VALSTYBINĖ
DUOMENŲ APSAUGOS
INSPEKCIJA

SPORTO KLUBUOSE ATLIEKAMO BIOMETRINIŲ DUOMENŲ TVARKYMO TEISĖTUMO TIKRINIMŲ APIBENDRINIMAS

2019-05-29

Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija), vykdydama Inspekcijos direktoriaus 2019 m. vasario 4 d. patvirtintą Valstybinės duomenų apsaugos inspekcijos 2019 metų prevencinių patikrinimų planą Nr. 3R-100(1.41.), atliko pirštų atspaudų tvarkymo teisėtumo patikrinimą 3 bendrovėms priklausančiuose sporto klubuose.

Atlikus patikrinimus nustatyta, kad tikrintos bendrovės tvarko ne piršto atspaudus, bet piršto atspaudo modelius – binarinius kodus. Tokių duomenų tvarkymo tikslai – praėjimo į sporto klubus, darbo vietą kontrolė.

Remiantis Direktyvos 95/46/EB 29 straipsniu įsteigtos Darbo grupės asmenų apsaugai tvarkant asmens duomenis 2012 m. balandžio 27 d. priimta Nuomone Nr. 3/2012 dėl biometrinių technologijų pokyčių (WP 193), piršto atspaudo modelis laikytinas *biometriniais* asmens duomenimis.

Biometriniai duomenys – po specialaus techninio apdorojimo gauti asmens duomenys, susiję su žmogaus fizinėmis, fiziologinėmis arba elgesio savybėmis, leidžiančiomis nustatyti arba patvirtinti to asmens tapatybę.

2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR), kuris pradėtas taikyti nuo 2018 m. gegužės 25 d., biometrinių duomenų tvarkymui skiriamas ypatingas dėmesys. 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 sąlygas.

Dėl sutikimo, kaip klientų pirštų atspaudų modelių teisėto tvarkymo sąlygos

Visos 3 patikrintos bendrovės Inspekcijai nurodė, kad pirštų atspaudų modelius jie tvarko remiantis BDAR 9 straipsnio 2 dalies a punktu, kuriame numatyta, kad draudimas tvarkyti specialių kategorijų asmens duomenis netaikomas, jei duomenų subjektas aiškiai *sutiko,* kad tokie asmens duomenys būtų tvarkomi vienu ar keliais nurodytais tikslais.

Pagal BDAR 4 straipsnio 11 punktą duomenų subjekto *sutikimas* – tai bet koks laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais, kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys. BDAR 7 straipsnio 2 dalyje numatyta, kad jeigu duomenų subjekto sutikimas duodamas rašytiniu pareiškimu, susijusiu ir su kitais klausimais, prašymas duoti sutikimą pateikiamas tokiu būdu, kad jis būtų aiškiai atskirtas nuo kitų klausimų, pateiktas suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba.

Atsižvelgiant į tai, kad tikrintos bendrovės saugo ne pačius pirštų atspaudus, o tik jų *modelius* (binarinius kodus), Inspekcija laikosi pozicijos, kad šiuos duomenis galima tvarkyti, gavus aiškius, nedviprasmiškus, tinkamai informuotų klientų *sutikimus* ir suteikiant jiems *alternatyvias* identifikavimosi galimybes (netvarkant pirštų atspaudų modelių).

Patikrinimų metu nustatyta, kad vienos iš 3 patikrintų bendrovių sporto klubuose klientams nėra pasiūloma lygiavertė, laisvai pasirenkama, identifikavimosi sporto klubuose alternatyva (nenaudojant

pirštų atspaudų modelių), t. y. klientų duodamas sutikimas tvarkyti jų pirštų atspaudų modelius nėra laisvas, todėl bendrovė klientų pirštų atspaudų modelius tvarko neteisėtai. Kitų 2 bendrovių sporto klubuose, nors ir suteikiama alternatyva klientams identifikuotis kitais būdais (nenaudojant pirštų atspaudų), tačiau visgi pirmenybė teikiama klientų identifikavimuisi piršto atspaudo modelio pagalba, t. y. kitos alternatyvos pasiūlomos tik tuomet, jeigu asmuo nesutinka su piršto atspaudo modelio tvarkymu.

Dėl teisės atšaukti sutikimą

Pastebėtina, kad tvarkant asmens duomenis asmens sutikimu, duomenų subjektas pagal BDAR 7 straipsnio 3 dalį turi teisę bet kuriuo metu *atšaukti* savo sutikimą. Sutikimo atšaukimas nedaro poveikio sutikimu pagrįsto duomenų tvarkymo, atlikto iki sutikimo atšaukimo, teisėtumui. Duomenų subjektas apie tai informuojamas prieš jam duodant sutikimą. Atšaukti sutikimą turi būti taip pat *lengva* kaip jį duoti.

Atliekant patikrinimus nustatyta, kad 1 iš 3 patikrintų bendrovių klientams, kaip duomenų subjektams, nepateikia visos BDAR 13 straipsnio 1 ir 2 dalyse nurodytos informacijos, pvz., apie teisę į duomenų perkeliamumą, teisę apriboti duomenų tvarkymą, bei neinformuoja apie jų teisę atšaukti savo sutikimą dėl biometrinių duomenų tvarkymo.

Dėl darbuotojų pirštų atspaudų modelių tvarkymo

Direktyvos 95/46/EB 29 straipsniu įsteigta Darbo grupė asmenų apsaugai tvarkant asmens duomenis 2012 m. balandžio 27 d. Nuomonėje Nr. 3/2012 dėl biometrinių technologijų pokyčių (WP 193) nurodė, kad „sutikimas, jeigu jis yra susijęs su darbo santykiais, turi būti vertinamas kritiškai ir turi būti tinkamai pagrįstas. Užuot siekę gauti sutikimą, darbdaviai galėtų išnagrinėti, ar teisėtu tikslu tikrai būtina naudoti darbuotojų biometrinius duomenis, ir įvertinti, ar toks darbuotojų biometrinių duomenų naudojimas turi įtakos jų pagrindinėms teisėms ir laisvėms. <...> Darbdavys visada turi ieškoti *mažiausiai* privatumą pažeidžiančių priemonių ir, jeigu įmanoma, pasirinkti su biometrinių duomenų tvarkymu nesusijusias priemones“.

Įvertinusi tai, kad pagal BDAR 9 straipsnio 1 dalį biometrinius duomenis tvarkyti draudžiama, nebent būtų bent viena iš šio straipsnio 2 dalyje numatytų sąlygų, o darbuotojo sutikimas dėl galios disbalanso *nelaikytinas laisvu*, Inspekcija nusprendė, kad darbuotojų pirštų atspaudų modeliai tvarkomi neteisėtai, nesant BDAR 9 straipsnio 2 dalyje nu matytos išimties ir tuo pažeidžiant BDAR 5 straipsnio 1 dalies a (teisėtumo principą) ir c (duomenų kiekio mažinimo principą) punktus bei 9 straipsnio 1 dalį.

Dėl poveikio duomenų apsaugai vertinimo

Atlikus tikrinimus nustatyta, kad ne visos bendrovės yra atlikusios poveikio duomenų apsaugai vertinimą, kaip to reikalauja BDAR 35 straipsnis. Inspekcija mano, kad, atsižvelgiant į pasikeitusį biometrinių duomenų teisinį vertinimą, pirštų atspaudų modelius tvarkančios bendrovės turėjo pareigą *atlikti poveikio duomenų apsaugai vertinimą*.

Atkreiptinas duomenų valdytojų dėmesys į tai, kad nepaisant to, jog Inspekcija iki BDAR taikymo pradžios buvo įvertinusi jų atliekamą asmens duomenų tvarkymo teisėtumą, duomenų valdytojas *nėra atleidžiamas* nuo pareigos atlikti poveikio duomenų apsaugai vertinimą. Šiuo atveju, Inspekcijos nuomone, biometrinių duomenų tvarkymo reguliavimo pokyčiai, t. y. jų priskyrimas specialių kategorijų asmens duomenims, yra ta aplinkybė, kuri reikalauja peržiūrėti asmens duomenų tvarkymo teisinius pagrindus bei įvertinti jų tvarkymo keliamus pavojus bei taikomas saugumo priemones šiems pavojams sumažinti, todėl ir poveikio duomenų apsaugai vertinimą tikrintos bendrovės turėjo atlikti.

Dėl techninių ir organizacinių duomenų saugumo priemonių

Atlikus patikrinimus, nustatyta, kad visos 3 bendrovės pakankamai *neužtikrina* tvarkomų pirštų atspaudų modelių *saugumo*.

Įvertinus asmens duomenų tvarkymo operacijų poveikį ir atitinkamų grėsmių atsiradimo tikimybę, nustatyta, kad bendras rizikos vertinimas (rizikos lygis) yra *aukštas*. Atsižvelgiant į tai, kad saugumo spragų viešas atskleidimas keltų dar didesnę riziką asmens duomenų saugumui, jos nebus viešai atskleidžiamos. Visgi, Inspekcija atkreipia dėmesį, kad tvarkant asmens duomenis automatiniu būdu, privaloma užtikrinti tinkamas organizacines ir technines saugumo priemones, kurios parenkamos įvertinus riziką, susijusią su pavojais fizinių asmenų teisėms ir laisvėms, prieš pradedant asmens duomenų tvarkymą automatiniu būdu. Atlikti tikrinimai parodė, kad dažnu atveju duomenų valdytojai neužtikrina net kai kurių esminių duomenų saugumo priemonių, tokių kaip:

- Detalaus organizacijos informacijos saugos valdymo nustatymas, aiškiai apibrėžiant ir dokumentuojant darbuotojų atsakomybes bei vaidmenis, prieigos kontrolės politikos nustatymas;
- Techninės, programinės ir tinklo įrangos inventorizavimo ir atnaujinimo įgyvendinimas;
- Pagrindinių procedūrų, kurių reikia laikytis incidento ar asmens duomenų saugumo pažeidimo atveju, nustatymas;
- Užtikrinimas, kad darbuotojai gebėtų konfidencialiai tvarkyti informaciją tiek techniniu, tiek asmeninio sąžiningumo požiūriu ir kad jie būtų tinkamai išmokyti IT sistemų saugumo kontrolės.

Atkreiptinas duomenų valdytojų dėmesys į tai, kad būtina turėti prieigų prie kompiuterinių darbo vietų kontrolės sistemą. Ne ką mažiau svarbu duomenų bazes ir taikomąsias programas, tarnybines stotis sukonfigūruoti taip, kad jos naudotų atskirą paskyrą su priskirtomis žemiausiomis operacinės sistemos privilegijomis. Kai prieiga prie naudojamų asmens duomenų yra vykdoma kompiuteriniu tinklu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus. Taip pat privaloma įgyvendinti fizinę patalpų, kuriose yra IT sistemų infrastruktūra, apsaugą nuo neautorizuotos prieigos.

Dar kartą primename apie Inspekcijos parengtas Tinkamų organizacinių ir techninių saugumo priemonių įgyvendinimo gaires asmens duomenų valdytojams ir duomenų tvarkytojams, kurias galite rasti šiuo adresu:

https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_tech_priemones_gaires_2018.pdf.

Atlikus minėtus tikrinimus bendrovėms pateikti nurodymai pašalinti Inspekcijos nustatytus pažeidimus. Vienai iš jų nurodyta sustabdyti klientų pirštų atspaudų modelių tvarkymą, iki kol bus atliktas poveikio duomenų apsaugai vertinimas ir užtikrinta atitiktis visiems BDAR reikalavimams, dviem – nutraukti darbuotojų pirštų atspaudų modelių tvarkymą, visoms trims – užtikrinti technines ir organizacines duomenų saugumo priemones.