29 STRAIPSNIO DUOMENŲ APSAUGOS DARBO GRUPĖ

16/LT
WP 243 rev.01

Duomenų apsaugos pareigūnų gairės

Priimta 2016 m. gruodžio 13 d.

Priimta su paskutiniais pakeitimais 2017 m. balandžio 5 d.

Ši darbo grupė sudaryta pagal Direktyvos 95/46/EB 29 straipsnį. Ji yra nepriklausomas Europos patariamasis organas duomenų apsaugos ir privatumo klausimais. Jos uždaviniai aprašyti Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 2002/58/EB 15 straipsnyje.

Sekretoriato paslaugas teikia Europos Komisijos Teisingumo ir vartotojų reikalų generalinio direktorato C direktoratas (Pagrindinės teisės ir teisinė valstybė), B-1049 Brussels, Belgium, Office No MO59 05/35.

Svetainė: http://ec.europa.eu/justice/data-protection/index_en.htm

ASMENŲ APSAUGOS TVARKANT ASMENS DUOMENIS DARBO GRUPĖ,

įkurta 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB,

atsižvelgdama į minėtos direktyvos 29 ir 30 straipsnius,

atsižvelgdama į savo Darbo tvarkos taisykles,

PRIĖMĖ ŠIAS GAIRES:

Turinys

1 Įvadas

2018 m. gegužės 25 d. įsigaliosiančiame Bendrajame duomenų apsaugos reglamente[1] nustatoma modernizuota, atskaitomybe pagrįsta Europos duomenų apsaugos reikalavimų laikymosi sistema. Šios naujos teisinės sistemos pagrindas daugeliui organizacijų bus duomenų apsaugos pareigūnas, padėsiantis laikytis Bendrojo duomenų apsaugos reglamento reikalavimų.

Pagal Bendrąjį duomenų apsaugos reglamentą tam tikriems duomenų valdytojams ir duomenų tvarkytojams privaloma paskirti duomenų apsaugos pareigūną[2]. Tai daryti privalės visos valdžios institucijos ir įstaigos (neatsižvelgiant į tai, kokius duomenis jos tvarko) ir kitos organizacijos, kurių pagrindinė veikla yra, be kita ko, dideliu mastu sistemingai stebėti asmenis arba dideliu mastu tvarkyti specialių kategorijų asmens duomenis.

Net 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 (toliau – WP29) skatina šią savanorišką praktiką.

Duomenų apsaugos pareigūno sąvoka nėra nauja. Nors Direktyvoje 95/46/EB[3] iš organizacijų nereikalaujama paskirti duomenų apsaugos pareigūno, keliose valstybėse narėse bėgant metams duomenų apsaugos pareigūno skyrimo praktika vis tiek buvo išplėtota.

Prieš priimant Bendrąjį duomenų apsaugos reglamentą, WP29 teigė, kad duomenų apsaugos pareigūnas yra atskaitomybės pagrindas ir kad paskyrus duomenų apsaugos pareigūną galima sudaryti palankesnes sąlygas laikytis reikalavimų, o, be to, verslo subjektams tai gali tapti konkurenciniu pranašumu[4]. Duomenų apsaugos pareigūnai ne tik padeda laikytis reikalavimų įgyvendindami atskaitomybės priemones (pvz., padeda atlikti poveikio duomenų apsaugai vertinimus ir atlieka arba padeda atlikti auditus), bet ir veikia kaip tarpininkai tarp įvairių suinteresuotųjų subjektų (pvz., priežiūros institucijų, duomenų subjektų ir organizacijos verslo padalinių).

Jei nesilaikoma Bendrojo duomenų apsaugos reglamento, duomenų apsaugos pareigūnai nėra už tai asmeniškai atsakingi. Bendrajame duomenų apsaugos reglamente aiškiai nustatyta, kad būtent duomenų valdytojas arba duomenų tvarkytojas privalo užtikrinti ir sugebėti įrodyti, kad duomenys

---

[1] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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) (OL L 119, 2016 5 4). Bendrasis duomenų apsaugos reglamentas yra svarbus Europos ekonominei erdvei (EEE) ir bus taikomas jį įtraukus į EEE susitarimą.

[2] Paskirti duomenų apsaugos pareigūną taip pat privaloma kompetentingoms institucijoms pagal 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016 5 4, p. 89–131) 32 straipsnį ir pagal nacionalinės teisės įgyvendinimo aktus. Nors šiose gairėse duomenų apsaugos pareigūno veiklos aspektai daugiausia aiškinami iš Bendrojo duomenų apsaugos reglamento perspektyvos, Duomenų apsaugos pareigūnų gairės taip pat aktualios pagal panašias Direktyvos 2016/680/ES nuostatas.

[3] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995 11 23, p. 31).

[4] Žr. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

tvarkomi laikantis reglamento nuostatų (24 straipsnio 1 dalis). Už duomenų tvarkymo atitiktį reikalavimams atsakingas duomenų valdytojas arba duomenų tvarkytojas.

Duomenų valdytojui arba duomenų tvarkytojui taip pat tenka itin svarbus vaidmuo – sudaryti duomenų apsaugos pareigūnui sąlygas veiksmingai atlikti savo užduotis. Duomenų apsaugos pareigūno paskyrimas yra pirmasis žingsnis, tačiau duomenų apsaugos pareigūnui taip pat reikia suteikti pakankamą autonomiją ir išteklių jo užduotims veiksmingai atlikti.

Bendrajame duomenų apsaugos reglamente duomenų apsaugos pareigūnas pripažįstamas vienu pagrindinių dalyvių naujojoje duomenų valdymo sistemoje, reglamente nustatytos jo paskyrimo sąlygos, statusas ir užduotys. Šių gairių tikslas – aiškiau išdėstyti atitinkamas Bendrojo duomenų apsaugos reglamento nuostatas siekiant padėti duomenų valdytojams ir duomenų tvarkytojams laikytis teisės akto ir padėti duomenų apsaugos pareigūnams atlikti savo funkciją. Gairėse taip pat pateikiamos geriausios patirties rekomendacijos, grindžiamos kai kurių ES valstybių narių įgyta patirtimi. WP29 stebės, kaip įgyvendinamos šios gairės, ir prireikus gali jas papildyti kita informacija.

2 Duomenų apsaugos pareigūno paskyrimas

2.1. Privalomas paskyrimas

Bendrojo duomenų apsaugos reglamento 37 straipsnio 1 dalyje reikalaujama, kad duomenų apsaugos pareigūnas būtų paskirtas trimis konkrečiais atvejais[5]:

a) duomenis tvarko valdžios institucija arba įstaiga[6];
b) duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus; arba
c) duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra specialių kategorijų duomenų[7] tvarkymas dideliu mastu arba[8] asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas[9] tvarkymas dideliu mastu.

Tolesniuose poskirsniuose WP29 pateikia gaires dėl kriterijų ir terminijos, vartojamų 37 straipsnio 1 dalyje.

Išskyrus atvejus, kai akivaizdu, kad organizacija neprivalo paskirti duomenų apsaugos pareigūno, WP29 rekomenduoja duomenų valdytojams ir duomenų tvarkytojams dokumentais įforminti vidinę analizę, atliktą siekiant nustatyti, ar turi būti skiriamas duomenų apsaugos pareigūnas, kad būtų galima

[5] Atkreipkite dėmesį, kad pagal 37 straipsnio 4 dalį Sąjungos arba valstybės narės teisėje duomenų apsaugos pareigūną gali būti reikalaujama paskirti ir kitais atvejais.
[6] Išskyrus teismus, kai jie vykdo savo teismines funkcijas. Žr. Direktyvos (ES) 2016/680 32 straipsnį.
[7] Pagal 9 straipsnį tai apima asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat genetinių duomenų ir biometrinių duomenų tvarkymą siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ar lytinę orientaciją.
[8] 37 straipsnio 1 dalies c punkte vartojamas žodis *ir*. Žr. tolesnį 2.1.5 skirsnį, kuriame paaiškinamas žodžio *ar* vartojimas vietoje žodžio *ir*.
[9] 10 straipsnis.

įrodyti, jog buvo tinkamai atsižvelgta į atitinkamus veiksnius[10]. Ši analizė sudaro atskaitomybės principu rengiamos dokumentacijos dalį. Priežiūros institucija gali šios analizės pareikalauti ir ji turi būti prireikus atnaujinama, pavyzdžiui, jeigu duomenų valdytojai ar duomenų tvarkytojai ima vykdyti naują veiklą arba teikti naujas paslaugas, galinčias patekti tarp 37 straipsnio 1 dalyje išvardytų atvejų.

Kai organizacija savanoriškai paskiria duomenų apsaugos pareigūną, jo paskyrimui, statusui ir užduotims taikomi 37–39 straipsnių reikalavimai, tarsi paskyrimas būtų buvęs privalomas.

Niekas neužkerta kelio organizacijai, kuri teisiškai neprivalo paskirti duomenų apsaugos pareigūno ir nepageidauja jo paskirti savanoriškai, vis tiek įdarbinti darbuotojų arba samdyti išorės konsultantų, kuriems būtų pavestos su asmens duomenų apsauga susijusios užduotys. Šiuo atveju svarbu užtikrinti, kad nekiltų painiavos dėl jų pareigybės pavadinimo, statuso, pareigų ir užduočių. Taigi, visuose įmonės vidaus pranešimuose ir bendraujant su duomenų apsaugos institucijomis, duomenų subjektais ir plačiąja visuomene reikėtų aiškiai nurodyti, kad šis asmuo ar konsultantas nėra duomenų apsaugos pareigūnas. [11]

Nesvarbu, ar duomenų apsaugos pareigūnas skiriamas privaloma tvarka, ar savanoriškai, jo veikla skirta visoms duomenų valdytojo ar duomenų tvarkytojo duomenų tvarkymo operacijoms.

[10] Žr. 24 straipsnio 1 dalį.

[11] Tai aktualu ir vyriausiesiems privatumo pareigūnams ar kitiems privatumo specialistams, šiandien jau dirbantiems kai kuriose įmonėse – jie gali ne visada atitikti Bendrojo duomenų apsaugos reglamento kriterijus, pavyzdžiui, dėl turimų išteklių ar nepriklausomumo garantijų, ir jeigu jie tų kriterijų neatitinka, jie negali būti laikomi ir vadinami duomenų apsaugos pareigūnais.

2.1.1 VALDŽIOS INSTITUCIJA ARBA ĮSTAIGA

Bendrajame duomenų apsaugos reglamente neapibrėžta, kas yra *valdžios institucija arba įstaiga*. WP29 mano, kad tokia sąvoka turi būti nustatyta pagal nacionalinę teisę. Taigi, valdžios institucijos ir įstaigos apima nacionalines, regionines ir vietos valdžios institucijas, tačiau pagal taikytinus nacionalinės teisės aktus ši koncepcija paprastai dar apima ir įvairias kitas viešosios teisės reglamentuojamas įstaigas[12]. Tokiais atvejais duomenų apsaugos pareigūną paskirti privaloma.

Užduotį viešojo intereso labui ir viešosios valdžios funkcijas gali vykdyti[13] ne tik valdžios institucijos ar įstaigos, bet ir kiti viešosios arba privatinės teisės reglamentuojami fiziniai ar juridiniai asmenys tokiuose kiekvienos valstybės narės nacionaliniu lygmeniu reglamentuojamuose sektoriuose kaip viešojo transporto paslaugos, vandens ir energijos tiekimas, kelių infrastruktūra, visuomeninis transliuotojas, socialinis būstas ar reguliuojamų profesijų drausminės atsakomybės organai.

Šiais atvejais duomenų subjektų padėtis gali būti labai panaši į tą, kai jų duomenis tvarko valdžios institucija ar įstaiga. Visų pirma duomenys gali būti tvarkomi panašiais tikslais ir asmenys dažnai turi vienodai mažai galimybių pasirinkti, ar jų duomenys bus tvarkomi ir kaip jie bus tvarkomi, arba tų galimybių apskritai neturi, taigi, jiems gali prireikti papildomos apsaugos, kuri gali būti suteikta paskyrus duomenų apsaugos pareigūną.

Nors tokiais atvejais ir neprivaloma, WP29 kaip gerąją patirtį rekomenduoja privačioms organizacijoms, vykdančioms užduotis viešojo intereso labui ar viešosios valdžios funkcijas, paskirti duomenų apsaugos pareigūną. Tokia duomenų apsaugos pareigūno veikla apima visas atliekamas duomenų tvarkymo operacijas, įskaitant nesusijusias su užduočių viešojo intereso labui arba oficialių pareigų vykdymu (pvz., darbuotojų duomenų bazės tvarkymas).

2.1.2 PAGRINDINĖ VEIKLA

Bendrojo duomenų apsaugos reglamento 37 straipsnio 1 dalies b ir c punktuose minima *duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla*. 97 konstatuojamojoje dalyje nurodyta, kad duomenų valdytojo pagrindinė veikla yra susijusi su jo *svarbiausia veikla ir nesusijusi su asmens duomenų tvarkymu kaip papildoma veikla*. *Pagrindine veikla* gali būti laikomos svarbiausios operacijos duomenų valdytojo arba duomenų tvarkytojo tikslams pasiekti.

Tačiau pagrindinė veikla neturėtų būti aiškinama kaip neapimanti visos veiklos, kai duomenų tvarkymas sudaro neatskiriamą duomenų valdytojo arba duomenų tvarkytojo veiklos dalį. Pavyzdžiui, pagrindinė ligoninės veikla yra teikti sveikatos priežiūros paslaugas. Tačiau ligoninė negalėtų saugiai ir veiksmingai teikti sveikatos priežiūros paslaugų netvarkydama duomenų apie sveikatą, pvz., pacientų medicinos dokumentų. Taigi, šių duomenų tvarkymas turėtų būti laikomas viena iš pagrindinių ligoninės veiklos sričių, todėl ligoninės turi paskirti duomenų apsaugos pareigūnus.

[12] Žr., pvz., *viešojo sektoriaus institucijos* ir *viešosios teisės reglamentuojamos įstaigos* apibrėžtį 2003 m. lapkričio 17 d. Europos Parlamento ir Tarybos direktyvos 2003/98/EB dėl viešojo sektoriaus informacijos pakartotinio naudojimo (OL L 345, 2003 12 31, p. 90) 2 straipsnio 1 ir 2 punktuose.

[13] 6 straipsnio 1 dalies e punktas.

Kitas pavyzdys – privati apsaugos paslaugų įmonė vykdo tam tikrų privačių prekybos centrų ir viešųjų erdvių stebėjimą. Stebėjimas yra įmonės pagrindinė veikla, kuri savo ruožtu yra susijusi su asmens duomenų tvarkymu. Taigi, ši įmonė taip pat turi paskirti duomenų apsaugos pareigūną.

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

2.1.3 DIDELIS MASTAS

37 straipsnio 1 dalies b ir c punktuose nurodyta, kad paskirti duomenų apsaugos pareigūną privaloma tada, kai asmens duomenys tvarkomi dideliu mastu. Bendrajame duomenų apsaugos reglamente neapibrėžta, kas yra duomenų tvarkymas dideliu mastu, tačiau 91 konstatuojamojoje dalyje pateikiamos tam tikros gairės[14].

Iš tikrųjų neįmanoma nurodyti tikslaus tvarkomų duomenų kiekio ar atitinkamų asmenų skaičiaus, kuris būtų taikytinas visais atvejais. Tačiau ilgainiui tam tikrose plačiai paplitusiose duomenų tvarkymo veiklos srityse gali susiformuoti standartinė praktika, kaip tiksliau ir (arba) kiekybiškai nustatyti, kas yra *didelis mastas*. WP29 taip pat planuoja prisidėti prie šios raidos skleisdama ir viešai skelbdama aktualių duomenų apsaugos pareigūno paskyrimo aplinkybių ribų pavyzdžius.

Bet kuriuo atveju 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

[14] Konstatuojamojoje dalyje teigiama, kad tai visų pirma turėtų būti taikoma *didelio masto duomenų tvarkymo operacijoms, kuriomis siekiama regioniniu, nacionaliniu ar viršnacionaliniu lygmeniu tvarkyti didelį kiekį asmens duomenų, kurios galėtų daryti poveikį daugeliui duomenų subjektų ir kurios gali kelti didelį pavojų*. Kita vertus, konstatuojamojoje dalyje konkrečiai teigiama, kad *asmens duomenų tvarkymas neturėtų būti laikomas didelio masto duomenų tvarkymu, jei tai yra atskirų gydytojų, kitų sveikatos priežiūros specialistų pacientų arba teisininko klientų asmens duomenų tvarkymas*. Svarbu atsižvelgti į tai, kad nors konstatuojamojoje dalyje pateikiami kraštutiniai pavyzdžiai (atskiro gydytojo tvarkomi duomenys ir visos šalies arba Europos mastu tvarkomi duomenys), tarp šių kraštutinumų yra didelė pilkoji zona. Be to, reikėtų nepamiršti, kad šioje konstatuojamojoje dalyje paminėti poveikio duomenų apsaugai vertinimai. Tai netiesiogiai reiškia, kad kai kurie elementai gali būti būdingi tik toms aplinkybėms ir nebūtinai tiksliai tokiu pačiu būdu taikomi duomenų apsaugos pareigūno paskyrimui.

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.

2.1.4 REGULIARUS IR SISTEMINGAS STEBĖJIMAS

Reguliaraus ir sistemingo duomenų subjektų stebėjimo sąvoka Bendrajame duomenų apsaugos reglamente nėra apibrėžta, bet *duomenų subjektų elgesio stebėsenos* sąvoka paminėta 24 konstatuojamojoje dalyje[15] ir akivaizdžiai apima visų formų stebėjimą ir profiliavimą internete, taip pat vartotojų elgesiu grindžiamos reklamos tikslais.

Vis dėlto stebėjimo sąvoka taikoma ne tik internetinėje aplinkoje, o internetinis sekimas turėtų būti laikomas tik vienu iš duomenų subjektų elgsenos stebėjimo pavyzdžių[16].

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.

Veiklos, kuri gali būti laikoma reguliariu ir sistemingu duomenų subjektų stebėjimu, 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

[15] *Siekiant nustatyti, ar duomenų tvarkymo veikla gali būti laikoma duomenų subjektų elgesio stebėsena, reikėtų įsitikinti, ar fiziniai asmenys internete atsekami, be kita ko, vėliau galbūt taikant asmens duomenų tvarkymo metodus, kuriais fiziniam asmeniui suteikiamas profilis, ypač siekiant priimti su juo susijusius sprendimus arba išnagrinėti ar prognozuoti jo asmeninius pomėgius, elgesį ir požiūrius.*

[16] Atkreipkite dėmesį, kad 24 konstatuojamojoje dalyje pagrindinis dėmesys skiriamas ekstrateritoriniam Bendrojo duomenų apsaugos reglamento taikymui. Be to, esama skirtumo tarp formuluotės *elgesio stebėsena* (3 straipsnio 2 dalies b punktas) ir formuluotės *reguliarus ir sistemingas stebėjimas* (37 straipsnio 1 dalies b punktas), kuri atitinkamai gali būti laikoma kita sąvoka.

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.

2.1.5 SPECIALIŲ KATEGORIJŲ DUOMENYS IR DUOMENYS APIE APKALTINAMUOSIUS NUOSPRENDŽIUS IR NUSIKALSTAMAS VEIKAS

37 straipsnio 1 dalies c punkte aptariamas specialių kategorijų duomenų tvarkymas pagal 9 straipsnį ir 10 straipsnyje nurodytų asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas. Nors nuostatoje vartojamas žodis *ir*, nėra politinės priežasties, dėl kurios abu kriterijai turėtų būti taikomi vienu metu. Todėl tekstas turėtų būti aiškinamas taip, tarsi jame būtų vartojamas žodis *arba*.

2.2. Duomenų tvarkytojo duomenų apsaugos pareigūnas

37 straipsnis dėl duomenų apsaugos pareigūno skyrimo taikomas ir duomenų valdytojams[17], ir duomenų tvarkytojams[18]. Atsižvelgiant į tai, kas atitinka privalomo paskyrimo kriterijus, kai kuriais atvejais duomenų apsaugos pareigūną paskirti privalo tik duomenų valdytojas arba tik duomenų tvarkytojas, o kitais atvejais – ir duomenų valdytojas, ir duomenų tvarkytojas.

Svarbu pabrėžti, kad net ir tuo atveju, kai duomenų valdytojas atitinka privalomo duomenų apsaugos pareigūno paskyrimo kriterijus, jo duomenų tvarkytojas nebūtinai privalo duomenų apsaugos pareigūną paskirti. Tačiau tai gali būti geroji patirtis.

Pavyzdžiai:

- Nedidelis šeimos verslas, veikiantis buitinių prietaisų platinimo srityje vieninteliame miestelyje, naudojasi duomenų tvarkytojo paslaugomis, kurio pagrindinė veikla yra teikti interneto svetainių analizės paslaugas ir pagalbą kuriant tikslinę reklamą ir rinkodarą. Šeimos verslo veikla ir jo klientai nelemia duomenų tvarkymo dideliu mastu, nes klientų mažai, o veikla – gana riboto pobūdžio. Tačiau duomenų tvarkytojo veikla, atsižvelgiant į tai, kad jis turi daug tokių klientų kaip ši nedidelė įmonė, kartu paėmus yra laikytina duomenų tvarkymu dideliu mastu. Todėl duomenų tvarkytojas pagal 37 straipsnio 1 dalies b punktą turi paskirti duomenų apsaugos pareigūną. O pats šeimos verslo subjektas duomenų apsaugos pareigūno paskirti neprivalo.

- Vidutinė čerpių gamybos įmonė savo profesinės sveikatos paslaugas subrangos pagrindu paveda teikti išorės duomenų tvarkytojui, kuris turi daug panašių klientų. Duomenų tvarkytojas pagal 37 straipsnio 1 dalies c punktą paskiria duomenų apsaugos pareigūną, jeigu duomenys tvarkomi dideliu mastu. Tačiau gamintojui prievolė paskirti duomenų apsaugos pareigūną taikoma nebūtinai.

---

[17] 4 straipsnio 7 punkte duomenų valdytojas apibrėžtas kaip asmuo arba organas, kuris nustato asmens duomenų tvarkymo tikslus ir priemones.

[18] 4 straipsnio 8 punkte duomenų tvarkytojas apibrėžtas kaip asmuo arba organas, kuris duomenų valdytojo vardu tvarko duomenis.

Duomenų tvarkytojo paskirtas duomenų apsaugos pareigūnas taip pat prižiūri duomenų tvarkytojo organizacijos veiklą, kai duomenų tvarkytojas veikia savo vardu (pvz., žmogiškųjų išteklių, IT veiklą, logistiką).

2.3. Vieno bendro duomenų apsaugos pareigūno paskyrimas kelioms organizacijoms

37 straipsnio 2 dalyje numatyta, kad grupė įmonių gali paskirti vieną bendrą duomenų apsaugos pareigūną, jeigu su juo yra *lengva susisiekti iš kiekvienos buveinės*. Lengvo susisiekimo sąvoka susijusi su duomenų apsaugos pareigūno, kaip duomenų subjektų[19], priežiūros institucijos[20] ir pačios organizacijos kontaktinio asmens, užduotimis, atsižvelgiant į tai, kad viena iš duomenų apsaugos pareigūno užduočių yra *informuoti duomenų valdytoją ir duomenų tvarkytoją ir duomenis tvarkančius darbuotojus apie jų prievoles pagal šį reglamentą ir konsultuoti juos šiais klausimais*[21].

Siekiant užtikrinti, kad su duomenų apsaugos pareigūnu, nesvarbu, ar jis dirba pačioje organizacijoje, ar už jos ribų, būtų lengva susisiekti, svarbu pasirūpinti, kad pagal Bendrojo duomenų apsaugos reglamento reikalavimus[22] būtų pateikti jo kontaktiniai duomenys.

Duomenų apsaugos pareigūnas, prireikus padedant jo grupei, turi turėti galimybę efektyviai bendrauti su duomenų subjektais[23] ir bendradarbiauti[24] su atitinkamomis priežiūros institucijomis. Be to, 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 į jį kreiptis (arba fiziškai, kai jis yra tose pačiose patalpose kaip ir darbuotojai, arba karštąja linija ar kitomis saugiomis ryšių priemonėmis).

Pagal 37 straipsnio 3 dalį vienas duomenų apsaugos pareigūnas gali būti skiriamas kelioms valdžios institucijoms arba įstaigoms, atsižvelgiant į jų organizacinę struktūrą ir dydį. Taikomi tie patys argumentai dėl išteklių ir bendravimo. Kadangi duomenų apsaugos pareigūnas yra atsakingas už įvairias užduotis, duomenų valdytojas arba duomenų tvarkytojas turi užtikrinti, kad vienas bendras duomenų apsaugos pareigūnas, prireikus padedant jo grupei, galėtų šias užduotis atlikti, nors jis paskirtas ir kelioms valdžios institucijoms ir įstaigoms.

[19] 38 straipsnio 4 dalis: *Duomenų subjektai gali kreiptis į duomenų apsaugos pareigūną visais klausimais, susijusiais jų asmeninių duomenų tvarkymu ir naudojimusi savo teisėmis pagal šį reglamentą*.

[20] 39 straipsnio 1 dalies e punktas: *atlieka kontaktinio asmens funkcijas priežiūros institucijai kreipiantis su duomenų tvarkymu susijusiais klausimais, įskaitant 36 straipsnyje nurodytas išankstines konsultacijas, ir prireikus konsultuoja visais kitais klausimais.*

[21] 39 straipsnio 1 dalies a punktas.

[22] Taip pat žr. 2.6 skirsnį.

[23] 12 straipsnio 1 dalis: *Duomenų valdytojas imasi tinkamų priemonių, kad visą 13 ir 14 straipsniuose nurodytą informaciją ir visus pranešimus pagal 15–22 ir 34 straipsnius, susijusius su duomenų tvarkymu, duomenų subjektui pateiktų glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba, ypač jei informacija yra konkrečiai skirta vaikui.*

[24] 39 straipsnio 1 dalies d punktas*: bendradarbiauja su priežiūros institucija.*

2.4. Galimybė susisiekti su duomenų apsaugos pareigūnu ir nustatyti jo vietą

Pagal Bendrojo duomenų apsaugos reglamento 4 skirsnį su duomenų apsaugos pareigūnu turi būti įmanoma veiksmingai susisiekti.

Siekdama užtikrinti, kad su duomenų apsaugos pareigūnu būtų įmanoma susisiekti, WP29 rekomenduoja, kad duomenų apsaugos pareigūnas dirbtų Europos Sąjungoje, neatsižvelgiant į tai, ar duomenų valdytojas arba duomenų tvarkytojas yra įsisteigęs Europos Sąjungoje.

Tačiau negalima atmesti galimybės, kad kai kuriais atvejais, kai duomenų valdytojas arba duomenų tvarkytojas Europos Sąjungoje neturi buveinės[25], duomenų apsaugos pareigūnas gali sugebėti veiksmingiau vykdyti savo veiklą, jeigu jis dirbs už ES ribų.

2.5. Duomenų apsaugos pareigūno ekspertinės žinios ir gebėjimai

37 straipsnio 5 dalyje numatyta, kad duomenų apsaugos pareigūnas *paskiriamas remiantis profesinėmis savybėmis, visų pirma duomenų apsaugos teisės ir praktikos ekspertinėmis žiniomis, taip pat gebėjimu atlikti 39 straipsnyje nurodytas užduotis*. 97 konstatuojamojoje dalyje numatyta, kad būtinas ekspertinių žinių lygis turėtų būti nustatomas atsižvelgiant į atliekamas duomenų tvarkymo operacijas ir reikiamą tvarkomų asmens duomenų apsaugą.

- **Ekspertinių žinių lygis**

Reikiamas ekspertinių žinių lygis nėra griežtai apibrėžtas, tačiau jis turi atitikti duomenų neskelbtinumą, sudėtingumą, kiekį ir organizacinius procesus. Pavyzdžiui, kai duomenų tvarkymo veikla yra itin sudėtinga arba tvarkoma daug neskelbtinų duomenų, duomenų apsaugos pareigūnui gali prireikti aukštesnio lygio ekspertinių žinių ir pagalbos. Taip pat padėtis skiriasi atsižvelgiant į tai, ar organizacija sistemingai, ar tik kartais perduoda asmens duomenis už Europos Sąjungos ribų. Taigi, duomenų apsaugos pareigūnas turėtų būti pasirenkamas atidžiai, deramai įvertinus organizacijoje kylančius duomenų apsaugos klausimus.

- **Profesinės savybės**

Nors 37 straipsnio 5 dalyje nenurodytos profesinės savybės, į kurias turėtų būti atsižvelgiama skiriant duomenų apsaugos pareigūną, svarbu tai, kad duomenų apsaugos pareigūnai privalo turėti nacionalinės ir Europos duomenų apsaugos teisės aktų bei praktikos žinių ir išsamiai suprasti Bendrąjį duomenų apsaugos reglamentą. Taip pat būtų naudinga, jeigu priežiūros institucijos skatintų tinkamą ir reguliarų duomenų apsaugos pareigūnų mokymą.

Naudingos žinios apie duomenų valdytojo verslo sektorių ir organizaciją. Be to, duomenų apsaugos pareigūnai turėtų gerai suprasti duomenų valdytojo vykdomas duomenų tvarkymo operacijas, informacines sistemas, duomenų saugumo ir duomenų apsaugos poreikius.

Valdžios institucijos ar įstaigos atveju duomenų apsaugos pareigūnas taip pat turėtų gerai išmanyti organizacijos administracines taisykles ir procedūras.

[25] Žr. Bendrojo duomenų apsaugos reglamento 3 straipsnį dėl teritorinės taikymo srities.

- **Gebėjimas atlikti užduotis**

Gebėjimas atlikti duomenų apsaugos pareigūnui skiriamas užduotis turėtų būti aiškinamas ir jo asmeninių savybių, ir žinių požiūriu, taip pat atsižvelgiant į jo statusą organizacijoje. Asmeninės savybės, pavyzdžiui, galėtų būti profesinis sąžiningumas ir aukšta profesinė etika; pagrindinė duomenų apsaugos pareigūno pareiga turėtų būti sudaryti sąlygas laikytis Bendrojo duomenų apsaugos reglamento. Duomenų apsaugos pareigūnas atlieka itin svarbų vaidmenį skatinant organizacijoje duomenų apsaugos kultūrą ir padeda įgyvendinti esminius Bendrojo duomenų apsaugos reglamento elementus, pvz., duomenų tvarkymo principus[26], duomenų subjektų teises[27], pritaikytąją ir standartizuotąją duomenų apsaugą[28], taip pat daryti duomenų tvarkymo veiklos įrašus[29], užtikrinti duomenų tvarkymo saugumą[30] ir teikti pranešimus apie duomenų saugumo pažeidimus[31].

- **Duomenų apsaugos pareigūno veikla pagal paslaugų sutartį**

Duomenų apsaugos pareigūnas savo pareigas gali eiti ir nedirbdamas duomenų valdytojo ar duomenų tvarkytojo organizacijoje, pagal paslaugų sutartį, sudarytą su asmeniu ar organizacija. Pastaruoju atveju būtina, kad kiekvienas organizacijos, atliekančios duomenų apsaugos pareigūno funkciją, narys įvykdytų visus taikytinus Bendrojo duomenų apsaugos reglamento 4 skirsnio reikalavimus (pvz., būtina, kad nė vienam nariui nekiltų interesų konfliktas). Nemažiau svarbu, kad kiekvienas toks narys būtų apsaugotas Bendrojo duomenų apsaugos reglamento nuostatomis (pvz., ne tik nebūtų nesąžiningai nutraukiama paslaugų sutartis dėl jo, kaip duomenų apsaugos pareigūno, veiklos, bet ir nebūtų nesąžiningai atleidžiamas iš darbo joks pavienis duomenų apsaugos pareigūno užduotis atliekančios organizacijos narys). Kartu galima taip suderinti individualius gebėjimus ir pranašumus, kad keli asmenys, dirbdami grupėje, galėtų efektyviau aptarnauti savo klientus.

Siekiant teisinio aiškumo ir gero organizavimo, taip pat siekiant užkirsti kelią grupės narių interesų konfliktams, rekomenduojama aiškiai paskirstyti užduotis duomenų apsaugos pareigūno grupės nariams ir vieną asmenį paskirti už klientą atsakingu vadovaujančiu kontaktiniu asmeniu. Apskritai taip pat būtų naudinga šiuos punktus nurodyti paslaugų sutartyje.

2.6. Duomenų apsaugos pareigūno kontaktinių duomenų paskelbimas ir nurodymas

Bendrojo duomenų apsaugos reglamento 37 straipsnio 7 dalyje reikalaujama, kad duomenų valdytojas arba duomenų tvarkytojas:

- paskelbtų duomenų apsaugos pareigūno kontaktinius duomenis ir
- nurodytų duomenų apsaugos pareigūno kontaktinius duomenis atitinkamoms priežiūros institucijoms.

Šiais reikalavimais siekiama užtikrinti, kad duomenų subjektai (ir organizacijoje, ir už jos ribų) ir priežiūros institucijos galėtų lengvai ir tiesiogiai susisiekti su duomenų apsaugos pareigūnu, neprivalėdamos į jį kreiptis per kitą organizacijos padalinį. Konfidencialumas ne mažiau svarbus:

[26] II skyrius.
[27] III skyrius.
[28] 25 straipsnis.
[29] 30 straipsnis.
[30] 32 straipsnis.
[31] 33 ir 34 straipsniai.

pavyzdžiui, darbuotojai gali vengti skųstis duomenų apsaugos pareigūnui, jeigu nebus užtikrintas jų pranešimų konfidencialumas.
Duomenų apsaugos pareigūnas privalo užtikrinti slaptumą arba konfidencialumą, susijusį su jo užduočių vykdymu, laikydamasis Sąjungos ar valstybės narės teisės (38 straipsnio 5 dalis).

Kontaktiniai duomenų apsaugos pareigūno duomenys turėtų apimti informaciją, kuria naudodamiesi duomenų subjektai ir priežiūros institucijos galėtų su juo lengvai susisiekti (pašto adresą, specialų telefono numerį ir (arba) e. pašto adresą). Atitinkamais atvejais bendravimo su visuomene tikslais būtų galima nurodyti ir kitas ryšių priemones, pvz., specialią karštąją liniją arba duomenų apsaugos pareigūnui adresuojamą specialią kontaktinę formą organizacijos svetainėje.

37 straipsnio 7 dalyje nereikalaujama į skelbiamus kontaktinius duomenis įtraukti duomenų apsaugos pareigūno vardo ir pavardės. Nors jų įtraukimas ir gali būti laikomas gerąja patirtimi, pats duomenų valdytojas ar duomenų tvarkytojas sprendžia, ar tai reikalinga ir naudinga konkrečiomis aplinkybėmis[32].

Vis dėlto nurodyti duomenų apsaugos pareigūno vardą ir pavardę priežiūros institucijai būtina, kad duomenų apsaugos pareigūnas veiktų kaip organizacijos ir priežiūros institucijos kontaktinis asmuo (39 straipsnio 1 dalies e punktas).

Kaip gerąją patirtį WP29 taip pat rekomenduoja organizacijai pranešti savo darbuotojams duomenų apsaugos pareigūno vardą, pavardę ir kontaktinius duomenis. Pavyzdžiui, duomenų apsaugos pareigūno vardas, pavardė ir kontaktiniai duomenys galėtų būti skelbiami organizacijos viduje – pateikiami intranete, vidaus telefono kataloge ir nurodomi organizacijos struktūros schemoje.

3 Duomenų apsaugos pareigūno statusas

3.1. Duomenų apsaugos pareigūno įtraukimas sprendžiant visus su asmens duomenų apsauga susijusius klausimus

Bendrojo duomenų apsaugos reglamento 38 straipsnyje numatyta, jog duomenų valdytojas ir duomenų tvarkytojas užtikrina, kad duomenų apsaugos pareigūnas būtų *tinkamai ir laiku įtraukiamas į visų su asmens duomenų apsauga susijusių klausimų nagrinėjimą.*

Itin svarbu, kad duomenų apsaugos pareigūnas arba jo grupė būtų kuo ankstyvesniu etapu įtraukiami į visus su duomenų apsauga susijusius klausimus. Kalbant apie poveikio duomenų apsaugai vertinimus, Bendrajame duomenų apsaugos reglamente konkrečiai numatyta į jų atlikimą įtraukti duomenų apsaugos pareigūną ir nurodyta, kad duomenų valdytojas, atlikdamas tokius poveikio vertinimus, konsultuojasi su duomenų apsaugos pareigūnu[33]. Užtikrinus, kad duomenų apsaugos pareigūnas būtų informuojamas ir su juo būtų konsultuojamasi nuo pat pradžių, bus lengviau laikytis Bendrojo

[32] Atkreiptinas dėmesys, kad 33 straipsnio 3 dalies b punkte, kuriame aprašoma informacija, kuri asmens duomenų pažeidimo atveju turi būti teikiama priežiūros institucijai ir duomenų subjektams, skirtingai negu 37 straipsnio 7 dalyje, taip pat konkrečiai reikalaujama pranešti duomenų apsaugos pareigūno vardą ir pavardę (o ne tik jo kontaktinius duomenis).
[33] 35 straipsnio 2 dalis.

duomenų apsaugos reglamento, bus skatinamas pritaikytosios privatumo apsaugos modelis, todėl tai turėtų būti standartinė organizacijos valdymo procedūra. Be to, svarbu, kad duomenų apsaugos pareigūnas organizacijoje būtų laikomas diskusijų partneriu ir kad jis dalyvautų atitinkamose darbo grupėse, organizacijoje priimančiose sprendimus dėl duomenų tvarkymo veiklos.

Taigi, organizacija turėtų užtikrinti, pavyzdžiui, kad:

- duomenų apsaugos pareigūnas būtų kviečiamas reguliariai dalyvauti vyresniosios ir vidurinio lygmens vadovybės posėdžiuose;
- jam būtų rekomenduojama dalyvauti ten, kur priimami sprendimai, turintys padarinių duomenų apsaugai. Visa aktuali informacija laiku turi būti perduodama duomenų apsaugos pareigūnui, kad jis galėtų suteikti tinkamą konsultaciją;
- visada būtų privaloma deramai atsižvelgti į duomenų apsaugos pareigūno nuomonę. Jeigu kyla nesutarimų, WP29 kaip gerąją patirtį rekomenduoja dokumentais įforminti priežastis, kodėl nebuvo vadovaujamasi duomenų apsaugos pareigūno konsultacija;
- įvykus duomenų saugumo pažeidimui ar kitam incidentui visada būtų privaloma nedelsiant pasikonsultuoti su duomenų apsaugos pareigūnu.

Atitinkamais atvejais duomenų valdytojas arba duomenų tvarkytojas galėtų parengti duomenų apsaugos gaires arba programas, kuriose būtų išdėstyta, kada turi būti konsultuojamasi su duomenų apsaugos pareigūnu.

3.2. Reikiami ištekliai

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*. Visų pirma turi būti įvertinami šie aspektai:

- aktyvi vyresniosios vadovybės parama duomenų apsaugos pareigūnui einant savo pareigas (pvz., valdybos lygmeniu);
- pakankamai laiko duomenų apsaugos pareigūnui jo pareigoms atlikti. Tai itin svarbu, kai vidinis duomenų apsaugos pareigūnas paskiriamas dirbti ne visą darbo dieną arba kai išorinis duomenų apsaugos pareigūnas vykdo ne tik duomenų apsaugos, bet ir kitas pareigas. Priešingu atveju vienas kitam prieštaraujantys prioritetai gali lemti tai, kad duomenų apsaugos pareigūno pareigos bus apleidžiamos. Itin svarbu turėti pakankamai laiko duomenų apsaugos pareigūno užduotims įvykdyti. Geroji patirtis būtų nustatyti tam tikrą duomenų apsaugos pareigūno funkcijoms vykdyti skirtą procentinę laiko dalį, jeigu jos vykdomos ne visą darbo dieną. Geroji patirtis taip pat būtų nustatyti funkcijoms atlikti reikalingą laiką bei tinkamą duomenų apsaugos pareigūno pareigų prioritetą ir parengti darbo planą (tai galėtų padaryti duomenų apsaugos pareigūnas arba organizacija);
- pakankama parama finansiniais ištekliais, infrastruktūra (aprūpinant patalpomis, priemonėmis, įranga), o prireikus – ir darbuotojais;
- oficialus pranešimas apie duomenų apsaugos pareigūno paskyrimą visiems darbuotojams, siekiant užtikrinti, kad organizacijoje būtų žinoma apie jo buvimą ir funkcijas;
- būtina galimybė naudotis kitomis tarnybomis, pvz., žmogiškųjų išteklių, teisės, IT, apsaugos ir kt., kad duomenų apsaugos pareigūnai iš tų kitų tarnybų galėtų gauti būtiną paramą, pagalbinius duomenis ir informaciją;

- nuolatinis mokymas. Duomenų apsaugos pareigūnams turi būti suteikta galimybė sekti naujausias tendencijas duomenų apsaugos srityje. Turėtų būti siekiama nuolat kelti duomenų apsaugos pareigūnų ekspertinių žinių lygį ir jie turėtų būti skatinami dalyvauti mokymo kursuose duomenų apsaugos klausimais ir kitomis formomis kelti kvalifikaciją, pvz., dalyvauti privatumo forumuose, praktiniuose seminaruose ir kt.;
- atsižvelgiant į organizacijos dydį ir struktūrą, gali prireikti sudaryti duomenų apsaugos pareigūno grupę (duomenų apsaugos pareigūnas ir jo darbuotojai). Tokiais atvejais turėtų būti aiškiai parengta grupės vidaus struktūra ir išdėstytos kiekvieno jos nario užduotys ir pareigos. Panašiai, 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 klientui paskirtas vadovaujantis kontaktinis asmuo.

Apskritai kuo sudėtingesnės ir (arba) jautresnės duomenų tvarkymo operacijos, tuo daugiau išteklių turi būti skiriama duomenų apsaugos pareigūnui. Duomenų apsaugos funkcija turi būti veiksminga ir pakankamai gerai aprūpinta ištekliais, palyginti su atliekamu duomenų tvarkymu.

3.3. Nurodymai ir *nepriklausomas pareigų ir užduočių atlikimas*

38 straipsnio 3 dalyje nustatytos tam tikros minimalios garantijos, padedančios užtikrinti, kad duomenų apsaugos pareigūnai galėtų pakankamai autonomiškai vykdyti savo užduotis organizacijoje. Duomenų valdytojai ir duomenų tvarkytojai visų pirma privalo užtikrinti, kad duomenų apsaugos pareigūnas *negautų jokių nurodymų dėl [savo] užduočių vykdymo*. 97 konstatuojamojoje dalyje priduriama, kad duomenų apsaugos pareigūnai, *nepriklausomai nuo to, ar jie yra duomenų valdytojo darbuotojai, savo pareigas ir užduotis turėtų galėti atlikti nepriklausomai*.

Tai reiškia, kad, vykdydami savo užduotis pagal 39 straipsnį, duomenų apsaugos pareigūnai neturi gauti nurodymų, kaip spręsti klausimą, pavyzdžiui, koks rezultatas turėtų būti pasiektas, kaip tirti skundą ir ar konsultuotis su priežiūros institucija. Be to, jiems neturi būti nurodoma laikytis tam tikro požiūrio į su duomenų apsaugos teise susijusį klausimą, pavyzdžiui, tam tikro teisės aiškinimo.

Tačiau duomenų apsaugos pareigūnų autonomija nereiškia, kad jie turi su 39 straipsnyje nurodytomis savo užduotimis nesusijusių įgaliojimų priimti sprendimus.

Duomenų valdytojas arba duomenų tvarkytojas ir toliau yra atsakingas už tai, kad būtų laikomasi duomenų apsaugos teisės, ir turi sugebėti tai įrodyti[34]. Jeigu duomenų valdytojas arba duomenų tvarkytojas priima sprendimus, kurie yra nesuderinami su Bendruoju duomenų apsaugos reglamentu ir duomenų apsaugos pareigūno konsultacija, duomenų apsaugos pareigūnui turėtų būti suteikta galimybė aiškiai pareikšti savo nesutikimą aukščiausio lygmens vadovybei ir sprendimus priimantiems asmenims. Šiuo klausimu 38 straipsnio 3 dalyje nurodyta, kad duomenų apsaugos pareigūnas tiesiogiai atsiskaito duomenų valdytojo arba duomenų tvarkytojo aukščiausio lygio vadovybei. 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.

[34] 5 straipsnio 2 dalis.

3.4. Duomenų apsaugos pareigūno atleidimas arba baudimas dėl jam nustatytų užduočių atlikimo

38 straipsnio 3 dalyje reikalaujama, kad *duomenų valdytojas arba duomenų tvarkytojas* neatleistų ir nebaustų duomenų apsaugos pareigūno *dėl jam nustatytų užduočių atlikimo*.

Šiuo reikalavimu padedama užtikrinti duomenų apsaugos pareigūnų autonomiją ir užtikrinti, kad jie veiktų nepriklausomai ir vykdydami savo duomenų apsaugos užduotis naudotųsi pakankama apsauga.

Pagal Bendrąjį duomenų apsaugos reglamentą nuobaudas draudžiama taikyti tik tuo atveju, jeigu jos skiriamos dėl dalykų, susijusių su duomenų apsaugos pareigūno pareigų atlikimu. Pavyzdžiui, duomenų apsaugos pareigūnas gali manyti, kad tam tikras duomenų tvarkymas gali kelti didelę riziką, ir gali patarti duomenų tvarkytojui atlikti poveikio duomenų apsaugai vertinimą, tačiau duomenų valdytojas arba duomenų tvarkytojas nesutinka su duomenų apsaugos pareigūno vertinimu. Tokiu atveju duomenų apsaugos pareigūno negalima atleisti už tai, kad jis suteikė šią konsultaciją.

Nuobaudos gali būti įvairios ir gali būti tiesioginės arba netiesioginės. Nuobauda, pavyzdžiui, gali būti tai, kad nepaaukštinamos asmens pareigos arba toks paaukštinimas vėlinamas; nesudaromos sąlygos daryti karjerą; neskiriami priedai, kuriuos gauna kiti darbuotojai. Šios nuobaudos nebūtinai turi būti faktiškai taikomos, užtenka vien grėsmės, kuria naudojamasi siekiant nubausti duomenų apsaugos pareigūną dėl priežasčių, susijusių su jo, kaip duomenų apsaugos pareigūno, veikla.

Taikant įprastą valdymo tvarką, kaip ir bet kurio kito darbuotojo ar rangovo atveju, ir taikant atitinkamą nacionalinę sutarčių arba darbo teisę ir baudžiamąją teisę, duomenų apsaugos pareigūną vis dėlto galima teisėtai atleisti dėl priežasčių, nesusijusių su jo, kaip duomenų apsaugos pareigūno, pareigų vykdymu (pavyzdžiui, dėl vagystės, fizinio, psichologinio ar seksualinio priekabiavimo ar panašaus labai netinkamo elgesio).

Šiuo klausimu pažymėtina, kad Bendrajame duomenų apsaugos reglamente nenurodyta, kaip duomenų apsaugos pareigūną galima atleisti ar pakeisti jį kitu asmeniu. Vis dėlto kuo stabilesnė duomenų apsaugos pareigūno sutartis ir kuo daugiau taikoma garantijų, kuriomis apsaugoma nuo nesąžiningo atleidimo iš darbo, tuo labiau tikėtina, kad duomenų apsaugos pareigūnas galės veikti nepriklausomai. Taigi, WP29 palankiai vertintų atitinkamas organizacijų pastangas.

3.5. Interesų konfliktas

38 straipsnio 6 dalyje duomenų apsaugos pareigūnui leidžiama *vykdyti kitas užduotis ir pareigas*. Tačiau straipsnyje organizacija įpareigojama užtikrinti, kad *dėl bet kokių tokių užduočių ir pareigų nekiltų interesų konfliktas*.

Interesų konflikto nebuvimas artimai susijęs su reikalavimu veikti nepriklausomai. Nors duomenų apsaugos pareigūnams leidžiama atlikti kitas funkcijas, kitas užduotis ir pareigas jam galima patikėti tik tuo atveju, jeigu jos nekelia interesų konflikto. Tai visų pirma reiškia, kad duomenų apsaugos pareigūnas negali organizacijoje eiti pareigų, pagal kurias jis turėtų 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 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. Be to, interesų konfliktas taip pat gali kilti, pavyzdžiui, jeigu išorinio duomenų apsaugos pareigūno paprašoma atstovauti duomenų valdytojui arba duomenų tvarkytojui teismuose, kai nagrinėjamos bylos, susijusios su duomenų apsaugos klausimais.

Priklausomai nuo organizacijos veiklos, dydžio ir struktūros, duomenų valdytojai arba duomenų tvarkytojai gali taikyti šią gerąją patirtį:

- nustatyti pareigybes, kurios būtų nesuderinamos su duomenų apsaugos pareigūno funkcijomis;
- šiuo tikslu parengti vidaus taisykles, kad būtų išvengta interesų konflikto;
- įtraukti bendresnio pobūdžio paaiškinimą apie interesų konfliktus;
- paskelbti, kad jų duomenų apsaugos pareigūnui nekyla interesų konflikto dėl jo, kaip duomenų apsaugos pareigūno, funkcijų vykdymo – taip būtų informuojama, kad šis reikalavimas yra suvokiamas;
- į organizacijos vidaus taisykles įtraukti apsaugos nuostatas ir užtikrinti, kad skelbimas apie laisvą duomenų apsaugos pareigūno pareigybę arba paslaugų sutartis būtų pakankamai tikslūs ir išsamūs ir taip būtų išvengta interesų konflikto. Šiuo klausimu taip pat reikėtų nepamiršti, kad interesų konfliktai gali būti įvairių formų, priklausomai nuo to, ar samdomas vidinis, ar išorinis duomenų apsaugos pareigūnas.

4 Duomenų apsaugos pareigūno užduotys

4.1. Stebėjimas, kaip laikomasi Bendrojo duomenų apsaugos reglamento

39 straipsnio 1 dalies b punkte duomenų apsaugos pareigūnams, be kitų pareigų, pavedama stebėti, kaip laikomasi Bendrojo duomenų apsaugos reglamento. Be to, 97 konstatuojamojoje dalyje nurodyta, kad duomenų apsaugos pareigūnas *duomenų valdytojui ar duomenų tvarkytojui* turėtų padėti *stebėti, kaip viduje laikomasi šio reglamento*.

Vykdydamas šias pareigas 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,
- informuoti duomenų valdytoją ar duomenų tvarkytoją, jį konsultuoti ir teikti jam rekomendacijas.

Stebėjimas, kaip laikomasi reglamento, nereiškia, kad duomenų apsaugos pareigūnas yra asmeniškai atsakingas už reglamento nesilaikymo atvejį. Bendrajame duomenų apsaugos reglamente aiškiai nustatyta, kad būtent duomenų valdytojas, o ne duomenų apsaugos pareigūnas, privalo įgyvendinti *tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento* (24 straipsnio 1 dalis). Už tai, kad duomenų apsauga atitiktų reikalavimus, atsakingas duomenų valdytojas kaip organizacija, o ne duomenų apsaugos pareigūnas.

4.2. Duomenų apsaugos pareigūno vaidmuo atliekant poveikio duomenų apsaugai vertinimą

Pagal 35 straipsnio 1 dalį poveikio duomenų apsaugai vertinimą prireikus privalo atlikti duomenų valdytojas, o ne duomenų apsaugos pareigūnas. Tačiau duomenų apsaugos pareigūnas gali atlikti labai svarbų ir naudingą vaidmenį padėdamas duomenų valdytojui. Vadovaujantis pritaikytosios duomenų apsaugos principu, 35 straipsnio 2 dalyje konkrečiai nurodyta, kad atlikdamas poveikio duomenų apsaugai vertinimą duomenų valdytojas *konsultuojasi* su duomenų apsaugos pareigūnu. 39 straipsnio 1 dalies c punkte duomenų apsaugos pareigūnui savo ruožtu nustatoma pareiga *paprašius* konsultuoti *dėl poveikio duomenų apsaugai vertinimo ir* stebėti *jo atlikimą pagal 35 straipsnį*.

WP29 rekomenduoja duomenų valdytojui kreiptis į duomenų apsaugos pareigūną konsultacijos, be kita ko, šiais klausimais [35]:

- 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.

Jeigu duomenų valdytojas nesutinka su duomenų apsaugos pareigūno suteikta konsultacija, poveikio duomenų apsaugai vertinimo dokumentacijoje turėtų būti raštu konkrečiai pagrįsta, kodėl neatsižvelgta į konsultaciją[36].

Be to, WP29 rekomenduoja, kad duomenų valdytojas, pavyzdžiui, ne tik duomenų apsaugos pareigūno sutartyje, bet ir darbuotojams, vadovybei (ir, atitinkamais atvejais – kitiems suinteresuotiesiems subjektams) teikiamoje informacijoje nurodytų tikslias duomenų apsaugos pareigūno užduotis ir jų sritį, ypač susijusią su poveikio duomenų apsaugai vertinimo atlikimu.

4.3. Bendradarbiavimas su priežiūros institucija ir kontaktinio asmens funkcija

[35] 39 straipsnio 1 dalyje paminėtos duomenų apsaugos pareigūno užduotys ir nurodyta, kad duomenų apsaugos pareigūnas *atlieka bent šias užduotis*. Taigi, niekas neužkerta kelio duomenų valdytojui pavesti duomenų apsaugos pareigūnui 39 straipsnio 1 dalyje konkrečiai nepaminėtas užduotis arba išsamiau aprašyti tas užduotis.

[36] 24 straipsnio 1 dalyje nurodyta, kad *atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų* ***ir galėtų įrodyti****, kad duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos*.

Pagal 39 straipsnio 1 dalies d ir e punktus duomenų apsaugos pareigūnas *bendradarbiauja su priežiūros institucija* ir *atlieka kontaktinio asmens funkcijas priežiūros institucijai kreipiantis su duomenų tvarkymu susijusiais klausimais, įskaitant 36 straipsnyje nurodytas išankstines konsultacijas, ir prireikus konsultuoja visais kitais klausimais*.

Šios užduotys susijusios su duomenų apsaugos pareigūno, kaip pagalbininko, vaidmeniu, paminėtu šių gairių įvade. Duomenų apsaugos pareigūnas veikia kaip kontaktinis asmuo, padedantis priežiūros institucijai gauti dokumentus ir informaciją, kad būtų įvykdytos 57 straipsnyje nurodytos užduotys ir būtų įvykdyti jos tyrimų vykdymo, taisomųjų veiksmų, leidimo išdavimo ir patariamieji įgaliojimai, nurodyti 58 straipsnyje. Kaip jau minėta, duomenų apsaugos pareigūnas privalo užtikrinti slaptumą arba konfidencialumą, susijusį su jo užduočių vykdymu, laikydamasis Sąjungos ar valstybės narės teisės (38 straipsnio 5 dalis). Tačiau įpareigojimu laikytis slaptumo ar konfidencialumo duomenų apsaugos pareigūnui nedraudžiama susisiekti su priežiūros institucija ir kreiptis į ją konsultacijos. 39 straipsnio 1 dalies e punkte numatyta, kad duomenų apsaugos pareigūnas prireikus gali konsultuotis su priežiūros institucija visais kitais klausimais.

4.4. Rizika pagrįstas požiūris

39 straipsnio 2 dalyje reikalaujama, kad duomenų apsaugos pareigūnas tinkamai įvertintų *su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus*.

Šiuo straipsniu primenamas bendras sveiko proto principas, galintis būti aktualus daugeliui duomenų apsaugos pareigūno kasdienio darbo aspektų. Iš esmės, vadovaujantis šiuo principu, duomenų apsaugos pareigūnas privalo savo veiklą suskirstyti prioritetais ir daugiausia dėmesio skirti tiems klausimams, kurie kelia didžiausią pavojų duomenų apsaugai. Šis principas nereiškia, kad duomenų apsaugos pareigūnas turėtų aplaidžiau stebėti, kaip laikomasi reglamento vykdant duomenų tvarkymo operacijas, kurių rizikos lygis palyginti žemas, tačiau duomenų apsaugos pareigūnas pagrindinį dėmesį turėtų skirti didelės rizikos sritims.

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.

4.5. Duomenų apsaugos pareigūno vaidmuo tvarkant įrašus

Pagal 30 straipsnio 1 ir 2 dalis ne duomenų apsaugos pareigūnas, o duomenų valdytojas arba duomenų tvarkytojas privalo tvarkyti *duomenų tvarkymo veiklos, už kurią jis atsako, įrašus* arba *su visų kategorijų duomenų tvarkymo veikla, vykdoma duomenų valdytojo vardu, susijusius įrašus.*

Praktikoje duomenų apsaugos pareigūnai dažnai sudaro sąrašus ir tvarko duomenų tvarkymo operacijų registrą, remdamiesi informacija, kurią jiems teikia įvairūs jų organizacijos padaliniai, atsakingi už

asmens duomenų tvarkymą. Ši praktika buvo išplėtota pagal daugelį dabartinių nacionalinės teisės aktų ir pagal ES institucijoms ir įstaigoms taikytinas duomenų apsaugos taisykles[37].

39 straipsnio 1 dalyje numatytas būtinų duomenų apsaugos pareigūno užduočių sąrašas. Taigi, niekas neužkerta kelio duomenų valdytojui arba duomenų tvarkytojui pavesti duomenų apsaugos pareigūnui duomenų valdytojo arba duomenų tvarkytojo 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.

Bet kuriuo atveju įrašai, kuriuos reikalaujama tvarkyti pagal 30 straipsnį, taip pat turėtų būti laikomi priemone, kuria duomenų valdytojui ir priežiūros institucijai, pateikus prašymą, suteikiama galimybė apžvelgti visą organizacijos vykdomą duomenų tvarkymo veiklą. Taigi, šie įrašai yra būtina reglamento laikymosi sąlyga ir veiksminga atskaitomybės priemonė.

[37] Reglamento (EB) Nr. 45/2001 24 straipsnio 1 dalies d punktas.

5 PRIEDAS. DUOMENŲ APSAUGOS PAREIGŪNO GAIRĖS: KĄ BŪTINA ŽINOTI

Šio priedo tikslas – paprastai ir suprantamai 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

1 Kurios organizacijos privalo paskirti duomenų apsaugos pareigūną?

Duomenų apsaugos pareigūną paskirti privaloma:

- jeigu duomenis tvarko valdžios institucija arba įstaiga (neatsižvelgiant į tai, kokie duomenys tvarkomi);
- jeigu duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus;
- jeigu 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, net jei duomenų apsaugos pareigūno paskirti neprivaloma, organizacijoms kartais gali būti naudinga jį paskirti savanoriškai. 29 straipsnio duomenų apsaugos darbo grupė (WP29) skatina šią savanorišką praktiką. Kai organizacija savanoriškai paskiria duomenų apsaugos pareigūną, jo paskyrimui, statusui ir užduotims taikomi tie patys reikalavimai, tarsi paskyrimas būtų buvęs privalomas.

Šaltinis: Bendrojo duomenų apsaugos reglamento 37 straipsnio 1 dalis

2 Ką reiškia sąvoka *pagrindinė veikla*?

Pagrindine 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 reikalingų pagalbinių funkcijų pavyzdžiai. Nors ši veikla yra reikalinga arba būtina, ji paprastai laikoma pagalbinėmis funkcijomis, o ne pagrindine veikla.

Šaltinis: Bendrojo duomenų apsaugos reglamento 37 straipsnio 1 dalies b ir c punktai

3 Ką reiškia sąvoka *dideliu mastu*?

Bendrajame duomenų apsaugos reglamente neapibrėžta, kas yra duomenų tvarkymas dideliu mastu. 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.

Šaltinis: Bendrojo duomenų apsaugos reglamento 37 straipsnio 1 dalies b ir c punktai

4 Ką reiškia sąvoka *reguliariai ir sistemingai stebėti*?

Reguliaraus 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.

Veiklos, kuri gali būti laikoma reguliariu ir sistemingu duomenų subjektų stebėjimu, 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.

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

- vykstantis arba pasitaikantis tam tikrais intervalais konkrečiu laikotarpiu;
- pasikartojantis arba kartojamas konkrečiais momentais;

- 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.

Šaltinis: Bendrojo duomenų apsaugos reglamento 37 straipsnio 1 dalies b punktas

5 Ar gali organizacijos duomenų apsaugos pareigūną paskirti bendrai? Jei taip, kokiomis sąlygomis?

Taip. Grupė įmonių gali paskirti vieną bendrą duomenų apsaugos pareigūną, jeigu su juo yra *lengva susisiekti iš kiekvienos buveinės*. Lengvo susisiekimo 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. Duomenų apsaugos pareigūnas, prireikus padedant jo grupei, turi turėti galimybę efektyviai bendrauti su duomenų subjektais ir bendradarbiauti su atitinkamomis priežiūros institucijomis. Tai reiškia, kad šis bendravimas turi vykti priežiūros institucijų ir duomenų subjektų vartojamomis viena arba keliomis kalbomis. Siekiant užtikrinti, kad duomenų subjektai galėtų susisiekti su duomenų apsaugos pareigūnu, labai svarbu suteikti galimybę į jį kreiptis (arba fiziškai, kai jis yra tose pačiose patalpose kaip ir darbuotojai, arba karštąja linija ar kitomis saugiomis ryšių priemonėmis).

Vienas duomenų apsaugos pareigūnas gali būti skiriamas kelioms valdžios institucijoms arba įstaigoms, atsižvelgiant į jų organizacinę struktūrą ir dydį. Taikomi tie patys argumentai dėl išteklių ir bendravimo. Kadangi duomenų apsaugos pareigūnas yra atsakingas už įvairias užduotis, duomenų valdytojas arba duomenų tvarkytojas turi užtikrinti, kad vienas bendras duomenų apsaugos pareigūnas, prireikus padedant jo grupei, galėtų šias užduotis atlikti, nors jis paskirtas ir kelioms valdžios institucijoms ir įstaigoms.

Šaltinis: Bendrojo duomenų apsaugos reglamento 37 straipsnio 2 ir 3 dalys

6 Kokioje vietoje turėtų dirbti duomenų apsaugos pareigūnas?

Siekdama užtikrinti, kad su duomenų apsaugos pareigūnu būtų įmanoma susisiekti, WP29 rekomenduoja, kad duomenų apsaugos pareigūnas dirbtų Europos Sąjungoje, neatsižvelgiant į tai, ar duomenų valdytojas arba duomenų tvarkytojas yra įsisteigęs Europos Sąjungoje. Tačiau negalima atmesti galimybės, kad kai kuriais atvejais, kai duomenų valdytojas arba duomenų tvarkytojas Europos Sąjungoje neturi buveinės, duomenų apsaugos pareigūnas gali sugebėti veiksmingiau vykdyti savo veiklą, jeigu jis dirbs už ES ribų.

7 Ar įmanoma paskirti išorinį duomenų apsaugos pareigūną?

Taip. 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.

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 taikytinus Bendrojo duomenų apsaugos reglamento reikalavimus.

Siekiant teisinio aiškumo ir gero organizavimo, taip pat siekiant užkirsti kelią grupės narių interesų konfliktams, gairėse rekomenduojama paslaugų sutartimi aiškiai paskirstyti užduotis išorinio duomenų apsaugos pareigūno grupės nariams ir vieną asmenį paskirti už klientą atsakingu vadovaujančiu kontaktiniu asmeniu.

Šaltinis: Bendrojo duomenų apsaugos reglamento 37 straipsnio 6 dalis

8 Kokias profesines savybes turėtų turėti duomenų apsaugos pareigūnas?

Duomenų apsaugos pareigūnas paskiriamas remiantis profesinėmis savybėmis, visų pirma duomenų apsaugos teisės ir praktikos ekspertinėmis žiniomis, taip pat gebėjimu atlikti savo užduotis.

Būtinas ekspertinių žinių lygis 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.

Atitinkami 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.

Šaltinis: Bendrojo duomenų apsaugos reglamento 37 straipsnio 5 dalis

9 Kokius išteklius duomenų valdytojas arba duomenų tvarkytojas turėtų suteikti duomenų apsaugos pareigūnui?

Duomenų apsaugos pareigūnas turi turėti išteklių, reikalingų jo užduotims atlikti.

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 užduotims 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 kitų tarnybų galėtų gauti būtiną paramą, pagalbinius duomenis ar informaciją;
- nuolatinis mokymas.

Šaltinis: Bendrojo duomenų apsaugos reglamento 38 straipsnio 2 dalis

10 Kokios yra apsaugos priemonės, kad duomenų apsaugos pareigūnas galėtų nepriklausomai atlikti savo užduotis? Ką reiškia *interesų konfliktas*?

Taikomos kelios apsaugos priemonės, kad duomenų apsaugos pareigūnas galėtų veikti nepriklausomai:

- duomenų valdytojai arba duomenų tvarkytojai negali duoti nurodymų dėl duomenų apsaugos pareigūno užduočių atlikimo;
- 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.

Dėl kitų duomenų apsaugos pareigūno užduočių ir pareigų neturi kilti interesų konflikto. Tai visų pirma reiškia, kad duomenų apsaugos pareigūnas negali organizacijoje eiti pareigų, pagal kurias jis turėtų 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 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. Be to, interesų konfliktas taip pat gali kilti, pavyzdžiui, jeigu išorinio duomenų apsaugos pareigūno paprašoma atstovauti duomenų valdytojui arba duomenų tvarkytojui teismuose, kai nagrinėjamos bylos, susijusios su duomenų apsaugos klausimais.

Šaltinis: Bendrojo duomenų apsaugos reglamento 38 straipsnio 3 ir 6 dalys

Duomenų apsaugos pareigūno užduotys

11 Ką reiškia *stebėti, ar laikomasi reglamento*?

Vykdydamas šias pareigas – 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,
- informuoti duomenų valdytoją ar duomenų tvarkytoją, jį konsultuoti ir teikti jam rekomendacijas.

Šaltinis: Bendrojo duomenų apsaugos reglamento 39 straipsnio 1 dalies b punktas

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

Ne. Duomenų apsaugos pareigūnai nėra asmeniškai atsakingi, jei nesilaikoma duomenų apsaugos reikalavimų. Būtent duomenų valdytojas arba duomenų tvarkytojas privalo užtikrinti ir sugebėti įrodyti, kad duomenys tvarkomi laikantis šio reglamento. Už tai, kad duomenų tvarkymas atitiktų reikalavimus, atsakingas duomenų valdytojas arba duomenų tvarkytojas.

13 Koks yra duomenų apsaugos pareigūno vaidmuo vertinant poveikį duomenų apsaugai ir tvarkant duomenų tvarkymo veiklos įrašus?

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 duomenų apsaugos reikalavimus.

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 kelio duomenų valdytojui arba duomenų tvarkytojui pavesti duomenų apsaugos pareigūnui duomenų valdytojo arba duomenų tvarkytojo 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.

Šaltinis: Bendrojo duomenų apsaugos reglamento 39 straipsnio 1 dalies c punktas ir 30 straipsnis

Priimta Briuselyje 2016 m. gruodžio 13 d.

Darbo grupės vardu
Pirmininkė

Isabelle FALQUE-PIERROTIN

Priimta su paskutiniais pakeitimais 2017 m. balandžio 5 d.

Darbo grupės
pirmininkė

Isabelle FALQUE-PIERROTIN