PATVIRTINTA
Pakruojo nestacionarių socialinių paslaugų
centro direktoriaus 2026 m. rugpjūčio 5 d.
įsakymu Nr. V – 388

ASMENS DUOMENŲ TVARKYMO IR ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų tvarkymo ir asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) nustato asmens duomenų tvarkymo organizavimo tvarką, darbuotojų pareigas ir atsakomybę, organizacines ir technines asmens duomenų apsaugos priemones, duomenų subjektų teisių įgyvendinimo bendrąsias nuostatas, taip pat asmens duomenų saugumo pažeidimų nustatymo, registravimo, vertinimo, valdymo ir reagavimo į juos tvarką Pakruojo nestacionarių socialinių paslaugų centre (toliau – Centras).
2. Aprašo tikslas – nustatyti vieningą ir rizika pagrįstą asmens duomenų apsaugos sistemą Centre, užtikrinančią, kad asmens duomenys būtų tvarkomi teisėtai, sąžiningai, skaidriai ir saugiai, gerbiant asmens privatumą, orumą, savarankiškumą ir individualius poreikius, taip pat nuolat vertinant ir gerinant taikomų asmens duomenų apsaugos priemonių veiksmingumą.
3. Šis Aprašas taikomas visiems Centro darbuotojams, praktiką atliekantiems asmenims, savanoriams, asmenims, dirbantiems pagal paslaugų teikimo sutartis, ir kitiems asmenims, kurie vykdydami savo funkcijas tvarko Centro valdomus asmens duomenis arba turi prieigą prie jų.
4. Aprašas taikomas visiems Centro tvarkomiems asmens duomenims, neatsižvelgiant į jų pateikimo ar saugojimo formą, įskaitant: popierinius dokumentus; elektroninius dokumentus; informacinėse sistemose tvarkomus duomenis; elektroninio pašto informaciją; vaizdo, garso ar kitus duomenis, jeigu jie tvarkomi vykdant Centro funkcijas.
5. Centras tvarko tik tuos asmens duomenis, kurie yra būtini teisės aktuose nustatytoms funkcijoms vykdyti, socialinėms paslaugoms teikti, darbo santykiams administruoti, sutartiniams įsipareigojimams vykdyti ar kitiems teisėtiems tikslams pasiekti.
6. Tvarkydamas asmens duomenis Centras vadovaujasi:
6.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo;
6.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;
6.3. Lietuvos Respublikos socialinių paslaugų įstatymu ir socialinių paslaugų teikimą reglamentuojančiais teisės aktais;
6.4. Lietuvos Respublikos dokumentų ir archyvų įstatymu bei dokumentų valdymą ir saugojimą reglamentuojančiais teisės aktais;
6.5. Lietuvos Respublikos kibernetinio saugumo įstatymu, kai jo nuostatos taikomos Centro veiklai;
6.6. kitais asmens duomenų tvarkymą ir informacijos saugumą reglamentuojančiais teisės aktais bei Centro vidaus teisės aktais.
7. Šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Bendrajame duomenų apsaugos reglamente ir kituose asmens duomenų apsaugą reglamentuojančiuose teisės aktuose.
8. Centras yra jo veikloje tvarkomų asmens duomenų valdytojas, išskyrus atvejus, kai teisės aktai, sutartys ar konkrečios informacinės sistemos veiklą reglamentuojantys dokumentai nustato kitokį Centro vaidmenį.

II SKYRIUS
ASMENS DUOMENŲ TVARKYMO PRINCIPAI IR TEISINIAI PAGRINDAI

9. Centro darbuotojai asmens duomenis tvarko tik tiek, kiek tai būtina jų pareigoms ir Centro funkcijoms vykdyti.

10. Draudžiama rinkti, kopijuoti, perduoti ar kitaip naudoti asmens duomenis, jeigu tai nėra susiję su darbuotojo atliekamomis funkcijomis arba nėra tam teisinio pagrindo.
11. Tvarkydami asmens duomenis darbuotojai privalo: užtikrinti jų konfidencialumą; naudoti tik tikslius ir aktualius duomenis; tvarkyti tik minimalius būtinus duomenis; naudoti duomenis tik tais tikslais, kuriais jie buvo surinkti; saugoti duomenis nuo neteisėtos prieigos, praradimo, pakeitimo ar sunaikinimo.
12. Asmens duomenys Centre tvarkomi tik esant bent vienam teisėtam tvarkymo pagrindui, nustatytam Bendrajame duomenų apsaugos reglamente ar kituose teisės aktuose.
13. Asmens duomenys Centre tvarkomi tik nustačius konkretų jų tvarkymo tikslą ir bent vieną taikytiną BDAR 6 straipsnio 1 dalyje nustatytą teisinį pagrindą:
13.1. duomenų subjektas davė sutikimą tvarkyti jo asmens duomenis vienu ar keliais konkrečiais tikslais;
13.2. duomenis būtina tvarkyti siekiant sudaryti arba vykdyti sutartį, kurios šalis yra duomenų subjektas;
13.3. duomenis būtina tvarkyti siekiant įvykdyti Centrui taikomą teisinę prievolę;
13.4. duomenis būtina tvarkyti siekiant apsaugoti duomenų subjekto ar kito fizinio asmens gyvybinius interesus;
13.5. duomenis būtina tvarkyti vykdant viešojo intereso užduotį arba Centrui pavestas viešosios valdžios funkcijas;
13.6. kitais BDAR ir Lietuvos Respublikos teisės aktuose nustatytais pagrindais.
Konkretus teisinis pagrindas nustatomas atsižvelgiant į duomenų tvarkymo tikslą ir nurodomas Centro asmens duomenų tvarkymo veiklos įrašuose bei, kai taikoma, duomenų subjektams teikiamoje informacijoje.
14. Specialių kategorijų asmens duomenys, įskaitant sveikatos, negalios, priklausomybių ir kitus jautrius duomenis, tvarkomi tik tada, kai yra nustatytas ne tik BDAR 6 straipsnio 1 dalyje nurodytas teisinis pagrindas, bet ir bent viena BDAR 9 straipsnio 2 dalyje nustatyta specialių kategorijų duomenų tvarkymo sąlyga. Tokie duomenys tvarkomi tik tokia apimtimi, kuri būtina konkrečiai Centro funkcijai vykdyti ar socialinei paslaugai teikti, taikant sustiprintas konfidencialumo ir saugumo priemones.
15. Darbuotojai, atlikdami savo funkcijas, privalo vadovautis principu „būtina žinoti", t. y. susipažinti tik su tais asmens duomenimis, kurie reikalingi jų tiesioginėms darbo funkcijoms vykdyti.
16. Sutikimas tvarkyti asmens duomenis naudojamas tik tada, kai duomenų tvarkymas nėra būtinas Centrui taikomai teisinei prievolei, viešojo intereso užduočiai, sutarties vykdymui ar kitam teisėtam tikslui įgyvendinti.
17. Sutikimas turi būti duotas laisva valia, būti konkretus, informuotas, nedviprasmiškas ir įrodomas. Asmuo prieš duodamas sutikimą informuojamas apie teisę jį bet kada atšaukti.
18. Sutikimo atšaukimas turi būti toks pat paprastas kaip ir jo davimas. Atšaukus sutikimą, duomenys nebetvarkomi sutikimu grindžiamu tikslu, išskyrus atvejus, kai yra kitas teisėtas jų tvarkymo pagrindas.
19. Atsisakymas duoti sutikimą dėl duomenų tvarkymo, kuris nėra būtinas socialinei paslaugai skirti ar teikti, negali lemti paslaugos neteikimo, jos kokybės pabloginimo ar kitų neigiamų pasekmių asmeniui.

III SKYRIUS
CENTRE TVARKOMI ASMENS DUOMENYS IR JŲ TVARKYMO TIKSLAI

20. Centras, vykdydamas teisės aktuose nustatytas funkcijas ir teikdamas socialines paslaugas, tvarko tik tuos asmens duomenis, kurie yra būtini konkrečiam duomenų tvarkymo tikslui pasiekti.
21. Centre tvarkomų asmens duomenų pagrindinės kategorijos:

Duomenų subjektai	Tvarkomi duomenys	Tvarkymo tikslas
Socialinių paslaugų gavėjų šeimos nariai, artimieji ir atstovai	Identifikaciniai, kontaktiniai, giminystės, atstovavimo ir kiti	Bendradarbiavimas organizuojant ir teikiant

	paslaugai organizuoti būtini duomenys	socialines paslaugas, atstovavimo teisės patikrinimas
Vaikai, kuriems teikiamos socialinės paslaugos.	Identifikaciniai, kontaktiniai, šeimos, ugdymo ir kiti būtini duomenys.	Vaiko interesų užtikrinimas ir paslaugų teikimas
Globėjai, budintys globotojai, įtėviai, šeimynų dalyviai	Identifikaciniai, kontaktiniai, kvalifikacijos, vertinimo dokumentų duomenys.	Globos centro funkcijų vykdymas
Asmeniniai asistentai, individualios priežiūros darbuotojai ir kiti paslaugas teikiantys asmenys	Identifikaciniai, kontaktiniai, kvalifikacijos, darbo organizavimo ir atsiskaitymo duomenys	Paslaugų organizavimas, administravimas ir kontrolė
Darbuotojai	Personalo administravimo duomenys.	Darbo santykių administravimas
Pretendentai į pareigas	Atrankos dokumentuose pateikti duomenys.	Atrankų organizavimas
Sutarčių šalys	Kontaktiniai ir atsiskaitymų duomenys.	Sutarčių vykdymas
Pareiškėjai	Prašymuose ir skunduose pateikti duomenys.	Prašymų ir skundų nagrinėjimas
Praktikantai ir savanoriai	Identifikaciniai, kontaktiniai, mokymosi, kvalifikacijos ir veiklos duomenys	Praktikos ir savanoriškos veiklos organizavimas
Renginių, mokymų ir kitų veiklų dalyviai	Identifikaciniai, kontaktiniai, dalyvavimo, atvaizdo ir kiti būtini duomenys	Renginių ir veiklų organizavimas, apskaita bei viešinimas, kai tam yra teisėtas pagrindas
Centro interneto svetainės ir socialinių tinklų lankytojai bei besikreipiantys asmenys	Paskyrų identifikaciniai duomenys, komentarai, žinutės ir kita paties asmens pateikta informacija	Komunikacija, paklausimų nagrinėjimas ir Centro veiklos viešinimas
Vaizdo stebėjimo teritorijoje esantys asmenys, jeigu Centre vykdomas vaizdo stebėjimas	Asmens atvaizdas, buvimo vieta ir laikas	Asmenų ir turto saugumo užtikrinimas
Skambinantys ir pokalbiuose dalyvaujantys asmenys, jeigu daromi garso įrašai	Balso įrašas, kontaktiniai ir pokalbio metu pateikti duomenys	Paslaugų kokybės, įrodymų ar kitais teisėtais tikslais
Skolininkai, išmokų, kompensacijų ar mokėjimų gavėjai	Identifikaciniai, finansiniai, atsiskaitymų ir įsiskolinimo duomenys	Mokėjimų administravimas ir apskaita

22. Priklausomai nuo teikiamos socialinės paslaugos pobūdžio, Centras gali tvarkyti ir kitus teisės aktuose numatytus asmens duomenis, jeigu tai būtina teisės aktuose nustatytoms funkcijoms vykdyti.
23. Specialių kategorijų asmens duomenys tvarkomi tik tais atvejais, kai tai leidžia teisės aktai ir kai šių duomenų tvarkymas yra būtinas socialinėms paslaugoms teikti arba kitoms Centro funkcijoms vykdyti.
24. Darbuotojai negali rinkti perteklinių duomenų ar naudoti jų kitais tikslais, negu jie buvo surinkti.

IV SKYRIUS
DARBUOTOJŲ PAREIGOS TVARKANT ASMENS DUOMENIS

25. Kiekvienas darbuotojas, tvarkantis asmens duomenis, atsako už jų konfidencialumą, vientisumą ir saugumą pagal savo kompetenciją.
26. Darbuotojas privalo:
26.1. tvarkyti tik tuos asmens duomenis, kurie reikalingi jo darbo funkcijoms atlikti;
26.2. užtikrinti, kad su asmens duomenimis negalėtų susipažinti tam neturintys teisės asmenys;
26.3. naudoti tik jam suteiktus prisijungimo duomenis;
26.4. saugoti prisijungimo slaptažodžius ir jų neatskleisti kitiems asmenims;
26.5. užrakinti kompiuterį palikdamas darbo vietą;
26.6. prieš perduodamas informaciją telefonu, elektroniniu paštu ar kitu būdu, įsitikinti gavėjo tapatybe ir teise gauti informaciją;
26.7. užtikrinti, kad spausdinti dokumentai nebūtų paliekami viešai prieinamose vietose;
26.8. nedelsdamas pranešti apie pastebėtą ar įtariamą asmens duomenų saugumo pažeidimą;
26.9. laikytis šiame Apraše ir kituose Centro vidaus teisės aktuose nustatytų reikalavimų.
27. Darbuotojui draudžiama:
27.1. naudoti asmens duomenis asmeniniais tikslais;
27.2. perduoti prisijungimo duomenis kitam asmeniui;
27.3. kopijuoti dokumentus, jei tai nėra būtina darbo funkcijoms vykdyti;
27.4. fotografuoti ar kitaip kopijuoti dokumentus asmeniniais įrenginiais, išskyrus atvejus, kai tai leidžiama Centro nustatyta tvarka;
27.5. aptarinėti socialinių paslaugų gavėjų asmens duomenis viešose vietose ar su asmenimis, kurie neturi teisės jų žinoti;
27.6. palikti dokumentus be priežiūros automobilyje, viešose vietose ar kitose nesaugiose vietose, jei dėl to kyla rizika neteisėtai susipažinti su juose esančiais duomenimis.
28. Darbuotojas, vykdamas pas socialinių paslaugų gavėją, pasiima tik tuos dokumentus ir informaciją, kurie būtini konkrečiai paslaugai suteikti.
29. Pasibaigus vizitui darbuotojas privalo patikrinti, ar paslaugų gavėjo gyvenamojoje vietoje nepaliko dokumentų, užrašų, laikmenų ar Centro įrenginių. Dokumentai nedelsiant grąžinami į jų saugojimo vietą Centre. Kai dėl darbo organizavimo dokumentų nedelsiant grąžinti nėra galimybės, jie iki grąžinimo saugomi uždaroje, pašaliniams asmenims neprieinamoje vietoje. Dokumentus su asmens duomenimis draudžiama palikti automobilyje matomoje vietoje ar jame laikyti ilgiau, negu būtina konkrečiai darbo funkcijai atlikti.
30. Kilus abejonių dėl asmens duomenų tvarkymo teisėtumo, darbuotojas prieš atlikdamas veiksmus konsultuojasi su tiesioginiu vadovu arba Centro paskirtu atsakingu asmeniu.
31. Tvarkant vaikų, asmenų su negalia, socialinę riziką patiriančių, smurtą ar krizę išgyvenančių, priklausomybių turinčių ir kitų pažeidžiamų asmenų duomenis taikomos sustiprintos konfidencialumo ir duomenų atskleidimo kontrolės priemonės.
32. Informacija apie asmenį jo šeimos nariams, artimiesiems ar kitiems asmenims teikiama tik patikrinus jų teisę tokią informaciją gauti. Vien šeimos, giminystės ar artimo ryšio faktas savaime nesuteikia teisės gauti asmens duomenis.
33. Kai duomenų subjekto vardu kreipiasi atstovas, prieš teikiant informaciją patikrinama jo tapatybė, atstovavimo pagrindas ir įgaliojimų apimtis.
34. Tvarkant vaiko duomenis pirmiausia vadovaujamasi geriausių vaiko interesų principu, atsižvelgiama į vaiko amžių, brandą ir teisę būti išklausytam.

V SKYRIUS
ORGANIZACINĖS IR TECHNINĖS ASMENS DUOMENŲ APSAUGOS PRIEMONĖS

35. Centras, atsižvelgdamas į tvarkomų asmens duomenų pobūdį, apimtį, tvarkymo tikslus bei galimą riziką duomenų subjektų teisėms ir laisvėms, taiko organizacines ir technines asmens duomenų apsaugos priemones, užtikrinančias tinkamą asmens duomenų saugumo lygį.
36. Centro direktorius užtikrina, kad darbuotojams būtų suteikiamos tik tos prieigos prie informacinių sistemų, dokumentų ir kitų informacijos išteklių, kurios būtinos jų darbo funkcijoms atlikti.
37. Darbuotojui pasikeitus pareigoms, darbo funkcijoms, išėjus ilgalaikių atostogų ar pasibaigus darbo, praktikos, savanorystės arba kitokiems teisiniams santykiams su Centru, jam suteiktos prieigos

nedelsiant peržiūrimos, apribojamos, pakeičiamos arba panaikinamos. Pasibaigus teisiniams santykiams, prieigos panaikinamos ne vėliau kaip paskutinę asmens darbo ar veiklos Centre dieną.
38. Darbuotojai naudojasi tik jiems suteiktais naudotojo vardais, slaptažodžiais ar kitomis autentifikavimo priemonėmis. Darbuotojams draudžiama perduoti prisijungimo duomenis kitiems asmenims arba naudotis kitam asmeniui suteiktomis prieigomis.
39. Darbuotojai privalo užtikrinti, kad darbo vietoje naudojami įrenginiai ir dokumentai nebūtų prieinami pašaliniams asmenims. Laikinai paliekant darbo vietą turi būti imamasi priemonių, kad tretieji asmenys negalėtų susipažinti su asmens duomenimis.
40. Popieriniai dokumentai, kuriuose yra asmens duomenų, saugomi rakinamose spintose, kabinetuose ar kitose saugiose vietose, kai jais nesinaudojama.
41. Elektroniniai dokumentai ir informacinėse sistemose tvarkomi duomenys saugomi Centro naudojamose informacinėse sistemose arba kitose Centro patvirtintose duomenų saugojimo vietose.
42. Darbuotojams draudžiama darbo dokumentus ir kitą informaciją, kurioje yra asmens duomenų, saugoti asmeniniuose įrenginiuose, asmeninėse debesijos paskyrose ar kitose Centro nepatvirtintose informacijos saugojimo vietose, išskyrus atvejus, kai tai leidžiama Centro vidaus teisės aktais arba Centro direktoriaus sprendimu.
43. Asmens duomenys elektroniniu paštu, kitomis elektroninių ryšių priemonėmis ar informacinėmis sistemomis perduodami tik įsitikinus, kad gavėjas turi teisę tokius duomenis gauti.
44. Jeigu perduodami didelės apimties asmens duomenys arba specialių kategorijų asmens duomenys, darbuotojai privalo naudoti saugius duomenų perdavimo būdus, atsižvelgdami į Centro taikomas organizacines ir technines priemones.
45. Darbuotojai, vykdami teikti socialinių paslaugų ne Centro patalpose, privalo užtikrinti, kad dokumentai ir mobilieji įrenginiai būtų apsaugoti nuo praradimo, vagystės ar neteisėtos prieigos.
46. Tvarkant asmens duomenis ne Centro patalpose, darbuotojai privalo užtikrinti, kad pašaliniai asmenys negalėtų susipažinti su dokumentuose ar įrenginiuose esančiais asmens duomenimis.
47. Dokumentai ir kitos laikmenos, kuriose yra asmens duomenų, naikinami tik pasibaigus jų saugojimo terminui, vadovaujantis dokumentų valdymą reglamentuojančiais teisės aktais ir Centro vidaus dokumentais, užtikrinant, kad asmens duomenų nebūtų galima atkurti.
48. Centro naudojamos informacinės sistemos, kompiuterinė įranga ir kita informacinių technologijų infrastruktūra prižiūrima taip, kad būtų užtikrintas tvarkomų asmens duomenų konfidencialumas, vientisumas, prieinamumas ir atsparumas galimiems saugumo incidentams.
49. Darbuotojai privalo nedelsdami informuoti tiesioginį vadovą arba kitą Centro paskirtą atsakingą asmenį apie pastebėtus informacinių technologijų veikimo sutrikimus ar aplinkybes, galinčias turėti įtakos asmens duomenų saugumui.

VI SKYRIUS
ASMENS DUOMENŲ TEIKIMAS IR SAUGOJIMAS

50. Centras asmens duomenis tretiesiems asmenims teikia tik teisės aktų nustatytais atvejais ir tvarka, kai tam yra teisėtas asmens duomenų tvarkymo pagrindas.
51. Asmens duomenys gali būti teikiami:
51.1. pačiam duomenų subjektui arba jo tinkamai įgaliotam atstovui;
51.2. valstybės ir savivaldybių institucijoms bei įstaigoms, kai jos turi teisę gauti tokius duomenis pagal teisės aktus;
51.3. teisėsaugos institucijoms, teismams ir kitoms teisės aktų įgaliotoms institucijoms;
51.4. duomenų tvarkytojams, su kuriais Centras yra sudaręs asmens duomenų tvarkymo sutartis arba kurie asmens duomenis tvarko teisės aktų nustatytais pagrindais;
51.5. kitiems asmenims, tik teisės aktuose nustatytais atvejais arba turint duomenų subjekto sutikimą, kai sutikimas yra tinkamas duomenų tvarkymo pagrindas.
52. Prieš teikdamas asmens duomenis darbuotojas privalo įsitikinti, kad:
52.1. prašantis asmuo ar institucija turi teisę gauti prašomus duomenis;
52.2. prašomi duomenys yra būtini nurodytam tikslui pasiekti;
52.3. perduodama tik tokia asmens duomenų apimtis, kuri būtina konkrečiam tikslui.

53. Kilus abejonių dėl asmens duomenų teikimo teisėtumo, darbuotojas asmens duomenų neteikia tol, kol sprendimo nepriima tiesioginis vadovas arba kitas Centro paskirtas atsakingas asmuo.
54. Asmens duomenys telefonu teikiami tik įsitikinus informacijos prašančio asmens tapatybe ir teise gauti tokią informaciją.
55. Elektroniniu paštu asmens duomenys perduodami tik naudojantis Centro elektroninio pašto priemonėmis ir įsitikinus, kad nurodytas gavėjo elektroninio pašto adresas yra teisingas.
56. Kai perduodami specialių kategorijų asmens duomenys arba didesnės apimties asmens duomenys, darbuotojai privalo naudoti saugesnius duomenų perdavimo būdus, jeigu tokie yra nustatyti Centro vidaus teisės aktuose.
57. Asmens duomenų dokumentai ir bylos saugomi teisės aktuose ir Centro dokumentacijos plane nustatytais terminais.
58. Pasibaigus dokumentų saugojimo terminui, dokumentai ir kitos laikmenos sunaikinami teisės aktų nustatyta tvarka, užtikrinant, kad asmens duomenų nebūtų galima atkurti.
59. Darbuotojams draudžiama savavališkai naikinti dokumentus, kuriuose yra asmens duomenų, arba keisti nustatytus jų saugojimo terminus.
60. Jeigu asmens duomenys perduodami kitai institucijai kartu su byla ar dokumentais, užtikrinama, kad perduodami tik tie dokumentai ir duomenys, kurie būtini konkrečiam tikslui arba kuriuos perduoti įpareigoja teisės aktai.

VII SKYRIUS
PRITAIKYTOJI DUOMENŲ APSAUGA IR POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

61. Prieš pradedant naują projektą, paslaugą ar duomenų tvarkymo procesą, diegiant ar keičiant informacinę sistemą, elektroninę priemonę, vaizdo stebėjimą, dirbtinio intelekto sprendimą ar kitą technologiją, turi būti įvertinti asmens duomenų apsaugos reikalavimai ir galimos rizikos duomenų subjektų teisėms ir laisvėms.
62. Naujuose procesuose ir sistemose pagal numatytuosius nustatymus tvarkomi tik konkrečiam tikslui būtini duomenys, ribojama jų apimtis, saugojimo trukmė ir prieinamumas.
63. Kai dėl planuojamo duomenų tvarkymo pobūdžio, apimties, konteksto ar tikslų gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, prieš pradedant tvarkymą atliekamas poveikio duomenų apsaugai vertinimas.
64. Sprendžiant, ar būtinas poveikio duomenų apsaugai vertinimas, privaloma konsultuotis su duomenų apsaugos pareigūnu.

VIII SKYRIUS
ASMENŲ FOTOGRAFAVIMAS, FILMAVIMAS IR INFORMACIJOS VIEŠINIMAS

65. Asmenų fotografavimas, filmavimas, garso įrašymas ir medžiagos viešinimas vykdomi tik iš anksto nustačius konkretų tikslą, duomenų apimtį, saugojimo laikotarpį ir teisėtą duomenų tvarkymo pagrindą.
66. Sutikimas fotografuoti ar filmuoti ir sutikimas viešinti asmens atvaizdą ar įrašą laikomi atskirais duomenų tvarkymo veiksmais. Asmeniui turi būti aiškiai nurodyta, kur, kokiu tikslu ir kiek laiko medžiaga bus skelbiama.
67. Net ir esant sutikimui negali būti viešinama žmogaus orumą galinti pažeisti, jį stigmatizuojanti ar nereikalingai jo sveikatos būklę, negalią, priklausomybę, socialinę riziką, patiriamą krizę, gyvenamąją vietą ar kitas jautrias aplinkybes atskleidžianti informacija.
68. Renginiuose, kuriuose fotografuojama ar filmuojama, dalyviai apie tai informuojami iš anksto arba prie įėjimo aiškiai matomu būdu. Asmenims, kurie nenori būti fotografuojami ar filmuojami, sudaroma reali galimybė apie tai pranešti ir, kiek objektyviai įmanoma, nepatekti į viešinamą medžiagą.
69. Prieš paskelbiant informaciją interneto svetainėje, socialiniuose tinkluose ar žiniasklaidoje, atsakingas darbuotojas patikrina, ar skelbiami tik būtini duomenys ir ar dokumentuose, nuotraukose bei jų metaduomenyse nėra perteklinių asmens duomenų.

IX SKYRIUS
DUOMENŲ SUBJEKTŲ TEISIŲ ĮGYVENDINIMAS

70. Centras užtikrina duomenų subjektų teisių įgyvendinimą vadovaudamasis BDAR, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais. Informacija apie duomenų subjektų teises ir jų įgyvendinimo tvarką pateikiama aiškia, glausta, skaidria, suprantama ir lengvai prieinama forma. Atsižvelgiant į asmens amžių, negalią, sveikatos būklę, kalbinius ar kitus individualius poreikius, informacija paaiškinama arba pateikiama asmeniui tinkamu būdu.
71. Duomenų subjektas turi teisę:
71.1. gauti informaciją apie savo asmens duomenų tvarkymą;
71.2. susipažinti su tvarkomais savo asmens duomenimis;
71.3. reikalauti ištaisyti netikslius ar papildyti neišsamius asmens duomenis;
71.4. teisės aktuose nustatytais atvejais, reikalauti ištrinti asmens duomenis arba apriboti jų tvarkymą;
71.5. nesutikti, kad jo asmens duomenys būtų tvarkomi, kai tokia teisė numatyta teisės aktuose;
71.6. pasinaudoti kitomis Bendrajame duomenų apsaugos reglamente nustatytomis teisėmis.
72. Duomenų subjektas prašymą dėl savo teisių įgyvendinimo Centrui gali pateikti raštu, elektroninių ryšių priemonėmis arba kitu Centro nustatytu būdu.
73. Gavęs duomenų subjekto prašymą darbuotojas jo nenagrinėja savarankiškai, jeigu toks nagrinėjimas nepriskirtas jo funkcijoms, bet nedelsdamas perduoda prašymą Centro direktoriaus paskirtam atsakingam asmeniui arba kitam kompetentingam darbuotojui.
74. Prieš įgyvendinant duomenų subjekto teises, Centras turi teisę įsitikinti prašymą pateikusio asmens tapatybe, jeigu tai būtina siekiant apsaugoti asmens duomenis nuo neteisėto atskleidimo.
75. Duomenų subjekto prašymas išnagrinėjamas ir informacija apie veiksmus, kurių imtasi, jam pateikiama nepagrįstai nedelsiant, bet ne vėliau kaip per vieną mėnesį nuo prašymo gavimo. Atsižvelgiant į prašymų sudėtingumą ir skaičių, šis terminas gali būti pratęstas dar dviem mėnesiams, apie pratęsimą ir jo priežastis informuojant duomenų subjektą per vieną mėnesį nuo prašymo gavimo.
76. Duomenų subjekto prašymas gali būti netenkinamas arba tenkinamas iš dalies tik teisės aktuose nustatytais atvejais. Sprendimas atsisakyti tenkinti prašymą turi būti pagrįstas ir apie jį teisės aktų nustatyta tvarka informuojamas prašymą pateikęs asmuo.
77. Darbuotojai privalo užtikrinti, kad duomenų subjektų teisės būtų įgyvendinamos nepažeidžiant kitų asmenų teisių ir laisvių, tarnybos, profesinės ar kitais teisės aktais saugomos paslapties reikalavimų.

X SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMAS

78. Kiekvienas Centro darbuotojas, pastebėjęs arba pagrįstai įtardamas galimą asmens duomenų saugumo pažeidimą, privalo nedelsdamas imtis šiame Apraše nustatytų veiksmų.
79. Asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi ar kitaip tvarkomi asmens duomenys arba be leidimo gaunama prieiga prie jų. Pažeidimas gali būti susijęs su asmens duomenų konfidencialumo, vientisumo arba prieinamumo praradimu.
80. Galimais asmens duomenų saugumo pažeidimais laikomi ir šie atvejai:
80.1. asmens duomenys išsiųsti netinkamam gavėjui;
80.2. prarasti dokumentai, bylos arba jų kopijos;
80.3. pamestas arba pavogtas kompiuteris, mobilusis telefonas, planšetinis kompiuteris ar kita laikmena, kurioje gali būti asmens duomenų;
80.4. neteisėtai prisijungta prie informacinės sistemos arba panaudoti kito darbuotojo prisijungimo duomenys;
80.5. asmens duomenys tapo prieinami teisės jų gauti neturintiems asmenims;
80.6. netyčia paskelbti arba paviešinti asmens duomenys;
80.7. netinkamai sunaikinti dokumentai ar laikmenos;
80.8. prarasta galimybė naudotis asmens duomenimis dėl techninių ar kitų priežasčių;

80.9. įvykęs arba įtariamas kibernetinis incidentas, galintis turėti įtakos asmens duomenų saugumui;
80.10. bet kuris kitas įvykis, galintis kelti grėsmę asmens duomenų konfidencialumui, vientisumui arba prieinamumui.
81. Darbuotojas neprivalo savarankiškai spręsti, ar konkretus įvykis laikytinas asmens duomenų saugumo pažeidimu. Kilus abejonėms, darbuotojas privalo apie įvykį pranešti šio Aprašo nustatyta tvarka.
82. Sąžiningas ir savalaikis darbuotojo pranešimas apie pastebėtą ar įtariamą asmens duomenų saugumo pažeidimą savaime nelaikomas darbuotojo kaltės pripažinimu. Sprendžiant darbuotojo atsakomybės klausimą vertinamos visos įvykio aplinkybės, darbuotojo veiksmai, neveikimas, kaltės forma ir tai, ar darbuotojas nedelsdamas pranešė apie įvykį bei ėmėsi priemonių galimoms pasekmėms sumažinti.
83. Kiekvienas galimas asmens duomenų saugumo pažeidimas turi būti įvertintas, dokumentuotas ir, jei reikia, registruojamas šio Aprašo nustatyta tvarka, nepriklausomai nuo to, ar buvo priimtas sprendimas apie jį pranešti priežiūros institucijai.

XI SKYRIUS
REAGAVIMAS Į ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS

84. Pastebėjęs arba gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą, darbuotojas privalo nedelsdamas imtis priemonių galimai žalai sumažinti, jeigu tai gali padaryti nepažeisdamas kitų teisės aktų reikalavimų ir savo kompetencijos ribų.
85. Atsižvelgdamas į pažeidimo pobūdį, darbuotojas gali atlikti vieną ar kelis iš šių veiksmų:
85.1. sustabdyti neteisingai siunčiamo elektroninio laiško siuntimą arba, jei įmanoma, paprašyti gavėjo jo nenaudoti ir ištrinti;
85.2. atsiimti netinkamai perduotus dokumentus;
85.3. užrakinti naudotojo paskyrą arba atsijungti nuo informacinės sistemos, jeigu įtariama neteisėta prieiga;
85.4. surasti ir apsaugoti pamestus dokumentus ar laikmenas;
85.5. atlikti kitus veiksmus, kurie gali sumažinti galimą žalą.
86. Darbuotojas apie kiekvieną pastebėtą ar įtariamą asmens duomenų saugumo pažeidimą nedelsdamas praneša savo tiesioginiam vadovui ir Centro direktoriaus paskirtam atsakingam asmeniui Aprašo 1 priede nustatyta forma, elektroniniu paštu, telefonu ar kitu greičiausiu prieinamu būdu. Jeigu darbuotojas informuoja tik tiesioginį vadovą, tiesioginis vadovas privalo nedelsdamas perduoti gautą informaciją atsakingam asmeniui. Žodžiu ar telefonu pateiktas pranešimas vėliau užfiksuojamas raštu.
87. Pranešime, kiek tai įmanoma, nurodoma:
87.1. pažeidimo pastebėjimo data ir laikas;
87.2. pažeidimo aplinkybės;
87.3. kokie asmens duomenys galėjo būti paveikti;
87.4. kiek asmenų galėjo būti paveikta;
87.5. kokių veiksmų jau buvo imtasi;
87.6. kita darbuotojui žinoma reikšminga informacija.
88. Jeigu pranešimo metu darbuotojas neturi visos informacijos apie įvykį, jis pateikia turimą informaciją, o paaiškėjus naujoms aplinkybėms jas nedelsdamas perduoda atsakingam asmeniui.
89. Darbuotojas privalo bendradarbiauti atliekant galimo asmens duomenų saugumo pažeidimo vertinimą ir pateikti visą turimą informaciją, reikalingą aplinkybėms nustatyti.
90. Darbuotojui draudžiama savarankiškai:
90.1. nuspręsti, kad įvykis nėra asmens duomenų saugumo pažeidimas, jeigu kyla pagrįstų abejonių;
90.2. nuslėpti arba sąmoningai nepranešti apie galimą pažeidimą;
90.3. naikinti, keisti ar kitaip šalinti informaciją, kuri gali būti reikšminga tiriant pažeidimą;
90.4. teikti informaciją apie pažeidimą viešai arba tretiesiems asmenims, jeigu tam nėra teisinio pagrindo ar Centro vadovo įgaliojimo.
91. Gavęs informaciją apie galimą pažeidimą, Centro direktoriaus paskirtas atsakingas asmuo nedelsdamas pradeda pažeidimo aplinkybių vertinimą, užregistruoja pranešimo gavimo datą ir laiką,

informuoja Centro direktorių ir duomenų apsaugos pareigūną, jeigu šias funkcijas atlieka kitas asmuo, bei organizuoja būtinus veiksmus pažeidimui sustabdyti ir galimoms pasekmėms sumažinti.
92. Jeigu pažeidimas susijęs su Centro naudojamomis informacinėmis sistemomis arba informacinių technologijų infrastruktūra, į pažeidimo vertinimą gali būti įtraukiami informacinių technologijų priežiūrą atliekantys darbuotojai ar paslaugų teikėjai.
93. Visi veiksmai, atlikti reaguojant į galimą asmens duomenų saugumo pažeidimą, dokumentuojami tiek, kiek tai būtina pažeidimo aplinkybėms nustatyti ir sprendimams pagrįsti.

XII SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VERTINIMAS IR PRANEŠIMŲ TEIKIMAS

94. Vertinimas pradedamas nedelsiant nuo momento, kai Centrui tampa žinoma, kad įvyko arba galėjo įvykti asmens duomenų saugumo pažeidimas. Vertinimo metu nustatoma, ar įvykis atitinka asmens duomenų saugumo pažeidimo požymius, koks pažeidimo pobūdis ir ar dėl jo gali kilti pavojus arba didelis pavojus fizinių asmenų teisėms ir laisvėms.
95. Vertinant asmens duomenų saugumo pažeidimą, atsižvelgiama į:
95.1. pažeidimo pobūdį – konfidencialumo, vientisumo ir (ar) prieinamumo pažeidimą;
95.2. paveiktų duomenų subjektų kategorijas, jų skaičių ir pažeidžiamumą;
95.3. paveiktų asmens duomenų kategorijas, jautrumą, apimtį ir įrašų skaičių;
95.4. galimybę tiesiogiai ar netiesiogiai nustatyti asmens tapatybę;
95.5. galimas fizines, materialines ir nematerialines pasekmes, įskaitant diskriminaciją, tapatybės vagystę, finansinius nuostolius, reputacijos žalą, konfidencialumo praradimą, psichologinę ar socialinę žalą;
95.6. tai, ar duomenys buvo apsaugoti šifravimo, pseudonimų suteikimo ar kitomis priemonėmis;
95.7. asmenį ar organizaciją, kuriems duomenys buvo neteisėtai atskleisti, ir jų patikimumą;
95.8. galimybę susigrąžinti duomenis, sustabdyti jų naudojimą ar kitaip sumažinti žalą;
95.9. priemones, kurių jau imtasi ar planuojama imtis;
95.10. tikimybę, kad pažeidimo pasekmės realiai pasireikš, ir galimą jų sunkumą.
96. Vertinant pažeidimą dalyvauja duomenų apsaugos pareigūnas. Atsižvelgiant į pažeidimo pobūdį, taip pat gali būti pasitelkiami Centro padalinių vedėjai, paslaugų teikėjai, duomenų tvarkytojai, teisės specialistai ir kiti kompetentingi asmenys.
97. Nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti rizika duomenų subjektų teisėms ir laisvėms, priimamas sprendimas dėl pranešimo priežiūros institucijai teisės aktų nustatyta tvarka.
98. Nustačius, kad dėl pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Centras apie pažeidimą informuoja paveiktus duomenų subjektus nepagrįstai nedelsdamas. Informacija pateikiama aiškia ir paprasta kalba, nurodant pažeidimo pobūdį, duomenų apsaugos pareigūno arba kito kontaktinio asmens duomenis, tikėtinas pažeidimo pasekmes ir priemones, kurių Centras ėmėsi ar siūlo imtis galimoms neigiamoms pasekmėms sumažinti.
99. Sprendime dėl pranešimo priežiūros institucijai ar duomenų subjektams nurodomi sprendimo motyvai ir jį pagrindžiančios aplinkybės.
100. Jeigu, atlikus vertinimą, nustatoma, kad apie pažeidimą neprivaloma pranešti priežiūros institucijai arba duomenų subjektams, tokio sprendimo motyvai dokumentuojami.
101. Jeigu po pirminio vertinimo paaiškėja naujos aplinkybės, galinčios turėti įtakos rizikos vertinimui, sprendimas dėl pranešimo priežiūros institucijai ar duomenų subjektams gali būti peržiūrimas.
102. Visi sprendimai, susiję su pažeidimo kvalifikavimu, rizikos vertinimu, pranešimu ar nepranešimu Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams, dokumentuojami. Dokumentuose nurodoma vertinimo data, dalyvavę asmenys, nustatytos aplinkybės, taikyti kriterijai, išvada, sprendimo motyvai, atlikti ir planuojami veiksmai.

XIII SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMAS

103. Centras registruoja visus jam žinomus asmens duomenų saugumo pažeidimus, taip pat galimus pažeidimus, dėl kurių buvo atliktas vertinimas, nepriklausomai nuo to, ar apie juos buvo pranešta Valstybinei duomenų apsaugos inspekcijai arba duomenų subjektams. Jeigu po vertinimo nustatoma, kad įvykis nelaikytinas asmens duomenų saugumo pažeidimu, registre nurodomi tokios išvados motyvai.
104. Asmens duomenų saugumo pažeidimų registrą tvarko Centro direktoriaus paskirtas atsakingas asmuo.
105. Į registrą įrašoma tiek informacijos, kiek būtina pažeidimo aplinkybėms, priimtiems sprendimams ir jų pagrindimui dokumentuoti.
106. Registre, atsižvelgiant į konkretaus pažeidimo pobūdį, gali būti nurodoma:
106.1. pažeidimo registravimo numeris;
106.2. pažeidimo nustatymo data ir laikas;
106.3. trumpas pažeidimo aprašymas;
106.4. pažeidimo aplinkybės;
106.5. galimai paveiktų asmens duomenų kategorijos;
106.6. galimai paveiktų duomenų subjektų kategorijos ir, jei žinoma, jų skaičius;
106.7. atliktas rizikos vertinimas;
106.8. priimti sprendimai;
106.9. informacija apie pranešimą priežiūros institucijai ir (ar) duomenų subjektams, jeigu toks buvo teiktas;
106.10. taikytos arba planuojamos priemonės pažeidimo pasekmėms pašalinti ir panašiems pažeidimams ateityje išvengti;
106.11. pažeidimo nagrinėjimo užbaigimo data.
107. Jeigu po pažeidimo registravimo paaiškėja naujų reikšmingų aplinkybių, registro įrašas papildomas.
108. Asmens duomenų saugumo pažeidimų registras ir su pažeidimo tyrimu susiję dokumentai saugomi teisės aktų nustatyta tvarka.
109. Registro duomenys naudojami:
109.1. pažeidimų analizei;
109.2. prevencinių priemonių planavimui;
109.3. darbuotojų mokymų poreikio nustatymui;
109.4. vidaus kontrolės priemonių tobulinimui;
109.5. teisės aktuose nustatytų pareigų įgyvendinimui.
110. Centro direktoriaus paskirtas atsakingas asmuo periodiškai analizuoja registruotus pažeidimus ir, prireikus, teikia Centro direktoriui pasiūlymus dėl organizacinių, techninių ar kitų priemonių, skirtų asmens duomenų apsaugai gerinti.

XIV SKYRIUS
DARBUOTOJŲ MOKYMAS, VIDAUS KONTROLĖ IR VEIKLOS GERINIMAS

111. Darbuotojams, praktikantams, savanoriams ir kitiems asmens duomenis tvarkantiems asmenims prieš suteikiant prieigą prie asmens duomenų organizuojamas pradinis supažindinimas su asmens duomenų apsaugos, konfidencialumo ir informacinio saugumo reikalavimais.
112. Periodiniai mokymai darbuotojams organizuojami ne rečiau kaip kartą per dvejus metus, taip pat pasikeitus teisės aktams, vidaus procedūroms, darbuotojo funkcijoms, įdiegus naujas sistemas arba nustačius reikšmingą ar pasikartojantį pažeidimą.
113. Centre ne rečiau kaip kartą per metus atliekamas pasirinktos asmens duomenų tvarkymo srities vidaus patikrinimas. Gali būti tikrinamas prieigų suteikimas, dokumentų saugojimas, duomenų teikimas, elektroninio pašto naudojimas, privatumo informacijos pateikimas, sutikimų administravimas, duomenų tvarkytojų veikla, duomenų saugumo pažeidimų valdymas ir ankstesnių rekomendacijų įgyvendinimas.

114. Nustačius trūkumų, parengiamas korekcinių ir prevencinių veiksmų planas, kuriame nurodomos priemonės, atsakingi asmenys ir įgyvendinimo terminai. Vėliau įvertinamas priemonių įgyvendinimas ir veiksmingumas.
113. Vertinant asmens duomenų apsaugos priemonių veiksmingumą gali būti renkamas darbuotojų, socialinių paslaugų gavėjų ir jų atstovų grįžtamasis ryšys apie privatumo, konfidencialumo, informacijos suprantamumo ir saugumo užtikrinimą. Gauti rezultatai naudojami Centro veiklai gerinti.

XV SKYRIUS
ATSAKOMYBĖ

114. Kiekvienas Centro darbuotojas, tvarkantis asmens duomenis, atsako už šiame Apraše ir kituose asmens duomenų apsaugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų laikymąsi pagal savo kompetenciją.
115. Darbuotojai privalo saugoti jiems vykdant darbo ar kitą veiklą tapusią žinomą informaciją, kurioje yra asmens duomenų, ir jos neatskleisti tretiesiems asmenims, išskyrus teisės aktuose nustatytus atvejus.
116. Pareiga saugoti asmens duomenų konfidencialumą galioja ir darbuotojui pasibaigus darbo ar kitiems teisiniams santykiams su Centru, jeigu teisės aktai nenustato kitaip.
117. Darbuotojai, pastebėję šio Aprašo reikalavimų pažeidimą, netinkamą asmens duomenų tvarkymo praktiką ar aplinkybes, galinčias kelti grėsmę asmens duomenų saugumui, privalo nedelsdami apie tai informuoti tiesioginį vadovą, duomenų apsaugos pareigūną arba Centro direktoriaus paskirtą atsakingą asmenį.
118. Centro padalinių vedėjai pagal savo kompetenciją užtikrina, kad jų vadovaujamuose padaliniuose:
118.1. asmens duomenis tvarkytų tik tokią teisę turintys darbuotojai;
118.2. darbuotojams būtų suteiktos tik jų funkcijoms būtinos prieigos;
118.3. dokumentai ir įrenginiai būtų saugomi nustatyta tvarka;
118.4. darbuotojai būtų supažindinti su šiuo Aprašu ir dalyvautų mokymuose;
118.5. būtų nedelsiant pranešama apie galimus asmens duomenų saugumo pažeidimus;
118.6. būtų įgyvendinamos po patikrinimų ar pažeidimų nustatytos korekcinės ir prevencinės priemonės.
119. Už šio Aprašo reikalavimų pažeidimus asmenys atsako Lietuvos Respublikos ir Europos Sąjungos teisės aktų nustatyta tvarka.

XVI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

120. Centro direktorius atsako už bendrą asmens duomenų apsaugos sistemos organizavimą, tinkamų žmogiškųjų, organizacinių ir techninių išteklių skyrimą, atsakingų asmenų paskyrimą, jų funkcijų nustatymą bei sprendimų dėl nustatytų rizikų valdymo priėmimą.
121. Centro darbuotojai su šiuo Aprašu supažindinami teisės aktų ir Centro vidaus dokumentų nustatyta tvarka.
122. Darbuotojai, tvarkantys asmens duomenis, privalo laikytis šio Aprašo reikalavimų vykdydami visas su asmens duomenų tvarkymu susijusias darbo funkcijas.
123. Pasikeitus Europos Sąjungos ar Lietuvos Respublikos teisės aktams, reglamentuojantiems asmens duomenų tvarkymą ir apsaugą, taikomos aktualių teisės aktų nuostatos. Prireikus šis Aprašas peržiūrimas ir atnaujinamas.
124. Šio Aprašo įgyvendinimui gali būti tvirtinami papildomi vidaus dokumentai, rekomendacijos, formos ar kitos organizacinės priemonės, jeigu jos neprieštarauja šiam Aprašui ir teisės aktams.
125. Šis Aprašas įsigalioja nuo jo patvirtinimo dienos, jeigu Centro direktoriaus įsakyme nenustatyta vėlesnė įsigaliojimo data.

Asmens duomenų tvarkymo ir asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo
1 priedas

PRANEŠIMO APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ FORMA

20_____ m. _____ d. Nr. _____

_____

(surašymo vieta)

I. INFORMACIJA APIE PAŽEIDIMĄ

1. Pažeidimo nustatymo data: _____
2. Pažeidimo nustatymo laikas: _____
3. Pažeidimą pastebėjęs darbuotojas

Vardas, pavardė _____

Pareigos _____

Telefonas / el. paštas _____

II. PAŽEIDIMO APRAŠYMAS

4. Trumpai aprašykite, kas įvyko

---

5. Kada, Jūsų žiniomis, įvyko pažeidimas?

☐ Data ir laikas žinomi

☐ Tikslus laikas nežinomas

☐ Kita _____

III. KOKIE ASMENS DUOMENYS GALĖJO BŪTI PAVEIKTI?

☐ Vardas, pavardė
☐ Asmens kodas
☐ Kontaktiniai duomenys
☐ Gyvenamosios vietos duomenys
☐ Socialinių paslaugų gavimo duomenys
☐ Sveikatos duomenys
☐ Finansiniai duomenys
☐ Darbuotojų duomenys
☐ Kita _____

IV. KOKIE ASMENYS GALĖJO BŪTI PAVEIKTI?

☐ Socialinių paslaugų gavėjai
☐ Vaikai
☐ Globėjai / budintys globotojai
☐ Darbuotojai
☐ Kandidatai į darbo vietą
☐ Paslaugų teikėjai
☐ Kita _____

Jeigu žinoma, nurodykite apytikslį asmenų skaičių: _____

V. KOKIŲ VEIKSMŲ JAU IMTASI?

☐ Sustabdytas neteisingas duomenų siuntimas
☐ Informuotas netinkamas gavėjas
☐ Dokumentai atgauti
☐ Užblokuota prieiga
☐ Informuotas tiesioginis vadovas
☐ Informuotas atsakingas asmuo
☐ Kita _____

VI. PAPILDOMA INFORMACIJA

Ar yra kitų aplinkybių, kurios gali būti svarbios vertinant pažeidimą?

VII. PRANEŠIMĄ PATEIKUSIO DARBUOTOJO PATVIRTINIMAS

Patvirtinu, kad šiame pranešime pateikiau visą man žinomą informaciją apie galimą asmens duomenų saugumo pažeidimą.

Data _____

Parašas _____

Pildo atsakingas asmuo

Pranešimo gavimo data _____

Pranešimą priėmė

(vardas, pavardė, pareigos)

Registracijos Nr. _____

Asmens duomenų tvarkymo ir asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo
2 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAS

Eil. Nr.	**Pažeidimo nustatymo data**	**Trumpas pažeidimo aprašymas**	**Paveiktų duomenų subjektų kategorijos**	**Paveiktų duomenų kategorijos**	**Rizikos vertinimas**	**Priimtas sprendimas**	**Pranešta priežiūros institucijai (taip / ne)**	**Informuoti duomenų subjektai (taip / ne)**	**Taikytos priemonės**	**Pažeidimas užbaigtas (data)**	**Pastabos**
1											
2											
3											
4											
5											

Registro pildymo paaiškinimai
Pažeidimo nustatymo data – data, kada darbuotojas pastebėjo arba Centrui tapo žinoma apie galimą pažeidimą.
Trumpas pažeidimo aprašymas – glaustai nurodomos pažeidimo aplinkybės (pvz., *„El. laiškas su paslaugų gavėjo duomenimis išsiųstas netinkamam gavėjui”*).
Paveiktų duomenų subjektų kategorijos – pavyzdžiui: socialinių paslaugų gavėjai; vaikai; globėjai; darbuotojai; kiti asmenys.
Paveiktų duomenų kategorijos – pavyzdžiui: identifikavimo duomenys; kontaktiniai duomenys; socialinių paslaugų duomenys; sveikatos duomenys; finansiniai duomenys; kita.
Rizikos vertinimas – trumpai nurodoma vertinimo išvada (pvz., *„rizika nenustatyta”, „nustatyta rizika”, „nustatyta didelė rizika“*).
Priimtas sprendimas – nurodoma, ar: pažeidimas pripažintas asmens duomenų saugumo pažeidimu; nuspręsta nepranešti priežiūros institucijai;
nuspręsta pranešti priežiūros institucijai; informuoti duomenų subjektai; atlikti kiti veiksmai.
Taikytos priemonės – trumpai nurodomos priemonės, kurių imtasi siekiant pašalinti pažeidimo pasekmes ir užkirsti kelią panašiems atvejams ateityje.

Asmens duomenų tvarkymo ir asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo
3 priedas

DARBUOTOJO VEIKSMŲ SCHEMA
KĄ DARYTI PASTEBĖJUS GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ?

PASTEBĖJOTE GALIMĄ PAŽEIDIMĄ?

▼

ĮVERTINKITE, AR GALITE NEDELSDAMI SUMAŽINTI GALIMĄ ŽALĄ

- sustabdyti el. laiško siuntimą
- susisiekti su netinkamu gavėju
- atsiimti dokumentus
- užrakinti naudotojo paskyrą
- apsaugoti dokumentus ar laikmenas

▼

NEDELSDAMI PRANEŠKITE

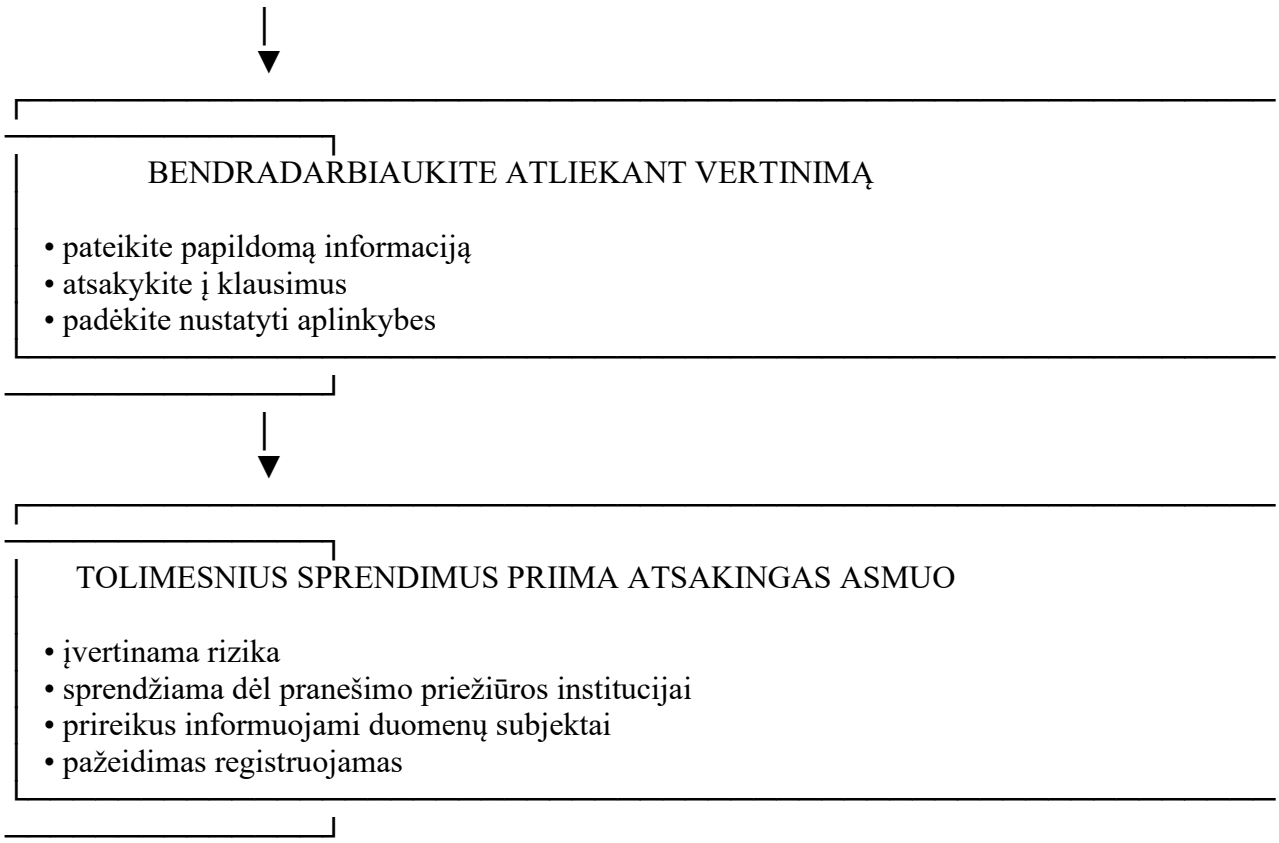
- Tiesioginiam vadovui
  arba
- Centro direktoriaus paskirtam atsakingam asmeniui

▼

PATEIKITE VISĄ TUO METU ŽINOMĄ INFORMACIJĄ

- kas įvyko
- kada pastebėta
- kokie duomenys galėjo būti paveikti
- kokių veiksmų jau ėmėtės

Jei reikia – užpildykite
Pranešimo apie galimą asmens duomenų saugumo pažeidimą formą.



ATMINKITE: jeigu abejojate – visada praneškite.

✓ Jūs neprivalote nustatyti, ar tai tikrai asmens duomenų saugumo pažeidimas.

✓ Jūsų pareiga – kuo greičiau pranešti apie galimą pažeidimą.

✓ Pranešimas apie galimą pažeidimą nėra darbuotojo kaltės pripažinimas.

✓ Laiku pranešus dažniausiai galima sumažinti arba visiškai išvengti neigiamų pasekmių.

Asmens duomenų tvarkymo ir asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo
4 priedas

DARBUOTOJO ATMINTINĖ APIE ASMENS DUOMENŲ APSAUGĄ KASDIENĖJE VEIKLOJE

RINKITE TIK TIEK DUOMENŲ, KIEK BŪTINA

✓ Tvarkykite tik tuos asmens duomenis, kurie reikalingi Jūsų darbo funkcijoms atlikti.
✓ Nesidomėkite informacija, kuri nėra susijusi su Jūsų darbu.
✓ Nenaudokite asmens duomenų kitais tikslais.

SAUGOKITE DOKUMENTUS

✓ Nepalikite bylų, dokumentų ar užrašų be priežiūros.
✓ Dokumentus laikykite tik tam skirtose vietose.
✓ Darbo dienos pabaigoje darbo vietoje neturi likti dokumentų su asmens duomenimis.
✓ Netinkamus dokumentus naikinkite nustatyta tvarka.

SAUGOKITE INFORMACINES SISTEMAS

✓ Naudokite tik savo prisijungimo duomenis.
✓ Niekam neatskleiskite slaptažodžių.
✓ Palikdami darbo vietą užrakinkite kompiuterį.
✓ Neatidarinėkite įtartinų elektroninių laiškų ar jų priedų.

SIŲSDAMI ELEKTRONINIUS LAIŠKUS

Prieš paspausdami „Siųsti", visada patikrinkite:
✓ Ar teisingai nurodytas gavėjas?
✓ Ar prisegtas tinkamas dokumentas?
✓ Ar siunčiami tik būtini asmens duomenys?
✓ Ar dokumente nėra kitų asmenų duomenų, kurių gavėjas neturi teisės matyti?

TEIKDAMI INFORMACIJĄ TELEFONU

✓ Pirmiausia įsitikinkite, kas skambina.
✓ Įvertinkite, ar asmuo turi teisę gauti informaciją.
✓ Kilus abejonėms – informacijos neteikite.
✓ Pasitarkite su vadovu arba atsakingu asmeniu.

TEIKDAMI PASLAUGAS ASMENS NAMUOSE

✓ Nepalikite dokumentų automobilyje matomoje vietoje.
✓ Dokumentus saugokite nuo pašalinių asmenų.
✓ Kalbėkite apie paslaugų gavėjus tik tiek, kiek tai būtina paslaugai suteikti.
✓ Įsitikinkite, kad dokumentų nepalikote paslaugų gavėjo namuose.

PASTEBĖJOTE GALIMĄ PAŽEIDIMĄ?

Nedelsdami:
✓ sumažinkite galimą žalą (jeigu galite);
✓ informuokite tiesioginį vadovą;

arba

✓ informuokite Centro direktoriaus paskirtą atsakingą asmenį;

✓ pateikite visą tuo metu žinomą informaciją.

PRISIMINKITE

✓ Pagalvokite prieš rinkdami ar perduodami duomenis.

✓ Saugokite dokumentus ir informacines sistemas.

✓ Kilus abejonėms – klauskite.

✓ Pastebėję galimą pažeidimą – nedelsdami praneškite.

AUKSINĖ TAISYKLĖ

Jeigu kyla bent menkiausia abejonė, ar galite tvarkyti arba atskleisti asmens duomenis – sustokite ir pasitarkite su tiesioginiu vadovu arba Centro direktoriaus paskirtu atsakingu asmeniu.

Asmens duomenų tvarkymo ir asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo
5 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO RIZIKOS VERTINIMO FORMA

20____ m. _____ d. Nr. _____

I. BENDROJI INFORMACIJA APIE ĮVYKĮ

1. Pažeidimo registracijos numeris:

_____

2. Data ir laikas, kada Centrui tapo žinoma apie galimą pažeidimą:

_____

3. Data ir laikas, kada, tikėtina, įvyko pažeidimas:

_____

☐ Tikslus laikas žinomas
☐ Tikslus laikas nežinomas
☐ Pažeidimas tęsiasi
☐ Pažeidimas sustabdytas

4. Pažeidimą pastebėjęs arba apie jį pranešęs asmuo:

Vardas, pavardė _____

Pareigos _____

Kontaktiniai duomenys _____

5. Pažeidimą vertinantis asmuo / vertinimo grupė:

_____
_____

6. Trumpas įvykio aprašymas:

_____
_____
_____

II. PAŽEIDIMO POBŪDIS

7. Kokio pobūdžio asmens duomenų saugumo pažeidimas įvyko arba galėjo įvykti?

☐ **Konfidencialumo pažeidimas** – asmens duomenys buvo neteisėtai arba netyčia atskleisti, perduoti ar tapo prieinami teisės juos gauti neturintiems asmenims.

☐ **Vientisumo pažeidimas** – asmens duomenys buvo neteisėtai arba netyčia pakeisti, sugadinti, papildyti ar kitaip iškraipyti.

☐ **Prieinamumo pažeidimas** – asmens duomenys buvo prarasti, sunaikinti arba laikinai ar nuolat tapo neprieinami.

☐ Įvyko kelių rūšių pažeidimas.

☐ Atlikus pirminį vertinimą nustatyta, kad įvykis nelaikytinas asmens duomenų saugumo pažeidimu.

8. Pažeidimo būdas ar aplinkybės:

☐ Duomenys išsiųsti netinkamam gavėjui
☐ Dokumentai perduoti netinkamam asmeniui
☐ Pamesti arba pavogti dokumentai
☐ Pamestas arba pavogtas įrenginys ar laikmena
☐ Neteisėta prieiga prie informacinės sistemos
☐ Panaudoti kito darbuotojo prisijungimo duomenys
☐ Duomenys paskelbti interneto svetainėje ar socialiniame tinkle
☐ Nepakankamai nuasmenintas dokumentas
☐ Netinkamai sunaikinti dokumentai ar laikmenos
☐ Kibernetinis incidentas
☐ Informacinės sistemos veiklos sutrikimas
☐ Žmogiškoji klaida
☐ Tyčinis asmens veiksmas
☐ Kita:

III. PAVEIKTI DUOMENŲ SUBJEKTAI

9. Kokios duomenų subjektų kategorijos paveiktos arba galėjo būti paveiktos?

☐ Socialinių paslaugų gavėjai
☐ Vaikai
☐ Asmenys su negalia
☐ Senyvo amžiaus asmenys
☐ Socialinę riziką patiriantys asmenys
☐ Smurtą ar krizę patiriantys asmenys
☐ Globėjai, budintys globotojai, įtėviai ar šeimynų dalyviai
☐ Socialinių paslaugų gavėjų šeimos nariai ar atstovai
☐ Darbuotojai
☐ Pretendentai į pareigas
☐ Praktikantai ar savanoriai

☐ Paslaugų teikėjai ar sutarčių šalys
☐ Kiti asmenys:

---

10. Apytikslis paveiktų duomenų subjektų skaičius:

☐ 1 asmuo
☐ 2–10 asmenų
☐ 11–50 asmenų
☐ 51–100 asmenų
☐ Daugiau kaip 100 asmenų
☐ Tikslus ar apytikslis skaičius kol kas nežinomas

Nurodykite žinomą ar apytikslį skaičių: _____

11. Ar tarp paveiktų asmenų yra pažeidžiamų duomenų subjektų?

☐ Ne
☐ Taip
☐ Nežinoma

Jeigu taip, nurodykite:

---

12. Pažeidžiamumą didinančios aplinkybės:

☐ Nepilnametystė
☐ Negalia
☐ Sveikatos būklė
☐ Priklausomybė nuo kitų asmenų pagalbos
☐ Socialinė rizika
☐ Patiriamas smurtas ar krizė
☐ Finansinis ar socialinis pažeidžiamumas
☐ Asmens ribotos galimybės suprasti pažeidimo pasekmes ar savarankiškai apsisaugoti
☐ Kita:

IV. PAVEIKTI ASMENS DUOMENYS

13. Kokios asmens duomenų kategorijos paveiktos arba galėjo būti paveiktos?

☐ Vardas, pavardė
☐ Asmens kodas
☐ Gimimo data
☐ Kontaktiniai duomenys

☐ Gyvenamosios vietos duomenys
☐ Šeimos sudėties ir šeiminių ryšių duomenys
☐ Socialinių paslaugų gavimo duomenys
☐ Socialinės situacijos duomenys
☐ Sveikatos duomenys
☐ Duomenys apie negalią
☐ Duomenys apie priklausomybę
☐ Duomenys apie smurtą, krizę ar socialinę riziką
☐ Finansiniai duomenys
☐ Banko sąskaitos duomenys
☐ Darbo užmokesčio duomenys
☐ Darbuotojų duomenys
☐ Prisijungimo duomenys ar slaptažodžiai
☐ Atvaizdas
☐ Vaizdo ar garso įrašas
☐ Parašas
☐ Dokumentų kopijos
☐ Kita:

---

14. Apytikslis paveiktų asmens duomenų įrašų skaičius:

☐ 1 įrašas
☐ 2–10 įrašų
☐ 11–50 įrašų
☐ 51–100 įrašų
☐ Daugiau kaip 100 įrašų
☐ Skaičius nežinomas

15. Duomenų jautrumo vertinimas:

☐ Nedidelio jautrumo duomenys
☐ Vidutinio jautrumo duomenys
☐ Didelio jautrumo duomenys
☐ Specialių kategorijų asmens duomenys
☐ Duomenys, kurių atskleidimas gali sukelti stigmatizaciją, diskriminaciją, smurtą, reputacijos ar kitą reikšmingą žalą

Vertinimo paaiškinimas:

---

16. Ar pagal paveiktus duomenis galima nustatyti asmens tapatybę?

☐ Taip, tiesiogiai
☐ Taip, susiejus su kita informacija
☐ Tik ribotomis aplinkybėmis
☐ Ne
☐ Nežinoma

V. DUOMENŲ APSAUGOS PRIEMONĖS IR NETEISĖTAS GAVĖJAS

17. Ar duomenys pažeidimo metu buvo apsaugoti?

☐ Duomenys buvo užšifruoti
☐ Dokumentas buvo apsaugotas slaptažodžiu
☐ Duomenims buvo suteikti pseudonimai
☐ Įrenginys buvo apsaugotas slaptažodžiu ar kita autentifikavimo priemone
☐ Duomenys buvo atsarginėje kopijoje
☐ Duomenys nebuvo papildomai apsaugoti
☐ Nežinoma
☐ Kita:

---

18. Kam asmens duomenys buvo arba galėjo būti neteisėtai atskleisti?

☐ Vienam žinomam fiziniam asmeniui
☐ Keliems žinomiems asmenims
☐ Kitai įstaigai ar organizacijai
☐ Neapibrėžtam asmenų ratui
☐ Duomenys paskelbti viešai
☐ Galimas gavėjas nežinomas
☐ Duomenys nebuvo atskleisti, tačiau tapo neprieinami ar buvo pakeisti
☐ Kita:

---

19. Ar neteisėtas gavėjas yra patikimas ir bendradarbiauja?

☐ Taip, patvirtino, kad duomenų nenaudojo, neperdavė ir ištrynė
☐ Taip, tačiau nėra galimybės patikrinti, ar duomenys sunaikinti
☐ Ne, gavėjas nebendradarbiauja
☐ Gavėjas nežinomas
☐ Netaikoma

Turimi patvirtinimai arba papildoma informacija:

VI. GALIMOS PASEKMĖS DUOMENŲ SUBJEKTAMS

20. Kokios galimos pažeidimo pasekmės?

☐ Duomenų subjektui reikšmingų pasekmių neturėtų kilti
☐ Privatumo praradimas
☐ Konfidencialios informacijos atskleidimas
☐ Diskriminacija
☐ Stigmatizacija
☐ Reputacijos pablogėjimas
☐ Tapatybės vagystė ar sukčiavimas
☐ Finansiniai nuostoliai
☐ Galimybės naudotis paslauga ar savo teisėmis apribojimas
☐ Fizinė žala ar grėsmė asmens saugumui
☐ Psichologinė ar emocinė žala
☐ Konfliktas šeimoje ar artimoje aplinkoje
☐ Smurto, persekiojimo ar spaudimo rizika
☐ Profesinės ar kitokios paslapties atskleidimas
☐ Kontrolės savo asmens duomenų atžvilgiu praradimas
☐ Kita:

---

21. Galimų pasekmių sunkumas:

☐ Nedidelis
☐ Vidutinis
☐ Didelis
☐ Labai didelis

Pagrindimas:

---

22. Tikimybė, kad pasekmės pasireikš:

☐ Maža
☐ Vidutinė
☐ Didelė
☐ Labai didelė

Pagrindimas:

VII. PRIEMONĖS, KURIŲ IMTASI

23. Kokių neatidėliotinų veiksmų imtasi pažeidimui sustabdyti ir žalai sumažinti?

☐ Sustabdytas duomenų siuntimas
☐ Susisiekta su netinkamu gavėju
☐ Paprašyta duomenis ištrinti arba grąžinti
☐ Gautas patvirtinimas apie duomenų ištrynimą
☐ Dokumentai arba laikmenos susigrąžinti
☐ Pakeisti slaptažodžiai
☐ Užblokuota naudotojo paskyra ar prieiga
☐ Atjungtas arba apsaugotas įrenginys
☐ Pašalinta viešai paskelbta informacija
☐ Atkurti prarasti ar sunaikinti duomenys
☐ Informuotas Centro direktorius
☐ Informuotas duomenų apsaugos pareigūnas
☐ Informuotas informacinių technologijų priežiūros paslaugų teikėjas
☐ Informuota kita atsakinga institucija ar organizacija
☐ Kita:

---

24. Priemonių atlikimo data, laikas ir atsakingi asmenys:

---

25. Ar atlikti veiksmai pašalino arba reikšmingai sumažino pavojų?

☐ Taip, pavojus pašalintas
☐ Taip, pavojus reikšmingai sumažintas
☐ Pavojus sumažintas tik iš dalies
☐ Ne
☐ Dar vertinama

Paaiškinimas:

VIII. BENDRAS RIZIKOS ĮVERTINIMAS

26. Atsižvelgiant į galimų pasekmių sunkumą ir jų atsiradimo tikimybę, nustatomas toks rizikos lygis:

Galimų pasekmių sunkumas	Maža tikimybė	Vidutinė tikimybė	Didelė arba labai didelė tikimybė
Nedidelis	Maža rizika	Maža rizika	Vidutinė rizika
Vidutinis	Maža rizika	Vidutinė rizika	Didelė rizika
Didelis	Vidutinė rizika	Didelė rizika	Didelė rizika
Labai didelis	Didelė rizika	Didelė rizika	Didelė rizika

27. Galutinė vertinimo išvada:

☐ **Rizika nenustatyta.** Mažai tikėtina, kad pažeidimas sukels pavojų fizinių asmenų teisėms ir laisvėms.

☐ **Nustatyta rizika.** Dėl pažeidimo gali kilti pavojus fizinių asmenų teisėms ir laisvėms.

☐ **Nustatyta didelė rizika.** Dėl pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms.

☐ Įvykis nepripažintas asmens duomenų saugumo pažeidimu.

28. Galutinės išvados pagrindimas:

IX. SPRENDIMAI DĖL PRANEŠIMŲ

29. Sprendimas dėl pranešimo Valstybinei duomenų apsaugos inspekcijai:

☐ Pranešti, nes nustatyta rizika duomenų subjektų teisėms ir laisvėms
☐ Nepranešti, nes mažai tikėtina, kad pažeidimas sukels pavojų
☐ Informacija dar renkama, sprendimas bus priimtas papildomai
☐ Netaikoma, nes įvykis nepripažintas asmens duomenų saugumo pažeidimu

Sprendimo motyvai:

---

30. Pranešimo Valstybinei duomenų apsaugos inspekcijai pateikimo terminas:

Sužinojimo apie pažeidimą data ir laikas _____

72 valandų termino pabaiga _____

Pranešimas pateiktas _____

Pranešimo registracijos ar patvirtinimo duomenys _____

Jeigu pranešta praėjus daugiau kaip 72 valandoms, nurodomos vėlavimo priežastys:

---

31. Sprendimas dėl duomenų subjektų informavimo:

☐ Informuoti, nes nustatyta didelė rizika
☐ Neinformuoti, nes didelė rizika nenustatyta
☐ Neinformuoti, nes pritaikytos priemonės, dėl kurių rizika nebegali pasireikšti
☐ Neinformuoti dėl kitų teisės aktuose nustatytų priežasčių
☐ Informacija dar renkama, sprendimas bus priimtas papildomai

Sprendimo motyvai:

---

32. Jeigu duomenų subjektai informuojami, nurodoma:

Informavimo data _____

Informavimo būdas _____

Informuotų asmenų skaičius _____

Už informavimą atsakingas asmuo _____

X. KOREKCINĖS IR PREVENCINĖS PRIEMONĖS

33. Nustatytos arba tikėtinos pažeidimo priežastys:

☐ Darbuotojo neatidumas
☐ Nepakankamos darbuotojo žinios
☐ Neaiški vidaus procedūra
☐ Nepakankama prieigų kontrolė
☐ Techninės apsaugos priemonių trūkumas
☐ Informacinės sistemos sutrikimas
☐ Paslaugų teikėjo ar duomenų tvarkytojo veiksmai
☐ Nepakankama dokumentų ar įrenginių apsauga
☐ Tyčiniai neteisėti veiksmai
☐ Kita:

---

34. Numatomos korekcinės ir prevencinės priemonės:

Eil. Nr.	Priemonė	Atsakingas asmuo	Įgyvendinimo terminas	Įvykdymo data ir rezultatas
1.				
2.				
3.				
4.				

35. Ar būtina papildomai:

☐ Atnaujinti vidaus dokumentus
☐ Patikslinti darbuotojų funkcijas
☐ Organizuoti darbuotojų mokymus
☐ Peržiūrėti suteiktas prieigas
☐ Įdiegti papildomas techninės saugumo priemones
☐ Peržiūrėti sutartį su duomenų tvarkytoju
☐ Atlikti poveikio duomenų apsaugai vertinimą
☐ Atlikti vidaus patikrinimą
☐ Kita:

XI. VERTINIMO PATVIRTINIMAS

36. Rizikos vertinimą atliko:

Vardas, pavardė _____

Pareigos _____

Data _____

Parašas _____

37. Duomenų apsaugos pareigūno išvada:

☐ Pritariu atliktam vertinimui ir siūlomiems sprendimams
☐ Pritariu iš dalies
☐ Nepritariu
☐ Duomenų apsaugos pareigūno išvada netaikoma

Pastabos ir rekomendacijos:

Vardas, pavardė _____

Data _____ Parašas _____

38. Centro direktoriaus sprendimas:

☐ Pritarti rizikos vertinimo išvadai
☐ Pavesti surinkti papildomą informaciją
☐ Pranešti Valstybinei duomenų apsaugos inspekcijai
☐ Informuoti duomenų subjektus
☐ Patvirtinti korekcines ir prevencines priemones
☐ Kitas sprendimas:

Centro direktorius

(vardas, pavardė)

(parašas)

(data)