PATVIRTINTA
Kelmės turizmo ir verslo
informacijos centro direktoriaus
2020 m. gegužės 4 d. įsakymu Nr. V-4.2

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pašalinimo ir pranešimo apie juos Kelmės turizmo ir verslo informacijos centro (toliau – Įstaiga) 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) (OL 2016 L 119, p. 1) (toliau – Reglamentas (ES) 2016/679).

3. Apraše vartojamos sąvokos:

3.1. **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;

3.2. **Atsakingas asmuo** – Įstaigos direktoriaus įsakymu paskirtas darbuotojas (darbuotojai) savanoris, narys ar kitas asmuo, atsakingas už asmens duomenų saugumo pažeidimų tyrimą, pašalinimą ir pranešimą apie juos Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) ir duomenų subjektams.

3.3. kitos Apraše vartojamos sąvokos atitinka Reglamente (ES) 2016/679 apibrėžtas sąvokas.

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 kokiu 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 skirtoje vietoje 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 neautomatiniu būdu susistemintos 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 prieiga 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 (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 Aprašas skirtas užtikrinti, kad Įstaigos darbuotojai sugebėtų laiku nustatyti galimus asmens duomenų saugumo pažeidimus bei suprastų, kokie veiksmai privalo būti atlikti valdant juos.

9. Aprašo privalo laikytis visi Įstaigos darbuotojai, savanoriai ar nariai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino.

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

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

11. Įstaigos 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 darbo valandą nuo pažeidimo paaiškėjimo momento, žodžiu (tiesiogiai ar telefonu) arba elektroniniu paštu informuoja direktorių ir Atsakingą asmenį;

11.2. užpildo šio Aprašo 2 priede nurodytos formos Pranešimą apie asmens duomenų saugumo pažeidimą ir nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo saugumo pažeidimo paaiškėjimo momento perduoda jį Atsakingam asmeniui;

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 Įstaigai, pateikdamas užpildytą šio 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 Įstaigai yra ilgesnis nei 24 valandos, duomenų tvarkytojas kartu su pranešimu pateikia Įstaigai paaiškinimą dėl uždelsto informacijos pateikimo.

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

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

15. Atsakingas asmuo, gavęs Įstaigos darbuotojo ar duomenų tvarkytojo pateiktą pranešimą apie asmens duomenų saugumo pažeidimą:

15.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

15.2. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

15.3. 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;

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

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

15.6. 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 užtikrinamas jų atsekamumas.

17. Jei asmens duomenų saugumo pažeidimas nustatomas, Atsakingas asmuo 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 mažesnį 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, negalią turintys asmenys), tuo didesnį 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 rimtumas; 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 Aprašo 3 priede nurodytos formos Asmens duomenų saugumo pažeidimo tyrimo ataskaitą.

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

22. Atsižvelgiant į saugumo pažeidimo tyrimo ataskaitą, Įstaigos 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 skirti 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, Atsakingas asmuo 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 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“.

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 nustačius, 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 Įstaiga, 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. Įstaiga 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 Įstaiga 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 Įstaigos 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, Įstaiga pasitarusi su teisėsaugos institucijomis ir atsižvelgdama į teisėtus teisėsaugos interesus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą apie saugumo pažeidimą iki to laiko, kai tai netrukdys saugumo pažeidimo tyrimams.

VI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

39. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale (Aprašo 4 priedas).

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

41. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

41.1. pažeidimo nustatymo aplinkybės (pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);

41.2. pažeidimo aplinkybės (pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

41.3. tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;

41.4. priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;

41.5. informacija apie pranešimą VDAI apie asmens duomenų saugumo pažeidimą:

41.5.1. jei apie asmens duomenų saugumo pažeidimą nebuvo pranešta VDAI, nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta VDAI, nurodoma pranešimo data ir numeris, taip pat, ar pranešimas teikiamas etapais;

41.5.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti VDAI, nurodomos tokio vėlavimo priežastys;

41.6. informacija apie pranešimą duomenų subjektui (subjektams) apie asmens duomenų saugumo pažeidimą:

41.6.1. jei apie asmens duomenų saugumo pažeidimą nebuvo pranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);

41.6.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodomos tokio vėlavimo priežastys;

41.7. kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

42. Asmens duomenų saugumo pažeidimų registravimo žurnalas yra tvarkomas elektronine forma ir saugomas pagal patvirtintą Įstaigos dokumentacijos planą.

43. Už Asmens duomenų saugumo pažeidimų registravimo žurnalo tvarkymą ir saugojimą atsakingas direktorius.

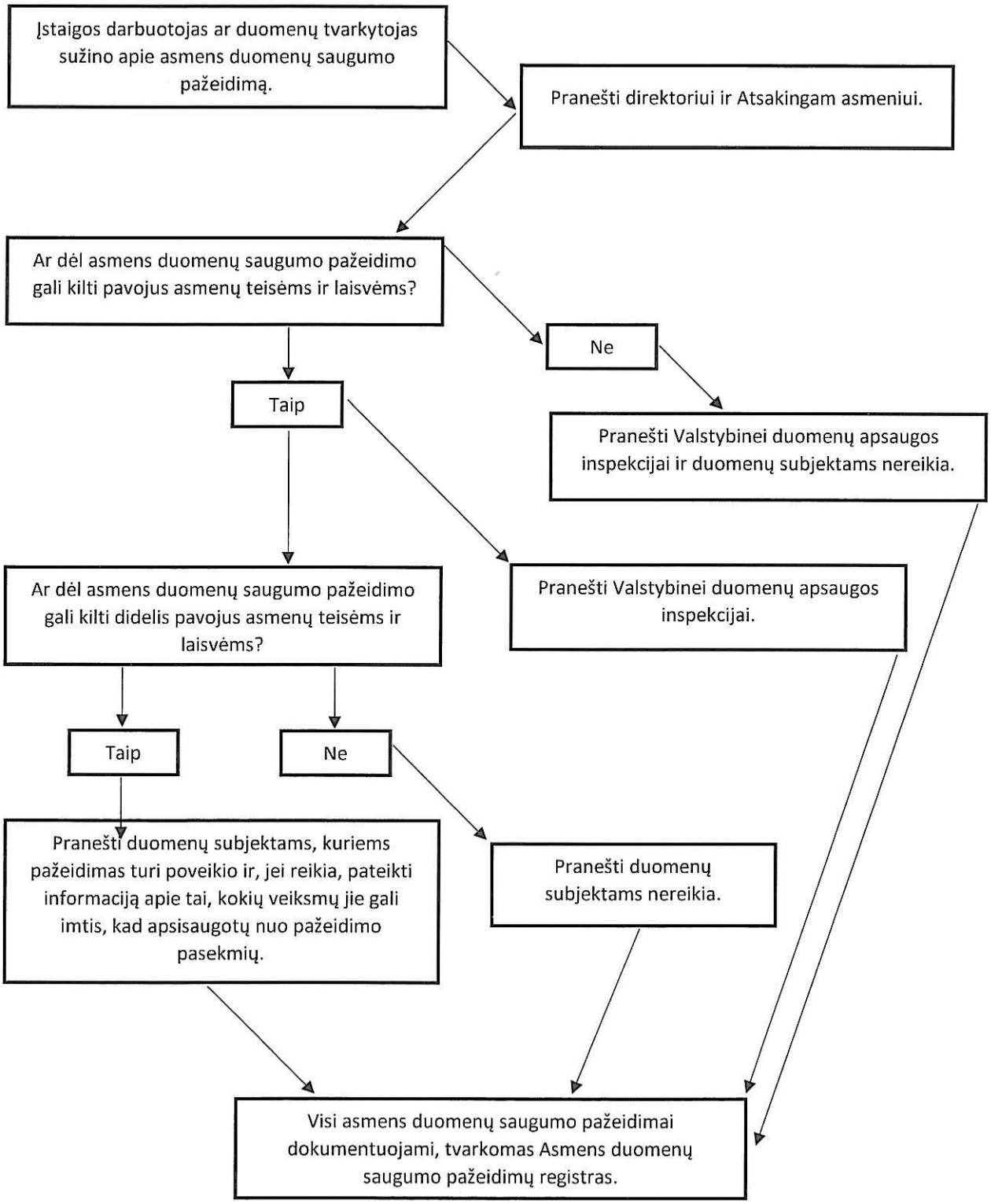
VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

44. Įstaigos darbuotojai su šiuo Aprašu bei jo pakeitimais supažindinami pasirašytinai.

45. Įstaigos darbuotojai, pažeidę šio Aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo 1 priedas

REIKALAVIMŲ PRANEŠTI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ VYKDYMO SCHEMA



Asmens duomenų saugumo pažeidimų
valdymo 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)

Kelmė

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., Įstaigos darbuotojai, nariai, savanoriai ar kiti asmenys, pateikę prašymus, skundus, asmenys, užsisakę Įstaigos naujienlaiškius ir kt.) ir apytikslis jų skaičius:

_____
_____
_____

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.)

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

(pareigos)	(parašas)	(vardas ir pavardė)

Asmens duomenų saugumo pažeidimų
valdymo 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 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.):

_____

_____

_____

☐ 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 (Įstaigos darbuotojai, savanoriai, nariai ar kiti asmenys, pateikę prašymus, skundus, asmenys, užsisakę Įstaigos 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 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):

_____

_____

Atsakingas asmuo:

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

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo 4 priedas

(Asmens duomenų saugumo pažeidimų registravimo žurnalo forma)

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

NEATITIKČIŲ REGISTRAVIMO ŽURNALAS

EIL. NR.	ĮRAŠO APIE NEATITIKTĮ DATA	NEATITIKTIES FIKSAVIMO LAIKAS (ESANT POREIKIUI)	NEATITIKTIES TIPAS	INFORMACIJĄ APIE NEATITIKĮ PATEIKĖ	NEATITIKTIES TURINYS	NEATITIKTIES IDENTIFIKAVIMO ŠALTINIS	PRIEŽASTYS	KOREKCINIS / PREVENCINIS, KOREGAVIMO VEIKSMAS	UŽ NEATITIKTIES PAŠALINIMĄ ATSAKINGI ASMENYS	IŠSPRENDIMO DATA	FAKTINĖ SPRENDIMO DATA	NEATITIKTIES SPRENDIMO STATUSAS	ATLIKTI VEIKSMAI, PRIIMTI SPRENDIMAI (KOMENTARAI)

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo 5 priedas

PAVOJAUS, KYLANČIO FIZINIŲ ASMENŲ TEISĖMS IR LAISVĖMS, VALDYMO PLANAS

VERTINIMO DATA:	
VERTINIMĄ ATLIKO:	

PAVOJUS	PAVOJAUS PRIEŽASTYS IR PASEKMĖS	PLANUOJAMOS VALDYMO PRIEMONĖS	ATSAKINGAS ASMUO	ĮGYVENDINTI IKI	PLANUOJAMI ĮGYVENDINTI VEIKSMAI	ĮGYVENDINTI VEIKSMAI	ĮGYVENDINTŲ VEIKSMŲ VEIKSMINGUMO VERTINIMAS	VERTINIMO ATLIKIMO DATA	VERTINIMĄ ATLIKUSIO ASMENS VARDAS, PAVARDĖ