# მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

## სიახლეები

ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება აუდიო და ვიდეომონიტორინგის შესახებ

ესტონეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიგნებები სტომატოლოგიურ კლინიკებში პერსონალური მონაცემების დამუშავების შესახებ

### ინფორმაცია საინიციატივო ჯგუფ "NYOB"-ს საჩივრების შესახებ ევროპარლამენტის წინააღმდეგ მონაცემთა უსაფრთხოების დარღვევის ინციდენტთან დაკავშირებით

2024 წლის 22 აგვისტოს, საინიციატივო ჯგუფმა სახელწოდებით (NOYB)[1] განაცხადა ევროპის მონაცემთა დაცვის საზედამხედველო ორგანოში ევროპარლამენტის წინააღმდეგ ორი[2] საჩივრის შეტანის თაობაზე, რომლებიც ეხება ევროპარლამენტის ადამიანური რესურსების მართვის პლატფორმის ("PEOPLE") -ის უსაფრთხოებასთან დაკავშირებულ ინციდენტს.

## სექტემბერი 2024

## საჩივრების შინაარსი

საინიციატივო ჯგუფის განცხადებით, 2024 წლის 26 აპრილს ევროპარლამენტმა ევროპის მონაცემთა დაცვის საზედამხედველო ორგანოს მიაწოდა ინფორმაცია პლატფორმა (“PEOPLE”)-ის უსაფრთხოებასთან დაკავშირებული ინციდენტის შესახებ. ინციდენტი შეეხო 8,000 მონაცემთა სუბიექტის პერსონალურ მონაცემებს, კერძოდ, პარლამენტის ამჟამინდელი და ყოფილი თანამშრომლების პერსონალურ მონაცემებს. უსაფრთხოების ინციდენტი შეეხო მონაცემთა სუბიექტების პერსონალურ მონაცემებს, მათ შორის, პირადობის დამადასტურებელ, ნასამართლეობის შესახებ, ბინადრობის შესახებ დოკუმენტებს, ხელშეკრულებებს, განსაკუთრებული კატეგორიის მონაცემებს, როგორიცაა, ქორწინების სერტიფიკატი, რომლის საფუძველზეც შესაძლებელია დასკვნის გაკეთება მონაცემთა სუბიექტის სექსუალური ორიენტის შესახებ.

საინიციატივო ჯგუფი პარლამენტს უჩივის მონაცემთა დაცვის ძირითად რეგულაციაში განსაზღვრული მონაცემთა მინიმიზაციის პრინციპის დარღვევის თაობაზე, კერძოდ, მინიმიზაციის პრინციპის დაუცველობაში მონაცემთა შეგროვებისდა შენახვის ნაწილში.
საინიციატივო ჯგუფის განცხადებით, უსაფრთხოების ინციდენტის შემდგომ, ევროპარლამენტმა უარიგანაცხადა მონაცემთა სუბიექტის მიერმონაცემთა წაშლის მოთხოვნის დაკმაყოფილებაზე. საინიციატივო ჯგუფმა ხაზიგაუსვა, მონაცემთა სუბიექტმა, რომელმაც მოითხოვა მონაცემთა წაშლა, წლების წინშეწყვიტა მუშაობა ევროპარლამენტში, თუმცა ევროპარლამენტმა უარიგანაცხადა მონაცემთა სუბიექტის პერსონალური მონაცემების წაშლაზე პარლამენტის მონაცემთა შენახვის წესით გათვალისწინებულ 10 წლიან ვადაზე დაყრდნობით.

## გატარებული ღონისძიებები

ევროპის მონაცემთა დაცვის საზედამხედველო ორგანო, პოლიცია, პარლამენტის კიბერუსაფრთხოების ჯგუფი და ლუქსემბურგის მონაცემთა დაცვის სამსახური იძიებენ უსაფრთხოების ინციდენტს. ადამიანური რესურსების მართვის პლატფორმა (“PEOPLE”) ამჟამად გამართვის პროცესშია და მისი აღდგენა მოკლე ვადაში იგეგმება. პარლამენტის თანამშრომლებმა მიიღეს ინფორმაცია და გაატარეს უსაფრთხოების კუთხით გათვალისწინებული ტექნიკურ-ორგანიზაციული ზომები.[1]

Australian Government

Geoscience Australia

# ინფორმაცია ავსტრალიის მთავრობის მიერ გამოქვეყნებული “ხელოვნური ინტელექტის პასუხისმგებლიანი გამოყენების პოლიტიკის დოკუმენტის“ შესახებ

ავსტრალიის მთავრობამ განაახლა ხელოვნური ინტელექტის პასუხისმგებლიანი გამოყენების შესახებ პოლიტიკის დოკუმენტი[1], რომელიც ძალაში პირველი სექტემბრიდან შევა.[2] პოლიტიკის დოკუმენტი სამი ნაწილისგან შედგება და აყალიბებს პრინციპებს ხელოვნური ინტელექტის გამოყენების შესახებ.

პოლიტიკის დოკუმენტის პირველი ნაწილი ეხება მომზადებას და დახმარების გაწევას, კერძოდ:

- ხელოვნური ინტელექტის მიღებისა და გამოყენებისათვის ნათელი და მკაფიო ანგარიშვალდებულებების ჩამოყალიბებას;
- ანგარიშვალდებული პირების იდენტიფიცირებას.

სტანდარტის თანახმად ანგარიშვალდებულმა პირებმა უნდა: [3]

- აიღონ პასუხისმგებლობა პოლიტიკის გატარების მიმართულებით;
- შეატყობინონ ინფორმაციული ტრანსფორმაციის სააგენტოს, როდესაც ხელოვნური ინტელექტის გამოყენება მაღალი რისკის შემცველია;
- მთავრობის წევრებთან კონტაქტის შენარჩუნება და კოორდინაცია, ფორუმებში და ღონისძიებებში მონაწილეობის მიღება;
- ხელოვნურ ინტელექტთან დაკავშირებულ ახალ მოთხოვნებთან შესაბამისობა.

დოკუმენტის მეორე ნაწილი განიხილავს ანგარიშვალდებულ პირთა პასუხისმგებლობის საკითხს.
ანგარიშვალდებული პირების პასუხისმგებლობაა:

- პროპორციული და მიზანზე მორგებული რისკის შემცირების მეთოდების გამოყენება;
- ხელოვნური ინტელექტის გამჭვირვალე გამოყენება და დაინტერესებული საზოგადოებისათვის შესაბამისი ინფორმაციის მიწოდება;
- გამჭვირვალობის განაცხადის გამოქვეყნება ხელოვნური ინტელექტის გამოყენებასთან დაკავშირებით (2025 წლის მარტიდან).

პოლიტიკის დოკუმენტის მესამე ნაწილი განვითარებაზე და გაერთიანებაზეა ორიენტირებული და მიმოიხილავს შემდეგ საკითხებს:

- ხელოვნური ინტელექტის გამოყენების განხილვა და შეფასება;
- პროექტის მართვის პროცესში უკუკავშირის მექანიზმების განვითარება.

# ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება აუდიო და ვიდეომონიტორინგის შესახებ

Data State Inspectorate Republic of Latvia

მონაცემთა სუბიექტის მიმართვის საფუძველზე ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ აუდიო და ვიდეომონიტორინგის შესახებ გადაწყვეტილება მიიღო.მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს წამოადგენდა უსაფრთხოებასთან დაკავშირებული სერვისების მიმწოდებელი კომპანია, რომლის ოფისში დანერგილი იყო სამეთვალყურეო “CCTV” სისტემა. აღნიშნული სისტემით ხორციელდება როგორც აუდიო, ისე ვიდეომონიტორინგი.

კომპანიის თანამშრომელმა “CCTV” სისტემით გადაღებული ვიდეოჩანაწერი მონაცემთა სუბიექტს (საჩივრის შემტან პირს) საკომუნიკაციო პლატფორმის, “WhatsApp”-სა და “Telegram”-ის საშუალებით გაუგზავნა. კომპანიის შინაგაწესის მიხედვით, თანამშრომლებს გადაღებულ ვიდეომასალაზე წვდომა არ აქვთ და არც საკუთარ მოწყობილობებზე შეუძლიათ მისი გაზიარება. შესაბამისად, თანამშრომელმა, რომელმაც ვიდეოჩანაწერი გაუგზავნა მონაცემთა სუბიექტს, დაამუშავა პირის პერსონალური მონაცემები მისი სამსახურებრივი ვალდებულებების ფარგლებს მიღმა და დამსაქმებლის უშუალო მითითების გარეშე. უფრო მეტიც, მოგვიანებით, კომპანიამ ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს აცნობა, რომ კადრები წაიშალა და თანამშრომელთან შრომითი ურთიერთობა შეწყდა.

დამუშავებისთვის პასუხისმგებელ პირს კომპანიაში დანერგილი ჰქონდა შესაბამისი წესები ავტორიზაციის მართვის, წვდომის მონიტორინგის, ვიდეომეთვალყურეობის, ვიდეოჩანაწერზე წვდომისა და არქივირების მექანიზმის, შენახვისა და ასლის შექმნის შესახებ. აღნიშნული ტექნიკური და ორგანიზაციული ზომები შესაბამისობაში იყო ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) 25-ე მუხლის პირველი პუნქტით განმტკიცებულ მოთხოვნებთან. გარდა ამისა, მონაცემთა დაცვის საზედამხედველო ორგანომ მიიჩნია, რომ დამუშავებისთვის პასუხისმგებელი პირი არ შეიძლება იყოს იმ თანამშრომლების ქმედებებზე პასუხისმგებელი, რომლებმაც განზრახ უგულებელყვეს კომპანიის მიერ დადგენილი წესები. აღნიშნულიდან გამომდინარე, მონაცემთა სუბიექტის საჩივარი არ დაკმაყოფილდა.

თუმცა, მოკვლევის პროცესში გამოვლინდა, რომ “CCTV” სისტემა აღჭურვილი იყო ხმის ჩამწერი ფუნქციით, ხოლო აუდიოჩაწერა მიმდინარეობდა მინისტრთა კაბინეტის 2022 წლის 21 ივნისის № 369 რეგულაციის საფუძველზე. რეგულაციით განსაზღვრულია, რომ კომპანიის პერსონალს შორის საუბარი უნდა ჩაიწეროს და შეინახოს არაუმეტეს სამი თვით. თუმცა შინაგან საქმეთა სამინისტროსთან კონსულტაციის შემდეგ, დადგინდა, რომ ვიდეოსათვალთვალო კამერების მეშვეობით დამზადებული აუდიოჩანაწერი არ განეკუთვნება რეგულაციის მოქმედების სფეროს, ვინაიდან “CCTV” სისტემის ჩანაწერში ისმის მხოლოდ ერთი ადამიანის ხმა და არა სრული დიალოგი. აქედან გამომდინარე, ლატვიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ კომპანიის მიერ განხორციელებული ქმედება არ იყო შესაბამისობაში “GDPR”-ის მე-5(1)(ა)(გ) და მე-6(1) მუხლებთან, ვინაიდან მონაცემთა დამუშავება (აუდიოჩაწერა) ხორციელდებოდა შესაბამისი საფუძვლის გარეშე.

# ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება კანონიერი წარმომადგენლის მიერ პერსონალური მონაცემების დამუშავების საკითხებთან დაკავშირებით

ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) ფიზიკური პირის კანონიერი წარმომადგენლის მიერ პერსონალური მონაცემების დამუშავების საკითხებზე იმსჯელა.[1] საქმის ფაქტობრივი გარემოებების თანახმად, მონაცემთა სუბიექტს დაენიშნა ადვოკატი, რომელსაც სამსახურებრივი უფლებამოსილების ფარგლებში მონაცემთა სუბიექტის პირად ინფორმაციასთან ჰქონდა შეხება.

მონაცემთა სუბიექტმა, კანონიერი წარმომადგენლის მიერ სამსახურებრივი უფლებამოსილების განხორციელებისას მოპოვებულ ინფორმაციაზე წვდომის მიზნით, ჰანოვერის ადგილობრივ სასამართლოს (“Amtsgericht Hannover – AG Hannover”) მიმართა. სასამართლომ არ დააკმაყოფილა განცხადება იმ საფუძვლით, რომ კანონიერი წარმომადგენელი, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-4 მუხლის მე-7 პუნქტის შესაბამისად, არ წარმოადგენდა დამუშავებისთვის პასუხისმგებელ პირს, რამდენადაც ასრულებდა სამსახურებრივ უფლებამოსილებას. აღნიშნულიდან გამომდინარე, GDPR”-ის მე-15 მუხლის თანახმად, არ ჰქონდა ინფორმაციაზე წვდომის უზრუნველყოფის ვალდებულება.

მონაცემთა სუბიექტმა ადგილობრივი სასამართლოს მიერ მიღებული გადაწყვეტილება გაასაჩივრა ჰანოვერის რაიონულ სასამართლოში (“Landgericht Hannover - LG Hannover”). სასამართლომ საკითხთან დაკავშირებით განმარტებების მისაღებად მიმართა ევროკავშირის მართლმსაჯულების სასამართლოს კითხვებით:

- რამდენად არის კანონიერი წარმომადგენელი დამუშავებისთვის პასუხისმგებელი პირი “GDPR”-ის მე-4 მუხლის მე-7 პუნქტის შესაბამისად;
- მოეთხოვება თუ არა კანონიერ წარმომადგენელს მონაცემთა სუბიექტისთვის ინფორმაციის წარდგენა “GDPR”-ის მე-15 მუხლის გათვალისწინებით.

ევროკავშირის მართლმსაჯულების სასამართლომ, “GDPR”-ის მე-4 მუხლის მე-7 პუნქტზე დაყრდნობით, დაადგინა,[2] რომ კანონიერი წარმომადგენელი, ამავდროულად, არის დამუშავებისთვის პასუხისმგებელი პირი.

პირველ რიგში, ყურადღება გამახვილდა “GDPR”-ის მე-2 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტზე, რომელიც პირადი ან ოჯახური საქმიანობის ფარგლებში პერსონალური მონაცემების დამუშავებისას რეგულაციის მოქმედებას გამორიცხავს. კანონიერი წარმომადგენელი პერსონალურ მონაცემებს სამსახურებრივი უფლებამოსილების განხორციელების ფარგლებში ამუშავებდა. კანონიერ წარმომადგენელს ეკისრებოდა ვალდებულება, მისი დაცვის ქვეშ მყოფი პირის სახელით განეხორციელებინა სხვადასხვა აქტივობა. აღნიშნულიდან გამომდინარე, კანონიერი წარმომადგენელი, ასევე, განსაზღვრავდა მონაცემთა დამუშავების მიზნებსა და საშუალებებს.

შესაბამისად, “CJEU”-ს გადაწყვეტილებით, კანონიერი წარმომადგენელი იყო დამუშავებისთვის პასუხისმგებელი პირი და მასზე გავრცელდებოდა “GDPR”-ით დადგენილი ვალდებულებები, მათ შორის, მონაცემთა სუბიექტის მიერ მონაცემებზე წვდომის უფლების უზრუნველყოფა (რეგულაციის მე-15 მუხლი).

## დანიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება სავარჯიშო დარბაზში სახის ამომცნობი სისტემის გამოყენებასთან დაკავშირებით


დანიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“Datatilsynet”), მოქალაქის მიმართვის საფუძველზე, სავარჯიშო დარბაზში სახის ამომცნობი სისტემის ფუნქციონირების შესახებ გადაწყვეტილება მიიღო.

ფაქტობრივი გარემოებების თანახმად, სახის ამომცნობი სისტემის გამოყენების მიზანი ფიზიკურ პირთა იდენტიფიცირება იყო. მონაცემთა სუბიექტი აცხადებდა, რომ დაწესებულებაში სახის ამომცნობი სისტემის გამოყენების შესაბამისი ალტერნატივა არ არსებობდა. დამუშავებისთვის პასუხისმგებელი პირის მტკიცებით, მომხმარებლებს მათი პერსონალური ინფორმაციის დამუშავების შესახებ ინფორმაცია კონფიდენციალობის პოლიტიკის დოკუმენტის მეშვეობით მიეწოდათ. ასევე, სახის ამომცნობი სისტემის გამოყენებაზე უარის თქმის შემთხვევაში, მომხმარებლებს სავარჯიშო დარბაზით შეეძლოთ ესარგებლათ სამუშაო საათებში ან დაკავშირებოდნენ კლიენტთა მომსახურების ცენტრს, რომელიც დისტანციურად გააღებდა შესასვლელ კარს.

საზედამხედველო ორგანომ აღნიშნა, რომ სახის ამომცნობი სისტემის გამოყენება არ ეწინააღმდეგება მონაცემთა დამუშავების პრინციპებს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის შესაბამისად. ამგვარი სისტემის გამოსაყენებლად, აუცილებელია შესაბამისი სამართლებრივი საფუძვლების არსებობა.

სახის ფოტოსურათების გამოყენება პირთა იდენტიფიცირებისთვის წარმოადგენს ბიომეტრიულ მონაცემებს “GDPR”-ის მე-4 მუხლის მე-14 პუნქტის შესაბამისად. “GDPR”-ის მე-9 მუხლზე დაყრდნობით, დამუშავებისთვის პასუხისმგებელ პირს ეკრძალება განსაკუთრებული კატეგორიის მონაცემის დამუშავება, თუ არ არსებობს რეგულაციის მე-9 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული საგამონაკლისო საფუძველი, კერძოდ, ნათლად გამოხატული თანხმობა.

მონაცემთა სუბიექტს პერსონალური მონაცემების ალტერნატიული საშუალებებით დამუშავების თაობაზე ინფორმაცია გასაგები ფორმით უნდა მიეწოდოს. მოცემულ შემთხვევაში, მხოლოდ სამუშაო საათებში სავარჯიშო დარბაზით სარგებლობის შესაძლებლობა არ გულისხმობდა სათანადო ალტერნატივას. ასევე, მონაცემთა სუბიექტს არ მიეწოდა სრულყოფილი ინფორმაცია პერსონალური მონაცემების დამუშავების საშუალების თაობაზე, რის საფუძველზეც თანხმობა არ იყო ნამდვილი.

შედეგად, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელ პირს შენიშვნა გამოუცხადა.


## ესტონეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიგნებები სტომატოლოგიურ კლინიკებში პერსონალური მონაცემების დამუშავების შესახებ

ესტონეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“DPI”) პერსონალური მონაცემების დამუშავების კანონიერების შესწავლის მიზნით განახორციელა ოთხი სტომატოლოგიური კლინიკის ინსპექტირება, რის საფუძველზეც ძირითადი მიგნებები და რეკომენდაციები გამოაქვეყნა.[1] ინფორმაციაში აღნიშნულია, რომ სამედიცინო დაწესებულებები ამუშავებენ პაციენტებთან დაკავშირებულ განსაკუთრებული კატეგორიის პერსონალურ ინფორმაციას, რაც მოითხოვს უსაფრთხოების სათანადო ზომების არსებობას. პირველ ეტაპზე, “DPI”-მ კლინიკებს პერსონალური მონაცემების დამუშავებასთან დაკავშირებით კითხვარი შეავსებინა და შესაბამისი დოკუმენტაციის მიწოდება დაავალა. შევსებული კითხვარის ანალიზის შემდეგ, განხორციელდა ადგილზე შემოწმება, რომლის ფარგლებშიც სამედიცინო დაწესებულების თანამშრომლებს უნდა გაეკეთებინათ განმარტებები დასმულ კითხვებზე, მათ შორის, დანერგილი უსაფრთხოების ზომების შესახებ. წარმოდგენილი ინფორმაციის შეფასების საფუძველზე, გამოიკვეთა რიგი ხარვეზები და გაიცა შესაბამისი რეკომენდაციები.[2] გამოვლენილი ხარვეზები შეეხებოდა:

- დოკუმენტაციასთან დაკავშირებულ ნაკლოვანებებს (პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული პროცედურები არ იყო სრულყოფილი);
- მონაცემთა უსაფრთხოების დარღვევასთან დაკავშირებით არასათანადო პროცედურის არსებობას;
- სამუშაოს შესრულების მიზნით პირადი მოწყობილობების გამოყენებას;
- პერსონალური მონაცემების შენახვასა და გამოყენებასთან დაკავშირებულ გარემოებებს;
- ინფორმაციულ უსაფრთხოებასთან დაკავშირებულ არასათანადო ზომებს;
- პაციენტთა პერსონალური ინფორმაციის არასათანადო დაცულობას;

- პერსონალურ მონაცემთა დაცვის თემატიკაზე დასაქმებულ პირთა ცნობიერების ნაკლებობას;
- მომხმარებლის თანხმობის გარეშე ვებგვერდზე არასაჭირო „მზა ჩანაწერების“ (“Cookies”) გამოყენებას;
- საკომუნიკაციო და ვიდეოსამეთვალყურეო სისტემების გამოყენების პროცესში ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებთან შეუსაბამობას.

იდენტიფიცირებულ ნაკლოვანებებზე დაყრდნობით, საზედამხედველო ორგანომ სტომატოლოგიური კლინიკების მიმართ წარადგინა რეკომენდაციები, რომელთა შესაბამისად:

- უნდა შემუშავდეს ინფორმაციული უსაფრთხოებისა და მონაცემთა დაცვის პოლიტიკის შესახებ სათანადო სტანდარტები;
- მონაცემებზე წვდომისა და ავთენტიფიკაციის თაობაზე დაინერგოს შესაბამისი მექანიზმები;
- უნდა გადამზადდნენ მონაცემთა დაცვის საკითხებზე დასაქმებული პირები;
- უზრუნველყოფილი იქნას ვებგვერდის უსაფრთხოება;
- რისკების გათვალისწინებით, ჩამოყალიბდეს მონაცემთა დამუშავებისა და შენახვის პრაქტიკა.

## ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება სკოლის მიერ პერსონალური მონაცემების არამართლზომიერი დამუშავების შესახებ

ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“GBA”) საგანმანათლებლო დაწესებულების მიერ პერსონალური მონაცემების დამუშავების მართლზომიერების შესახებ გადაწყვეტილება[1] მიიღო.

საქმის ფაქტობრივი გარემოებების თანახმად, მონაცემთა სუბიექტმა სკოლის ვაკანტურ თანამდებობაზე გამოცხადებულ კონკურსში მიიღო მონაწილეობა, თუმცა შეირჩა კონკრეტულ პოზიციაზე. აღნიშნულის თაობაზე გადაწყვეტილება სკოლის ციფრულ პლატფორმაზე (“Smartschool”) გამოქვეყნდა, რომელზეც წვდომა სკოლის 150 თანამშრომელს ჰქონდა. წარმოდგენილი ფაქტის შემდეგ, სკოლის საბჭომ განაცხადა, რომ გამოქვეყნებული ინფორმაცია იყო კონფიდენციალური და შეცდომით გახდა საჯაროდ ხელმისაწვდომი.

დამატებით, სკოლის დირექტორმა, რომელიც არ იყო ჩართული კონკურსის პროცესში, ელექტრონული ფოსტის მეშვეობით მონაცემთა სუბიექტს მისი სამოტივაციო წერილის შესახებ გაუგზავნა ინფორმაცია. წარმოდგენილ გარემოებაზე დაყრდნობით, მონაცემთა სუბიექტმა მიიჩნია, რომ საკონკურსო კომისიამ მისი სამოტივაციო წერილი გადასცა დირექტორს რომელიც წარმოადგენდა მესამე მხარეს. აღნიშნულის გათვალისწინებით, მონაცემთა სუბიექტმა ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოში საჩივარი შეიტანა.

საზედამხედველო ორგანომ, პირველ რიგში, აღნიშნა, რომ სკოლის ელექტრონულ პლატფორმაზე კონკურსის მონაწილე პირის სამსახურში აყვანაზე უარის თქმის შესახებ ინფორმაციის განთავსება და მასზე თანამშრომლების წვდომა შესაძლებელს ხდიდა პერსონალური მონაცემების მესამე მხარისთვის გადაცემას და იწვევდა მონაცემთა კონფიდენციალობის დარღვევას. ამასთან, განმარტა, რომ სკოლის ელექტრონულ პლატფორმაზე პერსონალური ინფორმაციის შეცდომით გამოქვეყნება გამოწვეული იყო სათანადო ტექნიკური და ორგანიზაციული ზომების არარსებობით.

“GBA”-მ, ასევე, ყურადღება გაამახვილა, რომ პირადი ინფორმაციის შემცველი დოკუმენტაცია, როგორიცაა, რეზიუმე და სამოტივაციო წერილი, გაეგზავნა მესამე მხარეს, სკოლის დირექტორს, რომელიც არ იყო კონკურსის მონაწილე პირთა შერჩევის პროცესში ჩართული.

წარმოდგენილი გარემოების გათვალისწინებით, საზედამხედველო ორგანომ დაადგინა, რომ არაუფლებამოსილ ადრესატებთან, ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის პირველ პუნქტზე დაყრდნობით, კანონიერი საფუძვლის გარეშე ინფორმაციის გამჟღავნებით დაირღვა კანონიერების პრინციპი, ხოლო პერსონალური მონაცემების ამ ფორმით გაზიარებით დაირღვა მთლიანობისა და კონფიდენციალობის პრინციპი “GDPR”-ის მე-5 მუხლის პირველი მუხლის „გ“ ქვეპუნქტის შესაბამისად. დამატებით, დამუშავებისთვის პასუხისმგებელი პირის მიერ სათანადო ტექნიკური და ორგანიზაციული ზომების მიღების არარსებობის გამო დაირღვა “GDPR”-ის 25-ე მუხლი. ამდენად, საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირის მიმართ სანქციის სახით გაფრთხილება გამოიყენა.

## დანიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (“Datilsynet”) გადაწყვეტილება ხელოვნური ინტელექტის გამოყენებით მონაცემთა დამუშავების შესახებ

მონაცემთა სუბიექტის მიმართვის საფუძველზე დანიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“Datilsynet”) კომპანია “IDA Forsikring”-ის მიერ სატელეფონო ზარების ჩაწერისა და ანალიზის შესახებ გადაწყვეტილება მიიღო.

კომპანია სერვისის გაუმჯობესების მიზნით მომხმარებლებთან სატელეფონო საუბარს იწერდა და შემდეგ ხელოვნური ინტელექტის (AI) მეშვეობით აანალიზებდა.

მოკვლევის ფარგლებში დანიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ მონაცემთა სუბიექტებისგან თანხმობის მიღების გზა არ იყო საკმარისად ცალსახა, რადგან მხოლოდ ერთი ზოგადი თანხმობით ხორციელდებოდა რიგი ინფორმაციის შეგროვება, ხოლო მომხმარებელს არ ჰქონდა შესაძლებლობა თანხმობა გაეცა ცალკეულ დამუშავებებზე. ასევე, დადგინდა, რომ მონაცემთა დამუშავება კანონიერად მიიჩნევა, როდესაც კომპანიაში დასაქმებული პირები თავიანთი სამსახურებრივი უფლებამოსილების ფარგლებში საუბრობენ ტელეფონზე, რამდენადაც არსებობს ლეგიტიმური მიზანი - სერვისის გაუმჯობესება.

“Datatilsynet”-მა დაადგინა, რომ “AI”-ის გამოყენება სატელეფონო ზარების ჩანაწერების გასაანალიზებლად არის მართლზომიერი და შეესაბამება მონაცემთა დაცვის კანონმდებლობას (არ არის აკრძალული “GDPR”-ის 9(1) მუხლით). “Datatilsynet”-მა ასევე, ხაზგასმით აღნიშნა, რომ “IDA Forsikring” იწერდა სატელეფონო საუბრებს კომპანიის პერსონალური მონაცემთა დაცვის პოლიტიკისა და “GDPR”-ის მე-13 მუხლის შესაბამისად.

დანიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ვერ აღმოაჩინა დარღვევა ხელოვნური ინტელექტის გამოყენებით მონაცემთა დამუშავებასთან დაკავშირებით, თუმცა მოუწოდა კომპანიას პროცესების მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის უზრუნველყოფისკენ.

## ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა სუბიექტის მიერ მონაცემებზე წვდომის უფლების შესახებ

მონაცემთა სუბიექტის მიმართვის საფუძველზე ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა სუბიექტის მიერ მონაცემებზე წვდომის უფლების შესახებ გადაწყვეტილება მიიღო.

“A” კომპანიის თანამშრომლებმა სამსახურებრივი ელ. ფოსტის მეშვეობით მიიღეს წერილი “B”კომპანიის მიერ ორგანიზებული აუქციონის შესახებ. აღსანიშნავია, რომ მსგავსი შინაარსის არასასურველი სარეკლამო წერილები მათ პერიოდულად ეგზავნებოდათ.

“A” კომპანიის პერსონალურ მონაცემთა დაცვის ოფიცერმა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-15 მუხლის შესაბამისად, “B”კომპანიისგან გამოითხოვა ინფორმაცია თუ როგორ მოიპოვა სამსახურებრივი ელ. ფოსტის მისამართები.

ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-12 მუხლი, რადგან კომპანიამ მონაცემთა სუბიექტს არ მიაწოდა მე-15 მუხლით განსაზღვრული ინფორმაცია, შესაბამისად, ხელი შეუშალა მონაცემთა სუბიექტის უფლების განხორციელებას. ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ საჩივარი დააკმაყოფილა და მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს დაავალა მონაცემთა სუბიექტის მოთხოვნის შესრულება 30 დღის განმავლობაში.

## ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა უკანონო დამუშავების შესახებ

მონაცემთა სუბიექტის მიმართვის საფუძველზე ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) მონაცემთა უკანონო დამუშავების შესახებ გადაწყვეტილება მიიღო.

მონაცემთა სუბიექტმა საჩივრით მიმართა მონაცემთა დაცვის ორგანოს პერსონალური მონაცემების, მათ შორის, ელ. ფოსტის მისამართის, უკანონო დამუშავების გამო. დამუშავებისთვის პასუხისმგებელმა პირმა სუბიექტების მონაცემები ხელმისაწვდომი გახადა, როგორც ორგანიზაციის წევრებისთვის, ისე გარეშე პირებისთვის. მიუხედავად მონაცემთა სუბიექტის მოთხოვნისა, აღნიშნული პრაქტიკა გაგრძელდა. მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მიუთითებდა, რომ ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაციის მე-9 მუხლის შესაბამისად, დამუშავება შრომითსამართლებრივი ურთიერთობის მიზნებისთვის აუცილებელი იყო. მართალია, მონაცემთა სუბიექტი გაზიარებაზე თანხმობას არ აცხადებდა, თუმცა ელექტრონული ფოსტის მისამართები სამსახურებრივი იყო.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მიიჩნია, რომ თანხმობის გარეშე მონაცემთა დამუშავება არამართლზომიერი ქმედება იყო, განსაკუთრებით მაშინ, როდესაც მონაცემთა სუბიექტმა მოითხოვა დამუშავებისა და სხვა პირებთან გაზიარების შეწყვეტა. ამასთან, დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა უსაფრთხოების რისკის შემცირების მიზნით არ იყენებდა საბაზისო მექანიზმებს, მაგალითად, როგორიცაა „ფარული ასლი“ (“Hidden Copy”).

“AEPD”-მ დაადგინა, რომ ქმედება არ შეესაბამებოდა “GDPR”-ის მე-6 მუხლის მოთხოვნას, რადგან არ არსებობდა დამუშავების სამართლებრივი საფუძველი. მიუხედავად იმისა, რომ მონაცემთა სუბიექტი მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ორგანიზაციაში დასაქმებული იყო, აღნიშნული არ წარმოადგენდა საკმარის არგუმენტს. ამდენად, ელექტრონული ფოსტის მისამართების სხვა პირებთან გაზიარებისთვის მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს დაეკისრა ჯარიმა 2 000 (ორი ათასი) ევროს ოდენობით.


# ინფორმაცია ნიდერლანდების მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ ტაქსის აპლიკაცია „უბერის“ მონაცემთა გადაცემის წესის დარღვევისთვის დაჯარიმების შესახებ

ნიდერლანდების მონაცემთა დაცვის საზედამხედველო ორგანომ ტაქსის კომპანია „უბერი“ €290 მილიონი ევროთი დააჯარიმა, ევროპელი ტაქსის მძღოლების შესახებ პერსონალური მონაცემების გადაცემისათვის ამავე კომპანიის ამერიკის სერვერებზე. ტაქსის კომპანია მონაცემებს გადასცემდა ისეთი მეთოდებით, რომელიც არ ფილტრავდა გადასაცემ ინფორმაციას.

ნიდერლანდების მონაცემთა დაცვის საზედამხედველო ორგანომ აღმოაჩინა, რომ ტაქსის აპლიკაცია ორი წლის განმავლობაში აგროვებდა და ამერიკის სერვერებზე ინახავდა ევროპელი ტაქსის მძღოლების განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს, მათ შორის, ფოტოსურათებს, პირადობის დამადასტურებელი, ტაქსის ლიცენზიების, გეოგრაფიული მდებარეობის, სამედიცინო და გადახდების ინფორმაციას.

საზედამხედველო ორგანოს განცხადებით, განსაკუთრებული კატეგორიის მონაცემები ამერიკის სერვერებზე მონაცემთა დაცვის ზომების გათვალისწინების გარეშე გადაიცემოდა, რაც მონაცემთა დაცვის ძირითადი რეგულაციის სერიოზულ დარღვევად მიიჩნევა. ბოლო ხუთი წლის განმავლობაში, მონაცემთა გადაცემისათვის წესების დარღვევისათვის კომპანია „უბერი“ მეხუთედ დაჯარიმდა.

**გამოძიების დაწყების საფუძველი**

ნიდერლანდების მონაცემთა დაცვის საზედამხედველო ორგანომ გამოძიება დაიწყო 170 ფრანგი ტაქსის მძღოლის მიერ 2021 წელს ფრანგულ არასამთავრობო ორგანიზაციაში „ადამიანის უფლებების ლიგა“ („Ligue des droits de l’Homme“) საჩივრის შეტანის საფუძველზე.

ტაქსის კომპანიის სათავო ოფისი ევროპის, აფრიკის და შუა აღმოსავლეთის რეგიონისათვის ამსტერდამშია დაფუძნებული, შესაბამისად, წინამდებარე გამოძიება ნიდერლანდების მონაცემთა დაცვის საზედამხედველო ორგანოს უფლებამოსილების სფეროში მოექცა. ნიდერლანდების მონაცემთა დაცვის საზედამხედველო ორგანომ გასულ წელს კომპანია „უბერი“ 10 მილიონი, ხოლო 2016 წელს 600 ათასი ევროს ოდენობით დააჯარიმა.

2023 წლის დეკემბერში საზედამხედველო ორგანომ გამოავლინა, რომ ტაქსის კომპანია დროულად არ პასუხობდა მონაცემთა სუბიექტების (კომპანიაში დასაქმებული მძღოლების) მოთხოვნებს იმ ინფორმაციის მიწოდების თაობაზე, რომელსაც კომპანია ფლობდა და ამუშავებდა კომპანიაში დასაქმებული მძღოლების შესახებ.

ამავდროულად, საფრანგეთის მონაცემთა საზედამხედველო ორგანოსთან თანამშრომლობით, ნიდერლანდების მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ კომპანიის მონაცემთა დაცვის პოლიტიკის დოკუმენტი არასრულ ინფორმაციას შეიცავდა მონაცემთა ამერიკის შეერთებულ შტატებში გადაცემის თაობაზე. საფრანგეთის საზედამხედველო ორგანომ წინამდებარე ჯარიმის მნიშვნელობას ხაზი გაუსვა, და აღნიშნა გამჭვირვალობის უდიდესი მნიშვნელობა მონაცემთა კანონიერად გადაცემისა და მონაცემთა სუბიექტების უფლებების დაცვისათვის.

ტაქსის კომპანია „უბერის“ საპასუხო განცხადება

ტაქსის კომპანია მონაცემთა სუბიექტებისათვის ინფორმაციის მოთხოვნაზე პასუხის დაგვიანების შემთხვევებს უარყოფს. კომპანიის განცხადებით 2023 წელს დაკისრებული ჯარიმის შესახებ გადაწყვეტილება გასაჩივრდა და კვლავ განხილვის პროცესშია.

ტაქსის კომპანიამ შეწყვიტა მონაცემთა გადაცემის ის პრაქტიკა, რომლისთვისაც დაჯარიმდა[5] და აპირებს გაასაჩივროს ბოლო, 2024 წლის ჯარიმა, ვინაიდან ჯარიმის შესახებ მონაცემთა დაცვის საზედამხედველო ორგანოს მსჯელობას დაუსაბუთებლად მიიჩნევს.

.

## ინფორმაცია გაერთიანებული სამეფოს მონაცემთა საზედამხედველო ორგანოს კონფიდენციალურობის პოლიტიკის ინსტრუმენტის ( ” Privacy Notice Generator”) შესახებ

2024 წლის 20 აგვისტოს გაერთიანებული სამეფოს საზედამხედველო ორგანომ გამოაქვეყნა კონფიდენციალურობის პოლიტიკის ონლაინ ინსტრუმენტი”Privacy Notice Generator“ [2]მცირე და საშუალო ზომის დაწესებულებებისათვის.

ინსტრუმენტი დაწესებულებებს ეხმარება პერსონალიზებული მონაცემთა დაცვის პოლიტიკის დოკუმენტის შემუშავებაში. მისი გამოყენება შეუძლიათ დაწესებულებებსა და ორგანიზაციებს, რომლებიც მუშაობენ ეკონომიკის, ფინანსების, სადაზღვევო, სამართლის, განათლების, ბავშვებზე მზრუნველობის, გაყიდვების, წარმოებისა და არაკომერციულ სფეროში. ინსტრუმენტი მიზნად ისახავს მონაცემთა დაცვის კანონმდებლობის მარტივად გასაგები რესურსებითა და ფორმატით გადმოცემას.

.

ინსტრუმენტი ორ სხვადასხვა ტიპის პოლიტიკის დოკუმენტს ქმნის: პირველი ტიპი გათვლილია ორგანიზაციის შიდა კომუნიკაციისა და გამოყენებისთვის, მეორე კი იქმნება ვებგვერდებზე გამოსაქვეყნებლად, გარე მომხმარებლებთან საკომუნიკაციო მიზნებისათვის. ინსტრუმენტი შეიქმნა საზედამხედველო ორგანოს სტრატეგიული გეგმის „ICO25“-ის ფარგლებში, საზედამხედველო ორგანოს მიერ შეთავაზებული მომსახურეობის გაუმჯობესებისა და მცირე ბიზნესებისათვის შესაბამისობის საკითხებში გარკვევის გასამარტივებლად.

საზედამხედველო ორგანოს განცხადებით, მცირე ბიზნესებთან სისტემატიური დიალოგის საფუძველზე დადგინდა, რომ ხშირად მცირე ბიზნესებს არ გააჩნიათ მონაცემთა მართვისათვის სათანადო დრო და რესურსები. ინსტრუმენტის შექმნის პროცესში მიმდინარეობდა კონსულტაციები პოტენციურ მომხმარებლებთან, მათი საჭიროებების მაქსიმალურად გათვალისწინების მიზნით.

ინსტრუმენტმა ჩაანაცვლა მონაცემთა სუბიექტების ინფორმირების წესი, რომელიც შაბლონის ფორმით იყო შედგენილი მცირე ბიზნესებისათვის. ბიზნესები ამ ფორმაზე დაყრდნობით მონაცემთა სუბიექტებს უხსნიდნენ, თუ როგორ იქნებოდა გამოყენებული მათი პერსონალური მონაცემები, თუმცა, წინამდებარე ფორმა არ იყო მარტივად აღსაქმელი და მცირე ბიზნესები ხშირად მიმართავდნენ კითხვებით საზედამხედველო ორგანოს.

გაზაფხულიდან ინსტრუმენტის სატესტო გამოყენება დაიწყო ორმოცმა ბიზნესმა. პირველ თვეში გამოსაცდელი რეჟიმით დაინტერესდა 5,000 დაწესებულება. ხელსაწყო უფასოა, იგი მომხმარებლებმა დადებითად შეაფასეს. გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანო მზადყოფნას გამოხატავს, დაეხმაროს ბიზნესებს ინსტრუმენტის გამოყენების საკითხებში.

# კომპანია “Meta” სოციალურ ქსელების მომხმარებელთა საჯაროდ ხელმისაწვდომ ფოტოებსა და პოსტებს საკუთარი ხელოვნური ინტელექტის შემოწმების მიზნით გამოიყენებს

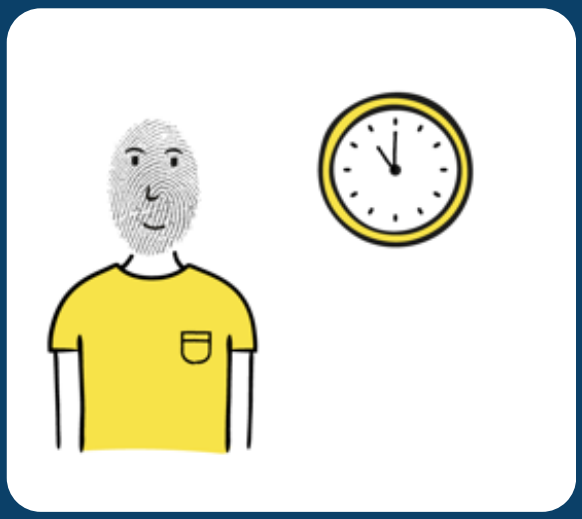
კომპანია “Meta”-ს მიერ საკუთარი ხელოვნური ინტელექტის შემოწმების მიზნით, „ფეისბუქსა“ და „ინსტაგრამში“ განთავსებული საჯარო ფოტოებისა და პოსტების გამოყენებას ფართო გამოხმაურება მოჰყვა. საკითხს განსაკუთრებული რეზონანსი ავსტრალიაში მოჰყვა, როდესაც რეგისტრირებული მომხმარებლებისთვის ცნობილი გახდა, რომ მათგან განსხვავებით, ევროკავშირის წევრ სახელმწიფოებში რეგისტრირებულ მომხმარებლებს შეეძლოთ უარი განეცხადებინათ საჯაროდ განთავსებული ფოტოებისა და პოსტების აღნიშნული მიზნით გამოყენებაზე.

მიმდინარე წლის ივლისში, კომპანია “Meta”-მ დაადასტურა, რომ შეჩერდებოდა ევროკავშირის წევრ სახელმწიფოებში რეგისტრირებული მომხმარებლების პერსონალურ მონაცემთა გამოყენება ხელოვნური ინტელექტის ტესტირებისთვის. მიუხედავად ამისა, მომხმარებლებს მიეცათ არჩევანის თავისუფლება, რათა საჯაროდ განთავსებული მონაცემები ხელმისაწვდომი გამხდარიყო დამუშავების აღნიშნული მიზნებისათვის.

ავსტრალიის ხელისუფლების წარმომადგენლებისთვის გაურკვეველი აღმოჩნდა ის სტანდარტი, რომელიც კომპანიამ ევროკავშირში რეგისტრირებული მომხმარებლების მიმართ დაადგინა. კომპანია “Meta”-მ განმარტა, რომ აღნიშნული გადაწყვეტილება ევროკავშირში მოქმედი პერსონალურ მონაცემთა დაცვის კანონმდებლობის მოთხოვნებიდან გამომდინარეობდა და სოციალური ქსელების მომხმარებელთა რაიმე ნიშნით დაყოფის მიზანს არ ატარებდა. ამდენად, ავსტრალიაში სოციალურ პლატფორმებზე 2007 წლიდან რეგისტრირებული მომხმარებლების მიერ საჯაროდ განთავსებული ფოტოები და პოსტები ხელოვნური ინტელექტის ტესტირებისთვის იქნება გამოყენებული, რომლის პრევენციის ერთადერთ საშუალებას მომხმარებლების მიერ საკუთარი მონაცემების წაშლა ან საჯარო გამოქვეყნების შეზღუდვა წარმოადგენს.

ავსტრალიაში რეგისტრირებულ მილიონობით მომხმარებელს კომპანია “Meta”-ს გადაწყვეტილება არჩევანის წინაშე აყენებს, შეწყვიტონ აღნიშნული სოციალური ქსელებით სარგებლობა ან მათი სარგებლობით ავტომატურად დაეთანხმონ საკუთარი მონაცემების გამოყენებას ხელოვნური ინტელექტის ტესტირებისთვის.

საგულისხმოა, რომ საკითხის შესაფასებლად ავსტრალიის ხელისუფლების წარმომადგენლები მთავრობას დროულ რეაგირებას სთხოვენ.



# ბელგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შესახებ

გაფრთხილების საფუძვლები:

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვისსაზედამხედველო ორგანომ(“ICO”) ბრიტანეთის ლეიბორისტული პარტიისმიმართ, მონაცემთასუბიექტების განცხადების საფუძველზე, გაფრთხილება გასცა.[1]საქმის ფაქტობრივი გარემოებების თანახმად, განმცხადებელთა მოთხოვნისმიუხედავად, პარტიამათ არაწვდიდა ინფორმაციას პერსონალური მონაცემების დამუშავების თაობაზე. აღსანიშნავია, რომ 2022 წლის ნოემბერშილეიბორისტულ პარტიას 352-მა სუბიექტმამიმართა, რომელთა 78%-ს პარტიისაგან კანონით განსაზღვრულ სამი თვისვადაში არმიუღია პასუხი, ხოლო 56%-მაერთი წლისდაგვიანებით მიიღოპასუხი. მიმართვისმიზეზი 2021 წლისოქტომბერში პარტიაზეგანხორციელებული კიბერშეტევა იყო. შესაბამისად, მონაცემთასუბიექტებს აინტერესებდათ, რა ინფორმაციას ინახავდა პარტიამათ შესახებ. მონაცემთა უსაფრთხოების დარღვევით (ინციდენტით) გამოწვეული მაღალი მიმართვიანობიდან გამომდინარე, პარტიამ ვერშეძლო კანონითგანსაზღვრულ ვადაშიმონაცემთა სუბიექტების მოთხოვნის შესაბამისად ინფორმაციის გაცემა.

საკითხისშესწავლის პროცესშიდიდი ბრიტანეთის საზედამხედველო ორგანომდაადგინა, რომმონაცემთა დაცვისსაკითხებზე ინფორმაციის მიღების სპეციალურსივრცეში (‘privacy inbox’) ფიქსირდებოდა 646 მონაცემთა სუბიექტის ინფორმაციის მოთხოვნის შესახებ განცხადება და 597 მოთხოვნა პერსონალური მონაცემების წაშლის თაობაზე, რომელთაგან ყველა პასუხგაუცემელი იყო.

საზედამხედველო ორგანოს მიერ საკითხის შესაწავლის დაწყების შემდგომ, პარტიამ შექმნა სამი თანამშრომლისგან შემდგარი ჯგუფი, რომელიც მხოლოდ მონაცემთა სუბიექტების მიერ მოთხოვნილ ინფორმაციაზე საპასუხოდ მუშაობდა. ასევე, პარტიამ შეიმუშავა სამოქმედო გეგმა და გამოყო ბიუჯეტი ინციდენტის საპასუხოდ ღონისძიებათა განსახორციელებლად. საზედამხედველო ორგანოს განცხადებით, პარტია სამოქმედო გეგმის შესაბამისად პასუხობს მონაცემთა სუბიექტების მოთხოვნებს, რათა უზრუნველყოს მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობა.

მონაცემთა სუბიექტების უფლებები:

მონაცემთასუბიექტის უფლებაა, მოითხოვოს ნებისმიერი ორგანიზაციისგან ანდაწესებულებისგან ინფორმაცია იმის თაობაზე, თუ რაინფორმაციას ფლობსდამუშავებისთვის პასუხისმგებელი პირი მისიპერსონალური მონაცემების შესახებ და მუშავდებათუ არამისი მონაცემი. მონაცემთა სუბიექტებს ასევე გააჩნიათინფორმაციის შესწორების, დაბლოკვის, განახლების, დამატების, განადგურების ანწაშლის მოთხოვნისუფლებაც.

საზედამხედველო ორგანომ ხაზგასმით აღნიშნა მონაცემთა სუბიექტების შესახებ მონაცემის სისწორის შენარჩუნების ვალდებულება. აგრეთვე, პარტია ვალდებული იყო დროულად ეპასუხა მონაცემთა სუბიექტების მოთხოვნებს პერსონალური მონაცემების დამუშავების თაობაზე.[1]

მონაცემთა სუბიექტების მიერ ინფორმაციის მოთხოვნაზე პასუხის ვადები გაერთიანებულ სამეფოში:

ბრიტანული „მონაცემთა დაცვის ძირითადი რეგულაციის“ თანახმად, მონაცემთა სუბიექტის ინფორმაციის მოთხოვნაზე საპასუხოდ დამუშავებისთვის პასუხისმგებელ პირს ერთი თვე აქვს განსაზღვრული, რაც შესაძლოა ორი თვით გაგრძელდეს, გამომდინარე მოთხოვნილი ინფორმაციის რაოდენობიდან და მოთხოვნის შესრულების სირთულიდან.

მონაცემთა სუბიექტების მიერ ინფორმაციის მოთხოვნაზე პასუხის ვადები საქართველოში:

აღსანიშნავია, რომ „პერსონალურ მონაცემთადაცვის შესახებ“ საქართველოს კანონისთანახმად, მონაცემთა სუბიექტს უფლება აქვს, მონაცემთა დამუშავებისთვის პასუხისმგებელი ან/და მონაცემთა დამუშავებაზე უფლებამოსილი პირისაგან ინფორმაცია მიიღოს მისი მოთხოვნიდან არაუგვიანეს 10 სამუშაო დღისა. აღნიშნული ვადა განსაკუთრებულ შემთხვევებში და სათანადო დასაბუთებით შეიძლება,გაგრძელდეს არაუმეტეს 10 სამუშაო დღით, რის შესახებაც მონაცემთა სუბიექტს დაუყოვნებლივ უნდა ეცნობოს.


## ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) გამო ტანსაცმლის მაღაზიათა ქსელის “UNIQLO”-ს დააჯარიმის შესახებ

2024 წლის 12 აგვისტოს, ესპანეთისპერსონალურ მონაცემთადაცვის საზედამხედველო ორგანომ გამოაქვეყნა ინფორმაცია ტანსაცმლის მაღაზიათა ქსელის “UNIQLO EUROPE LTD (UNIQLO)” ფილიალის 450 000 ევროს ოდენობითდაჯარიმების შესახებ, რომელიც შემდგომში 270 000 ევრომდე შემცირდა.

გადაწყვეტილების დასაბუთება:

საქმისფაქტობრივი გარემოებების თანახმად, სერვისის მიმწოდებელმა “UNIQLO”-ს მოსთხოვა გადახდების შესახებ ინფორმაცია, რომლის საპასუხოდელექტრონული ფოსტითგაგზავნილ იქნა UNIQLO-ს თანამშრომლების ფინანსურინფორმაციის შემცველიდოკუმენტი, კერძოდ, ივლისში კომპანიისმიერ დასაქმებულთათვის გადახდილ სამუშაოსანაზღაურება. დოკუმენტიაერთიანებდა შემდეგიტიპის პერსონალურ მონაცემებს:[1]პირთა სახელიდა გვარი, პირადობის დამადასტურებელი დოკუმენტების ნომრები, სოციალურ სერვისებზე წვდომის ნომრები, საბანკო ანგარიშების ნომრები. აღნიშნულიდან გამომდინარე, საზედამხედველო ორგანოსმონაცემთა სუბიექტისსაჩივარი 2023 წლის 31 მარტს წარედგინა.

2024 წლის 12 აგვისტოს, ესპანეთისპერსონალურ მონაცემთადაცვის საზედამხედველო ორგანომ გამოაქვეყნა ინფორმაცია ტანსაცმლის მაღაზიათა ქსელის “UNIQLO EUROPE LTD (UNIQLO)” ფილიალის 450 000 ევროს ოდენობითდაჯარიმების შესახებ, რომელიც შემდგომში 270 000 ევრომდე შემცირდა.

გადაწყვეტილების დასაბუთება:

საქმისფაქტობრივი გარემოებების თანახმად, სერვისის მიმწოდებელმა “UNIQLO”-ს მოსთხოვა გადახდების შესახებ ინფორმაცია, რომლის საპასუხოდელექტრონული ფოსტითგაგზავნილ იქნა UNIQLO-ს თანამშრომლების ფინანსურინფორმაციის შემცველიდოკუმენტი, კერძოდ, ივლისში კომპანიისმიერ დასაქმებულთათვის გადახდილ სამუშაოსანაზღაურება. დოკუმენტიაერთიანებდა შემდეგტიპის პერსონალურ მონაცემებს:[1]პირთა სახელიდა გვარი, პირადობის დამადასტურებელი დოკუმენტების ნომრები, სოციალურ სერვისებზე წვდომის ნომრები, საბანკო ანგარიშების ნომრები. აღნიშნულიდან გამომდინარე, საზედამხედველო ორგანოსმონაცემთა სუბიექტისსაჩივარი 2023 წლის 31 მარტს წარედგინა.

## ჰოლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება სახის ამომცნობი ტექნოლოგიისათვის მონაცემების უკანონოდ შეგროვების შესახებ

საქმის ფაქტობრივი გარემოებები:

ჰოლანდიისპერსონალურ მონაცემთადაცვის საზედამხედველო ორგანომ კომპანია “Clearview AI” 30.5 მილიონი ევროსოდენობით დააჯარიმა.

საქმისფაქტობრივი გარემოებების თანახმად, “Clearview AI” ამერიკულიკომპანიაა, რომელიცმომხმარებლებს სახისამომცნობი ტექნოლოგიების სფეროში საგამოძიებო მიზნებისათვის მომსახურებას სთავაზობდა. კერძოდ, კომპანიისმომხმარებლებს შეეძლოთფოტოსურათის მიწოდებისსაფუძველზე, დაედგინათფოტოზე გამოსახული პირის იდენტობა. აღსანიშნავია, რომკომპანიამ კანონისდარღვევით შექმნამონაცემთა ბაზა, რომელიც 30 ბილიონზემეტი ინდივიდის, მათ შორის, ჰოლანდიელთა სახისამსახველ ფოტოსურათს შეიცავდა.

მონაცემთაბაზის შესაქმნელად, “Clearview”ფოტოსურათებს ინტერნეტიდან ავტომატურ რეჟიმშიიღებდა (“data scraping”),[1]რის შემდეგაციგი, თითოეულიინდივიდის გამოსახულების შესაბამისად, ფოტოსურათებს უნიკალურბიომეტრიულ კოდადგარდაქმნიდა. აღსანიშნავია, რომ მონაცემთასუბიექტები არფლობდნენ კომპანიისმიერ მათიპერსონალური მონაცემების დამუშავების შესახებინფორმაცია. შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირს არჰქონდა მოპოვებული მათი თანხმობაპერსონალურ მონაცემთადამუშავებაზე.

ჰოლანდიისპერსონალურ მონაცემთადაცვის საზედამხედველო ორგანოს განცხადებით, სახის ამომცნობიტექნოლოგიები მხოლოდაუცილებელი საჭიროებების პირობებში უნდაიქნას გამოყენებული, ამავდროულად, განსაკუთრებული სიფრთხილის ზომების დაცვით. საზედამხედველო ორგანოსგანცხადებით, სახისამომცნობი ტექნოლოგიების როლი დანაშაულთან ბრძოლის დადამნაშავეების იდენტიფიცირების თვალსაზრისით, მნიშვნელოვანია. თუმცაამ სფეროშიმომსახურების გაწევაარა კერძობიზნესების, არამედსაჯარო სტრუქტურების უფლებამოსილების სფეროშიუნდა ექცეოდეს, ისიც მხოლოდდა მხოლოდგანსაკუთრებული საჭიროებების შემთხვევაში. მაგალითად, შესაძლებელია, რომ პერსონალურ მონაცემთადაცვის საზედამხედველო ორგანოსთან თანამშრომლობის საფუძველზე, პოლიციამ აწარმოოს ამგვარმონაცემთა ბაზა.

ჩადენილი სამართალდარღვევის შეფასება:

“Clearview AI”-მ განაცხადა, რომიგი მომხმარებლებს მომსახურებას ევროკავშირის ფარგლებს გარეთსთავაზობდა. ჰოლანდიისმონაცემთა დაცვისსაზედამხედველო ორგანომაღნიშნა, რომკომპანიამ დაარღვიაევროკავშირის „მონაცემთადაცვის ძირითადრეგულაციის“ წესებიდა შესაბამისად, მისი მომსახურებით სარგებლობაც კანონდარღვევას წარმოადგენდა, რის საფუძველზეც საზედამხედველო ორგანომ მონაცემთასუბიექტებს მოუწოდა, არ ისარგებლონ აღნიშნული მომსახურებით.

გარდა აღნიშნულისა,“Clearview AI”-ს არჰქონდა სამართლებრივი საფუძველი, რათა შეექმნა ფოტოსურათებისა და უნიკალურიბიომეტრიული კოდებისშემცველი მონაცემთაბაზა, რომელთაცდამატებით სხვაინფორმაცია უკავშირდება. მონაცემთა დაცვისშესახებ კანონმდებლობის საფუძველზე, მონაცემთა ბაზაშიაღრიცხულ მონაცემთასუბიექტებს გააჩნიათ პერსონალურ მონაცემებზე წვდომის უფლება. აღნიშნული გულისხმობს მონაცემთა სუბიექტების მიმართ კომპანიისვალდებულებას, მათიმოთხოვნის შემთხვევაში, განმარტოს თურა ინფორმაციას ფლობს მათზე. აღსანიშნავია, რომკომპანია არპასუხობდა მონაცემთასუბიექტების მოთხოვნებს მათ მონაცემებზე წვდომის უფლებისუზრუნველყოფის თაობაზე.

დამამძიმებელი გარემოებები:

კომპანიამსაქმიანობა არცჰოლანდიის საზედამხედველო ორგანოს მიერგამოძიების დაწყებისშემდგომ შეწყვიტა. შესაბამისად, საზედამხედველო ორგანომ გასცაბრძანება მონაცემთადამუშავების შეწყვეტისმოთხოვნის თაობაზე.

ამერიკული კომპანია ევროპული წარმომადგენლობის გარეშე:

დამუშავებისთვის პასუხისმგებელი პირიამერიკულ კომპანიასწარმოადგენდა დამას ევროკავშირში არ ჰყავდაწარმომადგენლობა. ამასთანავე, “Clearview AI”-ი პერსონალურ მონაცემთა დაცვისსაზედამხედველო ორგანოებმა არაერთხელ დააჯარიმეს ევროპელი მონაცემთასუბიექტების მონაცემთაუკანონო დამუშავების გამო.

ყოველივეზემოაღნიშნულის გათვალისწინებით, ჰოლანდიის პერსონალურ მონაცემთა დაცვისსაზედამხედველო ორგანომკომპანია სამართალდამრღვევად ცნო, ამასთან “Clearview AI”-ს დაკისრებული ჯარიმაარ გაუსაჩივრებია.

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