|  |
| --- |
| Praktikos egzamino vaizdo ir garso duomenų tvarkymo sprendimo viešojo pirkimo sutarties Nr.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  3 priedas |

(Projektas)

**STANDARTINĖS SUTARČIŲ SĄLYGOS ASMENS DUOMENŲ TVARKYMO SUTARTYSE**

202\_ m. \_\_\_\_\_ d.

Vilnius

**Akcinė bendrovė „Regitra“**, juridinio asmens kodas 110078991, buveinės adresas Liepkalnio g. 97A, LT-02121 Vilnius, tel. +370 5 219 0173, el. p. regitra@regitra.lt, [duomenų valdytojui atstovaujančio asmens vardas ir pavardė, pareigos, atstovavimo pagrindas] (toliau – duomenų valdytojas),

ir

[**duomenų tvarkytojo pavadinimas**, kodas, buveinės adresas, telefono ryšio numeris ir elektroninio pašto adresas; jeigu duomenų tvarkytojas fizinis asmuo – vardas ir pavardė, individualios veiklos pažymėjimo arba verslo liudijimo numeris, gyvenamosios vietos adresas, telefono ryšio numeris ir elektroninio pašto adresas], atstovaujamas [duomenų tvarkytojui atstovaujančio asmens vardas ir pavardė, pareigos, atstovavimo pagrindas] (toliau – duomenų tvarkytojas),

kiekvienas atskirai vadinamas „Šalimi“, o kartu „Šalimis“,

* vadovaudamosi 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas (ES) 2016/679),

**susitarė** dėl standartinių sutarčių sąlygų asmens duomenų tvarkymo sutartyse (toliau – Sąlygos), kurias sudaro Sąlygose nurodyti ir Sąlygų galiojimo laikotarpiu sudaryti priedai.

**I SKYRIUS**

**SĄLYGŲ TIKSLAS**

1. Siekiant įgyvendinti Reglamento (ES) 2016/679 28 straipsnio 3 dalį, nustatomos duomenų valdytojo ir duomenų tvarkytojo teisės bei pareigos, duomenų valdytojo vardu tvarkant asmens duomenis. Sąlygomis turi būti siekiama apsaugoti duomenų subjektų teises, mažinti konkrečią asmens duomenų apsaugos riziką ir užtikrinti duomenų valdytojo ir duomenų tvarkytojo santykių bei atitinkamų teisių ir pareigų aiškumą.

2. Teikdamas praktikos egzaminų (t. y. vaizdo su garsu ir kitais parametrais) įrašymo ir saugojimo paslaugas, duomenų tvarkytojas tvarkys asmens duomenis duomenų valdytojo vardu pagal šias Sąlygas. Asmens duomenų tvarkymo sąlygos nustatytos Sąlygų 1 priede.

**II SKYRIUS**

**ŠALIŲ ĮSIPAREIGOJIMAI**

3. Duomenų valdytojas:

3.1. įsipareigoja užtikrinti, kad asmens duomenys būtų tvarkomi laikantis Reglamento (ES) 2016/679 (žr. Reglamento (ES) 2016/679 24 straipsnį), kitų asmens duomenų apsaugą ir (ar) tvarkymą reglamentuojančių Europos Sąjungos ar jos valstybės narės[[1]](#footnote-2) teisės aktų ir šių Sąlygų;

3.2. turi teisę ir pareigą priimti sprendimus dėl asmens duomenų tvarkymo tikslų ir priemonių;

3.3. yra atsakingas, įskaitant, bet neapsiribojant, už tai, kad asmens duomenų tvarkymas, kurį duomenų tvarkytojui pavesta atlikti, turėtų teisinį pagrindą;

3.4. įsipareigoja bendradarbiauti su duomenų tvarkytoju dėl atliekamo asmens duomenų tvarkymo ir esant poreikiui, duoti papildomus nurodymus dėl asmens duomenų tvarkymo bei suteikti reikiamą informaciją, susijusią su šios Sutarties pagrindu tvarkomais asmens duomenimis, pagal šios Sutarties ir teisės aktų reikalavimus, jei tokios informacijos reikia duomenų tvarkytojo vykdomoms tvarkymo operacijoms užtikrinti.

4. Duomenų tvarkytojas įsipareigoja:

4.1. tvarkyti asmens duomenis tik pagal duomenų valdytojo pateiktus dokumentais įformintus nurodymus, išskyrus atvejus, kai to reikalaujama pagal Europos Sąjungos ar jos valstybės narės teisės aktus, kurie yra taikomi duomenų tvarkytojui (tokiais atvejais duomenų tvarkytojas informuoja duomenų valdytoją apie šiuos reikalavimus, išskyrus atvejus, kai teisės aktai draudžiama minėtą informaciją pateikti dėl svarbaus viešojo intereso). Tokie nurodymai pateikti Sąlygų 1 ir 3 prieduose. duomenų valdytojas taip pat gali pateikti tolesnius nurodymus viso asmens duomenų tvarkymo metu, tačiau tokie su Sąlygomis susiję nurodymai visada turi būti pagrįsti dokumentais;

4.2. tvarkyti asmens duomenis tik ta apimtimi ir laikotarpiu, kiek tai yra būtina siekiant tinkamai įvykdyti duomenų valdytojo nurodymus. Duomenų tvarkytojas neturi teisės tvarkyti asmens duomenų jokiais kitais tikslais, nei numatyta šioje ir (ar) šalių sudarytoje paslaugų teikimo sutartyje, nebent toks leidimas aiškiai nurodomas atskiru duomenų valdytojo nurodymu raštu.

4.3. bendradarbiauti su duomenų valdytoju ir nedelsiant, pagal jo prašymą, pateikti visą reikiamą su asmens duomenų tvarkymu susijusią informaciją bei vykdyti kitus duomenų valdytojo nurodymus dėl asmens duomenų tvarkymo. Informacija pateikiama ir nurodymai vykdomi per duomenų valdytojo nurodytą terminą, nebent Šalys suderina kitą terminą. Visi duomenų valdytojo nurodymai duomenų tvarkytojui turi būti dokumentuoti;

4.4. tuo atveju, kai įgaliotos valstybės institucijos ar bet kuris kitas asmuo, įskaitant duomenų subjektą, prašo duomenų tvarkytojo pateikti tvarkomus asmens duomenis ar kitą susijusią informaciją, duomenų tvarkytojas privalo nedelsiant tokį prašymą perduoti duomenų valdytojui. Prieš teikiant bet kokį atsakymą įgaliotai valstybės institucijai, duomenų tvarkytojas konsultuojasi su duomenų valdytoju ir atsižvelgia į duomenų valdytojo paaiškinimus, išskyrus atvejus, kai tokios informacijos atskleidimas duomenų valdytojui prieštarautų Europos Sąjungos ar jos valstybių narių teisės aktams;

4.5. nedelsiant informuoti duomenų valdytoją, jei duomenų valdytojo nurodymai, duomenų tvarkytojo nuomone, prieštarauja Reglamentui (ES) 2016/679 arba kitiems asmens duomenų apsaugą reglamentuojantiems Europos Sąjungos ar jos valstybių narių teisės aktams;

4.6. tvarkyti su asmens duomenų tvarkymo veikla, vykdoma duomenų valdytojo vardu, susijusius įrašus. Ši pareiga taikoma kiekvienam duomenų tvarkytojui ir, kai taikoma, duomenų tvarkytojo atstovui pagal Reglamento (ES) 2016/679 30 straipsnio 2 dalį.

5. Šios Sąlygos neatleidžia Šalių nuo kitų pareigų, kurios joms taikomos pagal Reglamentą (ES) 2016/679 ar kitus teisės aktus.

**III SKYRIUS**

**KONFIDENCIALUMAS**

6. Duomenų tvarkytojas prieigą prie duomenų valdytojo vardu tvarkomų asmens duomenų suteikia tik tiems asmenims, kuriems vadovauja duomenų tvarkytojas, ir kurie yra įpareigoti laikytis konfidencialumo arba kuriems taikoma teisinė konfidencialumo pareiga, ir tik tuo atveju, jei jiems būtina su jais susipažinti. Šalys užtikrina, kad:

6.1. Pasikeitus asmenims, kurie tvarko asmens duomenis, jų prieigos teisės prie duomenų valdytojo asmens duomenų panaikinamos ne vėliau nei paskutinę jo užduočių, dėl kurių jiems būtina prieiga prie duomenų valdytojo asmens duomenų, patikėtų tvarkyti duomenų tvarkytojui, dieną, o tuo atveju jei nutrūksta duomenų tvarkytojo darbuotojo darbo santykiai – ne vėliau nei paskutinę jo darbo dieną.

6.2. Asmenų, kuriems suteikta prieiga prie asmens duomenų, sąrašas turi būti periodiškai peržiūrimas ne rečiau kaip kartą kas 6 mėnesius. Vadovaujantis šia peržiūra, tokia prieiga prie asmens duomenų panaikinama, jei tokia prieiga nebereikalinga, todėl asmens duomenys nebegalės būti prieinami tiems asmenims.

7. Duomenų tvarkytojas duomenų valdytojo prašymu įrodo, kad asmenims, kuriems vadovauja duomenų tvarkytojas ir kuriems pavesta tvarkyti asmens duomenis, taikoma Sąlygų 6 punkte nurodyta konfidencialumo pareiga.

**IV SKYRIUS**

**DUOMENŲ TVARKYMO SAUGUMAS**

8. Vadovaujantis Reglamento (ES) 2016/679 32 straipsniu, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, atsižvelgiant į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms.

9. Duomenų valdytojas įvertina fizinių asmenų teisėms ir laisvėms galinčią kilti riziką tvarkant asmens duomenis ir įgyvendina priemones šiai rizikai sumažinti. Priklausomai nuo jų tinkamumo, priemonės gali būti šios:

9.1. asmens duomenų pseudonimizavimas ir (ar) šifravimas;

9.2. galimybė užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;

9.3. galimybė laiku atkurti prieinamumą ir prieigą prie asmens duomenų, įvykus fiziniam ar techniniam incidentui;

9.4. techninių ir organizacinių priemonių, užtikrinančių duomenų tvarkymo saugumą, reguliaraus testavimo, tikrinimo ir įvertinimo procesas.

10. Pagal Reglamento (ES) 2016/679 32 straipsnį duomenų tvarkytojas, nepriklausomai nuo duomenų valdytojo, taip pat įvertina duomenų tvarkymo riziką, susijusią su asmens duomenų tvarkymo veikla, kuriai atlikti duomenų valdytojas pasitelkė duomenų tvarkytoją, galinčią kilti fizinių asmenų teisėms ir laisvėms, ir įgyvendina priemones šiai rizikai sumažinti. Šiuo tikslu duomenų valdytojas duomenų tvarkytojui pateikia visą informaciją, reikalingą tokiai rizikai nustatyti ir įvertinti.

11. Be to, duomenų tvarkytojas padeda duomenų valdytojui užtikrinti duomenų valdytojo pareigų pagal Reglamento (ES) 2016/679 32 straipsnį vykdymą, teikdamas *inter alia* duomenų valdytojui informaciją apie technines ir organizacines priemones, kurias duomenų tvarkytojas jau įgyvendino pagal Reglamento (ES) 2016/679 32 straipsnį kartu su visa kita informacija, reikalinga duomenų valdytojui įvykdyti duomenų valdytojo pareigas pagal Reglamento (ES) 2016/679 32 straipsnį.

**V SKYRIUS**

**KITŲ DUOMENŲ TVARKYTOJŲ PASITELKIMAS**

12. Duomenų tvarkytojas turi laikytis Reglamento (ES) 2016/679 28 straipsnio 2 ir 4 dalyse nurodytų reikalavimų, kad galėtų pasitelkti kitą duomenų tvarkytoją (toliau – pagalbinis duomenų tvarkytojas).

13. Duomenų valdytojo sąlygos, kuriomis vadovaujantis duomenų tvarkytojas galės pasitelkti pagalbinius duomenų tvarkytojus, ir duomenų valdytojo įgaliotų pagalbinių duomenų tvarkytojų sąrašas pateikiamos Sąlygų 2 priede.

14. Duomenų tvarkytojas nepasitelkia pagalbinio duomenų tvarkytojo asmens duomenų tvarkymui pagal šias Sąlygas be išankstinio specialaus duomenų valdytojo rašytinio leidimo:

14.1. Duomenų tvarkytojas pasitelkia pagalbinius duomenų tvarkytojus tik gavęs specialų išankstinį duomenų valdytojo leidimą. Duomenų tvarkytojas turi raštu pateikti prašymą dėl specialaus leidimo bent jau 14 darbo dienų iki atitinkamo pagalbinio duomenų tvarkytojo pasitelkimo.

14.2. Jei duomenų valdytojas prieštarauja dėl asmens duomenų perdavimo pagalbiniam duomenų tvarkytojui, duomenų tvarkytojas privalo toliau vykdyti savo įsipareigojimus duomenų valdytojui pagal sudarytas sutartis.

15. Kai duomenų tvarkytojas konkrečiai duomenų tvarkymo veiklai duomenų valdytojo vardu atlikti pasitelkia pagalbinį duomenų tvarkytoją, sutartimi ar kitu teisės aktu pagal Sąjungos ar valstybės narės teisę, tam pagalbiniam duomenų tvarkytojui nustatomos tos pačios duomenų apsaugos prievolės, kaip ir prievolės, nustatytos Sąlygose ar kitame teisės akte, visų pirma prievolė pakankamai užtikrinti, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų Sąlygų ir Reglamento (ES) 2016/679 reikalavimus. Prieš pradėdamas tvarkyti asmens duomenis, duomenų tvarkytojas informuoja pagalbinį duomenų tvarkytoją apie tai, kurio duomenų valdytojo asmens duomenų tvarkymui jis yra pasitelkiamas, nurodydamas duomenų valdytojo tapatybę ir kontaktinius duomenis.

16. Sąlygų su pagalbiniu duomenų tvarkytoju kopija ir jos vėlesni pakeitimai, duomenų valdytojo prašymu, pateikiami duomenų valdytojui, tokiu būdu suteikiant duomenų valdytojui galimybę užtikrinti, kad pagalbiniam duomenų tvarkytojui taikomos tos pačios duomenų apsaugos prievolės, kaip yra nustatyta Sąlygose. Duomenų tvarkytojas turi informuoti duomenų valdytoją apie visus netinkamo pagalbinio duomenų tvarkytojo pareigų, nustatytų tokia sutartimi ar kitu teisės aktu, atvejus. duomenų valdytojui nėra privaloma pateikti asmens duomenų tvarkymo sutarties dėl su verslu susijusių nuostatų, kurios nedaro įtakos su pagalbiniu duomenų tvarkytoju sudarytos sutarties teisinėms asmens duomenų apsaugos sąlygoms.

17. Duomenų tvarkytojas turi susitarti su pagalbiniu duomenų tvarkytoju, jei toks pasitelkiamas, kad pirminio duomenų tvarkytojo bankroto atveju, duomenų valdytojas turi teisę tęsti duomenų tvarkymo santykius su pirminio duomenų tvarkytojo pasitelktu pagalbiniu duomenų tvarkytoju tiesiogiai ir (arba) teikti tiesioginius nurodymus dėl duomenų tvarkymo, pavyzdžiui, nurodyti pagalbiniam duomenų valdytojui ištrinti arba grąžinti asmens duomenis.

18. Duomenų tvarkytojas yra atsakingas už reikalavimą, kad pagalbinis duomenų tvarkytojas laikytųsi bent tų pareigų, kurios duomenų tvarkytojui taikomos pagal Sąlygas ir Reglamentą (ES) 2016/679. Jei pagalbinis duomenų tvarkytojas nevykdo asmens duomenų apsaugos prievolių, pirminis duomenų tvarkytojas, su kuriuo sudaryta asmens duomenų tvarkymo sutartis, išlieka visiškai atsakingas duomenų valdytojui už pagalbinio duomenų tvarkytojo prievolių vykdymą. Tai nedaro įtakos duomenų subjektų teisėms pagal Reglamentą (ES) 2016/679, ypač Reglamento (ES) 2016/679 79 ir 82 straipsniuose numatytoms teisėms, duomenų valdytojo ir duomenų tvarkytojo, įskaitant pagalbinius duomenų tvarkytojus, atžvilgiu.

**VI SKYRIUS**

**DUOMENŲ PERDAVIMAS Į TREČIĄSIAS VALSTYBES**[[2]](#footnote-3) **ARBA TARPTAUTINĖMS ORGANIZACIJOMS**

19. Duomenų tvarkytojas asmens duomenis gali perduoti į trečiąsias valstybes ar tarptautinėms organizacijoms tik gavęs duomenų valdytojo dokumentais įformintus nurodymus ir laikantis Reglamento (ES) 2016/679 V skyriaus reikalavimų.

20. Jei asmens duomenis trečiosioms valstybėms ar tarptautinėms organizacijoms reikia perduoti pagal Europos Sąjungos ar jos valstybės narės teisės aktus, kurių turi laikytis duomenų tvarkytojas, nors duomenų valdytojas nedavė nurodymų duomenų tvarkytojui tai atlikti, duomenų tvarkytojas informuoja duomenų valdytoją apie šį teisinį reikalavimą prieš duomenų perdavimą, nebent tas teisės aktas draudžia perduoti tokią informaciją.

21. Duomenų tvarkytojas be duomenų valdytojo dokumentais įformintų nurodymų arba be konkretaus reikalavimo pagal Europos Sąjungos ar jos valstybės narės teisės aktus negali pagal šias Sąlygas:

21.1. perduoti asmens duomenis duomenų valdytojui ar duomenų tvarkytojui trečiojoje valstybėje ar tarptautinėje organizacijoje;

21.2. perduoti asmens duomenų tvarkymą pagalbiniam duomenų tvarkytojui trečiojoje valstybėje;

21.3. leisti, kad asmens duomenis tvarkytų duomenų tvarkytojas trečiojoje valstybėje.

22. Duomenų valdytojo nurodymai ar leidimai dėl asmens duomenų perdavimo į trečiąją valstybę, įskaitant, jei taikoma, asmens duomenų perdavimo į trečiąsias valstybes Reglamento (ES) 2016/679 V skyriuje nustatytus pagrindai, kuriais duomenų valdytojo nurodymai yra grindžiami, pateikiami Sąlygų 3 priede.

23. Šios Sąlygos nėra standartinės duomenų apsaugos sąlygos, apibrėžtos Reglamento (ES) 2016/679 46 straipsnio 2 dalies c ir d punktuose, ir šalys negali remtis Sąlygomis kaip asmens duomenų perdavimo į trečiąsias valstybes ar tarptautinėms organizacijoms pagrindu pagal Reglamento (ES) 2016/679 V skyrių.

**VII SKYRIUS**

**PAGALBA DUOMENŲ VALDYTOJUI**

24. Atsižvelgdamas į duomenų tvarkymo pobūdį, duomenų tvarkytojas, kiek tai įmanoma, padeda duomenų valdytojui tinkamomis techninėmis ir organizacinėmis priemonėmis įvykdyti duomenų valdytojo prievoles atsakyti į prašymus naudotis duomenų subjekto teisėmis, nustatytomis Reglamento (ES) 2016/679 III skyriuje. Tai reiškia, kad duomenų tvarkytojas, kiek tai įmanoma, padeda duomenų valdytojui, kad duomenų valdytojas įgyvendintų:

24.1. teisę būti informuotam renkant asmens duomenis iš duomenų subjekto;

24.2. teisę būti informuotam, kai asmens duomenys yra gauti ne iš duomenų subjekto;

24.3. teisę susipažinti su duomenimis;

24.4. teisę reikalauti ištaisyti duomenis;

24.5. teisę reikalauti ištrinti duomenis („teisę būti pamirštam“);

24.6. teisę apriboti duomenų tvarkymą;

24.7. prievolę pranešti apie asmens duomenų ištaisymą ar ištrynimą arba duomenų tvarkymo apribojimą;

24.8. teisę į duomenų perkeliamumą;

24.9. teisę nesutikti su duomenų tvarkymu;

24.10. teisę, kad nebūtų taikomi sprendimai, pagrįsti vien automatiniu tvarkymu, įskaitant profiliavimą.

25. Be duomenų tvarkytojo prievolės padėti duomenų valdytojui pagal Sąlygų 11 punktą, duomenų tvarkytojas, atsižvelgdamas į tvarkymo pobūdį ir duomenų tvarkytojui prieinamą informaciją, taip pat padeda duomenų valdytojui užtikrinti:

25.1. Duomenų valdytojo pareigą nedelsiant ir, jei įmanoma, ne vėliau kaip per 72 valandas po to, kai apie tai sužinojo, pranešti apie asmens duomenų saugumo pažeidimą kompetentingai priežiūros institucijai – Valstybinei duomenų apsaugos inspekcijai, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms;

25.2. Duomenų valdytojo pareigą nepagrįstai nedelsiant pranešti duomenų subjektui apie asmens duomenų pažeidimą, kai asmens duomenų saugumo pažeidimas gali sukelti didelę riziką fizinių asmenų teisėms ir laisvėms;

25.3. Duomenų valdytojo pareigą atlikti numatytų asmens duomenų tvarkymo operacijų poveikio duomenų apsaugai vertinimą, kai asmens duomenų tvarkymo būdas gali sukelti didelę riziką fizinių asmenų teisėms ir laisvėms;

25.4. Duomenų valdytojo pareigą konsultuotis su kompetentinga priežiūros institucija – Valstybine duomenų apsaugos inspekcija prieš pradedant duomenų tvarkymą, jei poveikio duomenų apsaugos vertinimas rodo, kad duomenų tvarkymas sukeltų didelę riziką, jei duomenų valdytojas nesiimtų priemonių tai rizikai sumažinti.

26. Šalys Sąlygų 3 priede nustato tinkamas technines ir organizacines priemones, kurias turi taikyti duomenų tvarkytojas siekiant padėti duomenų valdytojui įgyvendinti duomenų subjekto teises ir vykdyti Reglamento (ES) 2016/679 33–36 straipsniuose įtvirtintas pareigas. Tai taikoma prievolėms, nurodytoms Sąlygų 25 punkte.

**VIII SKYRIUS**

**PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

27. Duomenų tvarkytojas, sužinojęs apie asmens duomenų saugumo pažeidimą, nepagrįstai nedelsdamas apie tai praneša duomenų valdytojui. Duomenų tvarkytojas praneša duomenų valdytojui per 24 (dvidešimt keturias) valandas po to, kai duomenų tvarkytojas sužinojo apie asmens duomenų saugumo pažeidimą, kad duomenų valdytojas galėtų įvykdyti duomenų valdytojo pareigą pranešti apie asmens duomenų saugumo pažeidimą kompetentingai priežiūros institucijai, pagal Reglamento (ES) 2016/679 33 straipsnį.

28. Sąlygų 25.1 papunktyje nurodyta duomenų tvarkytojo pareiga padėti duomenų valdytojui pranešti kompetentingai priežiūros institucijai apie asmens duomenų pažeidimą reiškia, kad duomenų tvarkytojas privalo duomenų valdytojui padėti gauti toliau išvardytą informaciją, kuri, remiantis Reglamento (ES) 2016/679 33 straipsnio 3 dalimi, turi būti nurodyta duomenų valdytojo pranešime kompetentingai priežiūros institucijai:

28.1. asmens duomenų pobūdis, įskaitant, jei įmanoma, atitinkamų duomenų subjektų kategorijos ir apytikslis jų skaičius bei atitinkamų asmens duomenų kategorijos ir apytikslis skaičius;

28.2. tikėtinos asmens duomenų pažeidimo pasekmės;

28.3. priemonės, kurių ėmėsi ar siūlo imtis duomenų valdytojas dėl asmens duomenų pažeidimo, įskaitant, jei reikia, priemones, skirtas sušvelninti galimą neigiamą pažeidimo poveikį;

28.4. bet kokia kita reikšminga informacija, kuri yra ar gali būti reikalinga duomenų valdytojui rengiant pranešimą arba atsakant į papildomus su asmens duomenų saugumo pažeidimu susijusius kompetentingos priežiūros institucijos raštus.

29. Sąlygų 3 priede nustatomi visi elementai, kuriuos turi pateikti duomenų tvarkytojas, padėdamas duomenų valdytojui pranešti kompetentingai priežiūros institucijai apie asmens duomenų saugumo pažeidimą. Jei duomenų tvarkytojas duomenų valdytojui pateikia ne visą informaciją apie asmens duomenų saugumo pažeidimą arba vėliau paaiškėja papildoma informacija, duomenų tvarkytojas privalo nepagrįstai nedelsdamas, bet ne vėliau kaip per 48 (keturiasdešimt aštuonias) valandas pateikti papildomą pranešimą duomenų valdytojui, nurodydamas visą trūkstamą informaciją.

30. Duomenų tvarkytojas duomenų valdytojo prašymu, papildomai prie Sąlygų 28 punkte nurodytos informacijos, pateikia dokumentų, pavyzdžiui, pagrindžiančių atliktus veiksmus, taikytas priemones ar atliktus vidinius patikrinimus ir jų išvadų, kopijas.

31. Duomenų tvarkytojas įsipareigoja imtis visų priemonių, kad padėtų duomenų valdytojui asmens duomenų saugumo pažeidimo atveju, siekiant sumažinti asmens duomenų saugumo pažeidimo neigiamas pasekmes, įskaitant dokumentavimą.

32. Duomenų tvarkytojas privalo skubiai pašalinti problemą ir užkirsti kelią tolesnei žalai, taip pat sumažinti tokio incidento padarinius, taip pat gavęs duomenų valdytojo nurodymus pritaikyti ir kitas taisomąsias priemones, skirtas užkirsti kelią analogiškiems incidentams.

33. Duomenų tvarkytojas turi dokumentuoti visus asmens duomenų saugumo pažeidimus, įtariamus pažeidimus, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kurių buvo imtasi. Toks dokumentavimas turi suteikti galimybę priežiūros institucijai patikrinti Reglamento (ES) 2016/679 ir kitų asmens duomenų apsaugos teisės aktų laikymąsi. Duomenų valdytojui pareikalavus, duomenų tvarkytojas turi pateikti šiuos dokumentus susipažinti, ypatingai, kai to reikalauja priežiūros institucija.

**IX SKYRIUS**

**DUOMENŲ TRYNIMAS IR GRĄŽINIMAS**

34. Pasibaigus asmens duomenų tvarkymo paslaugų teikimui, duomenų tvarkytojas privalo ištrinti visus asmens duomenis, tvarkomus duomenų valdytojo vardu, ir įrodyti duomenų valdytojui, kad tai padarė, nebent asmens duomenis reikia saugoti pagal Europos Sąjungos ar jos valstybės narės teisės aktus.

**X SKYRIUS**

**DUOMENŲ TVARKYTOJO AUDITAS IR TIKRINIMAS**

35. Duomenų tvarkytojas duomenų valdytojui suteikia visą informaciją, reikalingą įrodyti, kad laikomasi Reglamento (ES) 2016/679 28 straipsnyje ir Sąlygose nustatytų pareigų, ir sudaro sąlygas ir padeda atlikti duomenų valdytojui ar kitam duomenų valdytojo įgaliotam auditoriui auditą, įskaitant patikrinimus vietoje.

36. Duomenų valdytojo atliekamam duomenų tvarkytojo ir pagalbinių duomenų tvarkytojų auditui, įskaitant patikrinimus, taikomos Sąlygų 3 Priedo 7 ir 8 punktuose nurodytos procedūros.

37. Duomenų tvarkytojas turi suteikti priežiūros institucijoms, kurios pagal galiojančius teisės aktus turi prieigą prie duomenų valdytojo ir duomenų tvarkytojo įrenginių, arba atstovams, veikiantiems tokių priežiūros institucijų vardu, prieigą prie duomenų tvarkytojo fizinių priemonių ar atlikti kitus priežiūros institucijų nurodytus veiksmus auditui ar kitam patikrinimui atlikti. Šalys turi kompetentingų priežiūros institucijų prašymu pateikti šiose Sąlygose nurodytą informaciją, įskaitant auditų rezultatus.

**XI SKYRIUS**

**ATSAKOMYBĖ IR GINČŲ SPRENDIMAS**

38. Duomenų tvarkytojas yra atsakingas už visas sąnaudas, išlaidas, kompensacijas, žalą ir nuostolius, kuriuos duomenų valdytojui, duomenų valdytojo klientui, partneriui ar trečiajai šaliai padaro duomenų tvarkytojas, jo darbuotojas arba pagalbinis duomenų tvarkytojas netinkamai vykdant / pažeidžiant šią Sutartį, duomenų valdytojo nurodymus ir / ar Asmens duomenų apsaugos teisės aktus.

39. Visi šalių ginčai bus sprendžiami derybų būdu. Nepavykus ginčo išspręsti derybų būdu, ginčas sprendžiamas kompetentingame teisme pagal duomenų valdytojo registruotos buveinės adresą, vadovaujantis duomenų valdytojo šalies nacionaline teise.

**XI SKYRIUS**

**BAIGIAMOSIOS NUOSTATOS**

40. Sąlygos įsigalioja nuo jų pasirašymo dienos.

41. Asmens duomenų tvarkymo paslaugų teikimo laikotarpiu Sąlygos negali būti nutrauktos, jei šalys nėra susitarusios dėl kitų Sąlygų, reglamentuojančių asmens duomenų tvarkymo paslaugų teikimą.

42. Jei asmens duomenų tvarkymo paslaugų teikimas yra nutraukiamas, o asmens duomenys ištrinami pagal Sąlygų 34 punktą ir Sąlygų 3 Priedo 4 punktą, šios Sąlygos nutraukiamos automatiškai.

43. Nedarant poveikio jokioms Reglamento (ES) 2016/679 nuostatoms, duomenų tvarkytojui pažeidus pareigas pagal šias Sąlygas, duomenų valdytojas gali nurodyti duomenų tvarkytojui laikinai sustabdyti asmens duomenų tvarkymą, kol pastarasis laikysis šių Sąlygų arba Sąlygos bus nutrauktos. Duomenų tvarkytojas nedelsdamas informuoja duomenų valdytoją, jei dėl kokios nors priežasties jis negali vykdyti Sąlygų.

44. Duomenų valdytojas turi teisę nutraukti Sąlygas, jeigu:

44.1. Duomenų tvarkytojas iš esmės arba nuolat pažeidžia Sąlygas arba savo įsipareigojimus pagal Reglamentą (ES) 2016/679;

44.2. Duomenų tvarkytojas nesilaiko privalomo teismo arba priežiūros institucijos sprendimo dėl savo įsipareigojimų pagal Sąlygas arba Reglamentą (ES) 2016/679;

44.3. Duomenų tvarkytojas per protingą terminą neištaiso patikrinimo metu nustatytų trūkumų bei neįgyvendina nurodytų papildomų priemonių;

44.4. Duomenų valdytojas sustabdė duomenų tvarkytojo atliekamą asmens duomenų tvarkymą pagal Sąlygų 44.1, 44.2 ir (ar) 44.3. papunkčius ir atitiktis šioms Sąlygoms nėra atkurta per 14 darbo dienų.

45. Sąlygos turi pirmenybę prieš bet kokias panašias su asmens duomenų tvarkymu susijusias nuostatas kituose Šalių susitarimuose.

46. Kiekviena šalis paskiria asmenį, atsakingą už Sąlygų vykdymą:

46.1. Duomenų tvarkytojo atstovas: [pareigos] [vardas, pavardė], tel. [telefono numeris], el. paštas: [el. pašto adresas].

46.2. Duomenų valdytojo atstovas: [pareigos] [vardas, pavardė], tel. [telefono numeris], el. paštas: [el. pašto adresas].

**XII SKYRIUS**

**ŠALIŲ REKVIZITAI, PARAŠAI**

Duomenų valdytojo vardu: Duomenų tvarkytojo vardu:

*[pareigos [pareigos*

*vardas, pavardė vardas, pavardė*

*data] data]*

*A. V. A. V.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Standartinių sutarčių sąlygų asmens duomenų tvarkymo sutartyse

1 priedas

**INFORMACIJA APIE ASMENS DUOMENŲ TVARKYMĄ**

**1.Informacija apie asmens duomenų tvarkymą:**

**1.1. Duomenų tvarkytojo atliekamo asmens duomenų tvarkymo tikslas yra:**

Duomenų valdytojo organizuojamų vairavimo praktikos egzaminų (vaizdo su garsu ir kitais parametrais) įrašymas, įskaitant įrašymo sistemos priežiūrą ir įrašų saugojimą.

**1.2. Duomenų tvarkytojo asmens duomenų tvarkymas daugiausia susijęs su (tvarkymo pobūdžiu):**

1. Vaizdo su garsu (įskaitant kitus parametrus) įrašymo įrangos sistemos priežiūra (pvz., gedimų šalinimas jungiantis prie Sistemos ir (ar) įrangos ir (ar) kiti programinės įrangos priežiūros ir atnaujinimo darbai);
2. Vaizdo su garsu (įskaitant kitus parametrus) įrašų duomenų saugojimas duomenų tvarkytojo DC (įskaitant Sistemą).

**1.3. Duomenų tvarkymas apima šiuos asmens duomenis:**

Vaizdo (su garsu) stebėjimo duomenys užfiksuoti vairuotojų praktikos egzamino metu, transporto priemonėje (įskaitant egzaminuojamojo, egzaminuotojo ir (ar) trečiųjų asmenų veido atvaizdai, pokalbiai ir atliekami veiksmai).

Taip pat kiti įrašo parametrai: automobilio lokacijos koordinatės, Įrašo darymo data ir laikas (sekundės tikslumu), automobilio, kuriame veikia sumontuota Įranga, valstybinis numeris, informacija apie egzaminuotojo vietoje įrengtų papildomų pedalų paspaudimus (kuris pedalas ir kuriuo konkrečiu metu buvo nuspaustas).

**1.4. Duomenų tvarkymas apima šias duomenų subjektų kategorijas:**

Fiziniai asmenys (duomenų valdytojo klientai), laikantys praktikos vairavimo egzaminą, duomenų valdytojo darbuotojai, kiti praktikos vairavimo egzamino dalyviai (vertėjai).

**1.5. Duomenų tvarkytojas gali tvarkyti asmens duomenis duomenų valdytojo vardu, kai įsigalioja Sąlygos. Duomenų tvarkymo trukmė:**

Vaizdo su garsu (įskaitant kitus parametrus) įrašai duomenų tvarkytojo DC (įskaitant Sistemą) saugomi 6 mėnesius.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Standartinių sutarčių sąlygų dėl asmens duomenų tvarkymo sutartyse

2 priedas

**INFORMACIJA APIE PAGALBINIUS DUOMENŲ TVARKYTOJUS**

**1. Įgalioti pagalbiniai duomenų tvarkytojai:**

Įsigaliojus Sąlygoms, duomenų valdytojas leidžia pasitelkti šiuos pagalbinius duomenų tvarkytojus:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Pavadinimas, vardas, pavardė | Įmonės kodas / individualios veiklos pažymėjimo numeris arba verslo liudijimo numeris | Buveinės adresas / gyvenamosios vietos adresas | Asmens duomenų tvarkymo aprašymas  *(pvz., duomenų tvarkymo rūšis, tvarkomi asmens duomenys ir pan.)* | Asmens duomenų tvarkymo vieta |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Įsigaliojus Sąlygoms, duomenų valdytojas leidžia kitai šaliai Sąlygų 1 priedo 1.1 papunktyje nurodytais tikslais pasitelkti šiame Sąlygų priede nurodytus pagalbinius duomenų tvarkytojus, laikantis Sąlygų V skyriaus reikalavimų. Siekiant pasitelkti minėtus pagalbinius duomenų tvarkytojus asmens duomenų tvarkymui kitais tikslais nei tikslai, nustatyti Sąlygų 1 priedo 1.1 papunktyje, būtinas rašytinis duomenų valdytojo leidimas.

**2. Išankstinis pranešimas dėl leidimo suteikimo pagalbiniams duomenų tvarkytojams**

Duomenų tvarkytojas, norėdamas pasitelkti pagalbinį duomenų tvarkytoją Sąlygose nurodytų asmens duomenų tvarkymui, privalo duomenų valdytojui pateikti išankstinį pranešimą dėl leidimo suteikimo pagalbiniams duomenų tvarkytojams, bent 14 (keturiolika) darbo dienųiki atitinkamo pagalbinio duomenų tvarkytojo pasitelkimo. Pranešime, duomenų valdytojui, duomenų tvarkytojas pateikia informaciją susijusią su pagalbinio tvarkytojo tapatybe (pvz., pavadinimas / vardas ir pavardė; unikalų identifikatorių, adresu), asmens duomenų tvarkymo aprašymu bei kita su pagalbiniu tvarkytoju susijusia informacija. Duomenų valdytojas įvertinęs prašyme pateiktą informaciją, per 14 (keturiolika) darbo dienų, turi patvirtinti pagalbinį duomenų tvarkytoją bei suteikti leidimą asmens duomenų tvarkymui arba atsisakyti suteikti leidimą asmens nurodytam pagalbiniam duomenų tvarkytojui. Duomenų valdytojas, atsisakydamas suteikti leidimą, pateikia motyvuotą atsakymą, kodėl pagalbiniam duomenų tvarkytojui leidimas nebuvo suteiktas.

Duomenų tvarkytojas, gavęs leidimą pagalbinio duomenų tvarkytojo pasitelkimui, privalo nedelsiant, tačiau ne vėliau nei pagalbinio duomenų tvarkytojo asmens duomenų tvarkymo pradžios dieną, sudaryti rašytinę asmens duomenų tvarkymo sutartį su minėtu pagalbiniu duomenų tvarkytoju bei sudarytos sutarties sąlygas nedelsiant, bet ne vėliau nei per 3 (tris) darbo dienas perduoti duomenų valdytojui.

Duomenų tvarkytojas, norėdamas atnaujinti su pagalbiniu duomenų tvarkytoju sudarytą asmens duomenų tvarkymo sutartį, šios sutarties sąlygas privalo suderinti su duomenų valdytoju bei gauti leidimą minėtos sutarties atnaujinimui.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Standartinių sutarčių sąlygų dėl asmens duomenų tvarkymo sutartyse

3 priedas

**NURODYMAI, KAIP TVARKYTI ASMENS DUOMENIS**

**1. Duomenų tvarkymo nurodymas**

Duomenų tvarkytojas duomenų valdytojo vardu asmens duomenų tvarkymo metu atlieka šiuos veiksmus:

1. Vaizdo su garsu (įskaitant kitus parametrus) įrašymo įrangos sistemos priežiūra (pvz., gedimų šalinimas jungiantis prie Sistemos ir (ar) įrangos ir (ar) kiti programinės įrangos priežiūros ir atnaujinimo darbai);
2. Vaizdo su garsu (įskaitant kitus parametrus) įrašų duomenų saugojimas duomenų tvarkytojo DC (įskaitant Sistemą).

**2. Duomenų tvarkymo saugumas**

Atsižvelgiant į tai, kad atlikus asmens duomenų tvarkymo operacijos ir duomenų valdytojo pobūdžio grėsmės atsiradimo tikimybę bei galimą (tikėtiną) poveikį buvo nustatytas „aukštas“ rizikos lygis, asmens duomenų tvarkymui turėtų būti taikomas „aukštas“ saugumo lygis.

Duomenų tvarkytojas turi teisę ir privalo priimti sprendimus dėl techninių ir organizacinių saugumo priemonių naudojimo užtikrinti reikiamą (ir suderintą) duomenų saugumo lygį.

Tačiau duomenų tvarkytojas bet kuriuo atveju įgyvendina šias su duomenų valdytoju suderintas priemones:

|  |
| --- |
| **Paaiškinimai** |
| |  | | --- | | *Taikoma visoms rizikos lygio sistemoms (Ž, V, A)* | | *Taikoma jeigu sistema vidutinio rizikos lygio: (Ž, V, A), (V, A)* | | *Taikoma jeigu sistema aukšto rizikos lygio: (Ž, V, A), (V, A), (A)* |   *Ž – žemas rizikos lygis*  *V – vidutinis rizikos lygis*  *A – aukštas rizikos lygis* |

|  |
| --- |
| **Techninės ir organizacinės saugumo priemonės** |
|
| **Saugumo politika ir asmens duomenų apsaugai skirtos procedūros** |
| Asmens duomenų ir jų tvarkymo saugumas organizacijoje turi būti dokumentuotas kaip informacijos saugumo politikos dalis. (Ž, V, A) |
| Turėti atskirą specialią saugumo politiką, skirtą asmens duomenų tvarkymui, kurią patvirtino vadovybė, o visi darbuotojai ir susijusios išorinės šalys yra su ja supažindintos. *(V, A)* |
| Saugumo politikoje aptartos bent jau personalo funkcijos ir atsakomybės, asmens duomenų saugumui užtikrinti priimtos pradinės techninės ir organizacinės priemonės, duomenų tvarkytojai ar kitos šalys, dalyvaujančios tvarkant asmens duomenis. *(V, A)* |
| Saugumo politika turi būti peržiūrima ir prireikus, tikslinama kas pusmetį. *(A)* |
| **Vaidmenys ir atsakomybės** |
| Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal saugumo politiką. *(Ž, V, A)* |
| Turi būti aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras (vidaus organizacijos pertvarkymo ar darbuotojų atleidimo, funkcijų pasikeitimo metu). *(Ž, V, A)* |
| Reikėtų atlikti aiškų asmenų, atsakingų už konkrečias saugumo užduotis, paskyrimą, įskaitant saugos specialisto (saugos įgaliotinio) paskyrimą. *(V, A)* |
| Saugos specialistas turi būti oficialiai paskirtas (paskyrimą patvirtinant dokumentais). Saugos specialisto uždaviniai ir atsakomybės turi būti aiškiai nustatyti ir dokumentuoti *(A)* |
| Nesuderinamos pareigybės (funkcijos) ir atsakomybių sritys, pavyzdžiui, saugos specialisto pareigybė ir duomenų apsaugos pareigūno pareigybė, turi būti atskirtos, siekiant sumažinti neleistino ar netyčinio asmens duomenų keitimo ar netinkamo naudojimo galimybes. *(A)* |
| **Prieigos valdymas vietoje** |
| Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. need to know) principu. *(Ž, V, A)* |
| Būtina užtikrinti, kad prieigos kontrolės politika būtų detalizuota bei dokumentuota ir tame dokumente konkrečioms naudotojų pareigybėms būtų nustatytos atitinkamos prieigos kontrolės taisyklės, prieigos teisės ir apribojimai su asmens duomenų tvarkymu susijusių procesų ir procedūrų atžvilgiu. *(V, A)* |
| Prieigos kontrolę užtikrinančių funkcijų atskyrimas (pvz., prieigos užklausų, prieigos leidimų, pačios prieigos administravimas) turi būti aiškiai apibrėžtas ir dokumentuotas. *(V, A)* |
| Tam tikros pareigybės (funkcijos), turinčios dideles prieigos teises, turi būti aiškiai apibrėžtos ir priskirtos tik ribotam darbuotojų skaičiui. *(A)* |
| **Išteklių ir turto valdymas** |
| Turėti IT išteklių (naudojamų asmens duomenims tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą). IT išteklių registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę). IT išteklių registro tvarkymas turi būti priskirtas konkrečiam asmeniui, pvz., IT specialistui. *(Ž, V, A)* |
| IT išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas. Rekomenduojamas peržiūros dažnumas – kartą per 3 mėnesius. *(V, A)* |
| Visos pareigybės, turinčios prieigą prie IT išteklių, turi būti apibrėžtos ir patvirtintos dokumentais. *(V, A)* |
| **Pasikeitimų IT aplinkoje valdymas** |
| Būtina užtikrinti, kad visi IT sistemų pakeitimai būtų stebimi ir registruojami konkretaus asmens (pvz., IT arba saugos specialisto) bei vykdyti reguliarią šio proceso stebėsena. *(Ž, V, A)* |
| Turi būti įdiegta išsami ir dokumentais pagrįsta IT keitimų valdymo politika. Keitimų valdymo politiką turi apibrėžti: pokyčių įvedimo ir įdiegimo procedūras, pareigybes ir vartotojus, kurių teisės buvo pakeistos, pokyčių įdiegimo laiko terminus. Pokyčių valdymo politika turi būti reguliariai atnaujinama *(V, A)* |
| **Duomenų tvarkytojai** |
| Prieš pradedant duomenų tvarkymą, duomenų tvarkytojas ir subrangovas (pagalbinis duomenų tvarkytojas) turi būti apibrėžę, dokumentavę ir susitarę dėl formalių gairių ir procedūrų, kurios taikomos tais atvejais, kai asmens duomenis tvarko subrangovai. Šios gairės ir procedūros privaloma tvarka turi nustatyti tą patį asmens duomenų saugumo lygį, kokio yra reikalaujama pagal duomenų tvarkytojo ir duomenų valdytojo sudarytą duomenų tvarkymo sutartį. *(Ž, V, A)* |
| Turi būti formaliai su subrangovu sutarta, kad nustačius asmens duomenų saugumo pažeidimą, subrangovas apie tai nedelsdamas praneša duomenų tvarkytojui. *(Ž, V, A)* |
| Turi būti susitarta dėl formalių reikalavimų ir prievolių, kurios taikomos tarp duomenų tvarkytojo ir subrangovų. Pagal susitarimą, subrangovas turi pateikti dokumentais pagrįstus įrodymus dėl atitikties jam keliamiems reikalavimams. *(Ž, V, A)* |
| Turi būti reguliariai tikrinama subrangovo atitiktis nustatytų reikalavimų ir įsipareigojimų lygiui. *(V, A)* |
| Turi būti susitarta, kad subrangovo darbuotojams, kurie tvarko asmens duomenis, būtų taikomi konkretūs dokumentais įtvirtinti informacijos konfidencialumo, neatskleidimo susitarimai. *(A)* |
| **Asmens duomenų saugumo pažeidimai ir saugumo incidentai** |
| Turi būti nustatytą reagavimo į saugumo incidentus planas, užtikrinantis veiksmingą incidentų, susijusių su asmens duomenų saugumu, valdymą *(Ž, V, A)*. |
| Asmens duomenų saugumo pažeidimai turi būti fiksuojami (dokumentuojami). Apie juos nedelsiant pranešama atsakingiems asmenims. Turi būti nustatyta pranešimo apie asmens duomenų saugumo pažeidimus kompetentingoms institucijoms ir duomenų subjektams tvarka. *(Ž, V, A)*. |
| Saugumo incidentų likvidavimo planas turi būti patvirtintas dokumentais, tarp kurių būtų galimų saugumo incidento poveikio mažinimo priemonių sąrašas ir aiškus atskirų funkcijų paskirstymas. *(V, A)* |
| Visi saugumo incidentai, įskaitant ir asmens duomenų saugumo pažeidimus, turi būti fiksuojami kartu su visa susijusia informacija apie įvykį ir vėliau atliktus incidento poveikio mažinimo veiksmus *(A).* |
| **Verslo tęstinumo valdymas ir atsakas į incidentus** |
| Turi būti nustatytos pagrindinės procedūros ir kontrolės priemonės, kurių reikia laikytis saugumo incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas. *(Ž, V, A)* |
| Veiklos tęstinumo planas turi būti išsamiai apibūdintas ir patvirtintas dokumentais (laikantis bendros saugumo politikos). Jame turi būti pateiktas aiškus veiksmų planas ir funkcijų paskirstymas. (*V, A)* |
| Veiklos tęstinumo plane turi būti apibrėžtas garantuotos paslaugų kokybės lygis (angl. Service-level agreement (SLA), kuris nustatomas pagrindiniams veiklos procesams, kurie užtikrina asmens duomenų saugumą. *(V, A)* |
| Turi būti paskirti darbuotojai, turintys reikiamą atsakomybę, įgaliojimus ir kompetenciją valdyti veiklos tęstinumą saugumo incidento, asmens duomenų saugumo pažeidimo atveju *(A)* |
| Turi būti numatyta alternatyvi infrastruktūros priemonė organizacijos darbui, atsižvelgiant į organizaciją ir jai priimtiną IT sistemų prastovą. *(A)* |
| **Personalas** |
| Būtina užtikrinti, kad visi darbuotojai suprastų savo atsakomybes ir prievoles, susijusias su asmens duomenų tvarkymu. Apie funkcijas ir atsakomybes darbuotojai turi būti aiškiai informuojami prieš įdarbinant ir (arba) įvadinio proceso metu (prieš pradedant vykdyti jam paskirtas funkcijas ir darbus). *(Ž, V, A)* |
| Darbuotojai, prieš pradėdami eiti savo pareigas, turi būti pasirašytinai supažindinti su organizacijos saugumo politika, taip pat pasirašyti atitinkamus informacijos konfidencialumo ir neatskleidimo susitarimus *(V, A)* |
| Darbuotojai, atsakingi už aukštos rizikos asmens duomenų tvarkymo operacijas, turi laikytis konkrečių jiems taikomų konfidencialumo sąlygų (pagal jų darbo sutartį ar kitą teisės aktą). *(A)* |
| **Personalo mokymas** |
| Būtina užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo reikalavimus, susijusius su jų kasdieniu darbu. Darbuotojai, susiję su asmens duomenų tvarkymu, turi būti mokomi apie atitinkamus duomenų saugumo reikalavimus ir atsakomybes, rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Siūlomas mokymų periodiškumas – kartą per metus. *(Ž, V, A)* |
| Turi būti rengiamos struktūrinės nuolatinės personalo mokymų programos, tarp kurių būtų ir speciali programa, skirta mokyti naujus darbuotojus (duomenų apsaugos tema). *(V, A)* |
| Kiekvienais metais turi būti parengtas ir įgyvendintas mokymų planas, kuriame būtų nustatyti siektini tikslai ir uždaviniai. *(A)* |
| **Prieigos prie IT aplinkos kontrolė ir tapatumo nustatymas** |
| Turi būti įdiegta, įgyvendinta Prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras. *(Ž, V, A)* |
| Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas. *(Ž, V, A)* |
| Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį. *(Ž, V, A)* |
| Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio. *(Ž, V, A)* |
| Vartotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. hash form). |
| Turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius *(V, A)* |
| Turi būti apsibrėžta ir dokumentu įforminta speciali slaptažodžių politiką, kurioje yra nuostatos bent jau dėl slaptažodžio ilgumo, sudėtingumo, galiojimo laikotarpio bei priimtino nesėkmingų bandymų prisijungti skaičiaus. *(V, A)* |
| Privilegijuotiems vartotojams (pvz., sistemų administratoriams) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas dviejų veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamas dviejų veiksnių autentifikavimas. Autentifikavimo veiksniais gali būti slaptažodžiai, saugumo žetonai, USB raktai su slapta žyma, biometriniai duomenys ir kt. *(A)* |
| Turi būti naudojamas įrenginio autentifikavimas, garantuojantis, kad asmens duomenys tvarkomi tik naudojant konkrečius tinklo įrenginius. *(A)* |
| **Techninių žurnalų įrašai ir stebėsena** |
| Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). Rekomenduojamas saugojimo terminas – ne trumpiau kaip 6 mėnesiai. *(Ž, V, A)* |
| Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį *(Ž, V, A)* |
| Visi sistemų administratorių ir operatorių veiksmai (taip pat ir jų atliekamas vartotojo teisių papildymas, panaikinimas, keitimas) turi būti registruojami. *(V, A)* |
| Prieiga prie įrašųtaip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną. *(V, A)* |
| Stebėsenos sistema turi apdoroti techninius įrašus, ruošti sistemos būklės ataskaitas ir įspėti apie galimus pavojus. *(V, A)* |
| **Serverių ir duomenų bazių saugumas** |
| Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos (OS) privilegijomis. *(Ž, V, A)* |
| Duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie asmens duomenys, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus. *(Ž, V, A)* |
| Duomenų bazėse turėtų būti naudojamas šifravimas, įdiegiant atitinkamą programinę ar techninę įrangą, naudojantis naujausiomis geromis šifravimo praktikomis. *(V, A)* |
| Duomenų bazėse turi būti taikomi pseudonimizavimo metodai, atskiriant tiesioginius identifikatorius nuo esamų sąsajų su kitais duomenimis.. *(V, A)* |
| Duomenų bazėje turi būti taikomi autorizuotų užklausų, šifruotos paieškos ir kiti privatumo užtikrinimo metodai. *(A)* |
| **Personalo kompiuterizuotų darbo vietų saugumas** |
| Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų *(Ž, V, A)* |
| Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti atnaujinamos ne rečiau kaip kas savaitę, rekomenduojama kartą per parą ar dažniau. *(Ž)* |
| Naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotos programinės įrangos. *(Ž, V, A)* |
| IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Rekomenduojamas neaktyvios sesijos laikas – ne ilgiau kaip 15 min. *(Ž, V, A)* |
| Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant. *(Ž, V, A)* |
| Antivirusinės taikomosios programos ir jų informacijos apie virusus bei kenkimo programinę įrangą duomenų bazės turi būti atnaujinamos ne rečiau kaip kartą per parą. *(V, A)* |
| Turi būti uždrausta perduoti asmens duomenis iš kompiuterinių darbo vietų į išorinius saugojimo įrenginius (pvz., USB raktai, DVD, išorinius standžiuosius diskus ir kt.). *(A)* |
| Kompiuterinėse darbo vietoje naudojamuose operacinės sistemos diskuose turi būti įgalintas pilnas standžiojo disko šifravimas (angl. fulldisk encryption). *(A)* |
| **Tinklo ir ryšių saugumas** |
| Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS/SSL). *(Ž, V, A)* |
| Belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojamsir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidė prieiga turi būti apsaugota patikimais šifravimo mechanizmais. *(V, A)* |
| Reikėtų vengti nuotolinės prieigos prie IT sistemų. Tais atvejais, kai ši prieiga yra išties reikalinga, ji yra galima tik organizacijos paskirtam darbuotojui (pvz., sistemų administratoriui, saugumo specialistui) kontroliuojant ir stebint jos veikimą per iš anksto nustatytus įrenginius. *(V, A)* |
| Bet koks duomenų judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo ir prevencijos sistemas. *(V, A)* |
| Prisijungimas prie interneto neturi būti leidžiamas tarnybinėms stotims ir jose esančiai programinei įrangai, naudojamai asmens duomenims tvarkyti. *(A)* |
| Informacinės sistemos tinklas turi būti atskirtas nuo kitų duomenų valdytojo tinklų. *(A)* |
| Prieiga prie IT sistemos turi būti atliekama tik iš patvirtintų įrenginių ir terminalų, naudojant tam skirtastechnologijas, pvz., MAC adresų filtravimą arba tinklo prieigos kontrolę. *(A)* |
| **Sistemų ir išteklių atsarginės kopijos** |
| Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis. *(Ž, V, A)* |
| IT sistemų, kurios naudojamos asmens duomenų tvarkymui, atveju atsarginių kopijų saugojimui užtikrinti tokį deramą fizinės ir aplinkos apsaugos lygį, kuris atitinka siunčiančiosioms duomenų laikmenoms taikomus standartus. *(Ž, V, A)* |
| Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą. *(Ž, V, A)* |
| Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Rekomenduojamas atsarginių kopijų darymo dažnumas: - kasdien – pridedamoji kopija; - kas savaitę – pilna kopija. *(Ž, V, A)* |
| Atsarginės kopijos turi būti reguliariai testuojamos, siekiant užtikrinti, kad jos galėtų būti patikimai naudojamos ekstremalioje situacijoje. *(V, A)* |
| Reguliarus atsarginių kopijų kūrimas ar bent reguliarus papildantysis (angl. incremental) atsarginių kopijų kūrimas turi būti atliekamas bent kartą per parą. *(V, A)* |
| Atsarginės kopijos turi būti saugiai laikomos skirtingose vietose, kurios turi būti geografiškai nutolusios viena nuo kitos. *(V, A)* |
| Tuo atveju, jei atsarginių kopijų saugojimo paslaugą teikia trečioji šalis, IT sistemų, kurios naudojamos asmens duomenų tvarkymui, atsarginės kopijos dublikatas turi būti užšifruojamas dar prieš jį perduodant iš savo buvimo vietos. *(V, A)* |
| **Taikomųjų programų saugumas per jų gyvavimo ciklą** |
| Informacinėse sistemose naudojama programinė įranga (asmens duomenims tvarkyti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras (angl. frameworks), standartus (pvz., Agile, OWASP ir kt.). *(Ž, V, A)* |
| Prieš paleidžiant programinę įrangą, turi būti atliktas programinės įrangos ir infrastruktūros pažeidžiamumo ir atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti priimta naudoti, kol nėra pasiektas reikiamas saugumo lygis. *(V, A)* |
| Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai. *(V, A)* |
| Programinės įrangos atnaujinimai turi būti ištestuoti ir įvertinti prieš juos diegiant į darbo aplinką atitinkamomis veiklos sąlygomis. *(V, A)* |
| **Duomenų ištrynimas ir utilizavimas** |
| Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jei to padaryti neįmanoma (pvz., DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti. *(Ž, V, A)* |
| Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis *(Ž, V, A)* |
| Prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai (angl. Multiple passes of software-based overwriting). *(V, A)* |
| Jei saugiems duomenų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti sudaryta atitinkama paslaugų sutartis ir atliekamas sunaikintų įrašų protokolavimas. *(V, A)* |
| Po duomenų ištrynimo reikėtų imtis papildomų priemonių, pvz., gali būti atliktas nepageidaujamos magnetinės informacijos pašalinimas (išmagnetinimas). Priklausomai nuo konkretaus atvejo, reikėtų įvertinti fizinio sunaikinimo galimybes. *(A)* |
| Jei saugiems įrašų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti užtikrinta, kad šis procesas vyktų duomenų tvarkytojo patalpose, siekiant išvengti duomenų perdavimo trečiosioms šalims. Atskirais atvejais, kai to neįmanoma atlikti duomenų valdytojo ir (ar) tvarkytojo patalpose, sunaikinimas gali būti atliekamas kitoje fizinėje vietoje, tačiau tik stebint įgaliotam duomenų tvarkytojo atstovui. *(A)* |
| Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos. *(Ž, V, A)* |
| Būtina naudoti aiškią visų darbuotojų ir lankytojų identifikavimo sistemą, naudojant tinkamas priemones, pvz., visiems norintiems patekti į organizacijos patalpas tapatybę patvirtinančius darbo leidimus. *(V, A)* |
| Atitinkamos saugios zonos turėtų būti apibrėžtos ir apsaugotos tinkamomis patekimo kontrolės priemonėmis. Popierinis ar elektroninis registravimo rinkmenų žurnalas turi būti saugiai laikomas, prižiūrimas ir stebimas. *(V, A)* |
| Įsilaužimo (įsibrovimo) aptikimo sistemos turi būti įdiegtos visose saugumo zonose. *(V, A)* |
| Prireikus turi būti kuriamos fizinės kliūtys, kad būtų užkirstas kelias neteisėtam fiziniam prieinamumui. *(V, A)* |
| Laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos. *(V, A)* |
| Išorės subjektų personalui, įgyvendinančiam teikiamas palaikymo paslaugas, turi būti suteikta ribota prieiga prie saugių zonų. *(V, A)* |
| Tarnybinių stočių patalpoje turėtų būti įdiegta automatinė gaisro gesinimo sistema, uždara valdoma oro kondicionavimo sistema ir nepertraukiamo maitinimo šaltinis (UPS) *(V, A)* |

**3. Pagalba duomenų valdytojui**

Duomenų tvarkytojas, kiek tai įmanoma ir atsižvelgiant į toliau nurodytą pagalbos sritį bei apimtį, padeda Duomenų valdytojui pagal Sąlygų 24–26 punktus įgyvendinti šias technines bei organizacines priemones:

(1) duomenų subjektų prašymai turi būti nepagrįstai nedelsiant, bet ne vėliau nei 3 (tris) darbo dienos nuo prašymo gavimo, persiųsti duomenų valdytojui el. paštu: [dap@regitra.lt](mailto:dap@regitra.lt). Atsakymai duomenų subjektams turi būti parengti pagal duomenų valdytojo nurodymus. Duomenų tvarkytojas gautus prašymus vykdo tik laikydamasis duomenų valdytojo nurodymų;

(2) Duomenų valdytojo prašymu, duomenų tvarkytojas ne vėliau kaip per 10 (dešimt) darbo dienų informuoja Duomenų valdytoją apie taikomas asmens duomenų saugumo priemones bei teikia papildomus paaiškinimus, susijusius su taikomomis asmens duomenų saugumo priemonėmis;

(3) Duomenų valdytojo prašymu duomenų tvarkytojas pateikia savo ir (ar) pagalbinio duomenų valdytojo asmens duomenų saugumo pažeidimų žurnalo išrašą ne vėliau kaip per 10 (dešimt) darbo dienų;

(4) Įvykus asmens duomenų saugumo pažeidimui, duomenų tvarkytojas nedelsiant bet ne vėliau nei 24 (dvidešimt keturias) valandas informuoja duomenų valdytoją, pateikdamas: incidento aprašymą, jo pobūdį ir reikšmingumą (įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių), tikėtinas pasekmes ir priemones, kurių buvo imtasi ar ketinama / siūloma imtis šio incidento sukeltoms pasekmėms sumažinti ar galinčioms kilti pasekmėms išvengti, duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti reikalingos informacijos, vardas ir pavardė ar pavadinimas bei kontaktiniai duomenys. Kartu su pranešimu apie incidentą, susijusį su asmens duomenimis, pateikiama visa su šiuo incidentu susijusi informacija ir dokumentai, kurie gali būti reikalingi tam, kad duomenų valdytojas galėtų pritaikyti atitinkamas asmens duomenų saugumo priemones ir įvykdyti pareigą pranešti priežiūros institucijai ir duomenų subjektui (kai taikoma pagal asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimus) apie asmens duomenų saugumo pažeidimą.

**4. Duomenų saugojimo laikotarpis/duomenų trynimo procedūros**

Asmens duomenys saugomi duomenų tvarkytojo DC (įskaitant Sistemą) saugomi 6 mėnesius, nuo jų užfiksavimo dienos ir perkėlimo į serverį dienos, o šiam laikotarpiui pasibaigus, automatiškai ištrinami.

Nutraukęs asmens duomenų tvarkymo paslaugų teikimą, duomenų tvarkytojas ištrina asmens duomenis, atsižvelgiant į Sąlygų 34 punkto reikalavimus.

**5. Duomenų tvarkymo vieta**

Atsižvelgiant į Sąlygas, asmens duomenys turi būti saugomi duomenų tvarkytojo DC, esančiuose Lietuvos Respublikos teritorijoje.

**6. Nurodymai dėl asmens duomenų perdavimo į trečiąją valstybę ar tarptautinėms organizacijoms**

Jei duomenų valdytojas nenurodo Sąlygose arba vėliau nepateikia dokumentais pagrįstų nurodymų dėl asmens duomenų perdavimo į trečiąją valstybę ar tarptautinėms organizacijoms, duomenų tvarkytojas neturi teisės atlikti tokį perdavimą pagal šią Sąlygas.

**7. Procedūros, skirtos duomenų valdytojo atliekamiems Duomenų tvarkytojo asmens duomenų tvarkymo auditams, įskaitant patikrinimams vietoje**

Duomenų valdytojas arba duomenų valdytojo atstovas, turi teisę atlikti duomenų tvarkytojo patikrinimą bei patikrinti duomenų tvarkytojo tvarkomų asmens duomenų tvarkymo sąlygas, įskaitant fizines priemones, taip pat sistemas, naudojamas ir susijusias su duomenų tvarkymu, siekiant įsitikinti, ar duomenų tvarkytojas laikosi Reglamento (ES) 2016/679, galiojančių Europos Sąjungos ar jos valstybių narių asmens duomenų apsaugos nuostatų ir Sąlygų. Patikrinimai turi būti atliekami reguliariai (rekomenduojama kartą per metus).

***Duomenų tvarkytojo patikrinimas atliekamas šiomis sąlygomis:***

Duomenų valdytojas arba duomenų valdytojo atstovas, prieš 20 (dvidešimt) darbo dienų, raštu (sąlygose nurodytais rekvizitais) įspėja duomenų tvarkytoją apie planuojamo patikrinimo atlikimą bei pateikia klausimyną, kurį duomenų tvarkytojas turi užpildyti per nurodytą terminą. Duomenų tvarkytojas per nurodytą terminą (jeigu šalys nesusitarė kitaip), privalo išsamiai užpildyti gautą klausimyną ir (ar) pridėti prašomus dokumentus, įrodymus bei pateikti juos duomenų valdytojui.

Duomenų valdytojas arba duomenų valdytojo atstovas, per 20 (dvidešimt) darbo dienų, įvertina duomenų tvarkytojo pateiktus atsakymus ir dokumentus bei pateikia duomenų tvarkytojui, atlikto patikrinimo išvadas (kaip pvz., jog duomenų tvarkytojas laikosi (atitinka/neatitinka) Reglamento (ES) 2016/679 ir (ar) šių Sąlygų nuostatų). Remdamasis tokio patikrinimo rezultatais, duomenų valdytojas gali paprašyti imtis papildomų priemonių, kad būtų užtikrinta atitiktis Reglamentui (ES) 2016/679, galiojančioms Europos Sąjungos ar jos valstybių narių asmens duomenų apsaugos nuostatoms ir Sąlygoms. Duomenų tvarkytojui neįgyvendinus duomenų valdytojo nurodytų papildomų priemonių, šios Sąlygos ir (ar) pagrindinė paslaugų sutartis turi būti nutraukiama (vadovaujantis Sąlygų 44 punktu).

Be suplanuoto patikrinimo, duomenų valdytojas gali atlikti duomenų tvarkytojo patikrinimą (įskaitant fizinį duomenų tvarkymo vietos patikrinimą), kai duomenų valdytojas mano, kad to reikia.

**8. Procedūros, skirtos pagalbinių duomenų tvarkytojų atliekamų asmens duomenų tvarkymo auditams, įskaitant patikrinimams vietoje**

Duomenų tvarkytojas arba duomenų tvarkytojo atstovas, turi teisę atlikti pagalbinio duomenų tvarkytojo patikrinimą bei patikrinti pagalbinio duomenų tvarkytojo tvarkomų asmens duomenų tvarkymo sąlygas, įskaitant fizines priemones, taip pat sistemas, naudojamas ir susijusias su duomenų tvarkymu, siekiant įsitikinti, ar pagalbinis duomenų tvarkytojas laikosi Reglamento (ES) 2016/679, galiojančių Europos Sąjungos ar jos valstybių narių asmens duomenų apsaugos nuostatų ir sutartimi su duomenų tvarkytoju nustatytų asmens duomenų tvarkymo sąlygų. Patikrinimai turi būti atliekami reguliariai (rekomenduojama kartą per metus).

Pagalbinio duomenų tvarkytojo patikrinimas turi būti atliekamas šio priedo 7 punkte nustatytomis sąlygomis. Duomenų tvarkytojas užtikrina, jog pagalbinio duomenų tvarkytojo patikrinimui būtų taikomos tos pačios sąlygos, kaip ir duomenų valdytojo atliekamam duomenų tvarkytojo patikrinimui.

Tokių patikrinimų dokumentai nedelsiant pateikiami duomenų valdytojui susipažinti. Duomenų valdytojas gali užginčyti ataskaitos apimtį ir (arba) metodiką ir tokiais atvejais gali paprašyti atlikti naują patikrinimą pagal pakeistą taikymo sritį ir (arba) kitokią metodiką.

Jei reikia, duomenų valdytojas gali nuspręsti inicijuoti ir dalyvauti pagalbinio duomenų tvarkytojo patikrinime. Tai gali būti taikoma, jei duomenų valdytojas mano, kad duomenų tvarkytojas, prižiūrintis pagalbinį duomenų tvarkytoją, duomenų valdytojui nepateikė pakankamai dokumentų, kad būtų galima nustatyti, ar pagalbinis duomenų tvarkytojas atlieka duomenų tvarkymą pagal Sąlygas.

Remdamasis tokio patikrinimo rezultatais, duomenų valdytojas gali paprašyti imtis papildomų priemonių, kad būtų užtikrinta atitiktis Reglamentui (ES) 2016/679, galiojančioms Europos Sąjungos ar jos valstybių narių duomenų apsaugos nuostatoms ir Sąlygoms.

Duomenų valdytojo dalyvavimas pagalbinio duomenų tvarkytojo patikrinime nekeičia fakto, kad nurodytam duomenų tvarkytojui ir toliau tenka visa atsakomybė už pagalbinio duomenų tvarkytojo atitiktį Reglamentui (ES) 2016/679, galiojančioms Europos Sąjungos ar jos valstybių narių duomenų apsaugos nuostatoms ir Sąlygoms.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Sąlygose „valstybė narė“ suprantama kaip Europos Ekonominės Erdvės valstybė narė. [↑](#footnote-ref-2)
2. PASTABA. Trečiosios valstybės reiškia valstybes ne Europos Ekonominės Erdvės teritorijoje. [↑](#footnote-ref-3)