PATVIRTINTA
VšĮ Centro poliklinikos direktoriaus
2019 m. lapkričio 25 d
įsakymu Nr. V-122

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja VšĮ Centro poliklinikos (toliau – poliklinika) asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pašalinimo ir pranešimo apie juos pateikimo duomenų subjektui ir priežiūros institucijai tvarką.

2. Aprašas parengtas vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (ES) 2016/679).

3. Aprašu privalo vadovautis:

3.1. poliklinikos darbuotojai, dirbantys pagal darbo ar kitas sutartis (toliau – darbuotojai);

3.2. darbuotojai, kurie tvarko asmens duomenis arba atlikdami savo pareigas (ar pagal pavedimą) juos sužino.

4. Asmens duomenų saugumo pažeidimu laikomas bet koks saugumo incidentas, dėl kurio įvyksta vienas ar keli toliau numatyti pažeidimai:

4.1. konfidencialumo pažeidimas – netyčinis ar neteisėtas asmens duomenų atskleidimas arba prieigos prie asmens duomenų suteikimas tam teisės neturintiems asmenims, pavyzdžiui, duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo jos gauti, prisijungimo prie duomenų bazės slaptažodžio paviešinimas ir pan.;

4.2. prieinamumo pažeidimas – netyčinis ar neteisėtas prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas, pavyzdžiui, duomenų bazės ištrynimas nesant atsarginės kopijos, laikinas įprastinę poliklinikos veiklą sutrikdęs prieigos prie duomenų praradimas;

4.3. vientisumo pažeidimas – netyčia ar neteisėtai atlikti asmens duomenų pakeitimai, pavyzdžiui, trečiojo asmens, įgijusio neteisėtą prisijungimą prie duomenų bazės, įvykdyti joje esančių įrašų pakeitimai, programinės įrangos ar procedūrų sutrikimai, dėl kurių atsiranda duomenų netikslumų.

5. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos teisės aktuose, reglamentuojančiuose asmens duomenų tvarkymą ir apsaugą.

II SKYRIUS
DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMAS IR ANALIZĖ

6. Poliklinikos darbuotojas, sužinojęs ar pats nustatęs galimą asmens duomenų saugumo pažeidimą arba gavęs informacijos apie galimą asmens duomenų saugumo pažeidimą iš duomenų tvarkytojo ar kito šaltinio:

6.1. kuo skubiau elektroniniu paštu, telefonu, ir (ar) kitomis komunikacijos priemonėmis informuoja savo tiesioginį vadovą ir (ar) poliklinikos duomenų apsaugos pareigūną (toliau – pareigūnas);

6.2. užpildo Pranešimą apie asmens duomenų saugumo pažeidimą (Aprašo 1 priedas) ir nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo saugumo pažeidimo paaiškėjimo momento, perduoda jį pareigūnui arba atsakingam asmeniui;

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

7. Pareigūnas arba paskirtas asmuo, gavęs Pranešimą apie duomenų apsaugos pažeidimą:

7.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

7.2. konsultuojasi (jei reikia) su Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) duomenų apsaugos pareigūnu;

7.3. jei asmens duomenų saugumo pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkia IT specialistus;

7.4. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

7.5. 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 asmens duomenų saugumo pažeidimo pasekmes;

7.6. įvertina, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas saugumo pažeidimas (pvz., naudoti atsargines kopijas, siekiant atkurti prarastus ar sugadintus duomenis ar kt.);

7.7. nustato, ar apie asmens duomenų saugumo pažeidimą būtina pranešti VDAI;

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

8. Atsakingi darbuotojai pateikia pareigūnui arba paskirtam asmeniui, prašomą informaciją, susijusią su asmens duomenų saugumo pažeidimu ir tyrimu, per jo nurodytą terminą.

9. Jei asmens duomenų saugumo pažeidimas nustatomas, pareigūnas arba paskirtas asmuo papildomai įvertina pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms lygį.

10. Vertinant riziką, 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., 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).

11. Vertinant riziką, atsižvelgiama į konkrečias asmens duomenų saugumo pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika vertinama atsižvelgiant į šiuos kriterijus:

11.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis, nuo kurio gali priklausyti pavojaus duomenų subjektams dydis;

11.2. 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);

11.3. 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 mažesnį poveikį duomenų subjektams);

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

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

11.6. pasekmės, sukeltos fiziniams asmenims – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumas; taip pat atsižvelgiama į pasekmių ilgalaikiškumą (jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis).

12. Įvertinus riziką, nustatomas viena iš trijų rizikos tikimybių:

12.1. žema – dėl asmens duomenų saugumo pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms;

12.2. vidutinė – dėl asmens duomenų saugumo pažeidimo yra (gali) kilti pavojus fizinių asmenų teisėms ir laisvėms;

12.3. didelė – dėl asmens duomenų saugumo pažeidimo yra (gali) kilti didelis pavojus fizinių asmenų teisėms ir laisvėms.

13. Pareigūnas arba paskirtas asmuo, atlikęs asmens duomenų saugumo pažeidimo tyrimą, užpildo Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (Aprašo 2 priedas).

14. Asmens duomenų saugumo pažeidimo tyrimo ataskaita pateikiama poliklinikos direktoriui ir duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

15. Atsižvelgiant į Asmens duomenų saugumo pažeidimo tyrimo ataskaitą, poliklinikos 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.

16. Sprendžiant asmens duomenų saugumo pažeidimo pašalinimo klausimą bei tvirtinant priemonių planą, priklausomai nuo konkrečių pažeidimo aplinkybių pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą: 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, 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.

17. Visa gauta, renkama informacija fiksuojama tokiu būdu, kad atliekant vėlesnę peržiūrą būtų galima nustatyti aiškią chronologinę veiksmų seką ir situacijos eigą bei priemones, kurių buvo imtasi.

III SKYRIUS
DUOMENŲ SAUGUMO PAŽEIDIMO PAŠALINIMAS

18. Nustačius, kad įvyko asmens duomenų saugumo pažeidimas pirmiausia būtina imtis priemonių, kad pažeidimas būtų kuo skubiau apribotas (sustabdytas, nutrauktas, pašalintas). Konkretūs veiksmai asmens duomenų saugumo pažeidimui apriboti atliekami įvertinus konkretaus pažeidimo aplinkybes, mastą, specifiką ir kt.

19. Siekiant asmens duomenų saugumo pažeidimą apriboti, gali būti imamasi šių priemonių:

19.1. duomenų ištrynimas nuotoliniu būdu iš pamesto, pavogto ar kitaip prarasto įrenginio;

19.2 duomenų užšifravimas nuotoliniu būdu pamestame, pavogtame ar kitaip prarastame įrenginyje;

19.3. skubus kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti ar kitaip atskleisti duomenys, su prašymu neatidaryti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;

19.4. atskleisto tretiesiems asmenims prisijungimo prie duomenų bazės slaptažodžio pakeitimas;

19.5. prarastų duomenų atkūrimas iš turimos atsarginės kopijos.

IV SKYRIUS
PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

20. Tyrimo metu nustačius, kad asmens duomenų saugumo pažeidimas kelia arba tikėtinai gali kelti pavojų duomenų subjektų teisėms ir laisvėms, pareigūnas arba paskirtas asmuo nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai tapo žinoma apie pažeidimą, apie tai informuojama VDAI.

21. 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“, nustatyta tvarka ir sąlygomis, užpildant Pranešimo apie asmens duomenų saugumo pažeidimo 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“.

22. Išvadą dėl asmens duomenų saugumo pažeidimo buvimo ir rizikos fizinių asmenų teisėms ir laisvėms egzistavimo, pareigūnas arba paskirtas asmuo pateikia poliklinikos direktoriui (ar jo įgaliotam asmeniui), kuris sprendžia dėl tolesnių veiksmų. Jeigu įvertinus riziką abejojama, ar asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.

23. Jeigu įvertinus riziką nustatoma, kad apie asmens duomenų saugumo pažeidimą VDAI pranešti nereikia, tačiau po kurio laiko situacija pasikeičia, saugumo pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turi būti vertinamas iš naujo ir, jeigu reikia, pranešama VDAI (pvz., pamesta USB atmintinė, kurioje saugomi užšifruoti asmens duomenys 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 turi būti vertinamas iš naujo ir apie tokį pažeidimą reikia pranešti VDAI).

24. Tuo atveju, kai pagal asmens duomenų saugumo pažeidimo pobūdį būtina atlikti išsamesnį tyrimą, tačiau per 72 valandas dėl objektyvių priežasčių ištirti padarytą pažeidimą nėra įmanoma, informacija VDAI teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminį pranešimą.

25. Jeigu pateikus VDAI pranešimą ir atlikus tolesnį tyrimą yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo asmens duomenų saugumo pažeidimo, apie tai nedelsiant informuojama VDAI.

26. 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
DUOMENŲ VALDYTOJO PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

27. Tyrimo metu nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, poliklinika nedelsdama ir, jei įmanoma, praėjus ne daugiau kaip per 72 valandoms nuo to laiko, kai buvo sužinota apie pažeidimą, praneša apie tai duomenų subjektui, kurio teisėms ir laisvėms gali kilti didelis pavojus.

28. Duomenų subjektas informuojamas tiesiogiai, teikiant pranešimą, siunčiant jam pranešimą paštu, elektroniniu paštu ar kitu būdu. Pranešimas duomenų subjektui siunčiamas atskirai nuo kitos siunčiamos informacijos, tokios kaip naujienlaiškiai ar standartiniai pranešimai.

29. Pranešime duomenų subjektui pateikiama:

29.1. asmens duomenų saugumo pažeidimo pobūdžio aprašymas;

29.2. pareigūno arba kito kontaktinio asmens vardas, pavardė (pavadinimas) ir kontaktiniai duomenys;

29.3. tikėtinų asmens duomenų saugumo pažeidimo pasekmių aprašymas;

29.4. priemonių, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant (kai tinkama) 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.);

29.5. kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu, kuri, duomenų valdytojo manymu, turėtų būti pateikta duomenų subjektui.

30. Pranešimas duomenų subjektui neprivalomas, jei egzistuoja bet kuri iš šių aplinkybių:

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

30.2. poliklinika, įvykus asmens duomenų saugumo pažeidimui, ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

30.3. pranešimas duomenų subjektams apie įvykusi asmens duomenų saugumo pažeidimą pareikalautų neproporcingai didelių pastangų. Tokiu atveju apie pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

31. Poliklinika, atsižvelgdama į esamas pagrįstas aplinkybes ir teisėtus teisėsaugos institucijų reikalavimus, gali atidėti asmenų, kuriems asmens duomenų saugumo pažeidimas turi poveikio, informavimą iki to laiko, kol tai netrukdys saugumo pažeidimo tyrimui.

VI SKYRIUS
PRANEŠIMAS DUOMENŲ VALDYTOJUI NUO DUOMENŲ TVARKYTOJO

32. Jeigu poliklinika duomenis tvarko kaip duomenų tvarkytojas, o ne valdytojas, tuomet laikosi visų Aprašo II ir III skyriuose nustatytų reikalavimų ir, jeigu sutartyje su duomenų valdytoju nenumatyta kitaip, informuoja duomenų valdytoją apie įvykusį asmens duomenų saugumo pažeidimą.

33. Informuojant duomenų valdytoją apie asmens duomenų saugumo pažeidimą, pateikiama ta pati informacija, kaip ir VDAI. Duomenų valdytojui reikalaujant, teikiama visa kita su pažeidimo tyrimu susijusi informacija, galinti padėti duomenų valdytojui įgyvendinti pareigą pranešti priežiūros institucijai ir (ar) duomenų subjektams.

34. Duomenų valdytojo prašymu poliklinikos darbuotojai privalo bendradarbiauti, teikti visą reikiamą informaciją ir vykdyti visus duomenų valdytojo teikiamus nurodymus duomenų tvarkymo sutartyje nustatyta tvarka.

VII SKYRIUS
DUOMENŲ SAUGUMO PAŽEIDIMO DOKUMENTAVIMAS

35. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale (Aprašo 3 priedas).

36. Informacija apie pažeidimą registruojama nedelsiant, kai tik nustatomas pažeidimo faktas ir įvertinama rizika, bet ne vėliau kaip per 5 darbo dienas.

37. Kai pažeidimas laikytinas pašalintu, pareigūnas arba paskirtas asmuo sudaro prevencinių veiksmų planą, kuriuo būtų siekiama ateityje užkirsti kelią analogiškam ar panašiam pažeidimui įvykti, ir jis pateikiamas poliklinikos direktoriui spręsti dėl jo įgyvendinimo.

38. Reagavimo į duomenų saugumo pažeidimą procedūros schema nustatyta Aprašo 4 priede.

VIII SKYRIUS
ATSAKOMYBĖ

39. Visi darbuotojai privalo būti supažindinti ir vadovautis Aprašu pažeidimo atveju.

40. Asmenys, nesilaikantys arba pažeidę Aprašo reikalavimus, atsako teisės aktų nustatyta tvarka.

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
1 priedas

VIEŠOJI ĮSTAIGA CENTRO POLIKLINIKA

_____
(pareigų pavadinimas)

_____
(vardas, pavardė)

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____
(data, dokumento numeris)

Vilnius

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., darbuotojai, pacientai ir kt.) ir apytikslis jų skaičius (jei žinoma):

_____
_____
_____
_____
_____

5. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us):

☐ 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.)

☐ 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 skirtoje vietoje palikti dokumentai su asmens duomenimis ir kt.):

_____

_____

_____

_____

_____

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

_____

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
2 priedas

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

☐ Interneto svetainė

☐ Debesų kompiuterijos paslaugos

☐ Nešiojami / mobilūs įrenginiai

☐ Neautomatiniu būdu susistemintos 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.):

☐ Kiti asmens duomenys:

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

1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (darbuotojai, pacientai ir kt.):

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

1.8. Darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas, 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.):

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

(pareigos) (vardas, pavardė) (parašas)

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
3 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Pažeidimo nustatymo data, laikas ir vieta	Darbuotojas ar duomenų tvarkytojas, pranešęs apie pažeidimą (vardas, pavardė, pareigos ar pavadinimas)	Pažeidimo padarymo data ir vieta	Pažeidimo pobūdis, priežastys ir kitos aplinkybės	Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius	Asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius	Tikėtinos pažeidimo pasekmės bei pavojus fizinių asmenų teisėms ir laisvėms	Priemonės, kurių buvo imtasi pažeidimui pašalinti ir (ar) neigiamoms pažeidimo pasekmėms sumažinti	Informacija, ar apie pažeidimą buvo pranešta Valstybinei duomenų apsaugos inspekcijai, priimto sprendimo motyvai	Informacija, ar apie pažeidimą buvo pranešta duomenų subjektui (subjektams), priimto sprendimo motyvai	Kita informacija, susijusi su asmens duomenų saugumo pažeidimu
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											

_____

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
4 priedas

REAGAVIMO Į DUOMENŲ SAUGUMO PAŽEIDIMĄ VYKDYMO SCHEMA