

SUSITARIMAS DĖL ASMENS DUOMENŲ TVARKYMO

202_m. [mėnuo] [diena] d., [Vieta], Nr. [numeris]

_____ (duomenų valdytojo pavadinimas, kodas, buveinės adresas, telefono ryšio numeris ir elektroninio pašto adresas)

atstovaujamas _____ (toliau - **Valdytojas**),
(duomenų valdytojui atstovaujančio asmens vardas ir pavardė, pareigos, atstovavimo pagrindas)

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 _____
(toliau - **Tvarkytojas**), (duomenų tvarkytojui atstovaujančio asmens vardas ir pavardė, pareigos, atstovavimo pagrindas)

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

vadovaudamiesi 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**) nuostatomis,

sudarė šį susitarimą dėl asmens duomenų tvarkymo (toliau – **Susitarimas**). Susitarimas nustato ir sureguliuoja Šalių teises ir pareigas, susijusias su asmens duomenų (toliau – **Duomenys**) tvarkymu, kurį Tvarkytojas atlieka Valdytojo vardu, vykdydamas tarp Šalių sudarytą Pagrindinę sutartį (jos pavadinimas, sudarymo data ir numeris pateikiamas šio Susitarimo priede Nr. 1). Duomenys ir duomenų tvarkymo veiksmai, kuriuos atlieka Tvarkytojas, yra išvardinti šio Susitarimo priede Nr. 1.

I SKYRIUS SUSITARIMO TIKSLAS

1. Siekiant įgyvendinti Reglamento (ES) 2016/679 28 straipsnio 3 dalį, šiame Susitarime nustatomos Valdytojo ir Tvarkytojo teisės bei pareigos, Valdytojo vardu tvarkant Duomenis. Šiuo Susitarimu turi būti siekiama apsaugoti duomenų subjektų teises, mažinti konkrečių Duomenų apsaugos riziką ir užtikrinti Valdytojo ir Tvarkytojo santykių bei atitinkamų teisių ir pareigų aiškumą.
2. Detali informacija apie Duomenų tvarkymo tikslus, tvarkomų Duomenų kategorijas ir kitas sąlygas, kuriomis Tvarkytojas įsipareigoja tvarkyti Duomenis Valdytojo vardu yra nustatytos šio Susitarimo 1 priede.

II SKYRIUS ŠALIŲ ĮSIPAREIGOJIMAI

3. Valdytojas:

- 3.1. turi teisę ir pareigą priimti sprendimus dėl Duomenų tvarkymo tikslų ir priemonių;
- 3.2. yra atsakingas, įskaitant, bet neapsiribojant, už tai, kad Duomenų tvarkymas, kurį Tvarkytojui pavesta atlikti, turėtų teisinį pagrindą.
4. Tvarkytojas įsipareigoja:
 - 4.1. tvarkyti Duomenis tik ta apimtimi, kiek tai yra būtina Pagrindinės sutarties vykdymui pagal Valdytojo pateiktus nurodymus ir Priede Nr. 1 pateiktas sąlygas;
 - 4.2. nedelsiant informuoti Valdytoją, jei Valdytojo nurodymai, Tvarkytojo nuomone, prieštarauja Reglamentui (ES) 2016/679 arba kitiems Duomenų apsaugą reglamentuojantiems Europos Sąjungos ar jos valstybių narių teisės aktams;
 - 4.3. Reglamento (ES) 2016/679 nustatytais atvejais ir sąlygomis privalo tvarkyti Duomenų tvarkymo veiksmų, atliekamų Valdytojo vardu, registrą ir veiklos įrašus ir pagal pareikalavimą pateikti minėtą registrą ir veiklos įrašus Valdytojui ir, kai tai taikoma, priežiūros institucijai.
5. Šis Susitarimas neatleidžia Šalių nuo kitų pareigų, kurios joms taikomos pagal Reglamentą (ES) 2016/679 ar kitus teisės aktus.

III SKYRIUS KONFIDENCIALUMAS

6. Tvarkytojas įsipareigoja savo lėšomis užtikrinti Duomenų konfidencialumą bei garantuoja, kad prieigą prie Duomenų turės tik tie asmenys, kuriems vadovauja 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 Duomenis, jų prieigos teisės prie Duomenų panaikinamos ne vėliau nei paskutinę jo užduočių, dėl kurių jiems būtina prieiga prie Duomenų, dieną, o tuo atveju jei nutrūksta Tvarkytojo darbuotojo darbo santykiai – ne vėliau nei paskutinę jo darbo dieną;
 - 6.2. asmenų, kuriems suteikta prieiga prie Duomenų, prieigos teisės ir jų apimtis turi būti periodiškai (ne rečiau kaip kartą per 1 metus) peržiūrimos bei, vadovaujantis atlikta peržiūra, Tvarkytojas įsipareigoja panaikinti prieigą prie Duomenų tiems darbuotojams, kuriems tokia prieiga nebereikalinga.
7. Tvarkytojas, Valdytojo prašymu, privalo įrodyti, kad asmenims, kuriems vadovauja Tvarkytojas ir kuriems pavesta tvarkyti Duomenis, taikoma Susitarimo 6 punkte nurodyta konfidencialumo pareiga ir jie yra tinkamai apmokyti kaip vykdant savo pareigas tinkamai laikytis Duomenų tvarkymui taikomų reikalavimų.

IV SKYRIUS DUOMENŲ TVARKYMO SAUGUMAS

8. Vadovaujantis Reglamento (ES) 2016/679 32 straipsniu, Tvarkytojas įsipareigoja įgyvendinti 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, todėl įgyvendina priežiūros institucijos nustatytus¹ minimalius techninius ir organizacinius reikalavimus, kurie pateikiami Priede Nr. 2. Įvertinus Pagrindinę sutartimi ketinamą tvarkyti asmens duomenų pobūdį, aprėptį, kontekstą bei tikslus, Valdytojas paslaugų pirkimo dokumentuose gali numatyti papildomas technines ir organizacines priemones, kurios užtikrintų pavojų atitinkančio lygio saugumą.
9. Tvarkytojas taip pat įsipareigoja padėti Valdytojui užtikrinti Valdytojo pareigų pagal Reglamento (ES) 2016/679 32 straipsnį vykdymą, teikdamas *inter alia* Valdytojui informaciją apie technines ir organizacines priemones, kurias Tvarkytojas jau įgyvendino kartu su visa kita informacija, reikalinga Valdytojui įvykdyti Valdytojo pareigas.

¹ Taikomi Valstybinės duomenų apsaugos reikalavimai, numatyti gairėse „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“ (aktuali redakcija): https://vdai.lrv.lt/uploads/vdai/documents/files/VDAl_saugumo_priemoniu_gaires-2020-06-18.pdf

V SKYRIUS

KITŲ DUOMENŲ TVARKYTOJŲ PASITELKIMAS

10. Tvarkytojas Duomenų tvarkymui neturi teisės pasitelkti kito tvarkytojo ar pagalbinio tvarkytojo (toliau – Subtvarkytojas) be išankstinio raštiško Valdytojo sutikimo, jeigu šis nėra nurodytas Priede Nr. 1.
11. Tuo atveju, jei Tvarkytojas pageidauja pasitelkti Subtvarkytoją, Tvarkytojas pateikia Valdytojui raštišką prašymą, nurodydamas tokio Subtvarkytojo pavadinimą, adresą, kontaktinį asmenį ir detalų aprašymą, kokioms funkcijoms vykdyti Tvarkytojas ketina pasitelkti Subtvarkytoją. Valdytojas neprivalo pagrįsti atsisakymo leisti pasitelkti Subtvarkytoją. Tuo atveju, jei Valdytojas nepateikia atsakymo į Tvarkytojo prašymą, laikoma, kad Duomenų valdytojas nesutinka su Subtvarkytojo pasitelkimu. Tuo atveju, jei Valdytojas pritaria Subtvarkytojo pasitelkimui, Tvarkytojas į sutartį, sudaromą su Subtvarkytoju, įtraukia sąlygas, analogiškas šio Susitarimo nuostatoms.
12. Tvarkytojas yra pilnai atsakingas už bet kokį Subtvarkytojo padarytą Reglamento (ES) 2016/679, įstatymų, kitų teisės aktų, šio Susitarimo pažeidimą Valdytojo atžvilgiu.

VI SKYRIUS

DUOMENŲ PERDAVIMAS Į TREČIĄSIAS VALSTYBES ARBA TARPTAUTINĖMS ORGANIZACIJOMS

13. Tvarkytojas ir/arba jo pasitelkti Subtvarkytojai Duomenis gali perduoti už Europos Ekonominės Erdvės ribų į trečiąsias valstybes (toliau – Trečiosios valstybės) ar tarptautinėms organizacijoms tik gavęs Valdytojo rašytinius nurodymus ir laikantis Reglamento (ES) 2016/679 V skyriaus reikalavimų.
14. Jei Duomenis Trečiosioms valstybėms ar tarptautinėms organizacijoms reikia perduoti pagal Europos Sąjungos ar jos valstybės narės teisės aktus, kurių turi laikytis Tvarkytojas, nors Valdytojas nedavė nurodymų Tvarkytojui tai atlikti, Tvarkytojas informuoja Valdytoją apie šį teisinį reikalavimą prieš Duomenų perdavimą, nebent teisės aktai draudžia perduoti tokią informaciją.
15. Tvarkytojas, be Valdytojo dokumentais įformintų nurodymų arba be konkretaus reikalavimo pagal Europos Sąjungos ar jos valstybės narės teisės aktus, negali pagal šį Susitarimą:
 - 15.1. perduoti Duomenis valdytojui ar duomenų tvarkytojui Trečiojoje valstybėje ar tarptautinėje organizacijoje;
 - 15.2. perduoti Duomenų tvarkymą Subtvarkytojui Trečiojoje valstybėje;
 - 15.3. leisti, kad Tvarkytojas Duomenis tvarkytų Trečiojoje valstybėje.

VII SKYRIUS

PAGALBA VALDYTOJUI

16. Atsižvelgdamas į Duomenų tvarkymo pobūdį, Tvarkytojas, kiek tai įmanoma, padeda Valdytojui tinkamomis techninėmis ir organizacinėmis priemonėmis įvykdyti Valdytojo prievolos atsakyti į prašymus naudotis duomenų subjekto teisėmis, nustatytomis Reglamento (ES) 2016/679 III skyriuje.
17. Tvarkytojas, atsižvelgdamas į tvarkymo pobūdį ir Tvarkytojui prieinamą informaciją, esant Valdytojo prašymui, taip pat padeda bei teikia prašomą informaciją Valdytojui:
 - 17.1. rengiant pranešimą Valstybinei duomenų apsaugos inspekcijai apie Duomenų saugumo pažeidimą;
 - 17.2. rengiant pranešimą duomenų subjektui apie Duomenų saugumo pažeidimą;
 - 17.3. atliekant numatytą Duomenų tvarkymo operacijų poveikio duomenų apsaugai vertinimą.

VIII SKYRIUS

PRANEŠIMAS APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

18. Tvarkytojas, sužinojęs apie Duomenų saugumo pažeidimą arba incidentą, dėl kurio gali įvykti Duomenų saugumo pažeidimas, nepagrįstai nedelsdamas, bet ne vėliau kaip per 24 val. nuo sužinojimo, visais atvejais praneša Valdytojui ir raštu pateikia turimą Susitarimo 19 p. nurodytą informaciją.
19. Susitarimo 17.1 papunktyje nurodyta Tvarkytojo pareiga padėti Valdytojui pranešti kompetentingai priežiūros institucijai apie Duomenų pažeidimą reiškia, kad Tvarkytojas privalo Valdytojui pateikti bent

jau šią toliau išvardytą informaciją:

- 19.1. trumpą Duomenų incidento arba pažeidimo apibūdinimą;
- 19.2. paveiktų Duomenų aprašymą (asmens duomenų kategorijos (rūšys), susiję su pažeidimu; ar Duomenys, įvykus incidentui, buvo viešai prieinami; ar dėl incidento gali kilti pavojus asmenų saugumui ar sveikatai; ar incidento paveikti Duomenys buvo užšifruoti, ar jiems buvo taikomos kitos techninės apsaugos priemonės, jei tokia informacija žinoma ir koks paveiktų asmens Duomenų subjektų, susijusių su incidento arba pažeidimu, kiekis (skaičius));
- 19.3. incidento arba pažeidimo aprašymą (laikas arba laikotarpis, kurį incidentas tęsėsi; incidento tipas (bylų ar įrenginių praradimas ar pagrobimas, utilizavimas prieš tai neištrynus duomenų, duomenų atskleidimas žinomiems adresatams, duomenų paviešinimas, duomenų pakeitimas, sunaikinimas ar priegios apribojimas, priešlaikinis duomenų sunaikinimas);
- 19.4. Duomenų buvimo vieta (pvz., kompiuteryje, mobiliajame įrenginyje, tinkle, laikmenoje);
- 19.5. kur įvyko neleistina prieiga (pas Tvarkytoją viduje ar išorėje, pvz. pas pasitelktus Subtvarkytojus);
- 19.6. incidento arba pažeidimo priežastis (klaida ar tyčiniai veiksmai);
- 19.7. kokios tikėtinos, galimos incidento arba pažeidimo pasekmės;
- 19.8. priemonės, kurių ėmėsi ar siūlo imtis Valdytojas dėl Duomenų incidento ar pažeidimo, įskaitant, jei reikia, priemones, skirtas sušvelninti galimą neigiamą pažeidimo poveikį.

IX SKYRIUS

DUOMENŲ TRYNUMAS IR GRĄŽINIMAS

20. Pasibaigus Duomenų tvarkymo paslaugų teikimui, Tvarkytojas privalo nemokamai grąžinti visus Duomenis Valdytojui ir ištrinti esamas kopijas, nebent Duomenis reikia saugoti pagal Europos Sąjungos ar jos valstybės narės teisės aktus arba atskirus susitarimus su Valdytoju.
21. Valdytojo atskiru prašymu Tvarkytojas per 30 dienų nuo šio Susitarimo nutraukimo (nutūkimo, pabaigos) įsipareigoja atsiųsti Valdytojui raštišką patvirtinimą, kad visi Duomenys buvo grąžinti ir jokių Duomenų pas Tvarkytoją neliko.

X SKYRIUS

TVARKYTOJO AUDITAS IR TIKRINIMAS

22. Tvarkytojas Valdytojui suteikia visą informaciją, reikalingą įrodyti, kad laikomasi Reglamento (ES) 2016/679 28 straipsnyje ir Susitarime nustatytų pareigų, ir sudaro sąlygas bei padeda atlikti Valdytojui ar kitam Valdytojo įgaliotam auditoriui auditą, įskaitant patikrinimus vietoje.
23. Tvarkytojas turi suteikti priežiūros institucijoms, kurios pagal galiojančius teisės aktus turi prieigą prie Valdytojo ir Tvarkytojo įrenginių, arba atstovams, veikiantiems tokių priežiūros institucijų vardu, prieigą prie Tvarkytojo fizinių priemonių ar atlikti kitus priežiūros institucijų nurodytus veiksmus auditui ar kitam patikrinimui atlikti. Šalys turi kompetentingų priežiūros institucijų prašymu pateikti šiame Susitarime nurodytą informaciją, įskaitant auditų rezultatus.

XI SKYRIUS

BAIGIAMOSIOS NUOSTATOS

24. Susitarimas įsigalioja nuo jo pasirašymo dienos ir galioja tol, kol:
 - 24.1. pasibaigia ar nutraukiama anksčiau laiko Pagrindinė sutartis;
 - 24.2. atskiru Valdytojo pranešimu Tvarkytojas informuojamas apie šio Susitarimo nutraukimą.
25. Valdytojas turi teisę nutraukti šį Susitarimą ir Pagrindinę sutartį, jeigu Tvarkytojas iš esmės arba nuolat pažeidžia Susitarimą arba savo įsipareigojimus pagal Reglamentą (ES) 2016/679. Esminiais šio Susitarimo pažeidimais laikytinas Tvarkytojo elgesys pažeidžiantis Susitarimo reikalavimus, nurodytus 4.1. p., 6 p., 8 p., 10 p., 13 p., 16-18 p. bei 22 p.
26. Jei Duomenų tvarkymo paslaugų teikimas yra nutraukiamas, o Duomenys ištrinami arba grąžinami Valdytojui pagal Susitarimo 20 punktą Susitarimas gali būti nutrauktas bet kuriai Šaliai pateikus rašytinį

- pranešimą.
27. Nedarant poveikio jokioms Reglamento (ES) 2016/679 nuostatomis, Tvarkytojui pažeidus pareigas pagal šį Susitarimą, Valdytojas gali nurodyti Tvarkytojui laikinai sustabdyti Duomenų tvarkymą, kol pastarasis laikysis šio Susitarimo arba Susitarimas bus nutrauktas. Tvarkytojas nedelsdamas informuoja Valdytoją, jei dėl kokios nors priežasties jis negali vykdyti Susitarimo.
 28. Tvarkytojo atsakomybei, kuri kilo dėl Tvarkytojo tyčios ar didelio neatsargumo, pagal šį Susitarimą netaikomi jokie atsakomybės ribojimai, nepaisant to, kad tokie buvo numatyti Pagrindinėje sutartyje.
 29. Atsiradus nesutapimams tarp Susitarimo sąlygų ir kitų tarp Šalių sudarytų susitarimų, įskaitant Pagrindinę sutartį bei papildomus susitarimus (išskyrus, kai Šalys aiškiai raštu susitarė kitaip ir pasirašė tokį susitarimą), kurie buvo sudaryti arba turėjo būti sudaryti po šio Susitarimo sudarymo dienos, bus taikomos šio Susitarimo nuostatos.
 30. Kiekviena Šalis paskiria asmenį, atsakingą už Susitarimo vykdymą ir nurodo kontaktinius duomenis, kuriais kita Šalis komunikuos pranešdama apie Duomenų saugumo pažeidimus, duomenų subjektų prašymus ir kitą informaciją, susijusią su Duomenų tvarkymu pagal šį Susitarimą.
 31. Visi ginčai, kylantys dėl šio Susitarimo vykdymo, pakeitimo ar nutraukimo, bus sprendžiami derybų būdu.
 32. Tuo atveju, jeigu Šalys nepasiekia sutarimo dėl ginčo išsprendimo derybų būdu, ginčas sprendžiamas Pagrindinėje sutartyje numatytoje jurisdikcijoje ir pagal numatytą taikytiną teisę.
 33. Šio Susitarimo nuostatos neatleidžia Tvarkytojo nuo jo pareigų, prievolių ir įsipareigojimų, kurie taikomi Tvarkytojui pagal Reglamentą (ES) 2016/679.

XII SKYRIUS

ŠALIŲ REKVIZITAI, PARAŠAI

Valdytojo vardu:

pareigos
vardas, pavardė

Tvarkytojo vardu:

pareigos
vardas, pavardė

INFORMACIJA APIE ASMENS DUOMENŲ TVARKYMĄ

Paslaugų teikimo sutarties pavadinimas, data ir numeris, kurios pagrindu tarp šalių susiklosto Duomenų tvarkymo teisiniai santykiai	
Duomenų tvarkymo tikslas (-ai)	
Duomenų kategorijos (rūšys)	
Duomenų subjektų kategorijos	
Atliekami Duomenų tvarkymo veiksmai	
Duomenų tvarkymo (saugojimo) laikotarpis	
Tvarkytojo pasitelktų Subtvarkytojų sąrašas (jei žinomi šio Susitarimo sudarymo metu)	
Duomenų tvarkymo vieta (nurodoma, jei Duomenis Tvarkytojas arba jo pasitelktas Subtvarkytojas planuoja perduoti į kitas nei Europos ekonominės erdvės valstybes)	
Valdytojo paskirtas atsakingas asmuo ² (ir jo kontaktiniai duomenys).	
Tvarkytojo paskirtas atsakingas asmuo ³ (ir jo kontaktiniai duomenys)	

² Už Susitarimo vykdymą bei komunikaciją su Tvarkytoju Duomenų saugumo klausimais.

³ Už Susitarimo vykdymą bei komunikaciją, pranešant apie Duomenų saugumo pažeidimus, duomenų subjektų prašymus ir kitą informaciją, susijusią su Duomenų tvarkymu pagal šį Susitarimą.

REIKALAVIMAI TECHNINĖMS IR ORGANIZACINĖMS SAUGUMO PRIEMONĖMS

1. Organizacinės Duomenų saugumo priemonės:

1.1. Duomenų saugumo politika ir procedūros. Tvarkytojas privalo turėti Duomenų ir jų tvarkymo saugumo politiką (gali būti sudedamojo informacijos saugumo politikos dalis), kuri periodiškai peržiūrima ir prireikus atnaujinama.

1.2. Vaidmenys ir atsakomybės. Su Duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti. Keičiantis vaidmenims (pvz. vidaus organizacijos pertvarkymo, darbuotojų atleidimo, funkcijų pasikeitimo metu ar kt.), turi būti aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras.

1.3. Prieigos valdymo politika. Kiekvienam vaidmeniui, susijusiam su Duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. need to know) principu.

1.4. Išteklių ir turto valdymas. Tvarkytojas turi 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., tarnybinių stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę) bei šio registro tvarkymas (įskaitant periodines peržiūras ir atnaujinimus) turi būti priskirtas konkrečiam asmeniui, pvz., IT specialistui.

1.5. Keitimų valdymas. Tvarkytojas turi užtikrinti, kad visi esminiai IT sistemų keitimai būtų stebimi ir registruojami konkrečiam asmeniui (pvz., IT arba saugos specialisto) bei programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant Duomenis. Testuojant sistemas, naudojami tik testiniai duomenys, o kai tai neįmanoma, turi būti taikomos atitinkamai papildomos Duomenų apsaugos priemonės.

1.6. Duomenų tvarkytojai. Kai Tvarkytojas pasitelkia kitus Subtvarkytojus, jis privalo turėti nustatytas ir dokumentuotas gaires ir procedūras, reguliuojančias Subtvarkytojų parinkimą (įskaitant Valdytojo sutikimo gavimą) bei jų atliekamų Duomenų tvarkymą. Šios procedūros turi privalomai nustatyti ne mažesnę Duomenų apsaugos lygį nei taikomas pagal šį Susitarimą.

1.7. Duomenų saugumo incidentai ir pažeidimai. Tvarkytojas privalo turėti reagavimo į saugumo incidentus ir pažeidimus planą, kuris užtikrintų veiksmingą incidentų, susijusių su Duomenų saugumu, valdymą bei apimtų pranešimų pateikimo Valdytojui ir, esant poreikiui, kompetentingoms institucijoms bei duomenų subjektams, tvarką. Visi Duomenų saugumo pažeidimai turi būti fiksuojami (dokumentuojami).

1.8. Veiklos tęstinumas. Tvarkytojas turi nustatyti pagrindines procedūras, kurių reikia laikytis saugumo incidento ar Duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas Duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas.

1.9. Personalo konfidencialumas. Tvarkytojas turi užtikrinti, kad visi darbuotojai suprastų savo atsakomybes ir įsipareigojimus, susijusius su Duomenų tvarkymu. Vaidmenys ir atsakomybės turi būti aiškiai išdėstyti darbuotojui prieš pradedant vykdyti jam paskirtas funkcijas ir darbus.

1.10. Mokymai. Tvarkytojai turi užtikrinti, kad visi darbuotojai būtų pakankamai informuoti apie IT sistemų saugumo reikalavimus, susijusius su jų kasdieniu darbu. Darbuotojai, kurių darbas susijęs su Duomenų tvarkymu, turi būti periodiškai mokomi apie atitinkamus duomenų saugumo reikalavimus ir teisinius įpareigojimus.

2. Techninės asmens duomenų saugumo priemonės:

2.1. prieigų kontrolė ir autentifikavimas. Tvarkytojas turi įdiegti prieigų kontrolės sistemą, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras. Negalima naudoti bendrų paskyrų keliems vartotojams, jei tai neišvengiama, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi vienodus vaidmenis ir atsakomybes bei yra įdiegtas tinkamas konkrečiam vartotojo veiksmų atsekamumo mechanizmas. Taip pat turi būti įdiegtas autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos. Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis (sudaromas atsižvelgiant į tam tikrą

kompleksiškumo lygį), be to, prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio. Naudotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. hash form).

2.2. Techninių žurnalų įrašai ir stebėseną. Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai ar aplikacijai, naudojamai Duomenims tvarkyti ir turi fiksuoti visą įmanomą prieigų prie Duomenų informaciją (pvz., datą, laiką, peržiūrėjimo, keitimo, panaikinimo veiksmus). 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.

2.3. Tarnybinių stočių, duomenų bazių apsauga. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos (OS) privilegijomis. Duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie Duomenys, kurie yra reikalingi darbui, atitinkančiam Duomenų tvarkymo tikslus.

2.4. Darbo vietų apsauga. Darbuotojams ir kitiems naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų. Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti nuolat atnaujinamos. Naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotą programinę įrangą. IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.

2.5. Tinklo ir komunikacijos sauga. Visais atvejais, kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, ryšys turi būti šifruojamas kriptografiniais protokolais (pvz. TLS/SSL).

2.6. Atsarginės kopijos. Duomenų atsarginės kopijos ir jų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis. Atsarginių kopijų laikmenoms privalo būti užtikrintas pakankamas fizinis aplinkos ir patalpų saugos lygis. Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą. Pilnos atsarginės kopijos privalo būti daromos reguliariai.

2.7. Mobilieji, nešiojamieji įrenginiai. Mobilųjų, nešiojamųjų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimą. Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojama darbui su Tvarkytojo informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti. Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga Duomenims tvarkyti.

2.8. Programinės įrangos sauga. Tvarkytojo informacinėse sistemose naudojama programinė įranga (Duomenims tvarkyti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrimo taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras (angl. frameworks) ir standartus (pvz., Agile, OWASP ir kt.). Specifiniai saugos reikalavimai, susiję su Tvarkytojo veiklos ypatumais, turi būti apibrėžti pradinuose programinės įrangos kūrimo etapuose. Atliekant programavimą, Tvarkytojas turi laikytis duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos, o po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją, turi būti laikomasi pagrindinių saugos reikalavimų.

2.9. Duomenų naikinimas, šalinimas Elektroninė informacija ir duomenys turi būti sunaikinami neatkuriamai. Popieriniai dokumentai ir nešiojamos laikmenos turi būti susmulkinamos.

2.10. Fizinė sauga. Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.