Gairės

Sertifikavimo ir sertifikavimo kriterijų nustatymo pagal Reglamento 42 ir 43 straipsnius gairės Nr. 1/2018

3.0 versija

2019 m. birželio 4 d.

Priimta

Informacija apie versijas

3.0 versija	2019 m. birželio 4 d.	2 priedo įtraukimas (2 priedo 2.0 versija priimta 2019 m. birželio 4 d. po viešų konsultacijų)
2.1 versija	2019 m. balandžio 9 d.	Gairių klaidų ištaisymo priėmimas (45 punktas)
2.0 versija	2019 m. sausio 23 d.	Gairių priėmimas po viešų konsultacijų. Tą pačią dieną priimtas viešoms konsultacijoms skirtas 2 priedas (1.0 versija)
1.0 versija	2018 m. gegužės 25 d.	Gairių, dėl kurių rengiamasi skelbti konsultacijas, priėmimas

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 2018 m. gegužės 25 d. Darbo tvarkos taisyklių 12 ir 22 straipsnius,

atsižvelgdama į pagal BDAR 70 straipsnio 4 dalį 2018 m. gegužės 30 d. – 2018 m. liepos 12 d. vykusių viešų konsultacijų dėl gairių ir 2019 m. vasario 15 d. – 2019 m. kovo 29 d. vykusių viešų konsultacijų dėl 2 priedo rezultatus,

PRIĖMĖ ŠIAS GAIRES:

1 ĮVADAS

1. Bendrajame duomenų apsaugos reglamente (toliau – Reglamentas (ES) 2016/279, BDAR arba Reglamentas) nustatoma modernizuota, atskaitomybe ir pagrindinėmis teisėmis pagrįsta Europos duomenų apsaugos reikalavimų laikymosi sistema. Įvairios priemonės, kuriomis sudaromos geresnės sąlygos laikytis BDAR nuostatų, yra itin svarbūs šios naujos sistemos elementai. Tai, be kita ko, – konkrečiomis aplinkybėmis taikomi privalomi reikalavimai (įskaitant duomenų apsaugos pareigūnų skyrimą ir poveikio duomenų apsaugai vertinimų atlikimą) ir savanoriškos priemonės, pvz., elgesio kodeksai ir sertifikavimo mechanizmai.
2. Iki BDAR priėmimo 29 straipsnio darbo grupė nustatė, kad sertifikavimas galėtų atlikti svarbų vaidmenį atskaitomybės už duomenų apsaugą sistemoje1. Siekiant, kad sertifikavimas suteiktų aiškių įrodymų, jog laikomasi duomenų apsaugos, turėtų galioti aiškios taisyklės, kuriose būtų nustatyti sertifikavimo reikalavimai2. BDAR 42 straipsnyje numatytas teisinis pagrindas tokioms taisyklėms parengti.
3. BDAR 42 straipsnio 1 dalyje nurodyta:

   „Valstybės narės, priežiūros institucijos, [Europos duomenų apsaugos] Valdyba ir Komisija skatina nustatyti – visų pirma Sąjungos lygmeniu – duomenų apsaugos sertifikavimo mechanizmus ir duomenų apsaugos ženklus bei žymenis, kad būtų galima įrodyti, jog duomenų valdytojai ir duomenų tvarkytojai, vykdydami duomenų tvarkymo operacijas, laikosi šio reglamento. Atsižvelgiama į konkrečius labai mažų, mažųjų ir vidutinių įmonių poreikius.“

[1] 29 straipsnio darbo grupės nuomonė Nr. 3/2010 dėl atskaitomybės principo, WP173, 2010 m. liepos 13 d., 69–71 punktai.
[2] 29 straipsnio darbo grupės nuomonė Nr. 3/2010 dėl atskaitomybės principo (WP173), 69 punktas.

4. Sertifikavimo mechanizmai3 gali pagerinti skaidrumą ne tik duomenų subjektams, tačiau ir verslo verslui santykiams, pavyzdžiui, duomenų valdytojų ir duomenų tvarkytojų, tarpusavio santykiuose. BDAR 100 konstatuojamojoje dalyje teigiama, kad nustačius sertifikavimo mechanizmus galėtų padidėti skaidrumas, šio reglamento būtų geriau laikomasi, o duomenų subjektai galėtų įvertinti konkretaus produkto ar paslaugos duomenų apsaugos lygį4.

5. BDAR nenustatoma duomenų valdytojų ir duomenų tvarkytojų teisė į sertifikavimą ar sertifikavimo prievolė; pagal 42 straipsnio 3 dalį sertifikavimas yra savanoriškas procesas, skirtas padėti įrodyti, kad yra laikomasi BDAR. Valstybės narės ir priežiūros institucijos raginamos skatinti nustatyti sertifikavimo mechanizmus, jos nustatys suinteresuotųjų subjektų dalyvavimą sertifikavimo procese ir naudojimo cikle.

6. Be to, patvirtintų sertifikavimo mechanizmų laikymasis yra vienas iš veiksnių, į kuriuos priežiūros institucijos turi atsižvelgti kaip į sunkinančias arba lengvinančias aplinkybes spręsdamos, ar skirti administracinę baudą ir kokį baudos dydį nustatyti (83 straipsnio 2 dalies j punktas)5.

1.1 Gairių taikymo sritis

7. Šių gairių taikymo sritis yra ribota; jos nėra pagal BDAR vykdomo sertifikavimo procedūrinis vadovas. Šiomis gairėmis visų pirma siekiama nustatyti bendruosius reikalavimus ir kriterijus, kurie gali tikti visų rūšių sertifikavimo mechanizmams, nustatytiems pagal BDAR 42 ir 43 straipsnius. Šiuo tikslu gairėse:

    - išnagrinėjamas sertifikavimo, kaip atskaitomybės priemonės, loginis pagrindas;
    - išaiškinamos svarbiausios 42 ir 43 straipsniuose išdėstytos sertifikavimo nuostatų sąvokos ir
    - išaiškinama sritis, ką galima sertifikuoti pagal 42 ir 43 straipsnius, ir sertifikavimo tikslas;
    - padedama pasiekti, kad sertifikavimo rezultatas būtų prasmingas, vienareikšmiškas, kuo atkuriamesnis ir palyginamas, neatsižvelgiant į sertifikuojantį subjektą (palyginamumas).

8. BDAR numatyti keli būdai, kaip valstybės narės ir priežiūros institucijos gali įgyvendinti 42 ir 43 straipsnius. Gairėse pateikiama patarimų, kaip aiškinti ir įgyvendinti 42 ir 43 straipsnių nuostatas, gairės valstybėms narėms, priežiūros institucijoms ir nacionalinėms akreditavimo įstaigoms padės suformuoti nuoseklesnį, suderintą pagal BDAR vykdomo sertifikavimo mechanizmų įgyvendinimo metodą.

[3] Šiose gairėse sertifikavimo mechanizmai ir duomenų apsaugos ženklai bei žymenys kartu bus vadinami sertifikavimo mechanizmais. Žr. 1.3.2 punktą.
[4] 100 konstatuojamojoje dalyje teigiama, kad kurti sertifikavimo mechanizmus turėtų būti skatinama „siekiant didesnio skaidrumo ir geresnio šio reglamento laikymosi, <...> kad duomenų subjektai galėtų greitai įvertinti konkretaus produkto ar paslaugos duomenų apsaugos lygį“.
[5] Žr. 29 straipsnio darbo grupės Administracinių baudų taikymo ir nustatymo pagal Reglamentą (ES) 2016/679 gaires (WP 253).

9. Gairėse išdėstyti patarimai bus aktualūs:

    - kompetentingoms priežiūros institucijoms ir Europos duomenų apsaugos valdybai, kai jos tvirtins sertifikavimo kriterijus pagal 42 straipsnio 5 dalį, 58 straipsnio 3 dalies f punktą ir 70 straipsnio 1 dalies o punktą;
    - sertifikavimo įstaigoms, kai jos rengs ir peržiūrės sertifikavimo kriterijus, prieš teikdamos juos kompetentingai priežiūros institucijai tvirtinti pagal 42 straipsnio 5 dalį;
    - Europos duomenų apsaugos valdybai, kai ji pagal 42 straipsnio 5 dalį ir 70 straipsnio 1 dalies o punktą tvirtins Europos duomenų apsaugos ženklą;
    - priežiūros institucijoms, kai jos rengs savo sertifikavimo kriterijus;
    - Europos Komisijai, kuriai suteikiami įgaliojimai priimti deleguotuosius aktus siekiant nustatyti reikalavimus, į kuriuos pagal 43 straipsnio 8 dalį turi būti atsižvelgta duomenų apsaugos sertifikavimo mechanizmuose;
    - Europos duomenų apsaugos valdybai, kai ji teiks Europos Komisijai nuomonę dėl sertifikavimo reikalavimų pagal 70 straipsnio 1 dalies q punktą ir 43 straipsnio 8 dalį;
    - nacionalinėms akreditavimo įstaigoms, kurios turės atsižvelgti į sertifikavimo kriterijus siekdamos akredituoti sertifikavimo įstaigas pagal EN-ISO/IEC 17065/2012 ir papildomus reikalavimus, kaip nurodyta 43 straipsnyje, ir
    - duomenų valdytojams ir duomenų tvarkytojams, kai jie apibrėš savo BDAR vykdymo strategiją ir svarstys sertifikavimą kaip priemonę BDAR laikymuisi įrodyti.

10. Europos duomenų apsaugos valdyba paskelbs atskiras gaires, kaip nustatyti kriterijus, pagal kuriuos bus tvirtinama, kad sertifikavimo mechanizmai yra tinkami duomenims perduoti į trečiąsias valstybes arba tarptautinėms organizacijoms pagal 42 straipsnio 2 dalį.

1.2 Sertifikavimo pagal BDAR tikslas

11. 42 straipsnio 1 dalyje numatyta, kad sertifikavimo mechanizmai nustatomi, „kad būtų galima įrodyti, jog duomenų valdytojai ir duomenų tvarkytojai, vykdydami duomenų tvarkymo operacijas, laikosi šio reglamento“.

12. BDAR numatytos pavyzdinės aplinkybės, kuriomis patvirtinti sertifikavimo mechanizmai gali būti naudojami kaip vienas iš elementų, kuriais įrodoma, kaip duomenų valdytojai ir duomenų tvarkytojai laikosi prievolių, susijusių su:

    - tinkamų techninių ir organizacinių priemonių įgyvendinimu ir įrodymu, kaip nurodyta 24 straipsnio 1 ir 3 dalyse, 25 straipsnyje ir 32 straipsnio 1 ir 3 dalyse;
    - pakankamomis duomenų tvarkytojo garantijomis duomenų valdytojui, kaip nurodyta 28 straipsnio 1 dalyje, ir pakankamomis kito duomenų tvarkytojo garantijomis pirminiam duomenų tvarkytojui, kaip nurodyta 28 straipsnio 4 dalyje.

13. Kadangi pats sertifikavimas reikalavimų laikymosi neįrodo, o tiesiog yra vienas iš elementų, kuriuo naudojantis galima įrodyti reikalavimų laikymąsi, jis turėtų būti parengtas skaidriai.

Reikalavimų laikymuisi įrodyti reikalingi patvirtinamieji dokumentai, konkrečiai – rašytinės ataskaitos, kuriose ne tik pakartojama, bet ir aprašoma, kaip įvykdomi kriterijai, o jeigu jie iš pradžių nėra įvykdyti, tai aprašomos korekcijos ir taisomieji veiksmai bei jų tikslingumas, taip nurodant motyvus sertifikavimui suteikti ir išlaikyti. Tai apima bendrais bruožais išdėstytą konkretų sprendimą išduoti, atnaujinti arba atšaukti sertifikatą. Jame turėtų būti nurodytos kriterijų taikymo priežastys, argumentai ir juos taikant gauti įrodymai, taip pat pagal sertifikavimo metu surinktus faktus arba prielaidas padarytos išvados bei priimti sprendimai.

1.3 Pagrindinės sąvokos

14. Tolesniame skirsnyje nagrinėjamos 42 ir 43 straipsniuose išdėstytos pagrindinės sąvokos. Ši analizė padeda susidaryti vaizdą apie pagal BDAR vykdomo sertifikavimo pagrindines sąlygas ir sritį.

1.3.1 Sąvokos „sertifikavimas“ aiškinimas

15. BDAR sąvoka „sertifikavimas“ neapibrėžiama. Tarptautinė standartizacijos organizacija (ISO) pateikia universalią sertifikavimo apibrėžtį: tai – „nepriklausomos įstaigos suteiktas rašytinis patikinimas (sertifikatas), kad atitinkamas gaminys, paslauga ar sistema atitinka konkrečius reikalavimus“. Sertifikavimas taip pat žinomas kaip „trečiosios šalies atliekamas atitikties vertinimas“, o sertifikavimo įstaigos taip pat gali būti vadinamos „atitikties vertinimo įstaigomis“. Pagal EN-ISO/IEC 17000:2004 - Atitikties vertinimas -- Žodynas ir bendrieji principai (nurodomi pagal ISO17065) – sertifikavimas apibrėžiamas taip: „produktų, procesų, sistemų ir paslaugų atestavimas, kurį atlieka trečioji šalis“.

16. Atestavimas yra „patvirtinimas, pagrįstas atlikta vertinamąja analize, kad nustatytų reikalavimų įvykdymas įrodytas“ (ISO 17000:2004 5.2 skirsnis).

17. Kalbant apie sertifikavimą pagal BDAR 42 ir 43 straipsnius, sertifikavimas reiškia trečiosios šalies atliekamą atestavimą, susijusį su duomenų valdytojų ir duomenų tvarkytojų atliekamomis duomenų tvarkymo operacijomis.

1.3.2 Sertifikavimo mechanizmai, ženklai ir žymenys

18. BDAR neapibrėžiami sertifikavimo mechanizmai, ženklai ar žymenys, šios sąvokos vartojamos bendrai. Sertifikatas yra atitikties pareiškimas. Ženklas arba žymuo gali būti naudojami siekiant pažymėti sėkmingą sertifikavimo procedūros užbaigimą. Ženklu arba žymeniu paprastai vadinamas logotipas arba simbolis, kurio buvimas (kartu su sertifikatu) rodo, jog sertifikavimo objektas buvo nepriklausomai įvertintas atliekant sertifikavimo procedūrą ir atitinka nurodytus reikalavimus, išdėstytus norminiuose dokumentuose, pvz., reglamentuose, standartuose arba techninėse specifikacijose. Šie sertifikavimo pagal BDAR reikalavimai išdėstyti kaip papildomi reikalavimai, pridėti prie EN-ISO/IEC 17065/2012 pateiktų sertifikavimo įstaigų akreditavimo taisyklių ir kompetentingos priežiūros institucijos arba Valdybos patvirtintų sertifikavimo

kriterijų. Sertifikatas, ženklas arba žymuo pagal BDAR gali būti išduotas tik tada, kai akredituota sertifikavimo įstaiga arba kompetentinga priežiūros institucija atlieka nepriklausomą įrodymų vertinimą, nurodydama, kad sertifikavimo kriterijai yra įvykdyti.

19. Lentelėje pateiktas bendro pobūdžio sertifikavimo proceso pavyzdys.

Duomenų valdytojo arba duomenų tvarkytojo paraiškos teikimas	**Sertifikavimo įstaigos atliekama oficiali patikra**	**Vertinimas Pirminis vertinimas**	**Vertinimas Vertinimo objekto vertinimas**	**Vertinimas Rezultatų patvirtinimas**	**Kompetentingos priežiūros institucijos informavimas**	**Sertifikavimas**	**Stebėsena**	**Sertifikato atnaujinimas**
Ar vertinimo objekto aprašas yra vienareikšmis ir išsamus, įskaitant sąsajas?	Ar vertinimo objekto aprašas gali būti priimtas?	Kokie kriterijai taikytini?	Ar vertinimo objektas atitinka kriterijus?	Ar visi nurodyti aktualūs kriterijai atspindi vertinimo objektą?	Ar nurodytos priežastys, kodėl sertifikavimas suteiktas arba panaikintas?	Ar sertifikatas gali būti suteiktas?	Ar vertinimo objektas ir toliau atitinka kriterijus?	Ar duomenų tvarkymas ir toliau atitinka sertifikavimo kriterijus?
Ar gali būti suteikta galimybė susipažinti su vertinimo objekto duomenų tvarkymo veikla?	Ar visi dokumentai išsamūs ir juose pateikiama naujausia informacija?	Kokie vertinimo metodai taikytini?	Ar vertinimo objekto dokumentai tinkami?	Ar vertinimas pakankamai dokumentuotas?		Ar ataskaitos parengtos paskelbti?	Ar sertifikatas / ženklas / pasitikėjimo ženklas naudojamas tinkamai?	Ar skirta pakankamai dėmesio tobulintinoms sritims?
42 straipsnio 6 dalis	43 straipsnio 4 dalis	43 straipsnio 4 dalis	42 straipsnio 5 dalis, 43 straipsnio 4 dalis	43 straipsnio 4 dalis	43 straipsnio 1 dalis, 43 straipsnio 5 dalis	43 straipsnio 1 dalis 42 straipsnio 7 dalis	42 straipsnio 7 dalis	42 straipsnio 7 dalis

2 PRIEŽIŪROS INSTITUCIJŲ VAIDMUO

20. 42 straipsnio 5 dalyje numatyta, kad sertifikatą išduoda akredituota sertifikavimo įstaiga arba kompetentinga priežiūros institucija. Pagal BDAR sertifikatų išdavimas nėra privaloma priežiūros institucijų užduotis. Vietoj to BDAR numatyti keli skirtingi modeliai. Pavyzdžiui, priežiūros institucija gali nuspręsti pasinaudoti viena arba keliomis toliau nurodytomis galimybėmis:

- pati išduoti sertifikatą, taikydama savo sertifikavimo schemą;
- pati išduoti sertifikatą, taikydama savo sertifikavimo schemą, tačiau visą vertinimo procesą arba jo dalį perduoti trečiosioms šalims;
- sukurti savo sertifikavimo schemą ir pavesti sertifikavimo procedūrą atlikti sertifikavimo įstaigoms, kurios išduoda sertifikatus, ir
- skatinti rinkos dalyvius parengti sertifikavimo mechanizmus.

21. Priežiūros institucija taip pat turės apsvarstyti savo vaidmenį atsižvelgdama į nacionaliniu lygmeniu priimtus sprendimus dėl akreditavimo mechanizmų, ypač jeigu pati priežiūros institucija pagal BDAR 43 straipsnio 1 dalį yra įgaliota akredituoti sertifikavimo įstaigas. Taigi, kiekviena priežiūros institucija nustatys, kokį metodą taikyti siekiant įgyvendinti plataus pobūdžio ketinimą atlikti sertifikavimą pagal BDAR. Tai bus nustatoma ne tik atsižvelgiant į 57 ir 58 straipsniuose numatytas užduotis ir įgaliojimus, bet ir sertifikavimą numatant kaip vieną iš veiksnių, į kuriuos atsižvelgiama skiriant administracines baudas, taip pat apskritai sertifikavimą laikant viena iš atitikties įrodymo priemonių.

2.1 Priežiūros institucija kaip sertifikavimo įstaiga

22. Jeigu priežiūros institucija nusprendžia atlikti sertifikavimą, ji turės atidžiai įvertinti savo vaidmenį, susijusį su pagal BDAR jai paskirtomis užduotimis. Jos vaidmuo vykdant savo funkcijas turėtų būti skaidrus. Priežiūros institucija, atlikdama tyrimus ir vykdymo veiksmus, turės konkrečiai atsižvelgti į galių atskyrimo principą, kad išvengtų galimų interesų konfliktų.

23. Jeigu priežiūros institucija veikia kaip sertifikavimo įstaiga, ji turės užtikrinti, kad būtų tinkamai sudarytas sertifikavimo mechanizmas, ir parengti savo sertifikavimo kriterijus arba patvirtinti kitus sertifikavimo kriterijus. Be to, kiekviena sertifikatus išduodanti priežiūros institucija privalo periodiškai atlikti jų peržiūrą (57 straipsnio 1 dalies o punktas) ir turi įgaliojimus juos atšaukti, kai nevykdomi arba nebevykdomi sertifikavimo reikalavimai (58 straipsnio 2 dalies h punktas). Siekiant įvykdyti šiuos reikalavimus, naudinga parengti sertifikavimo procedūrą ir proceso reikalavimus, taip pat, jeigu, pvz., nacionalinėje teisėje nenurodyta kitaip, patvirtinti teisiškai vykdytiną susitarimą su konkrečia paraišką pateikusia organizacija dėl sertifikavimo veiklos vykdymo. Turėtų būti užtikrinta, kad šiame sertifikavimo susitarime būtų reikalaujama, kad pareiškėjas bent jau atitiktų sertifikavimo kriterijus, t. y. būtų sudaręs reikalingas sąlygas atlikti vertinimus, vykdytų kriterijų laikymosi stebėseną ir atliktų periodinę peržiūrą, įskaitant galimybę gauti informaciją ir (arba) patekti į patalpas, dokumentuotų ir skelbtų ataskaitas ir rezultatus bei nagrinėtų skundus. Be to, tikimasi, kad priežiūros institucija vadovausis ne tik 43 straipsnio 2 dalyje nustatytais reikalavimais, bet ir sertifikavimo įstaigų akreditavimo gairių reikalavimais.

2.2 Priežiūros institucijos papildomos užduotys, susijusios su sertifikavimu

24. Valstybėse narėse, kuriose pradeda veikti sertifikavimo įstaigos, priežiūros institucija, nepriklausomai nuo jos pačios veiklos, turi įgaliojimus ir užduotį:

    - įvertinti sertifikavimo schemos kriterijus ir parengti sprendimo projektą (42 straipsnio 5 dalis);
    - perduoti Valdybai sprendimo projektą, kai ji ketina patvirtinti sertifikavimo kriterijus (64 straipsnio 1 dalies c punktas, 64 straipsnio 7 dalis) ir atsižvelgti į Valdybos nuomonę (64 straipsnio 1 dalies c punktas ir 70 straipsnio 1 dalies t punktas);
    - patvirtinti sertifikavimo kriterijus (58 straipsnio 3 dalies f punktas), kol nepradėta vykdyti akreditavimo ir sertifikavimo veikla (42 straipsnio 5 dalis ir 43 straipsnio 2 dalies b punktas);

- paskelbti sertifikavimo kriterijus (43 straipsnio 6 dalis);
- veikti kaip kompetentinga institucija vykdant ES masto sertifikavimo schemas, pagal kurias gali būti išduoti Europos duomenų apsaugos valdybos patvirtinti Europos duomenų apsaugos ženklai (42 straipsnio 5 dalis ir 70 straipsnio 1 dalies o punktas), ir
- nurodyti sertifikavimo įstaigai a) neišduoti sertifikato arba b) atšaukti sertifikatą, kai nevykdomi arba nebevykdomi sertifikavimo reikalavimai (sertifikavimo procedūros ar kriterijai) (58 straipsnio 2 dalies h punktas).

25. BDAR priežiūros institucijai pavedama tvirtinti sertifikavimo kriterijus, tačiau nepavedama jų parengti. Siekdama pagal 42 straipsnio 5 dalį patvirtinti sertifikavimo kriterijus, priežiūros institucija turėtų aiškiai suprasti, kokios BDAR atitikties įrodymų apimties ir turinio tikėtis ir kaip atlikti savo užduotį stebėti ir užtikrinti Reglamento taikymą. Priede pateikiamos gairės, kaip, siekiant patvirtinti kriterijus, juos įvertinti taikant suderintą metodą.

26. 43 straipsnio 1 dalyje reikalaujama, kad sertifikavimo įstaigos, prieš išduodamos ar atnaujindamos sertifikatus, informuotų savo priežiūros instituciją, taip sudarydamos kompetentingai priežiūros institucijai sąlygas pagal 58 straipsnio 2 dalies h punktą įvykdyti savo įgaliojimus imtis taisomųjų veiksmų. Be to, 43 straipsnio 5 dalyje taip pat reikalaujama, kad sertifikavimo įstaigos kompetentingoms priežiūros institucijoms nurodytų priežastis, kodėl prašomas sertifikavimas buvo suteiktas arba panaikintas. Nors BDAR numatyta, kad priežiūros institucijos gali nustatyti, kaip veiklos lygmeniu gauti, pripažinti, peržiūrėti ir tvarkyti šią informaciją (pavyzdžiui, tai galėtų apimti technologinius sprendimus, kuriais sudaromos sąlygos sertifikavimo įstaigoms teikti ataskaitas), gali būti nustatytas procesas ir kriterijai, kaip tvarkyti informaciją ir ataskaitas, kurias sertifikavimo įstaiga pateikia dėl kiekvieno sėkmingo sertifikavimo projekto pagal 43 straipsnio 1 dalį. Remdamasi šia informacija, priežiūros institucija gali įvykdyti savo įgaliojimus nurodyti sertifikavimo įstaigai atšaukti sertifikatą arba jo neišduoti (58 straipsnio 2 dalies h punktas) ir stebėti bei užtikrinti reikalavimų ir sertifikavimo kriterijų taikymą pagal BDAR (57 straipsnio 1 dalies a punktas ir 58 straipsnio 2 dalies h punktas). Tai padės taikyti suderintą metodą ir užtikrinti, kad skirtingų sertifikavimo įstaigų sertifikatus būtų galima palyginti ir kad priežiūros institucijos žinotų organizacijos sertifikavimo būklę.

3 SERTIFIKAVIMO ĮSTAIGOS VAIDMUO

27. Sertifikavimo įstaigos vaidmuo yra taikant sertifikavimo mechanizmą ir patvirtintus kriterijus (43 straipsnio 1 dalis) išduoti, peržiūrėti, atnaujinti ir atšaukti sertifikatus (42 straipsnio 5 ir 7 dalys). Šiuo tikslu reikia, kad sertifikavimo įstaiga arba sertifikavimo schemos savininkas nustatytų ir sudarytų sertifikavimo kriterijus ir sertifikavimo procedūras, įskaitant reikalavimų laikymosi stebėsenos, peržiūros, skundų nagrinėjimo ir sertifikatų atšaukimo procedūras. Sertifikavimo kriterijai peržiūrimi atliekant akreditavimo procesą, kai apsvarstomos taisyklės ir procedūros, kurias taikant išduodami sertifikatai, ženklai arba žymenys (43 straipsnio 2 dalies c punktas).

28. Sertifikavimo mechanizmo ir sertifikavimo kriterijų buvimas yra reikalingi sertifikavimo įstaigai, kad ji pagal 43 straipsnį būtų akredituota. Labai svarbus poveikis sertifikavimo įstaigos veiklai priklauso nuo sertifikavimo kriterijų taikymo srities ir pobūdžio – šie kriterijai turi poveikį sertifikavimo procedūroms, o pastarosios turi poveikį kriterijams. Taikant konkrečius kriterijus, pavyzdžiui, gali prireikti konkrečių vertinimo metodų, tokių kaip patikrinimai vietoje ir kodeksų peržiūra. Tai yra privalomos akreditavimo procedūros, išsamiau paaiškintos akreditavimo gairėse.

29. Pagal BDAR sertifikavimo įstaiga privalo priežiūros institucijoms suteikti informaciją, ypač apie konkrečius sertifikatus, – tokios informacijos reikia siekiant stebėti, kaip taikomas sertifikavimo mechanizmas (42 straipsnio 7 dalis, 43 straipsnio 5 dalis, 58 straipsnio 2 dalies h punktas).

4 SERTIFIKAVIMO KRITERIJŲ TVIRTINIMAS

30. Sertifikavimo kriterijai yra sudedamoji bet kurio sertifikavimo mechanizmo dalis. Atitinkamai BDAR reikalaujama, kad sertifikavimo mechanizmo sertifikavimo kriterijus patvirtintų kompetentinga priežiūros institucija (42 straipsnio 5 dalis ir 43 straipsnio 2 dalies b punktas). Europos duomenų apsaugos ženklo atveju sertifikavimo kriterijus tvirtina Europos duomenų apsaugos valdyba (42 straipsnio 5 dalis ir 70 straipsnio 1 dalies o punktas). Toliau paaiškinami abu sertifikavimo kriterijų tvirtinimo būdai.

31. Europos duomenų apsaugos valdyba pripažįsta toliau nurodytus sertifikavimo kriterijų patvirtinimo tikslus:

    - tinkamai atspindėti fizinių asmenų apsaugos tvarkant asmens duomenis reikalavimus ir principus, nustatytus Reglamente (ES) 2016/679, ir
    - padėti nuosekliai taikyti BDAR.

32. Patvirtinimas suteikiamas, jei sertifikavimo kriterijai visapusiškai atitinka BDAR reikalavimą, kad sertifikavimo mechanizmu duomenų valdytojams ir duomenų tvarkytojams būtų sudarytos sąlygos įrodyti atitiktį BDAR.

4.1 Kompetentingos priežiūros institucijos atliekamas kriterijų patvirtinimas

33. Prieš sertifikavimo įstaigos akreditavimo procesą arba jo metu kompetentinga priežiūros institucija turi patvirtinti sertifikavimo kriterijus. Patvirtinti taip pat reikia atnaujintas arba papildomas tos pačios sertifikavimo įstaigos schemas arba kriterijų rinkinius pagal ISO 17065, kol ji dar nenaudoja pakeistų sertifikavimo mechanizmų (42 straipsnio 5 dalis ir 43 straipsnio 2 dalies b punktas). Priežiūros institucijos visus prašymus patvirtinti sertifikavimo kriterijus turi vertinti sąžiningai ir nediskriminuodamos, vadovaudamosi viešai prieinama procedūra, apimančia bendrąsias sąlygas, kurias reikia įvykdyti, ir patvirtinimo proceso aprašymą.

34. Konkrečioje valstybėje narėje sertifikavimo įstaiga gali išduoti sertifikatą tik remdamasi toje valstybėje narėje priežiūros institucijos patvirtintais kriterijais. Kitaip tariant, jeigu sertifikavimo įstaiga siekia teikti sertifikavimo paslaugą ir gauna akreditaciją, kompetentinga

priežiūros institucija turi patvirtinti sertifikavimo kriterijus. Žr. tolesnį skirsnį apie Europos masto sertifikavimo schemas.

4.2 Europos duomenų apsaugos valdybos atliekamas Europos duomenų apsaugos ženklo išdavimo kriterijų tvirtinimas

35. Sertifikavimo įstaiga taip pat gali išduoti sertifikatą remdamasi Europos duomenų apsaugos valdybos patvirtintais kriterijais Europos duomenų apsaugos ženklui gauti. Europos duomenų apsaugos valdybai patvirtinus sertifikavimo kriterijus pagal 63 straipsnį gali būti išduodamas Europos duomenų apsaugos ženklas (42 straipsnio 5 dalis). Atsižvelgdama į galiojančias sertifikavimo ir akreditavimo konvencijas, Europos duomenų apsaugos valdyba pripažįsta, kad pageidautina išvengti duomenų apsaugos sertifikavimo rinkos susiskaidymo. Ji pažymi, jog 42 straipsnio 1 dalyje numatyta, kad valstybės narės, priežiūros institucijos, Valdyba ir Komisija skatina nustatyti – visų pirma Sąjungos lygmeniu – duomenų apsaugos sertifikavimo mechanizmus.

4.2.1 Patvirtinimo paraiška

36. Kriterijų patvirtinimo paraišką Europos duomenų apsaugos valdybai pagal 42 straipsnio 5 dalį ir 70 straipsnio 1 dalies o punktą reikia pateikti per kompetentingą priežiūros instituciją, joje turi būti nurodytas schemos savininko, kandidato ar akredituotos sertifikavimo įstaigos ketinimas pasiūlyti visose valstybėse narėse esantiems duomenų valdytojams ir duomenų tvarkytojams skirto sertifikavimo mechanizmo kriterijus. Jeigu, kompetentingos priežiūros institucijos vertinimu, Europos duomenų apsaugos valdyba galėtų patvirtinti kriterijus, kompetentinga priežiūros institucija Europos duomenų apsaugos valdybai pateiks projektą.

37. Sprendimas, kur pateikti kriterijų patvirtinimo paraišką, bus priimamas pagal sertifikavimo schemos savininkų arba sertifikavimo įstaigų būstinės vietą.

38. Jei sertifikavimo įstaiga teikia paraišką, ji paprastai jau būna kreipusis dėl akreditacijos arba jau yra akredituota savo valstybės narės kompetentingos priežiūros institucijos arba nacionalinės akreditavimo įstaigos. Jeigu sertifikavimo įstaiga jau yra akredituota BDAR sertifikavimo mechanizmui taikyti, tai gali padėti integruoti patvirtinimų procesą.

4.2.2 Europos duomenų apsaugos ženklo kriterijai

39. Europos duomenų apsaugos valdyba koordinuos vertinimo procesą ir, kaip reikalaujama, patvirtins Europos duomenų apsaugos ženklą. Bus vertinamos šios sritys: kriterijų taikymo sritis ir tinkamumas bendro sertifikavimo funkcijai atlikti. Kai Europos duomenų apsaugos valdyba patvirtina kriterijus, už sertifikavimo įstaigos ES būstinę atsakinga kompetentinga priežiūros institucija turėtų nagrinėti skundus dėl paties mechanizmo ir informuoti kitas priežiūros institucijas. Ši priežiūros institucija taip pat yra kompetentinga imtis priemonių

sertifikavimo įstaigos atžvilgiu. Atitinkamais atvejais kompetentinga priežiūros institucija informuos kitas priežiūros institucijas ir Europos duomenų apsaugos valdybą.

40. Bendram sertifikavimui skirti sertifikavimo kriterijai turi atitikti ES masto poreikius ir jais turėtų būti numatytas konkretus mechanizmas šiems poreikiams patenkinti. Europos sertifikavimo mechanizmai turi būti skirti naudoti visose valstybėse narėse. Remiantis 42 straipsnio 5 dalimi, Europos duomenų apsaugos ženklo mechanizmą ir jo kriterijus turi būti įmanoma pritaikyti taip, kad atitinkamais atvejais būtų atsižvelgiama į nacionalines konkrečių sektorių, pvz., duomenų tvarkymo mokyklose, reglamentavimo nuostatas ir turi būti numatytas mechanizmo taikymas Europos mastu.

41. Pavyzdys: tarptautinė mokykla, teikianti mokymo paslaugas duomenų subjektams Sąjungoje, yra įsisteigusi valstybėje narėje „A“. Mokykla pageidauja savo internetinių paraiškų procesą sertifikuoti pagal ES masto sertifikavimo schemą, kad gautų Europos duomenų apsaugos ženklą. Ši mokykla siekia pateikti paraišką sertifikuoti duomenų tvarkymo operacijas, kurias atlieka valstybėje narėje „B“ įsisteigusi sertifikavimo įstaiga, ir atitinkamai gauti Europos duomenų apsaugos ženklą. Nustatant ženklo kriterijus, rengiamus ir dokumentuojamus pagal atitinkamą mechanizmą, turi būti įmanoma atsižvelgti į mokyklų veiklos reglamentavimo nuostatas, taikytinas valstybėje narėje „A“. Pagal minėtus kriterijus taip pat turėtų būti reikalaujama, kad mokyklos internetinių paraiškų procesas teiktų informaciją apie taikytinus valstybės narės duomenų apsaugos reikalavimus, kurie kitose valstybėse narėse gali skirtis, ir šiuos reikalavimus atitiktų. Vienas iš pavyzdžių – asmens duomenų rinkiniai, teikiami paraiškos tikslais, pvz., pažymiai vaikų darželyje arba testų rezultatai, skirtingi duomenų saugojimo laikotarpiai, finansinių ar biometrinių duomenų rinkimas arba tvarkymas, papildomi duomenų tvarkymo apribojimai.

- Aukšto lygio kriterijai Europos duomenų apsaugos ženklo mechanizmui patvirtinti:
  - Valdybos patvirtinti kriterijai;
  - paraiškų teikimas įvairiose jurisdikcijose, atitinkamais atvejais atsižvelgiant į nacionalinius teisinius reikalavimus ir konkrečių sektorių reglamentavimo nuostatas;
  -
- suderinti kriterijai, kuriuos įmanoma pritaikyti prie nacionalinių reikalavimų;
  - sertifikavimo mechanizmo aprašymas;
  - sertifikavimo susitarimai, bendrų Europos reikalavimų pripažinimas;
  - procedūros, kuriomis užtikrinami ir pateikiami nacionalinius skirtumus integruojantys sprendimai ir užtikrinama, kad ženklas padėtų įrodyti atitiktį BDAR, ir
  - visoms susijusioms priežiūros institucijoms aktualių ataskaitų kalba.

42. Priede taip pat išdėstyti patarimai dėl Europos duomenų apsaugos ženklo kriterijų.

4.2.3 Akreditacijos vaidmuo

43. Kaip pažymėta 4.2.1 punkte, kai nustatoma, kad tam tikri kriterijai tinka bendram sertifikavimui ir juos pagal 42 straipsnio 5 dalį atitinkamai patvirtina Valdyba, tada gali būti akredituojamos sertifikavimo įstaigos, kad jos pagal šiuos kriterijus vykdytų sertifikavimą Sąjungos lygmeniu.

44. Schemos, kurias ketinama taikyti tik konkrečiose valstybėse narėse, nebus tinkamos ES ženklams gauti. Norint gauti akreditaciją Europos duomenų apsaugos ženklo taikymo sričiai, bus būtina gauti akreditaciją valstybėje narėje, kurioje yra sertifikavimo įstaigos, ketinančios taikyti minėtą schemą, t. y. atsakingos už sertifikatų išdavimą ir savo subjektų bei patronuojamųjų įmonių vykdomos sertifikavimo veiklos valdymą kitose valstybėse narėse, būstinė. Kai kiti įmonės padaliniai ar biurai valdo ir atlieka sertifikavimą autonomiškai, kiekvienas iš šių padalinių ar biurų turės gauti atskirą akreditaciją valstybėje narėje, kurioje jis yra įsisteigęs. Kitaip tariant, akreditacija tik sertifikavimo įstaigos būstinės valstybėje narėje reikalinga tuo atveju, kai sertifikatus išduoda tik minėta būstinė. Ir priešingai, kai sertifikatus išduoda ir kiti sertifikavimo įstaigos padaliniai, turi būti akredituojami ir šie padaliniai.

45. Atitinkamai, jeigu sertifikavimo įstaiga nebuvo akredituota, kad galėtų išduoti Europos duomenų apsaugos ženklus, tada Europos duomenų apsaugos valdybos patvirtinti kriterijai negali būti naudojami, o ženklas negali būti išduodamas.

5 SERTIFIKAVIMO KRITERIJŲ PARENGIMAS

46. BDAR nustatyta sistema sertifikavimo kriterijams parengti. Pagrindiniai sertifikavimo procedūros reikalavimai aptarti 42 ir 43 straipsniuose, ten kartu numatyti ir būtinieji sertifikavimo procedūrų kriterijai, o sertifikavimo kriterijų pagrindas turi būti nustatomas pagal BDAR principus bei taisykles ir turi padėti įsitikinti, kad jie yra įgyvendinti.

47. Rengiant sertifikavimo kriterijus, daugiausia dėmesio turėtų būti skiriama galimybei juos patikrinti, taip pat jų reikšmingumui ir tinkamumui Reglamento laikymuisi įrodyti. Sertifikavimo kriterijai turėtų būti suformuluoti taip, kad jie būtų aiškūs ir suprantami ir kad juos būtų įmanoma praktiškai taikyti.

48. Rengiant sertifikavimo kriterijus, kai taikytina, turėtų būti atsižvelgiama, *inter alia*, į toliau nurodytus atitikties aspektus, padedančius įvertinti duomenų tvarkymo operaciją:

    - duomenų tvarkymo teisėtumą pagal 6 straipsnį;
    - duomenų tvarkymo principus pagal 5 straipsnį;
    - duomenų subjektų teises pagal 12–23 straipsnius;
    - įpareigojimą pranešti apie duomenų saugumo pažeidimus pagal 33 straipsnį;
    - įpareigojimą įgyvendinti pritaikytąją duomenų apsaugą ir standartizuotąją duomenų apsaugą pagal 25 straipsnį;

- jeigu taikytina, ar pagal 35 straipsnio 7 dalies d punktą buvo atliktas poveikio duomenų apsaugai vertinimas, ir
- pagal 32 straipsnį įgyvendintas technines ir organizacines priemones.

49. Šių aspektų įtraukimo į kriterijus mastas gali skirtis priklausomai nuo sertifikavimo taikymo srities, kuri gali apimti duomenų tvarkymo operacijų rūšį ir sertifikavimo sritį (pvz., sveikatos priežiūros sektorių).

5.1 Kas gali būti sertifikuojama pagal BDAR?

50. Europos duomenų apsaugos valdyba mano, kad BDAR numatyta plati pagal BDAR sertifikuojamų aspektų sritis, jeigu visų pirma stengiamasi padėti įrodyti, jog duomenų valdytojai ir duomenų tvarkytojai, vykdydami duomenų tvarkymo operacijas, laikosi šio reglamento (42 straipsnio 1 dalis).

51. Vertinant duomenų tvarkymo operaciją, kai taikytina, turi būti atsižvelgiama į tris pagrindinius komponentus:

    1. asmens duomenis (BDAR materialinė taikymo sritis);
    2. technines sistemas – infrastruktūrą, pvz., techninę ir programinę įrangą, naudojamą asmens duomenims tvarkyti, ir
    3. su duomenų tvarkymo operacijomis susijusius procesus ir procedūras.

52. Kiekvienas duomenų tvarkymo operacijose naudojamas komponentas turi būti įvertintas pagal nustatytus kriterijus. Įtakos gali turėti bent keturi skirtingi svarbūs veiksniai: 1) duomenų valdytojo ar duomenų tvarkytojo organizacinė ir teisinė struktūra; 2) duomenų tvarkymo operacijose dalyvaujantis skyrius, aplinka ir žmonės; 3) vertintinų elementų techninis aprašymas ir galiausiai 4) duomenų tvarkymo operacijai naudojama IT infrastruktūra, t. y. ir operacinės sistemos, virtualios sistemos, duomenų bazės, autentiškumo tikrinimo ir autorizacijos sistemos, maršrutizatoriai ir ugniasienės, saugyklos, ryšių infrastruktūra arba interneto prieiga ir su tuo susijusios techninės priemonės.

53. Visi trys pagrindiniai komponentai yra aktualūs kuriant sertifikavimo procedūras ir kriterijus. Priklausomai nuo sertifikavimo objekto, į juos gali būti atsižvelgiama skirtingai. Pavyzdžiui, kai kuriais atvejais tam tikrų komponentų galima nepaisyti, jeigu jie laikomi neaktualiais sertifikavimo objektui.

54. Siekiant dar tiksliau nurodyti, ką galima sertifikuoti pagal BDAR, BDAR išdėstytos papildomos gairės. Iš 42 straipsnio 7 dalies galima spręsti, kad sertifikatai pagal BDAR išduodami tik duomenų valdytojams ir duomenų tvarkytojams, todėl, pavyzdžiui, duomenų apsaugos pareigūnų sertifikuoti neįmanoma. 43 straipsnio 1 dalies b punkte nurodytas ISO 17065, kuriame numatytas sertifikavimo įstaigų, vertinančių produktų, paslaugų ir procesų atitiktį, akreditavimas. Duomenų tvarkymo operacija arba operacijų seka pagal ISO 17065 terminiją gali būti laikomos produktu arba paslauga ir atitinkamai gali būti sertifikuojamos. Pavyzdžiui, darbuotojų duomenų tvarkymas siekiant išmokėti darbo užmokestį arba administruoti

atostogas pagal BDAR yra operacijų seka ir pagal ISO terminiją gali būti laikomas produktu, procesu arba paslauga.

55. Remdamasi šiais argumentais, Europos duomenų apsaugos valdyba mano, kad pagal BDAR vykdomo sertifikavimo taikymo sritis orientuojama į duomenų tvarkymo operacijas ar jų seką. Tai gali būti valdymo procesai – tam tikros organizacinės priemonės, kurios atitinkamai yra duomenų tvarkymo operacijos sudedamosios dalys (pvz., valdymo procesas, sukurtas skundams nagrinėti, yra darbuotojų duomenų tvarkymo, vykdomo siekiant išmokėti darbo užmokestį, dalis).

56. Siekiant įvertinti duomenų tvarkymo operacijos atitiktį sertifikavimo kriterijams, turi būti pateiktas naudojimo atvejis. Pavyzdžiui, duomenų tvarkymo operacijai naudojamos techninės infrastruktūros naudojimo atitiktis priklauso nuo duomenų, kuriuos ši infrastruktūra yra suprojektuota apdoroti, kategorijų. Organizacinės priemonės priklauso nuo duomenų kategorijų bei kiekio ir duomenų tvarkymui naudojamos techninės infrastruktūros, atsižvelgiant į duomenų tvarkymo pobūdį, sritį, turinį ir tikslus, taip pat į pavojus duomenų subjektų teisėms ir laisvėms.

57. Be to, reikia nepamiršti, kad IT taikomosios programos gali būti labai skirtingos, net jeigu jos naudojamos tais pačiais duomenų tvarkymo tikslais. Todėl tai reikia apsvarstyti apibrėžiant sertifikavimo mechanizmų taikymo sritį ir rengiant sertifikavimo kriterijus, t. y. sertifikavimo taikymo sritis ir kriterijai neturėtų būti tokie siauri, kad į juos nepatektų skirtingai suprojektuotos IT taikomosios programos.

5.2 Sertifikavimo objekto nustatymas

58. Konkrečiuose sertifikavimo projektuose, vykdomuose pagal sertifikavimo mechanizmą, sertifikavimo mechanizmo taikymo sritis turi būti atskirta nuo objekto – vadinamojo vertinimo objekto. Sertifikavimo mechanizmo taikymo sritis gali būti apibrėžiama arba bendrai, arba ją susiejant su konkrečia duomenų tvarkymo rūšimi arba sritimi, taigi, ją nustatant jau gali būti įvardijami sertifikavimo objektai, priklausantys sertifikavimo mechanizmo taikymo sričiai (pvz., saugus duomenų laikymas ir skaitmeninėje saugykloje esančių asmens duomenų apsauga). Bet kuriuo atveju patikimas, prasmingas atitikties vertinimas gali būti atliktas tik tuomet, jeigu yra tiksliai aprašytas konkretus sertifikavimo projekto objektas. Turi būti aiškiai aprašyta, kurios duomenų tvarkymo operacijos yra įtrauktos į sertifikavimo objektą, o tada turi būti nurodyti pagrindiniai komponentai, t. y. kurie duomenys, procesai ir techninė infrastruktūra bus vertinami, o kurie – nebus. Tai darant visuomet turi būti apsvarstytos ir aprašytos sąsajos su kitais procesais. Aišku, kad tai, kas nėra žinoma, negali būti vertinama ir atitinkamai negali būti sertifikuojama. Bet kuriuo atveju konkretus sertifikavimo objektas turi turėti tam tikrą reikšmę sertifikavimu patvirtinamos žinios ar teiginio atžvilgiu ir turėtų neklaidinti naudotojo, kliento ar vartotojo.

59. [1 pavyzdys]

    Bankas klientams internetinės bankininkystės tikslais teikia interneto svetainės paslaugą. Naudojantis šia paslauga, galima atlikti pavedimus, pirkti akcijas, inicijuoti periodinio mokėjimo nurodymus ir tvarkyti sąskaitą. Bankas, taikydamas duomenų apsaugos

sertifikavimo mechanizmą, kurio bendroji taikymo sritis grindžiama bendraisiais kriterijais, pageidauja sertifikuoti toliau nurodytus elementus.

a) Saugus prisijungimas

Saugus prisijungimas yra duomenų tvarkymo operacija, kuri yra suprantama galutiniam naudotojui ir kuri yra aktuali duomenų apsaugos požiūriu, nes ji atlieka svarbų vaidmenį užtikrinant atitinkamų asmens duomenų saugumą. Todėl ši duomenų tvarkymo operacija yra reikalinga tam, kad būtų galima saugiai prisijungti, ir atitinkamai gali būti reikšmingas vertinimo objektas, jeigu sertifikate aiškiai nurodoma, kad sertifikuojama tik prisijungimo duomenų tvarkymo operacija.

b) Grafinė vartotojo sąsaja

Nors grafinė vartotojo sąsaja duomenų apsaugos požiūriu gali būti aktuali, galutinis naudotojas jos nesupranta ir todėl tai negali būti prasmingas vertinimo objektas. Be to, naudotojui neaišku, kurios interneto svetainės paslaugos ir atitinkamai kurios duomenų tvarkymo operacijos yra sertifikuotos.

c) Elektroninė bankininkystė

Grafinė vartotojo sąsaja kartu su vidiniu programavimu yra kaip internetinės bankininkystės paslaugos dalis atliekamos duomenų tvarkymo operacijos, o internetinės bankininkystės paslauga vartotojui gali būti reikšminga. Taigi, į vertinimo objektą turi būti įtraukta ir grafinė vartotojo sąsaja, ir vidinis programavimas. Kita vertus, duomenų tvarkymo operacijos, kurios nėra tiesiogiai susijusios su internetinės bankininkystės paslaugų teikimu, pvz., pinigų plovimo prevencijos tikslu vykdomos duomenų tvarkymo operacijos, į vertinimo objektą gali būti neįtrauktos.

Tačiau internetinės bankininkystės paslaugos, kurias bankas teikia per savo interneto svetainę, gali apimti ir kitas paslaugas, kurioms savo ruožtu reikalingos atskiros duomenų tvarkymo operacijos. Šiuo atžvilgiu kitos paslaugos gali apimti, pavyzdžiui, draudimo produkto pasiūlymą. Kadangi ši papildoma paslauga nėra tiesiogiai susijusi su internetinės bankininkystės paslaugų teikimo tikslu, ji į vertinimo objektą gali būti neįtraukta. Jeigu ši papildoma paslauga (draudimas) į vertinimo objektą neįtraukiama, interneto svetainėje integruotos šios paslaugos sąsajos yra vertinimo objekto dalis, todėl jos turi būti aprašytos, kad paslaugos būtų aiškiai atskirtos. Toks aprašymas reikalingas tam, kad būtų galima nustatyti ir įvertinti galimus duomenų srautus tarp abiejų paslaugų.

60. [2 pavyzdys]

Bankas savo klientams teikia paslaugą, kuria naudojantis galima susumuoti informaciją, susijusią su kelių bankų skirtingomis sąskaitomis ir kredito kortelėmis (sąskaitų sumavimas). Bankas pageidauja savo paslaugą sertifikuoti pagal BDAR. Kompetentinga priežiūros institucija yra patvirtinusi konkretų sertifikavimo kriterijų rinkinį, daugiausia skirtą šiai veiklos rūšiai. Sertifikavimo mechanizmo taikymo sritis apima tik toliau nurodytus atitikties aspektus:

- naudotojo autentiškumo tikrinimą ir
- priimtinus būdus gauti sumuotinus duomenis iš kitų bankų ar paslaugų.

Kadangi vertinimo objektą lemia pati šio sertifikavimo mechanizmo taikymo sritis, pagal siūlomą taikymo sritį neįmanoma reikšmingai susiaurinti vertinimo objekto ir sertifikuoti tik konkrečių ypatumų arba tik vieno duomenų tvarkymo veiksmo. Pagal šį scenarijų vertinimo objektas turi prilygti konkrečiai taikymo sričiai.

5.3 Vertinimo metodai ir vertinimo metodika

61. Siekiant atlikti atitikties vertinimą ir atitinkamai padėti įrodyti duomenų tvarkymo operacijų atitiktį, reikia įvardyti ir nustatyti vertinimo metodus ir vertinimo metodiką. Svarbu tai, ar vertintina informacija surenkama tik iš dokumentacijos (to savaime nepakaktų), ar ji aktyviai renkama vietoje, naudojant tiesioginę ar netiesioginę prieigą. Informacijos surinkimo būdas turi pasekmių sertifikavimo reikšmingumui, todėl jį reikėtų apibrėžti ir aprašyti.

    Sertifikatų išdavimo ir periodinės peržiūros procedūros turėtų apimti specifikacijas, kuriomis būtų nustatytas tinkamas, sertifikavimo kriterijus atitinkantis vertinimo lygis (išsamumas ir sudėtis) ir į kurias būtų įtraukta nuostata dėl:

    - informacijos apie taikytų vertinimo metodų ir duomenų, surinktų, pvz., atliekant patikrinimus vietoje arba iš dokumentacijos, apibūdinimą,
    - vertinimo metodų, kuriais pagrindinis dėmesys būtų skiriamas duomenų tvarkymo operacijoms (duomenims, sistemoms, procesams), ir duomenų tvarkymo tikslo,
    - duomenų kategorijų nustatymo, apsaugos poreikių ir ar dalyvauja duomenų tvarkytojai arba trečiosios šalys,
    - funkcijų nustatymo ir ar taikomas prieigos kontrolės mechanizmas, apibrėžtas pagal minėtas funkcijas ir atsakomybės sritis.

62. Vertinimo išsamumas turi poveikį sertifikavimo reikšmingumui ir vertei. Jeigu vertinimo išsamumas bus sumažintas pragmatiniais sumetimais arba siekiant sumažinti išlaidas, sumažės ir duomenų apsaugos sertifikavimo reikšmingumas. Kita vertus, sprendimai dėl vertinimo sudėties gali viršyti pareiškėjo finansines galimybes, o dažnai – ir vertintojų bei auditorių pajėgumus. Atitikties įrodymo tikslais galbūt ne visada būtina labai išsamiai išnagrinėti naudojamas IT sistemas, kad ši analizė išliktų reikšminga.

5.4 Vertinimo dokumentavimas

63. Sertifikavimas turėtų būti išsamiai ir visapusiškai dokumentuojamas. Nepakankamas dokumentavimas reiškia, kad tinkamas įvertinimas negali būti atliktas. Būtina sertifikavimo dokumentavimo funkcija – dokumentavimas suteikia vertinimo proceso, atliekamo pagal sertifikavimo mechanizmą, skaidrumą. Dokumentuose galima rasti atsakymus į klausimus dėl teisės aktuose išdėstytų reikalavimų. Sertifikavimo mechanizmuose turėtų būti numatyta standartizuota dokumentavimo metodika. Tada, atliekant vertinimą, sertifikavimo dokumentus bus galima palyginti su faktine būkle vietoje ir su sertifikavimo kriterijais.

64. Išsamūs dokumentai, kuriuose atsispindi sertifikavimo objektas ir taikyta metodika, yra naudingi siekiant skaidrumo. Remiantis 43 straipsnio 2 dalies c punktu, sertifikavimo mechanizmuose turėtų būti nustatytos sertifikatų peržiūros procedūros. Siekiant sudaryti

priežiūros institucijai sąlygas įvertinti, ar sertifikatas gali būti pripažįstamas ir kiek jis gali būti pripažįstamas atliekant oficialius tyrimus, išsamus dokumentavimas gali būti tinkamiausias ryšių palaikymo būdas. Todėl vertinimo metu parengtuose dokumentuose daugiausia dėmesio turėtų būti skiriama trims pagrindiniams aspektams:

- taikytų vertinimo metodų nuoseklumui ir suderinamumui;
- vertinimo metodų orientavimui į galimybę įrodyti, kad sertifikavimo objektas atitinka sertifikavimo kriterijus, taigi – ir Reglamentą, ir
- tam, kad vertinimo rezultatus patvirtino nepriklausoma ir nešališka sertifikavimo įstaiga.

5.5 Rezultatų dokumentavimas

65. 100 konstatuojamojoje dalyje pateikiama informacija apie tikslus, kurių siekiama nustatant sertifikavimą:

„siekiant didesnio skaidrumo ir geresnio šio reglamento laikymosi, reikėtų skatinti nustatyti sertifikavimo mechanizmus ir duomenų apsaugos ženklus bei žymenis, kad duomenų subjektai galėtų greitai įvertinti konkretaus produkto ar paslaugos duomenų apsaugos lygį;“

66. Siekiant didesnio skaidrumo, svarbų vaidmenį atlieka rezultatų dokumentavimas ir perdavimas. Sertifikavimo įstaigos, naudojančios į duomenų subjektus (kaip vartotojus ar klientus) orientuotus sertifikavimo mechanizmus, ženklus ar žymenis, turėtų suteikti lengvai prieinamą, suprantamą ir reikšmingą informaciją apie sertifikuotą (-as) duomenų tvarkymo operaciją (-as). Ši vieša informacija turėtų apimti bent jau

- vertinimo objekto aprašymą,
- nuorodą į patvirtintus kriterijus, taikytus konkrečiam vertinimo objektui,
- kriterijų vertinimo metodiką (vertinimą vietoje, dokumentavimą ir kt.) ir
- sertifikato galiojimo trukmę, be to,
- priežiūros institucijoms ir visuomenei ši informacija turėtų suteikti galimybę palyginti rezultatus.

6 SERTIFIKAVIMO KRITERIJŲ APIBRĖŽIMO GAIRĖS

67. Sertifikavimo kriterijai yra sudedamoji sertifikavimo mechanizmo dalis. Sertifikavimo procedūra apima reikalavimus, kaip, kas ir kokios sudėties vertinimą atlieka, kai vertinami konkretūs sertifikavimo projektai, apimantys konkretų vertinimo objektą. Sertifikavimo kriterijuose numatyti nominalūs reikalavimai, pagal kuriuos vertinama duomenų tvarkymo operacija, nurodyta vertinimo objekto apibrėžtyje. Šios sertifikavimo kriterijų apibrėžimo

gairės yra bendro pobūdžio patarimai, padėsiantys įvertinti sertifikavimo kriterijus, kad juos būtų galima patvirtinti.

- Tvirtinant arba apibrėžiant sertifikavimo kriterijus turėtų būti atsižvelgiama į toliau nurodytus bendrus aspektus. Sertifikavimo kriterijai:
- turėtų būti vienodi ir juos turėtų būti įmanoma patikrinti;
- turėtų būti įmanoma atlikti jų auditą, kad būtų lengviau įvertinti duomenų tvarkymo operacijas pagal BDAR, visų pirma nurodant tikslus ir praktines tų tikslų įgyvendinimo gaires;
- sertifikavimo kriterijai turėtų būti aktualūs tikslinei jų auditorijai, pvz., „verslas verslui“ ir „verslas vartotojui“;
- sertifikavimo kriterijais turėtų būti atsižvelgiama į kitus standartus (pvz., ISO standartus, nacionalinio lygmens standartus) ir reikiamais atvejais turėtų būti numatyta jų tarpusavio sąveika; be to,
- sertifikavimo kriterijai turėtų būti lankstūs ir jų mastą turėtų būti įmanoma pritaikyti įvairių rūšių ir dydžių organizacijoms, įskaitant labai mažas, mažąsias ir vidutines įmones, kaip numatyta 42 straipsnio 1 dalyje, ir vadovaujantis rizika pagrįstu metodu, kaip numatyta 77 konstatuojamojoje dalyje.

68. Maža vietinė įmonė, pvz., mažmeninės prekybos įmonė, paprastai atlieka ne tokias sudėtingas duomenų tvarkymo operacijas kaip didelė daugiašalė mažmeninės prekybos įmonė. Nors duomenų tvarkymo operacijų teisėtumo reikalavimai yra tie patys, turi būti atsižvelgiama į duomenų tvarkymo apimtį ir jo sudėtingumą; atitinkamai reikia, kad sertifikavimo mechanizmus ir jų kriterijus būtų galima pritaikyti prie atitinkamos duomenų tvarkymo veiklos masto.

6.1 Galiojantys standartai

69. Sertifikavimo įstaigos turės apsvarstyti, kaip nustatant konkrečius kriterijus turėtų būti atsižvelgiama į galiojančius aktualius dokumentus, pvz., elgesio kodeksus, techninius standartus arba nacionalines administracines ir teisines iniciatyvas. Būtų geriausia, jei kriterijai būtų suderinti su galiojančiais standartais, galinčiais padėti duomenų valdytojui arba duomenų tvarkytojui įvykdyti jiems BDAR nustatytus įpareigojimus. Tačiau jeigu pramonės standartuose daugiausia dėmesio dažnai skiriama organizacijos apsaugai nuo grėsmių ir jos saugumui, tai BDAR yra orientuotas į fizinių asmenų pagrindinių teisių apsaugą. Į šią skirtingą perspektyvą turi būti atsižvelgiama kuriant kriterijus ar tvirtinant kriterijus arba sertifikavimo mechanizmus, grindžiamus pramonės standartais.

6.2 Kriterijų apibrėžimas

70. Sertifikavimo kriterijai turi atitikti sertifikavimo mechanizmo arba schemos sertifikavimo pareiškimą (žinią arba teiginį) arba atitikti jo keliamus lūkesčius. Jau pačiame sertifikavimo

mechanizmo pavadinime gali atsispindėti taikymo sritis ir jis gali turėti poveikį kriterijų nustatymui.

71. [3 pavyzdys]

    Mechanizmas, vadinamas „SveikatosPrivatumoŽymuo“ (angl. *HealthPrivacyMark*) turėtų būti taikomas tik sveikatos priežiūros sektoriui. Sprendžiant iš ženklo pavadinimo galima tikėtis, kad buvo išnagrinėti su sveikatos duomenimis susiję duomenų apsaugos reikalavimai. Atitinkamai šio mechanizmo kriterijai turi būti pakankami, kad būtų įvertinti šio sektoriaus duomenų apsaugos reikalavimai.

72. [4 pavyzdys]

    Kai mechanizmas susijęs su duomenų tvarkymo operacijų, apimančių duomenų tvarkymo srities valdymo sistemas, sertifikavimu, jame turėtų būti nustatyti kriterijai, pagal kuriuos būtų galima pripažinti ir įvertinti valdymo procesus ir jų pagalbines technines bei organizacines priemones.

73. [5 pavyzdys]

    Kriterijai, taikomi mechanizmui, kuris yra susijęs su debesijos kompiuterija, turi būti rengiami atsižvelgiant į specialius techninius reikalavimus, reikalingus naudojimuisi debesijos paslaugomis. Pavyzdžiui, jeigu naudojami už ES ribų esantys serveriai, rengiant kriterijus turi būti atsižvelgiama į BDAR V skyriuje nustatytas sąlygas dėl duomenų perdavimo į trečiąsias valstybes.

74. Kriterijus, parengtus taip, kad tiktų įvairiems vertinimo objektams įvairiuose sektoriuose ir (arba) įvairiose valstybėse narėse, turėtų būti įmanoma taikyti įvairiems scenarijams; pagal juos turėtų būti įmanoma nustatyti tokias priemones, kurios tiktų mažo, vidutinio ar didelio masto duomenų tvarkymo operacijoms ir atspindėtų įvairios tikimybės ir rimtumo pavojų fizinių asmenų teisėms ir laisvėms, kaip numatyta BDAR. Atitinkamai kriterijus papildančios sertifikavimo procedūros (pvz., dokumentavimo, bandymų ar vertinimo metodo bei išsamumo) turi atitikti šiuos poreikius, be to, būtina sudaryti sąlygas, pvz., taikyti aktualius kriterijus konkretiems sertifikavimo projektams ir turėti galiojančias taisykles, kaip tai daryti. Taikant kriterijus turi būti lengviau įvertinti, ar suteikta pakankamai garantijų, kad bus įgyvendintos tinkamos techninės ir organizacinės priemonės.

6.3 Sertifikavimo kriterijų taikymo trukmė

75. Nors sertifikavimo kriterijai įvairiais laikotarpiais turi būti patikimi, jie neturėtų būti visiškai nekintami. Jie turi būti persvarstomi, pavyzdžiui, kai:

    - keičiama teisinė sistema;
    - Europos Sąjungos Teisingumo Teismas savo sprendimais pateikia sąlygų ir nuostatų išaiškinimą arba
    - sukuriamos techninės naujovės.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

(Andrea Jelinek)

1 PRIEDAS. PRIEŽIŪROS INSTITUCIJŲ UŽDUOTYS IR ĮGALIOJIMAI, SUSIJĘ SU SERTIFIKAVIMU PAGAL BDAR

	Nuostatos	Reikalavimai
Užduotys	43 straipsnio 6 dalis	Reikalaujama, kad priežiūros institucija 42 straipsnio 5 dalyje nurodytus kriterijus padarytų lengvai viešai prieinamus ir perduotų Valdybai.
	57 straipsnio 1 dalies n punktas	Reikalaujama, kad priežiūros institucija patvirtintų sertifikavimo kriterijus pagal 42 straipsnio 5 dalį.
	57 straipsnio 1 dalies o punktas	Numatyta, kad atitinkamais atvejais (t. y. kai priežiūros institucija išduoda sertifikatus) priežiūros institucija periodiškai atlieka išduotų sertifikatų peržiūrą pagal 42 straipsnio 7 dalį.
	64 straipsnio 1 dalies c punktas	Reikalaujama, kad priežiūros institucija Valdybai pateiktų sprendimo projektą, kai juo siekiama patvirtinti sertifikavimo kriterijus, nurodytus 42 straipsnio 5 dalyje.
Įgaliojimai	58 straipsnio 1 dalies c punktas	Numatyta, kad priežiūros institucija turi įgaliojimus atlikti išduotų sertifikatų peržiūrą pagal 42 straipsnio 7 dalį.
	58 straipsnio 2 dalies h punktas	Numatyta, kad priežiūros institucija turi įgaliojimus atšaukti sertifikatą arba nurodyti sertifikavimo įstaigai atšaukti sertifikatą, arba nurodyti sertifikavimo įstaigai neišduoti sertifikato.
	58 straipsnio 3 dalies e punktas	Numatyta, kad priežiūros institucija turi įgaliojimus akredituoti sertifikavimo įstaigas.
	58 straipsnio 3 dalies f punktas	Numatyta, kad priežiūros institucija turi įgaliojimus išduoti sertifikatus ir patvirtinti sertifikavimo kriterijus.

2 PRIEDAS

1 ĮVADAS

2 priede pateikiamos sertifikavimo kriterijų pagal 42 straipsnio 5 dalį peržiūros ir vertinimo gairės. Jame nustatomi aspektai, kuriuos duomenų apsaugos priežiūros institucija ir EDAV svarstys ir į kuriuos atsižvelgs, kai bus tvirtinami sertifikavimo mechanizmo sertifikavimo kriterijai. Į šiuos klausimus turėtų atsižvelgti sertifikavimo įstaigos ir schemos savininkai, rengiantys kriterijus ir teikiantys juos patvirtinti. Sąrašas nėra baigtinis, tačiau jame pateikiami būtiniausi aspektai, į kuriuos reikia atsižvelgti. Ne visi klausimai bus taikomi, tačiau rengiant kriterijus į juos reikėtų atsižvelgti ir gali tekti paaiškinti, kodėl kriterijai neapima tam tikrų aspektų. Kai kurie klausimai kartojami dėl skirtingos perspektyvos. Į šias gaires turėtų būti atsižvelgiama vadovaujantis BDAR nustatytais teisiniais reikalavimais ir, jei taikoma, nacionalinės teisės aktais.

2 SERTIFIKAVIMO MECHANIZMO TAIKYMO SRITIS IR VERTINIMO OBJEKTAS

a. Ar sertifikavimo mechanizmo (kuriame naudojami duomenų apsaugos kriterijai) taikymo sritis aiškiai aprašyta?

b. Ar sertifikavimo mechanizmo taikymo sritis suprantama tiems, kam jis skirtas, ir ar ji nėra klaidinanti?

- *Pavyzdys: „Patikimos bendrovės ženklas“ (angl. „Trusted Company Seal“) leidžia manyti, kad buvo patikrintas visos bendrovės duomenų tvarkymas, tačiau iš tiesų sertifikuojamos tik tam tikros duomenų tvarkymo operacijos, pavyzdžiui, mokėjimas internetu. Taigi taikymo sritis klaidinanti.*

c. Ar sertifikavimo mechanizmo taikymo sritis atspindi visus svarbius duomenų tvarkymo operacijų aspektus?

- *Pavyzdys: Pagal 9 straipsnio reikalavimus „Asmens sveikatos duomenų apsaugos žymuo“ (angl. „Privacy Health Mark“) reiškia, kad atsižvelgta į visus su sveikata susijusius vertinimo duomenis.*

d. Ar sertifikavimo mechanizmo taikymo sritis suteikia galimybę atlikti prasmingą duomenų apsaugos sertifikavimą atsižvelgiant į atitinkamų duomenų tvarkymo operacijų pobūdį, turinį ir su jomis susijusį pavojų?

- *Pavyzdys: Jei sertifikavimo mechanizmo taikymo sričiai priklausytų tik konkretūs duomenų tvarkymo procedūrų aspektai, pavyzdžiui, duomenų rinkimas, tačiau ne tolesnės duomenų tvarkymo operacijos, pavyzdžiui, duomenų tvarkymas siekiant sukurti reklamos profilius arba duomenų subjekto teisių valdymas, duomenų subjektams tai nebūtų prasminga.*

e. Ar sertifikavimo mechanizmo taikymo sritis apima asmens duomenų tvarkymą atitinkamoje paraiškos šalyje, ar tarptautinį duomenų tvarkymą ir (arba) perdavimą?

f. Ar sertifikavimo kriterijuose pakankamai išsamiai aprašoma, kaip turėtų būti apibrėžiamas vertinimo objektas?

- *Pavyzdys: Iš bendro taikymo „Privatumo apsaugos ženklo“ (angl. „Privacy Seal“), dėl kurio reikalaujama tik „sertifikuojamo duomenų tvarkymo specifikacijos“, nebūtų pakankamai aišku, kaip nustatyti ir apibūdinti vertinimo objektą.*
- *Pavyzdys: Turėtų būti išsamiai apibūdinti (specialiosios) taikymo srities „Asmens duomenų saugojimo saugykloje ženklo“ (angl. „The Privacy Vault Seal“), kuriuo patvirtinamas saugus duomenų laikymas, reikalavimai, kad iš jo kriterijų būtų aiški jo taikymo sritis, pavyzdžiui, saugyklos apibrėžtis, sistemos reikalavimai, privalomos techninės ir organizacinės priemonės. Tokiu atveju taikymo sritis sudaro sąlygas aiškiai apibrėžti vertinimo objektą.*

    (1) Ar kriterijuose reikalaujama, kad į vertinimo objektą būtų įtrauktas visų svarbių duomenų tvarkymo operacijų identifikavimas, duomenų srautų pavaizdavimas ir vertinimo objekto taikymo srities nustatymas?

    - *Pavyzdys: Sertifikavimo mechanizmu siūlomas duomenų valdytojų atliekamų duomenų tvarkymo operacijų pagal BDAR sertifikavimas išsamiau nenurodant taikymo srities (bendroji taikymo sritis). Pagal mechanizmo taikomus kriterijus reikalaujama, kad paraišką pateikiantis duomenų valdytojas nustatytų tikslinę duomenų tvarkymo operaciją (vertinimo objektą) duomenų tipų, sistemų ir procesų atžvilgiu.*

    (2) Ar pagal kriterijus reikalaujama, kad pareiškėjas paaiškintų, kada vertinamas duomenų tvarkymas pradedamas ir baigiamas? Ar pagal kriterijus reikalaujama, kad į vertinimo objektą būtų įtraukiamos sąsajos tais atvejais, kai tarpusavyje susijusios duomenų tvarkymo operacijos nėra įtraukiamos kaip vertinimo objekto dalis? Ar tai tinkamai pagrįsta?

    - *Pavyzdys: Vertinimo objektas, kurį apibūdinant pakankamai išsamiai aprašomas saityno paslaugos tvarkymas, pvz., įtraukiamas naudotojų registravimas, paslaugos teikimas, sąskaitų faktūrų teikimas, IP adresų registravimas, naudotojams ir trečiosioms šalims skirtos sąsajos, išskyrus serverių prieglobą (tačiau įskaitant tvarkymo ir techninių ir organizacinių priemonių susitarimus).*

g. Ar kriterijais užtikrinama, kad (atskiri) vertinimo objektai būtų suprantami tiems, kam jie skirti, įskaitant, jei tinka, duomenų subjektus?

3 BENDRIEJI REIKALAVIMAI

a. Ar visi kriterijų kataloge (t. y. visame sertifikavimo kriterijų rinkinyje) vartojami svarbūs terminai yra aiškiai apibrėžti, paaiškinti ir aprašyti?

b. Ar nustatytos visos norminės nuorodos?

c. Ar į kriterijus įtrauktos atsakomybės už duomenų apsaugą, procedūrų ir duomenų tvarkymo, patenkančių į sertifikavimo mechanizmo taikymo sritį, apibrėžtys?

4 DUOMENŲ TVARKYMO OPERACIJA, 42 STRAIPSNIO 1 DALIS

Ar, atsižvelgiant į sertifikavimo mechanizmo taikymo sritį (bendrąją arba specialiąją), kriterijai atspindi visas svarbias duomenų tvarkymo operacijų (duomenų, sistemų ir procesų) sudedamąsias dalis?

a. Ar pagal kriterijus reikalaujama nustatyti galiojančius duomenų tvarkymo pagrindus vertinimo objekto atžvilgiu?

b. Ar, atsižvelgiant į vertinimo objektą, pagal kriterijus pripažįstami visi reikiami duomenų tvarkymo etapai ir visas duomenų gyvavimo ciklas, įskaitant pašalinimą ir (arba) anonimizavimą?

c. Ar, atsižvelgiant į vertinimo objektą, pagal kriterijus reikalaujama duomenų perkeliamumo?

d. Ar, atsižvelgiant į duomenų objektą, kriterijai suteikia galimybę nustatyti specialias duomenų tvarkymo operacijų rūšis, pavyzdžiui, automatizuotą sprendimų priėmimą, profiliavimą, ir į jas atsižvelgti?

e. Ar, atsižvelgiant į vertinimo objektą, kriterijai suteikia galimybę nustatyti specialias duomenų kategorijas?

f. Ar kriterijai suteikia galimybę įvertinti atskirų duomenų tvarkymo operacijų pavojingumą ir duomenų subjektų teisių ir laisvių apsaugos poreikį ir ar pagal juos to reikalaujama?

g. Ar kriterijai suteikia galimybę tinkamai atsižvelgti į pavojus fizinių asmenų teisėms ir laisvėms ir ar pagal juos to reikalaujama?

…

5 DUOMENŲ TVARKYMO TEISĖTUMAS

a. Ar pagal kriterijus reikalaujama patikrinti atskirų duomenų tvarkymo operacijų teisėtumą, atsižvelgiant į duomenų tvarkymo tikslą ir būtinybę?

b. Ar pagal kriterijus reikalaujama patikrinti visus atskirų duomenų tvarkymo operacijų teisinio pagrindo reikalavimus?

6 PRINCIPAI, 5 STRAIPSNIS

a. Ar kriterijais tinkamai atsižvelgiama į visus 5 straipsnyje išdėstytus duomenų apsaugos principus?

b. Ar pagal kriterijus reikalaujama įrodyti, kad laikomasi su atskiru vertinimo objektu susijusio duomenų kiekio mažinimo principo?

…

7 BENDROSIOS DUOMENŲ VALDYTOJŲ IR DUOMENŲ TVARKYTOJŲ PRIEVOLĖS

a. Ar pagal kriterijus reikalaujama duomenų tvarkytojų ir duomenų valdytojų sutartinių susitarimų įrodymo?

b. Ar duomenų valdytojų ir duomenų tvarkytojų susitarimai yra vertinimo objektas?

c. Ar kriterijai atspindi duomenų valdytojo prievoles pagal IV skyrių?

d. Ar pagal kriterijus reikalaujama pateikti pagal 24 straipsnio 1 dalį duomenų valdytojo įgyvendintų techninių ir organizacinių priemonių peržiūros ir atnaujinimo įrodymų?

e. Ar pagal kriterijus tikrinama, ar organizacija įvertino, ar turėtų būti paskirtas duomenų apsaugos pareigūnas, kaip reikalaujama 37 straipsnyje? Jei taikytina, ar duomenų apsaugos pareigūnas atitinta 37–39 straipsnių reikalavimus?

f. Ar pagal kriterijus tikrinama, ar reikia duomenų tvarkymo veiklos įrašų pagal 30 straipsnio 5 dalį ir ar tinkamai įgyvendinami 30 straipsnio reikalavimai?

8 DUOMENŲ SUBJEKTŲ TEISĖS

a. Ar kriterijais tinkamai atsižvelgiama į duomenų subjekto teises į informaciją ir reikalaujama įgyvendinti atitinkamas priemones?

b. Ar pagal kriterijus reikalaujama, kad duomenų subjektams būtų suteikta pakankama arba lengvesnė prieiga prie jų duomenų ir jų kontrolė, įskaitant duomenų perkeliamumą?

c. Ar pagal kriterijus reikalaujama įgyvendinti priemones, kuriomis būtų suteikiama galimybė įsikišti į duomenų tvarkymo operaciją, siekiant užtikrinti duomenų subjektų teises ir leisti duomenis ištaisyti, ištrinti arba apriboti jų tvarkymą?

…

9 PAVOJAI FIZINIŲ ASMENŲ TEISĖMS IR LAISVĖMS

a. Ar kriterijai suteikia galimybę įvertinti pavojų fizinių asmenų teisėms ir laisvėms ir ar pagal juos to reikalaujama?

b. Ar pagal kriterijus numatoma pripažinta rizikos vertinimo metodika arba pagal juos tokios metodikos reikalaujama? Jei taip, ar tai proporcinga?

c. Ar kriterijai suteikia galimybę įvertinti numatomų duomenų tvarkymo operacijų poveikį fizinių asmenų teisėms ir laisvėms ir ar pagal juos to reikalaujama?

d. Ar pagal kriterijus reikalaujama iš anksto konsultuotis dėl likusio pavojaus, kuris negali būti sumažintas, remiantis poveikio duomenų apsaugai vertinimo rezultatais?

10 TECHNINĖS IR ORGANIZACINĖS PRIEMONĖS, KURIOMIS UŽTIKRINAMA APSAUGA

a. Ar pagal kriterijus reikalaujama taikyti technines ir organizacines priemones, kuriomis būtų užtikrinamas duomenų tvarkymo operacijų konfidencialumas?

b. Ar pagal kriterijus reikalaujama taikyti technines ir organizacines priemones, kuriomis būtų užtikrinamas duomenų tvarkymo operacijų vientisumas?

c. Ar pagal kriterijus reikalaujama taikyti technines ir organizacines priemones, kuriomis būtų užtikrinamas duomenų tvarkymo operacijų prieinamumas?

d. Ar pagal kriterijus reikalaujama taikyti priemones, kuriomis būtų užtikrinamas duomenų tvarkymo skaidrumas, susijęs su:

e. atskaitomybe;

f. duomenų subjektų teisėmis;

g. atskirų duomenų tvarkymo operacijų, pavyzdžiui, algoritmų skaidrumo, vertinimu?

h. Ar pagal kriterijus reikalaujama taikyti technines ir organizacines priemones, kuriomis būtų užtikrinamos duomenų subjektų teisės, pavyzdžiui, galimybė teikti informaciją arba teisė į duomenų perkeliamumą?

i. Ar pagal kriterijus reikalaujama taikyti technines ir organizacines priemones, kuriomis būtų suteikiama galimybė įsikišti į duomenų tvarkymo operaciją, siekiant užtikrinti duomenų subjektų teises ir leisti duomenis ištaisyti, ištrinti arba apriboti jų tvarkymą?

j. Ar pagal kriterijus reikalaujama taikyti priemones, kuriomis būtų suteikiama galimybė įsikišti į duomenų tvarkymo operaciją, siekiant pataisyti arba patikrinti sistemą arba procesą?

k. Ar pagal kriterijus reikalaujama taikyti technines ir organizacines priemones, kuriomis būtų užtikrinamas duomenų kiekio mažinimas, pavyzdžiui, duomenų atsiejimo arba atskyrimo nuo duomenų subjekto, anoniminimo arba pseudonimų suteikimo, arba duomenų sistemų atskyrimo priemones?

l. Ar pagal kriterijus reikalaujama imtis techninių priemonių, kad būtų įgyvendinta standartizuotoji duomenų apsauga?

m. Ar pagal kriterijus reikalaujama imtis techninių ir organizacinių priemonių, kuriomis būtų įgyvendinama pritaikytoji duomenų apsauga, pavyzdžiui, įgyvendinti duomenų apsaugos valdymo sistemą, skirtą duomenų apsaugos reikalavimams parodyti, apie juos informuoti, juos kontroliuoti ir įgyvendinti?

n. Ar pagal kriterijus reikalaujama imtis techninių ir organizacinių priemonių, kad darbuotojai, nuolat arba reguliariai turintys prieigą prie asmens duomenų, galėtų periodiškai gauti tinkamus mokymus?

o. Ar pagal kriterijus reikalaujama peržiūros priemonių?

p. Ar pagal kriterijus reikalaujama įsivertinimo / vidaus audito?

q. Ar pagal kriterijus reikalaujama imtis priemonių siekiant užtikrinti, kad pareiga pranešti apie asmens duomenų saugumo pažeidimą būtų vykdoma laiku ir tinkamai?

r. Ar pagal kriterijus reikalaujama, kad būtų įdiegtos ir patikrintos incidentų valdymo procedūros?

s. Ar pagal kriterijus reikalaujama stebėti pokyčius, susijusius su privatumo ir technologijų klausimais, ir atnaujinti schemą pagal reikalavimus?

…

11 KITOS PRIEMONĖS, KURIOMIS UŽTIKRINAMA DUOMENŲ APSAUGA

a. Ar pagal kriterijus reikalaujama įgyvendinti duomenų apsaugą stiprinančius metodus? Tai galėtų būti kriterijai, pagal kuriuos reikalaujama didinti duomenų apsaugą nenaudojant asmens duomenų arba jų naudojant mažiau ir (arba) šalinant arba mažinant pavojų duomenų apsaugai.

- *Pavyzdys: Kriterijai, pagal kuriuos reikalaujama didesnio nesusiejamumo naudojant į naudotoją sutelktą tapatybės duomenų tvarkymą, pavyzdžiui, atributais grindžiamus kredencialus (angl. „attribute –based credentials“, ABC), o ne į organizaciją sutelktą tapatybės duomenų tvarkymą, atspindėtų didesnės duomenų apsaugos techniką.*

b. Ar pagal kriterijus reikalaujama įgyvendinti tobulesnę duomenų subjektų kontrolę siekiant sudaryti palankesnes sąlygas apsispręsti ir pasirinkti?

…

12 KRITERIJAI, KURIAIS SIEKIAMA ĮRODYTI, KAD ĮDIEGTOS TINKAMOS ASMENS DUOMENŲ PERDAVIMO PRIEMONĖS

Kriterijai bus aptarti būsimose 42 straipsnio 2 daliai skirtose gairėse.

13 PAPILDOMI KRITERIJAI, SUSIJĘ SU EUROPOS DUOMENŲ APSAUGOS ŽENKLU

a. Ar kriterijus numatoma taikyti visoms valstybėms narėms?

b. Ar kriterijai suteikia galimybę atsižvelgti į valstybių narių duomenų apsaugos teisę arba scenarijus?

c. Ar pagal kriterijus reikalaujama vertinti atskirus vertinimo objektus atsižvelgiant į konkretiems sektoriams skirtus valstybių narių duomenų apsaugos teisės aktus?

d. Ar pagal kriterijus reikalaujama, kad duomenų valdytojas arba duomenų tvarkytojas teiktų duomenų subjektams ir suinteresuotosioms šalims valstybių narių kalbomis informaciją apie:

e. duomenų tvarkymą / vertinimo objektą;

f. duomenų tvarkymo / vertinimo objekto dokumentus;

g. vertinimo rezultatus?

…

14 BENDRAS KRITERIJŲ VERTINIMAS

a. Ar kriterijai atspindi visą sertifikavimo mechanizmo taikymo sritį (t. y. ar kriterijai išsamūs), kad suteiktų pakankamai garantijų, kad sertifikavimu galima pasitikėti?

- *Pavyzdys: Jei sertifikavimo mechanizmo taikymo sritis yra susijusi su sveikatos duomenų tvarkymo operacijomis, turėtų būti užtikrintas aukštas duomenų apsaugos lygis nustatant kriterijus, kuriais, pavyzdžiui, būtų užtikrinama, kad atliekamas nuodugnus vertinimas ir taikomi pritaikytosios privatumo apsaugos ir standartizuotosios privatumo apsaugos principai.*

b. Ar kriterijai atitinka duomenų tvarkymo operacijos mastą, atsižvelgiant į sertifikavimo mechanizmo taikymo sritį, informacijos slaptumą ir tvarkymo riziką?

c. Ar tikėtina, kad dėl šių kriterijų duomenų valdytojai ir duomenų tvarkytojai geriau laikysis duomenų apsaugos reikalavimų?

d. Ar bus geriau užtikrintos duomenų subjektų teisės į informaciją, įskaitant paaiškinimą duomenų subjektams, kokių rezultatų norima?