Gairės 4/2019 dėl 25 straipsnio

Pritaikytoji ir standartizuotoji duomenų apsauga

Versija 2.0

Priimta 2020 m. spalio 20 d.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Ankstesnės versijos

Versija 1.0	2019 m. lapkričio 13 d.	Gairių priėmimas viešoms konsultacijoms
Versija 2.0	2020 m. spalio 20 d.	Gairių priėmimas Europos duomenų apsaugos valdyboje po viešų konsultacijų

Turinys

Europos duomenų apsaugos valdyba,

atsižvelgdama į 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 (toliau – BDAR) 70 straipsnio 1 dalies e punktą,

atsižvelgdama į EEE susitarimą, ypač į jo XI priedą ir 37 protokolą su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018,

atsižvelgdama į savo Darbo tvarkos taisyklių 12 ir 22 straipsnius,

PRIĖMĖ ŠIAS GAIRES

Santrauka

Pasaulyje, kuris vis labiau skaitmeninamas, pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimų laikymasis yra labai svarbus skatinant privatumą ir duomenų apsaugą visuomenėje. Todėl labai svarbu, kad duomenų valdytojai rimtai žiūrėtų į šią atsakomybę ir rengdami duomenų tvarkymo operacijas vykdytų BDAR nustatytas prievoles.

Šiose gairėse pateikiamos bendros rekomendacijos dėl BDAR 25 straipsnyje nustatytos pritaikytosios ir standartizuotosios duomenų apsaugos (toliau – PSDA) prievolės. PSDA – tai prievolė, kuri taikoma visiems duomenų valdytojams, neatsižvelgiant į jų dydį ar duomenų tvarkymo sudėtingumą. Kad duomenų valdytojas galėtų įgyvendinti PSDA reikalavimus, labai svarbu, kad jis suprastų duomenų apsaugos principus ir duomenų subjekto teises ir laisves.

Pagrindinė prievolė – įgyvendinti *tinkamas* priemones ir būtinas apsaugos priemones, kuriomis užtikrinamas *veiksmingas duomenų apsaugos principų įgyvendinimas*, o kartu ir *duomenų subjekto teisių ir laisvių pritaikytoji ir standartizuotoji duomenų apsauga*. Pritaikyti ir standartizuoti apsaugos elementai, į kuriuos turėtų būti atsižvelgiama, nustatyti 25 straipsnyje. Šie elementai bus išsamiau išdėstyti šiose gairėse.

25 straipsnio 1 dalyje nustatyta, kad duomenų valdytojai į PSDA reikalavimus turi atsižvelgti vos pradėję planuoti naują duomenų tvarkymo veiksmą. Duomenų valdytojai PSDA įgyvendina *prieš* pradėdami tvarkyti duomenis ir *nuolat* duomenų tvarkymo metu reguliariai peržiūrėdami pasirinktų priemonių ir apsaugos priemonių veiksmingumą. PSDA taip pat taikoma esamoms sistemoms, kuriose tvarkomi asmens duomenys.

Gairėse taip pat pateikiamos rekomendacijos, kaip veiksmingai įgyvendinti 5 straipsnyje nustatytus duomenų apsaugos principus, išvardijant pagrindinius pritaikytosios ir standartizuotosios apsaugos elementus, ir pateikiant praktinių pavyzdžių. Duomenų valdytojas turi apsvarstyti, ar siūlomos priemonės yra tinkamos atsižvelgiant į konkrečias atitinkamo duomenų tvarkymo veiksmo aplinkybes.

Europos duomenų apsaugos valdyba teikia rekomendacijas, kaip duomenų valdytojai, tvarkytojai ir gamintojai gali bendradarbiauti, kad užtikrintų PSDA. Ji ragina pramonės duomenų valdytojus, taip pat duomenų tvarkytojus ir gamintojus naudoti PSDA kaip priemonę pasiekti konkurencinį pranašumą vykdant į duomenų valdytojus ir duomenų subjektus nukreiptą savo produktų rinkodarą. Europos

duomenų apsaugos valdyba taip pat ragina visus duomenų valdytojus naudotis sertifikavimu ir elgesio kodeksais.

1 TAIKYMO SRITIS

1. Gairėse daugiausia dėmesio tam, kaip duomenų valdytojai turėtų įgyvendinti PSDA, vykdydami BDAR 25 straipsnyje nustatytą prievolę.[1] Kitiems subjektams, pvz., duomenų tvarkytojams ir produktų, paslaugų ir taikomųjų programų gamintojams (toliau – gamintojai), kuriems 25 straipsnis nėra tiesiogiai taikomas, šios gairės taip pat gali būti naudingos kuriant BDAR reikalavimus atitinkančius produktus ir paslaugas, leidžiančias duomenų valdytojams vykdyti savo duomenų apsaugos prievoles.[2] BDAR 78 konstatuojamojoje dalyje taip pat nurodyta, kad į PSDA turėtų būti atsižvelgiama rengiant viešuosius konkursus. Nors visi duomenų valdytojai privalo integruoti PSDA į savo duomenų tvarkymo veiksmus, šia nuostata skatinama laikytis duomenų apsaugos principų, kuriuos taikydamos viešojo administravimo institucijos turėtų rodyti pavyzdį. Duomenų valdytojas yra atsakingas už tai, kad jo duomenų tvarkytojams ir pagalbiniams duomenų tvarkytojams tvarkant duomenis būtų vykdomos PSDA prievolės, todėl jis turėtų į tai atsižvelgti sudarydamas sutartis su šiomis šalimis.

2. 25 straipsnyje nustatytas reikalavimas duomenų valdytojams užtikrinti, kad tvarkant asmens duomenis taikoma duomenų apsauga būtų pritaikyta šiam tikslui ir būtų taikoma visuomet ir kad taip būtų viso duomenų tvarkymo ciklo metu. PSDA reikalavimas taip pat taikomas duomenų tvarkymo sistemoms, kurios buvo sukurtos prieš įsigaliojant BDAR. Duomenų valdytojai turi pasirūpinti, kad duomenų tvarkymo veiksmai būtų atnaujinti ir atitiktų BDAR nuostatas. Daugiau informacijos apie tai, kaip išlaikyti esamos sistemos atitiktį PSDA reikalavimams, pateikiama šių gairių 2.1.4 poskyryje. Šios nuostatos esmė – užtikrinti *tinkamą* ir *veiksmingą pritaikytąją* ir *standartizuotąją* duomenų apsaugą, o tai reiškia, kad duomenų valdytojai turėtų sugebėti įrodyti, jog tvarkydami duomenis taiko tinkamas priemones ir apsaugos priemones, kad užtikrintų duomenų apsaugos principų ir duomenų subjektų teisių bei laisvių veiksmingumą.

3. Gairių 2 skyriuje daugiausia dėmesio skiriama 25 straipsnyje nustatytų reikalavimų aiškinimui ir nagrinėjamos šia nuostata nustatytos teisinės prievolės. Pavyzdžiai, kaip taikyti PSDA atsižvelgiant į konkrečius duomenų apsaugos principus, pateikti 3 skyriuje.

4. Gairių 4 skyriuje nagrinėjama galimybė sukurti sertifikavimo mechanizmą, skirtą įrodyti atitiktį 25 straipsniui, o 5 skyriuje aprašyta, kaip priežiūros institucijos gali užtikrinti šio straipsnio vykdymą. Galiausiai šiose gairėse suinteresuotiesiems subjektams pateikiamos papildomų rekomendacijų, kaip sėkmingai įgyvendinti PSDA. Europos duomenų apsaugos valdyba pripažįsta, kad mažosioms ir vidutinėms įmonėms (toliau – MVĮ) nėra lengva nuosekliai laikytis PSDA prievolių, ir 6 skyriuje pateikia papildomų rekomendacijų konkrečiai MVĮ.

[1] Čia pateikti paaiškinimai taip pat taikytini Direktyvos (ES) 2016/680 20 straipsniui ir Reglamento (ES) 2018/1725 27 straipsniui.

[2] BDAR 78 konstatuojamojoje dalyje aiškiai nurodyta: „Plėtojant, kuriant, atrenkant ir naudojant taikomąsias programas, paslaugas ir produktus, kurie grindžiami asmens duomenų tvarkymu arba kurių atveju asmens duomenys yra tvarkomi siekiant įvykdyti tam tikrą užduotį, tokių produktų, paslaugų ir taikomųjų programų gamintojai, kurdami tokius produktus, paslaugas ir taikomąsias programas, turėtų būti skatinami atsižvelgti į teisę į duomenų apsaugą ir, tinkamai atsižvelgiant į techninių galimybių išsivystymo lygį, turėtų būti skatinami užtikrinti, kad duomenų valdytojai ir duomenų tvarkytojai galėtų vykdyti savo duomenų apsaugos prievoles.“

2 25 STRAIPSNIO „PRITAIKYTOJI DUOMENŲ APSAUGA IR STANDARTIZUOTOJI DUOMENŲ APSAUGA“ 1 IR 2 DALIES ANALIZĖ

5. Šio skyriaus tikslas – išnagrinėti 25 straipsnio 1 dalyje nustatytus pritaikytosios duomenų apsaugos ir 25 straipsnio 2 dalyje nustatytos standartizuotosios duomenų apsaugos reikalavimus ir pateikti jų įgyvendinimo gaires. Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga – tai viena kitą papildančios ir sustiprinančios sąvokos. Duomenų subjektai gaus daugiau naudos standartizuotąją duomenų apsaugą įgyvendindami kartu su pritaikytąja duomenų apsauga ir atvirkščiai.

6. PSDA reikalavimas privalomas visiems duomenų valdytojams, įskaitant mažas įmones ir tarptautines bendroves. Dėl šios priežasties įgyvendinti PSDA gali būti daugiau ar mažiau sudėtinga – tai priklauso nuo atskiros duomenų tvarkymo operacijos. Vis dėlto, neatsižvelgiant į dydį, PSDA įgyvendinimas visais atvejais gali būti naudingas tiek duomenų valdytojui, tiek duomenų subjektui.

2.1 25 straipsnio 1 dalis Pritaikytoji duomenų apsauga

2.1.1 Duomenų valdytojo pareiga tvarkant duomenis įgyvendinti tinkamas technines ir organizacines priemones ir būtinas apsaugos priemones

7. Pagal 25 straipsnio 1 dalį duomenų valdytojas įgyvendina *tinkamas* technines ir organizacines *priemones*, skirtas duomenų apsaugos principams įgyvendinti, ir į duomenų tvarkymą integruoja *būtinas apsaugos priemones*, kad jis atitiktų reglamento reikalavimus ir apsaugotų duomenų subjektų teises ir laisves. Tiek tinkamos priemonės, tiek būtinos apsaugos priemonės yra skirtos tam pačiam tikslui – apsaugoti duomenų subjektų teises ir užtikrinti, kad tvarkant jų asmens duomenis būtų užtikrinama jų asmens duomenų apsauga.

8. *Techninės ir organizacinės priemonės* ir būtinos *apsaugos priemonės* gali būti suprantamos plačiąja prasme kaip bet koks metodas ar būdas, kurį duomenų valdytojas gali naudoti tvarkydamas duomenis. Priemonės *tinkamos*, jei jos ir būtinos apsaugos priemonės yra tinkamos numatytam tikslui pasiekti, t. y. jas taikant duomenų apsaugos principai *veiksmingai* įgyvendinami[3]. Taigi tinkamumo reikalavimas yra glaudžiai susijęs su veiksmingumo reikalavimu.

9. Techninė ar organizacinė priemonė ir apsaugos priemonė gali būti tiek pažangių techninių sprendimų naudojimas, tiek darbuotojų pradinis mokymas. Atsižvelgiant į aplinkybes ir su atitinkamu duomenų tvarkymo veiksmu susijusius pavojus, būtų galima pateikti šiuos pavyzdžius: pseudonimų suteikimas asmens duomenims[4], turimų asmens duomenų saugojimas struktūrizuotu, dažnai taikomu kompiuterio skaitomu formatu, duomenų subjektams suteikiama galimybė įsikišti į duomenų tvarkymą, informacijos apie asmens duomenų saugojimą teikimas, kenkimo programinės įrangos aptikimo sistemų naudojimas, darbuotojų mokymas apie pagrindinę kibernetinę higieną, privatumo ir informacijos saugumo valdymo sistemų sukūrimas, sutartimi numatyta prievolė duomenų tvarkytojams įgyvendinti konkrečią duomenų kiekio mažinimo praktiką ir pan.

10. Nustatant, kokios priemonės yra tinkamos, gali būti naudingi asociacijų ir kitų įstaigų, atstovaujančių tam tikrų kategorijų duomenų valdytojams, pripažinti standartai, geriausia patirtis ir elgesio kodeksai. Vis dėlto duomenų valdytojas turi patikrinti, ar priemonės yra tinkamos konkretaus atitinkamo duomenų tvarkymo veiksmo atveju.

[3] Sąvoka „veiksmingumas“ aptariama 2.1.2 poskyryje.
[4] Apibrėžta BDAR 4 straipsnio 5 dalyje.

2.1.2 Skirta duomenų apsaugos principams veiksmingai įgyvendinti ir duomenų subjektų teisėms ir laisvėms apsaugoti

11. 5 straipsnyje yra išdėstomi *duomenų apsaugos principai* (toliau – principai); *duomenų subjektų teisės ir laisvės* – tai fizinių asmenų pagrindinės teisės ir laisvės, taip pat, visų pirma, jų teisė į asmens duomenų apsaugą, šių teisių apsauga 1 straipsnio 2 dalyje yra nurodoma kaip BDAR tikslas (toliau – teisės)[5]. Tikslią jų formuluotę galima rasti ES pagrindinių teisių chartijoje. Labai svarbu, kad duomenų valdytojas suprastų *principų* ir *teisių* prasmę, kadangi jais grindžiama BDAR nustatyta apsauga ir konkrečiai PSDA prievolė.

12. Įgyvendinant tinkamas technines ir organizacines priemones, priemonės ir apsaugos priemonės turėtų būti *parengtos* atsižvelgiant į veiksmingą kiekvieno iš pirmiau minėtų principų ir nustatytų teisių apsaugos įgyvendinimą.

Veiksmingumo klausimas

13. Pritaikytosios duomenų apsaugos koncepcijos esmė – veiksmingumas. Kadangi reikalaujama principus įgyvendinti veiksmingai, tai reiškia, kad siekdamas apsaugoti šiuos principus duomenų valdytojas turi įgyvendinti būtinas priemones ir apsaugos priemones, kad būtų užtikrintos duomenų subjektų teisės. Taikant kiekvieną įgyvendintą priemonę turėtų būti pasiekiami numatyti rezultatai tam duomenų tvarkymo atvejui, kurį numato atlikti duomenų valdytojas. Ši pastaba reiškia du dalykus.

14. Pirma, tai reiškia, kad pagal 25 straipsnį nėra reikalaujama įgyvendinti jokių konkrečių techninių ir organizacinių priemonių, veikiau reikalaujama, kad pasirinktos priemonės ir apsaugos priemonės turėtų būti konkrečiai skirtos tam, kad duomenų apsaugos principai būtų įgyvendinti konkretaus atitinkamo duomenų tvarkymo atveju. Atsižvelgiant į tai, priemonės ir apsaugos priemonės turėtų būti parengtos taip, kad jos veiktų tinkamai, o duomenų valdytojas turėtų galėti įgyvendinti papildomas priemones reaguodamas į padidėjusį pavojų[6]. Todėl tai, ar priemonės veiksmingos, priklausys nuo atitinkamo duomenų tvarkymo aplinkybių ir nuo tam tikrų elementų, į kuriuos turėtų būti atsižvelgiama nustatant duomenų tvarkymo būdus, vertinimo. Minėti elementai bus aptariami toliau esančiame 2.1.3 poskyryje.

15. Antra, duomenų valdytojai turėtų galėti įrodyti, kad šių principų buvo laikomasi.

16. Taikant įgyvendintas priemones ir apsaugos priemones turėtų būti pasiektas norimas su duomenų apsauga susijęs poveikis, o duomenų valdytojas turėtų turėti dokumentus, kuriais patvirtinamas techninių ir organizacinių priemonių įgyvendinimas[7]. Šiuo tikslu duomenų valdytojas gali nustatyti tinkamus pagrindinius veiklos rezultatų rodiklius (PVRR) veiksmingumui įrodyti. PVRR – duomenų valdytojo pasirinkta išmatuojama vertė, kuria parodoma, kaip veiksmingai duomenų valdytojas siekia savo duomenų apsaugos tikslo. PVRR gali būti *kiekybiniai*, pavyzdžiui, klaidingų teigiamų arba klaidingų neigiamų rezultatų procentinė dalis, skundų skaičiaus sumažinimas, atsakymo laiko sutrumpinimas

[5] Žr. BDAR 4 konstatuojamąją dalį.

[6] „Pagrindiniai duomenų valdytojams taikomi principai (t. y. teisėtumas, duomenų kiekio mažinimas, tikslo apribojimas, skaidrumas, duomenų vientisumas, duomenų tikslumas) turėtų išlikti tokie patys, neatsižvelgiant į duomenų tvarkymą ir duomenų subjektams kylantį pavojų. Tačiau deramas dėmesys tokio duomenų tvarkymo pobūdžiui ir aprėpčiai visada buvo neatsiejama šių principų taikymo dalis, kad juos būtų galima iš esmės keisti.“ 29 straipsnio darbo grupės pareiškimas dėl rizika grindžiamo požiūrio vaidmens duomenų apsaugos teisinėse sistemose. WP 218, 2014 m. gegužės 30 d., p. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Žr. 74 ir 78 konstatuojamąsias dalis.

duomenų subjektams naudojantis savo teisėmis, arba *kokybiniai*, pvz., veiklos rezultatų vertinimas, klasifikavimo skalių naudojimas ar ekspertų vertinimai. Kaip alternatyvą PVRR, duomenų valdytojas gali įrodyti, kad principai įgyvendinami veiksmingai, paaiškindamas savo pasirinktų priemonių ir apsaugos priemonių veiksmingumo vertinimą.

2.1.3 Elementai, į kuriuos reikia atsižvelgti

17. 25 straipsnio 1 dalyje išvardyti elementai, į kuriuos duomenų valdytojas turi atsižvelgti nustatydamas konkrečios duomenų tvarkymo operacijos priemones. Toliau pateiksime gaires, kaip šiuos elementus taikyti rengimo procese, apimančiame standartinių nustatymų rengimą. Tai, ar priemonė tinkama principams veiksmingai įgyvendinti, nustatoma naudojant visus šiuos elementus. Taigi kiekvienas iš šių elementų pats savaime nėra tikslas, bet vienas iš veiksnių, į kuriuos visus turi būti atsižvelgiama, kad uždavinys būtų įgyvendintas.

2.1.3.1 „Techninių galimybių išsivystymo lygis“

18. Sąvoka „techninių galimybių išsivystymo lygis“ vartojama įvairiuose ES *acquis*, pvz., aplinkos apsaugos ir produktų saugos srityse. BDAR „techninių galimybių išsivystymo lygis“[8] minimas ne tik 32 straipsnyje dėl saugumo priemonių[9][10], bet ir 25 straipsnyje, taip išplečiant šio kriterijaus taikymą visoms duomenų tvarkymo techninėms ir organizacinėms priemonėms.

19. 25 straipsnyje nurodyta prievolė atsižvelgti į „techninių galimybių išsivystymo lygį“ įpareigoja duomenų valdytojus, nustatant tinkamas technines ir organizacines priemones, **atsižvelgti į dabartinę** rinkoje esamų **technologijų pažangą**. Iš duomenų valdytojo reikalaujama žinoti apie technologijų pažangą ir nuolat domėtis nauja informacija apie ją, t. y. apie tai, kaip naudojamos technologijos gali kelti pavojų arba atverti galimybių duomenų tvarkymo operacijai, ir kaip įgyvendinti ir atnaujinti priemones ir apsaugos priemones, kuriomis *užtikrinamas veiksmingas* duomenų subjektų principų ir teisių *įgyvendinimas* atsižvelgiant į kintančią technologinę aplinką.

20. „Techninių galimybių išsivystymo lygis“ – dinamiška sąvoka, kuri negali būti statiškai apibrėžta konkrečiu laiku, bet turėtų būti *nuolat* vertinama atsižvelgiant į technologijų pažangą. Gali būti, kad atsižvelgdamas į technologijų pažangą, duomenų valdytojas nustatys, kad priemonė, anksčiau užtikrinusi tinkamą apsaugos lygį, tokios apsaugos daugiau nebeužtikrina. Todėl, jei nebus atsižvelgta į technologijų pokyčius, gali būti pažeistas 25 straipsnis.

21. „Techninių galimybių išsivystymo lygio“ kriterijus taikomas ne tik technologinėms, bet ir organizacinėms priemonėms. Tinkamų organizacinių priemonių nebuvimas gali sumažinti ar net panaikinti pasirinktos technologijos veiksmingumą. Gali būti taikomos, pvz., šios organizacinės priemonės: vidaus tvarkos priemonių priėmimas, atnaujinti mokymai technologijų, saugumo ir duomenų apsaugos srityse ir IT saugumo valdymo ir administravimo priemonės.

---

[8] Žr. Vokietijos Federalinio Konstitucinio Teismo 1978 m. sprendimą *Kalkar* (https://germanlawarchive.iuscomp.org/?p=67), kuriame pateiktas galimas objektyvus šios sąvokos apibrėžimo metodinis pagrindas. Juo remiantis, technologijų lygmuo „techninių galimybių išsivystymo lygis“ būtų nustatytas tarp technologijų lygmens „esamos mokslinės žinios ir moksliniai tyrimai“ ir labiau nusistovėjusių „visuotinai pripažintų technologinių taisyklių“. Taigi „techninių galimybių išsivystymo lygis“ gali būti suprantamas kaip paslaugos, technologijos ar produkto technologinis lygis, kuris egzistuoja rinkoje ir yra veiksmingiausias siekiant nustatytų tikslų.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security.

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/.

22. Įvairiose srityse taikomos ir pripažintos sistemos, standartai, sertifikavimas, elgesio kodeksai ir pan. gali būti svarbūs siekiant nustatyti „techninių galimybių išsivystymo lygį“ tam tikroje naudojimo srityje. Jei tokie standartai yra nustatyti ir juos taikant užtikrinamas aukštas duomenų subjekto apsaugos lygis laikantis teisinių reikalavimų arba juos viršijant, duomenų valdytojai turėtų į juos atsižvelgti rengdami ir įgyvendindami duomenų apsaugos priemones.

2.1.3.2 „Įgyvendinimo sąnaudos“

23. Siekdamas apsaugoti duomenų subjektų teises duomenų valdytojas gali atsižvelgti į įgyvendinimo sąnaudas, kai renkasi ir taiko tinkamas technines ir organizacines priemones ir būtinas apsaugos priemones, kuriomis veiksmingai įgyvendinami principai. Sąnaudos reiškia išteklius apskritai, įskaitant laiką ir žmogiškuosius išteklius.

24. Taikant sąnaudų elementą nėra reikalaujama, kad duomenų valdytojas skirtų neproporcingai daug išteklių, jei yra alternatyvių priemonių, kurios reikalauja mažiau išteklių, bet yra veiksmingos. Vis dėlto įgyvendinimo sąnaudos yra veiksnys, į kurį reikia atsižvelgti įgyvendinant pritaikytąją duomenų apsaugą, o ne priežastis jos neįgyvendinti.

25. Taigi taikant pasirinktas priemones užtikrinama, kad, neatsižvelgiant į sąnaudas, vykdant duomenų valdytojo numatytą duomenų tvarkymo veiklą asmens duomenys būtų tvarkomi nepažeidžiant principų. Duomenų valdytojas turėtų galėti valdyti bendras sąnaudas, kad galėtų veiksmingai įgyvendinti visus principus ir, atitinkamai, apsaugoti teises.

2.1.3.3 „Duomenų tvarkymo pobūdis, aprėptis, kontekstas ir tikslas“

26. Nustatydami reikalingas priemones duomenų valdytojai turi atsižvelgti į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslą.

27. Šie veiksniai turėtų būti aiškinami atsižvelgiant į jų reikšmę kitose BDAR nuostatose, pvz., 24, 32 ir 35 straipsniuose, siekiant parengti duomenų apsaugos principus, kurių turėtų būti laikomasis tvarkant duomenis.

28. Trumpai tariant, **pobūdžio** sąvoką galima suprasti kaip neatsiejamą[11] duomenų tvarkymo ypatybę. **Aprėptis** – tai duomenų tvarkymo mastas ir apimtis. **Kontekstas** – tai duomenų tvarkymo aplinkybės, kurios gali turėti įtakos duomenų subjekto lūkesčiams, o **tikslas** – tai duomenų tvarkymo paskirtis.

2.1.3.4 „Duomenų tvarkymo keliami įvairios tikimybės ir rimtumo pavojai fizinių asmenų teisėms ir laisvėms“

29. Daugelyje BDAR 24, 25, 32 ir 35 straipsnių nuostatų laikomasi nuoseklaus rizika grindžiamo metodo, siekiant nustatyti tinkamas technines ir organizacines priemones asmenims ir jų asmens duomenims apsaugoti ir laikytis BDAR reikalavimų. Saugotinos vertybės visada yra tos pačios (asmenys, saugomi užtikrinant jų asmens duomenų apsaugą), saugoma nuo tų pačių pavojų (asmenų teisėms), atsižvelgiant į tas pačias sąlygas (duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus).

30. Duomenų valdytojas, kai atlieka rizikos analizę siekdamas laikytis 25 straipsnio, turi nustatyti duomenų subjektų teisėms dėl principų pažeidimo kylančius pavojus, taip pat nustatyti tokių pavojų tikimybę ir

[11] Pavyzdžiui: asmens duomenų specialios kategorijos, automatinis sprendimų priėmimas, iškreiptas galios santykis, nenuspėjamas duomenų tvarkymas, sunkumai, su kuriais susiduria duomenų subjektas siekdamas pasinaudoti savo teisėmis ir pan.

rimtumą, kad galėtų įgyvendinti priemones, kuriomis būtų veiksmingai sumažinti nustatyti pavojai. Atliekant rizikos vertinimus labai svarbu duomenų tvarkymą įvertinti sistemingai ir išsamiai. Pavyzdžiui, tvarkydamas vaikų ir jaunimo iki 18 metų amžiaus (pažeidžiama grupė) asmens duomenis, duomenų valdytojas įvertina konkrečius pavojus, susijusius su tuo, kad nėra laisva valia duoto sutikimo (pažeidžiamas teisėtumo principas), o kito teisinio pagrindo nėra, ir įgyvendina atitinkamas priemones siekdamas panaikinti ir veiksmingai sumažinti nustatytus pavojus, susijusius su šia duomenų subjektų grupe.

31. Europos duomenų apsaugos valdybos poveikio duomenų apsaugai vertinimo (PDAV) gairėse[12], kuriose daugiausia dėmesio skiriama vertinimui, ar dėl duomenų tvarkymo operacijos gali kilti didelis pavojus duomenų subjektui, taip pat pateikiamos rekomendacijos, kaip įvertinti pavojų duomenų apsaugai ir kaip atlikti rizikos duomenų apsaugai vertinimą. Be to, šios gairės gali būti naudingos atliekant rizikos vertinimą pagal visus pirmiau minėtus straipsnius, įskaitant 25 straipsnį.

32. Taikant rizika grindžiamą metodą, neatmetama galimybė taikyti pradines reikšmes, geriausią patirtį ir standartus. Tai galėtų būti naudingas priemonių rinkinys duomenų valdytojams, kad jie galėtų spręsti su panašiais pavojais susijusius klausimus, kylančius panašiose situacijose (duomenų tvarkymo pobūdis, aprėptis, kontekstas ir tikslas). Nepaisant to, išlieka 25 straipsnyje (taip pat 24, 32 straipsniuose ir 35 straipsnio 7 dalies c punkte) nustatyta pareiga atsižvelgti „į duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms“. Todėl duomenų valdytojai, nors ir remdamiesi tokiomis priemonėmis, turi visada atlikti kiekvieno konkretaus duomenų tvarkymo veiksmo rizikos duomenų apsaugai vertinimą ir patikrinti tinkamų priemonių ir apsaugos priemonių veiksmingumą. Papildomai gali tekti atlikti arba atnaujinti esamą PDAV.

2.1.4 Laiko aspektas

2.1.4.1 Nustatant duomenų tvarkymo priemones

33. Pritaikytoji duomenų apsauga įgyvendinama „nustatant duomenų tvarkymo priemones“.

34. „Duomenų tvarkymo priemonės“ apima ir bendrus, ir detalius duomenų tvarkymo dizaino elementus, be kita ko, architektūrą, procedūras, protokolus, išdėstymą ir išvaizdą.

35. Sąvoka „nustatant duomenų tvarkymo priemones“ taikoma laikotarpiui, per kurį duomenų valdytojas nusprendžia, kaip duomenys bus tvarkomi ir kokios operacijos vyks, taip pat kokie mechanizmai bus naudojami duomenims tvarkyti. Priimdamas tokius sprendimus duomenų valdytojas privalo įvertinti tinkamas priemones ir apsaugos priemones, kad tvarkant duomenis principai ir duomenų subjektų teisės būtų veiksmingai įgyvendinami, taip pat atsižvelgti į tokius elementus kaip techninių galimybių išsivystymo lygis, įgyvendinimo sąnaudos, pobūdis, aprėptis, kontekstas, tikslas bei pavojai. Tai apima laiką, kai įsigyjama ir diegiama su duomenų tvarkymu susijusi programinė bei aparatinė įranga ir paslaugos.

36. Siekiant sėkmingai įgyvendinti principus ir apsaugoti duomenų subjektų teises labai svarbu anksti atsižvelgti į PSDA reikalavimus. Be to, žvelgiant iš sąnaudų ir naudos perspektyvos, duomenų valdytojams yra naudinga į PSDA atsižvelgti anksčiau, o ne vėliau, nes gali būti sudėtinga ir brangu vėliau keisti jau parengtus planus ir jau parengtas duomenų tvarkymo operacijas.

[12] 29 straipsnio darbo grupės Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų. WP 248 rev.01, 2017 m. spalio 4 d. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – patvirtinta Europos duomenų apsaugos valdybos.

2.1.4.2 Paties duomenų tvarkymo metu (atitikties duomenų apsaugos reikalavimams išlaikymas ir peržiūra)

37. Pradėjęs tvarkyti duomenis duomenų valdytojas privalo toliau išlaikyti atitiktį PSDA reikalavimams, t. y. toliau veiksmingai įgyvendinti principus siekdamas apsaugoti teises, užtikrinti naujausią techninių galimybių išsivystymo lygį, iš naujo įvertinti pavojaus lygį ir pan. Duomenų tvarkymo operacijų pobūdis, aprėptis ir kontekstas, taip pat su tuo susijęs pavojus gali keistis per tą laiką, kai duomenys tvarkomi, o tai reiškia, kad duomenų valdytojas privalo iš naujo įvertinti savo duomenų tvarkymo operacijas atlikdamas reguliarias pasirinktų priemonių ir apsaugos priemonių veiksmingumo peržiūras ir vertinimus.

38. Prievolė išlaikyti, peržiūrėti ir prireikus atnaujinti duomenų tvarkymo operacijas taip pat taikoma sistemoms, kurios buvo sukurtos anksčiau. Tai reiškia, kad ankstesnės sistemos, parengtos prieš įsigaliojant BDAR, turi būti peržiūrimos ir jų atitiktis turi būti patikrinta, kad būtų įgyvendintos priemonės ir apsaugos priemonės, kuriomis veiksmingai įgyvendinami principai ir duomenų subjektų teisės, kaip nurodyta šiose gairėse.

39. Ši prievolė taip pat taikoma bet kokiam duomenų tvarkymui, kurį atlieka duomenų tvarkytojai. Duomenų tvarkytojų vykdomos duomenų tvarkymo operacijos turėtų būti reguliariai peržiūrimos ir vertinamos siekiant užtikrinti, kad jos leidžia nuolat laikytis principų ir vykdyti duomenų valdytojo prievoles šioje srityje.

2.2 25 straipsnio 2 dalis Standartizuotoji duomenų apsauga

2.2.1 Standartizuotai tvarkomi tik tie asmens duomenys, kurie yra būtini kiekvienam konkrečiam duomenų tvarkymo tikslui

40. „Numatytoji nuostata“, kaip paprastai apibrėžiama informatikos srityje, reiškia jau esamą arba iš anksto nustatytos konfigūruojamosios nuostatos reikšmę, priskiriamą taikomajai programinei įrangai, kompiuterinei programai arba įrenginiui. Tokios nuostatos taip pat vadinamos išankstinėmis arba gamyklinėmis parinktimis (nuostatomis), ypač kai kalbama apie elektroninius prietaisus.

41. Taigi, kalbant apie asmens duomenų tvarkymą, sąvoka „standartizuotai“ taikoma sprendimams dėl konfigūracijos reikšmių ar duomenų tvarkymo parinkčių, kurios yra nustatytos ar numatytos duomenis tvarkančioje sistemoje, pvz., taikomojoje programinėje įrangoje, paslaugoje ar prietaise, arba tvarkymo rankiniu būdu procedūrai, kurią atliekant daromas poveikis surinktų asmens duomenų kiekiui, duomenų tvarkymo apimčiai, duomenų saugojimo laikotarpiui ir prieinamumui.

42. Duomenų valdytojas turėtų parinkti tokias numatytąsias duomenų tvarkymo nuostatas ir parinktis (ir už jas atsakyti), kad standartizuotai būtų atliekamas tik toks duomenų tvarkymas, kuris būtinas nustatytam, teisėtam tikslui pasiekti. Šiuo atveju duomenų valdytojai turi remtis savo vertinimu dėl duomenų tvarkymo būtinumo, atsižvelgdami į 6 straipsnio 1 dalyje nurodytus teisinius pagrindus. Tai reiškia, kad standartizuotai duomenų valdytojas renka ne daugiau duomenų, nei būtina, netvarko surinktų duomenų didesne apimtimi, nei būtina jų tikslams pasiekti, ir nesaugo duomenų ilgiau nei būtina. Pagrindinis reikalavimas yra tas, kad tvarkant duomenis būtų standartizuotai taikoma duomenų apsauga.

43. Duomenų valdytojas turi iš anksto nustatyti, kokiais nustatytais, aiškiai apibrėžtais ir teisėtais tikslais bus renkami ir tvarkomi asmens duomenys[13]. Priemonės turi būti automatiškai tinkamos užtikrinti, kad būtų tvarkomi tik tie asmens duomenys, kurie yra būtini kiekvienam konkrečiam duomenų tvarkymo tikslui pasiekti. EDAPP gairės, skirtos įvertinti priemonių, kuriomis ribojama teisė į asmens duomenų apsaugą, būtinumą ir proporcingumą, taip pat gali būti naudingos sprendžiant, kuriuos duomenis būtina tvarkyti, kad būtų pasiektas konkretus tikslas[14] [15] [16].

44. Jei duomenų valdytojas naudoja trečiosios šalies programinę įrangą arba standartinę programinę įrangą, jis turėtų atlikti produkto rizikos vertinimą ir užtikrinti, kad būtų išjungtos funkcijos, kurios neturi teisinio pagrindo arba yra nesuderinamos su numatytais duomenų tvarkymo tikslais.

45. Tas pats pasakytina ir apie organizacines priemones, kuriomis remiamos duomenų tvarkymo operacijos. Jos turėtų būti parengtos taip, kad iš pat pradžių būtų galima tvarkyti kuo mažesnį asmens duomenų kiekį, reikalingą konkrečioms operacijoms. Tai ypač turėtina omenyje tada, kai prieiga prie duomenų suteikiama darbuotojams, kurie atlieka įvairias funkcijas ir turi įvairius poreikius susipažinti su duomenimis.

46. Todėl tinkamos „techninės ir organizacinės priemonės“, susijusios su standartizuotąja duomenų apsauga, suprantamos taip pat, kaip aptarta pirmiau, 2.1.1 poskyryje, tačiau taikomos konkrečiai tam, kad būtų įgyvendintas duomenų kiekio mažinimo principas.

47. Pirmiau minėta prievolė tvarkyti tik tuos asmens duomenis, kurie yra būtini kiekvienam konkrečiam tikslui, taikoma šiems elementams.

2.2.2 Duomenų kiekio mažinimo prievolės matmenys

48. 25 straipsnio 2 dalyje išvardijami standartizuotosios duomenų kiekio mažinimo prievolės matmenys, nurodant, kad prievolė taikoma surinktų asmens duomenų kiekiui, jų tvarkymo apimčiai, jų saugojimo laikotarpiui ir jų prieinamumui.

2.2.2.1 „Surinktų asmens duomenų kiekis“

49. Duomenų valdytojai turėtų atsižvelgti tiek į asmens duomenų apimtį, tiek į duomenų tvarkymo tikslais reikalingų asmens duomenų rūšis, kategorijas ir išsamumo lygį. Priimant sprendimus priemonių parengimo metu, reikėtų atsižvelgti į padidėjusį pavojų vientisumo ir konfidencialumo, duomenų kiekio mažinimo ir saugojimo trukmės apribojimo principams, kai renkami dideli išsamių asmens duomenų kiekiai, ir palyginti jį su mažesniu pavojumi, renkant mažiau informacijos ir (arba) mažiau išsamią informaciją apie duomenų subjektus. Bet kuriuo atveju pagal standartinį nustatymą nerenkami asmens duomenys, kurie nebūtini konkrečiam duomenų tvarkymo tikslui. Kitaip tariant, jei tam tikrų kategorijų

[13] BDAR 5 straipsnio 1 dalies b, c, d ir e punktai.
[14] EDAPP, Gairės dėl priemonių, kuriomis ribojama teisė į duomenų apsaugą, būtinumo ir proporcingumo įvertinimo. 2019 m. vasario 25 d., edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.
[15] Taip pat žr. EDAPP, „Priemonių, kuriomis ribojama pagrindinė teisė į asmens duomenų apsaugą, būtinumo vertinimas: priemonių rinkinys“, https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en.
[16] Išsamiau apie būtinumą žr. 29 straipsnio darbo grupės Nuomonę Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį WP 217, 2014 m. balandžio 9 d. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lt.pdf.

asmens duomenys yra nebūtini arba jei nereikia išsamių duomenų, nes pakanka mažiau detalių duomenų, jokie pertekliniai asmens duomenys nerenkami.

50. Tokie patys standartizuotieji reikalavimai taikomi paslaugoms, neatsižvelgiant į tai, kokia platforma ar kokiu įrenginiu naudojamasi, t. y. galima rinkti tik konkrečiam tikslui būtinus asmens duomenis.

2.2.2.2 „Jų tvarkymo apimtis“

51. Asmens duomenys tvarkomi[17] tik tiek, kiek būtina. Duomenų tvarkymo tikslo galima siekti naudojant daug duomenų tvarkymo operacijų. Vis dėlto tai, kad tam tikri asmens duomenys yra būtini tikslui pasiekti, nereiškia, kad su tais duomenimis gali būti atliekamos visų rūšių ir dažnumo duomenų tvarkymo operacijos. Duomenų valdytojai taip pat turėtų būti atsargūs, kad neišplėstų 6 straipsnio 4 dalyje nurodytų „suderinamų tikslų“ ribų, ir turėti omenyje, koks duomenų tvarkymas atitiktų pagrįstus duomenų subjektų lūkesčius.

2.2.2.3 „Jų saugojimo laikotarpis“

52. Surinkti asmens duomenys nesaugomi, jei tai nėra būtina duomenų tvarkymo tikslu ir pagal 6 straipsnio 4 dalį nėra jokio kito suderinamo tikslo ir teisinio pagrindo. Duomenų valdytojas turėtų objektyviai pateisinti bet kokį duomenų saugojimą kaip būtiną pagal atskaitomybės principą.

53. Duomenų valdytojas apriboja saugojimo laikotarpį trukme, kiek yra būtina tikslui pasiekti. Jei asmens duomenys nebėra būtini duomenų tvarkymo tikslui, jie standartizuotai ištrinami arba nuasmeninami. Taigi saugojimo laikotarpio trukmė priklausys nuo atitinkamo duomenų tvarkymo tikslo. Ši prievolė yra tiesiogiai susijusi su 5 straipsnio 1 dalies e punkte nustatytu saugojimo trukmės apribojimo principu ir įgyvendinama standartizuotai, t. y. duomenų valdytojas turėtų būti įdiegęs sistemingas tvarkomų duomenų ištrynimo ar nuasmeninimo procedūras.

54. Asmens duomenų nuasmeninimas[18] yra alternatyva ištrynimui, jeigu atsižvelgiama į visus svarbius kontekstinius elementus ir reguliariai vertinama pavojaus tikimybė bei rimtumas, įskaitant pakartotinio identifikavimo pavojų[19].

2.2.2.4 „Jų prieinamumas“

55. Duomenų valdytojas turėtų nustatyti apribojimus, susijusius su tuo, kas turi galimybę susipažinti su asmens duomenimis, ir su tokios galimybės rūšimis, remdamasis būtinumo įvertinimu, taip pat užtikrinti, kad asmens duomenys iš tiesų būtų prieinami tiems, kam tai būtina ir kada tai būtina, pvz., kritinėse situacijose. Duomenų tvarkymo metu prieigos kontrolė turėtų būti taikoma visam duomenų srautui.

---

[17] Pagal BDAR 4 straipsnio 2 dalį duomenų tvarkymas – tai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.

[18] 29 straipsnio darbo grupės Nuomonė 05/2014 dėl nuasmeninimo metodų. WP 216, 2014 m. balandžio 10 d. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf.

[19] Žr. BDAR 4 straipsnio 1 dalį, BDAR 26 konstatuojamąją dalį, 29 straipsnio darbo grupės Nuomonę 05/2014 dėl nuasmeninimo metodų. Taip pat žr. šio dokumento 3 skirsnio poskirsnį „Saugojimo trukmės apribojimas“, kuriame nurodoma, kad duomenų valdytojas turi užtikrinti įdiegto (-ų) nuasmeninimo metodo (-ų) veiksmingumą.

56. 25 straipsnio 2 dalyje taip pat nurodyta, kad su asmens duomenimis negalima leisti susipažinti neribotam fizinių asmenų skaičiui be fizinio asmens įsikišimo. Duomenų valdytojas, prieš paskelbdamas asmens duomenis apie duomenų subjektą ar kitaip suteikdamas galimybę su jais susipažinti neribotam fizinių asmenų skaičiui, standartizuotai apriboja jų prieinamumą ir suteikia duomenų subjektui galimybę įsikišti.

57. Neribotam fizinių asmenų skaičiui suteikus galimybę susipažinti su asmens duomenimis, duomenys gali būti platinami net didesniu mastu nei numatyta iš pradžių. Tai ypač svarbu kalbant apie internetą ir paieškos sistemas. Tai reiškia, kad duomenų valdytojai turėtų standartizuotai suteikti duomenų subjektams galimybę įsikišti prieš suteikiant galimybę asmens duomenimis naudotis atvirajame internete. Tai ypač svarbu kalbant apie vaikus ir pažeidžiamas grupes.

58. Priklausomai nuo duomenų tvarkymo teisinių pagrindų, galimybė įsikišti gali būti suteikiama skirtingai, atsižvelgiant į duomenų tvarkymo aplinkybes. Pavyzdžiui, prašyti sutikimo suteikti galimybę viešai susipažinti su asmens duomenimis ar taikyti tokias privatumo nuostatas, kad patys duomenų subjektai galėtų kontroliuoti galimybę viešai susipažinti su duomenimis.

59. Net ir tuo atveju, kai asmens duomenys paviešinami su duomenų subjekto žinia ir sutikimu, tai nereiškia, kad bet kuris kitas prieigą prie asmens duomenų turintis duomenų valdytojas gali laisvai juos tvarkyti savo tikslais – tam būtinas atskiras teisinis pagrindas[20].

3 DUOMENŲ APSAUGOS PRINCIPŲ ĮGYVENDINIMAS ASMENS DUOMENŲ TVARKYMO OPERACIJOSE, PANAUDOJANT PRITAIKYTĄJĄ IR STANDARTIZUOTĄJĄ DUOMENŲ APSAUGĄ

60. Visuose duomenų tvarkymo veiklos rengimo etapuose, įskaitant viešuosius pirkimus, konkursus, užsakomųjų paslaugų pirkimą, kūrimą, paramą, techninę priežiūrą, bandymą, saugojimą, ištrynimą ir pan., duomenų valdytojas turėtų atsižvelgti į įvairius PSDA elementus, kurie bus parodyti šiame skyriuje išdėstytais pavyzdžiais, pateikiamais principų įgyvendinimo kontekste, ir juos apsvarstyti[21] [22] [23].

61. Duomenų valdytojai turi įgyvendinti principus, kad užtikrintų PSDA. Šie principai yra, be kita ko, skaidrumas, teisėtumas, sąžiningumas, tikslo apribojimas, duomenų kiekio mažinimas, tikslumas, saugojimo trukmės apribojimas, vientisumas, konfidencialumas ir atskaitomybė. Šie principai išdėstyti BDAR 5 straipsnyje ir 39 konstatuojamojoje dalyje. Reikėtų pabrėžti, kad siekiant visapusiškai suprasti, kaip įgyvendinti PSDA, svarbu suprasti kiekvieno iš šių principų prasmę.

62. Pateikdami pavyzdžius, kaip užtikrinti PSDA veikimą, surašėme kiekvieno principo **pagrindinius PSDA elementus**. Nors pavyzdžiais išryškinamas konkretus atitinkamas duomenų apsaugos principas, galimas sutapimas ir su kitais glaudžiai susijusiais principais. Europos duomenų apsaugos valdyba pabrėžia, kad toliau pateikti pagrindiniai elementai ir pavyzdžiai nėra nei išsamūs, nei privalomi, o pateikti kaip gairės kiekvieno principo atveju. Duomenų valdytojai turi įvertinti, kaip užtikrinti, kad būtų laikomasi šių principų, kalbant apie konkrečią atitinkamą duomenų tvarkymo operaciją.

[20] Žr. bylą Nr. 931/13 Satakunnan Markkinapörssi Oy ir Satamedia Oy / Suomija.
[21] Daugiau pavyzdžių galima rasti Norvegijos duomenų apsaugos institucijos gairėse „*Software Development with Data Protection by Design and by Default*“. 2017 m. lapkričio 28 d. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729.
[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers.
[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

63. Nors šiame skirsnyje daugiausia dėmesio skiriama principų įgyvendinimui, duomenų valdytojas taip pat turėtų įgyvendinti *tinkamus* ir *veiksmingus* būdus užtikrinti duomenų subjektų teisių apsaugą, taip pat pagal BDAR III skyrių, jei tokia prievolė dar nėra nustatyta pačiais principais.

64. Atskaitomybė – tai bendrasis principas, kurį taikant duomenų valdytojui nustatoma atsakomybė parinkti būtinas technines ir organizacines priemones.

3.1 Skaidrumas[24]

65. Duomenų valdytojas turi aiškiai ir atvirai nurodyti duomenų subjektui, kaip jis rinks ir naudos asmens duomens, taip pat kaip jais dalinsis. Taikant skaidrumo principą duomenų subjektams suteikiama galimybė suprasti ir prireikus pasinaudoti 15–22 straipsniuose nustatytomis savo teisėmis. Šis principas įtvirtintas 12, 13, 14 ir 34 straipsniuose. Taikant priemones ir apsaugos priemones, kuriomis remiamas skaidrumo principo įgyvendinimas, taip pat turėtų būti padedama įgyvendinti šiuos straipsnius.

66. Įgyvendinant skaidrumo principą pagrindiniai pritaikomieji ir standartizuotieji elementai gali būti šie:

- Aiškumas – informacija turi būti išdėstyta aiškiai, paprastai, glaustai ir suprantamai.
- Semantika – pateikiama informacija turėtų būti aiškiai suprantama atitinkamai auditorijai.
- Prieinamumas – informacija turi būti lengvai prieinama duomenų subjektui.
- Kontekstas – informacija turėtų būti pateikiama tinkamu laiku ir tinkama forma.
- Tinkamumas – informacija turėtų būti svarbi ir taikytina konkrečiam duomenų subjektui.
- Universalumas – informacija turi būti prieinama visiems duomenų subjektams, užtikrinant ir automatinio nuskaitymo galimybę, siekiant pagerinti ir automatizuoti skaitomumą bei aiškumą.
- Suprantamumas – duomenų subjektai turėtų gerai suprasti, ko jie gali tikėtis jų asmens duomenų tvarkymo atveju, ypač kai duomenų subjektai yra vaikai ar kitos pažeidžiamos grupės.
- Teikimas įvairiais kanalais – informacija turėtų būti teikiama įvairiais kanalais ir priemonėmis, ne tik kaip tekstas, kad tikimybė, jog informacija veiksmingai pasieks duomenų subjektą, būtų didesnė.
- Teikimas sluoksniais – informacija turėtų būti pateikiama tokiais sluoksniais, kad būtų ir išsami, ir suprantama, o kartu atspindėtų pagrįstus duomenų subjektų lūkesčius.

Pavyzdys[25]

Savo svetainėje duomenų valdytojas pateikia savo privatumo politikos aprašą, kad įvykdytų skaidrumo reikalavimus. Privatumo politikos aprašas neturėtų būti toks ilgas, kad vidutiniam duomenų subjektui būtų sudėtinga į jį įsigilinti ir jį suprasti. Informacija surašoma aiškiai ir glaustai, kad svetainės naudotojui būtų lengva suprasti, kaip tvarkomi jo asmens duomenys. Todėl duomenų valdytojas teikia informaciją sluoksniais, kuriuose pabrėžia svarbiausius dalykus. Išsamesnė informacija turi būti lengvai randama. Pateikiami išskleidžiamieji meniu ir nuorodos į kitus puslapius, kur išsamiau paaiškinamos politikos aprašo dalys ir vartojamos sąvokos. Duomenų valdytojas taip pat užtikrina, kad informacija būtų teikiama įvairiais kanalais, pateikiant vaizdo įrašus, kuriuose paaiškinami svarbiausi raštu

[24] Išsamesnės informacijos apie tai, kaip suprasti skaidrumo sąvoką, galima rasti 29 straipsnio darbo grupės Gairėse dėl skaidrumo pagal Reglamentą 2016/679. WP 260 rev.01, 2018 m. balandžio 11 d. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 – patvirtinta Europos duomenų apsaugos valdybos.

[25] Prancūzijos duomenų apsaugos tarnyba paskelbė keletą pavyzdžių, susijusių su geriausia vartotojų informavimo patirtimi ir kitais skaidrumo principais: https://design.cnil.fr/en/.

pateikiamos informacijos aspektai. Informacija įvairiuose puslapiuose turi būti suderinta siekiant užtikrinti, kad sluoksniais pateikta informacija ne didintų, o mažintų painiavą.

Privatumo politika duomenų subjektams turėtų būti lengvai randama. Todėl ji skelbiama ir nurodoma visuose atitinkamos interneto svetainės tinklalapiuose, kad duomenų subjektas visada rastų informaciją vienu spustelėjimu. Pateikiama informacija taip pat rengiama pagal geriausią patirtį ir laikantis universalumo standartų, kad būtų prieinama visiems.

Be to, reikalinga informacija taip pat turėtų būti pateikiama tinkamame kontekste ir tinkamu laiku. Kadangi duomenų valdytojas su svetainėje surinktais duomenimis atlieka daug duomenų tvarkymo operacijų, jis, norėdamas įvykdyti skaidrumo reikalavimus, turi ne tik parengti ir svetainėje nurodyti bendrą privatumo politiką. Duomenų valdytojas parengia informacijos srautą, pateikdamas duomenų subjektui reikiamą informaciją atitinkamame kontekste, pvz., naudodamas informacinius fragmentus arba iššokančiuosius langus. Pavyzdžiui, prašydamas duomenų subjekto įvesti asmens duomenis, duomenų valdytojas informuoja duomenų subjektą, kaip bus tvarkomi asmens duomenys ir kodėl tie asmens duomenys yra būtini duomenų tvarkymo tikslams.

3.2 Teisėtumas

67. Duomenų valdytojas turi nurodyti galiojantį asmens duomenų tvarkymo teisinį pagrindą. Taikomos priemonės ir apsaugos priemonės turėtų padėti įvykdyti reikalavimą užtikrinti, kad visas duomenų tvarkymo ciklas atitiktų atitinkamus teisinius duomenų tvarkymo pagrindus.

68. Įgyvendinant teisėtumo principą pagrindiniai pritaikomieji ir standartizuotieji elementai gali būti šie:
    - Tinkamumas – duomenys turi būti tvarkomi laikantis tinkamo teisinio pagrindo.
    - Diferencijavimas[26] – diferencijuojamas kiekvienos duomenų tvarkymo veiklos teisinis pagrindas.
    - Konkretus tikslas – tinkamas teisinis pagrindas turi būti aiškiai susietas su konkrečiu duomenų tvarkymo tikslu[27].
    - Būtinumas – kad tikslas būtų teisėtas, duomenų tvarkymas turi būti būtinas ir besąlyginis.
    - Savarankiškumas – duomenų subjektui turėtų būti suteikta kuo daugiau savarankiškumo asmens duomenų kontrolės srityje, laikantis teisinio pagrindo.
    - Sutikimo gavimas – sutikimas turi būti duotas laisva valia, konkretus, gavus tinkamą informaciją ir nedviprasmiškas[28]. Ypatingas dėmesys turėtų būti skiriamas vaikų ir jaunimo gebėjimui duoti informuoto asmens sutikimą.
    - Sutikimo atšaukimas – tuo atveju, kai sutikimas yra teisinis pagrindas, tvarkant duomenis turėtų būti lengviau sutikimą atšaukti. Atšaukti sutikimą turi būti taip pat lengva, kaip ir jį duoti. Jei taip nėra, tada duomenų valdytojo taikomas sutikimo mechanizmas neatitinka BDAR[29].
    - Interesų derinimas – tuo atveju, kai teisinis pagrindas yra teisėtas interesas, duomenų valdytojas turi pasverti interesus, ypatingą dėmesį skirdamas galios disbalansui, visų pirma

[26] Europos duomenų apsaugos valdybos gairės 2/2019 dėl asmens duomenų tvarkymo pagal Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies b punktą, kai duomenų subjektams teikiamos internetinės paslaugos. 2.0 versija, 2019 m. spalio 8 d. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_lt.pdf.
[27] Žr. toliau pateiktą skirsnį apie tikslo apribojimą.
[28] Žr. Gaires 05/2020 dėl sutikimo pagal Reglamentą 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_lt.
[29] Žr. Gaires 05/2020 dėl sutikimo pagal Reglamentą 2016/679, p. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_lt.

kalbant apie jaunesnius nei 18 metų vaikus ir kitas pažeidžiamas grupes. Turi būti numatomos priemonės ir apsaugos priemonės siekiant sumažinti neigiamą poveikį duomenų subjektams.

- Išankstinis nustatymas – teisinis pagrindas nustatomas prieš pradedant tvarkyti duomenis.
- Nutraukimas – jei teisinis pagrindas nebegalioja, duomenų tvarkymas atitinkamai nutraukiamas.
- Patikslinimas – jei duomenų tvarkymo teisinis pagrindas pagrįstai pasikeičia, faktinis duomenų tvarkymas turi būti patikslintas atsižvelgiant į naują teisinį pagrindą[30].
- Atsakomybės pasidalijimas – kai numatomas bendras duomenų valdymas, šalys turi aiškiai ir skaidriai pasidalyti savo atitinkamą atsakomybę duomenų subjekto atžvilgiu ir pagal tai parengti duomenų tvarkymo priemones.

Pavyzdys

Bankas planuoja teikti paslaugą, padėsiančią veiksmingiau tvarkyti paskolų paraiškas. Paslauga grindžiama idėja, kad bankas, prašydamas kliento leidimo, gali gauti duomenis apie klientą tiesiai iš viešųjų mokesčių administratorių. Šiame pavyzdyje neatsižvelgiama į asmens duomenų, kurie gauti iš kitų šaltinių, tvarkymą.

Būtina gauti asmens duomenis apie duomenų subjekto finansinę padėtį, kad duomenų subjekto prašymu būtų imtasi veiksmų prieš sudarant kredito sutartį[31]. Vis dėlto laikoma, kad asmens duomenis nėra būtina rinkti tiesiai iš mokesčių administratoriaus, nes klientas gali sudaryti sutartį pats pateikdamas mokesčių administratoriaus turimą informaciją. Nors bankas gali turėti teisėtą interesą gauti dokumentus tiesiai iš mokesčių administratorių, pvz., siekiant užtikrinti veiksmingą paskolų tvarkymą, suteikiant bankams tokią tiesioginę prieigą prie pareiškėjų asmens duomenų yra pavojų, susijusių su prieigos teisių naudojimu ar galimu piktnaudžiavimu jomis.

Įgyvendindamas teisėtumo principą, duomenų valdytojas suvokia, kad šiomis aplinkybėmis „būtina sudarant sutartį“ nėra tinkamas pagrindas tai duomenų tvarkymo daliai, kuri susijusi su asmens duomenų rinkimu tiesiogiai iš mokesčių administratorių. Tai, kad šis konkretus duomenų tvarkymo veiksmas kelia pavojų, kad duomenų subjektas mažiau dalyvaus tvarkant jo duomenis, taip pat yra svarbus veiksnys vertinant paties duomenų tvarkymo teisėtumą. Bankas daro išvadą, kad ši duomenų tvarkymo dalis turi būti grindžiama kitu duomenų tvarkymo teisiniu pagrindu. Konkrečioje valstybėje narėje, kurioje yra duomenų valdytojas, bankui pagal nacionalinę teisę leidžiama rinkti informaciją tiesiogiai iš viešųjų mokesčių administratorių, jei duomenų subjektas su tuo sutinka iš anksto.

Todėl bankas informaciją apie duomenų tvarkymą internetinėje paraiškų platformoje pateikia taip, kad duomenų subjektams būtų lengva suprasti, koks duomenų tvarkymas yra privalomas, o koks – neprivalomas. Pagal standartizuotąsias duomenų tvarkymo parinktis duomenų negalima gauti tiesiogiai iš kitų šaltinių nei pats duomenų subjektas, o tiesioginio informacijos gavimo parinktis pateikiama taip, kad neatgrasytų duomenų subjekto nuo jos nepateikimo. Bet koks sutikimas rinkti duomenis tiesiogiai iš kitų duomenų valdytojų yra laikina teisė susipažinti su tam tikra informacija.

Bet koks duotas sutikimas yra tvarkomas elektroniniu būdu ir dokumentuojamas, o duomenų subjektams pasiūlomas paprastas būdas kontroliuoti savo sutikimus ir juos atšaukti.

[30] Jei pradinis teisinis pagrindas yra sutikimas, žr. Gaires 05/2020 dėl sutikimo pagal Reglamentą 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_lt.

[31] Žr. BDAR 6 straipsnio 1 dalies b punktą.

Duomenų valdytojas prieš tai įvertina šiuos PSDA reikalavimus ir visus šiuos kriterijus įtraukia į viešojo pirkimo konkurso platformai įsigyti sąlygas. Duomenų valdytojas žino, kad jei PSDA reikalavimai nebus įtraukti į konkurso sąlygas, vėliau užtikrinti duomenų apsaugą gali būti per vėlu ar itin brangu.

3.3 Sąžiningumas

69. Sąžiningumas yra bendrasis principas, pagal kurį reikalaujama, kad asmens duomenys neturėtų būti tvarkomi duomenų subjektui nepateisinamai žalingu, neteisėtai diskriminuojančiu, netikėtu ar klaidinančiu būdu. Priemonėmis ir apsaugos priemonėmis, kuriomis įgyvendinamas sąžiningumo principas, taip pat remiamos duomenų subjektų teisės ir laisvės, visų pirma teisė į informaciją (skaidrumas), teisė įsikišti (prieiga, ištrynimas, duomenų perkeliamumas, taisymas) ir teisė apriboti duomenų tvarkymą (teisė, kad nebūtų taikomas automatizuotas individualių sprendimų priėmimas, taip pat duomenų subjektų nediskriminavimas tokiuose procesuose).

70. Įgyvendinant sąžiningumo principą pagrindiniai pritaikomieji ir standartizuotieji elementai gali būti šie:
    - Savarankiškumas – duomenų subjektams turėtų būti suteikta kuo daugiau savarankiškumo priimant sprendimus dėl jų asmens duomenų naudojimo, taip pat dėl to naudojimo ar duomenų tvarkymo apimties ir sąlygų.
    - Sąveika – duomenų subjektai turi turėti galimybę duomenų valdytojui nurodyti savo teises, susijusias su duomenų valdytojo tvarkomais asmens duomenimis, ir jomis pasinaudoti.
    - Lūkesčiai – duomenų tvarkymas turėtų atitikti duomenų subjektų pagrįstus lūkesčius.
    - Nediskriminavimas – duomenų valdytojas nesąžiningai nediskriminuoja duomenų subjektų.
    - Nesavanaudiškumas – duomenų valdytojas neturėtų savanaudiškai naudotis duomenų subjektų poreikiais ar pažeidžiamumu.
    - Vartotojų pasirinkimas – duomenų valdytojas neturėtų nesąžiningai susaistyti savo naudotojų. Kai asmens duomenys tvarkomi teikiant paslaugą, susijusią su nuosavybės teise, su tokia paslauga gali būti susaistoma, o tai gali būti nesąžininga, jei dėl to ribojama duomenų subjektų galimybė naudotis savo teise į duomenų perkeliamumą pagal 20 straipsnį.
    - Galios pusiausvyra – pasiekti galios pusiausvyrą turėtų būti pagrindinis duomenų valdytojo ir duomenų subjekto santykių tikslas. Turėtų būti vengiama galios disbalanso. Kai tai nėra įmanoma, galios disbalansas turėtų būti pripažįstamas ir į jį turėtų būti atsižvelgiama taikant tinkamas atsako priemones.
    - Draudimas perkelti riziką – duomenų valdytojai neturėtų perkelti įmonės patiriamos rizikos duomenų subjektams.
    - Draudimas klaidinti – duomenų tvarkymo informacija ir parinktys turėtų būti pateikiamos objektyviu ir neutraliu būdu, vengiant vartoti kalbą ar naudoti dizainą, kuriais siekiama klaidinti ar manipuliuoti.
    - Pagarba teisėms – duomenų valdytojas turi gerbti duomenų subjektų pagrindines teises ir įgyvendinti tinkamas priemones ir apsaugos priemones, taip pat turi nedaryti neigiamo poveikio tokioms teisėms, išskyrus atvejus, kai tai aiškiai pagrįsta teisės aktais.
    - Etika – duomenų valdytojas turėtų įvertinti įvairiapusiškesnį duomenų tvarkymo poveikį asmenų teisėms ir orumui.
    - Teisinga informacija – duomenų valdytojas turi pateikti informaciją apie tai, kaip jis tvarko asmens duomenis, taip pat turėtų veikti taip, kaip teigia, ir neklaidinti duomenų subjektų.

- Žmogaus įsikišimas – duomenų valdytojas turi užtikrinti *kvalifikuotą* žmogaus įsikišimą, galintį atskleisti šališkumus, kuriuos gali sukurti kompiuteriai, pagal 22 straipsnyje užtikrintą teisę į tai, kad nebūtų taikoma automatizuotų individualių sprendimų praktika[32].
- Teisingi algoritmai – reguliariai vertinti, ar algoritmai veikia pagal paskirtį ir tikslinti algoritmus siekiant sumažinti atskleistus šališkumus ir užtikrinti sąžiningą duomenų tvarkymą. Duomenų subjektai turėtų būti informuojami apie asmens duomenų tvarkymą, grindžiamą algoritmais, kuriuos pasitelkiant analizuojami arba prognozuojami aspektai, pvz., susiję su duomenų subjekto darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais, patikimumu arba elgesiu, vieta arba judėjimu[33].

1 pavyzdys

Duomenų valdytojas naudoja paieškos sistemą, kurioje tvarkomi daugiausia naudotojų sukurti asmens duomenys. Duomenų valdytojui naudingas didelis asmens duomenų kiekis ir galimybė tuos asmens duomenis naudoti tikslinei reklamai. Todėl duomenų valdytojas nori paveikti duomenų subjektus, kad jie leistų surinkti ir naudoti dar didesnį kiekį jų asmens duomenų. Sutikimas turi būti gaunamas duomenų subjektui pateikiant duomenų tvarkymo parinktis.

Įgyvendindamas sąžiningumo principą duomenų valdytojas, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslą, suvokia, kad negali pateikti galimybių taip, kad pastūmėtų duomenų subjektą leisti duomenų valdytojui surinkti daugiau asmens duomenų nei tuo atveju, jei parinktys būtų pateiktos vienodai ir neutraliai. Tai reiškia, kad duomenų valdytojai negali pateikti duomenų tvarkymo parinkčių taip, kad duomenų subjektams būtų sunku nesidalyti savo duomenimis ar kad jiems būtų sunku pakeisti savo privatumo nustatymus ir apriboti duomenų tvarkymą. Tai yra neskaidrių modelių, prieštaraujančių 25 straipsnio dvasiai, pavyzdžiai. Standartizuotosios duomenų tvarkymo parinktys neturėtų būti ribojančios privatumą, o tolesnio duomenų tvarkymo pasirinkimo galimybė turėtų būti pateikta taip, kad duomenų subjektas nebūtų spaudžiamas duoti sutikimą. Todėl duomenų valdytojas pateikia parinktis duoti sutikimą ar jo neduoti kaip du vienodai matomus pasirinkimus, tiksliai atspindėdamas kiekvieno pasirinkimo pasekmes duomenų subjektui.

2 pavyzdys

Kitas duomenų valdytojas tvarko asmens duomenis, teikdamas srautinio duomenų siuntimo paslaugą, kai naudotojai gali pasirinkti, ar užsisakyti įprastinį standartinės kokybės paslaugų abonementą, ar specialų aukštesnės kokybės paslaugų abonementą. Abonentams, užsisakiusiems specialųjį abonementą, teikiama pirmenybė teikiant klientų aptarnavimo paslaugas.

Atsižvelgiant į sąžiningumo principą, specialųjį abonementą užsisakiusiems abonentams teikiant pirmenybinę klientų aptarnavimo paslaugą negalima diskriminuoti įprastinį abonementą užsisakiusių abonentų galimybės naudotis savo teisėmis pagal BDAR 12 straipsnį. Tai reiškia, kad, nors specialaus abonemento turėtojams teikiama pirmenybė, dėl to negali pritrūkti tinkamų priemonių, kad būtų

[32] Žr. Gaires dėl automatizuoto individualių sprendimų priėmimo ir profiliavimo Reglamento 2016/679 tikslais https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826.
[33] Žr. BDAR 71 konstatuojamąją dalį.

galima nepagrįstai nedelsiant, bet kuriuo atveju ne vėliau kaip per vieną mėnesį nuo prašymų gavimo, reaguoti į įprastinių abonentų prašymus.

Prioritetiniai klientai gali mokėti už geresnes paslaugas, tačiau visi duomenų subjektai turi turėti vienodą ir nediskriminacinę galimybę įgyvendinti savo teises ir laisves pagal 12 straipsnį.

3.4 Tikslo apribojimas[34]

71. Duomenų valdytojas privalo rinkti duomenis nustatytais, aiškiai apibrėžtais ir teisėtais tikslais ir toliau netvarkyti duomenų tokiu būdu, kuris būtų nesuderinamas su jų surinkimo tikslu[35]. Todėl duomenų tvarkymas rengiamas atsižvelgiant į tai, kas būtina tikslams pasiekti. Jei ketinama toliau tvarkyti duomenis, duomenų valdytojas pirmiausia privalo įsitikinti, kad šio duomenų tvarkymo tikslai yra suderinami su pirminiais tikslais, ir atitinkamai parengti tokį duomenų tvarkymą. Ar naujas tikslas yra suderinamas, vertinama pagal 6 straipsnio 4 dalyje nustatytus kriterijus.

72. Įgyvendinant tikslo ribojimo principą pagrindiniai pritaikomieji ir standartizuotieji elementai gali būti šie:
    - Išankstinis nustatymas – teisėti tikslai nustatomi prieš rengiant duomenų tvarkymą.
    - Konkretumas – asmens duomenų tvarkymo tikslai yra nustatomi ir aiškiai apibrėžiami.
    - Tikslo orientavimas – duomenų tvarkymo tikslas turėtų būti orientyras rengiant duomenų tvarkymą ir nustatant duomenų tvarkymo ribas.
    - Būtinumas – tikslas lemia, kokie asmens duomenys yra būtini tvarkant duomenis.
    - Suderinamumas – bet koks naujas tikslas turi būti suderinamas su pradiniu tikslu, dėl kurio duomenys buvo surinkti, ir juo turi būti vadovaujamasi atitinkamai keičiant parengtas priemones.
    - Tolesnio duomenų tvarkymo ribojimas – duomenų valdytojas neturėtų sujungti duomenų rinkinių ar atlikti tolesnį duomenų tvarkymą naujais, nesuderinamais tikslais.
    - Pakartotinio naudojimo apribojimai – duomenų valdytojas turėtų naudoti technines priemones, įskaitant maišos funkciją ir šifravimą, kad apribotų galimybę pakeisti asmens duomenų paskirtį. Duomenų valdytojas taip pat turėtų taikyti organizacines priemones, pvz., politikos priemones ir sutartinius įsipareigojimus, kuriomis būtų ribojamas asmens duomenų pakartotinis naudojimas.
    - Peržiūra – duomenų valdytojas turėtų reguliariai peržiūrėti, ar duomenų tvarkymas yra būtinas tiems tikslams, dėl kurių duomenys buvo surinkti, ir išbandyti parengtas priemones pagal tikslo apribojimą.

Pavyzdys

Duomenų valdytojas tvarko savo klientų asmens duomenis. Duomenų tvarkymo tikslas – įvykdyti sutartį, t. y. galėti pristatyti prekes tinkamu adresu ir gauti užmokestį. Saugomi asmens duomenys yra pirkimo istorija, vardas ir pavardė / pavadinimas, adresas, e. pašto adresas ir telefono numeris.

[34] 29 straipsnio darbo grupė pateikė gaires, kaip suprasti tikslo apribojimo principą pagal Direktyvą 95/46/EB. Nors nuomonė nėra patvirtinta Europos duomenų apsaugos valdybos, ji vis tiek gali būti svarbi, nes BDAR šio principo formuluotė yra tokia pati. 29 straipsnio darbo grupės Nuomonė 03/2013 dėl tikslo apribojimo. WP 203, 2013 m. balandžio 2 d. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[35] BDAR 5 straipsnio 1 dalies b punktas.

Duomenų valdytojas svarsto galimybę pirkti ryšių su klientais valdymo (angl. *Customer Relationship Management*, CRM) produktą, kurį naudojant vienoje vietoje surenkami visi klientų duomenys, pvz., pardavimo, rinkodaros ir klientų aptarnavimo duomenys. Naudojant produktą suteikiama galimybė saugoti visus duomenis apie telefono skambučius, veiksmus, dokumentus, elektroninius laiškus ir rinkodaros kampanijas, kad būtų galima susidaryti visapusišką vaizdą apie klientą. Be to, naudodamas viešą informaciją CRM gali automatiškai analizuoti klientų perkamąją galią. Analizės tikslas – vykdyti tikslingesnę reklamos veiklą. Tokia veikla nėra susijusi su pradiniu teisėtu duomenų tvarkymo tikslu.

Kad atitiktų tikslo apribojimo principą, duomenų valdytojas reikalauja, kad produkto teikėjas įvertintų įvairios duomenų tvarkymo veiklos naudojant asmens duomenis suderinamumą su duomenų valdytojui svarbiais tikslais.

Gavęs įvertinimo rezultatus duomenų valdytojas vertina, ar naujas rinkodaros tikslas ir tikslinės reklamos tikslas suderinami su pradiniais tikslais, kurie buvo apibrėžti renkant duomenis, ir ar yra pakankamas teisinis pagrindas atitinkamam duomenų tvarkymui. Jei atlikus įvertinimą negaunamas teigiamas atsakymas, duomenų valdytojas nesinaudoja atitinkamomis funkcijomis. Kita vertus, duomenų valdytojas galėtų pasirinkti neatlikti vertinimo ir tiesiog nesinaudoti aprašytomis produkto funkcijomis.

3.5 Duomenų kiekio mažinimas

73. Tvarkomi tik tie asmens duomenys, kurie yra adekvatūs, tinkami ir apriboti to, kas **būtina** siekiant tikslo[36]. Todėl duomenų valdytojas turi iš anksto nustatyti, kokios duomenų tvarkymo sistemų savybės bei parametrai ir jų pagalbinės funkcijos yra leistinos. Duomenų kiekio mažinimu pagrindžiamas ir įgyvendinamas būtinumo principas. Toliau tvarkydamas duomenis, duomenų valdytojas turėtų periodiškai apsvarstyti, ar tvarkomi asmens duomenys vis dar adekvatūs, tinkami ir būtini, ar turi būti ištrinti arba nuasmeninti.

74. Duomenų valdytojai visų pirma turėtų įvertinti, ar jiems apskritai reikia tvarkyti asmens duomenis atitinkamais tikslais. Duomenų valdytojas turėtų patikrinti, ar atitinkami tikslai gali būti pasiekti tvarkant mažesnį kiekį asmens duomenų arba turint mažiau išsamių asmens duomenų ar apibendrintus asmens duomenis, ar apskritai netvarkant asmens duomenų[37]. Tokį patikrinimą reikėtų atlikti prieš pradedant bet kokį duomenų tvarkymą, bet jis taip pat galėtų būti atliekamas bet kuriuo duomenų tvarkymo ciklo metu. Tai atitinka ir 11 straipsnio reikalavimus.

75. Duomenų kiekio mažinimas taip pat gali būti susijęs su tapatybės nustatymo laipsniu. Jeigu siekiant duomenų tvarkymo tikslo nėra būtina, kad galutinis duomenų rinkinys būtų susijęs su asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta (pvz., statistikoje), tačiau tai būtina atliekant pirminį duomenų tvarkymą (pvz., prieš duomenų agregavimą), duomenų valdytojas ištrina ar nuasmenina asmens duomenis iš karto, kai tapatybės nustatymas tampa nebereikalingas. Tuo atveju, jei tolesnis tapatybės nustatymas reikalingas kitiems duomenų tvarkymo veiksmams, asmens duomenims turėtų būti suteikti pseudonimai, siekiant sumažinti pavojus duomenų subjektų teisėms.

76. Įgyvendinant duomenų kiekio mažinimo principą pagrindiniai pritaikomieji ir standartizuotieji elementai gali būti šie:

[36] BDAR 5 straipsnio 1 dalies c punktas.

[37] BDAR 39 konstatuojamojoje dalyje nurodyta: „...Asmens duomenys turėtų būti tvarkomi tik tuomet, jei asmens duomenų tvarkymo tikslo pagrįstai negalima pasiekti kitomis priemonėmis“.

- Duomenų tvarkymo vengimas – asmens duomenų tvarkymo apskritai reikia vengti, kai tai galima atsižvelgiant į atitinkamą tikslą.
- Apribojimas – renkamas tik toks asmens duomenų kiekis, koks būtinas tikslui pasiekti.
- Prieigos apribojimas – duomenų tvarkymas turi vykti taip, kad kuo mažiau žmonių reikėtų gauti prieigą prie asmens duomenų savo pareigoms atlikti, ir atitinkamai apriboti prieigą.
- Svarba – asmens duomenys turėtų būti svarbūs atliekant atitinkamą duomenų tvarkymą, o duomenų valdytojas turėtų galėti tai įrodyti.
- Būtinumas – kiekviena asmens duomenų kategorija turi būti būtina atsižvelgiant į konkrečius tikslus ir turėtų būti tvarkoma tik tuo atveju, jei tikslo neįmanoma pasiekti kitomis priemonėmis.
- Agregavimas – jei įmanoma, naudojami agreguoti duomenys.
- Pseudonimų suteikimas – pseudonimai suteikiami asmens duomenims iš karto, kai nebėra būtina turėti asmens duomenų, iš kurių tiesiogiai nustatoma tapatybė; tapatybės nustatymo raktai saugomi atskirai.
- Nuasmeninimas ir ištrynimas – kai asmens duomenys nėra (nebėra) būtini atitinkamam tikslui pasiekti, jie nuasmeninami arba ištrinami.
- Duomenų srautas – duomenų srautas turėtų būti pakankamai efektyvus, kad nebūtų sukurta daugiau kopijų nei būtina.
- „Techninių galimybių išsivystymo lygis“ – duomenų valdytojas turėtų taikyti atnaujintas ir tinkamas duomenų tvarkymo vengimo ir jų kiekio mažinimo technologijas.

1 pavyzdys

Knygynas siekia padidinti savo pajamas parduodamas knygas internetu. Knygyno savininkas nori parengti standartinę užsakymo formą. Kad klientai pateiktų visą jo norimą informaciją, knygyno savininkas reikalauja užpildyti visus formos laukelius (jei neužpildyti visi laukeliai, klientas negali pateikti užsakymo). Internetinės parduotuvės savininkas iš pradžių naudoja standartinę kontaktinę formą, kurioje prašoma pateikti informaciją, be kita ko, kliento gimimo datą, telefono numerį ir namų adresą. Tačiau ne visi formos laukeliai yra reikalingi knygoms pirkti ir pristatyti. Šiuo konkrečiu atveju, jei duomenų subjektas sumoka už produktą iš anksto, perkant produktą nėra reikalinga nurodyti duomenų subjekto gimimo datą ir telefono numerį. Tai reiškia, kad siekiant užsisakyti produktą negalima reikalauti užpildyti šiuos laukelius internetinėje formoje, išskyrus atvejus, kai duomenų valdytojas gali aiškiai įrodyti, kad tai yra būtina dėl kitų priežasčių ir kodėl būtina užpildyti šiuos laukelius. Be to, būna atvejų, kai adreso nereikės. Pavyzdžiui, užsisakydamas elektroninę knygą klientas gali ją parsisiųsti tiesiai į savo įrenginį.

Todėl internetinės parduotuvės savininkas nusprendžia sukurti dvi internetines formas: vieną – knygų užsakymui, kurioje yra kliento adreso laukelis, ir kitą – elektroninių knygų užsakymui be kliento adreso laukelio.

2 pavyzdys

Viešojo transporto bendrovė nori rinkti statistinę informaciją apie keleivių maršrutus. Tai leidžia tinkamai pritaikyti viešojo transporto tvarkaraščius ir nustatyti tinkamus traukinių maršrutus. Keleiviai turi pridėti savo bilietą prie skaitytuvo kiekvieną kartą, kai įlipa į transporto priemonę arba išlipa iš jos.

Įvertinęs riziką, kuri susijusi su keleivių teisėmis ir laisvėmis ir kuri kyla renkant informaciją apie keleivių kelionės maršrutus, duomenų valdytojas padaro išvadą, kad keleivių tapatybę galima nustatyti pagal bilieto identifikatorių tokiomis aplinkybėmis – nustatant konkretų maršrutą, kai keleiviai dirba ar gyvena retai apgyvendintose vietovėse. Todėl, turint omenyje, kad tai nėra būtina siekiant optimizuoti viešojo transporto traukinių tvarkaraščius ir maršrutus, duomenų valdytojas bilieto identifikatoriaus nesaugo. Pasibaigus kelionei, duomenų valdytojas saugo tik atskirų kelionės maršrutų duomenis, kad negalėtų nustatyti su konkrečiu bilietu susietų kelionių, o tik išsaugotų informaciją apie atskirus kelionės maršrutus.

Tais atvejais, kai vis dar gali kilti pavojus, kad asmens tapatybė bus nustatyta tiesiog pagal jo viešojo transporto maršrutą, duomenų valdytojas siekdamas sumažinti pavojų įgyvendina statistikos priemones, pvz., ištrina duomenis apie maršruto pradžią ir pabaigą.

3 pavyzdys

Kurjeris siekia įvertinti savo pristatymų veiksmingumą pagal pristatymo laiką, darbo grafiką ir degalų sąnaudas. Kad pasiektų šį tikslą, kurjeris turi tvarkyti tam tikrus asmens duomenis, susijusius tiek su darbuotojais (vairuotojais), tiek su klientais (adresai, siunčiami daiktai ir pan.). Ši duomenų tvarkymo operacija kelia pavojų, kad bus stebimi darbuotojai – tam reikia specialių teisinių apsaugos priemonių; taip pat yra pavojus, kad bus stebimi klientų įpročiai, remiantis ilgainiui surinkta informacija apie pristatytas prekes. Šiuos pavojus galima reikšmingai sumažinti tinkamai suteikiant pseudonimus darbuotojams ir klientams. Visų pirma, jei pseudonimų suteikimo raktai dažnai keičiami ir vietoj tikslių adresų vertinamos vietovės, siekiama veiksmingai sumažinti duomenų kiekį, ir duomenų valdytojas gali sutelkti dėmesį tik į pristatymo procesą bei išteklių optimizavimo tikslą, nevykdydamas asmenų (klientų ar darbuotojų) elgesio stebėsenos.

4 pavyzdys

Ligoninė renka duomenis apie savo pacientus ligoninės informacinėje sistemoje (elektroniniuose sveikatos įrašuose). Ligoninės darbuotojams reikia susipažinti su pacientų bylomis, kad galėtų priimti informacija pagrįstus sprendimus, susijusius su pacientų priežiūra ir gydymu ir kad galėtų dokumentuoti visus atliktus diagnostinius, priežiūros ir gydymo veiksmus. Standartizuotai galimybė susipažinti suteikiama tik tiems medicinos darbuotojams, kurie yra paskirti gydyti atitinkamą pacientą specializuotame departamente, kuriam priskirtas pacientas. Asmenų, galinčių susipažinti su paciento byla, yra daugiau, jei gydyme dalyvauja kiti departamentai ar diagnostikos skyriai. Po to, kai pacientas išrašomas ir parengiamos sąskaitos, galimybė susipažinti apribojama nedidele darbuotojų grupe kiekviename specializuotame departamente; jie, gavus atitinkamo paciento leidimą, atsako į kitų medicinos paslaugų teikėjų prašymus suteikti medicininę informaciją ar informaciją apie surengtas ar prašytas surengti konsultacijas.

3.6 Tikslumas

77. Asmens duomenys turi būti tikslūs ir nuolat atnaujinami, taip pat turi būti imamasi visų pagrįstų priemonių siekiant užtikrinti, kad netikslūs asmens duomenys, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi[38].

78. Reikalavimai turėtų būti vertinami atsižvelgiant į konkretaus duomenų panaudojimo pavojų ir pasekmes. Netikslūs asmens duomenys galėtų kelti pavojų duomenų subjektų teisėms ir laisvėms, pvz., kai dėl to neteisingai nustatoma diagnozė arba netinkamai vykdomas gydymo protokolas, arba dėl neteisingo asmens atvaizdo sprendimai gali būti priimami netinkamu pagrindu naudojant rankinį būdą, automatizuotą sprendimų priėmimą arba dirbtinį intelektą.

79. Įgyvendinant tikslumo principą pagrindiniai pritaikomieji ir standartizuotieji elementai gali būti šie:
    - Duomenų šaltinis – asmens duomenų šaltiniai turėtų būti patikimi duomenų tikslumo požiūriu.
    - Tikslumo laipsnis – kiekvieno asmens duomenų elemento tikslumas turėtų būti toks, koks būtinas nurodytiems tikslams pasiekti.
    - Išmatuojamas tikslumas – turi būti sumažintas klaidingų teigiamų / neigiamų rezultatų skaičius, pvz., šališkumai sprendimus priimant automatizuotai arba naudojant dirbtinį intelektą.
    - Tikrinimas – atsižvelgdamas į duomenų pobūdį ir į tai, kaip dažnai jie gali keistis, duomenų valdytojas turėtų su duomenų subjektu patikrinti asmens duomenų teisingumą prieš tvarkydamas duomenis ir įvairiais jų tvarkymo etapais (pvz., su asmens amžiumi susiję reikalavimai).
    - Ištrynimas / taisymas – duomenų valdytojas nedelsdamas ištrina arba ištaiso netikslius duomenis. Duomenų valdytojas tam sudaro palankesnes sąlygas visų pirma tada, kai duomenų subjektai yra ar buvo vaikai ir jie vėliau siekia pašalinti tokius asmens duomenis[39].
    - Klaidų sklaidos vengimas – duomenų valdytojai turėtų sumažinti susikaupusių klaidų poveikį duomenų tvarkymo grandinėje.
    - Galimybė susipažinti – pagal BDAR 12–15 straipsnius duomenų subjektams turėtų būti pateikta informacija apie asmens duomenis ir apie tai, kaip veiksmingai su jais susipažinti, kad jie galėtų kontroliuoti jų tikslumą ir prireikus juos ištaisyti.
    - Nuolatinis tikslumas – turėtų būti užtikrintas duomenų tikslumas visuose tvarkymo etapuose, todėl svarbiose pakopose turėtų būti atliekami tikslumo patikrinimai.
    - Naujumas – asmens duomenys atnaujinami, jei tai būtina tikslui pasiekti.
    - Duomenų rengimas – siekiant sumažinti netikslumą, naudoti technologines ir organizacines rengimo priemones, pvz., pateikti ne laisvos formos teksto laukelius, o iš anksto nustatytus, glaustus pasirinkimus.

1 pavyzdys

Kurdama draudimą perkančių klientų profilius draudimo bendrovė norėtų naudoti dirbtinį intelektą (DI), kad remdamasi šiais profiliais galėtų priimti sprendimus apskaičiuodama draudimo riziką. Spręsdama, kaip turėtų būti parengti jos DI sprendimai, draudimo bendrovė nustato duomenų tvarkymo būdus ir, pasirinkdama pardavėjo siūlomą DI taikomąją programą ir spręsdama, kaip mokyti DI, atsižvelgia į pritaikytąją duomenų apsaugą.

[38] BDAR 5 straipsnio 1 dalies d punktas.
[39] Plg. 65 konstatuojamąją dalį.

Spręsdamas, kaip mokyti DI, duomenų valdytojas turėtų turėti tikslius duomenis, kad gautų tikslius rezultatus. Todėl duomenų valdytojas turėtų užtikrinti, kad DI mokymui naudojami duomenys būtų tikslūs.

Įsitikinęs, kad turi galiojantį teisinį pagrindą mokyti DI panaudojant asmens duomenis iš didelio esamų klientų poaibio, duomenų valdytojas pasirenka populiaciją reprezentuojančią klientų grupę, kad išvengtų ir šališkumo.

Tuomet iš atitinkamos duomenų tvarkymo sistemos renkami klientų duomenys, be kita ko, duomenys apie draudimo rūšį, pvz., sveikatos draudimą, būsto draudimą, kelionių draudimą ir pan., taip pat viešųjų registrų, prie kurių jie turi teisėtą prieigą, turimus duomenis. Visiems duomenims yra suteikiami pseudonimai, o po to jie perduodami į dirbtinio intelekto modelio mokymui skirtą sistemą.

Siekdamas užtikrinti, kad DI mokymui naudojami duomenys būtų kuo tikslesni, duomenų valdytojas renka duomenis tik iš duomenų šaltinių, kuriuose pateikiama teisinga ir naujausia informacija.

Draudimo bendrovė patikrina, ar DI yra patikimas ir teikia nediskriminuojančius rezultatus tiek DI kūrimo metu, tiek prieš išleisdama galutinę produkto versiją. Kai baigiamas DI visapusiško mokymo procesas ir jis veikia, draudimo bendrovė naudoja gautus rezultatus pagrįsdama draudimo rizikos vertinimus, bet sprendimą, ar suteikti draudimą, priima nesikliaudama tik DI, išskyrus atvejus, kai sprendimas priimamas pagal BDAR 22 straipsnio 2 dalyje nustatytas išimtis.

Draudimo bendrovė taip pat reguliariai peržiūrės dirbtinio intelekto teikiamus rezultatus siekdama laikytis patikimumo kriterijaus ir, prireikus, tikslins algoritmą.

2 pavyzdys

Duomenų valdytojas yra sveikatos įstaiga, kuri ieško metodų, kaip užtikrinti savo klientų registruose saugomų asmens duomenų vientisumą ir tikslumą.

Tais atvejais, kai du asmenys atvyksta į įstaigą tuo pačiu metu ir jiems taikomas toks pat gydymas, yra pavojus, kad jie bus supainioti, jei vienintelis jų atskyrimo parametras yra vardas ir pavardė. Siekiant užtikrinti tikslumą, duomenų valdytojui reikia unikalaus identifikatoriaus kiekvienam asmeniui, todėl reikia daugiau informacijos nei tik kliento vardas ir pavardė.

Įstaiga naudoja kelias sistemas, kuriose saugoma asmeninė klientų informacija, ir turi užtikrinti, kad su klientu susijusi informacija būtų teisinga, tiksli ir nuosekli visose sistemose bet kuriuo metu. Įstaiga nustatė keletą pavojų, kurie gali kilti pasikeitus informacijai vienoje sistemoje, bet nepasikeitus kitoje.

Duomenų valdytojas nusprendžia sumažinti pavojų pasitelkdamas maišos metodą, kurį galima naudoti paciento kortelės duomenų vientisumui užtikrinti. Paciento kortelės įrašams ir su jais susijusiam klientui sukuriamos nekintamos kriptografinės laiko žymos, kad prireikus bet kokius pakeitimus būtų galima atpažinti, susieti ir atsekti.

3.7 Saugojimo trukmės apribojimas

80. Duomenų valdytojas privalo užtikrinti, kad asmens duomenys būtų saugomi tokia forma, kad asmenų tapatybę būtų galima nustatyti ne ilgiau nei tai būtina siekiant tikslų, dėl kurių asmens duomenys tvarkomi[40].
Labai svarbu, kad duomenų valdytojas tiksliai žinotų, kokius asmens duomenis įmonė tvarko ir kodėl. Duomenų tvarkymo tikslas yra lemiamas kriterijus, pagal kurį sprendžiama, kiek laiko asmens duomenys turi būti saugomi.

81. Taikant priemones ir apsaugos priemones, kuriomis įgyvendinamas duomenų saugojimo trukmės apribojimo principas, yra papildomos duomenų subjektų teisės ir laisvės, visų pirma teisė reikalauti ištrinti duomenis ir teisė nesutikti.

82. Įgyvendinant saugojimo trukmės apribojimo principą pagrindiniai pritaikomieji ir standartizuotieji elementai gali būti šie:
    - Ištrynimas ir anoniminimas – duomenų valdytojas turėtų taikyti aiškias vidaus procedūras ir funkcijas, susijusias su ištrynimu ir (arba) anoniminimu.
    - Anoniminimo / ištrynimo veiksmingumas – duomenų valdytojas užtikrina, kad nebūtų įmanoma iš naujo identifikuoti nuasmenintų duomenų arba atkurti ištrintų duomenų, ir turėtų patikrinti, ar tai įmanoma.
    - Automatizavimas – tam tikrų asmens duomenų ištrynimas turėtų būti automatizuotas.
    - Saugojimo kriterijai – duomenų valdytojas nustato, kokie duomenys ir kokia jų saugojimo trukmė būtini tikslui pasiekti.
    - Pagrindimas – duomenų valdytojas turi galėti pagrįsti, kodėl tikslui pasiekti ir atitinkamų asmens duomenų atveju būtinas toks duomenų saugojimo laikotarpis, taip pat sugebėti atskleisti argumentus ir teisinius pagrindus, kuriais grindžiamas toks saugojimo laikotarpis.
    - Duomenų saugojimo taisyklių vykdymo užtikrinimas – duomenų valdytojas užtikrina, kad būtų laikomasi vidaus saugojimo taisyklių, ir atlieka patikrinimus, ar organizacija taiko savo politiką.
    - Atsarginės kopijos / registracijos žurnalai – duomenų valdytojai nustato, kokie asmens duomenys būtini atsarginėms kopijoms bei registracijos žurnalams ir kiek laiko juos reikia saugoti.
    - Duomenų srautas – duomenų valdytojai turėtų fiksuoti asmens duomenų srautą ir visas saugomas jo kopijas, taip pat siekti riboti jų laikiną saugojimą.

Pavyzdys

Duomenų valdytojas renka asmens duomenis turėdamas duomenų tvarkymo tikslą administruoti duomenų subjekto narystę. Asmens duomenys ištrinami, kai narystė nutraukiama ir nėra teisinio pagrindo toliau saugoti duomenis.

Duomenų valdytojas pirmiausia parengia duomenų saugojimo ir ištrynimo vidaus procedūrą. Pagal šią procedūrą, pasibaigus saugojimo laikotarpiui darbuotojai asmens duomenis ištrina rankiniu būdu. Darbuotojai laikosi procedūros, pagal kurią reguliariai trinami ir taisomi duomenys, esantys bet kokiuose prietaisuose, atsarginėse kopijose, registracijos žurnaluose, elektroniniuose laiškuose ir kitose atitinkamose laikmenose.

Kad ištrynimas būtų veiksmingesnis ir kad būtų išvengta klaidų, duomenų valdytojas pakeisdamas šią procedūrą įdiegia automatinę sistemą, kad duomenys būtų ištrinami automatiškai, patikimai ir

[40] BDAR 5 straipsnio 1 dalies c punktas.

reguliariau. Sistema sukonfigūruota taip, kad būtų laikomasi nustatytos duomenų ištrynimo procedūros, ir duomenys būtų trinami iš anksto nustatytais reguliariais intervalais, pašalinant asmens duomenis iš visų bendrovės saugojimo laikmenų. Duomenų valdytojas reguliariai peržiūri duomenų saugojimo procedūrą ir atlieka jos bandymus, taip pat užtikrina, kad ji atitiktų atnaujintą duomenų saugojimo politiką.

3.8 Vientisumas ir konfidencialumas

83. Vientisumo ir konfidencialumo principas, be kita ko, apima apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo, taikant tinkamas technines ar organizacines priemones. Asmens duomenų saugumui užtikrinti reikia imtis tinkamų priemonių, kurios parengtos siekiant išvengti duomenų saugumo pažeidimų ir juos valdyti, užtikrinti tinkamą duomenų tvarkymo užduočių vykdymą ir kitų principų laikymąsi ir sudaryti palankesnes sąlygas veiksmingai naudotis asmenų teisėmis.

84. 78 konstatuojamojoje dalyje nurodyta, kad viena iš PSDA priemonių galėtų būti galimybės *kurti ir tobulinti apsaugos priemones* suteikimas duomenų valdytojui. Kartu su kitomis PSDA priemonėmis 78 konstatuojamojoje dalyje siūloma duomenų valdytojams nustatyti pareigą nuolat vertinti, ar jie visada naudoja tinkamas duomenų tvarkymo priemones ir ar pasirinktomis priemonėmis iš tikrųjų siekiama pašalinti esamus pažeidžiamumus. Be to, duomenų valdytojai turėtų reguliariai peržiūrėti su asmens duomenimis susijusias ir jų saugumą užtikrinančias informacijos saugumo priemones ir duomenų saugumo pažeidimų nagrinėjimo procedūrą.

85. Įgyvendinant vientisumo ir konfidencialumo principą pagrindiniai pritaikomieji ir standartizuotieji elementai gali būti šie:
    - Informacijos saugumo valdymo sistema (ISVS) – reikia turėti veikiančias informacijos saugumo politikos ir procedūrų valdymo priemones.
    - Rizikos analizė – reikia vertinti asmens duomenų saugumui kylančius pavojus, atsižvelgiant į poveikį asmenų teisėms, ir imtis priemonių nustatytų pavojų atžvilgiu. Naudoti atliekant rizikos vertinimą; sukurti ir išlaikyti visapusišką, sistemingą ir realistišką grėsmių modeliavimą ir parengtos programinės įrangos atakos perimetro analizę, siekiant sumažinti atakos vektorius ir galimybes išnaudoti silpnąsias vietas ir pažeidžiamumus.
    - Pritaikytasis saugumas – rengiant ir kuriant sistemą reikia kuo anksčiau atsižvelgti į saugumo reikalavimus, taip pat nuolat integruoti ir atlikti atitinkamus bandymus.
    - Techninė priežiūra – reikia reguliariai peržiūrėti ir bandyti programinę įrangą, aparatinę įrangą, sistemas, paslaugas ir pan., siekiant nustatyti su duomenų tvarkymu susijusių sistemų pažeidžiamumus.
    - Prieigos kontrolės valdymas – tik įgaliotas personalas, kuriam informacija būtina, turėtų galėti susipažinti su asmens duomenimis, būtinais jų vykdomoms duomenų tvarkymo užduotims atlikti, o duomenų valdytojas įgaliotam personalui turėtų suteikti skirtingas prieigos teises.
        - Prieigos apribojimas (vykdytojai) – duomenų tvarkymas turi vykti taip, kad kuo mažiau žmonių reikėtų gauti prieigą prie asmens duomenų savo pareigoms atlikti, ir prieiga turi būti atitinkamai apribota.
        - Prieigos apribojimas (turinys) – kiekvienos duomenų tvarkymo operacijos atveju prieiga suteikiama tik prie tų kiekvieno duomenų rinkinio elementų, kurie būtini tai operacijai atlikti. Be to, atitinkamų darbuotojų prieigą prie duomenų reikia apriboti taip, kad jie galėtų susipažinti tik su į jų kompetenciją patenkančių duomenų subjektų duomenimis.

    - Prieigos atskyrimas – duomenų tvarkymas turi vykti taip, kad nė vienam asmeniui nebūtų reikalinga visapusiška prieiga prie visų apie duomenų subjektą surinktų duomenų, o tuo labiau – prie visų tam tikros duomenų subjektų kategorijos asmens duomenų.
- Saugus perdavimas – perduodami duomenys apsaugomi nuo neteisėtos ir netyčinės prieigos ir pakeitimų.
- Saugus saugojimas – saugomi duomenys apsaugomi nuo neteisėtos prieigos ir pakeitimų. Turėtų būti nustatytos procedūros, siekiant įvertinti centralizuoto ar decentralizuoto duomenų saugojimo pavojų ir kokioms asmens duomenų saugojimo kategorijoms šis pavojus kyla. Kai kuriems duomenims gali reikėti taikyti papildomas saugumo priemones arba atskirti nuo kitų duomenų.
- Pseudonimų suteikimas – asmens duomenims bei atsarginėms kopijoms / registracijos žurnalams turėtų būti suteikti pseudonimai, šia saugumo priemone siekiant kuo labiau sumažinti galimų duomenų saugumo pažeidimų pavojų ir tam panaudojant, pvz., maišos arba šifravimo priemones.
- Atsarginės kopijos / registracijos žurnalai – atsarginės kopijos daromos ir registracijos žurnalai vedami tiek, kiek būtina informacijos saugumui užtikrinti; audito seka ir įvykių stebėsena vykdoma kaip įprasta saugumo kontrolės priemonė. Jie saugomi nuo neteisėtos ar netyčinės prieigos ir pakeitimų, taip pat reguliariai peržiūrimi, o kilę incidentai turėtų būti sprendžiami nedelsiant.
- Veiklos atkūrimas po ekstremaliųjų įvykių / veiklos tęstinumas – reikia laikytis veiklos atkūrimo po ekstremaliųjų įvykių ir veiklos tęstinumo reikalavimų, kad po didelių incidentų būtų galima atkurti turimus asmens duomenis.
- Apsauga atsižvelgiant į kylantį pavojų – visų kategorijų asmens duomenys turėtų būti saugomi taikant priemones, kurios yra tinkamos atsižvelgiant į kylantį saugumo pažeidimo pavojų. Su ypatingu pavojumi susiję duomenys turėtų būti, kai įmanoma, saugomi atskirai nuo kitų asmens duomenų.
- Reagavimo į saugumo incidentus valdymas – reikia taikyti įprastą tvarką, procedūras ir naudoti išteklius, siekiant nustatyti, suvaldyti ir tvarkyti duomenų saugumo pažeidimus, apie juos pranešti ir iš jų pasimokyti.
- Incidentų valdymas – duomenų valdytojas turėtų būti nustatęs pažeidimų ir incidentų nagrinėjimo procedūras siekdamas, kad duomenų tvarkymo sistema veiktų geriau. Tokios procedūros yra, be kita ko, pranešimų procedūros, pvz., pranešimų (priežiūros institucijai) valdymas ir (duomenų subjektų) informavimas.

Pavyzdys

Duomenų valdytojas siekia gauti didelį kiekį asmens duomenų, kurie yra elektroninius (pacientų) sveikatos įrašus saugančioje medicinos duomenų bazėje, ir perkelti juos į specialų bendrovės duomenų bazės serverį, kad galėtų tvarkyti gautus duomenis kokybės užtikrinimo tikslais. Bendrovė įvertino, kad išrašų nukreipimas į serverį, kuris prieinamas visiems bendrovės darbuotojams, gali sukelti didelį pavojų duomenų subjektų teisėms ir laisvėms. Kadangi gautus pacientų duomenų išrašus būtina tvarkyti tik vienam bendrovės departamentui, duomenų valdytojas nusprendžia apriboti prieigą prie specialaus serverio ir ją suteikti tik to skyriaus darbuotojams. Be to, siekiant dar labiau sumažinti pavojų, prieš perkeliant duomenis jiems bus suteikti pseudonimai.

Siekdama reguliuoti prieigą ir sušvelninti žalos, kurią gali padaryti kenkimo programinė įranga, bendrovė nusprendžia atskirti tinklą ir nustatyti prieigos prie serverio kontrolę. Be to, bendrovė įdiegia saugumo stebėjimo ir įsibrovimo aptikimo bei prevencijos sistemą ir atskiria serverį nuo kasdienio

naudojimo. Įdiegiama automatizuota audito sistema prieigai ir pokyčiams stebėti. Tokiu būdu, sukonfigūravus tam tikrus su naudojimu susijusius įvykius, parengiamos ataskaitos ir automatiniai įspėjimai. Duomenų valdytojas užtikrins, kad darbuotojams prieiga prie duomenų būtų suteikiama, tik jei jiems būtina juos žinoti, ir kad suteikiama prieiga būtų tinkamo lygmens. Netinkamas naudojimas gali būti greitai ir lengvai aptinkamas.

Kai kurie išrašai turi būti lyginami su naujais išrašais, todėl reikalaujama, kad jie būtų saugomi tris mėnesius. Duomenų valdytojas nusprendžia juos perkelti į atskiras duomenų bazes tame pačiame serveryje ir juos saugoti naudodamas skaidrų ir stulpelio lygio šifravimą. Stulpelio duomenų iššifravimo raktai saugomi specialiuose saugumo moduliuose, kuriais gali naudotis tik įgaliotas personalas, bet negali jų gauti.

Geresnis sistemos veikimas ir didesnis patikimumas užtikrinamas nagrinėjant būsimus incidentus. Duomenų valdytojas supranta, kad prevencinės ir veiksmingos priemonės bei apsaugos priemonės turėtų būti įtrauktos į visus asmens duomenų tvarkymo veiksmus, kurių imamasi dabar ir ateityje, ir kad tai gali padėti ateityje užkirsti kelią tokiems duomenų saugumo pažeidimo incidentams.

Duomenų valdytojas šias saugumo priemones parengia siekdamas užtikrinti tikslumą, vientisumą ir konfidencialumą, taip pat siekdamas užkirsti kelią kenkimo programinės įrangos plitimui kibernetinių išpuolių metu ir užtikrinti, kad sprendimai geriau veiktų. Naudojant tinkamai veikiančias saugumo priemones stiprinamas duomenų subjektų pasitikėjimas.

3.9 Atskaitomybė[41]

86. Atskaitomybės principu nustatyta, kad duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi visų pirmiau minėtų principų, ir turi sugebėti įrodyti, kad jų laikomasi.

87. Duomenų valdytojas turi galėti įrodyti, kad laikosi principų. Šiuo tikslu duomenų valdytojas gali įrodyti, kokį poveikį turi priemonės, kurių imtasi siekiant apsaugoti duomenų subjektų teises ir kodėl šios priemonės laikomos tinkamomis ir veiksmingomis. Pavyzdžiui, įrodydamas, kodėl priemonė yra tinkama siekiant užtikrinti, kad būtų veiksmingai laikomasi saugojimo trukmės apribojimo principo.

88. Kad galėtų atsakingai tvarkyti asmens duomenis, duomenų valdytojas turėtų turėti žinių apie duomenų apsaugą ir galėti ją įgyvendinti. Tai reiškia, kad duomenų valdytojas turėtų suprasti, kokios duomenų apsaugos prievolės jam nustatytos BDAR, ir sugebėti jų laikytis.

4 REGLAMENTO 25 STRAIPSNIO 3 DALIS – SERTIFIKAVIMAS

89. Remiantis 25 straipsnio 3 dalimi, sertifikavimas pagal 42 straipsnį gali būti naudojamas kaip atitikties PSDA reikalavimams įrodymas. Kita vertus, dokumentai, kuriais įrodoma, kad laikomasi PSDA reikalavimų, taip pat gali būti naudingi sertifikavimo procese. Tai reiškia, kad tais atvejais, kai duomenų valdytojo ar duomenų tvarkytojo atliekamai duomenų tvarkymo operacijai išduotas sertifikatas pagal 42 straipsnį, priežiūros institucijos į tai atsižvelgia atlikdamos atitikties BDAR vertinimą, visų pirma kiek tai susiję su PSDA.

90. Kai duomenų valdytojo ar duomenų tvarkytojo atliekamai duomenų tvarkymo operacijai išduotas sertifikatas pagal 42 straipsnį, elementai, kurie naudojami siekiant įrodyti, kad laikomasi 25 straipsnio 1 ir 2 dalies nuostatų, yra susiję su rengimo procesais, t. y. duomenų tvarkymo operacijos priemonių

[41] Žr. 74 konstatuojamąją dalį, kurioje nurodomas reikalavimas duomenų valdytojams įrodyti taikomų priemonių veiksmingumą.

nustatymo procesas, valdymas ir techninės bei organizacinės priemonės, kuriomis įgyvendinami duomenų apsaugos principai. Duomenų apsaugos sertifikavimo kriterijus nustato sertifikavimo įstaigos arba sertifikavimo schemos savininkai ir vėliau patvirtina kompetentinga priežiūros institucija arba Europos duomenų apsaugos valdyba. Daugiau informacijos apie sertifikavimo mechanizmus skaitytojai ras Europos duomenų apsaugos valdybos gairėse dėl sertifikavimo[42] ir kitose susijusiose gairėse, paskelbtose Europos duomenų apsaugos valdybos svetainėje.

91. Net ir tada, kai duomenų tvarkymo operacija sertifikuota pagal 42 straipsnį, duomenų valdytojas tebeturi atsakomybę nuolat stebėti, kaip laikomasi 25 straipsnyje nustatytų PSDA kriterijų, ir siekti, kad jų būtų laikomasi geriau.

5 25 STRAIPSNIO VYKDYMO UŽTIKRINIMAS IR PASEKMĖS

92. Pagal 58 straipsnyje išvardytas procedūras priežiūros institucijos gali įvertinti, ar laikomasi 25 straipsnio. Įgaliojimai imtis taisomųjų veiksmų yra nurodyti 58 straipsnio 2 dalyje ir apima įspėjimus, papeikimus, nurodymus patenkinti duomenų subjekto prašymus pasinaudoti savo teisėmis, duomenų tvarkymo apribojimus ar draudimą, administracines baudas ir pan.

93. PSDA yra dar vienas veiksnys nustatant piniginių sankcijų už BDAR pažeidimus dydį (žr. 83 straipsnio 4 dalį)[43][44].

6 REKOMENDACIJOS

94. Nors 25 straipsnyje duomenų valdytojai ir duomenų tvarkytojai nėra tiesiogiai minimi, pripažįstama, kad būtent jie yra pagrindiniai PSDA taikytojai, todėl jie turėtų žinoti, kad duomenų valdytojams taikomas reikalavimas tvarkyti asmens duomenis naudojant tik tokias sistemas ir technologijas, kuriose įdiegti duomenų apsaugos elementai.

95. Tvarkydami duomenis duomenų valdytojų vardu arba teikdami sprendimus duomenų valdytojams, duomenų tvarkytojai ir gamintojai turėtų naudotis savo praktine patirtimi, kad stiprintų klientų, įskaitant MVĮ, pasitikėjimą ir teiktų jiems rekomendacijas rengiant / perkant sprendimus, kuriais duomenų apsauga įtraukiama į duomenų tvarkymą. Tai taip pat reiškia, kad kuriant produktus ir paslaugas turėtų būti siekiama padėti duomenų valdytojui tenkinti savo poreikius.

96. Įgyvendinant 25 straipsnį reikėtų atsižvelgti į tai, kad pagrindinis priemonių rengimo tikslas yra *veiksmingas* principų *įgyvendinimas* ir duomenų subjektų teisių *apsauga*, taikant tinkamas duomenų tvarkymo priemones. Siekdami sudaryti palankesnes sąlygas nustatyti PSDA ir sustiprinti šios prievolės vykdymą, duomenų valdytojams, gamintojams ir duomenų tvarkytojams teikiame šias rekomendacijas:

---

[42] Europos duomenų apsaugos valdybos Sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento 42 ir 43 straipsnius gairės Nr. 1/2018, 3.0 versija, 2019 m. birželio 4 d., https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_lt.pdf.

[43] BDAR 83 straipsnio 2 dalies d punkte nustatyta, kad nustatant baudas už BDAR pažeidimą „deramai atsižvelgiama“ į „duomenų valdytojo arba duomenų tvarkytojo atsakomybės dydį, atsižvelgiant į jų pagal 25 ir 32 straipsnius įgyvendintas technines ir organizacines priemones“.

[44] Daugiau informacijos apie baudas pateikta 29 straipsnio darbo grupės Gairėse dėl administracinių baudų taikymo ir nustatymo, taikant Reglamentą 2016/679. WP 253, 2017 m. spalio 3 d. ec.europa.eu/newsroom/document.cfm?doc_id=47889 – patvirtinta Europos duomenų apsaugos valdybos.

- Duomenų valdytojai turėtų galvoti apie duomenų apsaugą jau *pradiniuose* duomenų tvarkymo operacijos planavimo *etapuose*, net prieš nustatydami duomenų tvarkymo būdus.
- Jei duomenų valdytojas yra paskyręs duomenų apsaugos pareigūną, Europos duomenų apsaugos valdyba ragina pasirūpinti, kad duomenų apsaugos pareigūnas aktyviai dalyvautų įtraukiant PSDA reikalavimus į viešųjų pirkimų ir kūrimo procedūras, taip pat visame duomenų tvarkymo cikle.
- Duomenų tvarkymo operacija gali būti *sertifikuojama*. Galimybė gauti duomenų tvarkymo operacijos sertifikatą duomenų valdytojui reiškia galimybę gauti pridėtinę vertę, kai jis renkasi iš gamintojų ar duomenų tvarkytojų siūlomos įvairios duomenų tvarkymo programinės įrangos, aparatinės įrangos, paslaugų ir (arba) sistemų. Todėl gamintojai turėtų siekti įrodyti, kad jų siūlomame duomenų tvarkymo sprendimo kūrimo cikle laikomasi PSDA reikalavimų. Sertifikavimo ženklas taip pat gali padėti duomenų subjektams renkantis iš skirtingų prekių ir paslaugų. Galimybė gauti duomenų tvarkymo sertifikatą gali suteikti konkurencinį pranašumą gamintojams, duomenų tvarkytojams ir duomenų valdytojams ir netgi padidinti duomenų subjektų pasitikėjimą tuo, kaip tvarkomi jų asmens duomenys. Jei sertifikavimo galimybės nėra, duomenų valdytojai turėtų siekti gauti kitas *garantijas*, kad gamintojai ar duomenų tvarkytojai laikosi PSDA reikalavimų.
- Duomenų valdytojai, duomenų tvarkytojai ir gamintojai turėtų atsižvelgti į jiems nustatytas prievoles suteikti vaikams iki 18 metų ir kitoms pažeidžiamoms grupėms specialią apsaugą pagal PSDA reikalavimus.
- Gamintojai ir duomenų tvarkytojai turėtų siekti sudaryti palankesnes sąlygas įgyvendinti PSDA, kad padėtų duomenų valdytojui laikytis 25 straipsnyje nustatytų prievolių. Kita vertus, duomenų valdytojai neturėtų rinktis gamintojų ar duomenų tvarkytojų, jei jie nesiūlo sistemų, kuriomis naudojantis duomenų valdytojui suteikiama galimybė arba padedama laikytis 25 straipsnio nuostatų, nes duomenų valdytojams teks atsakomybė už nepakankamą jų įgyvendinimą.
- Gamintojai ir duomenų tvarkytojai turėtų atlikti aktyvų vaidmenį užtikrinant, kad laikomasi „techninių galimybių išsivystymo lygio“ kriterijų, ir pranešti duomenų valdytojams apie bet kokius „techninių galimybių išsivystymo lygio“ pakeitimus, kuriais gali būti paveiktas jų taikomų priemonių veiksmingumas. Duomenų valdytojai turėtų įtraukti šį reikalavimą į sutartis, siekdami užtikrinti, kad jie būtų nuolat informuojami.
- Europos duomenų apsaugos valdyba rekomenduoja duomenų valdytojams reikalauti iš gamintojų ir duomenų tvarkytojų įrodyti, kaip jų siūloma aparatine įranga, programine įranga, paslaugomis ar sistemomis suteikiama galimybė duomenų valdytojui laikytis atskaitomybės reikalavimų pagal PSDA, pvz., naudojant pagrindinius veiklos rezultatų rodiklius įrodyti priemonių ir apsaugos priemonių veiksmingumą įgyvendinant principus ir teises.
- Europos duomenų apsaugos valdyba pabrėžia, kad reikia suderinto požiūrio siekiant veiksmingai įgyvendinti principus ir teises, taip pat ragina pagal 40 straipsnį elgesio kodeksus rengiančias asociacijas ar įstaigas į juos įtraukti ir konkretiems sektoriams skirtas gaires dėl PSDA.
- Duomenų valdytojai turėtų būti sąžiningi duomenų subjektams ir skaidriai nurodyti, kaip jie vertina ir įrodo veiksmingą PSDA įgyvendinimą, tokiu pat būdu kaip duomenų valdytojai įrodo, kad laikosi BDAR pagal atskaitomybės principą.
- Privatumo didinimo technologijos, kurių parengtumas yra techninių galimybių išsivystymo lygio, gali būti naudojamos kaip priemonė pagal PSDA reikalavimus, jei tinkama taikant rizika

grindžiamą metodą. Naudojant privatumo didinimo technologijas nebūtinai įvykdomos 25 straipsnyje nustatytos prievolės. Duomenų valdytojai įvertina, ar naudojant priemonę galima tinkamai ir veiksmingai įgyvendinti duomenų apsaugos principus ir duomenų subjektų teises.

- Naudojant veikiančias ankstesnes sistemas taikomos tos pačios PSDA prievolės kaip ir naudojant naujas sistemas. Jei ankstesnės sistemos kol kas neatitinka PSDA reikalavimų ir negalima atlikti pakeitimų, kad būtų laikomasi tų prievolių, tai naudojant ankstesnę sistemą tiesiog nėra laikomasi BDAR prievolių ir ji negali būti naudojama asmens duomenims tvarkyti.
- 25 straipsnyje nėra numatyta žemesnė reikalavimų riba MVĮ atveju. Laikytis 25 straipsnio nuostatų MVĮ gali padėti šie aspektai:
    - anksti atlikti rizikos vertinimus;
    - iš pradžių duomenis tvarkyti nedidele apimtimi, o vėliau padidinti apimtį ir sudėtingumą;
    - ieškoti gamintojų ir duomenų tvarkytojų, kurie suteikia garantijas, kad laikomasi PSDA reikalavimų, pvz., turi sertifikatus ir laikosi elgesio kodekso;
    - pasitelkti gerų rezultatų pasiekusius partnerius;
    - bendrauti su duomenų apsaugos institucijomis;
    - susipažinti su duomenų apsaugos institucijų ir Europos duomenų apsaugos valdybos paskelbtomis gairėmis;
    - laikytis elgesio kodeksų, jei jie yra;
    - siekti gauti profesionalią pagalbą ir rekomendacijas.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

(Andrea Jelinek)