავშირებული პერსონალური ინფორმაციის დამუშავების კანონიერ საფუძვლებზეც არის ყურადღება გამახვილებული. უნდა არსებობდეს მინიმუმ ერთი საფუძველი, რათა დამუშავდეს ჯანმრთელობის შესახებ ინფორმაცია. ამასთანავე, არცერთი საფუძველი არის უპირატესი, უსაფრთხო ან უფრო მნიშვნელოვანი. საფუძვლის განსაზღვრა დამოკიდებულია კონკრეტულ მიზანზე და დასაქმებულების ჯანმრთელობის შესახებ ინფორმაციის დამუშავების კონტექსტზე. "ICO" რჩევით მიმართავს დამსაქმებლებს, რომ მათი დასაქმებული პირების ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავებამდე განსაზღვრონ კანონიერი საფუძველი.

ფოტო: flaticon.com

დამსაქმებელმა დასაქმებული პირის ჯანმრთელობასთან დაკავშირებული პერსონალური ინფორმაციის დამუშავებამდე უნდა გაითვალისწინოს შემდეგი ფაქტორები:

- ☑ წინასწარ განსაზღვრული მიზნის მისაღწევად აუცილებელია ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავება. არ არსებობს მიზნის მისაღწევად სხვა ნაკლებად „ინვაზიური" საშუალება;
- ☑ ჯანმრთელობასთან დაკავშირებული ინფორმაციის დასამუშავებლად არსებობს შესაბამისი კანონიერი საფუძვლები;
- ☑ თუ ვერ დადასტურდება, რომ დასაქმებული პირის თანხმობა მისი პერსონალური მონაცემების დასამუშავებლად არ არის ნამდვილი და თავისუფალი ნებით გაცემული, არ უნდა მოხდეს ინფორმაციის დამუშავება;
- ☑ აღრიცხულია თუ რა მონაცემები უნდა დამუშავდეს კონკრეტულ შემთხვევაში;

- ☑ ჯანმრთელობის შესახებ პერსონალური მონაცემების შეგროვება და გამოყენება არის ადეკვატური, შესაბამისი და აუცილებელი; არ შეიცავს იმაზე მეტ ინფორმაციას, ვიდრე საჭიროა მიზნის მისაღწევად;
- ☑ წინასწარ შემუშავებულია პერსონალური მონაცემების შენახვის პოლიტიკა და ვადა;
- ☑ ინფორმაცია ინახება ზუსტი ფორმით და საჭიროების შემთხვევაში ხდება მისი განახლება;
- ☑ ჯანმრთელობასთან დაკავშირებული მონაცემების დასაცავად მიღებულია უსაფრთხოების შესაბამისი ზომები.

ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანო კრძალავს “Yango” ტაქსის მიერ პერსონალური მონაცემების ფინეთიდან რუსეთში გადაცემას

10.09.2023

ფოტო: gdprbuzz.com

ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანომ გამოსცა ბრძანება “Yandex LLC”-სა და “Ridetech International B.V.”-ს მიმართ, რათა შეჩერდეს “Yango” ტაქსის სერვისის მიერ შეგროვებული ნებისმიერი მომხმარებლის პერსონალური მონაცემების რუსეთში გადაცემა და შეწყდეს შეგროვებული პერსონალური მონაცემების დამუშავება.[4] საქმის შემდგომი შესწავლის მიზნით, ფინეთის საზედამხედველო ორგანომ დროებითი ბრძანების აღსრულება 26 სექტემბრამდე გადადო.[5]

ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანოსთვის ცნობილი გახდა იმ საკანონმდებლო

[4] GDPRbuzz, <https://gdprbuzz.com/news/finnish-dpa-bans-yango-taxi-service-transfers-of-personal-data-from-finland-to-russia-temporarily/>, [10.09.2023].

[5] Office of the Data Protection Ombudsman, <https://tietosuoja.fi/en/-/data-protection-authorities-continue-investigating-the-yango-taxi-service-s-data-transfers>, [10.09.2023].

რეფორმის შესახებ, რომელიც რუსეთში სექტემბრის დასაწყისიდან შევა ძალაში. ცვლილებების თანახმად, რუსეთის ფედერაციის უსაფრთხოების სამსახურს უფლება ექნება, მიიღოს ტაქსის ოპერაციებთან დაკავშირებით დამუშავებული მონაცემები. “Yango” ტაქსის აპლიკაციაში შეგროვებული ინფორმაცია შეიძლება, შეიცავდეს, მაგალითად, მომხმარებლის ადგილსამყოფელისა და ტაქსით მგზავრობის მისამართის შესახებ მონაცემებს.

ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანო მიიჩნევს, რომ რუსეთში საკანონმდებლო რეფორმის შემდეგ “Yango”-ს მიერ ევროკავშირის კანონმდებლობის მოთხოვნების შესაბამისად პერსონალური მონაცემების დაცვა შეუძლებელია. ამიტომ, აუცილებელი გახდა მონაცემთა გადაცემის შეჩერების შესახებ ბრძანების გამოცემა.

აღსანიშნავია, რომ ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მიღებულია გადაუდებელი პროცედურების საფუძველზე, რასაც ითვალისწინებს ევროკავშირის „მონაცემთა დაცვის ზოგადი რეგულაცია“ (“GDPR”). აღნიშნული პროცედურა საშუალებას იძლევა, ცალკეული ქმედებები განხორციელდეს საგამონაკლისო შემთხვევებში. გადაუდებელი პროცედურების მიხედვით, პირთა უფლებებისა და თავისუფლებების დაცვის მიზნით, საზედამხედველო ორგანოებს აქვთ უფლებამოსილება, დაუყოვნებლივ მიიღონ დროებითი ღონისძიება მაქსიმუმ სამი თვის ხანგრძლივობით.

OFFICE OF
THE DATA PROTECTION OMBUDSMAN

ფოტო: tietosuoja.fi

განახლებული ინფორმაციით, ფინეთის მონაცემთა დაცვის ომბუდსმენის ოფისმა, ნიდერლანდებისა და ნორვეგიის მონაცემთა დაცვის საზედამხედველო ორგანოებმა ევროპის ეკონომიკურ ზონაში “Yango” ტაქსის სერვისის ოპერაციები შეისწავლეს. მონაცემთა დაცვის საზედამხედველო ორგანოების ანგარიშის მიხედვით, როგორც დადგინდა, ტაქსებთან დაკავშირებული კანონმდებლობა, რომელიც რუსეთში სექტემბრის დასაწყისში შევიდა ძალაში, არ ვრცელდება ევროპის ეკონომიკურ ზონაში “Yango”-ს ოპერაციებზე. საკითხთან დაკავშირებით ფინეთის მონაცემთა დაცვის ომბუდსმენი განაგრძობს საკითხის შესწავლას.

ფოტო: yango.com

მონაცემთა დაცვის საზედამხედველო ორგანოებმა, დამატებითი ინფორმაციის გამოვლენის შემდეგ, დაასკვნეს, რომ რუსეთის კანონმდებლობის "Yango"-ს სერვისების ოპერაციებზე გავრცელების საკითხი შემდგომ შესწავლას საჭიროებდა. მაშინაც კი, თუ დადგინდება, რომ ტაქსებთან დაკავშირებულ კანონმდებლობაში განხორციელებული ცვლილებები "Yango"-ს ოპერაციებზე არ ვრცელდება, ტაქსის სერვისების მიერ მონაცემთა გადაცემის საკითხების შესწავლას ფინეთის საზედამხედველო ორგანო, ჰოლანდიისა და ნორვეგიის მონაცემთა დაცვის საზედამხედველო ორგანოებთან აქტიური თანამშრომლობით, მომავალშიც გააგრძელებს. შესწავლის ფარგლებში ასევე შეფასდება კომპანიების ანგარიში პერსონალური მონაცემების დამუშავებასთან დაკავშირებით, მათ მიერ დაგეგმილი და განხორციელებული ცვლილებების შესახებ.

აღსანიშნავია, რომ ფინეთის, ნიდერლანდებისა და ნორვეგიის მონაცემთა დაცვის საზედამხედველო ორგანოები "Yango"-ს მიერ მონაცემთა გადაცემის კანონიერების შესწავლას ფინეთის მონაცემთა დაცვის ომბუდსმენის მიერ გადაუდებელი პროცედურის დაწყებამდეც ახორციელებდნენ. შესწავლის შედეგად დადგინა, რომ "Yango" ტაქსის მიერ შეგროვებული პერსონალური მონაცემები რუსეთს გადაეცა.

შესაძლებელია, რომ რუსეთის უსაფრთხოების სამსახურს რუსეთში გადაცემულ მონაცემებზე წვდომა ჰქონდეს, მიუხედავად ტაქსებთან დაკავშირებული კანონმდებლობის ფარგლებისა, თუმცა საქმის შესწავლა ჯერ კიდევ გრძელდება. ამჟამად, მონაცემთა დაცვის საზედამხედველო ორგანოების შესწავლის ძირითადი მიმართულება "Yango"-ს მიერ პერსონალური მონაცემების გადაცემის კანონიერებაა.

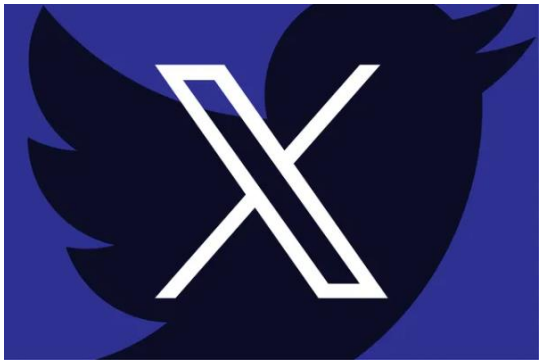
ფინეთის მონაცემთა დაცვის ომბუდსმენს ფინეთში "Yango" ტაქსის სერვისის ფუნქციონირების აკრძალვის უფლება არ აქვს. მას კომპანიის მიერ პერსონალური მონაცემების დამუშავებასთან დაკავშირებით მხოლოდ დროებითი ზომების მიღება შეუძლია. ჰოლანდიური კომპანია "Ridetech International B.V."-ს განცხადებით, იგი პასუხისმგებელია ტაქსის სერვისებთან დაკავშირებით პერსონალური მონაცემების

დამუშავებაზე. შესაბამისად, საბოლოო გადაწყვეტილების მიღება შეუძლია მხოლოდ ჰოლანდიის მონაცემთა დაცვის საზედამხედველო ორგანოს ან „მონაცემთა დაცვის ევროპულ საბჭოს“ (“EDPB”).

სოციალური ქსელი “X” ბიომეტრული მონაცემებისა და დასაქმების ისტორიის შეგროვებას იწყებს

31.08.2023

პლატფორმა “X”, წარსულში ცნობილი როგორც “Twitter”, მომხმარებელთა შესახებ დამატებითი ინფორმაციის შეგროვებას იწყებს.[6] კერძოდ, სოციალურმა ქსელმა განაახლა კონფიდენციალურობის პოლიტიკა, რომლის თანახმად, იგი ბიომეტრულ მონაცემებსა და დასაქმების ისტორიას შეაგროვებს.



ფოტო: theverge.com

კონფიდენციალურობის პოლიტიკაში აღნიშნულია, რომ თანხმობის საფუძველზე, დაცულობის, უსაფრთხოებისა და იდენტიფიკაციის მიზნებისთვის, შესაძლებელია ბიომეტრული მონაცემების შეგროვება და გამოყენება. დოკუმენტში არ არის აღნიშნული დეტალები იმის შესახებ, თუ რა სახის ბიომეტრული ინფორმაცია დამუშავდება ან როგორ გეგმავს “X”-ი მათ შეგროვებას, თუმცა ბიომეტრული მონაცემები ზოგადად მოიცავს თითის ანაბეჭდებს, თვალის ფერადი გარსის ნიმუშებს ან სახის მახასიათებლებს.

ბიომეტრული მონაცემების გამოყენების ერთ-ერთი შესაძლებლობა პინკოდის გარეშე ავტორიზაციაა. აპლიკაციების ერთ-ერთი დეველოპერის დასკვნების თანახმად, “X”-ი გეგმავს „გასაღების“ (“passkeys”) მხარდაჭერის გაშვებას, რომლის მეშვეობით შესაძლებელია მოწყობილობის თითის ანაბეჭდის, სახის ამოცნობის მექანიზმის ან პინის გამოყენება ანგარიშში შესასვლელად. თუმცა, არაკომერციული ორგანიზაცია — “FIDO Alliance”, რომელიც მხარს უჭერს „გასაღების“ გამოყენებას, აცხადებს, რომ ბიომეტრული მონაცემები მოწყობილობაზე რჩება და არ იგზავნება არცერთ დისტანციურ სერვერზე.

[6] The Verge, <https://www.theverge.com/2023/8/31/23853618/x-privacy-policy-update-biometrics-job-history>, [31.08.2023].

კონფიდენციალურობის პოლიტიკაში ასევე აღნიშნულია, რომ "X"-ის მიერ შესაძლებელია, შეგროვდეს ინდივიდის დასაქმების, აგრეთვე, განათლების შესახებ ისტორია, დასაქმების უპირატესობების, უნარებისა და შესაძლებლობების შესახებ ინფორმაცია, სამსახურის ძიების მიზნით განხორციელებული აქტივობა. აღნიშნული ჩანაწერი, სავარაუდოდ, დაკავშირებულია სამუშაოს ძიების თავისებურებებთან. კერძოდ, პლატფორმამ უკვე გამოუშვა კომპანიების დაქირავების ფუნქციონალის ბეტა ვერსია და ასევე, გეგმავს ვიდეო და აუდიოზარების დამატებას, ტელეფონის ნომრის საჭიროების გარეშე.

მოქმედ კონფიდენციალობის პოლიტიკაში[7], ბიომეტრული მონაცემების ან დასაქმების ისტორიასთან დაკავშირებული ინფორმაციის შეგროვების თაობაზე არაფერია აღნიშნული. განახლებული კონფიდენციალურობის პოლიტიკა მიმდინარე წლის სექტემბრის ბოლოს შევა ძალაში.

ფოტო: twitter.com

ინფორმაციისთვის, ივლისში სოციალური ქსელი "X" ერთ-ერთ ერთობლივ სარჩელში[8] იქნა მოხსენიებული, იმ მიზეზით, რომ მის მიერ მონაცემთა დამუშავება ილინოისის ბიომეტრული ინფორმაციის კონფიდენციალურობის შესახებ აქტს არღვევდა. სარჩელში აღნიშნულია, რომ "X"-მა სათანადოდ არ უზრუნველყო პირთა ინფორმირება იმის თაობაზე, რომ იგი პლატფორმაზე ატვირთული თითოეული ფოტოდან აგროვებდა ან/და ინახავდა ბიომეტრულ მახასიათებლებს.

„პირადი ცხოვრების ხელშეუხებლობის ფორუმის მომავალმა" გენერირებადი ხელოვნური ინტელექტის ორგანიზაციული მიზნებისთვის გამოყენებასთან დაკავშირებით გასათვალისწინებელი პუნქტების სია გამოაქვეყნა

01.08.2023

2023 წლის 1-ელ აგვისტოს „პირადი ცხოვრების ხელშეუხებლობის ფორუმის მომავალმა" ("Future of Privacy Forum (FPF)") გენერირებადი ხელოვნური ინტელექტის

[7] Twitter, <https://twitter.com/en/privacy#twitter-privacy-1>, [31.08.2023].

[8] Mark Martell v. X Corp., Case No.: 2023CH06416, 11/9/2023, https://s3.amazonaws.com/jnswire/jns-media/4e/52/13288870/2023ch06416.pdf.

ორგანიზაციული მიზნებისთვის გამოყენებასთან დაკავშირებით გასათვალისწინებელი პუნქტების სია გამოაქვეყნა.[9] აღნიშნული სია[10] განახლებადი დოკუმენტია, რომელიც ორგანიზაციებს საშუალებას აძლევს, შეამოწმონ მათი შიდა პოლიტიკა და პროცედურები. აღნიშნულით კომპანიებს შესაძლებლობა აქვთ, დარწმუნდნენ, რომ თანამშრომლების მიერ გენერირებადი ხელოვნური ინტელექტის სისტემებით სარგებლობის დროს, გამოყენებული იქნება ისეთი ინსტრუმენტები, რომლებიც ამცირებს მონაცემთა უსაფრთხოებისა და კონფიდენციალურობის რისკებს, პატივს სცემს ინტელექტუალური საკუთრების უფლებას და ინარჩუნებს მომხმარებელთა ნდობას.

ფოტო: fpf.org

გენერირებადი ხელოვნური ინტელექტი არის ხელოვნური ინტელექტის კატეგორია, რომელიც წარმოქმნის ახალ შედეგებს იმ მონაცემთა საფუძველზე, რომელთა დამუშავებისთვისაც იგი შეიქმნა. ე. წ. „დიდი მოცულობის ენობრივი მოდელები“ (“Large Language Models (LLMs)”) არის გენერირებადი ხელოვნური ინტელექტის პოპულარული ტიპი, რომელიც ქმნის პასუხებს „არამანქანურ ენაზე“ დასმული შეკითხვებისთვის. „დიდი მოცულობის ენობრივი მოდელების“ მაგალითებია “Google Bard”-სა და “Open AI”-ის “ChatGPT”-ი (ე. წ. „ჩატბოტები“), “Microsoft”-ის ხელოვნურ ინტელექტზე მომუშავე საძიებო სისტემა “Bing”-ი, “Midjourney”-ი და “Open AI”-ის “DALL-E” (სურათის გენერატორები). გენერირებადი ხელოვნური ინტელექტის ინსტრუმენტებს შესაძლებლობა აქვთ, შეადგინონ ელექტრონული წერილი ან კომპიუტერული კოდი, ასახონ ანგარიშები ან შექმნან „ბლოგ პოსტები“, მიაწოდონ მომხმარებელს ბიოგრაფიული ინფორმაცია, შეასრულონ მომხმარებელთა მომსახურების ფუნქციები, შექმნან სურათები და დაწერონ მხატვრული ნაწარმოებები.

გენერირებადი ხელოვნური ინტელექტის საერთო პოპულარობის ზრდასთან ერთად, მატულობს სამუშაო სივრცეში შესაბამისი ინსტრუმენტების გამოყენებაც.

[9] Future of Privacy Forum, <https://fpf.org/blog/fpf-releases-generative-ai-internal-policy-checklist-to-guide-development-of-policies-to-promote-responsible-employee-use-of-generative-ai-tools/>, [31.08.2023].

[10] იხ.:<https://fpf.org/wp-content/uploads/2023/07/Generative-AI-Checklist.pdf>, [31.08.2023].

დასაქმებულები იყენებენ გენერირებადი ხელოვნური ინტელექტის ინსტრუმენტებს ყველა სფეროში, მათ შორის, დასაქმების ეტაპზე. შესაბამისად, ორგანიზაციებმა უნდა გაითვალისწინონ სამართლებრივი და სოციალური რისკები, მიღებული/მისაღები სარგებელი და ხელოვნური ინტელექტის ინსტრუმენტების ტექნიკური უზრუნველყოფისა და გამოყენების გრძელვადიანი შედეგები.

ორგანიზაციები, ხშირად, აახლებენ შიდა პოლიტიკასა და პროცედურებს, რათა უზრუნველყონ ხელოვნური ინტელექტის ინსტრუმენტების პასუხისმგებლიანი, სამართლებრივი და ეთიკური გამოყენება. დასაქმებულები უნდა გადამზადდნენ ორგანიზაციის პოლიტიკასა და პროცესებთან დაკავშირებით, რათა სათანადოდ აღიქვან, თუ როგორ მუშაობს (ან არ მუშაობს) ხელოვნური ინტელექტის ინსტრუმენტები; რა რისკებია ორგანიზაციისთვის აღნიშნული ინსტრუმენტების არამართებული გამოყენების შემთხვევაში.

გენერირებადი ხელოვნური ინტელექტის შესახებ გასათვალისწინებელი პუნქტების სია შეიქმნა 30-ზე მეტი სექტორული კომპანიისა და ორგანიზაციის პრაქტიკოსებსა და ექსპერტებთან ჩატარებული კონსულტაციების შედეგად.

კონსულტაციები მიზნად ისახავდა:

- ☑ თანამშრომელთა მიერ გენერირებადი ხელოვნური ინტელექტის ინსტრუმენტების გამოყენების მოცულობის, მიღებული სარგებლისა და ზიანის დადგენას;
- ☑ ორგანიზაციის მართვის პროცესში ხელოვნური ინტელექტის გამოყენების შემთხვევების განსაზღვრას;
- ☑ იმ ზომების იდენტიფიცირებას, რომლებიც გამოიყენება კომპანიის მონაცემებისა და ინფრასტრუქტურის დასაცავად.

ფოტო: fpf.org

მსჯელობა დაეთმო გენერირებად ხელოვნურ ინტელექტთან დაკავშირებული სახელმძღვანელოების, შესაბამისი პოლიტიკის დოკუმენტებისა და პროცედურების განხილვას, რომლებიც დაინერგა ორგანიზაციებში

თანამშრომლების მიერ გენერირებადი ხელოვნური ინტელექტის ინსტრუმენტების გამოყენების სამართავად.

„პირადი ცხოვრების ხელშეუხებლობის ფორუმის მომავალის“ მიერ შემუშავებული გასათვალისწინებელი პუნქტების სია მოიცავს მითითებებს შემდეგ საკითხებთან დაკავშირებით:

- ☑ მონაცემთა გამოყენება მონაცემთა დაცვისა და უსაფრთხოების შესახებ არსებული კანონებისა და პოლიტიკის შესაბამისად;
- ☑ თანამშრომელთა განათლება და კვალიფიკაციის ამაღლება;
- ☑ ხელოვნური ინტელექტის გამოყენების ინსტრუქცია თანამშრომლებისთვის;
- ☑ გენერირებადი ხელოვნური ინტელექტის გამოყენების შედეგები.

მონაცემთა გამოყენება მონაცემთა დაცვისა და უსაფრთხოების შესახებ არსებული კანონებისა და პოლიტიკის შესაბამისად:

უფლებამოსილმა პირებმა უნდა განაახლონ არსებული შიდა პოლიტიკის დოკუმენტები და პროცედურები, რათა გათვალისწინებულ იქნეს თანამშრომელთა მიერ გენერირებადი ხელოვნური ინტელექტის დაგეგმილი ან ნებადართული გამოყენება. თანამშრომლებმა უნდა იცოდნენ, რომ მიმდინარე ან სამომავლო ვალდებულებები ვრცელდება ხელოვნური ინტელექტის ინსტრუმენტების გამოყენებაზე.

თანამშრომელთა განათლება და კვალიფიკაციის ამაღლება:

უფლებამოსილმა პირებმა უნდა აცნობონ თანამშრომლებს სამუშაო სივრცეში გენერირებადი ხელოვნური ინტელექტის ინსტრუმენტების გამოყენების ზეგავლენისა და შედეგების შესახებ; ასევე, ხელოვნური ინტელექტის ინსტრუმენტების პასუხისმგებლიანი გამოყენების, რისკებისა და არსებული ეთიკური მოსაზრებების შესახებ თანამშრომლები უნდა უზრუნველყონ შესაბამისი ტრენინგებითა და რესურსებით, უფლებამოსილმა პირებმა თანამშრომლებს რეგულარულად უნდა მიაწოდონ ინფორმაცია სამართლებრივი და ეთიკური ვალდებულებების შესახებ.

ხელოვნური ინტელექტის გამოყენების ინსტრუქცია თანამშრომლებისთვის:

ორგანიზაციებმა თანამშრომლებს უნდა მიაწოდონ მკაფიო მითითებები, თუ როდის და რა ვითარებაში გამოიყენონ ორგანიზაციული ანგარიშები გენერირებადი ხელოვნური ინტელექტის ინსტრუმენტებისთვის ისევე, როგორც ინფორმაცია სამუშაო სივრცეში აღნიშნული ხელსაწყოების დაშვებულ და აკრძალულ გამოყენებასთან დაკავშირებით არსებული პოლიტიკის შესახებ.

გენერირებადი ხელოვნური ინტელექტის გამოყენების შედეგები:

უნდა დაინერგოს შესაბამისი სისტემები, რომლებიც შეახსენებს თანამშრომლებს, გადაამოწმონ გენერირებადი ხელოვნური ინტელექტის ინსტრუმენტების მიერ მიღებული შედეგები, მათ შორის, საკითხები, რომლებიც შეეხება სიზუსტეს, დროულობას, მიუკერძოებლობის ან ინტელექტუალური საკუთრების უფლებების შესაძლო დარღვევას. ორგანიზაციებმა უნდა განსაზღვრონ, უნდა გაიცეს თუ არა კომპენსაცია მათზე, ვისი ინტელექტუალური საკუთრებაც დაკავშირებულია ხელოვნური ინტელექტის მიერ მიღებულ შედეგებზე. როდესაც გენერირებადი ხელოვნური ინტელექტი გამოიყენება კოდირებისთვის, შესაბამისმა პერსონალმა უნდა შეამოწმოს და დაადასტუროს შედეგები უსაფრთხოების ზომების მოწყვლადობასთან დაკავშირებით.

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