

PATVIRTINTA

Biudžetinės įstaigos „Skaitlis“ direktoriaus 2022 m. vasario 22 įsakymu Nr. V-9

PAKEITIMAI

Biudžetinės įstaigos „Skaitlis“ direktoriaus 2024 m. kovo 18 d. įsakymu Nr. V-15

BIUDŽETINĖS ĮSTAIGOS „SKAITLIS“ ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I SKYRIUS

BENDROSIOS NUOSTATOS

1. Biudžetinės įstaigos „Skaitlis“ asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) reglamentuoja asmens duomenų tvarkymą Biudžetinės įstaigos „Skaitlis“ (toliau – Įstaiga), užtikrinant 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų duomenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ir kitų teisės aktų, nustatančių asmens duomenų tvarkymą ir apsaugą, nuostatų laikymąsi ir įgyvendinimą, reguliuoja asmens duomenų tvarkymo principus, įtvirtina organizacines ir technines duomenų apsaugos priemonės, darbuotojų stebėseną ir asmens duomenų tvarkytojų funkcijas.

(2 punktas pakeistas BĮ „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15)

2. Asmens duomenų valdytoja ir (ar) tvarkytoja – biudžetinė įstaiga „Skaitlis“, juridinio asmens kodas 300035837. Įstaigos duomenų tvarkytojais gali būti ir kiti fiziniai ir juridiniai asmenys, kuriems šių duomenų tvarkymas pavedamas duomenų tvarkymo sutartimi ar kitu dokumentu.

3. Įstaiga, vykdydama asmens duomenų tvarkymą, vadovaujasi BDAR, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (toliau – ADTAĮ) ir kituose teisės aktuose, susijusiuose su asmens duomenų tvarkymu ir apsauga, įtvirtintais asmens duomenų tvarkymo reikalavimais.

4. Asmens duomenų subjektų teisių įgyvendinimo tvarka reglamentuojama Įstaigos patvirtintame *Asmens duomenų subjektų teisių įgyvendinimo apraše*.

5. Šių Taisyklių privalo laikytis visi Įstaigoje dirbantys darbuotojai ir kiti asmenys, kurie tvarko Įstaigoje esančius asmens duomenis arba eidami savo pareigas juos sužino.

6. Šiose Taisyklėse vartojamos sąvokos ir sutrumpinimai:

Klientas	Vilniaus miesto savivaldybės kontroliuojamas viešojo sektoriaus subjektas, kurio finansinė apskaita organizuojama centralizuotai ir yra perduota tvarkyti Įstaigai
Vidaus administravimas	veikla, kuria užtikrinamas Įstaigos savarankiškas funkcionavimas (struktūros tvarkymas, personalo valdymas, finansinių išteklių valdymas ir naudojimas, dokumentų saugojimas, raštvedybos tvarkymas)
Asmens duomenys	bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima tiesiogiai arba netiesiogiai nustatyti visų pirma pagal

	identifikatorių, kaip antai vardą ir pavardę, asmens kodą, buvimo vietos duomenis ir interneto identifikatorių, arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius
Duomenų subjektas	fiziniai asmenys, kurių duomenis tvarko Įstaiga
Duomenų tvarkymas	bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimasis arba sunaikinimas
Duomenų apsaugos pareigūnas	Įstaigoje paskirtas darbuotojas, atliekantis BDAR nustatytas duomenų apsaugos pareigūno funkcijas
BDAR	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų duomenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB
Kitos Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos BDAR ir ADAĮ.	

II SKYRIUS

ASMENS DUOMENŲ SUBJEKTŲ KATEGORIJOS, DUOMENŲ TVARKYMO TIKSLAI IR TEISINIS PAGRINDAS

7. Įstaigoje neautomatiniu būdu susistemintose rinkmenose ir (arba) automatiniu būdu tvarkomi šių duomenų subjektų kategorijų asmens duomenys:

7.1. Duomenų valdytojo statusu tvarkomi asmens duomenys:

7.1.1. buvusių ir esamų Įstaigos darbuotojų, dirbančių pagal darbo sutartis, praktikantų asmens duomenys, tvarkomi darbo sutarties sudarymo ir vykdymo, vidaus administravimo, darbų saugos užtikrinimo, darbo užmokesčio ir kitų mokėjimų apskaičiavimo ir mokėjimo tikslais; korupcijos prevencijos ir skaidrumo užtikrinimo tikslais, taip pat Įstaigos veiklos viešinimo tikslais;

7.1.2. pretendentų į Įstaigos darbuotojus asmens duomenys, tvarkomi vidaus administravimo tikslais ir vykdomos atrankos skaidrumo bei viešinimo tikslais;

7.1.3. Įstaigos organizuojamų viešųjų pirkimų procedūrose dalyvaujančių tiekėjų (tiekėjo – fizinio asmens ar tiekėjo – juridinio asmens atstovų) asmens duomenys, tvarkomi viešųjų pirkimų procedūrų organizavimo ir vykdymo tikslais;

7.1.4. Įstaigos tiekėjų (tiekėjo – fizinio asmens ar tiekėjo – juridinio asmens atstovų), su kuriais sudarytos prekių, darbų, paslaugų sutartys (sandoriai), asmens duomenys, tvarkomi sutarčių sudarymo ir vykdymo, vidaus administravimo tikslais;

7.1.5. asmenų, pateikusių Įstaigai skundą, pranešimą, pareiškimą ar prašymą, asmens duomenys, tvarkomi asmenų informavimo, skundų, pranešimų, pareiškimų ar prašymų nagrinėjimo, paslaugų teikimo, vidaus administravimo (dokumentų valdymo) tikslais;

7.1.6. į vaizdo kamerų stebėjimo lauką patekusių duomenų subjektų vaizdo duomenys, tvarkomi Įstaigos pastatų (patalpų), teritorijų ir juose esančio materialiojo turto, informacijos saugumo užtikrinimo tikslais; asmenų, kurie lankosi Įstaigoje, ir Įstaigos darbuotojų saugumo užtikrinimo tikslais;

7.1.7. asmenų, skambinančių į Įstaigą telefonais, balso ir pokalbių duomenys, tvarkomi vidaus administravimo (asmenų aptarnavimo) tikslais; asmenų aptarnavimo kokybės užtikrinimo, vienodos praktikos formavimo tikslais;

7.1.8. asmenų, pateikusių Įstaigai sutikimą tvarkyti jų duomenis, tvarkomi tikslais, kurie nurodyti sutikime;

7.2. Duomenų tvarkytojo statusu tvarkomi asmens duomenys:

7.2.1. buvusių ir esamų Kliento (-ų) darbuotojų, dirbančių pagal darbo sutartį, (toliau – darbuotojai) asmens duomenys, tvarkomi finansinės (buhalterinės) apskaitos tvarkymo ir darbo užmokesčio apskaičiavimo tikslais; mokėjimų vykdymo tikslais;

7.2.2. Kliento (-ų) įstaigas (ugdymo įstaigas, vykdančias ikimokyklinio, priešmokyklinio ugdymo, bendrojo ugdymo ir/ ar neformaliojo švietimo programas, arba dienos socialinės globos centrus) lankančių mokinių ir jų tėvų (globėjų, rūpintojų) asmens duomenys, tvarkomi finansinės (buhalterinės) apskaitos tvarkymo tikslais, mokėtinų sumų už Kliento suteiktas paslaugas apskaičiavimo tikslais, mokėjimo įsipareigojimų vykdymo ir kontrolės tikslais;

7.2.3. Kliento (-ų) tiekėjų (fizinį asmenų), su kuriais Kliento sudarytos prekių, darbų ar paslaugų sutartys (sandoriai), ir nuomininkų (fizinį asmenų) asmens duomenys, tvarkomi finansinės (buhalterinės) apskaitos tvarkymo tikslais, mokėtinų sumų už Kliento suteiktų paslaugų apskaičiavimo tikslais, mokėjimo įsipareigojimų vykdymo ir kontrolės tikslais;

7.2.4. Klientui (-ams) įsiskolinusių asmenų duomenys, tvarkomi įsiskolinimų administravimo ir išieškojimo tikslais.

8. Įstaigoje tvarkomų asmens duomenų sąrašas pateikiamas ir tikslai detalizuojami Asmens duomenų tvarkymo veiklos įrašų registre, kuris pildomas Įstaigoje Taisyklių [III skyriaus](#) nustatyta tvarka.

9. Įstaiga tvarko duomenų subjektų asmens duomenis toliau nurodytais teisiniais pagrindais:

9.1. asmens duomenys tvarkomi siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba duomenų subjekto prašymu siekiant imtis veiksmų prieš sudarant sutartį (BDAR 6 str.1 d. b punktas);

9.2. tvarkyti asmens duomenis Įstaigą įpareigoja atitinkami teisės aktai (BDAR 6 str. 1 d. c punktas).

9.3. asmens duomenys tvarkomi dėl Įstaigos teisėto intereso (BDAR 6 str. 1 d. f punktas).

9.4. duomenų subjektas davė sutikimą Įstaigai, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais. Asmens sutikimo pagrindu duomenys tvarkomi tuo atveju, kai, atsižvelgiant į duomenų tvarkymo tikslą ar duomenų kiekį, Įstaiga neturi kito iš ankščiau paminėtų pagrindų tvarkyti asmens duomenis. Jeigu asmens duomenys, atsižvelgiant į jų kiekį ir tvarkymo tikslus, gali būti tvarkomi bent vienu iš BDAR įtvirtintų pagrindų, duomenų subjekto sutikimas nėra privalomas.

10. Tvarkydama asmenų duomenis, kurie perduodami Įstaigai duomenų tvarkytojo statusu, Įstaiga, kaip teisėto tvarkymo pagrindu, remiasi BDAR 6 str. 1 d. b punktu, nes tvarkyti asmens duomenis būtina, siekiant atlikti užduotis, įvykdyti sutartį arba pasinaudoti iš sutarčių kylančiomis teisėmis, BDAR 6 str. 1 d. c punktu, nes tam tikrus asmens duomenis būtina tvarkyti, kad būtų įvykdyta duomenų valdytojų ir/ ar tvarkytojų taikoma teisinė prievolė arba BDAR 6 str. 1 d. f punktu, kai duomenys tvarkomi, siekiant teisėtų interesų.

11. Įstaiga, kaip duomenų tvarkytojas, tvarko asmens duomenis viešojo sektoriaus subjektų (duomenų valdytojų) vardu, vadovaudamasis Lietuvos Respublikos Vyriausybės 2018 m. gegužės 23 d. nutarimu Nr. 488 „Dėl centralizuoto viešojo sektoriaus subjektų buhalterinės apskaitos organizavimo tvarkos aprašo patvirtinimo“. Šiuo teisės aktu reglamentuotas asmens duomenų tvarkymas atliekamas centralizuoto viešojo

sektorius subjektų buhalterinės apskaitos organizavimo tikslu.

12. Įstaigoje asmens duomenys nėra tvarkomi tiesioginės rinkodaros tikslais. Įstaigos veikloje nėra vykdomas profiliavimas.

13. Įstaigoje tvarkomi asmens duomenys nėra perduodami į trečiąsias valstybes arba tarptautinėms organizacijoms.

III SKYRIUS

ASMENS DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

14. Įstaigoje yra tvarkomi asmens duomenų tvarkymo veiklos įrašai pagal šiose Taisyklėse patvirtintą formą ([Taisyklių 1 priedas](#)) pildant Asmens duomenų tvarkymo veiklos įrašų registrą.

15. Asmens duomenų tvarkymo įrašai pildomi ir tvarkomi elektronine forma.

16. Už Asmens duomenų tvarkymo veiklos įrašų registro pildymą ir tvarkymą atsakingas duomenų apsaugos pareigūnas.

17. Asmens duomenų tvarkymo veiklos įrašų registre pateikiama ši privaloma informacija:

17.1. duomenų subjektų ir asmens duomenų kategorijos – kokių kategorijų duomenų subjektų asmens duomenys ir kokių kategorijų asmens duomenys yra tvarkomi;

17.2. asmens duomenų tvarkymo tikslas – koku tikslu yra tvarkomi duomenys;

17.3. duomenų gavėjai – kam gali būti perduodami asmens duomenys;

17.4. asmens duomenų saugojimo terminai – kiek laiko saugomi šie asmens duomenys (nurodomas laikotarpis mėnesiais ar metais arba kriterijus, pagal kurį tas laikotarpis nustatomas).

18. Asmens duomenų tvarkymo veiklos įrašų registro duomenis tvarko ir, esant poreikiui, papildo duomenų apsaugos pareigūnas, remdamasis informacija, kurią jam teikia darbuotojai (struktūriniai padaliniai), atsakingi už atitinkamų asmens duomenų tvarkymą. Darbuotojai (struktūriniai padaliniai), atsakingi už atitinkamų asmens duomenų tvarkymą, nedelsdami informuoja duomenų apsaugos pareigūną apie pasikeitimus, atsiradusius jiems tvarkant asmens duomenis.

19. Jei darbuotojas pastebi, kad duomenų tvarkymo veiklos įrašai neapima tam tikrų duomenų rinkimo, naudojimo ir saugojimo, apie tai turi nedelsdamas informuoti duomenų apsaugos pareigūną ir gauti jo konsultaciją.

20. Gavęs darbuotojo informaciją, duomenų apsaugos pareigūnas turi nustatyti, ar darbuotojo pranešime nurodytas asmens duomenų rinkimas, naudojimas ir (arba) saugojimas atitinka BDAR bei kitus duomenų apsaugos įstatymus, ir, jei reikia, atnaujina Asmens duomenų tvarkymo veiklos įrašų registrą.

21. Duomenų apsaugos pareigūnas periodiškai, ne rečiau kaip vieną kartą per metus, tikrina, ar Įstaigos vykdoma asmens duomenų tvarkymo veikla atitinka Asmens duomenų tvarkymo veiklos įrašų registrą. Duomenų apsaugos pareigūnas patikrai atlikti gali pasitelkti Įstaigos darbuotojus.

22. Duomenų apsaugos pareigūnas, kai Įstaigoje pasikeičia asmens duomenų tvarkymo veiksmas, asmens duomenų tvarkymo operacijos arba Įstaigoje įvyksta struktūriniai, technologiniai ar kitokie pakeitimai, kurie turi įtakos asmens duomenų tvarkymui, peržiūri Asmens duomenų tvarkymo veiklos įrašų registre esančią informaciją ir esant poreikiui ją atnaujina.

23. Asmens duomenų tvarkymo veiklos įrašų registras/ jo išrašas, gavus prašymą, pateikiamas Valstybinei duomenų apsaugos inspekcijai jos prašyme nurodytais terminais.

IV SKYRIUS

BENDRIEJI ASMENS DUOMENŲ TVARKYMO PRINCIPAI

24. Įstaigoje visi asmens duomenys tvarkomi vadovaujantis BDAR 5 straipsnio 1 dalyje nustatytų teisėtumo, sąžiningumo ir skaidrumo, tikslo apribojimo, duomenų kiekio mažinimo, tikslumo, saugojimo trukmės apribojimo, vientisumo ir konfidencialumo principais.

25. Asmens duomenys gali būti tvarkomi tik tuo tikslu, kuriuo yra renkami. Jeigu asmens duomenys nėra būtini tam, kad būtų pasiektas konkretus tikslas, jie negali būti tvarkomi. Konkrečiam tikslui pasiekti yra tvarkomas kiek įmanoma mažesnis kiekis asmens duomenų. Asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, turi būti nedelsiant ištrinami arba ištaisomi. Asmens duomenys tvarkomi ir saugomi ne ilgiau, negu nustatytas jų saugojimo terminas, kuris turi būti ne ilgesnis, negu yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi.

26. Įstaigoje asmens duomenys gali būti tvarkomi tik tada, jeigu yra bent viena iš BDAR 6 straipsnio 1 dalyje įtvirtintų teisėto tvarkymo sąlygų.

27. Įstaigos darbuotojai, įgyvendindami BDAR nustatytus asmens duomenų tvarkymo ir apsaugos principus, privalo laikytis šių reikalavimų:

27.1. Asmens duomenis rinkti nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkyti tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis (**tikslo apribojimo principas**); Įstaigos darbuotojai turi teisę rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti asmens duomenis tik atlikdami savo tiesiogines funkcijas, apibrėžtas pareigybės aprašyme ar kitame Įstaigos lokaliniame teisės akte arba Įstaigos direktoriaus pavedimu; Įstaigos darbuotojams draudžiama savavališkai rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti asmens duomenis;

27.2. Tvarkomi asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (**duomenų kiekio mažinimo principas**); Įstaigos darbuotojai neturi rinkti, naudoti ir saugoti asmens duomenų, kurie nėra reikalingi jų darbo funkcijoms atlikti;

27.3. Tvarkomi asmens duomenys turi būti tikslūs ir prireikus atnaujinami (**tikslumo principas**); Įstaigos darbuotojai privalo užtikrinti, kad Įstaigoje tvarkomi asmens duomenys būtų tikslūs, o duomenys, kurie nėra tikslūs, būtų nedelsiant ištrinami arba ištaisomi;

27.4. **Asmens duomenys turi būti tvarkomi** įgyvendinant Įstaigoje įdiegtas technines ir organizacines priemones, kurių reikalaujama pagal BDAR, siekiant apsaugoti duomenų subjekto teises ir laisves (**saugumo užtikrinimo principas**); Įstaigos darbuotojai turi užtikrinti, kad asmens duomenys būtų renkami, naudojami ir saugojami laikantis vidaus procedūrų ir užtikrinant asmens duomenų apsaugą nuo neleistinos prieigos, neteisėto rinkimo, naudojimo ir saugojimo, netyčinio praradimo ir sunaikinimo;

27.5. Tvarkomus asmens duomenis laikyti tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi (**saugojimo trukmės apribojimo principas**); Įstaigos darbuotojai turi užtikrinti, kad jo tvarkomi asmens duomenys būtų saugojami tik Įstaigoje nustatyta laikotarpį;

27.6. **Tvarkomi tokiu būdu, kad būtų apribota galimybė kitiems asmenims (kuriems duomenys nėra būtini jų darbo funkcijoms atlikti) sužinoti tvarkomus asmens duomenis (prieigos prie asmens duomenų ribojimo principas)**; nė vienam Įstaigos darbuotojui ir / ar kitiems subjektams neturi būti suteikta prieiga prie asmens duomenų, išskyrus tuos atvejus, kai šie duomenys yra būtini jų darbo funkcijoms atlikti;

27.7. Tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (**vientisumo ir konfidencialumo principas**).

V SKYRIUS

ASMENS DUOMENŲ TVARKYMO TERMINAI

28. Asmens duomenys tvarkomi ir saugomi ne ilgiau, nei to reikalauja duomenų tvarkymo tikslai.

29. Įstaigoje nustatytas bendrasis duomenų saugojimo terminas yra 10 metų, kuris taikomas, atsižvelgiant į Lietuvos Respublikoje galiojantį bendrąjį ieškinio senaties terminą pareikšti, vykdyti arba apginti teisinius reikalavimus.

30. Atskirų rūšių duomenims taikomi specialūs asmens duomenų saugojimo terminai:

30.1. dokumentuose ar bylose esantys asmens duomenys, saugomi terminus, nustatytus pagal Bendrųjų dokumentų saugojimo terminų rodyklę (patvirtintą Lietuvos vyriausiojo archyvaro 2011 m. kovo 9 d. įsakymu Nr. V-100), atsižvelgiant į dokumento ar bylos, kuriuose šie duomenys yra nurodyti, rūšį. Pasibaigus dokumento, kuriame šie duomenys yra nurodyti, saugojimo terminui, dokumentas sunaikinamas Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka ar priimamas sprendimas dėl dokumento saugojimo termino pratęsimo.

30.2. viešųjų pirkimų dokumentai (paraiškos ir pasiūlymai, jų nagrinėjimo ir vertinimo dokumentai, protokolai, kiti su pirkimu susiję dokumentai) saugomi 5 metus po pirkimo pabaigos, po to sunaikinami;

30.3. telefono įrašai saugomi 6 mėnesius, po to ištrinami;

(30.4. papunktis pakeistas BI „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15)

30.4. vaizdo kamerų, stebinančių įėjimą į pastatą ir patalpas, kuriose įsikūrusi Įstaiga, įrašai saugomi patalpų nuomotojo nustatytą laikotarpį;

30.5. LR specialiųjų tyrimų tarnybos pateikta išvada dėl darbuotojo tinkamumo einamoms pareigoms saugoma darbuotojo sutarties galiojimo laikotarpiu, pasibaigus darbo santykiams nedelsiant sunaikinama;

30.6. siekiančių įsidarbinti Įstaigoje pretendentų asmens duomenys ir atrankoje (konkurse) užimti pareigybę Įstaigoje dalyvavusių pretendentų testo žodžiu (pokalbio) eigai fiksuoti daromi skaitmeniniai garso įrašai saugomi 1 mėnesį nuo konkurso rezultatų paskelbimo dienos, po to ištrinami;

30.7. pranešimai, teikiami vadovaujantis Lietuvos Respublikos pranešėjų apsaugos įstatymu ir Lietuvos Respublikos Vyriausybės 2018 m. lapkričio 14 d. nutarime Nr. 1133 „Dėl Lietuvos Respublikos pranešėjų apsaugos įstatymo įgyvendinimo“, ir jų nagrinėjimo metu tvarkomi duomenys saugomi penkerius metus nuo paskutinio priimto sprendimo nagrinėjant atitinkamą informaciją.

30.8. Duomenų tvarkytojo statusu Įstaigoje tvarkomi asmens duomenys saugomi sutarčių, sudarytų su Klientais, galiojimo laikotarpiu, bet ne ilgiau negu Bendrųjų dokumentų saugojimo terminų rodyklėje, patvirtintoje Lietuvos vyriausiojo archyvaro 2011 m. kovo 9 d. įsakymu Nr. V-100, nurodytą terminą. Pasibaigus dokumento, kuriame šie duomenys yra nurodyti, saugojimo terminui (kuris nustatytas rodyklėje) dokumentas sunaikinamas Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka ar priimamas sprendimas dėl dokumento saugojimo termino pratęsimo.

30.9. Darbuotojo elektroninio pašto dėžutėje surinkti asmens duomenys (persiųsti ir/ ar gauti dokumentai, ataskaitos, lentelės ar kitokios formos informacijos atvaizdas, kuriuose yra asmens duomenys) gali būti saugomi elektroninio pašto dėžutėje ne ilgiau negu 6 mėnesius nuo jų gavimo/ persiuntimo. Darbuotojai privalo užtikrinti, kad suėjus nustatytam terminui visi asmens duomenys iš pašto dėžutės būtų pašalinti, esant būtinumui (t.y. nustačius, kad saugoti tam tikrus asmens duomenis toliau yra būtina) perkeltiant juos į duomenų bazes.

31. Pasibaigus asmens duomenų saugojimo terminui, jis gali būti pratęstas, jeigu Įstaiga nustato, kad saugoti asmens duomenis toliau yra būtina, ypač atsižvelgiant į būtinybę panaudoti asmens duomenis kaip įrodymą ikiteisminiame ar kitokiame tyrime, įskaitant ir Valstybinės duomenų apsaugos inspekcijos vykdomame tyrime, civilinėje, administracinėje ar baudžiamojoje byloje ar kitais teisės aktų nustatytais atvejais. Jeigu Įstaiga nustato, kad saugoti tam tikrus asmens duomenis toliau yra būtina priimamas

sprendimas dėl dokumento saugojimo termino pratęsimo.

32. Jei surinkti asmens duomenys reikalingi, siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus arba kaip įrodymai ikiteisminiame ar kitame tyrime, civilinėje, administracinėje ar baudžiamojoje byloje, duomenys gali būti saugomi tiek, kiek yra būtina tokiems tikslams pasiekti pagal teisminę, administracinę arba neteisminę procedūrą ir sunaikinami nedelsiant, kai tampa nebereikalingi.

VI SKYRIUS

TECHNINĖS IR ORGANIZACINĖS ASMENS DUOMENŲ SAUGUMO PRIEMONĖS

33. Įstaigoje yra įdiegtos organizacinės ir techninės duomenų saugumo priemonės, skirtos užtikrinti tinkamą automatinio būdu tvarkomų duomenų saugumą, taip pat apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo. Įstaigoje taikomų Duomenų apsaugos priemonių sąrašas patvirtintas šių [Taisyklių 2 priede](#).

34. Įstaigos Informacinių technologijų skyrius yra atsakingas už automatinio būdu tvarkomų duomenų saugumo priemonių parinkimą taip, kad duomenų tvarkymas atitiktų BDAR ir būtų užtikrintas automatinio būdu tvarkomų duomenų saugumas, šių priemonių įdiegimą ir įgyvendinimo kontrolę.

35. Įstaigos Informacinių technologijų skyrius periodiškai, ne rečiau kaip vieną kartą per metus, ir kiekvieną kartą atsiradus poreikiui (kai Įstaigoje pasikeičia asmens duomenų tvarkymo veiksmai, asmens duomenų tvarkymo operacijos arba Įstaigoje įvyksta struktūriniai, technologiniai ar kitokie pakeitimai, kurie turi įtakos asmens duomenų tvarkymui automatinio būdu, gavus darbuotojų pranešimus dėl galimo Įstaigoje įdiegtų techninių saugumo priemonių patikimumo) privalo vertinti, ar Įstaigoje įdiegtos automatinio būdu tvarkomų duomenų saugumo priemonės yra pakankamos. Nustačius, kad Įstaigoje įdiegtos automatinio būdu tvarkomų duomenų saugumo priemonės yra nepakankamos, Informacinių technologinių skyriaus vadovas privalo kreiptis į Įstaigos direktorių su konkrečiais pasiūlymais inicijuoti papildomų priemonių įsigijimą ir įdiegimą.

36. Kiekvienas įstaigoje dirbantis darbuotojas ir kiti asmenys, kurie tvarko Įstaigoje saugomus asmens duomenis, atlikdami savo darbo funkcijas ir tvarkydami asmens duomenis, privalo įgyvendinti Įstaigoje taikomas organizacines ir technines asmens duomenų saugumo priemones ir vykdyti reikalavimus, aprašytus [Taisyklių VII skyriuje](#).

VII SKYRIUS

REIKALAVIMAI ASMENIMS, TVARKANTIEMS ASMENS DUOMENIS

37. Kiekvienas įstaigoje dirbantis darbuotojas ir kiti asmenys tvarkydami Įstaigoje asmens duomenis privalo:

37.1. laikytis pagrindinių asmens duomenų tvarkymo reikalavimų ir saugumo reikalavimų, įtvirtintų BDAR, ADTAĮ, šiose Taisyklėse ir kituose teisės aktuose;

37.2. laikytis šių [Taisyklių IV skyriuje](#) aprašytų asmens duomenų tvarkymo ir apsaugos principų;

37.3. laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jis susipažino vykdydamas savo funkcijas, išskyrus, jeigu tokia informacija buvo vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas; pareiga saugoti asmens duomenų paslaptį galioja ir perėjus dirbti į kitas pareigas ar pasibaigus darbo santykiams Įstaigoje;

37.4. asmens duomenis rinkti nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau jų netvarkyti

su tais tikslais nesuderinamu būdu. Vertinant, ar duomenys gali būti tvarkomi kitais tikslais nei tais, kuriais buvo surinkti, kai tikslų suderinamumas nėra akivaizdus, turi būti konsultuojamai su duomenų apsaugos pareigūnu;

37.5. rinkdami ir tvarkydami asmens duomenis laikytis tikslingumo, proporcingumo ir duomenų kiekio mažinimo principų, t. y. nereikalauti iš Klientų ar duomenų subjektų pateikti tų duomenų, kurie nėra būtini Įstaigos funkcijoms vykdyti, nekaupiti ir netvarkyti perteklinių duomenų ir duomenų, kurie nėra būtini atitinkamiems tikslams pasiekti, taip pat neteikti Klientams ir/ ar Steigėjui perteklinių duomenų, kurie nėra būtini jų nurodytiems tikslams pasiekti;

37.6. laikytis šiose Taisyklėse nustatytų organizacinių ir techninių asmens duomenų saugumo priemonių, siekiant užkirsti kelią netyčiniam ar neteisėtam tvarkomų asmens duomenų sunaikinimui, praradimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui;

37.7. neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su asmens duomenimis asmeniui, kuris nėra įgaliotas tvarkyti asmens duomenų;

37.8. su asmens duomenimis atlikti tik tuos veiksmus, kuriems atlikti Įstaigos darbuotojui yra suteiktos teisės;

37.9. tvarkyti asmens duomenis tik tuo tikslu, kuriuo yra renkami;

37.10. nedelsiant pranešti Įstaigos direktoriui ir/ ar duomenų apsaugos pareigūnui apie bet kokią įtartina situaciją, kuri gali kelti grėsmę Įstaigoje tvarkomų asmens duomenų saugumui;

37.11. įvykus duomenų saugumo incidentui, apie duomenų saugumo incidentus ir saugumo priemones, kurių imtasi siekiant apsaugoti asmens duomenis, nedelsiant informuoti Įstaigos duomenų apsaugos pareigūną;

38. Prieš kiekvieną asmens duomenų tvarkymo operaciją (veiksmą) darbuotojas turi įvertinti, ar toks asmens duomenų tvarkymas atitinka [Taisyklių IV skyriuje](#) nurodytus principus ir reikalavimus bei užtikrinti, kad duomenų tvarkymo operacija (veiksmas) atitiktų minėtus reikalavimus. Įstaigoje tvarkomi konkretūs asmens duomenys, jų tvarkymo tikslai, saugojimo terminai bei tvarkymo teisiniai pagrindai yra fiksuojami Asmens duomenų tvarkymo veiklos įrašų registre, kuris pildomas Įstaigoje [Taisyklių III skyriuje](#) nustatyta tvarka. Darbuotojas turi įsitikinti, kad kiekviena jo atliekama asmens duomenų tvarkymo operacija (veiksmas) atitinka Asmens duomenų tvarkymo veiklos įrašų registre nurodytus duomenis (asmens duomenų tvarkymo pagrindą ir tikslą, saugojimo terminą ir kitus registre užfiksuotus duomenys). Jei darbuotojas pastebi, kad Asmens duomenų tvarkymo veiklos įrašai neapima tam tikros operacijos, apie tai turi nedelsdamas informuoti duomenų apsaugos pareigūną ir gauti jo konsultaciją.

39. Darbuotojai privalo taip organizuoti savo darbą taip, kad būtų apribota galimybė kitiems asmenims sužinoti tvarkomus asmens duomenis. Ši nuostata įgyvendinama taikant „Švaraus stalo ir švaraus ekrano“ politiką:

39.1. pasitraukus iš darbo vietos negalima palikti dokumentų su tvarkomais asmens duomenimis be priežiūros taip, kad juose esančią informaciją galėtų perskaityti asmenys, neturintys teisės dirbti su konkrečiais asmens duomenimis;

39.2. dirbti su dokumentais taip, kad jų (ar jų fragmentų) negalėtų perskaityti atsitiktiniai asmenys (Įstaigos lankytojai);

39.3. trumpam pasitraukus iš darbo vietos privaloma įjungti slaptažodžiu apsaugotą kompiuterio ekrano užsklandą, kad kiti asmenys nepamatytų ekrane rodomos informacijos ir neturėtų prieigos prie kompiuteryje tvarkomų duomenų;

39.4. net ir trumpam išeinant iš kabineto, jei kabinete nebelieka kitų darbuotojų, privaloma užrakinti duris;

39.5. baigus darbą privaloma uždaryti visus kompiuterio programų langus ir išjungti kompiuterį;

39.6. baigus darbą negalima palikti ant stalo dokumentų (jų kopijų) ir duomenų laikmenų, privaloma sudėti juos į rakinamas spintas;

39.7. nebereikalingi dokumentai turi būti ne išmetami, o sunaikinami dokumentų naikintuvu;

39.8. dokumentai iš spausdintuvų ir kopijavimo aparatų turi būti išimami nedelsiant asmens, kuris inicijavo spausdinimą ar kopijavimą;

39.9. darbuotojas išeinantis iš darbo kabineto paskutinis, privalo patikrinti, ar patikimai uždaryti langai, ir užrakinti duris.

40. Dokumentai bei jų kopijos, dokumentų projektai, finansavimo, buhalterinės apskaitos ir atskaitomybės ar kitos bylos, kuriose yra asmens duomenų, turi būti saugomos rakinamose spintose.

41. Dokumentai, kuriuose yra asmens duomenų, neturi būti laikomi visiems prieinamoje matomoje vietoje.

42. Nesant būtinybės, dokumentai, kuriuose yra asmens duomenų, neturi būti kopijuojami ar kitaip dauginami.

43. Dokumentų kopijos, kuriose nurodomi duomenų subjekto duomenys, turi būti sunaikinamos tokiu būdu, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio, pavyzdžiui, susmulkinant, tačiau jokių būdu neišmetant į šiukšliadėžę ar nepaliekant duomenų šalia jos ar kitoje atviroje vietoje. Automatinio būdu surinkti duomenys sunaikinami ištrinant nebereikalingas asmens duomenų bylas iš saugojimo laikmenos taip, kad jų nebūtų galima atgaminti. Už duomenų sunaikinimą atsakingas duomenis naikinantis darbuotojas.

44. Darbuotojai, vykdantys duomenų subjekto duomenų tvarkymo funkcijas, privalo tvarkyti dokumentus saugiai, vengiant nereikalingų kopijų su duomenų subjekto duomenimis kaupimo ir kt.).

45. Darbuotojai gali atskleisti, perduoti asmens duomenis, supažindinti ar kitaip suteikti prieigą prie asmens duomenų tik tiems darbuotojams, kurie pagal pareigas ar atskirus pavedimus turi teisę dirbti su asmens duomenimis, vadovaujantis principu „Būtina žinoti“. Principas „Būtina žinoti“ reiškia, kad asmens duomenys gali būti atskleisti teisę ar atitinkamus leidimus susipažinti su atitinkamais duomenimis turintiems asmenims, kuriems vykdant darbo funkcijas reikalinga susipažinti su duomenimis. Asmeniui gali būti patikėti tik tokios apimties asmens duomenys, kokios reikia to asmens darbo funkcijoms atlikti.

46. Darbuotojai, kurie automatinio būdu tvarko asmens duomenis, privalo laikytis Įstaigoje patvirtintos *Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos reikalavimų* ir šių specialiųjų reikalavimų:

46.1. Darbuotojai, kurie automatinio būdu tvarko asmens duomenis arba iš kurių kompiuterių galima patekti į Įstaigos informacines sistemas, kuriose yra saugomi asmens duomenys, savo kompiuteriuose privalo naudoti slaptažodžius. Darbuotojas privalo laikyti paslapyje slaptažodžius ir neleisti kitiems asmenims jais naudotis.

46.2. Slaptažodžiai esant būtinybei (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei ir pan.) turi būti keičiami periodiškai, taip pat susidarius tam tikroms aplinkybėms (pvz.: pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims).

46.3. Nesant būtinybės, rinkmenos su Klientų, kitų fizinių asmenų duomenimis neturi būti dauginamos skaitmeniniu būdu, t. y. kuriamos rinkmenų kopijos vietiniuose kompiuterių diskuose, nešiojamose laikmenose, nuotolinėse rinkmenų talpyklose ir kt.

46.4. Esant būtinybei persiųsti duomenis Klientui, Steigėjui, kompetentingai institucijai ar jų įgaliotiems darbuotojams elektroniniu paštu informacija gali būti siunčiama tik adresato darbovietės serveryje sukurtu darbinio elektroniniu paštu, nekeliančių abejonių dėl elektroninio pašto saugumo ir patikimumo. Draudžiamas informacijos ir duomenų siuntimas į asmenines el. pašto dėžutes ir/ ar į Įstaigos nepatvirtintas

trečiųjų šalių viešąsias elektroninio pašto sistemas ir saugojimo serverius (pvz., naudojant paskyras „Google Gmail“, „Mail.ru“, „Hotmail“ ir kt.), išskyrus toliau nurodytame punkte nustatytą atvejį.

46.5. Atsiskaitymo lapeliai Kliento darbuotojams gali būti siunčiami Kliento darbuotojams į atitinkamo darbuotojo asmeninę elektroninio pašto dėžutę, kuri nurodyta Kliento darbuotojo pateiktame prašyme (kuriame Kliento darbuotojas aiškiai išreiškia pageidavimą gauti atsiskaitymo lapelį prašyme nurodytu elektroniniu paštu). Tokiu atveju atsiskaitymo lapeliai gali būti siunčiami asmeniniu elektroniniu paštu tik jei siunčiama informacija yra apsaugota naudojant slaptažodį ar kitą šifravimą. Šifravimo raktai ar slaptažodžiai informacijos gavėjui turi būti perduodami naudojant kitus perdavimo būdus ar kanalus – draudžiama šifravimo kodus, slaptažodžius siųsti tuo pačiu elektroniniu paštu.

46.6. Darbinį elektroninį paštą mobiliuose įrenginiuose (išmaniuosiuose telefonuose) leidžiama naudoti tik naudojant įrenginį, apsaugotą užrakinimo kodu, slaptažodžiu, biometrinės apsaugos priemonėmis (piršto anspaudas ar veido atpažinimas);

46.7. Darbuotojai, kurių darbo kompiuteriuose saugomi asmens duomenys arba iš kurių kompiuterių galima patekti į Įstaigos informacines sistemas, kuriose yra saugomi asmens duomenys, savo darbo kompiuteriuose turi naudoti slaptažodžius; „svečio“ (angl. *guest*) tipo, t. y. neapsaugoti slaptažodžiais, vartotojai yra draudžiami. Šiuose kompiuteriuose taip pat reikia naudoti ekrano užsklandą su slaptažodžiu.

47. Jei darbuotojas abejoja Įstaigoje įdiegtų techninių saugumo priemonių patikimumu, jis privalo kreiptis į tiesioginį vadovą, o pastarasis į Informacinių technologijų skyriaus vadovą, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir įdiegimas.

VIII SKYRIUS

DUOMENŲ APSAUGOS PAREIGŪNAS

48. Įstaigos duomenų apsaugos pareigūnas stebi ir kontroliuoja, kaip Įstaigoje yra laikomasi BDAR, ADTAI ir kitų asmens duomenų apsaugą reglamentuojančių teisės aktų nuostatų.

49. Pareigūno vardas, pavardė ir kontaktiniai duomenys skelbiami Įstaigos interneto svetainėje www.skaitlis.lt.

50. Duomenų apsaugos pareigūnas turi teisę:

50.1. būti informuotas ir įsitraukti į visų su asmens duomenų apsauga ir privatumu susijusių klausimų nagrinėjimą Įstaigoje;

50.2. susipažinti su asmens duomenimis, dalyvauti duomenų tvarkymo operacijose;

50.3. atlikdamas savo funkcijas gauti visus reikiamus išteklius (laiko, tinkamų darbo sąlygų ir kt.) bei galimybę išlaikyti ekspertines duomenų apsaugos teisės ir praktikos žinias.

51. Duomenų apsaugos pareigūnas Įstaigoje vykdo šias užduotis:

51.1. padeda užtikrinti, kad Įstaigoje vykdomas asmens duomenų tvarkymas atitiktų BDAR, kitų asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų reikalavimus, tinkamai įvertinant duomenų tvarkymo operacijas, duomenų tvarkymo pobūdį, aprėptį, kontekstą, tikslus, potencialų pavojų;

51.2. stebi, kaip laikomasi BDAR ir kitų asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų reikalavimų, Taisyklių, kitų vidaus dokumentų, susijusių su asmens duomenų apsauga;

51.3. sprendžia, ar Įstaigoje dėl tam tikros vykdomos asmens duomenų tvarkymo operacijos turi būti atliekamas poveikio duomenų apsaugai vertinamas, kaip tai aprašyta [Taisyklių XIV skyriuje](#); nustačius, kad toks vertinimas yra būtinas, inicijuoja jo atlikimą;

51.4. informuoja Įstaigos direktorių ir kitus darbuotojus apie jų pareigas pagal BDAR ir kitus asmens

duomenų teisinę apsaugą reglamentuojančius teisės aktus ir juos konsultuoja dėl konkrečių pareigų vykdymo;

51.5. informuoja Įstaigos direktorių apie bet kokias neatitiktis, pažeidimus asmens duomenų apsaugos srityje, kuriuos pareigūnas nustato vykdydamas savo funkcijas;

51.6. konsultuoja Įstaigos darbuotojus, dirbančius su asmens duomenimis, asmens duomenų teisinės apsaugos klausimais;

51.7. bendradarbiauja, yra kontaktinis asmuo bendradarbiaujant su Valstybine duomenų apsaugos inspekcija;

51.8. vykdo kitas šiose Taisyklėse nustatytas funkcijas.

52. Duomenų apsaugos pareigūnas privalo užtikrinti slaptumą ir (ar) konfidencialumą, susijusį su jo užduočių vykdymu, laikydamasis Europos Sąjungos ar valstybės narės teisės aktų reikalavimų.

53. Duomenų apsaugos pareigūnas yra nepriklausomas asmens duomenų apsaugos klausimais. Duomenų subjektai gali kreiptis į pareigūną visais klausimais, susijusiais su jų asmens duomenų tvarkymu ir savo teisių pagal BDAR įgyvendinimu. Konkrečias užduotis ar veiksmus, būtinus įgyvendinant asmens duomenų apsaugos reikalavimus, išskyrus Taisyklėse tiesiogiai aptartus atvejus, atlieka už asmens duomenų tvarkymą atsakingas atitinkamas Įstaigos skyrius.

IX SKYRIUS

DUOMENŲ TEIKIMAS

54. Asmens duomenys trečiosioms šalims gali būti teikiami:

54.1. subjektams, kuriems asmens duomenis teikti Įstaigą įpareigoja Lietuvos Respublikos įstatymai ar kiti teisės aktai – tų teisės aktų vykdymo tikslu;

54.2. valdžios institucijoms, vadovaujantis jų pateiktais teisiniais reikalavimais;

54.3. Įstaigos ir Klientų darbuotojų asmens duomenys: socialinio draudimo mokesčio administravimo tikslu – Valstybinio socialinio draudimo fondo valdybai prie Socialinės apsaugos ir darbo ministerijos, mokesčių administravimo tikslu – Valstybinei mokesčių inspekcijai prie Lietuvos Respublikos finansų ministerijos;

54.4. Įstaigos ir Klientų darbuotojų, prekių ir paslaugų tiekėjų (fizinių asmenų) asmens duomenys – Antstolių kontoroms, vadovaujantis jų pateiktais reikalavimais dėl atitinkamos Antstolių kontoros žinioje esančių vykdomųjų bylų;

54.5. asmenų, pateikusių Įstaigai skundą, pranešimą, pareiškimą ar prašymą, ir duomenų valdytojų (fizinių asmenų) asmens duomenys ginčo dėl Įstaigos priimto sprendimo teisėtumo nagrinėjimo tikslu – teismams ir (ar) darbo ginčų komisijoms ar kitoms ikiteisminėms institucijoms, kitiems asmenims, įgaliotiems pagal kompetenciją nagrinėti gautą prašymą ar skundą;

54.6. ginčo nagrinėjimo tikslu – ikiteisminį tyrimą arba kitą tyrimą atliekančiai įstaigai, prokurorui, teismui ar darbo ginčų komisijoms dėl jų žinioje esančių administracinių, civilinių, darbo ar baudžiamųjų bylų, taip pat teisinių paslaugų teikėjams, teikiantiems Įstaigai teisinio atstovavimo paslaugas;

54.7. Įstaigos ir/ ar Kliento veiklos patikrinimo, audito, analizės ar kito įvertinimo tikslais – finansinį, mokesčių ar valdymo auditą atliekantiems auditoriams ar kitus patikrinimus atliekantiems asmenims;

54.8. Valstybinei darbo inspekcijai, vykdančiai patikrinimus ar nelaimingo atsitikimo darbe tyrimus;

54.9. Lietuvos statistikos departamentui pagal teisės aktų reikalavimus;

54.10. atsiskaitymų vykdymo tikslu – bankams ar kitoms finansinėms įstaigoms;

(54.11. papunktis pakeistas BJ „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15)

54.11. asmenų, patekusių į vaizdo stebėjimo lauką, vaizdo duomenys galimų teisės aktų pažeidimų nustatymo tikslu – ikiteisminio tyrimo institucijoms, teismams ar kitoms valstybės įgaliotoms institucijoms;

54.12. asmenų, skambinusių į Įstaigą telefonu, pokalbių duomenys galimų teisės aktų pažeidimų nustatymo tikslu – ikiteisminio tyrimo institucijoms, teismams ar kitoms valstybės įgaliotoms institucijoms;

54.13. trečiajai šaliai, teikiančiai paslaugas Įstaigai, įskaitant teisės, finansų, mokesčių patarėjams, draudikams, turint teisėtą pagrindą asmens duomenims teikti;

54.14. Įstaigos sudarytų su trečiaisiais asmenimis (prekių ar paslaugų teikėjais) sutarčių įgyvendinimo ir/ ar administravimo tikslu – sutarties šalims turint teisėtą pagrindą asmens duomenims teikti;

54.15. Įstaigai ir/ ar Klientui įsiskolinusių asmenų duomenis – skolos išieškojimo paslaugas teikiantiems subjektams pagal sudarytą skolų išieškojimo paslaugų teikimo sutartį;

54.16. kitoms šalims, kai to reikalaujama pagal įstatymus arba tai yra būtina siekiant apsaugoti Įstaigos teisėtus interesus – asmens duomenų teikimą reglamentuojančių teisės aktų nustatytais atvejais ir tvarka.

55. Įstaiga duomenų subjektų duomenis duomenų gavėjams taip pat gali teikti pagal teisės aktų reikalavimus, taikomus duomenų teikėjui ir gavėjui, arba vienkartinį duomenų gavėjo prašymą, nepažeisdama teisės aktuose įtvirtintų reikalavimų ir asmens duomenų konfidencialumo užtikrinimo bei laikydamosi duomenų valdytojo atskaitomybės principo.

56. Vienkartinio duomenų teikimo atveju Įstaiga, teikdama asmens duomenis pagal trečiosios šalies vienkartinį prašymą, pirmenybę teikia duomenų teikimui elektroninių ryšių priemonėmis, jeigu prašyme nenurodyta kitaip. Siekiant įgyvendinti BDAR 5 straipsnio 1 dalies f punkte įtvirtintą konfidencialumo principą, prašymai pateikti asmens duomenis nagrinėjami tik tinkamai nustačius asmens tapatybę.

57. Siekiant įgyvendinti BDAR 5 straipsnio 2 dalyje įtvirtintą duomenų valdytojo atskaitomybės principą, duomenys trečiosioms šalims gali būti teikiami tik tada, kai duomenų gavėjas teiktame prašyme nurodo aplinkybes, pagrindžiančias, kad duomenų tvarkymas (teikimas) atitinka BDAR 5 straipsnyje įtvirtintus principus ir yra pagrįstas bent viena BDAR 6 straipsnio 1 dalyje arba 9 straipsnio 2 dalyje įtvirtinta teisėto duomenų tvarkymo sąlyga. Prašyme privaloma nurodyti:

57.1. duomenų gavimo konkretų ir aiškiai apibrėžtą tikslą;

57.2. duomenų tvarkymo (gavimo) teisinį pagrindą, įtvirtintą Lietuvos Respublikos arba Europos Sąjungos teisės aktuose, konkrečią jų nuostatą, suteikiančią teisę duomenų gavėjui gauti asmens duomenis, ir teisėto tvarkymo sąlygą, įtvirtintą BDAR 6 straipsnio 1 dalyje arba 9 straipsnio 2 dalyje (kai prašoma specialių kategorijų asmens duomenų), kurią atitinka nurodytas teisėto tvarkymo (gavimo) pagrindas;

57.3. duomenų tvarkymo (teikimo) teisinį pagrindą, įtvirtintą Lietuvos Respublikos arba Europos Sąjungos teisės aktuose, konkrečią jų nuostatą, suteikiančią teisę Įstaigai pateikti duomenis duomenų gavėjui, ir teisėto tvarkymo sąlygą BDAR 6 straipsnio 1 dalyje arba 9 straipsnio 2 dalyje (kai prašoma specialių kategorijų asmens duomenis), kurią atitinka nurodytas teisėto tvarkymo (teikimo) pagrindas;

57.4. konkrečią prašomų duomenų apimtį, t. y. kokių konkrečių duomenų prašoma: vardo, pavardės, paskirtos išmokos dydžio ir pan. Prašymai pateikti visą turimą informaciją apie asmenį nelaikytini konkrečiais;

57.5. kai duomenis pateikti prašoma vadovaujantis BDAR 6 straipsnio 1 dalies e arba f punktais, prašyme turi būti išsamiai pagrįsta, kodėl šių asmenų interesai yra viršesni už duomenų subjekto teises ir laisves arba kodėl toks duomenų tvarkymas yra būtinas viešajam interesui ir valdžios funkcijoms įgyvendinti;

57.6. kai nurodoma, kad duomenis pateikti prašoma vadovaujantis BDAR 6 straipsnio 1 dalies e arba f punktais, duomenų gavėjas privalo įgyvendinti duomenų subjekto, kurio duomenis prašo pateikti, teisę

nesutikti su duomenų tvarkymu (teikimu) ir pateikti tai patvirtinančius įrodymus.

58. Asmens duomenų teikimui valstybės ir savivaldybės institucijoms ir įstaigoms, kai šios institucijos ir įstaigos pagal konkretų paklausimą gauna asmens duomenis įstatymų nustatytoms kontrolės funkcijoms vykdyti, taikomos visos šiame skyriuje aptartos duomenų teikimo (gavimo) sąlygos.

59. Įstaigos tvarkomi asmens duomenys ir Klientų perduoti tvarkyti asmens duomenys gali būti teikiami Steigėjui – Vilniaus miesto savivaldybei Įstaigos ir/ ar Klientų veiklos finansavimo, planavimo, priežiūros ir kontrolės tikslais pagal Steigėjo pareikalavimą.

60. Įstaigos ir Steigėjo darbuotojai be papildomo teisinio reikalavimo gali būti asmens duomenų gavėjais, jeigu jie dalyvauja duomenų valdytojo arba duomenų tvarkytojo vykdomose tvarkymo operacijose arba šie duomenys yra būtini darbuotojo funkcijoms vykdyti. Teikdamas duomenis duomenų gavėjams, Įstaigos darbuotojas, siekdamas užtikrinti duomenų konfidencialumą, turi teisę reikalauti duomenų gavėjo (darbuotojo) nurodyti duomenų gavimo tikslą ir konkrečią duomenų apimtį.

X SKYRIUS

ASMENS DUOMENŲ TVARKYTOJAI

61. Tais atvejais, kai Įstaiga įgalioja duomenų tvarkytoją atlikti asmens duomenų tvarkymo veiksmus, tarp Įstaigos ir duomenų tvarkytojo turi būti sudaroma rašytinė asmens duomenų tvarkymo sutartis arba kitoks oficialus dokumentas.

62. Sprendimą perduoti duomenų subjekto duomenų tvarkymą asmens duomenų tvarkytojui priima Įstaigos direktorius arba jo įgaliotas asmuo.

63. Įstaiga, sutartimi įgaliodama duomenų tvarkytoją tvarkyti asmens duomenis, nurodo, kad asmens duomenys būtų tvarkomi atsižvelgiant į asmens duomenų tvarkymą reglamentuojančius teisės aktus, Įstaigos nurodymus, taip pat nurodoma, kokius asmens duomenų tvarkymo veiksmus privalo atlikti duomenų tvarkytojas Įstaigos vardu, duomenų tvarkytojo įsipareigojimai Įstaigai, įskaitant įsipareigojimą laikytis BDAR įtvirtintų reikalavimų, duomenų tvarkymo trukmė, pobūdis, asmens duomenų rūšis, duomenų subjektų kategorijos, duomenų tvarkytojo pareiga ištrinti arba grąžinti Įstaigai asmens duomenis, jų kopijas, pabaigus Įstaigai teikti paslaugas.

64. Įstaiga, sudarydama sutartį su duomenų tvarkytoju, be kita ko, nurodo, kad duomenų tvarkytojas privalo užtikrinti Įstaigos perduodamų tvarkyti duomenų konfidencialumą, o ketindamas tvarkymui pasitelkti trečiuosius asmenis (kitus duomenų tvarkytojus), duomenų tvarkytojas privalo informuoti Įstaigą ir užtikrinti, kad pasitelktas subtvarkytojas laikytųsi tų pačių reikalavimų, kurie nustatyti tvarkytojui.

65. Aukščiau nurodytos nuostatos gali būti tiek įtraukiamos į pagrindinę sutartį, tiek aptariamose atskirame susitarime dėl asmens duomenų saugumo.

66. Siekiant tinkamai valdyti asmens duomenų judėjimą, Įstaigoje yra tvarkomas duomenų tvarkytojų registras pagal patvirtintą formą (**Taisyklių 3 priedas**). Už duomenų tvarkytojų registro pildymą atsakingas duomenų apsaugos pareigūnas.

XI SKYRIUS

VAIZDO IR GARSO DUOMENŲ TVARKYMO YPATUMAI

(67-69 punktai pakeisti BJ „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15)

67. Pastato, esančio V. Gerulaičio g. 1, LT-08200, Vilniuje, ir įeigos į patalpas, kuriose įsikūrusi Įstaiga, vaizdo stebėjimą vykdo patalpų nuomotojas, esantis vaizdo duomenų valdytoju.

68. Vaizdo duomenys renkami darant vaizdo duomenų įrašą. Vaizdo duomenys renkami, tvarkomi ir

saugomi duomenų valdytojo nustatyta tvarka ir terminais.

69. *Vaizdo duomenų įrašų atsargines kopijas Įstaiga gali rinkti ir turėti tokiais atvejais:*

69.1. *vaizdo duomenys teikiami **Taisyklių 70 punkte** nurodytiems subjektams;*

69.2. *kai yra nustatoma pagrįstas poreikis vaizdo duomenų įrašą saugoti ilgesnį laikotarpį dėl vaizdo įrašų duomenų panaudojimo kaip įrodymo ikiteisminiame tyrime, civilinėje, administracinėje ar baudžiamojame byloje, kituose teisiniuose procesuose siekiant apginti Įstaigos ir (ar) trečiųjų asmenų pagrįstas teises ir laisves ar kitais įstatymų nustatytais atvejais.*

70. *Vaizdo duomenys gali būti teikiami ikiteisminį tyrimą arba kitą tyrimą atliekančiai įstaigai, prokurorui, teismui ar darbo ginčų komisijoms dėl jų žinioje esančių administracinių, civilinių, darbo ar baudžiamųjų bylų kaip įrodymai ar kitais įstatymų nustatytais atvejais.*

71. *Prieiga prie vaizdo duomenų gali būti suteikta tik tam Įstaigos darbuotojui, kuriam asmens duomenys yra reikalingi jam priskirtoms funkcijoms vykdyti.*

72. *Įgyvendinant duomenų subjekto teisę susipažinti su savo vaizdo duomenimis, užtikrinama trečiųjų asmenų teisė į privatų gyvenimą, t. y. duomenų subjektui susipažįstant su vaizdo įrašu, jeigu vaizdo įrašė matomi kiti asmenys, kurių tapatybė gali būti nustatyta, ar kita informacija, kuri gali pažeisti trečiųjų asmenų privatumą, šie vaizdai turi būti retušuoti ar kitais būtais panaikinama galimybė identifikuoti trečiuosius asmenis.*

73. *Duomenų subjektas apie duomenų tvarkymą vykdant vaizdo stebėjimą informuojamas iškabinant informacines lenteles su filmavimo kameros simboliu prieš patenkant į patalpas ar teritoriją, kurioje vykdomas vaizdo stebėjimas.*

74. *(neteko galios BJ „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15).*

75. *Įstaigoje yra įrašomi interesantų konsultavimo telefonu pokalbiai.*

76. *Pokalbių telefonu duomenų valdytojas – Įstaiga, kuri pati tvarko duomenis. Duomenų tvarkytojai nėra pasitelkiami.*

77. *Pokalbių telefonu duomenys renkami darant garso įrašą. Įrašomi Įstaigos telefonų įeinantys ir išeinantys pokalbiai. Garso įrašai saugomi Įstaigos serveryje.*

78. *Pokalbiai telefonu įrašomi ir pokalbių įrašų duomenys tvarkomi siekiant užtikrinti Įstaigos aptarnavimo bei teikiamų konsultacijų telefonu kokybę ir vienodos praktikos formavimą, interesantų prašymų ir skundų nagrinėjimo objektyvumą.*

79. *Telefoninio pokalbio metu įrašomi šie duomenys: skambinančiojo asmens telefono numeris, asmenį aptarnaujančio darbuotojo telefono numeris, pokalbio laikas, trukmė ir pokalbio garso įrašas. Pokalbio garso įrašė fiksuojami tie duomenys, kuriuos asmuo ir darbuotojas pateikia vieno pokalbio metu.*

80. *Duomenų subjektas apie garso įrašo darymą ir garso įrašuose fiksuojamų asmens duomenų tvarkymą informuojamas prieš pradėdant daryti garso įrašą.*

81. *Aptarnavimo telefonu kokybės vertinimas perklausant telefoninių pokalbių įrašus vykdomas šiais atvejais: 1) kai atliekamas periodinis asmenų aptarnavimo telefonu kokybės vertinimas; 2) kai yra gautas asmens pranešimas ar skundas dėl galimai netinkamai telefonu suteiktų paslaugų kokybės.*

82. *Teisė perklausti telefoninių pokalbių įrašus suteikiama Įstaigos skyrių vadovams, Įstaigos direktoriui ir jo pavaduotojams, pokalbyje dalyvavusiam Įstaigos darbuotojui, taip pat kitiems įgaliotiems Įstaigos subjektams, dalyvaujantiems administracinėje ir (ar) tarnybinio nusižengimo tyrimo procedūroje, nagrinėjant asmens skundą dėl galimai netinkamai Įstaigos darbuotojo suteiktos paslaugos.*

83. *Organizuojant konkursus (atrankas) eiti Įstaigoje pareigas pretendentų testo žodžiu (pokalbio) eiga fiksuojama darant skaitmeninį garso įrašą, jis perkeliamas į kompiuterinę laikmeną, pridedamas prie*

konkurso protokolo. Pretendentas apie garso įrašo darymą ir garso įrašuose fiksuojamų asmens duomenų tvarkymą informuojamas prieš testo žodžiu (pokalbio) pradžią.

84. Pokalbiai atrankos metu įrašomi ir pokalbių įrašų duomenys tvarkomi įgyvendinant Lietuvos Respublikos Vyriausybės 2017 m. birželio 21 d. nutarimu Nr. 496 patvirtinto Konkursų valstybės ir savivaldybių įmonėse, iš valstybės, savivaldybių ir Valstybinio socialinio draudimo fondo biudžetų bei iš kitų valstybės įsteigtų fondų lėšų finansuojamose valstybės ir savivaldybių įstaigose ir viešosiose įstaigose, kurių savininkė yra valstybė ar savivaldybė, organizavimo ir vykdymo tvarkos aprašo reikalavimus ir siekiant užtikrinti atrankos skaidrumą.

(85 punktas pakeistas BĮ „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15)

85. Garso duomenų saugumas užtikrinamas Įstaigoje organizacinėmis ir techninėmis priemonėmis, nurodytomis [Taisyklių VI skyriuje](#).

86. Vaizdo ir garso duomenų saugojimo terminai nurodyti šių [Taisyklių V skyriuje](#). Pasibaigus nustatytam terminui, duomenys sunaikinami. Jei vaizdo ir/ ar garso įrašų duomenys naudojami kaip įrodymai ikiteisminiame ar kitame tyrime, civilinėje, administracinėje ar baudžiamojoje byloje ar kitais įstatymų nustatytais atvejais, vaizdo ir/ ar garso duomenys gali būti saugomi tiek, kiek reikalinga šiems duomenų tvarkymo tikslams, ir sunaikinami nedelsiant, kai tampa nebereikalingi.

87. Įstaigos darbuotojai, turintys prieigos teisę prie vaizdo ir/ ar garso duomenų, pastebėję vaizdo ir/ ar duomenų saugumo pažeidimus (veiksmus ar neveikimą, galinčius sukelti ar sukeliančius grėsmę asmens duomenų saugumui), turi informuoti Įstaigos duomenų apsaugos pareigūną. Tolimesnė procedūra vykdoma [Taisyklių XV skyriuje](#) nustatyta tvarka.

88. Duomenų subjektų teisės, susijusios su vaizdo ir garso duomenų tvarkymu, įgyvendinamos Įstaigos patvirtintame Asmens duomenų subjektų teisių įgyvendinimo apraše.

XII SKYRIUS

REIKALAVIMAI SUTIKIMUI KAIP ASMENS DUOMENŲ TVARKYMO PAGRINDUI

89. Asmens duomenys sutikimo pagrindu tvarkomi:

89.1. kai, atsižvelgiant į duomenų tvarkymo tikslą ar duomenų kiekį, Įstaiga neturi kito teisinio pagrindo tvarkyti asmens duomenis ar įvykdyti kitus BDAR nustatytus įpareigojimus visa apimtimi; jeigu asmens duomenys, atsižvelgiant į jų kiekį ir tvarkymo tikslus, gali būti tvarkomi bent vienu iš Taisyklėse, BDAR, ADTAI įtvirtintų pagrindų, duomenų subjekto sutikimas papildomai nėra prašomas pateikti;

89.2. kai tai labiausiai atitinka Įstaigos interesus ir padidintos rizikos atvejais sumažina asmens duomenų tvarkymo neteisėtumo riziką.

90. Duomenų subjekto sutikimai gali būti renkami šiais būdais: raštu, įskaitant gautus elektroninėmis priemonėmis, žodžiu ar veiksmais, jeigu yra galimybė įrodyti, kad toks sutikimas buvo duotas, ir jeigu duomenų subjektas savo veiksmais aiškiai sutinka su siūlomu jo asmens duomenų tvarkymu. Pirmenybė kiekvienu atveju yra teikiama duomenų subjekto sutikimams, gautiems raštu (įskaitant gautus elektroninėmis priemonėmis), o kiti sutikimo būdai gali būti naudojami tik kiekvienu konkrečiu atveju įsitikinus, kad yra įmanoma įrodyti duomenų subjekto sutikimo davimo faktą. Duomenų subjekto tylėjimas, iš anksto pažymėti laukai arba neveikimas nelaikomi duomenų subjekto sutikimu.

91. Visais atvejais, kai asmens duomenys yra tvarkomi duomenų subjekto sutikimo pagrindu, Įstaiga privalo kaupti ir turėti įrodymus, kad duomenų subjektas davė sutikimą.

92. Kai asmens duomenys yra tvarkomi sutikimo pagrindu, tvarkomi tik tie asmens duomenys, kurie nurodyti sutikime, tik tais tikslais, kurie nurodyti sutikime, ir su jais atliekamos tik tos tvarkymo operacijos

(veiksmai), kurios nurodytos sutikime. Jeigu keičiasi tvarkomų duomenų kiekis, tvarkymo tikslas ar tvarkymo operacijos (veiksmai), privaloma gauti papildomą sutikimą tokiam duomenų tvarkymui arba turi egzistuoti kitas Taisyklėse, BDAR, ADTAI įtvirtintas asmens duomenų tvarkymo teisinis pagrindas.

93. Visais atvejais sutikimas turi būti gaunamas prieš atliekant duomenų tvarkymo operacijas (veiksnius), dėl kurių renkamas sutikimas.

94. Duomenų subjektas turi teisę bet kuriuo metu atšaukti savo sutikimą. Duomenų subjektui atšaukus sutikimą, draudžiama tvarkyti asmens duomenis tais tikslais ir atlikti duomenų tvarkymo operacijas (veiksnius), kurios buvo atliekamos tokio sutikimo pagrindu, išskyrus atvejus, kai tokiam duomenų tvarkymui egzistuoja kitas Taisyklių, BDAR ar ADTAI įtvirtintas asmens duomenų tvarkymo teisinis pagrindas.

95. Sutikimas galioja iki jo atšaukimo momento arba iki sutikime nurodyto jo galiojimo termino pabaigos.

96. Sutikimas ir jame nurodyti asmens duomenys gali būti saugomi dešimt metų nuo sutikimo atšaukimo arba jo galiojimo termino pabaigos, arba nuo Įstaigos sprendimo nebetvarkyti asmens duomenų sutikime nustatytais tikslais priėmimo dienos, išskyrus atvejus, kai teisės aktai numato kitokį duomenų saugojimo terminą. Jei sutikimo duomenys naudojami kaip įrodymai ikiteisminiame ar kitokiame tyrime, įskaitant ir Valstybinės duomenų apsaugos inspekcijos vykdomame tyrime, civilinėje, administracinėje ar baudžiamojoje byloje arba kitais įstatymų nustatytais atvejais, asmens duomenys gali būti saugomi tiek, kiek reikia šiems duomenų tvarkymo tikslams, ir sunaikinami nedelsiant, kai tampa nebereikalingi.

XIII SKYRIUS

TINKAMAS DUOMENŲ SUBJEKTŲ INFORMAVIMAS

97. Tuo atveju, jei duomenų teisinio tvarkymo pagrindu nėra teisinė prievolė ar su duomenų subjektu sudaryta sutartis, asmuo informuojamas apie jo duomenų tvarkymą.

98. Informacija apie Įstaigoje atliekamą duomenų subjekto asmens duomenų tvarkymą, nurodyta BDAR 13 ir 14 straipsniuose, pateikiama:

98.1. Įstaigos interneto svetainėje www.skaitlis.lt;

(98.2 papunktis pakeistas BĮ „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15)

98.2. informacinio pobūdžio lentelėse apie vaizdo stebėjimą pastate, kuriame įsikūrusi Įstaiga;

98.3. bendravimo su duomenų subjektu metu tokiu būdu, koku jis kreipiasi į Įstaigą.

99. Kai duomenų subjekto duomenys renkami tiesiogiai iš duomenų subjekto, informacija, pateikiama asmens duomenų gavimo metu, tokiu būdu, koku duomenų subjektas kreipiasi į Įstaigą.

100. Kai duomenų subjekto asmens duomenys renkami ne tiesiogiai iš duomenų subjekto, apie asmens duomenų tvarkymą informuojama:

100.1. per pagrįstą laikotarpį nuo asmens duomenų gavimo, bet ne vėliau kaip per vieną mėnesį, atsižvelgiant į konkrečias asmens duomenų tvarkymo aplinkybes;

100.2. jeigu asmens duomenys bus naudojami ryšiams su duomenų subjektu palaikyti – ne vėliau kaip pirmą kartą susisiekiant su duomenų subjektu;

100.3. Įstaiga turi teisę neteikti BDAR 13 ir 14 straipsniuose numatytos informacijos, jeigu:

100.4. informaciją duomenų subjektams apie Įstaigos duomenų tvarkytojo statusu tvarkomus asmens duomenis įsipareigojo pateikti duomenų valdytojas, kuris perdavė Įstaigai tvarkyti duomenis;

100.5. duomenų subjektas šią informaciją jau turi, ir tiek, kiek tos informacijos jis turi;

100.6. tokios informacijos pateikimas neįmanomas arba tam reikėtų neproporcingų pastangų;

100.7. asmens duomenų gavimas ar atskleidimas aiškiai nustatytas Europos Sąjungos teisės aktuose arba Lietuvos Respublikos teisės aktuose, kuriuose nustatytos tinkamos teisėtų duomenų subjektų interesų apsaugos priemonės.

XIV SKYRIUS

DARBUOTOJŲ STEBĖSENA

101. Įstaigoje yra atliekama nuolatinė darbuotojų stebėseną.

102. Atliekant darbuotojų stebėseną Įstaigoje, siekiama šių tikslų:

102.1. apsaugoti Įstaigos konfidencialią informaciją ir komercines paslaptis nuo neteisėto atskleidimo;

102.2. apsaugoti Įstaigos technologijas nuo įsilaužimų, virusų ar kitokio neigiamo poveikio;

102.3. apsaugoti Įstaigos turtą ir turtinius interesus;

102.4. užtikrinti tinkamą darbo organizavimą ir tvarką, darbuotojų darbinių funkcijų tinkamą įgyvendinimą ir pareigų vykdymą.

103. Siekiant šiame skyriuje nustatytų stebėsenos tikslų, Įstaigoje saugoma visa naudojant technologijas gaunama, siunčiama, apdorojama ar sukaupia informacija, įskaitant, bet neapsiribojant elektroniniu paštu siunčiama ir gaunama informacija, iš interneto parsisiunčiama informacija, naršymo internete istorija, kompiuterinėje (IT) ir komunikacinėje (TEL) įrangoje laikoma informacija. Ši informacija yra saugoma Įstaigoje 2 (du) mėnesius automatinio būdu darant atsargines kopijas (archyvą).

104. Darbuotojų stebėseną atliekama peržiūrint ir tikrinant šiame Taisyklių skyriuje nurodytą informaciją, išskyrus Įstaigos darbuotojų atskirtą ir kaip asmeninę aiškiai pažymėtą informaciją.

105. Informaciją gali peržiūrėti ir tikrinti tik Įstaigos direktorius ir (arba) jo įgalioti asmenys be išankstinio darbuotojo įspėjimo.

106. Esant įtarimui dėl darbuotojo galimai atliktų neteisėtų veiksmų, Įstaigos direktorius ir (arba) jo įgalioti asmenys gali peržiūrėti ir patikrinti darbuotojo asmeninę informaciją, esančią Įstaigai priklausančiose technologijose. Apie tokį patikrinimą iš anksto nepranešama, jeigu išankstinis pranešimas galėtų sutrukdyti patikrinimo eigai, pakenkti patikrinimo objektyvumui ar pan.

107. Atliekant stebėseną, duomenys analizuojami tokia apimtimi, kokia reikalinga įtariamam pažeidimui ar kitam patikrinimo pagrindui ištirti.

108. Prireikus Įstaiga, iš anksto informavusi darbuotojus, gali naudoti ir kitokias stebėsenos priemones, įskaitant, bet neapsiribojant garso ir vaizdo įrašymu, transporto priemonės vietos nustatymo ir kitomis priemonėmis, laikydamasi asmens duomenų teisinės apsaugos reikalavimų.

Elektroninio pašto stebėjimas

109. Įstaigoje vykdomas sisteminis elektroninio pašto stebėjimas, kurio tikslas – užtikrinti Įstaigos darbuotojų ir kitų asmenų, kurie siunčia duomenis elektroninėmis priemonėmis, turimos informacijos saugumą, vientisumą ir konfidencialumą.

110. Elektroninio pašto duomenys gali būti pateikti tik teisėsaugos institucijoms ar kitoms valstybės institucijoms, kurioms toks duomenų pateikimas yra privalomas pagal teisės aktų reikalavimus.

Elektroninių kortelių stebėjimas

111. Įstaigoje vykdomo elektroninių kortelių (leidimų pateikti į patalpas) stebėjimo tikslas – užtikrinti Įstaigos darbuotojų tinkamą darbo organizavimą ir tvarką, darbuotojų darbinių funkcijų tinkamą įgyvendinimą ir pareigų vykdymą, darbuotojų ir kitų asmenų, kurie lankosi Įstaigoje, saugumą, Įstaigos turto

ir dokumentų saugumą.

112. Įstaigos patalpose elektroninėmis kortelėmis fiksuojami duomenys apie darbuotojo atvykimo ir išvykimo laiką.

113. *(neteko galios BĮ „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15).*

114. Elektroninių kortelių stebėjimo duomenys gali būti teikiami teisėsaugos institucijoms ar kitoms valstybės institucijoms, kurioms toks duomenų pateikimas yra privalomas pagal teisės aktų reikalavimus.

115. Darbuotojai, susipažindinami su Taisyklėmis, taip pat patvirtina, kad jiems yra žinomas faktas apie Įstaigoje vykdomą elektroninių paštų ir elektroninių kortelių stebėjimą, jų tikslą.

116. Elektroninių paštų ir elektroninių kortelių stebėjimo duomenys negali būti naudojami kitiems tikslams, nesusijusiems su Taisyklėse apibrėžtais tikslais.

XV SKYRIUS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO IR REAGAVIMO Į TOKIUS PAŽEIDIMUS TVARKA

117. Duomenų valdytojo darbuotojai, turintys prieigos teisę prie duomenų, pastebėję duomenų saugumo pažeidimus (asmenų neveikimą ar veiksmus, galinčius sukelti ar sukeliančius grėsmę duomenų saugumui), turi informuoti duomenų apsaugos pareigūną.

118. Įvertinę duomenų apsaugos pažeidimo rizikos veiksnius, pažeidimo poveikio laipsnį, žalą ir padarinius, vadovaudamiesi Reagavimo į asmens duomenų saugumo pažeidimus procedūra ([Taisyklių 4 priedas](#)), atsakingi darbuotojai priima sprendimus dėl priemonių, reikiamų duomenų apsaugos pažeidimui ir jo padariniams pašalinti.

XVI SKYRIUS

POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

119. Tais atvejais, kai, atsižvelgiant į asmens duomenų ir duomenų subjektų kategoriją, duomenų tvarkymo pobūdį, aprėptį, kontekstą, tikslus, duomenų subjektų teisėms bei laisvėms gali kilti didelis pavojus, Įstaiga, prieš pradėdama vykdyti duomenų tvarkymo operacijas (veiksmus) ir tvarkyti duomenis, atlieka numatytų duomenų tvarkymo operacijų poveikio duomenų apsaugai vertinimą.

120. Poveikis duomenų apsaugai vertinamas, kai:

120.1. duomenų tvarkymo operacija patenka į Valstybinę duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų sąrašą, kurioms poveikio duomenų apsaugai vertinimas yra privalomas;

120.2. duomenų tvarkymo operacija nepatenka į Valstybinę duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų sąrašą, kurioms poveikio duomenų apsaugai vertinimo reikalavimas yra privalomas, tačiau Įstaiga įvertina, kad duomenų tvarkymo operacija, atsižvelgiant į Taisyklių 122 punkte įtvirtintus kriterijus, duomenų subjektų teisėms bei laisvėms gali kelti didelį pavojų;

120.3. pasikeitus duomenų tvarkymo operacijų (veiksmų) įgyvendinimo sąlygoms ir kai tai gali lemti didelį pavojų duomenų subjektų teisėms ir laisvėms.

120.4. Ar duomenų tvarkymo operacijos (veiksmai) gali kelti didelį pavojų duomenų subjektų teisėms ir laisvėms, sprendžiama kiekvieną kartą atsižvelgiant į šiuos kriterijus:

120.5. sisteminga asmens duomenų ar duomenų subjektų stebėsena;

120.6. neskelbtini duomenys arba labai asmeniškai duomenys, pavyzdžiui, specialių kategorijų

asmens duomenys;

120.7. didelio masto duomenų tvarkymas (susijusių duomenų subjektų skaičius, tvarkomų duomenų kiekis, tvarkomų duomenų įvairovė, duomenų tvarkymo veiklos trukmė ir pastovumas, geografinis duomenų tvarkymo mastas);

120.8. duomenų rinkinių siejimas ir derinimas;

120.9. su pažeidžiamais duomenų subjektais susiję duomenys (pavyzdžiui, vaikų duomenys, darbuotojai, labiau pažeidžiami subjektai, kuriems reikalinga speciali apsauga, segmentai, kai galima nustatyti nelygiaverčius duomenų subjekto ir duomenų valdytojo santykius);

120.10. naujų technologijų ar organizacinių sprendimų būdų taikymas;

120.11. dėl duomenų tvarkymo duomenų subjektams užkertamas kelias naudotis savo teisėmis, paslaugomis arba sudaryti sutartis;

120.12. kitos aplinkybės, rodančios galimą didelį pavojų subjektų teisėms ir laisvėms.

121. Kuo daugiau [Taisyklių 122 punkte](#) įtvirtintų kriterijų atitinka konkreti duomenų tvarkymo operacija (veiksmai), tuo didesnė tikimybė, kad duomenų tvarkymo operacija (veiksmai) gali kelti didelį pavojų duomenų subjektų teisėms ir laisvėms.

122. Poveikio duomenų apsaugai vertinimą inicijuoja duomenų apsaugos pareigūnas, kuris vertinimui atlikti gali siūlyti pasitelkti darbuotojus, kurie tvarko konkrečius asmens duomenis.

123. Poveikio duomenų apsaugai vertinimas atliekamas pagal [Taisyklių 5 priede](#) aprašytą poveikio duomenų apsaugai vertinimo procedūrą.

124. Kai duomenų tvarkymo apimtis, pobūdis, kontekstas ir tikslas yra labai panašūs į duomenų tvarkymą, kurio poveikis duomenų apsaugai buvo atliktas, galima iš naujo nevertinti poveikio duomenų apsaugai, o pasinaudoti dėl panašaus duomenų tvarkymo atliktu poveikio duomenų apsaugai vertinimu.

XVII SKYRIUS

BAIGIAMOSIOS NUOSTATOS

125. Darbuotojai su Taisyklėmis bei jos pakeitimais supažindinami pasirašytinai arba elektroninėmis priemonėmis. Darbuotojai privalo laikytis jose nustatytų įpareigojimų, atlikdami savo darbo funkcijas vadovautis Taisyklėse nustatytais principais. Priėmus naują darbuotoją, jis su Taisyklėmis privalo būti supažindintas pirmąją jo darbo dieną.

126. Įstaigos darbuotojai pažeidę Taisyklės, ADTAĮ ir (ar) BDAR atsako teisės aktų nustatyta tvarka.

127. Pasikeitus asmens duomenų tvarkymą reglamentuojantiems teisės aktams, Taisyklės privalo būti peržiūrimos ir atnaujinamos.

128. Taisyklėse įtvirtintos nuostatos gali būti papildomos ar išsamiau įtvirtinamos kituose Įstaigos veiklą reguliuojančiuose vidaus dokumentuose. Visais atvejais turi būti vadovaujamasi Taisyklėmis. Jeigu duomenų apsaugos klausimais yra prieštaravimų tarp Taisyklių ir kitų Įstaigos vidaus dokumentų, turi būti vadovaujamasi Taisyklių nuostatomis.

129. Kaip neatskiriama Taisyklių dalis kartu taikytini šie priedai:

1 priedas. Asmens duomenų tvarkymo veiklos įrašų registro forma;

2 priedas. Asmens duomenų apsaugos priemonių sąrašas;

3 priedas. Duomenų tvarkytojų registro forma;

4 priedas. Reagavimo į asmens duomenų saugumo pažeidimus procedūra;

5 priedas. Poveikio duomenų apsaugai vertinimo procedūra.

Biudžetinės įstaigos „Skaitlis“ asmens duomenų
tvarkymo taisyklių 1 priedas

(Asmens duomenų tvarkymo veiklos įrašų registro forma)

	Tvarkomų asmens duomenų kategorijos ir tvarkymo tikslai	Darbuotojai, turintys teisę tvarkyti asmens duomenis	Duomenų saugojimo vieta	Numatomi duomenų saugojimo terminai	Asmens duomenų šaltinis	Asmens duomenų gavėjų kategorijos	Duomenų įvedimo, keitimo data (-os)
Duomenų subjektų kategorija:							

Biudžetinės įstaigos „Skaitlis“ asmens duomenų
tvarkymo taisyklių 2 priedas

DUOMENŲ APSAUGOS PRIEMONIŲ SĄRAŠAS

1. Organizacinės duomenų saugumo priemonės:

1.1. Prieiga prie asmens duomenų, tvarkomų automatinio būdu, suteikiama tik tam darbuotojui, kuriam asmens duomenys yra reikalingi jo darbu funkcijoms vykdyti. Darbo santykiams pasibaigus, prieigos buvusiam darbuotojui panaikinamos.

1.2. Kiekvienam darbuotojui, kuriam suteikta prieiga prie asmens duomenų, tvarkomų automatinio būdu, suteikiamas unikalus prisijungimo vardas ir vienkartinis slaptažodis, kuris žinomas tik atitinkamam darbuotojui. Slaptažodžiai esant būtinybei (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei ir pan.) turi būti keičiami, taip pat susidarius tam tikroms aplinkybėms (pvz.: pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims).

1.3. Užtikrinama, kad visi su asmens duomenų tvarkymu susiję darbuotojai būtų įsipareigoję neatskleisti asmens duomenų. Įstaigos darbuotojai pasirašo susitarimus dėl konfidencialios informacijos apsaugos ir supažindinami su Įstaigoje patvirtintu konfidencialios informacijos sąrašu.

1.4. Įstaigos patalpos rakinamos. Į patalpas, kuriose yra tvarkomi asmens duomenys, patenka tik įgalioti asmenys. Įgalioti asmenys, kurie nėra Įstaigos darbuotojai, ir klientai į nurodytas patalpas patenka tik lydimi Įstaigos darbuotojų.

1.5. Naikinant dokumentus ir informacinėse sistemose tvarkomus duomenis, kurių saugojimo terminas yra pasibaigęs, dokumentai, kuriuose nurodomi asmens duomenys, bei jų kopijos, informacinėse sistemose tvarkomi duomenys turi būti sunaikinti taip, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio.

1.6. Duomenų subjektų ir/ ar Klientų pateikti dokumentai bei jų kopijos, finansavimo, buhalterinės apskaitos ir atskaitomybės ar kitos bylos, kuriose yra asmens duomenų, saugomos rakinamose spintose.

1.7. Taikoma „Švaraus stalo ir švaraus ekrano politika“.

1.8. Dokumentai, kuriuose yra asmens duomenų, nėra ir negali būti laikomi visiems prieinamoje matomoje vietoje ir/ ar taip, kad neturintys teisės asmenys nekliudomai galėtų su jais susipažinti.

1.9. Prieiga prie asmens duomenų suteikiama tik tiems asmenims, kuriems asmens duomenys yra reikalingi jų funkcijoms vykdyti, vadovaujantis principu „Būtina žinoti“.

1.10. Dokumentai, kuriuose yra asmens duomenys, tvarkomi, įtraukiami į apskaitą ir saugomi vadovaujantis Dokumentų tvarkymo ir apskaitos taisyklių, patvirtintų Lietuvos vyriausiojo archyvaro 2011 m. liepos 4 d. įsakymu Nr. V-118 „Dėl Dokumentų tvarkymo ir apskaitos taisyklių patvirtinimo“, reikalavimais.

1.11. Įstaigos ir Klientų finansavimo, buhalterinės apskaitos ir atskaitomybės, personalo ir/ ar kitos bylos, kuriose yra asmens duomenų, pasibaigus kiekvieniems kalendorinėms metams iki balandžio 1 d. perduodami saugojimui į archyvą.

1.12. Įstaigoje reglamentuota asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarka.

1.13. Jei darbuotojas abejoja Įstaigoje įdiegtų techninių saugumo priemonių patikimumu, jis privalo kreiptis į tiesioginį vadovą, o pastarasis į Įstaigos Informacinių technologijų skyriaus vadovą, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir įdiegimas.

1.14. Įvykus duomenų saugumo incidentui, apie duomenų saugumo incidentus ir saugumo priemones, kurių imtasi siekiant apsaugoti asmens duomenis, nedelsiant informuojamas duomenų apsaugos pareigūnas.

2. Patalpų fizinė apsauga:

2.1. patalpos rakinamos;

2.2. *pastatą, kurio patalpose yra įsikūrusi Įstaiga, ir įeigą į patalpas, prižiūri apsauginis;*

- 2.3. (neteko galios BJ „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15);
- 2.4. veikia asmenų įėjimo į patalpas, kuriose įsikūrusi Įstaiga, kontrolės sistema (elektroninė);
- 2.5. Įeiga į patalpas stebima vaizdo kameromis.

Automatiniu būdu tvarkomų duomenų saugumo priemonės

3. Programinės įrangos naudotojai:

- 3.1. prieigos prie asmens duomenų slaptažodžiai suteikiami, keičiami ir saugomi užtikrinant jų konfidencialumą;
- 3.3. prieiga prie asmens duomenų suteikiama tik tiems asmenims, kuriems asmens duomenys yra reikalingi jų funkcijoms vykdyti;
- 3.4. valdoma naudotojų teisė naudotis programine įranga;
- 3.5. užtikrinama tinkama prieigos prie asmens duomenų apsauga, valdymas ir kontrolė. Prieigos teisės prie asmens duomenų suteikiamos, naikinamos ir keičiamos užtikrinant, kad prieigos teisės prie asmens duomenų būtų suteikiamos tik legaliems naudotojams ir tik tokia apimtimi, kiek jos būtinos darbuotojų pareiginėms funkcijoms atlikti. Prieigos teisės prie asmens duomenų naikinamos pasibaigus Įstaigos ir jo darbuotojo darbo santykiams, pasikeitus darbo funkcijoms, kurioms vykdyti prieiga nereikalinga;
- 3.6. su duomenimis galima atlikti tik tuos veiksmus, kuriems atlikti naudotojui yra suteiktos teisės.

4. Prieiga prie vidinio tinklo:

- 4.1. vidinis tinklas apsaugotas ugniasienėmis;
- 4.2. nutolę įrenginiai prie vidinio tinklo jungiasi saugiu ryšio kanalu (VPN);
- 4.3. kontroliuojama naudotojų prieiga prie vidinio tinklo;
- 4.4. tinklu siunčiama informacija šifruojama;
- 4.5. naudojamos ryšio ir tinklo srautų atakų prevencijos priemonės.

5. Atsarginių duomenų kopijų ir laikmenų naudojimas:

- 5.1. kompiuterinė įranga ir laikmenos valdomos centralizuotai;
- 4.4. atsarginės duomenų kopijos ir laikmenos yra šifruojamos;
- 4.5. kompiuterinė įranga ir laikmenos valdomos centralizuotai.

6. Apsauga nuo vagystės:

- 6.1. apribota fizinė prieiga prie tarnybinių stočių ir kompiuterinių darbo vietų;
- 6.2. apribota programinė prieiga prie tarnybinių stočių, kompiuterinių darbo vietų ir jose esančių duomenų;
- 6.3. kompiuterinėse darbo vietose pagrindiniai duomenys nesaugomi.

7. Apsauga nuo piktnaudžiavimo duomenų perdavimo tinklu:

- 7.1. įdiegta speciali duomenų perdavimo tinklo srauto stebėjimo įranga;

8. Programinės įrangos klaidos:

- 8.1. naudojama tik legali programinė įranga, kuri prižiūrima laikantis gamintojo reikalavimų;
- 8.2. diegiami operacinių sistemų ir naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai.

9. Apsauga nuo kenkėjiškos programinės įrangos:

- 9.1. tarnybines stotyse ir kompiuterinėse darbo vietose įdiegta antivirusinė programinė įranga;
- 9.2. darbuotojai supažindinti ir žino, kaip elgtis pastebėjus kenkėjišką programinę įrangą.

10. Duomenų atstatymo gebėjimai:

10.1. numatyta duomenų atstatymo iš atsarginių kopijų procedūra.

11. Programinės įrangos naudojimas:

- 11.1. draudžiamas ir kontroliuojamas nelegalios (neleistinos) programinės įrangos naudojimas;
- 11.2. nuolat atliekama kompiuterinėse darbo vietose naudojamos programinės įrangos kontrolė;
- 11.3. naudotojai patys negali diegti programinės įrangos.

12. Naudotojų švietimas:

- 12.1. naudotojai mokomi dirbti su programine įranga;
- 12.2. naudotojams parengtos tikslios ir išsamios darbo instrukcijos.

13. Apsauga nuo duomenų perdavimo tinklo įrangos gedimų:

- 13.1. įranga prižiūrima pagal gamintojo rekomendacijas;
- 13.2. priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai;
- 13.3. stebima duomenų perdavimo tinklo būklė.

14. Apsauga nuo kompiuterinės įrangos gedimų:

- 14.1. įranga prižiūrima pagal gamintojo rekomendacijas;
- 14.2. priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai;
- 14.3. svarbiausios kompiuterinės įrangos techninė būklė nuolat stebima;
- 14.4. svarbiausiai kompiuterinei įrangai yra įsigyta garantinės priežiūros paslauga.

15. Apsauga nuo užliejimo:

- 15.1. tinkamai suplanuotos ir įrengtos svarbiausios kompiuterinės įrangos laikymo patalpos; *(pakeistas BĮ „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15)*
- 15.2. patalpos yra viršutiniame 4 aukšte, kuriame egzistuoja minimali staigaus užsiliejimo rizika.

16. Apsauga nuo gaisro:

- 16.1. patalpose yra ugnies gesintuvai;
- 16.2. įrengti dūmų ir karščio davikliai;
- 16.3. dokumentai ir bylos laikomi nedegiose metalinėse spintose;

17. Apsauga nuo temperatūros ir drėgmės svyravimų:

(pakeistas BĮ „Skaitlis“ direktoriaus 2024-03-18 d. įsakymu Nr.V-15)

- 17.1. tarnybinių stočių patalpose įrengta kondicionavimo sistema;
- 17.2. kondicionavimo įranga prižiūrima pagal gamintojo reikalavimus;
- 17.3. kondicionavimo įrangos priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai.

18. Apsauga nuo elektros srovės tiekimo sutrikimų:

- 18.1. svarbiausiai kompiuterinei įrangai skirti nenutrūkstamo maitinimo šaltiniai (UPS);
- 18.2. stebima elektros srovės tiekimo būklė.

19. Apsauga nuo maitinimo ir ryšio linijų gedimų:

- 19.1. kabeliai yra izoliaciniuose vamzdžiuose;
- 19.2. elektros ir duomenų kabeliai saugiai atskirti.

Biudžetinės įstaigos „Skaitlis“ asmens duomenų
tvarkymo taisyklių 3 priedas

(Asmens duomenų tvarkytojų registro forma)

Eil. Nr.	Duomenų tvarkytojas	Sutarties su duomenų tvarkytoju sudarymo data, pobūdis	Perduotų asmens duomenų subjektų kategorijos	Perduotų duomenų tvarkymo tikslas	Sutarties su duomenų tvarkytoju pasibaigimo data	Papildoma informacija (pildoma esant poreikiui)
1	2	3	4	5	6	7

REAGAVIMO Į ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪRA

I. SĄVOKOS

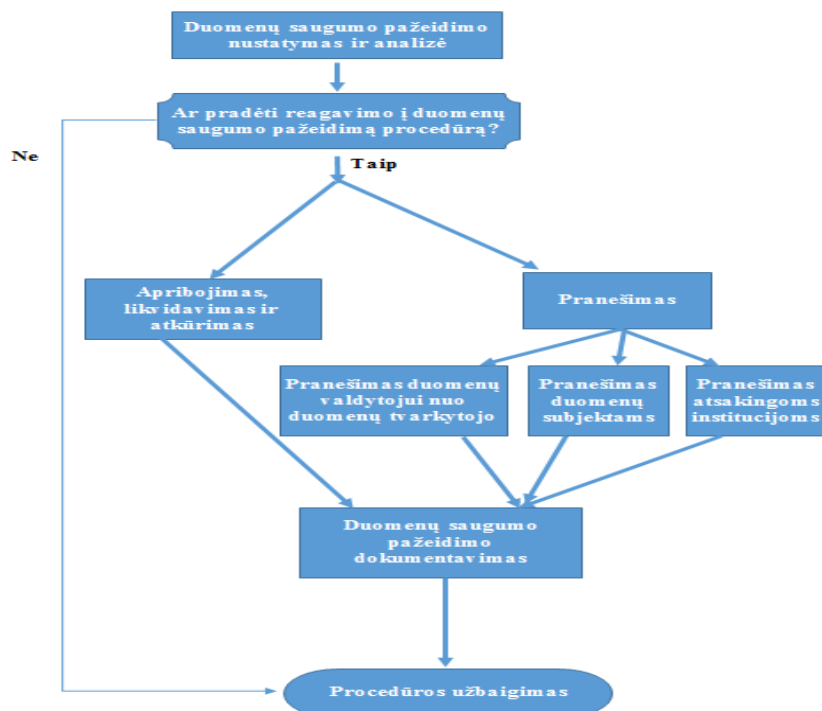
1. **Duomenų saugumo pažeidimas** reiškia pažeidimą, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.
2. **Įstaiga** – biudžetinė įstaiga „Skaitlis“, juridinio asmens kodas 300035837.
3. **Už duomenų saugą atsakingas asmuo** – duomenų apsaugos pareigūnas arba Įstaigos direktoriaus paskirtas kitas darbuotojas, turintis kompetenciją imtis reagavimo į Duomenų saugumo pažeidimą procedūros vykdymo.
4. **Priežiūros institucija** reiškia Valstybinė duomenų apsaugos inspekcija.
5. **Procedūra** reiškia šią Reagavimo į asmens duomenų saugumo pažeidimus procedūrą.

II. APIMTIS

6. Ši procedūra taikoma įvykus asmens duomenų saugumo pažeidimui pagal BDAR 33 straipsnį ir 34 straipsnį.
7. Šiame dokumente išdėstyta procedūra turėtų būti vadovaujama reaguojant į duomenų saugumo pažeidimą, atsižvelgiant į konkrečios situacijos faktines aplinkybes.

III. ATSAKOMYBĖ

8. Visi asmenys, turintys prieigą prie Įstaigos tvarkomų asmens duomenų privalo žinoti ir vadovautis šia Procedūra duomenų saugumo pažeidimo atveju.



IV. PROCEDŪRA – DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMAS IR ANALIZĖ

9. Kaip ir galima spręsti iš [Procedūros 1 punkte](#) nurodyto apibrėžimo, saugumo pažeidimu laikomas toks saugumo incidentas, dėl kurio įvyksta (konkretus pažeidimas gali patekti į daugiau nei vieną kategoriją):
 - 9.1. Konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama prieiga tam teisės neturintiems asmenims. Tokio pobūdžio pažeidimo pavyzdžiais galėtų būti duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio paviešinimas ir pan.;
 - 9.2. Pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami. Tokio pobūdžio pažeidimu galėtų būti duomenų bazės ištrynimas nesant atsarginės kopijos, iš kurios būtų galima atkurti prarastus duomenis. Pasiekiamumo pažeidimu, kuris turėtų būti aprašytas, būtų ir laikinas įprastinę Įstaigos veiklą sutrikdęs prieigos prie duomenų praradimas;
 - 9.3. Vientisumo pažeidimas – netyčia ar neteisėtai atliekami asmens duomenų pakeitimai. Tai galėtų būti trečiojo asmens, įgijusio neteisėtą prisijungimą prie duomenų bazės, įvykdyti joje esančių įrašų pakeitimai.
10. Kai yra nustatomas duomenų saugumo pažeidimas, jį nustatęs darbuotojas turi kuo skubiau informuoti už duomenų saugą atsakingą asmenį asmeniškai, el. paštu, telefonu, ir/arba kitomis komunikacijos priemonėmis.
11. Už duomenų saugą atsakingas asmuo atlieka pradinį vertinimą tam, kad nuspręstų dėl tinkamo veiksmų plano. Šis vertinimas turėtų apimti šiuos pagrindinius veiksnius:
 - 11.1. Poveikio informacinių technologijų (toliau – IT) infrastruktūrai apimtis;
 - 11.2. Informaciniai ištekliai, kuriems gali kilti arba yra kilęs pavojus (kokios duomenų bazės yra arba gali būti paveiktos);
 - 11.3. Tikėtina duomenų saugumo pažeidimo trukmė (kada prasidėjo ir kada buvo sustabdytas pažeidimas arba kaip skubiai tikėtina galima būtų tai padaryti);
 - 11.4. Paveikti duomenų subjektai ir poveikio jiems apimtis (ar paveikti tik konkrečios duomenų subjektų grupės duomenys, kokia konkrečios grupės dalis yra paveikta ir pan.);
 - 11.5. Pradiniai duomenų saugumo pažeidimo pasekmių požymiai (tai galėtų būti prieigos prie duomenų praradimas, nustatyti neteisėti duomenų pakeitimai, rasti paviešinti duomenys ir pan.).
12. Aukščiau nurodyta informacija turėtų būti fiksuojama tokiu būdu, kad atliekant vėlesnę peržiūrą būtų galima susidaryti aiškų chronologiską suvokimą apie situacijos eigą ir priemones, kurių buvo imtasi.
13. Atsižvelgdamas į aukščiau aprašytą pradinę analizę, Už duomenų saugą atsakingas asmuo pagal [Procedūros 11 punkte](#) nurodytus kriterijus įvertina, ar duomenų saugumo pažeidimo apimtis ir faktinis ar galimas poveikis lemia Reagavimo į duomenų saugumo pažeidimus procedūros pradėjimą.

V. PROCEDŪRA – REAGAVIMO Į DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS PRADĖJIMAS

14. Formalus reagavimas į Duomenų saugumo pažeidimą visais atvejais turėtų būti pradėtas tada, jei nustatytos bet kurios iš toliau nurodytų aplinkybių:
 - 14.1. Prarastas arba gali būti prarastas reikšmingas kiekis asmens duomenų;
 - 14.2. Duomenų pažeidimas tikėtina gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms;
 - 14.3. Daromas poveikis dideliame duomenų subjektų skaičiui;
 - 14.4. Bet kokia kita situacija, kuri gali sukelti reikšmingą poveikį Įstaigai ir/arba duomenų subjektams.
15. Jei nusprendžiama nepradėti Procedūros, tada [Procedūros 11 punkte](#) aprašytas vertinimas turi būti tinkamai dokumentuotas už duomenų saugą atsakingo asmens ir ši Procedūra užbaigta.

VI. PROCEDŪRA – DUOMENŲ SAUGUMO PAŽEIDIMO APRIBOJIMAS, LIKVIDAVIMAS IR ATKŪRIMAS

16. Pirmasis žingsnis sprendžiant duomenų saugumo pažeidimo klausimą yra jo apribojimas. Konkretūs veiksmai, atliktini norint tai pasiekti priklauso nuo konkretaus pažeidimo aplinkybių, bet tai galėtų būti tokie veiksmai kaip:
 - 16.1. Duomenų ištrynimasis nuotoliniu būdu iš pamesto ar pavogto įrenginio;
 - 16.2. Kuo skubesnis kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti duomenys, su prašymu neatidarinėti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;
 - 16.3. Atskleisto tretiesiems asmenims prisijungimo prie duomenų bazės slaptažodžio pakeitimas;
 - 16.4. Prarastų duomenų atkūrimas iš turimos atsarginės kopijos.
17. Vykdam šią procedūrą reikia imtis atsargumo priemonių tam, kad būtų užtikrinta, jog būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį duomenų saugumo pažeidimą (pavyzdžiui, užfiksuojama, kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės, kam konkrečiai buvo per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su duomenimis).
18. Veiksmai, skirti atitaisyti žalą, sukeltą duomenų saugumo pažeidimo, turėtų būti nukreipti ne vien į esamo pažeidimo priežasties pašalinimą, bet ir skirti neleisti duomenų saugumo pažeidimui pasikartoti. Turėtų būti nustatytas bet koks pažeidžiamumas, kuris gali būti išnaudotas siekiant įvykdyti pažeidimą.
19. Prireikus gali būti pasitelkiama IT specialistų ar teisininkų pagalba.
20. Atkūrimo stadijoje sistemos turėtų būti pagal galimybes atstatytos į ankstesnę būklę, tačiau turėtų būti imamasi būtinų veiksmų tam, kad būtų atsižvelgta į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdam duomenų saugumo pažeidimą.

VII. PROCEDŪRA – DUOMENŲ VALDYTOJO PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

21. Įstaiga, kaip duomenų valdytojas, nedelsdama privalo informuoti Priežiūros instituciją apie duomenų saugumo pažeidimą tada, jei Už duomenų saugą atsakingas asmuo nustato, kad duomenų saugumo pažeidimas tikėtina gali kelti pavojų duomenų subjektų, paveiktų duomenų saugumo pažeidimo, teisėms ir laisvėms. Pavojų keliančiu laikytinas toks pažeidimas, dėl kurio duomenų subjektas galėtų patirti kūno sužalojimą, materialinę ar nematerialinę žalą, teisių apribojimą, diskriminaciją, galėtų būti pavogta ar suklastota asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala.
22. Jei duomenų saugumo pažeidimas kelia pavojų duomenų subjektų teisėms ir laisvėms, Už duomenų saugą atsakingas asmuo ne vėliau kaip per 72 valandas nuo Įstaigos sužinojimo apie pažeidimą Priežiūros institucijai pateikia tokią informaciją:
 - 22.1. Duomenų saugumo pažeidimo pobūdį, įskaitant, jeigu įmanoma, atitinkamai paveiktų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;
 - 22.2. Kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis;
 - 22.3. Tikėtinų duomenų saugumo pažeidimo pasekmių aprašymą;
 - 22.4. Priemonės, kurių ėmėsi arba planuoja imtis Įstaiga tam, kad būtų pašalintas duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti.
23. Jeigu visos informacijos neįmanoma pateikti tuo pačiu metu, tolesnė informacija nepagrįstai nedelsiant gali būti teikiama etapais.

VIII. PROCEDŪRA – DUOMENŲ VALDYTOJO PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

24. Kai dėl duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, Įstaiga nepagrįstai nedelsdama praneša apie asmens duomenų saugumo pažeidimą duomenų subjektams. Didelį pavojų keliančiu gali būti laikytinas bet kuris [Procedūros 21 punkte](#) nurodytų pasekmių riziką keliantis pažeidimas tada, jei tokios pažeidimo pasekmės yra labai tikėtinos, tvarkomi jautrūs asmens duomenys (pavyzdžiui, duomenys apie sveikatą), pažeidimas turi neigiamą poveikį dideliame duomenų subjektų skaičiui ir pan.

25. Už duomenų saugą atsakingas asmuo duomenų subjektui aiškia ir paprasta kalba aprašo duomenų saugumo pažeidimo pobūdį ir pateikia bent jau žemiau nurodytą informaciją:
 - 25.1. Kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis;
 - 25.2. Tikėtinų duomenų saugumo pažeidimo pasekmių aprašymą;
 - 25.3. Priemonės, kurių ėmėsi arba planuoja imtis Įstaiga tam, kad būtų pašalintas duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti.
26. Šios [Procedūros 25 punkte](#) nurodytas komunikavimas su duomenų subjektu nebus reikalingas tada, jei egzistuoja bet kuri iš šių aplinkybių:
 - 26.1. Įstaiga įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems duomenų saugumo pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės;
 - 26.2. Įstaiga vėliau ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;
 - 26.3. Tai pareikalautų neproporcingai daug pastangų. Tokiu atveju apie įvykusį duomenų saugumo pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.
27. Priežiūros institucija, apsvarsčiusi, kokia yra tikimybė, kad dėl duomenų saugumo pažeidimo kils didelis pavojus, gali pareikalausti, kad Įstaiga informuotų duomenų subjektus apie duomenų saugumo pažeidimą. Už duomenų saugą atsakingas asmuo gavęs tokį nurodymą turi nedelsdamas jį vykdyti.

IX. DUOMENŲ SAUGUMO PAŽEIDIMO DOKUMENTAVIMAS IR PROCEDŪROS UŽBAIGIMAS

28. Už duomenų saugą atsakingas asmuo, gavęs supažindinto su duomenų saugumo pažeidimo ir jo pašalinimo aplinkybėmis Įstaigos direktoriaus pritarimą, priima sprendimą užbaigti Procedūrą tada, kai duomenų saugumo pažeidimas laikytinas pašalintu, o visoms reikalingoms šalims apie pažeidimą yra pranešta.
29. Visi veiksmai, kurių imamasi Procedūros metu turi būti aprašomi ir visi susiję įrašai apie duomenų saugumo pažeidimą peržiūrimi tam, kad būtų užtikrintas jų išbaigtumas, tikslumas ir atitiktis atitinkamam teisiniam reguliavimui.

Biudžetinės įstaigos „Skaitlis“ asmens duomenų
tvarkymo taisyklių 5 priedas

POVEIKIO DUOMENŲ APSAUGAI VERTINIMO PROCEDŪRA

I. SĄVOKOS

1. **Didelis pavojus fizinių asmenų teisėms ir laisvėms** – atvejai, kai dėl asmens duomenų tvarkymo arba dėl galimo asmens duomenų saugumo pažeidimo duomenų subjektams gali būti sunkiau naudotis savo teisėmis ir laisvėmis, duomenų subjektas gali patirti atskirtį arba diskriminaciją, finansinių nuostolių, gali būti pakenkta jo reputacijai arba atsirasti kitokių rimtų padarinių kasdieniam fizinio asmens gyvenimui.
2. **Duomenų tvarkymo operacija** – vienas ar keli duomenų tvarkymo veiksmai.
3. **Fizinių asmenų teisės ir laisvės** – teisės į duomenų apsaugą ir privatumą, taip pat kitos pagrindinės teisės ir laisvės, pavyzdžiui, žodžio laisvė, minties laisvė, judėjimo laisvė, diskriminacijos draudimas, teisė į laisvę, sąžinės ir tikėjimo laisvė ir kt.
4. **Pavojus** – įvykis ir jo padariniai (žala), įvertinti atsižvelgiant į jų rimtumą ir tikimybę.
5. **Poveikio duomenų apsaugai vertinimas** (toliau – PDAV) – procesas, skirtas duomenų tvarkymo operacijai aprašyti ir tokios duomenų tvarkymo operacijos reikalingumui ir proporcingumui įvertinti, padedantis valdyti pavojų, kuris fizinių asmenų teisėms ir laisvėms kyla dėl asmens duomenų tvarkymo, apimantis pavojaus įvertinimą ir jo pašalinimo priemonių nustatymą. Pagrindiniai principai, susiję su BDAR nurodytu PDAV, pateikti šios [Procedūros A priede](#). PDAV atlikimas schemiškai pavaizduotas šios [Procedūros B priede](#).
6. **Poveikio duomenų apsaugai vertinimo koordinatorius** (toliau – PDAV koordinatorius) – paskirtas darbuotojas, atsakingas už poreikio atlikti PDAV nustatymą ir PDAV atlikimą arba PDAV koordinavimą (jei PDAV atlikti pavesta darbuotojų grupei) šios Procedūros nustatyta tvarka. Paprastai PDAV koordinatoriumi skiriamas projekto, kurį įgyvendinus būtų atliekama duomenų tvarkymo operacija, kuriai taikomas reikalavimas atlikti PDAV, vadovas.
7. Kitos šioje Procedūroje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Taisyklėse ir BDAR.
8. **Procedūra** – ši poveikio duomenų apsaugai vertinimo procedūra.

II. APIMTIS

9. Šis dokumentas nustato duomenų tvarkymo operacijų poveikio duomenų apsaugai vertinimo atlikimo pagrindus, eigą, procedūrą ir reikalavimus, siekiant užtikrinti BDAR laikymąsi ir įgyvendinimą.
10. Šia procedūra vadovaujamas tais atvejais, kai dėl numatomo duomenų tvarkymo, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms ir laisvėms gali kilti didelis pavojus.

III. POVEIKIO DUOMENŲ APSAUGAI VERTINIMO ATLIKIMO PAGRINDAI

11. **PDAV** atliekamas šiais atvejais:
 - 11.1. kai duomenų tvarkymo operacija yra įtraukta į Valstybinės duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti PDAV, sąrašą;
 - 11.2. kai planuojama rinkti arba kitaip tvarkyti naujus asmens duomenis (pavyzdžiui, sisteminga darbuotojų veiklos, darbuotojų darbo vietos, veiklos internete ir pan. stebėseną) ir dėl asmens duomenų tvarkymo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, vertinant asmens duomenų tvarkymą pagal šios [Procedūros IV skyriuje](#) nurodytus kriterijus;

- 11.3. kai keičiasi jau tvarkomų asmens duomenų tvarkymo procesas (būdas, tikslas ir pan.) arba aplinka (pavyzdžiui, diegiama nauja informacinių technologijų sistema, teikiama nauja paslauga, atsiranda naujas procesas, naujos rizikos, susijusios su įvykdytomis kibernetinėmis atakomis ir pan.) ir dėl asmens duomenų tvarkymo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, vertinant asmens duomenų tvarkymą pagal šios [Procedūros IV skyriuje](#) nurodytus kriterijus;
 - 11.4. gavus priežiūros institucijos (Valstybinės duomenų apsaugos inspekcijos, administracinės veiklos priežiūrą atliekančio subjekto ir pan.) rekomendaciją atlikti PDAV.
12. PDAV gali būti neatliekamas šiais atvejais:
- 12.1. kai duomenų tvarkymas negali kelti didelio pavojaus fizinių asmenų teisėms ir laisvėms, vertinant asmens duomenų tvarkymą pagal šios [Procedūros IV skyriuje](#) nurodytus kriterijus;
 - 12.2. kai duomenų tvarkymo pobūdis, aprėptis, kontekstas ir tikslai yra labai panašūs į duomenų tvarkymą, kurio PDAV buvo atliktas (tokiais atvejais galima pasinaudoti dėl panašaus duomenų tvarkymo atliktu PDAV).
13. PDAV turi būti atliktas prieš pradedant tvarkyti asmens duomenis arba kai tvarkant asmens duomenis atsiranda objektyvi būtinybė atlikti PDAV, atsižvelgiant į šios [Procedūros 11 punkte](#) nurodytus atvejus.
14. PDAV gali būti atliekamas dėl kelių duomenų tvarkymo operacijų, kurios panašios savo pobūdžiu, apimtimi, kontekstu, tikslu ir kylančiais pavojais asmens duomenų saugumui.

IV. KRITERIJAI, KURIAIS REMIANTIS NUSTATOMA, AR DĖL DUOMENŲ TVARKYMO OPERACIJOS GALI KILTI DIDELIS PAVOJUS FIZINIŲ ASMENŲ TEISĖMS IR LAISVĖMS

15. Siekiant nustatyti duomenų tvarkymo operacijas, dėl kurių reikia atlikti PDAV, atsižvelgiama į BDAR 35 straipsnio 1 dalyje bei 35 straipsnio 3 dalies a–c punktuose nustatytus konkrečius elementus, Valstybinės duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti PDAV, sąrašą, BDAR 71, 75, 91 konstatuojamąsias dalis bei kitas BDAR nuorodas į duomenų tvarkymo operacijas, dėl kurių gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, bei įvertinami šie kriterijai:
- 15.1. atliekamas su fiziniais asmenimis susijusių asmeninių aspektų vertinimas arba balų skyrimas, įskaitant profiliavimą ir prognozavimą, visų pirma remiantis aspektais, susijusiais su duomenų subjekto darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu (pavyzdžiui, naudotojo elgesio profilio sudarymas, remiantis interneto svetainės naudojimu, ir pan.);
 - 15.2. automatizuotai (technologinėmis priemonėmis, be jokio žmogaus įsikišimo) priimami sprendimai, duomenų subjektams sukeliantys teisinį arba panašų rimtą poveikį (pavyzdžiui, duomenų tvarkymas gali lemti asmenų atskirtį arba diskriminaciją);
 - 15.3. atliekama sisteminga stebėseną, t. y. duomenų tvarkymas, kuris reikalingas duomenų subjektų stebėsenos arba kontrolės tikslais, įskaitant tinkluose surinktus duomenis arba sistemingą viešos vietos stebėjimą dideliu mastu;
 - 15.4. tvarkomi neskelbtini duomenys arba labai asmeniškai duomenys (pavyzdžiui, specialių kategorijų asmens duomenys, duomenys apie apkaltinamuosius nuosprendžius ar nusikalstamas veikas, vietos nustatymo duomenys ir pan.);
 - 15.5. duomenys tvarkomi dideliu mastu (vertinant, ar duomenys tvarkomi dideliu mastu, turi būti atsižvelgiama į susijusių duomenų subjektų skaičių (konkretų skaičių arba atitinkamą gyventojų dalį), tvarkomų duomenų kiekį ir intervalą ir (arba) skirtingų tvarkomų duomenų įvairovę, duomenų tvarkymo veiklos trukmę arba pastovumą, geografinį duomenų tvarkymo veiklos mastą);
 - 15.6. atliekamos sudėtingos duomenų tvarkymo operacijos (pavyzdžiui, keli asmens duomenų tvarkymo tikslai ir (ar) duomenų valdytojai, duomenų rinkinių siejimas ir derinimas, kai duomenų tvarkymo operacijos atliekamos taip, kad viršija pagrįstus duomenų subjekto lūkesčius, ir pan.);
 - 15.7. tvarkomi duomenys, susiję su pažeidžiamais duomenų subjektais (pavyzdžiui, vaikais, darbuotojais, labiau pažeidžiamais gyventojais, kuriems reikalinga speciali apsauga, ir visais atvejais, kai galima nustatyti nelygiavertius duomenų subjekto ir duomenų valdytojo santykius);

- 15.8. naudojamosi inovatyviais organizaciniais-techniniais sprendimais (pavyzdžiui, pirštų atspaudų ir veido atpažinimo derinimas siekiant užtikrinti geresnę fizinės prieigos kontrolę);
- 15.9. kai dėl paties duomenų tvarkymo duomenų subjektas negali įgyvendinti savo teisių, pasinaudoti paslaugomis arba sudaryti sutarties (pavyzdžiui, jei Įstaiga tikrina pretendentes į darbuotojus Įtariamųjų, kaltinamųjų ir nuteistųjų asmenų registre, kad nuspręstų, ar priimti juos į atitinkamas pareigas).

V. POREIKIO ATLIKTI POVEIKIO DUOMENŲ APSAUGAI VERTINIMĄ NUSTATYMAS

16. Poreikį atlikti PDAV paprastai nustato PDAV koordinatorius, užpildydamas poreikio atlikti PDAV nustatymo klausimyną, kurio pavyzdinė forma nustatyta šios Procedūros C priede.
17. Jei duomenų tvarkymo operacija nėra įtraukta į Valstybinės duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti PDAV, sąrašą, tokios duomenų tvarkymo operacijos PDAV paprastai atliekamas, kai planuojamas duomenų tvarkymas atitinka bent du iš šios Procedūros 15.1–15.9 papunkčiuose nurodytų kriterijų. Kuo daugiau kriterijų, nurodytų šios Procedūros 15.1–15.9 papunkčiuose, atitinka planuojamas duomenų tvarkymas, tuo labiau tikėtina, kad dėl duomenų tvarkymo operacijos gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms ir yra pagrindas atlikti PDAV.
18. Užpildytas poreikio atlikti PDAV nustatymo klausimynas pateikiamas Įstaigos direktoriui, kuris, įvertinęs klausimyne užfiksuotą informaciją ir išvadą dėl PDAV atlikimo, jį patvirtina arba atmeta.
19. Jei Įstaiga, kaip duomenų valdytojas, nusprendžia neatlikti PDAV šios [Procedūros 11 punkte](#) nurodytais atvejais, manydama, kad dėl duomenų tvarkymo negali kilti didelis pavojus fizinio asmens teisėms ir laisvėms, toks sprendimas turi būti pagrįstas, nurodant priežastis, dėl kurių nuspręsta neatlikti PDAV.

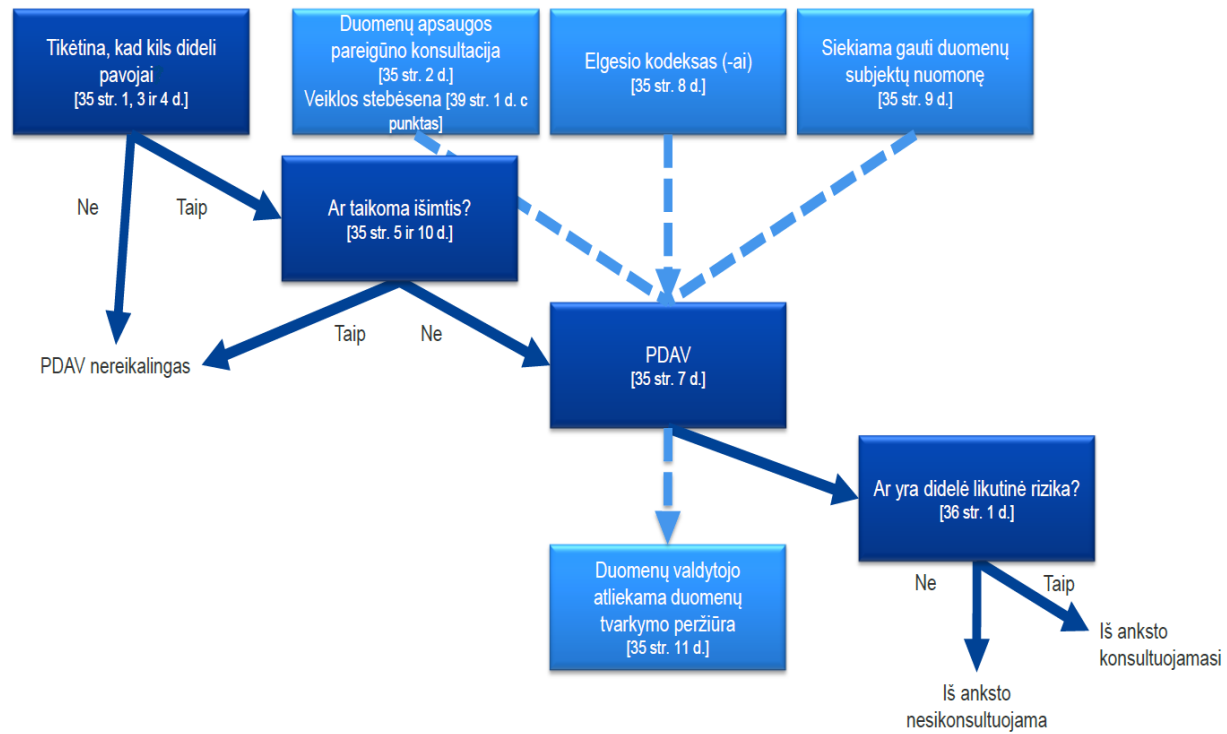
VI. POVEIKIO DUOMENŲ APSAUGAI VERTINIMO ATLIKIMAS

20. Jei yra priimtas sprendimas atlikti PDAV, Įstaigos direktorius organizuoja PDAV atlikimą, įvertindamas poreikio atlikti PDAV nustatymo klausimyne nurodytą siūlymą dėl darbuotojų, kurių dalyvavimas atliekant PDAV būtų reikšmingas pagal jų turimas kompetencijas ir atliekamas asmens duomenų tvarkymo funkcijas.
21. PDAV paprastai atlieka PDAV koordinatorius arba PDAV atlikti gali būti pavesta darbuotojų grupei, kuri paprastai sudaroma iš PDAV koordinatoriaus, darbuotojo, atsakingo už informacines technologijas, bei kitų asmenų, kurie atliks duomenų tvarkymo operacijas ir (arba) yra su jomis susiję.
22. Įstaigos direktoriaus sprendimu PDAV atlikti gali būti pasitelkti išorės konsultantai, specialistai, ekspertai (teisininkai, informacinių technologijų specialistai, saugumo ekspertai, etikos specialistai ir pan.), jeigu Įstaigos žmoniškųjų ir (ar) laiko išteklių nepakanka PDAV tinkamai atlikti.
23. PDAV koordinatorius PDAV atlikimo rezultatus fiksuoja PDAV atlikimo ataskaitoje, kurios pavyzdinė forma nustatyta šios Procedūros D priede.
24. Nustatant pavojus fizinio asmens teisėms ir laisvėms ir juos vertinant (PDAV atlikimo ataskaitos 5 dalis) turi būti atsižvelgiama į pavojų kilmę, pobūdį, specifiką ir rimtumą, t. y. į kiekvieną pavojų (neteisėtą prieigą prie asmens duomenų, nepageidaujamą asmens duomenų pakeitimą ir asmens duomenų praradimą) iš duomenų subjektų perspektyvos, taip pat į žalos (pavojaus poveikio), kuri duomenų subjektams gali kilti dėl asmens duomenų tvarkymo arba galimo asmens duomenų saugumo pažeidimo, tikimybę ir sunkumą (žala gali būti fizinė, materialinė ir (arba) nematerialinė).
25. Pavojus fizinio asmens teisėms ir laisvėms, atsižvelgiant į pavojaus ir pavojaus poveikio fiziniam asmeniui pobūdį, gali būti:
 - 25.1. mažas (kai asmens duomenų tvarkymas arba galimas asmens duomenų saugumo pažeidimas duomenų subjektų teisėms ir laisvėms įtakos neturės arba padariniai kasdieniam fizinio asmens gyvenimui bus mažareikšmiai);
 - 25.2. vidutinis (kai dėl asmens duomenų tvarkymo arba dėl galimo asmens duomenų saugumo pažeidimo duomenų subjektams gali būti sunkiau laikinai naudotis savo teisėmis ir laisvėmis, pasinaudoti Įstaigos teikiamomis paslaugomis, gali atsirasti kitokių neigiamų padarinių kasdieniam fizinio asmens gyvenimui);

- 25.3. didelis (kai dėl asmens duomenų tvarkymo arba dėl galimo asmens duomenų saugumo pažeidimo duomenų subjektams gali būti sunku arba neįmanoma pasinaudoti savo teisėmis ir laisvėmis, duomenų subjektas gali patirti atskirtį ar diskriminaciją, finansinių nuostolių, gali būti pakenkta jo reputacijai arba atsirasti kitokių rimtų neigiamų padarinių kasdieniam fizinio asmens gyvenimui).
26. Pavojaus įvertinimas ir bendro pavojaus lygio nustatymas atliekamas vadovaujantis pavojaus įvertinimo ir bendro pavojaus lygio nustatymo lentele, kuri pateikta šios Procedūros E priede.
27. Priemonės, kurių galima imtis siekiant sumažinti ar pašalinti pavojus (pavyzdžiui, saugumo priemonės, kuriomis užtikrinama asmens duomenų apsauga ir įrodoma, kad laikomasi BDAR reikalavimų: duomenų šifravimas ir kitos techninės priemonės, reikšmingas asmenų, turinčių prieigą prie tam tikrų asmens duomenų, rato apribojimas, reikalavimų prieigos teisės turinčių vartotojų identifikavimui sugriežtinimas ir pan.), nustatomos atsižvelgiant į pavojaus mažinimo ir šalinimo priemonių rekomendacijas, kurios pateiktos šios Procedūros F priede.
28. Jei planuojamos pavojaus fizinių asmenų teisėms ir laisvėms mažinimo ir šalinimo priemonės yra imlios finansiniu ir laiko atžvilgiu, jų įgyvendinimui reikalingos kompleksinės priemonės ir (ar) keli vykdytojai ir pan., šios priemonės bei informacija apie jų įgyvendinimą gali būti fiksuojama atskirame pavojaus, kylančio fizinių asmenų teisėms ir laisvėms, mažinimo ir šalinimo priemonių plane, kurio pavyzdinė forma nustatyta šios Procedūros G priede.
29. PDAV koordinatorius užtikrina, kad būtų atliktas pavojaus, kylančio fizinių asmenų teisėms ir laisvėms, mažinimo ir šalinimo priemonių plane (jei toks planas buvo rengtas) nustatytų priemonių įgyvendinimo veiksmingumo vertinimas. Asmuo, įgyvendinęs plane numatytas priemones, negali vertinti jų veiksmingumo. Įgyvendinus numatytas priemones, iš naujo atliekamas pavojaus vertinimas (paprastai jį atlieka PDAV koordinatorius).
30. Įstaiga, kaip duomenų valdytojas, gali nuspręsti, kad kai kurie pavojai (net ir dideli) yra priimtini, įvertinus planuojamo asmens duomenų tvarkymo naudą bei neproporcingas pavojų mažinimo ir šalinimo priemonių įgyvendinimo sąnaudas.
31. Jei atliekant PDAV paaiškėja, kad tvarkant asmens duomenis kiltų didelis pavojus duomenų subjektų teisėms ir laisvėms, jei Įstaiga, kaip duomenų valdytojas, nesiimtų priemonių pavojui sumažinti, Įstaiga, prieš pradėdamas tvarkyti asmens duomenis, turi iš anksto konsultuotis su Valstybine duomenų apsaugos inspekcija. Įstaiga, kreipdamasi dėl išankstinės konsultacijos, Valstybinei duomenų apsaugos inspekcijai pateikia BDAR 36 straipsnio 3 dalyje nurodytą informaciją.
32. Atliekant PDAV, darbuotojai, kuriems yra pavesta atlikti naujas duomenų tvarkymo operacijas ir (arba) yra su jomis susiję, PDAV koordinatoriui privalo pateikti visą informaciją, kurios pagrindu yra pildoma PDAV ataskaita bei pavojaus, kylančio fizinių asmenų teisėms ir laisvėms, mažinimo ir šalinimo priemonių planas (jei reikia), ir bendradarbiauti atliekant PDAV (PDAV koordinatoriui paprašius, pateikti papildomą informaciją ir (ar) dokumentus, pagal kompetenciją teikti konsultacijas ir pan.).

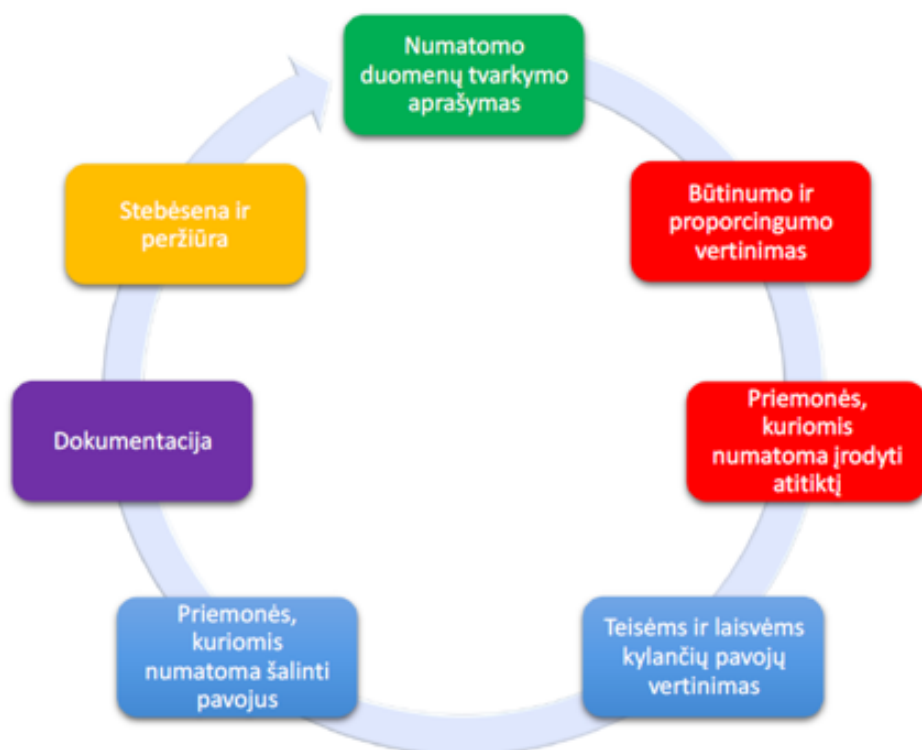
Poveikio duomenų apsaugai vertinimo procedūra
A priedas

**PAGRINDINIAI PRINCIPAI, SUSIJĘ SU BDAR NURODYTU POVEIKIO DUOMENŲ APSAUGAI
VERTINIMU**



Poveikio duomenų apsaugai vertinimo procedūra
B priedas

POVEIKIO DUOMENŲ APSAUGAI VERTINIMO ATLIKIMAS



Poveikio duomenų apsaugai vertinimo procedūra
C priedas

(Poreikio atlikti poveikio duomenų apsaugai vertinimą nustatymo klausimyno forma)

Biudžetinė įstaiga „Skaitlis“

(Duomenų valdytojo pavadinimas)

TVIRTINU

(parašas)

(vardas ir pavardė)

**POREIKIO ATLIKTI POVEIKIO DUOMENŲ APSAUGAI VERTINIMĄ NUSTATYMO
KLAUSIMYNAS**

Nr.

(data)

(numeris)

(vieta)

Duomenų tvarkymo operacija:			
Eil. Nr.	Klausimas	Atsakymas Taip / Ne	Pastabos
1.	Ar duomenų tvarkymo operacija yra įtraukta į Valstybinės duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašą?		
2.	Ar tai nauja duomenų tvarkymo operacija?		
3.	Ar atliekant duomenų tvarkymo operaciją bus renkami, naudojami, saugomi ar kitaip tvarkomi asmens duomenys?		
4.	Ar atliekant duomenų tvarkymo operaciją duomenų subjektai privalės teikti duomenis apie save (asmens duomenis)?		
5.	Ar asmens duomenys bus atskleisti tretiesiems asmenims (organizacijoms, kitiems duomenų valdytojams, kitiems asmenims ir pan.), kuriems prieš tai nebuvo teikti asmens duomenys?		
6.	Ar asmens duomenys bus tvarkomi naujais tikslais, t. y. iki šiol asmens duomenys nebuvo šiais tikslais tvarkomi?		
7.	Kokiu teisiniu pagrindu vadovaujantis duomenų tvarkymo operacijos metu bus tvarkomi asmens duomenys? <i>Nurodyti bent vieną iš Reglamento (ES) 2016/679 6, 9 ir (ar) 10 straipsnyje įtvirtintų</i>		

	<i>teisėto asmens duomenų tvarkymo pagrindų. Jeigu asmens duomenys tvarkomi vadovaujantis Lietuvos Respublikos teisės aktais, nurodyti tokių teisės aktų pavadinimus, straipsnius, dalis, punktus.</i>		
8.	Ar duomenų tvarkymo operacijos metu bus naudojamos naujos technologijos, kurios gali būti laikomos nesaugiomis, neužtikrinančiomis asmenų privatumo? Jei taip, kokios?		
9.	Ar duomenų tvarkymo operacijos metu bus priimami sprendimai, kurie gali padaryti reikšmingą poveikį duomenų subjektams? Jei taip, kokie?		
10.	Ar duomenų tvarkymo operacijos metu su duomenų subjektais bus kontaktuojama taip, kad gali būti pažeistas jų privatumas (pavyzdžiui, siunčiami elektroniniai laiškai ar SMS žinutės, skambinama telefonu ir pan.)?		
11.	Ar bus atliekamas vertinimas arba balų skyrimas, įskaitant profiliavimą ir prognozavimą, visų pirma remiantis aspektais, susijusiais su duomenų subjekto darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu?		
12.	Ar bus priimami automatizuoti sprendimai, duomenų subjektams sukeliantys teisinį arba panašų rimtą poveikį?		
13.	Ar bus atliekama sisteminga stebėseną, t. y. duomenų tvarkymas, kuris reikalingas duomenų subjektų stebėsenos arba kontrolės tikslais, įskaitant tinkluose surinktus duomenis arba sistemingą viešos vietos stebėjimą dideliu mastu?		
14.	Ar bus tvarkomi neskelbtini duomenys arba labai asmeniškai duomenys (pavyzdžiui, specialių kategorijų asmens duomenys, duomenys apie apkaltinamuosius nuosprendžius ar nusikalstamas veikas, vietos nustatymo duomenys, finansiniai duomenys, elektroniniai laiškai ir kt.)?		
15.	Ar asmens duomenys bus tvarkomi dideliu mastu?		
16.	Ar bus atliekamos sudėtingos duomenų tvarkymo operacijos? Jei taip, kokios?		
17.	Ar bus tvarkomi duomenys, susiję su pažeidžiamais duomenų subjektais? Jei taip, kokiais?		
18.	Ar bus naudojamos inovatyviais organizaciniais-techniniais sprendimais? Jei taip, kokiais?		
19.	Ar dėl paties duomenų tvarkymo duomenų subjektams užkertamas kelias naudotis savo teisėmis, paslaugomis arba sudaryti sutartis?		

Išvados: klausimyną užpildęs darbuotojas nustato, ar yra poreikis atlikti poveikio duomenų apsaugai vertinimą, ir nurodo savo siūlymą dėl poveikio duomenų apsaugai vertinimo atlikimo (yra poreikis atlikti poveikio duomenų apsaugai vertinimą ar ne) bei siūlymą pagrindžiančius motyvus. Nustačius, kad yra poreikis atlikti poveikio duomenų apsaugai vertinimą, gali būti teikiamas siūlymas dėl darbuotojų, kurių dalyvavimas atliekant poveikio duomenų apsaugai vertinimą būtų reikšmingas pagal jų turimas kompetencijas ir atliekamas asmens duomenų tvarkymo funkcijas.

Klausimyną užpildžiusio

darbuotojo pareigos

(parašas)

(vardas ir pavardė)

Poveikio duomenų apsaugai vertinimo procedūra
D priedas

(Poveikio duomenų apsaugai vertinimo atlikimo ataskaitos forma)

Biudžetinė įstaiga „Skaitlis“

(Duomenų valdytojo pavadinimas)

TVIRTINU

(parašas)

(vardas ir pavardė)

POVEIKIO DUOMENŲ APSAUGAI VERTINIMO ATLIKIMO ATASKAITA

Nr.

(data)

(numeris)

(vieta)

1. Priežastys, dėl kurių būtina atlikti poveikio duomenų apsaugai vertinimą

Planuojamos vykdyti veiklos aprašymas, jos tikslai ir planuojamos atlikti asmens duomenų tvarkymo operacijos. Paaiškinimas, kodėl būtina atlikti poveikio duomenų apsaugai vertinimą. Jei reikia, prie formos pridedami susiję dokumentai.

2. Asmens duomenų tvarkymo aprašymas

Aprašomi asmens duomenų rinkimo, naudojimo, saugojimo ir naikinimo veiksmai, nurodoma, iš kokių šaltinių bus renkami duomenys, kam bus teikiami (galima pateikti asmens duomenų tvarkymo veiksmų schemą). Aprašoma, kokie asmens duomenų tvarkymo veiksmai gali kelti pavojų fizinių asmenų teisėms ir laisvėms.

Aprašomas tvarkymo mastas: kokių kategorijų asmens duomenys bus tvarkomi; ar bus tvarkomi specialių kategorijų asmens duomenys arba duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas; kiek duomenų, kaip dažnai bus renkama ir naudojama; kaip ilgai bus saugomi asmens duomenys; nurodomas apytikslis duomenų subjektų skaičius bei geografinė duomenų tvarkymo aprėptis.

Aprašomas duomenų tvarkymo pobūdis: kokio pobūdžio santykiai sieja Įstaigą su duomenų subjektais; ar duomenų subjektai turės galimybę kontroliuoti duomenų tvarkymą; ar duomenų subjektai gali numatyti, kad jų asmens duomenys bus taip tvarkomi; ar bus tvarkomi vaikų ir kitų pažeidžiamų asmenų duomenys; įvertinama, ar toks duomenų tvarkymas yra saugus; ar duomenų tvarkymo technologijos yra naujos, ar egzistuojančios technologijos bus panaudotos kitaip; koks yra technologijų išsivystymo lygis šioje srityje; ar yra kokių nors visuomeninių ar pan. problemų ar klausimų, į kuriuos būtina atsižvelgti; nurodoma, ar yra įsipareigojimas laikytis patvirtinto elgesio kodekso ar patvirtinto sertifikavimo mechanizmo.

Aprašomi asmens duomenų tvarkymo tikslai: kokių rezultatų siekiama gauti; kokių poveikį tai turės fiziniams asmenims; kokia yra tokio duomenų tvarkymo nauda Įstaigai bei kitiems asmenims.

3. Konsultacijos

Aprašoma, kaip planuojama sužinoti suinteresuotų asmenų nuomonę, arba pagrindžiama, kodėl to daryti nebūtina (pavyzdžiui, dėl duomenų saugumo ar konfidencialumo reikalavimų, dėl neproporcingai didelės administracinės naštos ir pan.); kokių asmenų nuomonę planuojama gauti; kokie asmenys bus pasitelkti Įstaigoje, ar bus pasitelkti duomenų tvarkytojai; ar planuojama konsultuotis su duomenų saugos ekspertais ar kitokių sričių ekspertais.

4. Būtinumo ir proporcingumo įvertinimas

Aprašomas asmens duomenų tvarkymo teisėtumas ir tvarkymo proporcingumas: nurodomas teisėto tvarkymo pagrindas; įvertinama, ar tvarkant asmens duomenis bus pasiektas Įstaigos tikslas; ar tą patį rezultatą įmanoma pasiekti kitaip; kaip bus išvengta veiklos sutrikimų; kaip bus užtikrinta duomenų kokybė ir įgyvendintas duomenų kiekio mažinimo principas; kokia informacija bus pateikta duomenų subjektams; kaip Įstaiga planuoja įgyvendinti duomenų subjektų teises; kaip bus užtikrinta, kad duomenų tvarkytojas, jei toks pasitelkiamas, laikytųsi reikalavimų; kaip bus užtikrintas į užsienio valstybes teikiamų asmens duomenų saugumas.

5. Pavojų nustatymas ir įvertinimas

<i>Aprašomas pavojus ir poveikio fiziniam asmeniui pobūdis.</i>	Žalos tikimybė	Žalos sunkumas	Bendras pavojaus lygis
	<i>Mažai tikėtina, tikėtina ar labai tikėtina</i>	<i>Minimali, reikšminga ar sunki</i>	<i>Mažas, vidutinis ar didelis</i>

6. Priemonių sumažinti ar pašalinti pavojus nustatymas

<i>Nurodomos papildomos priemonės, kurių galima imtis siekiant sumažinti ar pašalinti didelį ar vidutinį pavojų.</i>				
Pavojus	Priemonės sumažinti ar pašalinti pavojų	Priemonės pritaikymo rezultatas	Likęs pavojaus lygis	Priemonė patvirtinta
		<i>Pašalinta, sumažinta, priimtina rizika</i>	<i>Mažas, vidutinis ar didelis</i>	<i>Taip, ne</i>

7. Išvados ir sprendimai

Nurodomos priemonės ir įvardijamas likęs pavojus	Vardas, pavardė, data, parašas	Pastabos
Priemonės patvirtintos:		<i>Ištraukti numatytas priemones į veiklos planą, nustatant atlikimo terminą ir atsakingus asmenis</i>
Likęs pavojus pripažintas priimtina rizika:		<i>Jei priimtina rizika pripažintas didelis pavojus, privaloma kreiptis dėl išankstinės konsultacijos į Valstybinę duomenų apsaugos inspekciją</i>

Poveikio duomenų apsaugai
vertinimo koordinadorius

(parašas)

(vardas ir pavardė)

**PAVOJAUS ĮVERTINIMO IR BENDRO PAVOJAUS LYGIO NUSTATYMO
LENTELĖ**

Žalos sunkumas	Sunki	Mažas pavojus	Didelis pavojus	Didelis pavojus
	Reikšminga	Mažas pavojus	Vidutinis pavojus	Didelis pavojus
	Minimali	Mažas pavojus	Mažas pavojus	Mažas pavojus
		Mažai tikėtina	Tikėtina	Labai tikėtina
		Žalos tikimybė		

Poveikio duomenų apsaugai vertinimo procedūros
F priedas

PAVOJAUS MAŽINIMO IR ŠALINIMO PRIEMONIŲ REKOMENDACIJOS

Pavojaus lygis	Rekomenduojamos pavojaus mažinimo ar šalinimo priemonės
Mažas	Papildomų pavojaus mažinimo ir (ar) šalinimo priemonių galima nenumatyti, išskyrus atvejus, kai joms įgyvendinti nereikia didelių sąnaudų. Turi būti užtikrinta, kad veiktų esamos pavojaus mažinimo ir (ar) šalinimo priemonės.
Vidutinis	Rekomenduotina numatyti pavojaus mažinimo ir (ar) šalinimo priemones, įgyvendinti tokias pavojaus mažinimo ir (ar) šalinimo priemones, kurios nėra labai imlios finansiniu ir laiko atžvilgiu, tačiau yra pakankamos sumažinti pavojaus lygį arba jį pakankamai kontroliuoti.
Didelis	Būtina išsamiai išnagrinėti situaciją, nustatyti pavojaus mažinimo ir (ar) šalinimo priemones. Šios priemonės turi būti nustatytos pavojaus, kylančio fizinių asmenų teisėms ir laisvėms, mažinimo ir šalinimo priemonių plane. Priemonės gali būti susijusios ne tik su veiksmais Įstaigos viduje, apie nustatytą labai didelį pavojų fizinių asmenų teisėms ir laisvėms gali būti informuota Valstybinė duomenų apsaugos inspekcija. Nustatytos pavojaus mažinimo ir (ar) šalinimo priemonės turi būti įgyvendintos per nustatytą laikotarpį. Turi būti atliekamas priemonių įgyvendinimo veiksmingumo vertinimas. Įgyvendinus numatytas priemones, iš naujo turi būti atliktas pavojaus vertinimas.

(Pavojaus, kylančio fizinių asmenų teisėms ir laisvėms, mažinimo ir šalinimo priemonių plano forma)

Biudžetinė įstaiga „Skaitlis“
(Duomenų valdytojo pavadinimas)

TVIRTINU

(parašas)

(vardas ir pavardė)

PAVOJAUS, KYLANČIO FIZINIŲ ASMENŲ TEISĖMS IR LAISVĖMS, MAŽINIMO IR ŠALINIMO PRIEMONIŲ PLANAS

(data) Nr. _____
(numeris)

(vieta)

Eil. Nr.	Pavojaus priežastis (kilmė)	Pavojaus pasekmė	Planuojamos pavojaus mažinimo ir (ar) šalinimo priemonės	Vykdytojo pareigos, vardas ir pavardė	Įgyvendinimo terminas	Planuojami pavojaus mažinimo ir (ar) šalinimo priemonės įgyvendinimo veiksmai	Įgyvendini mo žyma	Veiksmingum o vertinimas	Vertini mo atlikim o data	Vertinimą atlikusio asmens pareigos, vardas ir pavardė
1.										
2.										
