VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

PATIKRINIMŲ DĖL REIKALAVIMŲ, SUSIJUSIŲ SU DUOMENŲ APSAUGOS PAREIGŪNO VEIKLA, ĮGYVENDINIMO REZULTATŲ APIBENDRINIMAS

2023 m.

Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija), vadovaudamasi Valstybinės duomenų apsaugos inspekcijos 2022 metų planinių patikrinimų ir stebėsenos planu, atliko patikrinimus dėl reikalavimų, susijusių su duomenų apsaugos pareigūno (toliau – DAP) veikla, įgyvendinimo. Patikrinimai buvo atliekami, naudojant patvirtintą kontrolinį klausimyną.

Inspekcija, apibendrindama atliktų patikrinimų rezultatus, išskyrė toliau pateiktus dažniausiai nustatytus su DAP veikla susijusius neatitikimus 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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) reikalavimams.

DAP paskyrimas, jam keliami reikalavimai ir pavedamos užduotys

1. Interesų konfliktas. Patikrinimų metu nustatyta, kad dalis duomenų valdytojų paskyrė DAP duomenų valdytojo vadovą arba paskirtas DAP atliko saugos įgaliotinio ar kitas funkcijas, kurios susijusios su sprendimų priėmimu dėl asmens duomenų tvarkymo tikslų, apimties ir kt.

BDAR 38 straipsnio 6 dalyje reglamentuota, jog DAP gali vykdyti ir kitas užduotis bei pareigas, tačiau duomenų valdytojas arba duomenų tvarkytojas turi užtikrinti, kad dėl bet kokių tokių užduočių ir pareigų nekiltų interesų konfliktas. 29 straipsnio duomenų apsaugos darbo grupės 2016-12-13 duomenų apsaugos pareigūnų gairėse (toliau – DAP gairės) (3.5 dalis „Interesų konfliktas“) yra pažymėta, kad: *„<...> DAP negali organizacijoje eiti pareigų, pagal kurias jis turėtų nustatyti asmens duomenų tvarkymo tikslus ir priemones. <...> Paprastai tokios interesų konfliktą galinčios sukelti pareigybės organizacijoje, be kita ko, gali būti vyresniosios vadovybės pareigybės (pvz., generalinis direktorius, operacijų vadovas, vyriausiasis finansininkas, vyriausiasis gydytojas, rinkodaros padalinio vadovas, žmogiškųjų išteklių arba IT padalinio vadovas), tačiau tai gali būti ir žemesnio lygio pareigos organizacijos struktūroje, jeigu vykdant tas pareigas arba funkcijas reikia nustatyti duomenų tvarkymo tikslus ir priemones.“*

Atsižvelgdama į tai, Inspekcija pakartotinai atkreipia dėmesį į tai, kad DAP negali eiti pareigų, susijusių su asmens duomenų tvarkymo tikslų ir priemonių nustatymu.

2. Paskiriami keli DAP, tačiau nėra atskirtos jų atsakomybės. Inspekcija atkreipia dėmesį, kad DAP gairėse nustatyta, jog atsižvelgiant į organizacijos dydį ir struktūrą, gali prireikti sudaryti DAP grupę (DAP ir jo darbuotojai). Tokiais atvejais turėtų būti aiškiai parengta grupės vidaus struktūra ir išdėstytos kiekvieno jos nario užduotys ir pareigos. Panašiai, kai DAP funkciją atlieka išorinis paslaugų teikėjas, tam subjektui dirbanti asmenų grupė gali veiksmingai atlikti DAP užduotis kaip komanda, kuriai vadovauja klientui paskirtas vadovaujantis kontaktinis asmuo. Be kita ko, aiškinant sistemiškai tiek DAP gaires, tiek BDAR, Inspekcija pažymi, jog yra kalbama apie vieno asmens, kaip DAP paskyrimą, kartu sudarant galimybę turėti komandą.

Inspekcija atkreipia dėmesį, kad jeigu yra poreikis turėti ne vieną DAP, turėtų būti paskiriamas vienas DAP ir sudaroma jo komanda su atitinkamai aiškiai nustatytomis DAP atsakomybėmis ir funkcijų pasidalinimu.

3. DAP veiklos tęstinumo neužtikrinimas. Patikrinimų metu nustatyta, kad dalis duomenų valdytojų yra pasitelkę DAP išorės paslaugų teikėjus. Tai nėra draudžiama, tačiau patikrinimų metu pasitaikė atvejų, kai DAP paslaugų teikimo sutartyje nustatytas paslaugų teikimo ribojimas valandomis, pavyzdžiui, kad DAP paslaugos apima ne daugiau kaip 60 valandų per metus ir duomenų valdytojas nėra nusimatęs priemonių dėl DAP veiklos tęstinumo, kai baigsis numatytas valandų limitas.

Inspekcija pažymi, kad turi būti užtikrinamas DAP veiklos tęstinumas, todėl tokiais atvejais turi būti nustatytas konkretus procesas, kas atliks DAP funkcijas, pasibaigus nustatytam valandų limitui dėl DAP funkcijų paslaugų teikimo.

DAP atskaitomybė ir informavimas apie paskirtą DAP

1. Nėra užtikrinamas periodinis atsiskaitymas vadovybei. BDAR 38 straipsnio 3 dalyje reglamentuota, kad DAP tiesiogiai atsiskaito duomenų valdytojo arba duomenų tvarkytojo aukščiausio lygio vadovybei. DAP gairėse yra papildomai paaiškinta, kad „*tokiomis tiesioginėmis ataskaitomis užtikrinama, kad vyresnioji vadovybė (pvz., direktorių valdyba) žinotų apie duomenų apsaugos pareigūno konsultacijas ir rekomendacijas, kurias jis teikia vykdydamas savo įgaliojimus informuoti ir konsultuoti duomenų valdytoją arba duomenų tvarkytoją. Kitas tiesioginio ataskaitų teikimo pavyzdys yra aukščiausio lygio vadovybei teikiamos duomenų apsaugos pareigūno veiklos metinės ataskaitos rengimas*.“ Patikrinimų metu nustatyta, kad dalis duomenų valdytojų nėra reglamentavę atsiskaitymų vadovybei formos ir nėra užtikrinamas atsiskaitymų aukščiausiajai vadovybei periodiškumas.

Inspekcija pažymi, kad turi būti reglamentuotas DAP atsiskaitymo duomenų valdytojo vadovybei periodiškumas ir atsiskaitymo forma.

2. Nepakankamas darbuotojų informavimas apie paskirtą DAP. Patikrinimų metu nustatyta, kad nors yra paskiriamas DAP, nurodomi jo kontaktiniai duomenys interneto ar duomenų valdytojo intraneto svetainėje, bet nėra imamasi papildomų informavimo priemonių, kad darbuotojai žinotų apie paskirtą DAP ir jo atliekamas funkcijas.

Inspekcija atkreipia dėmesį, kad darbuotojai turi būti tinkamai informuojami (pavyzdžiui, periodiškai išsiunčiant informaciją / priminimus) apie paskirtą DAP ir jo funkcijas, kad galėtų lengvai ir tiesiogiai susisiekti su DAP ir spręsti klausimus, susijusius su BDAR taikymu.

3. Apie paskirtą ar pasikeitusį DAP nėra informuojama Inspekcija. BDAR 37 straipsnio 7 dalyje reikalaujama, kad duomenų valdytojas arba duomenų tvarkytojas nurodytų DAP kontaktinius duomenis atitinkamoms priežiūros institucijoms. Patikrinimų metu nustatyta, kad dalis duomenų valdytojų nebuvo informavę Inspekcijos apie paskirtą ar pasikeitusį DAP.

Atsižvelgiant į tai, Inspekcija pakartotinai primena, kad jeigu yra paskiriamas DAP arba jeigu pasikeitė DAP ar DAP nebevykdo DAP pareigų, Inspekcija turi būti informuota apie tokį pasikeitimą.

DAP teikiamos konsultacijos, BDAR laikymosi priežiūra, auditai ir kitos atliekamos funkcijos

1. Nepritarimas DAP nuomonei. BDAR 39 straipsnio 1 dalies a ir b punktuose reglamentuota, kad DAP informuoja duomenų valdytoją arba duomenų tvarkytoją ir duomenis tvarkančius darbuotojus apie jų prievoles pagal šį reglamentą ir kitus Sąjungos arba valstybės narės apsaugos nuostatas ir konsultuoja juos šiais klausimais; stebi, kaip laikomasi šio reglamento, kitų Sąjungos arba nacionalinės duomenų apsaugos nuostatų ir duomenų valdytojo arba duomenų tvarkytojo politikos asmens duomenų apsaugos srityje, įskaitant pareigų pavedimą, duomenų tvarkymo operacijose dalyvaujančių darbuotojų informuotumo didinimą bei mokymą ir susijusius auditus. Patikrinimų metu nustatyta, kad nėra atskirai dokumentuota procedūra, kokių veiksmų imamasi bei kas priima sprendimus, jeigu nepritariama DAP nuomonei.

Atsižvelgiant į tai, Inspekcija pažymi, kad turi būti nustatytas procesas, kokie veiksmai turi būti atliekami, kai nepritariama DAP nuomonei.

2. Reikalavimų, susijusių su auditų atlikimu, neįgyvendinimas. BDAR 39 straipsnio 1 dalies b punkte nustatyta, kad DAP stebi, kaip laikomasi BDAR, kitų Sąjungos arba nacionalinės duomenų apsaugos nuostatų ir duomenų valdytojo arba duomenų tvarkytojo politikos asmens duomenų apsaugos srityje bei atlieka susijusius auditus. BDAR 39 straipsnio 2 dalyje reglamentuota, kad DAP, vykdydamas savo užduotis, tinkamai įvertina su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus. DAP gairėse yra paaiškinta, kad „<...> *duomenų apsaugos pareigūnas privalo savo veiklą suskirstyti prioritetais ir daugiausia dėmesio skirti tiems klausimams, kurie kelia didžiausią pavojų duomenų apsaugai.* <...> *Šis atrankusis pragmatinis požiūris turėtų padėti duomenų apsaugos pareigūnams konsultuoti duomenų valdytoją, kokią metodiką naudoti atliekant poveikio duomenų apsaugai vertinimą, kokių sričių vidaus ar išorės duomenų apsaugos auditas turėtų būti atliekamas, kokius vidinius mokymus organizuoti už duomenų tvarkymo veiklą atsakingiems darbuotojams ar vadovybei ir kokioms duomenų tvarkymo operacijoms skirti daugiau savo laiko ir išteklių*“. Patikrinimų metu nustatyta, kad nors BDAR numatyta, kad DAP privalo atlikti atitikties BDAR reikalavimams vertinimus ir (ar) auditus, tačiau tik maža dalis DAP šiuos vertinimus / auditus buvo atlikę.

Atsižvelgiant į tai, DAP privalo periodiškai atlikti atitikties BDAR reikalavimams vertinimus / auditus ir su vertinimo / audito rezultatais supažindinti duomenų valdytoją. Atitinkamai duomenų valdytojas turėtų suteikti visas galimybes šiuos vertinimus / auditus DAP atlikti.

Daugiau informacijos apie reikalavimus dėl DAP galite rasti čia:

- Valstybinės duomenų apsaugos inspekcijos rekomendacija dėl duomenų apsaugos pareigūnų skyrimo viešajame sektoriuje ir jų veiklos reglamentavimo ypatumų>>
- 29 straipsnio duomenų apsaugos darbo grupės 2016-12-13 duomenų apsaugos pareigūnų gairės>>
- CNIL Practical Guide GDPR for Data protection officers>>