

PATVIRTINTA
Sveikatos apsaugos ministerijos
Ekstremalių sveikatai situacijų centro
direktoriaus 2025 m. birželio d.
įsakymu Nr.

ASMENS DUOMENŲ TVARKYMO SVEIKATOS APSAUGOS MINISTERIJOS EKSTREMALIŲ SVEIKATAI SITUACIJŲ CENTRE TAISYKLĖS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Asmens duomenų tvarkymo Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro taisyklių (toliau – Taisyklės) tikslas – reglamentuoti asmens duomenų tvarkymą Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centre (toliau – Centras), nustatyti pagrindines asmens duomenų tvarkymo, duomenų subjekto teisių įgyvendinimo ir duomenų apsaugos technines bei organizacines priemones, poveikio duomenų apsaugai vertinimo, asmens duomenų saugumo pažeidimų valdymo priemones, siekiant užtikrinti 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) (OL 2016 L 119, p. 1) (toliau – Reglamentas (ES) 2016/679), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo bei kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir apsaugą, laikymąsi ir įgyvendinimą.

2. Taisyklės privalomos visiems Centro darbuotojams, dirbantiems pagal darbo sutartis ir valstybės tarnautojams (toliau – Darbuotojai), kurie tvarko asmens duomenis.

3. Taisyklėse nurodytų asmens duomenų valdytojas yra Centras, kuris užtikrina, kad asmens duomenys Centre būtų tvarkomi laikantis Reglamente (ES) 2016/679, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir kituose teisės aktuose nustatytų reikalavimų. Taisyklėse nurodytus asmens duomenis teisės aktų nustatytais atvejais ir tvarka gali tvarkyti ir kiti subjektai (asmens duomenų valdytojai ir tvarkytojai).

4. Centras, kaip asmens duomenų valdytojas, atlikdamas teisės aktuose nustatytas funkcijas, turi teisę gauti iš kitų valstybės ir savivaldybių institucijų, įstaigų, organizacijų ir trečiųjų asmenų informaciją Centro kompetencijai priskirtais klausimais ir teisės aktų nustatyta tvarka tvarkyti asmens duomenis.

5. Šiose Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679 ir Lietuvos Respublikos teisės aktuose. Taisyklėse nustatytos nuostatos atitinka Reglamento (ES) 2016/679 24, 25, 32 ir kitų straipsnių reikalavimus, atsižvelgiant į riziką ir tvarkomų duomenų pobūdį.

II SKYRIUS ASMENS DUOMENŲ SAMPRATA

6. Asmens duomenys suprantami kaip bet kokia informacija, tiek tiesiogiai, tiek netiesiogiai identifikuojanti arba galinti identifikuoti bet kokią gyvą fizinį asmenį (toliau – duomenų subjektą).

7. Asmens duomenys gali būti išreikšti raidėmis, skaičiais, grafiniu, fotografiniu vaizdu, vaizdo ir garso įrašu bei kitomis formomis.

8. Asmens duomenimis gali būti rašytinė informacija, taip pat kompiuterio, kito įrenginio atmintyje, informacinėje sistemoje ar bet kokioje laikmenoje saugoma (tvarkoma) informacija apie duomenų subjektą.

9. Asmens tapatybė gali būti nustatyta tiesiogiai iš atitinkamos informacijos (pvz. vardas ir pavardė, asmens kodas) arba netiesiogiai identifikuojama iš turimos informacijos kartu su kita informacija, t. y. skirtinga informacija, kuri surinkta kartu, gali atskleisti konkretaus asmens tapatybę.

10. Nėra baigtinio asmens duomenų sąrašo. Asmens duomenimis laikytini: vardas, pavardė, asmens kodas, gyvenamosios vietos (korespondencijos) adresas, telefono ryšio numeris, elektroninio pašto adresas, banko sąskaitos numeris, išsilavinimo duomenys, diplomų ir sertifikatų duomenys, darbovietė, pajamos ir darbo užmokestis, darbo sąlygos, duomenys apie turtą, išlaidas, skolas, duomenys apie sveikatą (sveikatos būklė, kraujo grupė ir kt.), vaizdo duomenys, biometriniai duomenys (pvz. piršto antspaudas, veido šablonas), šeimos narių duomenys (jei jie siejami su duomenų subjektu), pomėgiai, buvimo vietos ir (ar) judėjimo duomenys, komunikacijos, elgesio duomenys, interneto protokolo (IP) adresas, interneto naršymo duomenys, informacija apie elgseną internete ir kt.

11. Asmens duomenimis nėra laikoma:

11.1. informacija apie juridinį asmenį atskirai nuo jo savininkų, vadovų, valdymo organų narių, darbuotojų informacijos;

11.2. informacija apie valdžios institucijas, įstaigas, organizacijas;

11.3. informacija apie mirusį asmenį (išskyrus, jeigu tai vienaip ar kitaip susiję / gali būti susiję su gyvais fiziniais asmenimis, pvz., paveldėtojų duomenys);

11.4. anoniminė informacija, kuomet anonimiškumas užtikrinamas taip, kad asmens tapatybė negali arba nebegali būti nustatyta (anonimiškumas yra galutinis ir negrįžtamas, t. y. objektyviai panaikinant bet kokias sąsajas su asmens tapatybę identifikuojančiais duomenimis, kuomet Centras praranda realią ir objektyvią galimybę disponuojamuose informacijos šaltiniuose nustatyti konkretų asmenį), įskaitant duomenų tvarkymą statistiniais ar tyrimų tikslais.

III SKYRIUS

ASMENS DUOMENŲ TVARKYMAS

12. Centre asmens duomenys tvarkomi automatinio būdu ir (arba) neautomatinio būdu susistemintose rinkmenose.

13. Asmens duomenys Centre renkami / gaunami iš duomenų subjektų ir (ar) jų atstovų, fizinių ar juridinių asmenų, besikreipiančių į Centrą su pranešimais, prašymais, reikalavimais, skundais ar kitais pagrindais, Centro valdomų vidinių informacinių sistemų, duomenų tvarkytojų ir duomenų teikėjų, išorinių registų ir informacinių sistemų, juridinių ir fizinių asmenų, su kuriais Centras yra pasirašęs paslaugų teikimo, bendradarbiavimo ar kitokio pobūdžio sutartis, juridinių ir fizinių asmenų, kurie Centrai pateikia asmens duomenis, reikalingus Centro funkcijoms ir teisės aktų nustatytais prievolėms vykdyti, taip pat viešai prieinamų šaltinių (atvirų duomenų).

14. Centras asmens duomenis tikslina, naudoja ir atnauja savo arba duomenų subjekto iniciatyva. Savo iniciatyva Centras turi teisę tikslinti, taisyti ir atnaujinti asmens duomenis tada, kai gaunama informacija apie pasikeitusius asmens duomenis. Duomenų subjekto prašymai dėl asmens duomenų patikslinimo, ištaisymo ar atnaujinimo nagrinėjami Centro duomenų subjektų teisių įgyvendinimo aprašo nustatyta tvarka.

15. Apie atliktą asmens duomenų ištaisymą, ištyrinimą arba tvarkymo apribojimą, vykdumą pagal Reglamento (ES) 2016/679 16 straipsnį, 17 straipsnio 1 dalį, 18 straipsnį, Centras teisės aktų nustatytais terminais, o jei tokie terminai nenustatyti – per 20 darbo dienų nuo šių veiksmų atlikimo dienos, praneša Centro direktorius arba jo įgaliotas asmuo apie tai duomenų subjektams, nebent to padaryti būtų neįmanoma arba tai pareikalautų neproporcingų sąnaudų.

16. Už asmens duomenų taisymą, tikslinimą, atnaujinimą yra atsakingi Centro Darbuotojai, tvarkantys asmens duomenis.

17. Asmens duomenys Centro nustatytais duomenų tvarkymo tikslais konkrečiu atveju tvarkomi tik tiek, kiek yra būtina tam tikslui pasiekti (duomenų minimizavimas).

IV SKYRIUS

ASMENS DUOMENŲ TVARKYMO PRINCIPAI

18. Centro Darbuotojai, tvarkantys Centro, kaip duomenų valdytojo, surinktus asmens duomenis, privalo laikytis šių principų:

18.1. teisėtumo, sąžiningumo ir skaidrumo principo, t. y. asmens duomenis duomenų subjekto atžvilgiu tvarkyti teisėtu, sąžiningu ir skaidriu būdu;

18.2. tikslo apribojimo principo, t. y. asmens duomenis tvarkyti tik Centro nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkyti jų su tais tikslais nesuderinamu būdu. Tolesnis asmens duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais nėra laikomas nesuderinamas su pirminiais tikslais. Kitu, nei pirminiu tikslu, asmens duomenis galima tvarkyti, jei tam yra teisėtas pagrindas. Tvarkymo mastas neturi viršyti būtino siekiant nustatyto tikslo.

18.3. duomenų kiekio mažinimo principo, t. y. tvarkyti adekvačius, proporcingus ir tinkamus asmens duomenis, kurių būtent turinio, formos ir apimties prasme reikia Centro duomenų tvarkymo tikslų įgyvendinimui;

18.4. tikslumo principo, t. y. tvarkyti tik tikslus (aktuales) asmens duomenis ir prireikus juos atnaujinti (įtaisyti) arba nedelsiant ištrinti;

18.5. saugojimo trukmės apribojimo principo, t. y. asmens duomenis tvarkyti tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau nei tai yra būtina tais duomenų tvarkymo tikslais, kuriais asmens duomenys yra tvarkomi. Pasiekus asmens duomenų tvarkymo tikslą, asmens duomenys turi būti nedelsiant ištrinti (sunaikinti) arba nuasmeninti. Asmens duomenys gali būti saugomi ilgesnį laikotarpį, jeigu tam yra teisėtas tikslas bei pagrindas ir tik tiek, kiek reikia naujam tikslui pasiekti.

18.6. vientisumo ir konfidencialumo principo, t. y. tvarkyti asmens duomenis tokiu būdu, kad taikant atitinkamas organizacines ir technines saugumo priemones būtų užtikrintas pakankamas asmens duomenų saugumas, įskaitant apsaugą nuo asmens duomenų tvarkymo be leidimo arba neteisėto asmens duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo. Prieiga prie asmens duomenų Centro nustatyta tvarka gali būti suteikiama tik tiems asmenims, kuriems asmens duomenys yra reikalingi jų funkcijoms vykdyti („būtina žinoti“ / „būtina darbui“);

18.7. atskaitomybės principo, t. y. tvarkyti asmens duomenis taip, kad Centras galėtų aiškiai, lengvai ir pagrįstai įrodyti, jog laikomasi asmens duomenų apsaugos principų ir reikalavimų. Darbuotojai, tvarkantys asmens duomenis, yra atsakingi už asmens duomenų apsaugos principų ir reikalavimų laikymąsi;

18.8. pritaikytosios duomenų apsaugos principo, t. y. atsižvelgiant į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus duomenų subjektams, tiek nustatant duomenų tvarkymo priemones, tiek paties duomenų tvarkymo metu, įgyvendinti (taikyti) tinkamas technines ir organizacines priemones (pvz., šifravimą, pseudonimų suteikimą), kuriomis siekiama veiksmingai įgyvendinti duomenų apsaugos principus (pvz., duomenų kiekio mažinimo principą) ir į duomenų tvarkymą integruoti būtinas apsaugos priemones, kad jis atitiktų Reglamento (ES) 2016/679 reikalavimus ir apsaugotų duomenų subjektų teises bei teisėtus interesus;

18.9. standartizuotos duomenų apsaugos principo, t. y. įgyvendinti tinkamas technines ir organizacines priemones, kuriomis užtikrinama, kad standartizuotai būtų tvarkomi tik tie asmens duomenys, kurie yra būtini kiekvienam konkrečiam duomenų tikslui pasiekti. Ta prievolė taikoma surinktų asmens duomenų kiekiui, jų tvarkymo apimčiai, jų saugojimo laikotarpiui ir jų prieinamumui. Visų pirma, tokiomis priemonėmis užtikrinama, kad standartizuotai, be fizinio asmens įsikišimo, su asmens duomenimis negalėtų susipažinti neribotas fizinių asmenų skaičius.

V SKYRIUS

ASMENS DUOMENŲ TVARKYMO TIKSLAI IR PAGRINDAI

19. Centro konkretūs asmens duomenų tvarkymo tikslai, teisiniai pagrindai, tvarkomų asmens duomenų kategorijos, jų apimtis ir kitos duomenų tvarkymo sąlygos yra numatytos Centro duomenų tvarkymo veiklos įrašuose, taip pat Centrai vykdamas Reglamento (ES) 2016/679 13 ir 14 straipsniuose nustatytą prievolę informuoti duomenų subjektus apie asmens duomenų tvarkymą, parengtuose informaciniuose pranešimuose, stenduose, lentelėse, skirtuose tikslinei duomenų subjektų grupei ir (ar) asmens duomenų tvarkymo operacijai arba operacijoms.

20. Centre asmens duomenys tvarkomi remiantis Reglamento (ES) 2016/679 6 straipsnio 1 dalyje, o specialiųjų kategorijų asmens duomenys – ir laikantis Reglamento (ES) 2016/679 9 straipsnio 2 dalyje nurodytų asmens duomenų teisėtų duomenų tvarkymo sąlygų (teisinių pagrindų). Kiti teisės aktai gali numatyti papildomas ir (ar) specialias asmens duomenų tvarkymo sąlygas.

21. Jeigu Centre siekiama pradėti tvarkyti asmens duomenis Centro teisėto intereso pagrindu (Reglamento (ES) 2016/679 6 straipsnio 1 dalies f punktas), Centro direktoriaus įgaliotas asmuo, kuris atsakingas už naujai pradedamų tvarkyti duomenų įgyvendinimą, privalo užpildyti teisėto intereso vertinimo (balanso) testą (1 priedas). Duomenų apsaugos pareigūnas teikia konsultacijas, atliekant ir įforminant teisėto intereso vertinimą.

VI SKYRIUS

DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

22. Centro vykdoma asmens duomenų tvarkymo veikla privalo aiškiai atitikti duomenų tvarkymo veiklos įrašuose nurodytą veiklą, tvarkomi tik duomenų tvarkymo veiklos įrašuose nurodyti asmens duomenys ir tik nurodytu tikslu bei teisiniu pagrindu.

23. Veiklos įrašus rengia Centro direktoriaus įsakymu paskirti Darbuotojai, bendradarbiaudami kartu su Centro duomenų apsaugos pareigūnu.

24. Duomenų tvarkymo veiklos įrašai turi būti teisingi, aktualūs ir išsamūs, tiksliai atspindėti Centro realiai vykdomą duomenų tvarkymą.

25. Duomenų tvarkymo veiklos įrašai tvarkomi raštu, įskaitant elektroninėmis priemonėmis.

26. Duomenų tvarkymo veiklos įrašė pateikiama Reglamento (ES) 2016/679 30 straipsnio 1 dalyje nurodyta informacija, kurioje aprašoma Centro, kaip duomenų valdytojo veikla.

27. Duomenų tvarkymo veiklos įrašų forma pateikiama Taisyklių 2 priede.

28. Jeigu Centro veiklos įrašas neatitinka Centro realaus asmens duomenų tvarkymo poreikio, veiklos įrašas nedelsiant patikslinamas arba parengiamas naujas veiklos įrašas. Apie veiklos įrašo neatitikimus bei patikslinimą ar naujo veiklos įrašo parengimą informuojamas duomenų apsaugos pareigūnas.

29. Duomenų apsaugos pareigūnas patikrina, ar veiklos įrašė pateikta visa Taisyklių 26 punkte nurodyta informacija, ir Centro Darbuotojo pateiktą veiklos įrašą leidžia laikyti tinkamu arba rekomenduoja veiklos įrašą patikslinti.

30. Duomenų apsaugos pareigūnas tvarko duomenų tvarkymo veiklos įrašų registracijos žurnalą (3 priedas).

31. Duomenų tvarkymo veiklos įrašai viešai neskelbiami ir teikiami tik Valstybinei duomenų apsaugos inspekcijai šios prašymu.

32. Centre ne rečiau nei kartą per metus tikrinama, ar Centre vykdoma asmens duomenų tvarkymo veikla atitinka duomenų tvarkymo veiklos įrašus. Už šias patikras yra atsakingas duomenų apsaugos pareigūnas. Atliekant patikrą tikrinamos ne mažiau kaip trys duomenų tvarkymo veiklos. Duomenų apsaugos pareigūno atliktos patikros rezultatai įforminami išvada, kurioje nurodoma, ar Centro vykdoma asmens duomenų tvarkymo veikla atitinka duomenų tvarkymo veiklos įrašus, nurodomi trūkumai, jeigu tokių nustatoma, ir pateikiamos rekomendacijos, kaip juos ištaisyti. Patikros išvada teikiama Centro direktoriui susipažinti.

VII SKYRIUS

DUOMENŲ APSAUGOS PAREIGŪNO PASKYRIMAS IR FUNKCIJOS

33. Pagal Reglamento (ES) 2016/679 37 straipsnį Centre paskiriamas duomenų apsaugos pareigūnas, kuris gali būti Centro Darbuotojas arba trečioji šalis, teikianti Centrui duomenų apsaugos pareigūno paslaugas pagal paslaugų teikimo sutartį. Pareigūno funkcijos apima konsultacijas Darbuotojams, pagalbą atliekant vertinimus, duomenų subjektų užklausų koordinavimą bei bendradarbiavimą su priežiūros institucijomis, kaip numatyta Reglamento (ES) 2016/679 39 straipsnyje.

34. Duomenų apsaugos pareigūnas skiriamas (samdomas), atsižvelgiant į profesinę kompetenciją, įgytas duomenų apsaugos teisės ir praktikos ekspertines žinias, taip pat gebėjimą atlikti jam pavestas funkcijas.

35. Apie duomenų apsaugos pareigūno paskyrimą Centras raštu praneša Valstybinei duomenų apsaugos inspekcijai.

36. Centras užtikrina, kad duomenų apsaugos pareigūnas būtų tinkamai ir laiku įtraukiamas į visų, su asmens duomenų apsauga susijusių klausimų nagrinėjimą.

37. Duomenų apsaugos pareigūno nuomonę (konsultaciją) būtina gauti raštu (pvz. el. paštu ar dokumentų valdymo sistemos dokumentu). Jeigu priimant sprendimus, susijusius su asmens duomenų tvarkymu, į duomenų apsaugos pareigūno nuomonę visiškai ar iš dalies neatsižvelgiama, neatsižvelgimo motyvai išdėstomi raštu.

38. Centras padeda duomenų apsaugos pareigūnui atlikti jam pavestas funkcijas, suteikdama toms funkcijoms atlikti būtinus išteklius, taip pat suteikdama galimybę susipažinti su asmens duomenimis, stebėti duomenų tvarkymo operacijas ir išlaikyti bei gerinti savo ekspertines žinias.

39. Duomenų apsaugos pareigūnas negali patirti neigiamų pasekmių dėl pavestų funkcijų objektyvaus vykdymo. Duomenų apsaugos pareigūnas tiesiogiai atsiskaito Centro direktoriui.

40. Duomenų subjektai gali kreiptis į duomenų apsaugos pareigūną visais klausimais, susijusiais su asmens duomenų tvarkymu ir naudojimusi savo teisėmis pagal Reglamentą (ES) 2016/679.

41. Duomenų apsaugos pareigūnas privalo užtikrinti konfidencialumą, susijusį su jo funkcijų vykdymu.

42. Duomenų apsaugos pareigūnas atlieka Reglamento (ES) 2016/679 39 straipsnyje numatytas funkcijas, o būtent, informuoja Centrą ir jo Darbuotojus, tvarkančius asmens

duomenis, apie prievoles pagal Reglamentą (ES) 2016/679 ir kitus teisės aktus, konsultuoja su tuo susijusiais klausimais, taip pat stebi, kaip laikomasi Reglamento (ES) 2016/679 ir kituose teisės aktuose nustatytų reikalavimų, įskaitant pareigų pavidimą, užtikrina duomenų tvarkymo operacijose dalyvaujančių asmenų informuotumo didinimą bei mokymą, švietimą, atlieka auditus, patikrinimus, taip pat konsultuoja dėl poveikio duomenų apsaugai vertinimo, bendradarbiauja su Valstybine duomenų apsaugos inspekcija, atlieka kontaktinio asmens tarp Centro ir Valstybinės duomenų apsaugos inspekcijos vaidmenį ir prireikus konsultuoja visais kitais klausimais, be to, atlikdamas šias funkcijas, tinkamai įvertina su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus.

43. Duomenų apsaugos pareigūnas gali vykdyti ir kitas funkcijas bei pareigas, tačiau Centras užtikrina, kad dėl tokių funkcijų ir pareigų nekiltų interesų konfliktas (pvz., duomenų apsaugos pareigūnas negali nustatyti Centro duomenų tvarkymo tikslų, susijusių su veiklos procesais) bei duomenų apsaugos pareigūnas turėtų pakankamus išteklius (pvz., laiko resursus) vykdyti tiesiogines funkcijas ir kelti ekspertinių žinių lygį.

44. Duomenų apsaugos pareigūno kontaktai skelbiami viešai Centro interneto svetainėje <https://essc.lrv.lt/lt/>, taip pat nurodomi privatumo pranešimuose, raštuose, susijusiuose su asmens duomenų tvarkymo klausimais.

45. Duomenų apsaugos pareigūnas bendradarbiauja su Centro Darbuotojais ir gauna iš jų jam pavestų funkcijų atlikimui reikalingą informaciją, susijusią su asmens duomenų tvarkymu (pvz., informaciją, reikalingą įvertinti atitiktį).

46. Duomenų apsaugos pareigūnas asmeniškai arba kartu su kitais Centro Darbuotojais (pvz., saugos įgaliotiniu ir kitais), išorės ekspertais nuolat inicijuoja ir vykdo bendrus, specializuotus ir kompleksinius asmens duomenų apsaugos mokymus, švietimo akcijas, rengia metodinę edukacinę ir pagalbinę medžiagą (pvz., pranešimai, lankstinukai, atmintinės, instrukcijos).

47. Duomenų apsaugos pareigūnas konsultuoja, derina vidaus teisės aktus, reglamentuojančius Centro asmens duomenų tvarkymo procesus, taip pat asmens duomenų tvarkymo sutartis, duomenų teikimo, perdavimo, bendradarbiavimo susitarimus, kitus asmens duomenų tvarkymo procesuose rengiamus, formuojamus dokumentus.

48. Centro Darbuotojai gali bet kada kreiptis į duomenų apsaugos pareigūną dėl konsultacijos: kai sprendžiama pradėti tvarkyti asmens duomenis (nauju būdu; keisti esamą asmens duomenų tvarkymą ir pan.), sprendžiant, kokias apsaugos priemones (įskaitant technines ir organizacines) taikyti, siekiant sumažinti riziką duomenų subjektų teisėms ir interesams; ruošiant vidaus dokumentus, kuriuose nustatomi asmens duomenų tvarkymo procesai; tiriant galimai įvykusį asmens duomenų saugumo pažeidimą; sprendžiant, ar atlikti poveikio duomenų apsaugai vertinimą ir kokia metodika vadovautis jį atliekant; kai kyla klausimų dėl Darbuotojų asmens duomenų tvarkymo Centro viduje.

IX SKYRIUS

BENDROSIOS DARBUOTOJŲ PAREIGOS ASMENS DUOMENŲ APSAUGOS SRITYJE

49. Kiekvienas Centro Darbuotojas privalo:

49.1. tvarkydamas asmens duomenis įsitikinti, kad yra laikomasi visų reikalavimų, numatytų Taisyklėse;

49.2. tvarkyti asmens duomenis tik tuo tikslu ir ta apimtimi, kiek jų reikia darbo funkcijoms atlikti;

49.3. visais atvejais įsitikinti, kad tvarkoma duomenų kategorija yra įtraukta į duomenų tvarkymo veiklos įrašus, o tvarkymo tikslas atitinka bent vieną iš duomenų tvarkymo

veiklos įrašuose nurodytų tikslų; apie jų poreikį tvarkyti naujas duomenų kategorijas ir (ar) naujais tikslais informuoti Centro direktorių bei duomenų apsaugos pareigūną;

49.4. visais atvejais prieš perduodant asmens duomenis tretiesiems asmenims įsitikinti, kad tokia duomenų gavėjų kategorija yra įtraukta į duomenų tvarkymo veiklos įrašus, o jei ketinama duomenis perduoti už Europos ekonominės erdvės (toliau – EEE) ribų – kad atitinkamas duomenų gavėjas yra įtrauktas į duomenų tvarkymo veiklos įrašus; apie poreikį perduoti duomenis duomenų tvarkymo veiklos įrašuose nenurodytai duomenų gavėjų kategorijai arba už EEE ribų veikiančiam trečiajam asmeniui, nenurodytam duomenų tvarkymo veiklos įrašuose, informuoti Centro direktorių bei duomenų apsaugos pareigūną;

49.5. įsitikinti, kad kiekvienas asmuo buvo informuotas apie jo asmens duomenų tvarkymą, o duomenų tvarkymo numatytais atvejais yra davęs sutikimą duomenų tvarkymui; jei asmuo nebuvo informuotas apie jo duomenų tvarkymą ir (ar) nebuvo gautas jo sutikimas, įteikti informacinį pranešimą (6 priedas) ir (ar) paprašyti asmens sutikimo pagal atitinkamai asmenų kategorijai pritaikytą formą (7 priedas), jei konkrečiu atveju nėra tinkama nei viena iš Centro naudojamų tipinių informacinių pranešimų ar sutikimų formų, Darbuotojas apie tai nedelsiant turi informuoti Centro direktorių ir duomenų apsaugos pareigūną;

49.6. atsižvelgiant į atliekamų darbo funkcijų pobūdį, užtikrinti, kad visi Centro valdomi asmens duomenys būtų tikslūs ir prireikus atnaujinami;

49.7. tvarkydamas duomenis, elgtis rūpestingai ir atsargiai, turėdami omenyje tai, kad Darbuotojo veiksmai, susiję su duomenimis, kelia pavojų asmenų pagrindinėms teisėms ir laisvėms (rasinė ar etninė kilmė, sveikatos duomenys, teistumo duomenys ir kt.);

49.8. įgyvendinti ir naudoti technines ir organizacines duomenų apsaugos priemones, užtikrinančias duomenų apsaugą nuo neleistinos prieigos, neteisėto rinkimo, naudojimo ir saugojimo, netyčinio praradimo, sunaikinimo ar sugadinimo, kaip tai nustatyta šiose Taisyklėse, vidaus tvarkos taisyklėse ir kituose Centro vidaus dokumentuose;

49.9. neatskleisti informacijos apie Centro taikomas technines ir organizacines duomenų apsaugos priemones, įskaitant bet neapsiribojant Centro vidaus dokumentais, jokiems tretiesiems asmenims, prieš tai neįsitikinus jų teise gauti tokią informaciją bei laikytis konfidencialumo įpareigojimų pasirašant konfidencialumo laikymosi pasižadėjimą (4 priedas). Konfidencialios informacijos sąrašas pateikiamas 5 priede;

49.10. nesaugoti asmens duomenų jokiose Darbuotojui priklausančiose asmeninėse atmintinėse, kompiuterinėje ar programinėje įrangoje (internetinėse duomenų saugyklose, atmintinėse, kompiuteriuose, telefonuose ir pan.), nebent konkrečiu atveju Centras leistų Darbuotojui naudoti konkrečias asmenines priemones darbo funkcijų vykdymui;

49.11. neišnešti iš Centro dokumentų, kuriuose yra užfiksuoti Centro duomenų subjektų asmens duomenys, nebent tai yra absoliučiai būtina teikiant paslaugas;

49.12. nepalikti Centro dokumentų lankytojams prieinamose vietose;

49.13. kreiptis į duomenų apsaugos pareigūną ir gauti jo konsultaciją, susijusią su Taisyklių arba teisės aktų, reglamentuojančių asmens duomenų apsaugą taikymu, aiškinimu, pažeidimu ar atitikimu Taisyklėms arba asmens duomenų apsaugos teisės aktams;

49.14. su asmenų prašymais, susijusiais su duomenų subjektų teisių įgyvendinimu, elgtis rūpestingai ir atidžiai; gavę bet kokį asmens prašymą, susijusį su asmens duomenimis nedelsdami, ne vėliau kaip per 1 (vieną) darbo dieną nuo asmens prašymo gavimo raštu informuoti Centro direktorių bei duomenų apsaugos pareigūną;

49.15. raštu informuoti Centro direktorių bei duomenų apsaugos pareigūną apie asmens duomenų saugumo pažeidimą Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo nurodyta tvarka;

49.16. pagal savo kompetenciją imtis pagrįstų veiksmų, kad duomenų subjekto pažeidimas nepasikartotų;

49.17. bendradarbiauti su kitais Darbuotojais ir (ar) paslaugų teikėjais atliekant duomenų subjekto pažeidimo valdymą, asmenų prašymų valdymą, Valstybinės duomenų apsaugos inspekcijos ar Žurnalistų etikos inspektoriaus paklausimų valdymą ir kitas Centro nustatytas su duomenų tvarkymu susijusias procedūras;

49.18. pateikti Centro direktoriui ir duomenų apsaugos pareigūnui bet kokią prašomą informaciją, susijusią su asmens duomenų saugumo pažeidimu;

49.19. Centro direktoriaus leidimu vykdyti duomenų apsaugos pareigūno nurodymus dėl duomenų tvarkymo.

X SKYRIUS SPECIALIEJI ASMENS DUOMENŲ TVARKYMO CENTRE REIKALAVIMAI

50. Centras įgyvendina Taisyklėse nurodytas organizacines ir technines asmens duomenų saugumo priemonės, skirtas užtikrinti tinkamą asmens duomenų saugumą, taip pat apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo.

51. Pasikeitus duomenų subjektų asmens duomenims ir duomenų subjektams apie tai raštu informavus Centrą, toks duomenų subjekto raštas saugomas elektroninėje dokumentų valdymo sistemoje.

52. Naikinant dokumentus, kurių saugojimo terminas yra pasibaigęs, Centro dokumentai, kuriuose nurodomi asmens duomenys, bei jų kopijos turi būti sunaikinti taip, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio.

53. Duomenų subjektų pateikti dokumentai bei jų kopijos, finansavimo, buhalterinės apskaitos ir atskaitomybės, archyvinės ir kitos bylos, kuriose yra asmens duomenų, saugomos rakinamose spintose, seifuose arba patalpose. Dokumentai, kuriuose yra asmens duomenų, neturi būti laikomi taip, kad neturintys teisės asmenys nekliudomai galėtų su jais susipažinti.

54. Archyviniam saugojimui perduoti dokumentai (bylos) saugomi Centro archyve dokumentų saugykloje.

55. Vietinio tinklo, t. y., uždaro Centro tinklo, kuriami visi tinklo informaciniai resursai yra laikomi ir tvarkomi centralizuotai, tarnybinėje stotyje (serveryje), o naudojami lokaliai per vartotojų asmeninius kompiuterius (interesantus, kurie gali dalintis pagrindiniais tinklo ištekliais (išorinės atminties talpa, spausdintuvas ir kt.), su kitais tinklo vartotojais), sritys, kuriose yra saugomi asmens duomenys, privalo būti apsaugotos prieigos prie asmens duomenų slaptažodžiais arba turi būti slaptažodžiai suteikiami, keičiami ir naikinami duomenų valdytojo nustatyta tvarka.

56. Centro interneto svetainėje turi būti maksimaliai apribotos galimybės viešai veikiančioms interneto paieškos sistemoms bei paieškos variklių robotams kopijuoti Centro anksčiau skelbtos, bet iš Centro interneto svetainės jau pašalintos, informacijos kopijų. Kompiuterinė įranga turi būti apsaugota nuo kenksmingos programinės įrangos (antivirusinių programų įdiegimas, atnaujinimas ir pan.). Asmens duomenų tvarkymo keliamos rizikos vertinimo atlikimo tvarka ir saugumo pažeidimų valdymas, reagavimo į šiuos pažeidimus veiksmai, duomenų atsarginių kopijų darymo, saugojimo ir duomenų atkūrimo iš atsarginių duomenų kopijų tvarka nustatoma informacinių sistemų valdytojo tvirtinamuose informacinės sistemos saugos nuostatuose bei kituose saugos politiką įgyvendinančiuose teisės aktuose.

XI SKYRIUS DUOMENŲ SUBJEKTO INFORMAVIMAS

57. Kai asmens duomenys gaunami iš paties duomenų subjekto, duomenų subjektui pateikiama informacija apie asmens duomenų tvarkymą, nurodyta Reglamento (ES) 2016/679 13 straipsnyje, užpildant nurodytą formą (6 priedas).

58. Taisyklių 58 punkte nurodyta informacija duomenų subjektui pateikiama prieš gaunant jo asmens duomenis arba jų gavimo metu.

59. Taisyklių 58 punkte nurodyta informacija neteikiama, jeigu duomenų subjektas tą informaciją jau turi.

60. Kai asmens duomenys gaunami ne iš paties duomenų subjekto, Centras privalo duomenų subjektui pateikti Reglamento (ES) 2016/679 14 straipsnyje nurodytą informaciją apie asmens duomenų tvarkymą, užpildant Taisyklių 6 priede nurodytą formą.

61. Šių Taisyklių 61 punkte nurodyta informacija duomenų subjektui pateikiama:

61.1. ne vėliau kaip per vieną mėnesį nuo asmens duomenų gavimo;

61.2. pirmą kartą susisiekiant su duomenų subjektu, jeigu jo asmens duomenys bus naudojami ryšiams su juo palaikyti;

61.3. pirmą kartą atskleidžiant asmens duomenis kitam duomenų gavėjui, jeigu numatoma tai daryti.

62. Taisyklių 62 punktas netaikomas, jeigu:

62.1. duomenų subjektas jau yra gavęs informaciją;

62.2. tokios informacijos pateikti yra neįmanoma arba tam reikėtų neproporcingų pastangų, arba jeigu dėl pareigos informuoti gali būti sunku pasiekti duomenų tvarkymo tikslus arba neįmanoma jų pasiekti. Tokiais atvejais imamasi tinkamų priemonių fizinių asmenų teisėms ir laisvėms, ir teisėtiems interesams apsaugoti, įskaitant viešą informacijos apie asmens duomenų tvarkymą paskelbimą Centro interneto svetainėje <https://essc.lrv.lt/lt/>;

62.3. duomenų gavimas ar atskleidimas aiškiai nustatytas teisės aktuose;

62.4. asmens duomenys privalo būti išlaikomi konfidencialūs, laikantis teisės aktuose reglamentuojamos profesinės, komercinės ar valstybinės paslapties prievolės.

63. Jeigu Centras ketina toliau tvarkyti asmens duomenis kitu tikslu, negu tas, kuriuo jie buvo renkami, prieš toliau tvarkydama asmens duomenis, Centras pateikia duomenų subjektui informaciją apie kitą tikslą ir informaciją, nurodytą Taisyklių 58 ir (ar) 61 punktuose.

64. Centro Darbuotojai, kurie savo veikloje tvarko asmens duomenis, parengę pranešimus dėl privatumo duomenų subjektams, kurių duomenis tvarko atlikdami Centro nuostatuose ar pareigybės aprašyme nustatytas funkcijas, teikia susipažinti duomenų apsaugos pareigūnui, kuris registruoja privatumo pranešimus Privatumo pranešimų registracijos žurnale (7 priedas).

65. Centro interneto svetainės skyriuje „Asmens duomenų apsauga“ skelbiami duomenų subjektams aktualūs Centro privatumo pranešimai. Duomenų apsaugos pareigūnas teikia konsultacijas dėl aktualių privatumo pranešimų viešinimo.

66. Už duomenų subjekto informavimą atsakingas Darbuotojas, kuris renka ir tvarko to duomenų subjekto duomenis. Dėl informavimo pareigos tinkamo vykdymo konsultuojamasi su duomenų apsaugos pareigūnu.

XII SKYRIUS

POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS IR KONSULTACIJOS SU PRIEŽIŪROS INSTITUCIJA

67. Kai, atsižvelgiant į asmens duomenų ir duomenų subjektų kategorijas, duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms ir laisvėms gali kilti didelis pavojus, Centras, prieš pradėdamas tvarkyti asmens duomenis, atlieka numatytą tvarkyti duomenų tvarkymo operacijų (veiksmų) poveikio duomenų apsaugai vertinimą.

68. Poveikio duomenų apsaugai vertinimas atliekamas:

68.1. kai duomenų tvarkymo operacija (veiksmas) patenka į duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašą, patvirtintą Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. kovo 14 d. įsakymu Nr. 1T-35 (1.12E) „Dėl duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“ (toliau – Duomenų tvarkymo operacijų sąrašas);

68.2. kai duomenų tvarkymo operacija (veiksmas) nepatenka į duomenų tvarkymo operacijų sąrašą, tačiau vertinama, kad duomenų tvarkymo operacija (veiksmas) fizinių asmenų teisėms ir laisvėms gali kelti didelį pavojų;

68.3. pasikeitus duomenų tvarkymo operacijų (veiksmų) sąlygoms ir kai tai gali lemti didelį pavojų fizinių asmenų teisėms ir laisvėms;

68.4. kitais šiose Taisyklėse nustatytais atvejais.

69. Kriterijai, į kuriuos atsižvelgiama priimant sprendimą, kad duomenų tvarkymo operacijos (veiksmai) gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms yra šie:

69.1. 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 ar elgesiu, vieta arba judėjimu;

69.2. duomenų tvarkymas priimant automatizuotus sprendimus, sukeliančius teisinį arba kitokį reikšmingą poveikį duomenų subjektui (pvz., duomenų tvarkymas gali lemti asmenų atskirtį arba diskriminaciją);

69.3. neskelbtinų arba labai asmeniškų duomenų Reglamento (ES) 2016/679 9 straipsnyje nurodytų specialiųjų kategorijų asmens duomenų; Reglamento (ES) 2016/679 10 straipsnyje nurodytų asmens duomenų, susijusių su apkaltinamaisiais nuosprendžiais ar nusikalstamomis veikomis; asmens duomenų, susijusių su namų ūkiu ir veikla (pvz., elektroniniai ryšiai, kurių konfidencialumas turi būti apsaugotas) arba susijusių su pagrindinių teisių įgyvendinimu (pvz., vietos duomenys, kurių rinkimas gali reikšti judėjimo laisvės apribojimą), arba kurių pažeidimas būtų aiškiai susijęs su rimtais padariniais kasdieniam duomenų subjekto gyvenimui (pvz., finansiniai duomenys, kurie gali būti panaudoti atliekant su sukčiavimu susijusį mokėjimą) tvarkymas. Šis kriterijus netaikomas asmens duomenims, kuriuos viešai paskelbė duomenų subjektas arba trečiosios šalys;

69.4. sisteminga stebėseną: duomenų tvarkymas duomenų subjektų stebėsenos arba kontrolės tikslais, įskaitant sistemingą viešosios vietos stebėjimą dideliu mastu;

69.5. didelio masto duomenų tvarkymas;

69.6. duomenų rinkinių siejimas ir derinimas;

69.7. su pažeidžiamais duomenų subjektais susijusių duomenų tvarkymas;

69.8. naujų technologijų ar organizacinių sprendimų taikymas (pvz., telefoninių pokalbių įrašymas);

69.9. atvejai, kai dėl paties duomenų tvarkymo duomenų subjektams užkertamas kelias naudotis savo teisėmis, paslaugomis arba sudaryti sutartis ar kitus susitarimus;

69.10. kitos aplinkybės, rodančios galimą didelį pavojų fizinių asmenų teisėms ir laisvėms.

70. Kuo daugiau Taisyklių 69 punkte nustatytų kriterijų atitinka duomenų tvarkymo operacija (veiksmas), tuo didesnė tikimybė, kad tokia operacija (veiksmas) gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms. Dėl būtinybės atlikti poveikio duomenų apsaugai vertinimą konsultuojamasi su duomenų apsaugos pareigūnu.

71. Jei duomenų tvarkymo operacija (veiksmas) atitinka du ar daugiau Taisyklių 69 punkte nustatytų kriterijų, tačiau vertinama, kad tokia operacija (veiksmas) negali kelti didelio pavojaus duomenų subjektų teisėms ir laisvėms, toks sprendimas ir jo argumentai išdėstomi

raštu ir kartu su duomenų apsaugos pareigūno nuomone pateikiami Centro direktoriui susipažinti.

72. Už poveikio duomenų apsaugai vertinimą atsakingi Centro Darbuotojai, kurie tvarkys asmens duomenis arba inicijuoja duomenų tvarkymo operacijos (veiksmo) poreikį. Jei Centro žmogiškųjų, laiko ar kitų išteklių nepakanka, kad poveikio duomenų apsaugai vertinimas būtų atliktas tinkamai, gali būti pasitelkiami išorės konsultantai, specialistai ekspertai (teisės, informacinių technologijų, kibernetinio saugumo, etikos ir kitų sričių).

73. Poveikio duomenų apsaugai vertinimas atliekamas raštu. Panašių didelį pavojų keliančių duomenų tvarkymo operacijų (veiksmų) sekai išnagrinėti galima atlikti vieną poveikio duomenų apsaugai vertinimą. Įvertinime privalo būti pateikta bent jau Reglamento (ES) 2016/679 35 straipsnio 7 dalyje nurodyta informacija. Atlikdami poveikio duomenų apsaugai vertinimą Centro Darbuotojai konsultuojasi su duomenų apsaugos pareigūnu.

74. Poveikio duomenų apsaugai vertinimo ataskaitos rekomenduojama forma pateikiama Valstybinės duomenų apsaugos inspekcijos internetinėje svetainėje <https://vdai.lrv.lt/lt/naudinga-informacija/rekomendacijos-gaires-ir-kt/work/>.

75. Jeigu, atsižvelgiant į numatomos duomenų tvarkymo operacijos (veiksmo) pobūdį, yra įmanoma, Centras siekia išsiaiškinti duomenų subjektų ar jų atstovų nuomonę apie numatomą duomenų tvarkymą, nepažeisdama komercinių, viešųjų interesų apsaugos ir duomenų tvarkymo operacijų (veiksmų) saugumo reikalavimų.

76. Poveikio duomenų apsaugai vertinimą atlikęs Centro Darbuotojas parengtą poveikio duomenų apsaugai ataskaitą pateikia susipažinti Centro direktoriui, atitinkamos informacinės sistemos saugos įgaliotiniui, duomenų apsaugos pareigūnui ir už šio sprendimo dėl vertinamos duomenų tvarkymo operacijos (veiksmo) priėmimą ir jo įgyvendinimą atsakingam asmeniui.

77. Prieš pradėdama duomenų tvarkymo operacijas (veiksmus), kuriuos gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms, Centro išankstinių konsultacijų teikimo taisyklių, patvirtintų Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-84 (1.12E) „Dėl išankstinių konsultacijų teikimo taisyklių patvirtinimo“ (su vėlesnėmis patvirtintomis redakcijomis) nustatytais atvejais privalo konsultuotis su Valstybine duomenų apsaugos inspekcija.

78. Duomenų tvarkymo operacijos (veiksmi), kurios gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms, gali būti atliekamos tik tada, kai Centras visiškai ir tinkamai įgyvendina Valstybinės duomenų apsaugos inspekcijos rekomendacijas, nurodymus ir priemones, gautus pasikreipus išankstinės konsultacijos.

79. Prekės ir (ar) paslaugos, susijusios su duomenų tvarkymu tokiu būdu, kuris gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms, gali būti perkamos tik tada, jeigu tam tikros prekės ir (ar) paslaugos pardavėjas yra atlikęs poveikio duomenų apsaugai vertinimą, Centrai yra pateikta susipažinti tokio vertinimo išvada ir pardavėjas patvirtina, kad jo prekė ar paslauga atitinka Reglamento (ES) 2016/679 reikalavimus.

80. Kai duomenų tvarkymo pobūdis, aprėptis, kontekstas ir tikslas yra labai panašūs į duomenų tvarkymą, kurio poveikis duomenų apsaugai buvo įvertintas, galima iš naujo nevertinti poveikio duomenų apsaugai, o atsižvelgti į dėl panašaus duomenų tvarkymo atliktą poveikio duomenų apsaugai vertinimą.

XIII SKYRIUS

PRITAIKYTOJI IR STANDARTIZUOTOJI ASMENS DUOMENŲ APSAUGA

81. Centras, kaip duomenų valdytojas, tiek nustatydamas duomenų tvarkymo priemones, tiek tvarkydamas duomenis įgyvendina tinkamas technines ir organizacines priemones asmens duomenų saugumui užtikrinti. Centras, nustatydamas tinkamas technines ir

organizacines priemonės, turi atsižvelgti į techninių galimybių pažangos lygį, įgyvendinimo sąnaudas ir duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į duomenų tvarkymo keliamus pavojus fizinių asmenų teisėms ir laisvėms. Pritaikytosios duomenų apsaugos principas įpareigoja Centrą imtis techninių ir organizacinių priemonių ankstyvuosiuose duomenų tvarkymo operacijų (veiksmų) rengimo etapuose, kad privatumo ir duomenų apsaugos principai būtų įgyvendinami nuo pat duomenų tvarkymo pradžios, o kiekviena nauja programa ar sistema, kurioje tvarkomi asmens duomenys, būtų kuriama ir diegiama atsižvelgiant į tokių duomenų apsaugą. Į privatumą turi būti atsižvelgiama visą programos ar sistemos gyvavimo ciklą.

82. Priemonių, taikomų įgyvendinant pritaikytosios duomenų apsaugos principą, pavyzdžiai:

- 82.1. audito ir saugos reikalavimų įgyvendinimo priemonių priežiūros vykdymas;
- 82.2. asmens duomenų konfidencialumo užtikrinimas;
- 82.3. asmens duomenų naudojimo ribojimas;
- 82.4. galimybės stebėti asmens duomenų tvarkymą suteikimas duomenų subjektams;
- 82.5. galimybės tobulinti ir įgyvendinti naujas asmens duomenų apsaugos priemonės užtikrinimas;

- 82.6. kontrolės galimybė;
- 82.7. kuo greitesnis duomenų anonimizavimas;
- 82.8. pseudonimų suteikimas;
- 82.9. asmens duomenų tvarkymo skaidrumas;
- 82.10. renkamo asmens duomenų kiekio ribojimas;
- 82.11. tinkamas darbuotojų mokymas;
- 82.12. saugių sistemų diegimas.

83. Standartizuotoji duomenų apsauga reiškia pareigą duomenų valdytojui užtikrinti, kad asmens duomenys būtų tvarkomi užtikrinant aukščiausią privatumo apsaugos lygį, o su asmens duomenimis negalėtų susipažinti neribotas asmenų skaičius.

84. Priemonių, skirtų standartizuotosios duomenų apsaugos principui įgyvendinti, pavyzdžiai:

- 84.1. standartizuotai tvarkomi tik tie duomenys, kurie yra būtini tam tikram duomenų tvarkymo tikslui;
- 84.2. technologinės priemonės turi būti suprojektuotos taip, kad būtų galima išvengti nebūtino asmens duomenų tvarkymo;
- 84.3. numatytosios asmens duomenų apsaugos nuostatos;
- 84.4. funkcionalumai, skirti asmens duomenims tvarkyti, neturi būti prieinami tiems Darbuotojams, kuriems jie nėra būtini funkcijoms atlikti.

84.5. prekės ir (ar) paslaugos, susijusios su duomenų tvarkymu, gali būti perkamos tik tada, jeigu tam tikros prekės ir (ar) paslaugos pardavėjas užtikrina, kad jo siūloma prekė ar paslauga atitinka pritaikytosios ir standartizuotosios asmens duomenų apsaugos principus ir Centrai yra pateikiami dokumentai, kuriais pardavėjas patvirtina, kad jo prekė ar paslauga atitinka Reglamento (ES) 2016/679 reikalavimus.

XIV SKYRIUS

ASMENS DUOMENŲ SAUGUMO POLITIKA

85. Asmens duomenų saugumas (toliau – ir duomenų sauga) apima tris pagrindinius elementus:

- 85.1. asmens duomenų konfidencialumą – apsaugą nuo nesankcionuoto atskleidimo;

85.2. asmens duomenų vientisumą – apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;

85.3. asmens duomenų prieinamumą – užtikrinimą, kad Centre asmens duomenys būtų prieinami tada, kai jie yra reikalingi.

86. Bendrieji duomenų saugos tikslai:

86.1. užtikrinti tinkamą ir efektyvų asmens duomenų valdymą, siekiant išvengti veiklos sutrikdymo dėl asmens duomenų konfidencialumo, vientisumo ar prieinamumo pažeidimo ir įgyvendinant gerąją praktiką atitinkančias technines ir organizacines priemones;

86.2. užtikrinti atitiktį duomenų saugą reglamentuojančių teisės aktų reikalavimams, atliekant kasmetinį atitikties vertinimą ir šalinant nustatytus trūkumus;

86.3. užtikrinti efektyvų rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant sumažinti riziką iki priimtino lygio, atliekant kasmetinį rizikos vertinimą ir įgyvendinant valdymo priemones;

86.4. užtikrinti Centro informacinės sistemos tęstinumą, atliekant periodinį veiklos tęstinumo valdymo plano veiksmingumo išbandymą ir jo priežiūrą.

87. Duomenų saugos reikalavimai nustatomi:

87.1. vadovaujantis teisės aktuose nustatytais informacijos saugos, kibernetinio saugumo ir asmens duomenų apsaugos reikalavimais;

87.2. atsižvelgiant į Centro veiklos tikslus ir veiklos reikalavimus;

87.3. atsižvelgiant į suinteresuotų šalių lūkesčius ir poreikius, išreikštus informacijos saugą reglamentuojančiuose teisės aktuose, duomenų teikimo, tvarkymo ir kitokio pobūdžio sutartyse;

87.4. vertinant duomenų saugos riziką.

88. Duomenų saugos valdymas yra užtikrinamas nuosekliai planuojant, įgyvendinant, vertinant ir tobulinant Centro elektroninės saugos (kibernetinio saugumo) politiką, vadovaujantis Centro informacinės sistemos ir Centro naudojamų valstybės informacinių sistemų duomenų saugos nuostatais ir kitais saugos politiką reglamentuojančiais teisės aktais ir standartais.

89. Centras:

89.1. nustato bendruosius duomenų saugos valdymo tikslus;

89.2. nustato duomenų saugos tobulinimo uždavinius ir priemones, ir juos įtraukia į veiklos planavimo dokumentus;

89.3. laikosi Lietuvos Respublikos galiojančiuose teisės aktuose ir sutartyse nustatytų pareigų duomenų saugos srityje;

89.4. užtikrina reikiamų išteklių suteikimą;

89.5. sudaro sąlygas Darbuotojams plėsti žinias duomenų saugos srityje.

90. Už Taisyklių 90 punkte nustatytų pareigų vykdymą atsako Centro Darbuotojai pagal kompetenciją.

91. Centras nuolat gerina duomenų saugos valdymo veiksmingumą, įgyvendindamas informacijos saugos politiką ir tikslus, organizuodama duomenų saugos valdymo vidaus auditą, nustatydamą neatitiktis ir jas šalindama, vykdydama duomenų saugos valdymo korekcinis veiksmus ir reguliariai aptardama duomenų saugos klausimus.

92. Duomenų saugos nuostatos skelbiamos suinteresuotoms šalims joms prieinama ir suprantama forma. Vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu, informacija apie Centre įgyvendintas saugos priemones ir Centro valdomų valstybės informacinių išteklių pažeidžiamumą yra konfidenciali ir teikiama, jeigu galimybė teikti šią informaciją yra numatyta įstatymuose ar jų pagrindu priimtuose kituose norminiuose teisės aktuose. Duomenų saugos nuostatos peržiūrimos periodiškai, ne rečiau kaip kartą per metus, ir prireikus tikslinamos.

93. Centro techninės ir organizacinės priemonės turi užtikrinti tokio lygio saugumą, kuris atitiktų saugotinių duomenų pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms ir juos tvarkant kylančias rizikas.

94. Įvertinus Taisyklių 90 punkte nurodytas aplinkybes ir nustačius asmens duomenų saugumo lygį, Centre taikomos techninės ir organizacinės priemonės, skirtos asmens duomenims apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat bet kokio kito neteisėto tvarkymo ir visų pirma susijusios su:

- 94.1. asmens duomenų saugumo politika ir procedūromis;
- 94.2. vaidmenimis ir atsakomybėmis;
- 94.3. prieigų prie asmens duomenų valdymo politika;
- 94.4. išteklių ir turto valdymu;
- 94.5. keitimų valdymu;
- 94.6. duomenų tvarkytojais;
- 94.7. asmens duomenų saugumo pažeidimais ir kitais incidentais;
- 94.8. veiklos tęstinumu;
- 94.9. personalo pareigos užtikrinti konfidencialumą vykdymu;
- 94.10. personalo mokymais;
- 94.11. prieigų prie asmens duomenų kontrole ir autentifikavimu;
- 94.12. techninių žurnalų įrašais ir stebėseną;
- 94.13. darbo vietų apsauga;
- 94.14. tinklo ir komunikacijos sauga;
- 94.15. atsarginėmis kopijomis;
- 94.16. mobiliaisiais (nešiojamaisiais) įrenginiais;
- 94.17. programinės įrangos sauga;
- 94.18. duomenų naikinimu, šalinimu;
- 94.19. fizine sauga.

95. Duomenų saugos priemonės, taikomos asmens duomenims, tvarkomiems Centro informacinėje sistemoje ir Centro naudojamose valstybės informacinėse sistemose, apsaugoti, nustatytos Centro informacinės sistemos ir Centro naudojamų informacinių sistemų duomenų saugos nuostatuose ir kituose saugos dokumentuose.

96. Centro paskirtas saugos įgaliotinis stebi, kontroliuoja ir prižiūri duomenų saugos politikos įgyvendinimą. Centro saugos įgaliotinio paskyrimas nenaikina kiekvieno Darbuotojo pareigos įgyvendinti ir taikyti duomenų saugos priemones ir atsakomybės už tų priemonių įgyvendinimą ir taikymą.

97. Darbuotojai, kurie naudojami Centro suteiktu elektroniniu paštu, interneto prieiga ir kita informacinių ir komunikacinių technologijų įranga, privalo vadovautis Taisyklių, Centro informacinės sistemos saugos nuostatų ir kitų teisės aktų, reglamentuojančių elektroninės informacijos saugą, nuostatomis, o kilus klausimų dėl duomenų saugos priemonių taikymo, – kreiptis į Centro saugos įgaliotinį.

XV SKYRIUS

ASMENS DUOMENŲ PERDAVIMAS TRETIESIEMS ASMENIMS

98. Centras turi teisę pasitelkti duomenų tvarkytoją asmens duomenų tvarkymo operacijoms (veiksmams) atlikti.

99. Sutartis ar kitas susitarimas dėl asmens duomenų tvarkymo su paslaugų teikėju (duomenų tvarkytoju) sudaromi vadovaujantis Standartinėmis sutarčių sąlygomis.

100. Centras, prieš pasitelkdamas duomenų tvarkytoją pagal sutartį, įvertina, ar duomenų tvarkytojas yra pajėgus pakankamai užtikrinti, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos taip, kad asmens duomenų tvarkymas atitiktų Reglamento (ES) 2016/679 ir Taisyklių reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga. Taip pat duomenų tvarkytojas įsipareigoja laikytis Reglamento (ES) 2016/679 28 straipsnyje nustatytų sąlygų

101. Centro Darbuotojas, inicijuojantis pirkimą, nustatęs, kad paslaugos teikėjas tvarkys asmens duomenis Centro vardu, konsultuojantis kartu su Centro duomenų apsaugos pareigūnu, turi parengti Taisyklių 100 punkte nurodytos sutarties ar kito susitarimo, kuriuose nustatomos asmens duomenų tvarkymo sąlygos, projektą ir nurodyti už tokios sutarties ar kito susitarimo ar jos (jo) asmens duomenų tvarkymą atsakingą asmenį, Centro duomenų apsaugos pareigūno kontaktus.

102. Kitiems asmenims (ne duomenų tvarkytojams) Centro tvarkomi asmens duomenys gali būti teikiami:

102.1. duomenų subjektui paprašius ar sutikus;

102.2. kai pareiga teikti asmens duomenis Centrai kyla iš teisės aktų reikalavimų;

102.3. kai teisė gauti asmens duomenis nustatyta duomenų gavėjo veiklą reglamentuojančiuose teisės aktuose ir yra kita Reglamento (ES) 2016/679 6 straipsnio 1 dalyje nustatyta teisėto duomenų tvarkymo sąlyga.

103. Prašymai dėl asmens duomenų teikimo teikiami ir nagrinėjami Duomenų subjektų teisių įgyvendinimo aprašo tvarka, o tiek, kiek duomenų subjekto teisių įgyvendinimo nereglamentuoja Duomenų subjektų teisių įgyvendinimo tvarka, prašymai teikiami ir nagrinėjami Asmenų aptarnavimo, jų prašymų ir skundų nagrinėjimo Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centre taisyklėse nustatyta tvarka.

104. Asmens duomenys viešosios informacijos rengėjų ir (ar) skleidėjų atstovams, žurnalistams teikiami Lietuvos Respublikos visuomenės informavimo įstatymo nustatyta tvarka.

105. Priimant sprendimą dėl asmens duomenų teikimo, konsultuojamasi su duomenų apsaugos pareigūnu, išskyrus atvejus, kai teikiama asmens duomenis sudaranti informacija yra paskelbta viešai arba dėl tokios informacijos teikimo duomenų gavėjui analogiškais tikslais duomenų apsaugos pareigūnas jau yra pateikęs savo nuomonę.

106. Asmens duomenų teikimą tretiesiems asmenims iš Centro informacinės sistemos ir Centro naudojamų valstybės informacinių sistemų reglamentuoja šio registro ar tam tikros informacinės sistemos nuostatai.

107. Siekiant tinkamai valdyti asmens duomenų judėjimą, duomenų apsaugos pareigūnas skaitmeniniu būdu tvarko Centro pasitelktų duomenų tvarkytojų ir kitų duomenų gavėjų (gaunančių asmens duomenis pagal duomenų teikimo sutartis) registrą (9 priedas).

XVI SKYRIUS

ASMENS DUOMENŲ PERDAVIMAS Į TREČIĄSIAS VALSTYBES IR TARPTAUTINĖMS ORGANIZACIJOMS

108. Perduoti asmens duomenis į trečiąją valstybę arba tarptautinei organizacijai galima tik esant bent vienai iš šių sąlygų:

108.1. yra priimtas Europos Komisijos sprendimas, kad atitinkama trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba atitinkama tarptautinė organizacija užtikrina tinkamo lygio apsaugą;

108.2. jeigu Centras yra nustatęs tinkamas asmens duomenų saugumo priemones, įskaitant tokias, kurios užtikrintų duomenų subjektams galimybę naudotis duomenų subjekto teisėmis ir veiksmingomis duomenų subjekto teisių gynimo priemonėmis;

108.3. jeigu yra bent viena iš Reglamento (ES) 2016/679 49 straipsnio 1 dalyje nurodytų sąlygų.

XVII SKYRIUS

ASMENS DUOMENŲ SKELBIMAS

109. Centras asmens duomenis skelbia viešai Lietuvos Respublikos Konstitucijos, Lietuvos Respublikos teisėkūros pagrindų įstatymo, Bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms ir mobiliosioms programoms aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2003 m. balandžio 18 d. nutarimu Nr. 480 „Dėl Bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms ir mobiliosioms programoms aprašo patvirtinimo“, kitų asmens duomenų skelbimą reglamentuojančių teisės aktų ir duomenų subjekto sutikime (kai taikoma) nustatyta apimtimi ir pagrindais. Šie duomenys skelbiami Centro svetainėje <https://essc.lrv.lt/lt/>.

110. Centro darbuotojų kontaktiniai duomenys skelbiami jų pareigų ėjimo ar įgaliojimų laikotarpiu, išskyrus atvejus, kai teisės aktuose nustatyta kitaip.

111. Pasibaigus asmens duomenų skelbimo terminui, tų duomenų skelbimas nutraukiamas ir asmens duomenys yra perduodami archyviniam saugojimui ar sunaikinami.

XVIII SKYRIUS

BAIGIAMOSIOS NUOSTATOS

112. Centro vidaus teisės aktuose ar kituose dokumentuose nustatomi reikalavimai, susiję su asmens duomenų tvarkymu, negali prieštarauti Taisyklių nuostatom.

113. Centre ne rečiau kaip kartą per metus vykdomi Darbuotojų mokymai Reglamento (ES) 2016/679, Taisyklių taikymo ir įgyvendinimo bei kitais asmens duomenų apsaugos klausimais.

114. Duomenų subjektas turi teisę Valstybinei duomenų apsaugos inspekcijai skusti Centro veiksmus ar neveikimą, susijusius su duomenų subjekto teisių įgyvendinimu.

115. Darbuotojai, pažeidę Taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.

116. Taisyklės peržiūrimos ir atnaujinamos ne rečiau nei kartą per metus, o pasikeitus asmens duomenų tvarkymo sąlygoms ar Lietuvos Respublikoje galiojantiems teisės aktams, reglamentuojantiems asmens duomenų tvarkymą – nedelsiant.

(Teisėto intereso vertinimo (balanso testo) forma)

TEISĖTO INTERESO VERTINIMAS (BALANSO TESTAS)

Duomenų valdytojas:	
Asmens duomenų tvarkymo tikslas:	
Duomenų kategorijos:	
Vertinimo tipas:	

A) TEISĖTO INTERESO IDENTIFIKAVIMAS

1. Koks yra asmens duomenų tvarkymo tikslas?

2. Ar asmens duomenų tvarkymas yra būtinas siekiant vieno ar kelių organizacinių tikslų?

3. Ar asmens duomenų tvarkymas yra būtinas siekiant vieno ar kelių trečiosios šalies tikslų?

4. Ar BDAR arba kiti teisės aktai numato, kad asmens duomenų tvarkymas nagrinėjamu tikslu yra tvarkymas teisėto intereso pagrindu?

B) BŪTINUMAS

5. Kuo šis duomenų tvarkymas yra svarbus ar būtinas duomenų valdytojui.

6. Kuo šis duomenų tvarkymas yra svarbus ar būtinas kitiems asmenims?

7. Ar yra kitų efektyvių būdų pasiekti tuos pačius tikslus?
C) BALANSAS
8. Ar duomenų subjektas gali pagrįstai tikėtis, kad jo asmens duomenys tvarkomi šiuo tikslu?
9. Ar asmens duomenų tvarkymas prisideda prie duomenų subjektui skirtų prekių/paslaugų gerinimo?
10. Ar tikėtina, kad duomenų tvarkymas neigiamai paveiks duomenų subjekto teises?
11. Ar tikėtina, kad duomenų tvarkymas sukels žalą duomenų subjektui?
12. Ar netvarkant asmens duomenų šiuo tikslu tai neigiamai paveiks duomenų valdytoją?
13. Ar netvarkant asmens duomenų šiuo tikslu tai neigiamai paveiks trečiasis šalis?
14. Ar asmens duomenys tvarkomi duomenų subjekto interesais?
15. Ar teisėtas duomenų valdytojo interesas tvarkyti asmens duomenis šiuo tikslu yra suderinamas su duomenų subjekto interesu?
16. Koks egzistuoja ryšys tarp duomenų subjekto ir duomenų valdytojo?
17. Koku būdu tvarkomi asmens duomenys? Ar Bendrasis duomenų apsaugos reglamentas (ES) 2016/679 nustato specialias tokių asmens duomenų tvarkymo sąlygas?

18. Ar egzistuoja abipusis ryšys tarp duomenų subjekto ir duomenų valdytojo? Jei taip, kiek jis glaudus?
19. Ar asmens duomenys gaunami tiesiogiai iš duomenų subjekto?
20. Ar tarp šalių egzistuoja galios disbalansas?
21. Ar duomenų subjektas yra informuojamas apie jo asmens duomenų tvarkymą? Jei taip, ar pateikta informacija aiški ir suprantama?
22. Ar duomenų subjektas gali daryti įtaką jo duomenų tvarkymui?
23. Ar duomenų tvarkymo apimtis gali būti minimizuota siekiant sumažinti grėsmę privatumui?
D) SAUGUMO PRIEMONĖS
E) IŠVADOS

Data:

Vertinimą atliko:

(Vardas, pavardė, pareigos, parašas)

Asmens duomenų tvarkymo
Sveikatos apsaugos ministerijos
Ekstremalių sveikatai situacijų
centro taisyklių
2 priedas

(Duomenų valdytojo duomenų tvarkymo veiklos įrašų forma)

Duomenų valdytojas:			
Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras (jei taikoma, ir bendro duomenų valdytojo) ar jo atstovo pavadinimas (jei fizinis asmuo – vardas ir pavardė)			
Pašto adresas	Telefono ryšio numeris	Elektroninio pašto adresas	Kitos ryšių priemonės
Duomenų apsaugos pareigūnas:			
Duomenų apsaugos pareigūno vardas ir pavardė			
Pašto adresas	Telefono ryšio numeris	Elektroninio pašto adresas	Kitos ryšių priemonės
Duomenų tvarkymo tikslas			
Duomenų subjektų kategorijų aprašymas			
Asmens duomenų kategorijų aprašymas			
Duomenų gavėjų kategorijos			
Asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai (kai taikoma):			
Trečiosios valstybės arba tarptautinės organizacijos, kuriai perduodami asmens duomenys pavadinimas:		BDAR 49 straipsnio 1 dalies antroje pastraipoje nurodytais duomenų perdavimų atvejais tinkamų apsaugos priemonių dokumentai:	
Kita informacija, susijusi su asmens duomenų perdavimu:			
Numatomi asmens duomenų saugojimo, ištrynimo terminai (kai įmanoma)			
Bendras duomenų saugumo priemonių (nurodytų BDAR 32 straipsnio 1 dalyje) aprašymas (kai įmanoma):			
Techninės saugumo priemonės:		Organizacinės saugumo priemonės:	
Kita informacija			
Duomenų tvarkymo veiklos įrašų užpildymo, atnaujinimo data (-os)			

Asmens duomenų tvarkymo
Sveikatos apsaugos ministerijos
Ekstremalių sveikatai situacijų
centro taisyklių
3 priedas

(Duomenų tvarkymo veiklos įrašų žurnalo forma)

Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras

DUOMENŲ TVARKYMO VEIKLOS ĮRAŠŲ ŽURNALAS

Duomenų apsaugos pareigūnas – _____
(vardas, pavardė, kontaktiniai duomenys)

Eil. Nr.	Asmens duomenų tvarkymo tikslas (pvz., vidaus administravimas ir t. t.)	Asmens duomenų tvarkymo teisinis pagrindas (pvz., sutikimas, sutartinė prievolė, teisinė prievolė, viešasis interesas ir t. t.)	Duomenų subjekto grupės (pvz., darbuotojai, vartotojai ir t. t.)	Asmens duomenų kategorijos* (pvz., vardas, pavardė, asmens kodas ir t. t.)	Duomenų gavėjų kategorijos (pvz., Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos ir t. t.)	Asmens duomenų saugojimo, ištrynimo terminai (pvz., 10 metų po sutarties sudarymo, 14 kalendorinių dienų ir t. t.)	Techninių ir organizacinių saugumo priemonių aprašymas (pvz., darbuotojų konfidencialumo pareiga, antivirusinės programos ir t. t.)	Duomenų šaltiniai (pvz., duomenų subjekto pateikti duomenys ir t. t.)	Darbuotojai (struktūriniai padaliniai), atsakingi už asmens duomenų tvarkymą	Duomenų įvedimo, keitimo data (datos)
1.										
2.										

* Kai taikoma, asmens duomenų perdavimai į trečiąją valstybę arba tarptautinei organizacijai, įskaitant tos trečiosios valstybės arba tarptautinės organizacijos pavadinimą, ir Reglamento (ES) 2016/679 49 straipsnio 1 dalies antroje pastraipoje nurodytais duomenų perdavimų atvejais tinkamų apsaugos priemonių dokumentai.

(Konfidencialumo laikymosi pasižadėjimo forma tretiesiems asmenims)

(vardas, pavardė, pareigos)

**Sveikatos apsaugos ministerijos
Ekstremalių sveikatai situacijų centro
Direktoriui**

KONFIDENCIALUMO LAIKYMOSI PASIŽADĖJIMAS

(data)

(miestas)

Aš,

(vardas, pavardė)

1. Pripažįstu, kad atlikdamas (-a) darbą ir visas kitas pareigas, kurias man gali tekti vykdyti pagal darbo sutartį, valstybės tarnautojo ir valstybės pareigūno funkcijas, paslaugų teikimo sutartį ar vadovybės nurodymą, galiu gauti ir gausiu informacijos, kuri yra išskirtinė Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro nuosavybė.

2. Pasižadu:

2.1 saugoti duomenis, sudarančius Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro konfidencialią informaciją, kurie tapo arba taps žinomi, ir neatskleisti konfidencialios informacijos tretiesiems asmenims nei darbo, funkcijų vykdymo arba paslaugų teikimo sutarties galiojimo metu, nei pasibaigus darbo, funkcijų arba paslaugų teikimo laikotarpiui neatsižvelgiant į priežastis, išskyrus atvejus, kai:

2.1.1 konfidenciali informacija gali būti atskleidžiama darbuotojams, kurie vykdydami darbo funkcijas, turi teisę susipažinti su konfidencialia informacija.

2.1.2 gaunamas Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro direktoriaus leidimas.

2.1.3 to reikalauja Lietuvos Respublikos teisės aktai.

2.2 saugoti sužinotą konfidencialią informaciją ir imtis reikiamų priemonių, kad konfidenciali informacija nebūtų prieinama ir atskleista tretiesiems asmenims;

2.3 naudoti gautą konfidencialią informaciją išskirtinai tik Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro interesams.

2.4 konfidencialios informacijos nekopijuoti, nefotografuoti arba kitu būdu nedauginti, nedaryti jokių pakeitimų ir nenaudoti asmeniniams tikslams arba savo šeimos, giminaičių arba trečiųjų asmenų interesais be aiškaus išankstinio Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro direktoriaus raštiško sutikimo;

2.5 saugoti man patikėtus dokumentus, kuriuose yra duomenys, sudarantys konfidencialią informaciją tokiu būdu, kad tretieji asmenys neturėtų galimybės su jais susipažinti arba pasinaudoti.

3. Patvirtinu, kad:

3.1 man išaiškinta, kad Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro konfidencialią informaciją sudaro visa informacija apibrėžta Konfidencialios informacijos sąraše, su kuriuo esu pasirašytinai supažindintas (-a).

3.2 esu įspėtas (-a), kad pažeidus konfidencialumo pasižadėjimą man grės ir Lietuvos Respublikos teisės aktuose nustatyta atsakomybė.

3.3. konfidencialumo įsipareigojimas galioja 3 metus po darbo santykių, funkcijų vykdymo ar paslaugų teikimo pasibaigimo.

(parašas) (Vardas, pavardė)

Asmens duomenų tvarkymo
Sveikatos apsaugos ministerijos
Ekstremalių sveikatai situacijų
centro taisyklių
5 priedas

Konfidencialios informacijos sąrašas

Eil. Nr.	Konfidencialios informacijos turinys, dokumentas	Duomenų šaltinis/Dokumentą išdavusi įstaiga	Taikomos duomenų apsaugos priemonės	Darbuotojas, sprendžiantis, kuriems asmenims galima disponuoti konfidencialia informacija	Asmenys, kuriems leidžiama disponuoti konfidencialia informacija
1	2	3	4	5	6
1.	Darbo sutartis/ įsakymas dėl priėmimo į pareigas (nurodyta konfidenciali informacija, darbuotojo asmens duomenys, reikalingi įdarbinimo procesui užtikrinti)	Darbo sutartį sudaręs /į pareigas priimamas darbuotojas	Darbo sutartys / įsakymai laikomi dokumentų valdymo sistemoje, saugomi asmens bylose ar archyve	Direktorius	Pagal pareigybes aprašymus, direktoriaus vidaus dokumentais paskirti asmenys
2.	Centro darbuotojų sveikatos duomenys	Visos sveikatos priežiūros paslaugas teikiančios įmonės, Asmens su negalia teisių apsaugos agentūra	Saugoma asmens byloje	Direktorius	Pagal pareigybes aprašymus, direktoriaus vidaus dokumentais paskirti asmenys
3.	Visa informacija, susijusi su Centro darbuotojais (Centro darbuotojų asmens kodai, socialinio draudimo numeriai, tautybė, pilietybė, išsilavinimas, atestacija, asmeniniai kontaktiniai duomenys, darbuotojų darbo užmokestis ir su tuo susijusi informacija, bei kita informacija apie Centro darbuotojus)	Duomenis pateikę darbuotojai / Valstybinio socialinio draudimo fondo valdybos teritoriniai skyriai	Saugoma dokumentų valdymo sistemoje, asmens byloje ir prie buhalterinių dokumentų	Direktorius	Pagal pareigybes aprašymus, direktoriaus vidaus dokumentais paskirti asmenys
4.	Visa informacija, susijusi su gaunama bei siunčiama korespondencija (darbuotojų bet kokiomis priemonėmis (paštu, el. paštu, per kurjerius ir kt.) gaunamus, siunčiamus bei	Įmonės, įstaigos, fiziniai asmenys, Centras	Saugoma dokumentų valdymo sistemoje, administracijoje	Direktorius	Pagal pareigybes aprašymus, direktoriaus vidaus dokumentais paskirti asmenys

	ruošiamus laiškus, atsakymus į užklaimus, kitą korespondenciją)					
5.	Centras ar jo darbuotojų naudojami slaptažodžiai, kt. prisijungimo duomenys, slaptažodžiai, susiję su prisijungimu prie Centro kompiuterinės sistemos, elektroninio pašto, internetinio banko, patalpų signalizacijos ir kt.	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Pagal pareigybės aprašymus, direktoriaus vidaus dokumentais paskirti asmenys
6.	Viešųjų pirkimų vykdymo metu gauta konfidenciali informacija	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Saugoma dokumentų valdymo sistemoje, administracijoje	Direktorius	Pagal pareigybės aprašymus, direktoriaus vidaus dokumentais paskirti asmenys
7.	Inžinerinė dokumentacija (techniniai projektai, kadastriniai duomenys ir pan.)	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Saugoma administracijoje	Direktorius	Pagal pareigybės aprašymus, direktoriaus vidaus dokumentais paskirti asmenys
8.	Bet kokia kita informacija, kurią Centro vidaus dokumentai, Centro direktorius arba jo paskirtas asmuo įvardija kaip konfidencialią	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Saugoma dokumentų valdymo sistemoje, administracijoje	Direktorius	Pagal pareigybės aprašymus, direktoriaus vidaus dokumentais paskirti asmenys
9.	Bet kokia informacija apie Pareiškėjus, kuri darbuotojui buvo atvirai pateikta arba atskleista, nurodant, kad tokia informacija turi būti laikoma konfidencialia	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Saugoma dokumentų valdymo sistemoje, administracijoje	Direktorius	Pagal pareigybės aprašymus, direktoriaus vidaus dokumentais paskirti asmenys
10.	Bet kokia informacija susijusi su bylų nagrinėjimu.	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Centro direktorius ar jo paskirtas atsakingas darbuotojas	Saugoma dokumentų valdymo sistemoje, administracijoje	Direktorius	Pagal pareigybės aprašymus, direktoriaus vidaus dokumentais paskirti asmenys

Taikomos bendros dokumentų, duomenų apsaugos priemonės:

- Dokumentai laikomi rakinamose metalinėse spintose.
- Centro darbuotojų kabinetai yra rakinami. Po darbo valandų Centro patalpos yra rakinamos ir pridudamos apsaugos tarnybai.
- Už raktų apsaugą atsakingi Centro darbuotojai.

(Privatumo pranešimo forma)

PRIVATUMO PRANEŠIMAS

(Duomenų subjekto kategorija ir tvarkomų asmens duomenų tikslas)

Informuojame Jus, kad Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centre (toliau – Centras) asmens duomenys yra tvarkomi laikantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 96/46/EB (toliau – BDAR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, Lietuvos Respublikos elektroninių ryšių įstatymo ir kitų susijusių teisės aktų bei kontroliuojančių institucijų nurodymų, gairių ir rekomendacijų. Norėdami sužinoti daugiau, atidžiai perskaitykite šį pranešimą.

1. Kokia yra šio dokumento paskirtis?

2. Kas yra atsakingas už Jūsų (bei atstovaujamo asmens) asmens duomenų tvarkymą bei apsaugą?

Už Jūsų (ir Jūsų atstovaujamo asmens) asmens duomenų tvarkymą atsakingi:

Duomenų valdytojas: _____

Juridinio asmens kodas: _____

Pašto adresas: _____

Telefono ryšio numeris: _____

Elektroninio pašto adresas: _____

Duomenų apsaugos pareigūnas: _____

3. Kokius duomenis apie Jus renkame, kuo remdamiesi ir kiek laiko juos tvarkome?

Asmens duomenų kategorijos	
Asmens duomenų šaltinis	
Duomenų tvarkymo teisinis pagrindas	
Duomenų tvarkymo terminas	

4. Ar priimame automatizuotus sprendimus? Ar profiliuojame?

5. Kam perduodame Jūsų asmens duomenis? Ar perduodame informaciją apie Jus už Europos Ekonominės erdvės ribų?

6. Kokias teises Jūs turite?

Jei norite imtis žemiau nurodytų veiksmų, prašome kreiptis į Centro duomenų apsaugos pareigūną el. paštu duomenu.sauga@essc.sam.lt, kaip tai nurodyta šiame punkte. Atkreipiame Jūsų dėmesį, jog šioms teisėms taikomos įstatymų numatytos sąlygos ir išimtys. Jūs, kaip duomenų subjektas (bei atstovas), turite teisę:

- Žinoti (būti informuotam) apie savo asmens duomenų tvarkymą – šią teisę įgyvendiname Jums pateikdami susipažinti šį privatumo pranešimą;
- Susipažinti su tvarkomais savo asmens duomenimis;
- Reikalauti ištaisyti savo asmens duomenis;
- Reikalauti ištrinti savo asmens duomenis („teisė būti pamirštam“), jei tai galima pagrįsti bent viena iš priežasčių, numatytų BDAR 17 str. 1 d.;
- Prašyti apriboti savo asmens duomenų tvarkymą, kai taikomas vienas iš atvejų, numatytų BDAR 18 str. 1 d.;
- Reikalauti nesutikti su savo asmens duomenų tvarkymu (BDAR 21 str.).

Jei manote, kad tvarkydami Jūsų asmens duomenis, mes pažeidžiame duomenų apsaugos teisės aktus, turite teisę pateikti skundą Valstybinei duomenų apsaugos inspekcijai paštu L. Sapiegos g. 17, LT-10312, Vilnius, el. paštu ada@ada.lt ar kitais Valstybinės duomenų apsaugos inspekcijos interneto svetainėje (www.vdai.lrv.lt) pateikiamais būdais.

Jeigu Jūs turite klausimų, komentarų ar nusiskundimų, susijusių su tuo, kaip mes renkame, tvarkome Jūsų duomenis, mūsų duomenų apsaugos pareigūnas gali Jums padėti.

Kreiptis dėl savo teisių įgyvendinimo galite Centro nustatyta tvarka. Ši tvarka reglamentuota Centro Duomenų subjektų teisių įgyvendinimo Centro apraše.

Kilus klausimams ar norėdami įgyvendinti savo teises, susisiekite su mumis el. paštu info@essc.sam.lt arba atvykite Centro adresu M. K. Čiurlionio g. 23, LT-44356 Kaunas.

7. Ar šis pranešimas bus atnaujintas?

Šis privatumo pranešimas yra peržiūrimas ir, nustačius poreikį, atnaujinamas bent kartą per metus. Paskutinį kartą pranešimas atnaujintas: _____

Susipažinau:

(parašas)

(vardas, pavardė)

(Sutikimo dėl asmens duomenų tvarkymo forma)

**SVEIKATOS APSAUGOS MINISTERIJOS
EKSTREMALIŲ SVEIKATAI SITUACIJŲ CENTRAS**

SUTIKIMAS DĖL ASMENS DUOMENŲ TVARKYMO

(Data)

(Vieta)

Aš, _____,
(asmens vardas, pavardė/ pavadinimas, gimimo data/ juridinio asmens kodas)

Sutinku, kad duomenų valdytojas Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras (toliau – Centras), buveinės adresas: M. K. Čiurlionio g. 23, LT-44356 Kaunas, el. pašto adresas info@essc.sam.lt. Tvarkytų šiuos mano asmens duomenis:

1. _____
2. _____
3. _____
4. _____

3. Asmens duomenų tvarkymo tikslai:

1. _____
2. _____
3. _____
4. _____

4. Asmens duomenų tvarkymo teisinis pagrindas

5. Duomenų šaltinis. Nurodyti mano duomenys gauti iš

6. Asmens duomenų gavėjai. Mano asmens duomenys gali būti perduoti:

6.1. duomenų tvarkytojams, kurie atlieka tam tikrus darbus ir teikia paslaugas (informacinių technologijų bendrovės, kurios duomenis tvarko, kad užtikrintų informacinių sistemų kūrimą, tobulinimą ir palaikymą; bendrovės, kurios užtikrina pranešimų klientams siuntimą, teikia apsaugos ir kitas paslaugas, įskaitant teisės, finansų, mokesčių, verslo valdymo, personalo administravimo, buhalterinės apskaitos paslaugas);

6.2. teismui, teisėsaugos įstaigoms ar valstybės institucijoms tiek, kiek tokį teikimą nustato teisės aktų reikalavimai (pvz.: antstoliams, teismams ir kt.);

6.3. kitiems fiziniams / juridiniams asmenims mano sutikimu, jei toks sutikimas gaunamas dėl konkretaus atvejo;

6.4. _____.

7. Turiu šias teises: teisę prašyti, kad man būtų leista susipažinti su mano asmens duomenimis ir juos ištaisyti arba ištrinti, teisę apriboti duomenų tvarkymą, teisę nesutikti, kad asmens

duomenys būtų tvarkomi, taip pat teisę į asmens duomenų perkeliamumą. Šias teises galiu įgyvendinti teisės aktų nustatyta tvarka.

8. Turiu teisę bet kada atšaukti sutikimą tvarkyti mano duomenis. Sutikimo atšaukimas nedaro poveikio sutikimu pagrįsto asmens duomenų tvarkymo, atlikto iki sutikimo atšaukimo, teisėtumui.

9. Mano asmens duomenys bus saugomi _____ laikotarpį. Šis terminas gali būti pratęstas, jei asmens duomenys yra naudojami arba gali būti naudojami kaip įrodymai ar informacijos šaltinis ikiteisminiame ar kitokiame tyrime, įskaitant ir Valstybinės duomenų inspekcijos vykdomame tyrime, civilinėje, administracinėje ar baudžiamojoje byloje ar kitais įstatymų nustatytais atvejais. Tokiu atveju asmens duomenys gali būti saugomi tiek, kiek reikalinga šiems duomenų tvarkymo tikslams, ir sunaikinami nedelsiant, kai tampa nebereikalingi.

10. Šie duomenys nebus naudojami automatizuotų sprendimų priėmimui mano atžvilgiu, įskaitant profiliavimą.

11. Aš turiu teisę skusti Centro veiksmus (neveikimą) Valstybinei duomenų apsaugos inspekcijai ir teismui teisės aktų nustatyta tvarka, taip pat skusti teismui Valstybinės duomenų apsaugos inspekcijos veiksmus (neveikimą).

Vardas pavardė

Parašas

Data

Asmens duomenų tvarkymo
Sveikatos apsaugos ministerijos Ekstremalių sveikatai
situacijų centro taisyklių
8 priedas

(Pasitelktų duomenų tvarkytojų ir kitų duomenų gavėjų (gaunančių asmens duomenis pagal duomenų teikimo sutartis) registro forma)

PASITELKTŲ DUOMENŲ TVARKYTOJŲ IR KITŲ DUOMENŲ GAVĖJŲ (GAUNANČIŲ ASMENS DUOMENIS PAGAL
DUOMENŲ TEIKIMO SUTARTIS) REGISTRAS

Eil. Nr.	Bendrovės/įstaigos (duomenų tvarkytojo) pavadinimas	Sutarties objektas	Teikiami asmens duomenys sutarties pagrindu	Kada pasirašyta asmens duomenų tvarkymo sutartis arba priedas prie sutarties arba papildytos sutarties sąlygos

PATVIRTINTA
Sveikatos apsaugos ministerijos
Ekstremalių sveikatai situacijų centro
direktorius 2025 m. birželio d.
įsakymu Nr.

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMO, TYRIMO, PRANEŠIMO APIE JUOS IR DOKUMENTAVIMO TVARKOS APRAŠAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos aprašas (toliau – Tvarkos aprašas) reglamentuoja asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pašalinimo ir pranešimo apie juos ir dokumentavimo tvarką, už šių veiksmų atlikimą atsakingus asmenis ir (ar) padalinius Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centre (toliau – Centras).

2. Tvarkos aprašas parengtas vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1) (toliau – Reglamentas) (ES) 2016/679) 33 ir 34 straipsniais, Europos Parlamento ir Tarybos direktyvos 95/46/EB 29 straipsnio darbo grupės 2017 m. spalio 3 d. patvirtintomis gairėmis dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679 (toliau – 29 straipsnio darbo grupės gairės) ir susijusiomis Valstybinės duomenų apsaugos inspekcijos rekomendacijomis.

3. Tvarkos apraše vartojamos sąvokos:

3.1. **Priežiūros institucija** – Valstybinė duomenų apsaugos inspekcija (toliau – VDAI);

3.2. **Atsakingas darbuotojas** – Centro direktoriaus įsakymu paskirtas darbuotojas, dirbantis pagal darbo sutartį ar valstybės tarnautojas (darbuotojai), atsakingas už asmens duomenų saugumo pažeidimų tyrimą, pašalinimą ir pranešimą apie juos VDAI ir duomenų subjektams.

3.3. kitos Tvarkos apraše vartojamos sąvokos atitinka Reglamente (ES) 2016/679 apibrėžtas sąvokas. Šiuose teisės aktuose jos apibrėžtos taip:

3.3.1. **asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių, arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius;

3.3.2. **asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio netychia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiūsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.

4. Galimi šie asmens duomenų saugumo pažeidimai:

4.1. konfidencialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie jų suteikimas;

4.2. vientisumo pažeidimas – neleistinas arba netyčinis asmens duomenų pakeitimas;

4.3. prieinamumo pažeidimas – neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas.

5. Atsižvelgiant į aplinkybes, saugumo pažeidimas vienu metu gali būti susijęs su asmens duomenų konfidencialumu, vientisumu ir prieinamumu, taip pat su bet koku jų deriniu.

6. Asmens duomenų saugumo pažeidimas gali įvykti dėl šių priežasčių:

6.1. žmogiškoji klaida (pvz., asmens duomenys persiųsti ne tam adresatui, kuriam jie buvo skirti; ne saugojimui skirtose vietose palikti dokumentai, kuriuose yra asmens duomenų; pamesti nešiojami / mobilūs įrenginiai (telefonas, nešiojamas kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys ir kt.);

6.2. vagystė (pvz., pavogti nešiojami / mobilūs įrenginiai, kuriuose saugomi asmens duomenys; pavogtos neautomatinio būdu susisteminčios bylos, kuriose yra asmens duomenų ir kt.);

6.3. kibernetinė ataka (pvz., duomenų bazėje ar informacinėje sistemoje esantys asmens duomenys užšifruojami, naudojant išpirkos reikalaujančią programą; internete paskelbiami informacinių sistemų naudotojų vardai ir slaptažodžiai ir kt.);

6.4. neleistina (neautorizuota) prieiga prie asmens duomenų (pvz., įgaliojimų neturintys asmenys patenka į patalpas, kuriose saugomos bylos su asmens duomenimis; įgaliojimų neturintys asmenys prisijungia prie duomenų bazių ar informacinių sistemų ir kt.);

6.5. įrenginių ar programinės įrangos gedimas, saugos sistemos spragos (pvz., energijos tiekimo nutrūkimas, dėl kurio negalima prieiti prie asmens duomenų; programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas informacinių sistemų naudotojams, klaida ir kt.);

6.6. nenumatytos (force majeure) aplinkybės ir kitos priežastys (pvz., gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys ir kt.).

7. Asmens duomenų saugumo pažeidimas, galintis kelti pavojų asmenų teisėms ir laisvėms yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą (pvz., asmuo gali patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, pakenkta jo reputacijai, prarastas duomenų, kurie laikomi profesine paslaptimi, konfidencialumas ir kt.).

8. Šis Tvarkos aprašas skirtas užtikrinti, kad Centro darbuotojai sugebėtų laiku nustatyti galimus asmens duomenų saugumo pažeidimus bei suprastų, kokie veiksmai privalo būti atlikti valdant juos.

9. Tvarkos aprašo privalo laikytis visi Centro darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino.

10. Šio Tvarkos aprašo rekomenduojama laikytis juridiniams asmenims, esantiems Centro duomenų tvarkytojams (toliau – duomenų tvarkytojai), kuriems pagal Reglamento (ES) 2016/679 33 straipsnio 2 dalį yra nustatyta prievolė pranešti Centrai apie kiekvieną asmens duomenų saugumo pažeidimą.

II SKYRIUS

PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

11. Centro darbuotojas, nustatęs galimą asmens duomenų saugumo pažeidimą arba kai informacija apie galimą saugumo pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio:

11.1. nedelsdamas, bet ne vėliau kaip per 1 valandą nuo pažeidimo paaiškėjimo momento, žodžiu (tiesiogiai ar telefonu) arba elektroniniu paštu informuoja Centro direktorių ar Atsakingą asmenį ir Centro duomenų apsaugos pareigūną;

11.2. užpildo šio Tvarkos aprašo 2 priede nurodytos formos Pranešimą apie asmens duomenų saugumo pažeidimą ir nedelsdamas, bet ne vėliau kaip per 2 valandas nuo saugumo pažeidimo paaiškėjimo momento perduoda jį Centro direktoriui ar Atsakingam asmeniui bei Centro duomenų apsaugos pareigūnui;

11.3. jei įmanoma, imasi priemonių pašalinti saugumo pažeidimą ir (ar) priemonių sumažinti jo sukeltas neigiamas pasekmes.

12. Duomenų tvarkytojas, nustatęs galimą asmens duomenų saugumo pažeidimą, nedelsdamas, bet ne vėliau kaip per 24 valandas nuo pažeidimo paaiškėjimo momento, apie tai praneša Centrai, pateikdamas užpildytą šio Tvarkos aprašo 2 priede nurodytos formos pranešimą apie asmens duomenų saugumo pažeidimą.

13. Tuo atveju, jei terminas nuo momento, kai duomenų tvarkytojui tapo žinoma apie saugumo pažeidimą iki pranešimo Centrai yra ilgesnis nei 24 valandos, duomenų tvarkytojas kartu su pranešimu pateikia Centrai paaiškinimą dėl uždelsto informacijos pateikimo.

14. Duomenų tvarkytojas pateikia visą Centro prašomą informaciją, susijusią su saugumo pažeidimu ir jo tyrimu, per Centro nurodytą laiką.

fIII SKYRIUS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

15. Atsakingas asmuo, gavęs Centro darbuotojo ar duomenų tvarkytojo pateiktą pranešimą apie asmens duomenų saugumo pažeidimą, konsultuodamasis su Centro duomenų apsaugos pareigūnu:

15.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

15.2. jei saugumo pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkia Centro ar duomenų tvarkytojo IT ir kibernetinio saugumo specialistus ar paslaugas teikiančius tiekėjus;

15.3. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

15.4. jei asmens duomenų saugumo pažeidimas padarytas, nustato pažeidimo pobūdį, priežastis, asmens duomenų kategorijas, jų pobūdį ir kiekį, duomenų subjektų kategorijas ir jų kiekį, įvertina padarytą žalą fiziniams asmenims bei tikėtinas pažeidimo pasekmes;

15.5. įvertina, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas saugumo pažeidimas;

15.6. nustato, ar apie saugumo pažeidimą būtina pranešti VDAI;

15.7. nustato, ar apie saugumo pažeidimą būtina pranešti duomenų subjektams.

16. Atliekant asmens duomenų saugumo pažeidimo tyrimą ir siekiant nustatyti, ar pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir turi būti užtikrinamas jų atsekamumas.

17. Jei asmens duomenų saugumo pažeidimas nustatomas, Atsakingas asmuo, konsultuodamasis su duomenų apsaugos pareigūnu papildomai įvertina pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms lygį.

18. Vertinant rizikos lygį, atsižvelgiama į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:

18.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis: nuo padaryto pažeidimo pobūdžio gali priklausyti pavojaus duomenų subjektams dydis;

18.2. asmens duomenų pobūdis, jautrumas ir kiekis – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautrumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavojus;

18.3. galimybė identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiems asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, todėl pažeidimas padarys mažesnę poveikį duomenų subjektams);

18.4. fizinio asmens specifiniai ypatumai – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavojus, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalia turintys asmenys), tuo didesnę poveikį pažeidimas gali jiems padaryti;

18.5. nukentėjusių duomenų subjektų skaičius – nustatomas nukentėjusių asmenų skaičius: kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnis žalos pavojus;

18.6. pasekmės, sukeltos fiziniams asmenims – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumai; taip pat atsižvelgiama į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis.

19. Įvertinus riziką nustatomas vienas iš trijų rizikos tikimybių lygių – maža, vidutinė ar didelė rizikos tikimybė.

20. Atsakingas asmuo, atlikęs asmens duomenų saugumo pažeidimo tyrimą, užpildo šio Tvarkos aprašo 3 priede nurodytos formos Asmens duomenų saugumo pažeidimo tyrimo ataskaitą.

21. Saugumo pažeidimo tyrimo ataskaita yra pateikiama Centro direktoriui ir duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmiais.

22. Atsižvelgiant į saugumo pažeidimo tyrimo ataskaitą, Centro direktorius, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl saugumo pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

23. Sprendžiant asmens duomenų saugumo pažeidimo pašalinimo klausimą, bei tvirtinant priemonių planą, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą. Priklausomai nuo konkrečių pažeidimo aplinkybių, turėtų būti atlikti tokie veiksmai, kaip: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamo / mobilaus įrenginio (telefono, nešiojamo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuriam jie buvo skirti, kuo skubiau kreiptis į jį su prašymu ištrinti atsiųstus asmens duomenis be galimybės juos atkurti; pakeisti prisijungimo prie duomenų bazės ar informacinės sistemos vardus ir slaptažodžius, jeigu jie tapo žinomi tretiesiems asmenims; atkuriant prarastus ar sugadintus asmens duomenis, naudoti atsargines kopijas ir kt.

24. Siekiant apriboti ar sustabdyti asmens duomenų saugumo pažeidimą, būtina kiek įmanoma tiksliau surinkti duomenų ir įrodymų apie įvykusį saugumo incidentą (pvz., kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės ar informacinės sistemos, kam per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su asmens duomenimis ir kt.).

25. Priemonių plane turi būti numatyti veiksmai, nukreipti ne vien į esamo saugumo pažeidimo priežasties pašalinimą, pavojaus fizinių asmenų teisėms ir laisvėms sumažinimą ar pašalinimą, bet taip pat neleisti pasikartoti pažeidimui. Būtina atsižvelgti į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant saugumo pažeidimą bei imtis priemonių tuos trūkumus pašalinti.

IV SKYRIUS

PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

26. Tyrimo metu nustačius, kad asmens duomenų saugumo pažeidimas buvo, Centro direktorius arba Atsakingas darbuotojas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai tapo žinoma apie pažeidimą, apie tai informuoja VDAI, išskyrus atvejus, kai saugumo pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms.

27. VDAI informuojama pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto VDAI direktoriaus 2018 m. liepos 27 d. įsakymu Nr. 1T-72(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“ (su visais aktualiais pakeitimais), nustatyta tvarka ir sąlygomis, užpildant atitinkamą pranešimo apie asmens duomenų saugumo pažeidimą formą, patvirtintą VDAI direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“.

28. Jeigu įvertinus riziką, abejojama, ar asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.

29. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie saugumo pažeidimą VDAI pranešti nereikia, po kurio laiko situacija gali pasikeisti, todėl saugumo pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., pamesta USB atmintinė, kurioje saugomi asmens duomenys, užšifruoti taikant pažangų algoritmą – jeigu yra atsarginės

duomenų kopijos ir nėra pavojaus šifro saugumui, apie tokį saugumo pažeidimą pranešti VDAI nereikia, tačiau jei vėliau paaiškėja, kad gali kilti pavojus šifro saugumui, pažeidimo keliamas pavojus bus vertinamas iš naujo ir apie tokį pažeidimą reikės pranešti VDAI).

30. Tuo atveju, kai, priklausomai nuo pažeidimo pobūdžio, būtina atlikti išsamesnį tyrimą, nustatyti visus svarbius faktus, susijusius su pažeidimu, ir per 72 valandas dėl objektyvių priežasčių nėra įmanoma ištirti padarytą pažeidimą, informacija VDAI teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminį pranešimą.

31. Jeigu po pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai asmens duomenų saugumo pažeidimo nebuvo, apie tai nedelsiant informuojama VDAI.

32. Tuo atveju, kai yra įtariama, kad asmens duomenų saugumo pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą.

V SKYRIUS

PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

33. Tyrimo metu nustatius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Atsakingas asmuo nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo to laiko, kai buvo sužinota apie pažeidimą, praneša apie tai duomenų subjektui, kurio teisėms ir laisvėms gali kilti didelis pavojus.

34. Duomenų subjektas informuojamas tiesiogiai, t. y., siunčiant jam pranešimą paštu, elektroniniu paštu, trumpąja žinute (SMS) ar kitu būdu. Pranešimas duomenų subjektui siunčiamas atskirai nuo kitos siunčiamos informacijos, kaip naujienlaiškiai ar standartiniai pranešimai.

35. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jis turėtų imtis, kad apsisaugotų nuo neigiamų pažeidimo pasekmių. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama ši informacija:

35.1. asmens duomenų saugumo pažeidimo pobūdžio ir tikėtinų pažeidimo pasekmių aprašymas;

35.2. priemonių, kurių ėmėsi Centras, kad būtų pašalintas saugumo pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti aprašymas;

35.3. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

35.4. kita reikšminga informacija, susijusi su pažeidimu, kuri, Atsakingo asmens manymu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

36. Pranešimo apie asmens duomenų saugumo pažeidimą duomenų subjektams teikti nereikia jeigu:

36.1. Centras įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su duomenimis, jie būtų nesuprantami (pvz., asmens duomenų šifravimo priemonės);

36.2. iš karto po pažeidimo Centras ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;

36.3. tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai didelių pastangų, pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi. Tokiu atveju apie pažeidimą viešai paskelbiama Centro interneto svetainėje, spaudoje, pasitelkiami ne vienas, o keli informavimo būdai arba taikomos panašios priemonės, kuriomis duomenų subjektai būtų efektyviai informuojami (pvz., vien tik pranešimas interneto svetainėje nėra efektyvi informavimo priemonė).

37. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie saugumo pažeidimą duomenų subjektams pranešti nereikia, po kurio laiko situacija gali pasikeisti, todėl pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą ir duomenų bazėje esantys asmens duomenys užšifruojami – jei atlikus tyrimą, paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenis ir jokio kito kenksmingo poveikio duomenų bazei nėra, apie saugumo pažeidimą reikės pranešti tik VDAI, tačiau jei vėliau paaiškėja, kad prarastas ne tik duomenų prieinamumas, bet ir konfidencialumas, saugumo pažeidimo keliamas pavojus bus vertinamas iš naujo bei sprendžiama, ar atsižvelgiant į tikėtinas saugumo pažeidimo pasekmes reikia apie jį pranešti duomenų subjektams).

38. Tam tikromis aplinkybėmis, kai tai yra pagrįsta, Centras pasitaręs su teisėsaugos institucijomis ir atsižvelgdamas į teisėtus teisėsaugos interesus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą apie saugumo pažeidimą iki to laiko, kai tai netrukdytų saugumo pažeidimo tyrimams.

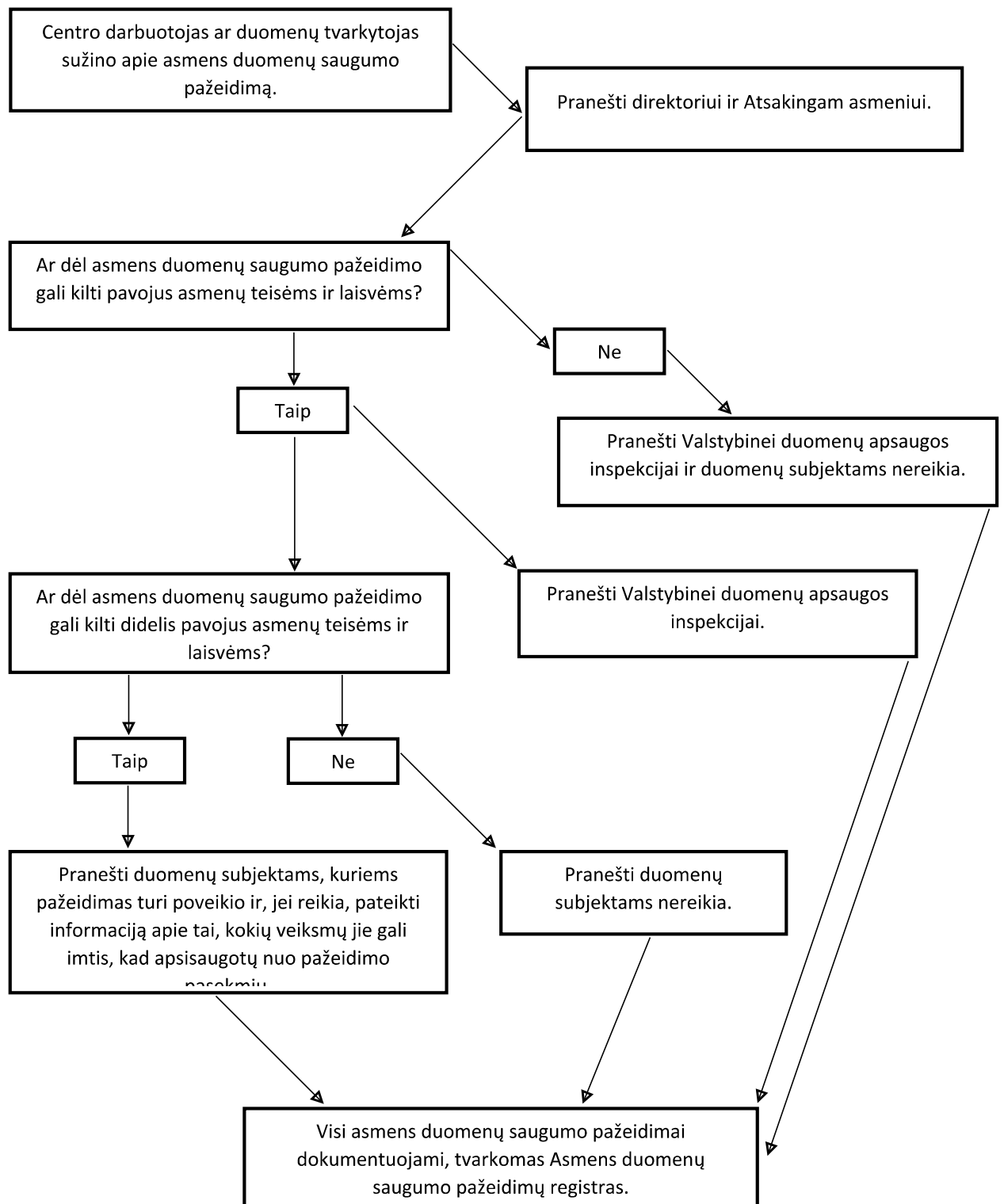
VI SKYRIUS

BAIGIAMOSIOS NUOSTATOS

39. Centro darbuotojai su šiuo Tvarkos aprašu bei jo pakeitimais supažindinami elektroninės dokumentų valdymo sistemos priemonėmis; darbuotojai, kurie neturi prieigos prie elektroninės dokumentų valdymo sistemos, su Tvarkos aprašu supažindinami pasirašytinai.

40. Centro darbuotojai, pažeidę šio Tvarkos aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

REIKALAVIMŲ PRANEŠTI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ VYKDYMO SCHEMA



Asmens duomenų saugumo pažeidimų
nustatymo, tyrimo, pranešimo apie juos
ir dokumentavimo tvarkos aprašo
2 priedas

(Pranešimo apie asmens duomenų saugumo pažeidimą forma)

(juridinio asmens pavadinimas)

(struktūrinio padalinio pavadinimas)

(pareigų pavadinimas)

(vardas, pavardė)

**PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

Nr. _____
(data, dokumento numeris)

Kaunas

Informuoju apie asmens duomenų saugumo pažeidimą, pateikdamas turimą informaciją:

1. Asmens duomenų saugumo pažeidimo nustatymo data, laikas ir vieta:

2. Asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta:

3. Asmens duomenų saugumo pažeidimo esmė ir aplinkybės:

4. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (pvz., Centro darbuotojai, asmenys, pateikę prašymus, skundus, asmenys, užsisakę Centro naujienlaiškius ir kt.) ir apytikslis jų skaičius:

-
-
5. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us):
- ☐ Asmens tapatybę patvirtinantis duomenys (vardas, pavardė, gimimo data, lytis ir kt.)
 - ☐ Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.)
 - ☐ Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.)
 - ☐ Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.)
 - ☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas
 - ☐ Kiti asmens duomenys (įrašyti):
-
-
-
-
-

6. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

7. Kokių veiksmų (priemonių) buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti prisijungimo prie informacinės sistemos slaptažodžiai, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimui skirtose vietose palikti dokumentai su asmens duomenimis ir kt.):

(pareigos)

(parašas)

(vardas ir pavardė)

Asmens duomenų saugumo pažeidimų
nustatymo, tyrimo, pranešimo apie juos ir
dokumentavimo tvarkos aprašo
3 priedas

(Asmens duomenų saugumo pažeidimo tyrimo ataskaitos forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO ATASKAITA

_____ Nr. _____
(data, dokumento numeris)

1. Asmens duomenų saugumo pažeidimo aprašymas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:

Asmens duomenų saugumo pažeidimo data _____ laikas _____

Asmens duomenų saugumo pažeidimo nustatymo data _____ laikas _____

1.2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us):

- ☐ Informacinė sistema
- ☐ Duomenų bazė
- ☐ Tarnybinė stotis
- ☐ Internetinė svetainė
- ☐ Debesų kompiuterijos paslaugos
- ☐ Nešiojami / mobilūs įrenginiai
- ☐ Neautomatiniu būdu susistmintos bylos (archyvas)
- ☐ Kita (įrašyti): _____

1.3. Asmens duomenų saugumo pažeidimo pobūdis (pažymėti tinkamą (-us):

- ☐ Konfidencialumo pažeidimas (neautorizuota prieiga ar atskleidimas)
- ☐ Vientisumo pažeidimas (neautorizuotas asmens duomenų pakeitimas)
- ☐ Prieinamumo pažeidimas (asmens duomenų praradimas, sunaikinimas)

1.4. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us) ir aprašyti):

- ☐ Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.): _____

☐ Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.): _____

☐ Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.):

☐ Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.):

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

☐ Kiti asmens duomenys:

1.5. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (Centro darbuotojai, asmenys, pateikę prašymus, skundus, asmenys, užsisakę Centro naujienlaiškius ir kt.):

1.7. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:

1.8. Darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, telefono numeris, elektroninio pašto adresas):

1.9. Duomenų tvarkytojas, pranešęs apie asmens duomenų saugumo pažeidimą (pavadinimas, kontaktinio asmens duomenys (vardas, pavardė, telefono numeris, elektroninio pašto adresas):

2. Asmens duomenų saugumo pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms įvertinimas

2.1. Specifiniai fizinių asmenų, kurių asmens duomenų saugumas buvo pažeistas, ypatumai (vaikai, asmenys su negalia ir kt.):

2.2. Galimybė identifikuoti fizinį asmenį (pvz., iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užšifruoti, anonimizuoti, arba iki saugumo pažeidimo asmens duomenims šifravimas nebuvo taikomas ir kt.):

2.3. Kas gavo prieigą prie asmens duomenų, kurių saugumas pažeistas?

2.4. Ar buvo kokių kitų įvykių ar aplinkybių, turėjusių poveikį asmens duomenų saugumo pažeidimo padarymui?

2.5. Kokia žala padaryta fiziniams asmenims (duomenų subjektams)?

2.6. Galimos asmens duomenų saugumo pažeidimo pasekmės:

2.6.1. Konfidencialumo pažeidimo atveju (pažymėti tinkamą (-us):

☐ Asmens duomenų išplitimas ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pvz., asmens duomenys išplito internete)

☐ Skirtingos informacijos susiejimas (pvz., gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)

☐ Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pvz., komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)

☐ Kita:

2.6.2. Vientisumo pažeidimo atveju (pažymėti tinkamą (-us):

☐ Pakeitimas į neteisingus duomenis, dėl ko asmuo gali netekti galimybės naudotis paslaugomis

☐ Pakeitimas į kitus duomenis, kad asmens duomenų tvarkymas būtų nukreiptas tam tikra linkme (pvz., pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)

☐ Kita:

2.6.3. Prieinamumo pažeidimo atveju (pažymėti tinkamą (-us):

☐ Dėl asmens duomenų trūkumo negalima teikti paslaugų (pvz., administracinių procesų sutrikdymas, dėl ko negalima prieiti prie tvarkomų asmens duomenų ir įgyvendinti duomenų subjekto teisę susipažinti su jo tvarkomais asmens duomenimis)

☐ Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pvz., tam tikra informacija iš informacinės sistemos išnyko, dėl ko negalima tinkamai suteikti administracinės paslaugos)

☐ Kita:

2.7. Asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis:

☐ Žema rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms)

☐ Vidutinė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra / gali kilti pavojus fizinių asmenų teisėms ir laisvėms)

☐ Didelė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra / gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms)

2.8. Kokių veiksmų / priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?

2.9. Kokios taikytos priemonės, siekiant sumažinti neigiamą poveikį duomenų subjektams?

2.10. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliesiems asmenims?

2.11. Techninės ir / ar organizacinės saugumo priemonės, kurios įgyvendintos dėl asmens duomenų saugumo pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų:

2.12. Techninės ir / ar organizacinės saugumo priemonės, kurios ketinamos įgyvendinti dėl asmens duomenų saugumo pažeidimo, įskaitant ir priemones sumažinti asmens duomenų saugumo pažeidimo pasekmes:

3. Pranešimų apie asmens duomenų saugumo pažeidimą pateikimas

3.1. Ar pranešta Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) apie asmens duomenų saugumo pažeidimą?

☐ Taip

Pranešimo VDAI data numeris

☐ Ne (nurodomos nepranešimo VDAI priežastys):

☐ Apie duomenų saugumo pažeidimą pranešta VDAI vėliau nei per 72 valandas (nurodomos vėlavimo pranešti VDAI priežastys):

3.2. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą?

☐ Taip

Pranešimo duomenų subjektui data numeris (jeigu pranešimas užregistruotas)

Pranešimo duomenų subjektui būdas (pažymėti tinkamą (-us): ☐ paštu ☐ elektroniniu paštu ☐ trumpąja žinute (SMS) ☐ kitais būdais

Informuotų duomenų subjektų skaičius

Pranešimo duomenų subjektui turinys:

☐ Ne (nurodomos nepranešimo duomenų subjektui priežastys):

☐ Apie duomenų saugumo pažeidimą duomenų subjektams pranešta vėliau nei per 72 valandas (nurodomos vėlavimo pranešti duomenų subjektui priežastys):

☐ Apie saugumo pažeidimą pranešta viešai (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta):

3.3. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių (jeigu taip, nurodoma rašto data ir numeris):

Atsakingas asmuo:

(pareigos)	(parašas)	(vardas ir pavardė)

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras
Dokumento pavadinimas (antraštė)	DĖL 2024 M. VASARIO 1 D. SVEIKATOS APSAUGOS MINISTERIJOS EKSTREMALIŲ SVEIKATAI SITUACIJŲ CENTRO DIREKTORIAUS ĮSAKYMO NR. V-8 „DĖL ASMENS DUOMENŲ TVARKYMO SVEIKATOS APSAUGOS MINISTERIJOS EKSTREMALIŲ SVEIKATAI SITUACIJŲ CENTRE TAISYKLIŲ, DUOMENŲ SUBJEKTŲ PRAŠYMŲ, SKUNDŲ IR PAKLAUSIMŲ, SUSIJUSIŲ SU ASMENS DUOMENŲ TVARKYMU, ĮGYVENDINIMO TAISYKLIŲ IR ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMO, TYRIMO, PRANEŠIMO APIE JUOS IR DOKUMENTAVIMO TVARKOS APRAŠO PATVIRTINIMO IR KAI KURIŲ TEISĖS AKTŲ PRIPAŽINIMO NETEKUSIAIS GALIOS“ PAKEITIMO
Dokumento registracijos data ir numeris	2025-06-12 Nr. V-50
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Audronė Sviklaitė Direktorius
Parašo sukūrimo data ir laikas	2025-06-12 14:12
Parašo formatas	Trumpalaikio galiojimo (XAdES-T)
Laiko žymoje nurodytas laikas	2025-06-12 14:12
Informacija apie sertifikavimo paslaugų teikėją	SK ID Solutions EID-Q 2021E
Sertifikato galiojimo laikas	2025-03-05 11:00 - 2030-03-05 23:59
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Laura Butkevičė Vyriausiasis specialistas
Parašo sukūrimo data ir laikas	2025-06-12 15:07
Parašo formatas	Einamojo galiojimo (XAdES-EPES)
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016
Sertifikato galiojimo laikas	2023-02-27 19:18 - 2026-02-27 19:18
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	2
Pagrindinio dokumento pridedamų dokumentų skaičius	0
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	3_Asmens duomenų tvarkymo taisyklės (2).docx
Pridedamo dokumento registracijos data ir numeris	-
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	8_Asmens duomenų saugumo pažeidimų tvarkos aprašas (2).docx
Pridedamo dokumento registracijos data ir numeris	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elpako v.20250605.1
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Tikrinant dokumentą nenustatyta jokių klaidų (2025-07-08)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2025-07-08 nuorašą suformavo Ieva Liutkevičienė

Paieškos nuoroda	-
Papildomi metaduomenys	-