VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

DUK. Ar gali darbdavys naudoti veido atpažinimo technologiją patekimo į patalpas kontrolės tikslu?

2026 m. lapkričio 23 d.

Valstybinė duomenų apsaugos inspekcija (toliau – VDAI) sulaukia organizacijų klausimų dėl veido atpažinimo technologijų diegimo ir naudojimo siekiant kontroliuoti patekimą į įmonės komercines, gamybines patalpas ar teritoriją.

Atsižvelgiant į Bendrojo duomenų apsaugos reglamento (toliau – BDAR) 4 straipsnio 14 punkte pateiktą biometrinių duomenų sąvoką, veido atpažinimas (taip pat ir veido atvaizdų palyginimas) yra biometrinių duomenų tvarkymas, todėl naudojant veido atpažinimo technologiją būtina laikytis asmens duomenų apsaugos reikalavimų, numatytų BDAR.

Pagal BDAR 9 straipsnio 1 dalį biometriniai duomenys priskiriami prie specialių kategorijų asmens duomenų ir jų tvarkymui keliami griežtesni reikalavimai, t. y. pagal bendrą taisyklę juos tvarkyti draudžiama, išskyrus 9 straipsnio 2 dalyje numatytas išimtis, pavyzdžiui:

- kai duomenų subjektas aiškiai sutiko, kad tokie asmens duomenys būtų tvarkomi vienu ar keliais nurodytais tikslais, arba
- esant kitoms BDAR 9 straipsnio 2 dalies b–j punktuose nurodytoms draudimo tvarkyti specialių kategorijų duomenis išimtims.

Taigi, įmonėje siekiant įdiegti veido atpažinimo technologiją patekimo į patalpas ar teritoriją kontrolės tikslu reikia nustatyti teisėto asmens duomenų tvarkymo sąlygą pagal BDAR 6 straipsnį ir draudimo tvarkyti specialių kategorijų duomenis išimtį pagal BDAR 9 straipsnį.

Pažymėtina, kad prieš diegiant veido atpažinimo technologiją būtina atlikti poveikio duomenų apsaugai vertinimą[1], kuriame taip pat turėtų būti įvertinta, ar tokios priemonės diegimas yra *būtinas ir proporcingas*, atsižvelgiant į duomenų tvarkymo tikslą, jų tvarkymo kontekstą, t. y. kur ir kokiomis aplinkybėmis technologija bus naudojama, ir poveikį asmeniui, kurio biometriniai asmens duomenys būtų tvarkomi. Rekomenduojama pagrįsti, kaip biometrinių duomenų naudojimas atitinka organizacijos poreikius, bei nustačius, kad tokių duomenų tvarkymas galimas, rinktis mažiau privatumą ribojančias alternatyvas (pavyzdžiui, paties darbdavio biometrinio šablono kopijos nesaugomos).

Duomenų valdytojas privalo užtikrinti, kad duomenų subjekto (darbuotojo) sutikimas būtų išreikštas aiškiu pareiškimu[2]. Jei asmuo nesutinka su aptariamu duomenų tvarkymu arba atšaukia anksčiau išreikštą sutikimą, jam privalo būti sudaryta galimybė patekti į įmonės komercines, gamybines patalpas ar teritoriją netvarkant jo biometrinių duomenų (išskyrus atvejus, kai toks duomenų tvarkymas yra

[1] BDAR 35 straipsnio 3 dalies b punktas ir Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo 4 punktas.

[2] Plačiau apie reikalavimus sutikimui skaitykite Europos duomenų apsaugos valdybos Gairėse 05/2020 dėl sutikimo pagal Reglamentą 2016/679. Pastebėtina, kad dėl darbdavio ir darbuotojo galios disbalanso darbuotojo sutikimas paprastai nėra tinkamas pagrindas tvarkyti biometrinius duomenis. Juo galima remtis tik išimtinėmis aplinkybėmis, kai atsisakymas sutikti ar sutikimo atšaukimas nesukelia neigiamų pasekmių.

reglamentuojamas teisės aktu), pavyzdžiui, pasinaudojant raktu, prieigos kortele, suvedant unikalų PIN kodą ar pan. (be papildomų apribojimų ar išlaidų).

Atkreiptinas dėmesys, kad jeigu biometrinių duomenų tvarkymas negali būti grindžiamas duomenų subjekto sutikimu, toks tvarkymas gali būti vykdomas tik tuo atveju, jei tai aiškiai reglamentuota Europos Sąjungos ar nacionaliniuose teisės aktuose (pavyzdžiui, vykdant teisinę prievolę arba vadovaujantis sudaryta kolektyvine sutartimi (BDAR 9 straipsnio 2 dalies b punktas) arba dėl svarbaus viešojo intereso (BDAR 9 straipsnio 2 dalies g punktas)).

Pastebėtina, kad vien siekis užtikrinti patogesnį ar greitesnį patekimą į patalpas ar teritoriją savaime nepagrindžia veido atpažinimo technologijos naudojimo būtinumo.

Prieš pasirenkant tokią technologiją, būtina įvertinti numatomo duomenų tvarkymo teisėtumą, būtinumą, proporcingumą, atitiktį duomenų kiekio mažinimo principui ir įvertinti, ar to paties tikslo negalima pasiekti mažiau privatumą ribojančiomis priemonėmis.

Plačiau apie biometrinių duomenų tvarkymą skaitykite:

1. 29 straipsnio darbo grupės Nuomonė 3/2012 dėl biometrinių technologijų pokyčių;
2. 29 straipsnio darbo grupės Nuomonė 2/2012 dėl veido atpažinimo internetinėse ir mobiliosiose paslaugose;
3. Jungtinės Karalystės Informacijos komisaro biuro (ICO) Gairės dėl specialių kategorijų asmens duomenų tvarkymo;
4. Prancūzijos Nacionalinės informacijos ir laisvių komisijos (CNIL) parengtas „DUK. Biometrinė patekimo kontrolė darbo vietose: kokiomis sąlygomis?“.
