

WP243 PRIEDAS. DAŽNAI UŽDUODAMI KLAUSIMAI

Šio priedo tikslas – paprasta ir suprantama forma atsakyti į kai kuriuos pagrindinius klausimus, kurie gali kilti organizacijoms dėl naujų Bendrojo duomenų apsaugos reglamento reikalavimų paskirti duomenų apsaugos pareigūną.

Duomenų apsaugos pareigūno paskyrimas (37 straipsnis)

1 Kurios organizacijos privalo paskirti duomenų apsaugos pareigūną (37 straipsnio 1 dalis)?

Bendrajame duomenų apsaugos reglamente reikalaujama, kad duomenų apsaugos pareigūnas būtų paskirtas trimis konkrečiais atvejais:

- duomenis tvarko valdžios institucija arba įstaiga (neatsižvelgiant į tai, kokie duomenys tvarkomi);
- duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus, ir
- duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra specialių kategorijų duomenų tvarkymas dideliu mastu arba asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu.

Atkreipkite dėmesį, kad Sąjungos arba valstybės narės teisėje duomenų apsaugos pareigūną gali būti reikalaujama paskirti ir kitais atvejais. Galiausiai, kai Bendrajame duomenų apsaugos reglamente konkrečiai nereikalaujama paskirti duomenų apsaugos pareigūno, organizacijoms kartais gali būti naudinga jį paskirti savanoriškai. 29 straipsnio duomenų apsaugos darbo grupė (WP29) skatina šią savanorišką praktiką.

Daugiau informacijos žr. gairių 2.1 skirsnyje.

2 Ką reiškia sąvoka pagrindinė veikla (37 straipsnio 1 dalies b ir c punktai)?

Pagrindinė veikla gali būti laikomos svarbiausios operacijos duomenų valdytojo arba duomenų tvarkytojo tikslams pasiekti. Ji taip pat apima visą veiklą, kai duomenų tvarkymas sudaro neatskiriamą duomenų valdytojo arba duomenų tvarkytojo veiklos dalį. Pavyzdžiui, duomenų apie sveikatą, tokių kaip pacientų medicinos dokumentai, tvarkymas turėtų būti laikomas viena iš pagrindinių ligoninės veiklos sričių, todėl ligoninės turi paskirti duomenų apsaugos pareigūnus.

Kita vertus, visos organizacijos vykdo tam tikrą pagalbinę veiklą, pavyzdžiui, moka darbo užmokestį savo darbuotojams arba vykdo standartinę IT sistemų priežiūros veiklą. Tai yra pagrindinei organizacijos veiklai arba pagrindiniam verslui reikalingos pagalbinės funkcijos. Nors ši veikla yra reikalinga arba būtina, ji paprastai laikoma pagalbinėmis funkcijomis, o ne pagrindine veikla.

Daugiau informacijos žr. gairių 2.1.2 skirsnyje.

3 Ką reiškia sąvoka dideliu mastu (37 straipsnio 1 dalies b ir c punktai)?

Bendrajame duomenų apsaugos reglamente neapibrėžta, kas yra didelis mastas. WP29 rekomenduoja nustatant, ar duomenų tvarkymas vykdomas dideliu mastu, visų pirma atsižvelgti į šiuos veiksnius:

- susijusių duomenų subjektų skaičių – konkretų skaičių arba atitinkamo gyventojų skaičiaus

procentinę dalį;

- įvairių tvarkomų duomenų vienetų kiekį ir (arba) intervalą;
- duomenų tvarkymo veiklos trukmę arba pastovumą;
- geografinę duomenų tvarkymo veiklos aprėptį.

Duomenų tvarkymo dideliu mastu pavyzdžiai:

- pacientų duomenų tvarkymas ligoninės įprastinės veiklos metu;
- asmens kelionių naudojantis viešojo transporto sistema duomenų tvarkymas (pvz., sekimas naudojant kelionės korteles);
- tarptautinio greitojo maisto tinklo klientų geografinės vietos duomenų tvarkymas tikruoju laiku statistikos tikslais, kai tai daro šioje srityje besispecializuojantis duomenų tvarkytojas;
- klientų duomenų tvarkymas draudimo bendrovės arba banko įprastinės veiklos metu;
- asmens duomenų tvarkymas paieškos sistemoje vartotojų elgesiu grindžiamos reklamos tikslais;
- duomenų (turinio, srauto, vietos duomenų) tvarkymas, kai tai daro telefono ryšio arba interneto paslaugų teikėjai.

Pavyzdžiai, kai duomenų tvarkymas nelaikomas duomenų tvarkymu dideliu mastu:

- asmens duomenų tvarkymas, kai tai daro pavienis gydytojas;
- asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas, kai tai daro pavienis advokatas.

Daugiau informacijos žr. gairių 2.1.3 skirsnyje.

4 Ką reiškia sąvoka *reguliariai ir sistemingai stebėti* (37 straipsnio 1 dalies b punktas)?

Reguliarus ir sistemingo duomenų subjektų stebėjimo sąvoka Bendrajame duomenų apsaugos reglamente nėra apibrėžta, bet ji akivaizdžiai apima visų formų stebėjimą ir profiliavimą internete, taip pat vartotojų elgesiu grindžiamos reklamos tikslais. Vis dėlto stebėjimo sąvoka taikoma ne tik internetinėje aplinkoje.

WP29 vertinimu, sąvoka *reguliarus* reiškia vieną arba keletą šių dalykų:

- vykstantis arba pasitaikantis tam tikrais intervalais konkrečiu laikotarpiu;
- pasikartojantis arba kartojamas konkrečiu metu;
- vykstantis nuolat arba periodiškai.

WP29 vertinimu, sąvoka *sistemingas* reiškia vieną arba keletą šių dalykų:

- vykstantis pagal tam tikrą sistemą;
- iš anksto suplanuotas, suorganizuotas arba metodiškas;
- vykdomas kaip bendro duomenų rinkimo plano dalis;
- vykdomas kaip strategijos dalis.

Pavyzdžiai: telekomunikacijų tinklo eksploatavimas, telekomunikacijų paslaugų teikimas; pakartotinis kreipimasis e. paštu; profiliavimas ir vertinimas balais rizikos vertinimo tikslais (pvz., siekiant įvertinti kreditingumą, nustatyti draudimo įmokas, užkirsti kelią sukčiavimui, nustatyti pinigų plovimo atvejus); vietos sekimas, pavyzdžiui, mobiliosiomis programėlėmis; lojalumo programos; vartotojų elgesiu grindžiama reklama; savijautos, fizinės formos ir sveikatos duomenų stebėjimas dėvimais

įrenginiais; apsauginė vaizdo stebėjimo sistema; sujungtieji įrenginiai, pvz., išmanieji skaitikliai, išmanieji automobiliai, namų automatizavimas ir kt.

Daugiau informacijos žr. gairių 2.1.4 skirsnyje.

5 Ar gali organizacijos duomenų apsaugos pareigūną paskirti bendrai? Jei taip, kokiomis sąlygomis (37 straipsnio 2 ir 3 dalys)?

Bendrajame duomenų apsaugos reglamente numatyta, kad įmonių grupė gali paskirti vieną bendrą duomenų apsaugos pareigūną, jeigu su juo yra *lengva susisiekti iš kiekvienos buveinės*. Lengvo susisiektimo sąvoka susijusi su duomenų apsaugos pareigūno, kaip kontaktinio asmens, užduotimis palaikyti ryšius su duomenų subjektais, priežiūros institucijomis, taip pat pačioje organizacijoje. Siekiant užtikrinti, kad su duomenų apsaugos pareigūnu, nesvarbu, ar jis dirba pačioje organizacijoje, ar už jos ribų, būtų lengva susisiekti, svarbu pasirūpinti, kad būtų pateikti jo kontaktiniai duomenys, kaip nurodyta Bendrajame duomenų apsaugos reglamente. Duomenų apsaugos pareigūnas turi turėti galimybę efektyviai bendrauti su duomenų subjektais ir bendradarbiauti su atitinkamomis priežiūros institucijomis. Tai reiškia, kad šis bendravimas turi vykti priežiūros institucijų ir atitinkamų duomenų subjektų vartojamomis viena arba keliomis kalbomis. Siekiant užtikrinti, kad duomenų subjektai galėtų susisiekti su duomenų apsaugos pareigūnu, labai svarbu suteikti galimybę asmeniškai į jį kreiptis (arba fiziškai, kai jis yra tose pačiose patalpose kaip ir darbuotojai, arba karštąja linija ar kitomis saugiomis ryšių priemonėmis).

Daugiau informacijos žr. gairių 2.3 skirsnyje.

6 Ar įmanoma paskirti išorinį duomenų apsaugos pareigūną (37 straipsnio 6 dalis)?

Taip. Pagal 37 straipsnio 6 dalį duomenų apsaugos pareigūnas gali būti duomenų valdytojo arba duomenų tvarkytojo personalo narys (vidinis duomenų apsaugos pareigūnas) arba atlikti užduotis pagal paslaugų teikimo sutartį. Tai reiškia, kad duomenų apsaugos pareigūnas gali būti išorinis ir šiuo atveju jis savo funkcijas gali vykdyti pagal paslaugų sutartį, sudarytą su asmeniu ar organizacija.

Jeigu duomenų apsaugos pareigūnas yra išorinis, tokiam duomenų apsaugos pareigūnui taikomi visi 37–39 straipsnių reikalavimai. Kaip nurodyta gairėse, kai duomenų apsaugos pareigūno funkciją atlieka išorinis paslaugų teikėjas, tam subjektui dirbanti asmenų grupė gali veiksmingai atlikti duomenų apsaugos pareigūno užduotis kaip komanda, kuriai vadovauja paskirtas vadovaujantis kontaktinis asmuo ir *už klientą atsakingas* asmuo. Šiuo atveju būtina, kad kiekvienas išorinės organizacijos, atliekančios duomenų apsaugos pareigūno funkciją, narys įvykdytų visus atitinkamus Bendrojo duomenų apsaugos reglamento reikalavimus.

Siekiant teisinio aiškumo ir gero organizavimo, gairėse rekomenduojama paslaugų sutartyje aiškiai paskirstyti užduotis išorinės duomenų apsaugos pareigūno grupės nariams ir vieną asmenį paskirti už klientą atsakingu vadovaujančiu kontaktiniu asmeniu.

Daugiau informacijos žr. gairių 2.3, 2.4 ir 3.5 skirsniuose.

7 Kokias profesines savybes turėtų turėti duomenų apsaugos pareigūnas (37 straipsnio 5 dalis)?

Bendrajame duomenų apsaugos reglamente reikalaujama, kad duomenų apsaugos pareigūnas būtų *paskiriamas remiantis profesinėmis savybėmis, visų pirma duomenų apsaugos teisės ir praktikos ekspertinėmis žiniomis, taip pat gebėjimu atlikti 39 straipsnyje nurodytas užduotis.*

Būtiną ekspertinių žinių lygį turėtų būti nustatomas atsižvelgiant į atliekamas duomenų tvarkymo operacijas ir reikiamą tvarkomų asmens duomenų apsaugą. Pavyzdžiui, kai duomenų tvarkymo veikla yra itin sudėtinga arba tvarkoma daug neskelbtinų duomenų, duomenų apsaugos pareigūnui gali prireikti aukštesnio lygio ekspertinių žinių ir pagalbos.

Reikiami gebėjimai ir ekspertinės žinios – tai, be kita ko:

- nacionalinės ir Europos duomenų apsaugos teisės aktų ir praktikos ekspertinės žinios, taip pat išsamus Bendrojo duomenų apsaugos reglamento supratimas;
- atliekamų duomenų tvarkymo operacijų supratimas;
- informacinių technologijų ir duomenų saugumo išmanymas;
- žinios apie verslo sektorių ir organizaciją;
- gebėjimas organizacijoje skatinti duomenų apsaugos kultūrą.

Daugiau informacijos žr. gairių 2.4 skirsnyje.

Duomenų apsaugos pareigūno statusas (38 straipsnis)

8 Kokie ištekliai turėtų būti skiriami duomenų apsaugos pareigūnui, kad jis galėtų atlikti savo užduotis?

Bendrojo duomenų apsaugos reglamento 38 straipsnio 2 dalyje reikalaujama, kad organizacija padėtų savo duomenų apsaugos pareigūnui suteikdama jo *užduotims atlikti būtinus išteklius, taip pat suteikdama galimybę susipažinti su asmens duomenimis, dalyvauti duomenų tvarkymo operacijose ir išlaikyti savo ekspertines žinias.*

Atsižvelgiant į duomenų tvarkymo operacijų pobūdį ir organizacijos veiklą bei dydį, duomenų apsaugos pareigūnui turėtų būti suteikiami šie ištekliai:

- aktyvi vyresniosios vadovybės parama duomenų apsaugos pareigūnui einant savo pareigas;
- pakankamai laiko duomenų apsaugos pareigūnui jo pareigoms atlikti;
- pakankama parama finansiniais ištekliais, infrastruktūra (aprūpinant patalpomis, priemonėmis, įranga), o prireikus – ir darbuotojais;
- oficialus pranešimas apie duomenų apsaugos pareigūno paskyrimą visiems darbuotojams;
- galimybė naudotis kitomis organizacijos tarnybomis, kad duomenų apsaugos pareigūnas iš tų tarnybų galėtų gauti būtiną paramą, pagalbinius duomenis ar informaciją;
- nuolatinis mokymas.

Daugiau informacijos žr. gairių 3.2 skirsnyje.

9 Kokios yra apsaugos priemonės, kad duomenų apsaugos pareigūnas galėtų nepriklausomai atlikti savo užduotis (38 straipsnio 3 dalis)?

Taikomos kelios apsaugos priemonės, kad duomenų apsaugos pareigūnai galėtų veikti nepriklausomai, kaip nurodyta 97 konstatuojamojoje dalyje:

- duomenų valdytojai arba duomenų tvarkytojai negali duoti nurodymų dėl duomenų apsaugos pareigūno užduočių vykdymo;
- duomenų tvarkytojas negali duomenų apsaugos pareigūno atleisti arba bausti dėl jam nustatytų užduočių atlikimo;
- užtikrinama, kad dėl galimų kitų užduočių ir pareigų nekiltų interesų konflikto.

Daugiau informacijos žr. gairių 3.3–3.5 skirsniuose.

10 Dėl kokių kitų duomenų apsaugos pareigūno užduočių ir pareigų gali kilti interesų konfliktas (38 straipsnio 6 dalis)?

Duomenų apsaugos pareigūnas negali organizacijoje eiti pareigų, kurias vykdant jam reikėtų nustatyti asmens duomenų tvarkymo tikslus ir priemones. Dėl kiekvienos organizacijos specifinės struktūros į tai turi būti atsižvelgiama kiekvienu konkrečiu atveju.

Paprastai tokios interesų konfliktą galinčios sukelti pareigybės, 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.

Daugiau informacijos žr. gairių 3.5 skirsnyje.

Duomenų apsaugos pareigūno užduotys (39 straipsnis)

11 Ką apima sąvoka *stebėti, kaip laikomasi [Bendrojo duomenų apsaugos] reglamento* (39 straipsnio 1 dalies b punktas)?

Vykdydamas šias užduotis – stebėti, kaip laikomasi reglamento, – duomenų apsaugos pareigūnas visų pirma gali:

- rinkti informaciją duomenų tvarkymo veiklai identifikuoti,
- nagrinėti ir tikrinti, ar duomenų tvarkymo veikla atitinka reikalavimus, ir
- informuoti duomenų valdytoją ar duomenų tvarkytoją, jį konsultuoti ir teikti jam rekomendacijas.

Daugiau informacijos žr. gairių 4.1 skirsnyje.

12 Ar duomenų apsaugos pareigūnas yra asmeniškai atsakingas, jei nesilaikoma Bendrojo duomenų apsaugos reglamento?

Ne, duomenų apsaugos pareigūnai nėra asmeniškai atsakingi, jei nesilaikoma Bendrojo duomenų apsaugos reglamento. Bendrajame duomenų apsaugos reglamente aiškiai nustatyta, kad būtent duomenų valdytojas arba duomenų tvarkytojas privalo užtikrinti ir sugebėti *įrodyti, kad duomenys tvarkomi laikantis šio reglamento* (24 straipsnio 1 dalis). Už tai, kad duomenų tvarkymas atitiktų reikalavimus, atsakingas duomenų valdytojas arba duomenų tvarkytojas.

13 Koks yra duomenų apsaugos pareigūno vaidmuo vertinant poveikį duomenų apsaugai (37 straipsnio 1 dalies c punktas) ir tvarkant duomenų tvarkymo veiklos įrašus (30 straipsnis)?

Poveikio duomenų apsaugai klausimu duomenų valdytojas arba duomenų tvarkytojas turėtų kreiptis į duomenų apsaugos pareigūną konsultacijos, be kita ko, šiais klausimais:

- ar atlikti poveikio duomenų apsaugai vertinimą;
- kokia metodika vadovautis atliekant poveikio duomenų apsaugai vertinimą;
- ar poveikio duomenų apsaugai vertinimą atlikti pačioje organizacijoje, ar jį užsakyti;
- kokias apsaugos priemones (įskaitant technines ir organizacines priemones) taikyti siekiant sumažinti riziką duomenų subjektų teisėms ir interesams;
- ar tinkamai atliktas poveikio duomenų apsaugai vertinimas ir ar jo išvados (ar toliau tvarkyti duomenis ir kokias apsaugos priemones taikyti) atitinka Bendrojo duomenų apsaugos reglamento nuostatas.

Daugiau informacijos žr. gairių 4.2 skirsnyje.

Kalbant apie duomenų tvarkymo veiklos įrašus, būtent duomenų valdytojas arba duomenų tvarkytojas, o ne duomenų apsaugos pareigūnas, privalo tvarkyti duomenų tvarkymo operacijų įrašus. Vis dėlto niekas neužkerta duomenų valdytojui arba duomenų tvarkytojui kelio pavesiti duomenų apsaugos pareigūnui duomenų valdytojo atsakomybe tvarkyti duomenų tvarkymo operacijų įrašus. Tokie įrašai turėtų būti laikomi viena iš priemonių, kuriomis duomenų apsaugos pareigūnui sudaromos sąlygos atlikti savo užduotis stebėti, kaip laikomasi reikalavimų, informuoti ir konsultuoti duomenų valdytoją arba duomenų tvarkytoją.

Daugiau informacijos žr. gairių 4.4 skirsnyje.