PATVIRTINTA
VšĮ Klaipėdos rajono savivaldybės Gargždų
ligoninės vyriausiosios gydytojos
2019 m. kovo 27 d. įsakymu Nr. 25

VŠĮ KLAIPĖDOS RAJONO SAVIVALDYBĖS GARGŽDŲ LIGONINĖS ASMENS DUOMENŲ PAŽEIDIMŲ APTIKIMO, SUSTABDYMO IR NAGRINĖJIMO TVARKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės (toliau – Įstaiga) asmens duomenų pažeidimų nagrinėjimo taisyklės (toliau – Taisyklės) reguliuoja asmens duomenų pažeidimų nagrinėjimo, pranešimo Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams tvarką. Pranešimai apie asmens duomenų saugumo pažeidimus teikiami Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) ir duomenų subjektams, vadovaujantis:

1.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR) 33 ir 34 straipsniais;

1.2. Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo (toliau – Įstatymas) 29 ir 30 straipsniais.

2. Šioje tvarkoje vartojamos sąvokos atitinka BDAR ir Įstatyme vartojamas sąvokas. Asmens duomenų saugumo pažeidimas šiuose teisės aktuose apibrėžiamas kaip:

2.1. Asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (BDAR 4 straipsnio 12 punktas);

2.2. Asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio neatsargiai arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (Įstatymo 2 straipsnio 2 dalis).

3. Įvykus ar įtariant įvykus asmens duomenų saugumo pažeidimui, Įstaiga, apie asmens duomenų saugumo pažeidimą (toliau – Pažeidimas) praneša Valstybinei duomenų apsaugos Inspekcijai, pateikdama pranešimą apie asmens duomenų saugumo pažeidimą (toliau – Pranešimas), išskyrus, kai tikėtina, kad toks Pažeidimas nekels pavojaus asmenų teisėms ir laisvėms. Kai dėl Pažeidimo pobūdžio ir rizikos rimtumo kyla didelė grėsmė fizinių asmenų teisėms ir laisvėms, duomenų valdytojas apie Pažeidimą privalo pranešti ir duomenų subjektui.

4. Įstaiga, siekiant tinkamai įgyvendinti BDAR reikalavimus susijusius su Pažeidimais, vadovaujasi Europos Parlamento ir Tarybos direktyvos 95/46/EB 29 straipsnio darbo grupės 2017 m. spalio 3 d. parengtomis Pranešimo apie asmens duomenų saugumo pažeidimą gairėmis pagal Reglamentą 2016/679.

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

5. Įstaigos darbuotojas, dirbantis pagal darbo sutartį (toliau – Darbuotojas), vos sužinojęs, kad nebuvo užtikrintas asmens duomenų saugumas:

5.1. nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo asmens duomenų saugumo pažeidimo paaiškėjimo momento informuoja įstaigos vadovą ir duomenų apsaugos pareigūną;

5.2. užpildo Įstaigos patvirtintą Pranešimą apie asmens duomenų saugumo pažeidimą ir nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo pažeidimo paaiškėjimo momento perduoda jį Įstaigos duomenų apsaugos pareigūnui.

5.3. imasi priemonių pašalinti asmens duomenų saugumo pažeidimą ir priemonių galimoms neigiamoms jo pasekmėms sumažinti.

6. Duomenų tvarkytojai, sužinoję apie asmens duomenų saugumo pažeidimą, nedelsiant, bet ne vėliau kaip per 1 darbo dieną, apie tai Įstaigai, pateikdami pranešimą, numatytą Reglamento (ES) 2016/679 33 straipsnio 3 dalyje.

7. Atsakingas už asmens duomenų saugą darbuotojas, gavęs Įstaigos darbuotojo užpildytą pranešimą ar duomenų tvarkytojo pranešimą:

7.1. nedelsiant nagrinėja pranešime nurodytas aplinkybes;

7.2. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

7.3. jei asmens duomenų saugumo pažeidimas padarytas, nustato asmens duomenų kategorijas, įskaitant specialių kategorijų asmens duomenis, kurios buvo susijusios su pažeidimu, pažeidimo priežastys, lėmusios asmens duomenų saugumo pažeidimą, apimtis (duomenų subjektų kategorijos ir skaičius), žala padaryta asmeniui;

7.4. pasitelkia Įstaigos informacines technologijas prižiūrintį asmenį ar išorinį paslaugų teikėją ar duomenų tvarkytojų atstovus, atsakingus už asmens duomenų saugą, jei asmens duomenų saugumo pažeidimas yra susijęs su elektroninės informacijos saugos ir kibernetinio saugumo incidentu;

7.5. nustato, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas (pvz., naudoti atsargines kopijas, siekiant atkurti prarastus ar sugadintus duomenis);

7.6. nustato, ar būtina nedelsiant pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą.

8. Duomenų tvarkytojai pateikia Įstaigai visą jos prašomą informaciją, susijusią su informavimu apie asmens duomenų saugumo pažeidimą ir jo tyrimu, per Įstaigos nurodytą terminą.

9. Duomenų tvarkytojas apie Pažeidimą gali pranešti tiesiogiai VDAI, jeigu tai yra aiškiai numatyta duomenų tvarkymo sutartyje su duomenų valdytoju. Tačiau bet kuriuo atveju teisinę prievolę pranešti VDAI turi duomenų valdytojas.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS

10. Įstaigos duomenų apsaugos pareigūnas, sužinojęs apie galimą Pažeidimą, kaip įmanoma greičiau atlieka pirminį tyrimą, siekiant išsiaiškinti ir nustatyti, ar Pažeidimas iš tikrųjų įvyko, bei kokios galimos pasekmės asmenims (t. y. įvertinti riziką).

11. Galimi asmens duomenų saugumo Pažeidimo tipai:

11.1. „Konfidencialumo Pažeidimas“ – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

11.2. „Prieinamumo Pažeidimas“ – kai netyčia arba neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;

11.3. „Vientisumo Pažeidimas“ – kai asmens duomenys pakeičiami be leidimo ar netyčia. Priklausomai nuo aplinkybių, Pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

12. Priklausomai nuo Pažeidimo tipo, atliekant pirminį tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, išsaugomi esamos situacijos įrodymai bei vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės.

13. Vertinant riziką, kuri gali atsirasti dėl Pažeidimo, atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika vertinama remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus:

13.1. Pažeidimo tipą;

13.2. Asmens duomenų pobūdį, apimtis (pvz., specialių kategorijų asmens duomenys);

13.3. Kaip lengvai identifikuojamas fizinis asmuo;

13.4. Pasekmių rimtumą fiziniams asmenims;

13.5. Specialias fizinio asmens savybes (pvz., duomenys susiję su vaikais ar kitais pažeidžiamais asmenimis);

13.6. Nukentėjusiųjų fizinių asmenų skaičių;

13.7. Specialias duomenų valdytojo savybes (pvz., veiklos pobūdį).

14. Vertinant riziką, laikoma, kad 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., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

15. Įvertinus riziką rekomenduotina nustatyti, kad yra:

15.1. Žema rizikos tikimybė;

15.2. Vidutinė rizikos tikimybė;

15.3. Didelė (aukšta) rizikos tikimybė.

16. Asmens duomenų saugumo pažeidimo ataskaita yra pateikiama Įstaigos vadovui ir duomenų tvarkytojo vadovui, jei asmens duomenų saugumo pažeidimas susijęs su duomenų tvarkytojo tvarkomais asmens duomenimis.

17. Atsižvelgiant į Asmens duomenų saugumo pažeidimo ataskaitą, prireikus priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl asmens duomenų saugumo pažeidimo, tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Įstaigos vadovas.

IV SKYRIUS
PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI

18. Atsakingas už asmens duomenų saugą darbuotojas nedelsiant ir, jei įmanoma, nepraėjus 72 valandoms nuo to laiko, kai buvo sužinota apie asmens duomenų saugumo pažeidimą, informuoja Inspekciją, pateikdamas Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nurodytą informaciją.

19. Jeigu, priklausomai nuo Pažeidimo pobūdžio, duomenų valdytojui yra būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su Pažeidimu (pvz., dar nėra išsiaiškinta Pažeidimo apimtis), ir per 72 val. nuo sužinojimo apie Pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, Pranešimui reikalinga informacija galėtų būti teikiama etapais. Pranešime Inspekcijai yra pateikiama tuo metu prieinama informacija, nurodyta Reglamento (ES) 2016/679 33 straipsnio 3 dalyje, vėlavimo priežastys ir kada bus pateikta kita detalesnė informacija.

20. Esant galimybei, apie informacijos teikimą etapais, VDAI informuojama teikiant pirminį Pranešimą.

21. Tuo atveju, kai asmens duomenų saugumo pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms, apie padarytą asmens duomenų saugumo pažeidimą Inspekcija nėra informuojama.

22. 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.

23. Kai padarytas asmens duomenų saugumo pažeidimas yra susijęs su kibernetiniu incidentu, informacija apie kibernetinį incidentą, susijusį su asmens duomenų saugumo pažeidimu, pateikiama Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytoms valstybės institucijoms šio įstatymo nustatyta tvarka ir atvejais.

24. Jeigu po Pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo jokio Pažeidimo, apie tai nedelsiant turėtų būti informuojama VDAI ir pažymėta Žurnale.

25. Jeigu Pažeidimas paveikia fizinių asmenų duomenis daugiau negu vienoje valstybėje narėje ir yra reikalinga pranešti priežiūros institucijai, duomenų valdytojas turėtų pranešti vadovaujančiai priežiūros institucijai (BDAR preambulės 55 punktas). Jeigu duomenų valdytojas abejoja kuri priežiūros institucija yra vadovaujanti, bet Pažeidimas įvyko Lietuvos Respublikoje, tuomet jis turėtų pranešti VDAI. Šiuo atveju, teikiant Pranešimą, rekomenduotina nurodyti, ar toks Pažeidimas apima ir kitose valstybėse narėse esančias duomenų valdytojo buveines, ir kuriose valstybėse narėse esančius duomenų subjektus Pažeidimas galėjo paveikti.

V SKYRIUS
PRANEŠIMAS DUOMENŲ SUBJEKTUI

26. Atsakingas už asmens duomenų saugą darbuotojas nedelsiant ir, jei įmanoma, nepraėjus 72 valandoms nuo to laiko, kai buvo sužinota apie asmens duomenų saugumo pažeidimą, praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui, kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir

laisvėms, Reglamento (ES) 2016/679 34 straipsnyje nustatyta tvarka, išskyrus šiame straipsnyje numatytas išimtis.

27. Pranešime duomenų subjektui aiškia ir paprasta kalba turėtų būti pateikiama:

27.1. Pažeidimo pobūdžio aprašymas;

27.2. Duomenų apsaugos pareigūno vardas, pavardė (pavadinimas) ir kontaktiniai duomenys;

27.3. Tikėtinų Pažeidimo pasekmių aprašymas;

27.4. Priemonių, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas Pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas (pvz., kad apie Pažeidimą yra informuota VDAI ir, kad yra gautas patarimas dėl Pažeidimo tvarkymo ir jo poveikio sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);

27.5. Kita reikšminga informacija, susijusi su Pažeidimu, kuri, duomenų valdytojo manymu, turėtų būti pateikta duomenų subjektui.

28. Duomenų subjektai apie Pažeidimą informuoti tiesiogiai, siunčiant jiems pranešimą el. paštu, SMS, paštu ar pan. Šis pranešimas turi būti atskirtas nuo kitos siunčiamos informacijos, tokios kaip nuolatiniai atnaujinimai, naujienlaiškiai ar standartiniai pranešimai.

29. Jei tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai daug pastangų, vietoj to apie įvykusį Pažeidimą Įstaiga gali paskelbti viešai arba taikyti panašią priemonę, kuria duomenų subjektai būtų informuojami taip pat efektyviai, pvz., pranešimas žinomos interneto svetainės antraštėje ar pranešimuose, žinomos reklamos spausdintoje žiniasklaidoje.

30. Įstaiga pasirenka tokius pranešimo duomenų subjektui būdus, kurie maksimaliai didintų galimybę tinkamai pranešti informaciją visiems nukentėjusiems asmenims.

31. Įstaiga gali pasirinkti kelis pranešimo duomenų subjektui apie Pažeidimą būdus.

32. Duomenų subjektas gali būti informuojamas apie asmens duomenų saugumo pažeidimą vėliau, nesilaikant šios Tvarkos 26 punkte nustatyto termino, jei yra įgyvendinamos tinkamos priemonės, kuriomis siekiama užkirsti kelią besikartojantiems ar panašiems asmens duomenų saugumo pažeidimams.

33. Duomenų tvarkytojai suteikia Įstaigai pagalbą, kurios reikia, kad būtų tinkamai pranešta apie asmens duomenų saugumo pažeidimą duomenų subjektui.

34. Esant Pažeidimui, pranešimo duomenų subjektui teikti nereikia, jeigu:

34.1. Įstaiga įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikio;

34.2. Iš karto po Pažeidimo Įstaiga ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus asmenų teisėms ir laisvėms;

34.3. Tai pareikalautų neproporcingai daug pastangų susisiekti su asmenimis (pvz., kai jų kontaktiniai duomenys buvo prarasti dėl Pažeidimo arba pirma nežinomi). Tokiu atveju vietoj to apie Pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

35. Duomenų valdytojas turi gebėti įrodyti VDAI, kad jis įvykdė vieną ar daugiau šios Tvarkos 34 punkte nurodytų sąlygų.

36. VDAI informavimas apie Pažeidimą neatleidžia duomenų valdytojo nuo pareigos informuoti duomenų subjektą.

VI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

37. Visi Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, turi būti registruojami duomenų valdytojo Žurnale.

38. Atsakingas už asmens duomenų saugą darbuotojas informaciją apie asmens duomenų saugumo pažeidimą įrašo į šios Tvarkos 3 priede nurodytos formos Asmens duomenų saugumo pažeidimų registravimo žurnalą.

39. Informacija apie Pažeidimą į Žurnalą įvedama nedelsiant, kai tik nustatomas Pažeidimo faktas ir įvertinama rizika (ne ilgiau kaip per 5 darbo dienas). Esant būtinybei, Žurnale esanti informacija turi būti papildoma ir (ar) koreguojama.

40. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

40.1. Visi su Pažeidimu susiję faktai – Pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

40.2. Pažeidimo poveikis ir pasekmės;

40.3. Taisomieji veiksmai (techninės priemonės), kurių buvo imtasi;

40.4. Priežastys dėl su Pažeidimu susijusių sprendimų priėmimo (pvz., kodėl duomenų valdytojas nusprendė nepranešti apie Pažeidimą VDAI ir (ar) duomenų subjektui, t. y. kodėl nusprendė, kad tikėtina, jog Pažeidimas negali sukelti pavojaus fizinių asmenų teisėms ir laisvėms, arba kokią sąlygą įvykdė, kuomet pranešti apie Pažeidimą duomenų subjektui nereikia);

40.5. Pranešimo VDAI pateikimo vėlavimo priežastys (jeigu Pranešimą vėluojama pateikti ar Pranešimas teikiamas etapais);

40.6. Informacija, susijusi su pranešimu duomenų subjektui (pvz., ar buvo pranešta, kodėl nepranešta ir pan.);

40.7. Kita reikšminga, Įstaigos manymu svarbi informacija, susijusi su Pažeidimu (pvz., kad tyrimo metu nustatyta, jog faktiškai Pažeidimo nebuvo, o buvo tik saugumo incidentas).

41. Asmens duomenų saugumo pažeidimų registravimo žurnalas tvarkomas raštu, įskaitant elektroninę formą, ir saugomas pagal Įstaigos patvirtintą dokumentų saugojimo tvarką.

42. Atsakingas už asmens duomenų saugą darbuotojas yra atsakingas už Asmens duomenų saugumo pažeidimų registravimo žurnalo pildymą.

43. Žurnale esantys įrašai periodiškai peržiūrimi siekiant numatyti, kokios prevencijos priemonės turi būti įgyvendintos bei kaip bus kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje analogiški Pažeidimai nesikartotų.

Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo tvarkos
1 priedas

KLAIPĖDOS RAJONO SAVIVALDYBĖS GARGŽDŲ LIGONINĖ

Kodas 163530625, Tilto g. 2, LT-96137 Gargždai. Tel. (8-46) 452476. Faks. (8-46) 453372, el .paštas: info@gargzdul.lt

Valstybinei duomenų apsaugos inspekcijai

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____Nr. _____
(data) (rašto numeris)

1.Asmens duomenų saugumo pažeidimo apibūdinimas

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 / mobilus įrenginiai
☐ Neautomatiniu būdu susistemintos bylos (archyvas)
☐ Kita _____

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

☐ Asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas)
☐ Asmens duomenų vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas)
☐ Asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas)

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

_____

1.5. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (atskiriamos pagal jai būdingą požymį):

_____

_____

1.6. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-as):

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

_____

_____

☐ Specialių kategorijų asmens duomenys (duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, sveikatos duomenys, duomenys apie lytinį gyvenimą ir lytinę orientaciją):

_____

_____

_____

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

_____

_____

☐ Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai (pavyzdžiui, asmens kodas, mokėtojo kodas, slaptažodžiai):

_____

_____

☐ Kiti:

_____

_____

☐ Nežinomi (pranešimo teikimo metu)

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

_____

1.8. Kita duomenų valdytojo nuomone reikšminga informacija apie asmens duomenų saugumo pažeidimą:

_____

_____

_____

_____

_____

2. Galimos asmens duomenų saugumo pažeidimo pasekmės

2.1. Konfidencialumo praradimo atveju:

☐ Asmens duomenų išplitimas labiau nei yra būtina ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pavyzdžiui, asmens duomenys išplito internete)
☐ Skirtingos informacijos susiejimas (pavyzdžiui, gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)
☐ Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pavyzdžiui, komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)
☐ Kita

_____
_____
_____
_____
_____
_____

2.2. Vientisumo praradimo atveju:

☐ Pakeitimas į neteisingus duomenis dėl ko asmuo gali netekti galimybės naudotis paslaugomis
☐ Pakeitimas į galiojančius duomenis, kad asmens duomenų tvarkymas būtų nukreiptas (pavyzdžiui, pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)
☐ Kita

_____
_____
_____
_____
_____
_____

2.3. Duomenų prieinamumo praradimo atveju:

☐ Dėl asmens duomenų trūkumo negalima teikti paslaugų (pavyzdžiui, administracinių procesų sutrikdymas, dėl ko negalima prieiti, pavyzdžiui, prie asmens sveikatos istorijų ir teikti pacientams sveikatos paslaugų, arba įgyvendinti duomenų subjekto teises)
☐ Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pavyzdžiui, asmens sveikatos istorijoje neliko informacijos apie asmens alergijas, tam tikra informacija iš mokesčių deklaracijos išnyko, dėl ko negalima tinkamai apskaičiuoti mokesčių ir pan.)
☐ Kita

_____
_____
_____
_____
_____
_____

2.4. Kita:

3. Priemonės, kurių imtasi siekiant pašalinti pažeidimą ar sumažinti jo pasekmes

3.1. Taikytos priemonės siekiant sumažinti poveikį duomenų subjektams:

3.2. Taikytos priemonės siekiant pašalinti asmens duomenų saugumo pažeidimą:

3.3. Taikytos priemonės siekiant, kad pažeidimas nepasikartotų:

3.4. Kita:

4. Siūlomos priemonės sumažinti asmens duomenų saugumo pažeidimo pasekmems

5. Duomenų subjektų informavimas apie asmens duomenų saugumo pažeidimą

5.1. Duomenys apie informavimo faktą:

☐ Taip, duomenų subjektai informuoti (nurodoma data)_____
☐ Ne, bet jie bus informuoti (nurodoma data)_____
☐ Ne

5.2. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, neinformavimo priežastys:

☐ Ne, nes nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodoma kodėl)

_____

_____

_____

☐ Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami (nurodomos kokios)

_____

_____

_____

_____

☐ Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos kokios)

_____

_____

_____

_____

☐ Ne, nes tai pareikalautų neproporcingai daug pastangų ir apie tai viešai paskelbta (arba taikyta panaši priemonė) (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta)

_____

_____

☐ Ne, nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas

5.3. Informacija, kuri buvo pateikta duomenų subjektams (gali būti pridėtas pranešimo duomenų subjektui kopija):

_____

_____

_____

_____

_____

_____

_____

5.4. Būdas, kokiu duomenų subjektai buvo informuoti:

☐ Paštu
☐ Elektroniniu paštu
☐ Kitu būdu _____

5.5. Informuotų duomenų subjektų skaičius _____

6. Asmuo galintis suteikti daugiau informacijos apie asmens duomenų saugumo pažeidimą (duomenų apsaugos pareigūnas ar kitas kontaktinis asmuo)

6.1. Vardas ir pavardė_____

6.2. Telefono ryšio numeris _____

6.3. Elektroninio pašto adresas _____

6.4. Pareigos _____

6.5. Darbovietės pavadinimas ir adresas _____

_____

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

_____
_____
_____
_____
_____
_____
_____

8. Kita reikšminga informacija

_____
_____
_____
_____
_____
_____
_____
_____
_____

_____	_____	_____
(pareigos)	(parašas)	(vardas, pavardė)

_____

Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo tvarkos
2 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

201__ m. _____ mėn. __ d. Nr. _____

1. Asmens duomenų saugumo pažeidimo aprašymas	
1.1. Asmens duomenų saugumo pažeidimo nustatymo data, valanda (minučių tikslumu) ir vieta	
1.2. Darbuotojas ar duomenų tvarkytojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, telefonas, adresas)	
1.3. Asmens duomenų saugumo pažeidimo padarymo data ir vieta	
1.4. Asmens duomenų saugumo pažeidimo pobūdis, esmė ir aplinkybės	
1.5. Duomenų subjektų kategorijos ir jų skaičius	
1.6. Kaip ilgai tęsėsi asmens duomenų saugumo pažeidimas?	
1.7. Asmens duomenų kategorijos, susijusios su asmens duomenų saugumo pažeidimu:	
1.7.1. Asmens duomenys	
1.7.2. Specialių kategorijų asmens duomenys	
2. Asmens duomenų saugumo pažeidimo rizikos įvertinimas	

2.1. Priežastys, lėmusios asmens duomenų saugumo pažeidimą (pvz., duomenų ar įrangos, kurioje yra saugomi asmens duomenys, vagystė, netinkamos prieigos kontrolės priemonės, leidžiančios neteisėtai naudotis asmens duomenimis, įrangos gedimas, žmogiška klaida, įsilaužimo ataka ir pan.)	
2.2. Asmens duomenų saugumo pažeidimo pasekmės:	
2.2.1. Atsitiktinai arba neteisėtai sunaikinti asmens duomenys	
2.2.2. Atsitiktinai arba neteisėtai prarasti asmens duomenys	
2.2.3. Atsitiktinai arba neteisėtai pakeisti asmens duomenys	
2.2.4. Be duomenų subjekto sutikimo atskleisti asmens duomenys	
2.2.5. Sudaryta galimybė naudotis asmens duomenimis	
2.2.6. Kita	
2.3. Ar pažeistų asmens duomenų pobūdis kelia didesnę žalos riziką?	
2.4. Kas turėjo prieigą prie pažeistų asmens duomenų iki asmens duomenų saugumo pažeidimo padarymo?	
2.5. Kas gavo prieigą prie pažeistų asmens duomenų?	
2.6. Ar buvo kokių kitų įvykių, kurie galėjo turėti poveikį asmens duomenų saugumo pažeidimo padarymui?	
2.7. Ar iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užkoduoti, anonimizuoti ar kitaip lengvai neprieinami?	
2.8. IT sistemos, įrenginiai, įranga, įrašai, susiję su asmens duomenų saugumo pažeidimu	

2.9. Ar tai yra sisteminė klaida ar vienetinis incidentas?	
2.10. Kokia žala buvo padaryta duomenų subjektui ar Įmonei (tapatybės vagystė, grėsmė fiziniam saugumui ir emocinei gerovei, žala reputacijai, teisinė atsakomybė, konfidencialumo, saugumo nuostatų pažeidimas ir pan.)?	
2.11. Kokių veiksmų/priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?	
2.12. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?	
2.13. Techninės ir/ar organizacinės saugumo priemonės, kurios įgyvendintos ar ketinamos įgyvendinti dėl asmens duomenų saugumo pažeidimo	
3. Pranešimų pateikimas	
3.1. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą:	(Pranešimo turinys)
3.1.1. Taip	
3.1.2. Ne	
3.2. Pranešimo duomenų subjektui būdas (elektroninio pašto pranešimu ar SMS pranešimu ir kt.)	
3.3. Ar pranešta Inspekcijai apie asmens duomenų saugumo pažeidimą:	
3.3.1. Taip	(rašto data ir numeris)
3.3.2. Ne	
3.4. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių:	
3.4.1. Taip	(rašto data ir numeris, adresatas)
3.4.2. Ne	

3.5. Ar pranešta valstybės institucijoms, nurodytoms Lietuvos Respublikos kibernetinio saugumo įstatyme, apie kibernetinį incidentą, susijusį su asmens duomenų saugumo pažeidimu:	
3.5.1. Taip	(rašto data ir numeris, adresatas)
3.5.2. Ne	
3.6. Nepranešimo apie asmens duomenų saugumo pažeidimą duomenų subjektui priežastys	
3.7. Vėlavimo pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą priežastys	
3.8. Nepranešimo apie asmens duomenų saugumo pažeidimą Inspekcijai priežastys	
3.9. Vėlavimo pranešti Inspekcijai apie asmens duomenų saugumo pažeidimą priežastys	
Įmonės duomenų apsaugos pareigūnas	(vardas, pavardė, parašas)

Pranešimo apie asmens duomenų saugumo
pažeidimą pateikimo tvarkos
3 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Asmens duomenų saugumo pažeidimo aprašymas	Pradžia (metai, mėnuo, diena, valanda)	Pabaiga (metai, mėnuo, diena, valanda)	Pašalino (vardas, pavardė, parašas)	Įmonės duomenų apsaugos pareigūnas (vardas, pavardė, parašas)