PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTO PRIE VIDAUS REIKALŲ MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTE PRIE VIDAUS REIKALŲ MINISTERIJOS TVARKOS APRAŠO PATVIRTINIMO

2022 m. d. Nr.
Vilnius

Įgyvendindamas Rekomendacijų, pateiktų vidaus audito 2021 m. lapkričio 30 d. ataskaitoje Nr. 60-8 „Duomenų apsaugos pagal Bendrąjį duomenų apsaugos reglamentą vertinimas“, įgyvendinimo priemonių plano, patvirtinto Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2022 m. vasario 9 d. įsakymu Nr. 1-79 „Dėl vidaus audito 2021 m. lapkričio 30 d. ataskaitoje nr. 60-8 „Duomenų apsaugos pagal Bendrąjį duomenų apsaugos reglamentą vertinimas“ pateiktų rekomendacijų įgyvendinimo priemonių plano patvirtinimo“, 13 priemonę:

1. T v i r t i n u Asmens duomenų saugumo pažeidimų valdymo Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos tvarkos aprašą (pridedama).

2. P a v e d u :

2.1. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos (toliau – Departamentas) struktūrinių ir teritorinių struktūrinių padalinių vadovams:

2.1.1. organizuojant pavaldžių padalinių veiklą, pagal kompetenciją užtikrinti šiuo įsakymu patvirtinto tvarkos aprašo nuostatų laikymąsi;

2.1.2. organizuoti pavaldžių pareigūnų, karjeros valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, supažindinimą su šio įsakymo 1 punktu patvirtintu tvarkos aprašu.

2.2. Departamento duomenų apsaugos pareigūnui kontroliuoti šio įsakymo vykdymą.

2.3. Departamento Komunikacijos skyriui paskelbti šį įsakymą Departamento interneto svetainėje.

Direktoriaus pavaduotojas,
atliekantis direktoriaus funkcijas
Vidaus tarnybos pulkininkas Mindaugas Kanapickas

PATVIRTINTA
Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2022 m. d. įsakymu Nr.

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTE PRIE VIDAUS REIKALŲ MINISTERIJOS TVARKOS APRAŠAS

ISKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos tvarkos aprašas (toliau – Tvarkos aprašas) nustato asmens duomenų saugumo pažeidimų aptikimo, tyrimo, pašalinimo ir pranešimo apie juos teikimo Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI), duomenų subjektui, Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos (toliau – Departamentas) atsakingiems asmenims tvarką.

2. Tvarkos 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) (toliau – Reglamentas), taip pat kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymo reikalavimus.

3. Tvarkos apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente ir Lietuvos Respublikos teisės aktuose.

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, asmens duomenų 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 nešiojamieji / mobilieji įrenginiai (telefonas, nešiojamasis kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys ir kt.);

6.2. vagystė (pvz., pavogti nešiojamieji / mobilieji 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. nenugalimos jėgos *(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. Tvarkos aprašo paskirtis – užtikrinti, kad Departamento pareigūnai, karjeros valstybės tarnautojai ar darbuotojai, dirbantys pagal darbo sutartis (toliau – Departamento darbuotojai), sugebėtų laiku nustatyti galimus asmens duomenų saugumo pažeidimus bei suprastų, kokie veiksmai privalo būti atlikti valdant juos, atsižvelgiant į Reikalavimų pranešti apie asmens duomenų saugumo pažeidimą vykdymo schemą (Tvarkos aprašo 1 priedas).

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

10. Tvarkos aprašo nuostatų rekomenduojama laikytis juridiniams asmenims, sutartinių įsipareigojimų su Departamentu pagrindais esantiems Departamento duomenų tvarkytojais (toliau – duomenų tvarkytojai), kuriems pagal Reglamento 33 straipsnio 2 dalį yra nustatyta prievolė pranešti Departamentui apie kiekvieną asmens duomenų saugumo pažeidimą.

IISKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

11. Departamento darbuotojas, nustatęs galimą asmens duomenų saugumo pažeidimą arba gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio:

11.1. nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo asmens duomenų saugumo pažeidimo sužinojimo momento, žodžiu (tiesiogiai ar telefonu) arba elektroniniu paštu informuoja tiesioginį vadovą ir Departamento duomenų apsaugos pareigūną;

11.2. užpildo Pranešimą apie asmens duomenų saugumo pažeidimą (Tvarkos aprašo 2 priedas) (toliau – pranešimas) ir nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo saugumo pažeidimo sužinojimo momento, perduoda pasirašytą pranešimą Departamento vadovui, kuris rezoliucija nukreipia tolesniam vykdymui Departamento duomenų apsaugos pareigūnui;

11.3. jei įmanoma, nedelsdamas imasi priemonių pašalinti saugumo pažeidimą ir (ar) priemonių sumažinti jo sukeltus neigiamus padarinius.

IIISKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

12. Departamento duomenų apsaugos pareigūnas, šio Tvarkos aprašo 11.1 ir 11.2 papunkčiuose nurodyta tvarka gavęs informaciją apie asmens duomenų saugumo pažeidimą, atlieka šias asmens duomenų saugumo pažeidimo tyrimo procedūras:

12.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

12.2. prireikus konsultuojasi su VDAI;

12.3. jei asmens duomenų saugumo pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkia Departamento struktūrinių padalinių ar duomenų tvarkytojo informacinių technologijų (IT) specialistus ir informacinių sistemų saugos specialistus;

12.4. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

12.5. 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 pažeidimo pasekmes;

12.6. 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.);

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

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

13. Departamento darbuotojai, atsakingi už asmens duomenų tvarkymą, pateikia Departamento duomenų apsaugos pareigūnui visą jo prašomą informaciją, susijusią su asmens duomenų saugumo pažeidimu ir tyrimu, per jo nurodytą terminą.

14. 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.

15. Jei asmens duomenų saugumo pažeidimas nustatomas, Departamento duomenų apsaugos pareigūnas papildomai įvertina pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms lygį.

16. 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:

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

16.2. 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;

16.3. 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);

16.4. 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;

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

16.6. 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.

17. Įvertinus riziką, nustatomas vienas iš trijų rizikos tikimybių lygių: mažas, vidutinis ar didelis.

18. Departamento duomenų apsaugos pareigūnas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, užpildo Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (Tvarkos aprašo 3 priedas).

19. Asmens duomenų saugumo pažeidimo tyrimo ataskaita yra pateikiama Departamento vadovui ir (ar) duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

20. Atsižvelgiant į Asmens duomenų saugumo pažeidimo tyrimo ataskaitą, Departamento vadovas, jei reikia, tvirtina priemonių planą, kuriame numatomos būtinos techninės, organizacinės, administracinės ir kitos priemonės dėl asmens duomenų saugumo pažeidimo pašalinimo, taip pat paskiria atsakingus tokio priemonių plano vykdytojus ir nustato priemonių įgyvendinimo terminus. Šį priemonių planą rengia Departamento duomenų apsaugos pareigūnas.

21. Sprendžiant asmens duomenų saugumo pažeidimo pašalinimo klausimą bei tvirtinant priemonių planą, atsižvelgiant į konkrečias pažeidimo aplinkybes, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamojo / mobiliojo įrenginio (telefono, nešiojamojo 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.

22. Siekiant apriboti ar sustabdyti asmens duomenų saugumo pažeidimą, būtina kiek įmanoma tiksliau surinkti duomenis ir įrodymus 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.).

23. Priemonių plane turi būti numatytos prevencinės ir kitos priemonės, užtikrinančios, kad asmens duomenų saugumo pažeidimas nepasikartotų.

IVSKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

24. Tyrimo metu nustačius, kad asmens duomenų saugumo pažeidimas buvo, Departamento duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai jam tapo žinoma apie pažeidimą, apie tai raštu informuoja VDAI, išskyrus atvejus, kai saugumo pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms.

25. 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“ (toliau – Pranešimas).

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

27. Jeigu įvertinus riziką nustatoma, kad apie 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).

28. Tuo atveju, kai pagal 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.

29. 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.

30. 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.

VSKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

31. Tyrimo metu nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Departamento duomenų apsaugos pareigūnas 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 pavojus.

32. Duomenų subjektas informuojamas tiesiogiai, t. y. siunčiant jam pranešimą paštu arba elektroniniu paštu arba trumpąja žinute (SMS) ar kitu būdu.

33. 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:

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

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

33.3. Departamento duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

33.4. kita reikšminga informacija, susijusi su pažeidimu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

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

34.1. Departamentas 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);

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

34.3. tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai didelių pastangų, pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi.

35. Jeigu įvertinus riziką nustatoma, kad apie saugumo pažeidimą duomenų subjektui pranešti nereikia, tačiau po kurio laiko situacija pasikeitė, pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą, 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).

36. Departamentas, atsižvelgdamas į esamas pagrįstas aplinkybes ir teisėtus teisėsaugos institucijų reikalavimus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą iki to laiko, kol tai netrukdys saugumo pažeidimo ar kitam tyrimui.

VISKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

37. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, registruojami Asmens duomenų saugumo pažeidimų Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos registravimo žurnale (toliau – Asmens duomenų saugumo pažeidimų registravimo žurnalas) (Tvarkos aprašo 4 priedas).

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

39. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

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

39.2. 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);

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

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

39.5. informacija apie (ne)pranešimą VDAI:

39.5.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta 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;

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

39.6. informacija apie pranešimą ar nepranešimą duomenų subjektui (subjektams):

39.6.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta 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);

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

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

40. Asmens duomenų saugumo pažeidimų registravimo žurnalas yra tvarkomas ir saugomas pagal patvirtintą Departamento dokumentacijos planą.

41. Už Asmens duomenų saugumo pažeidimų registravimo žurnalo pildymą, tvarkymą ir saugojimą atsakingas Departamento duomenų apsaugos pareigūnas.

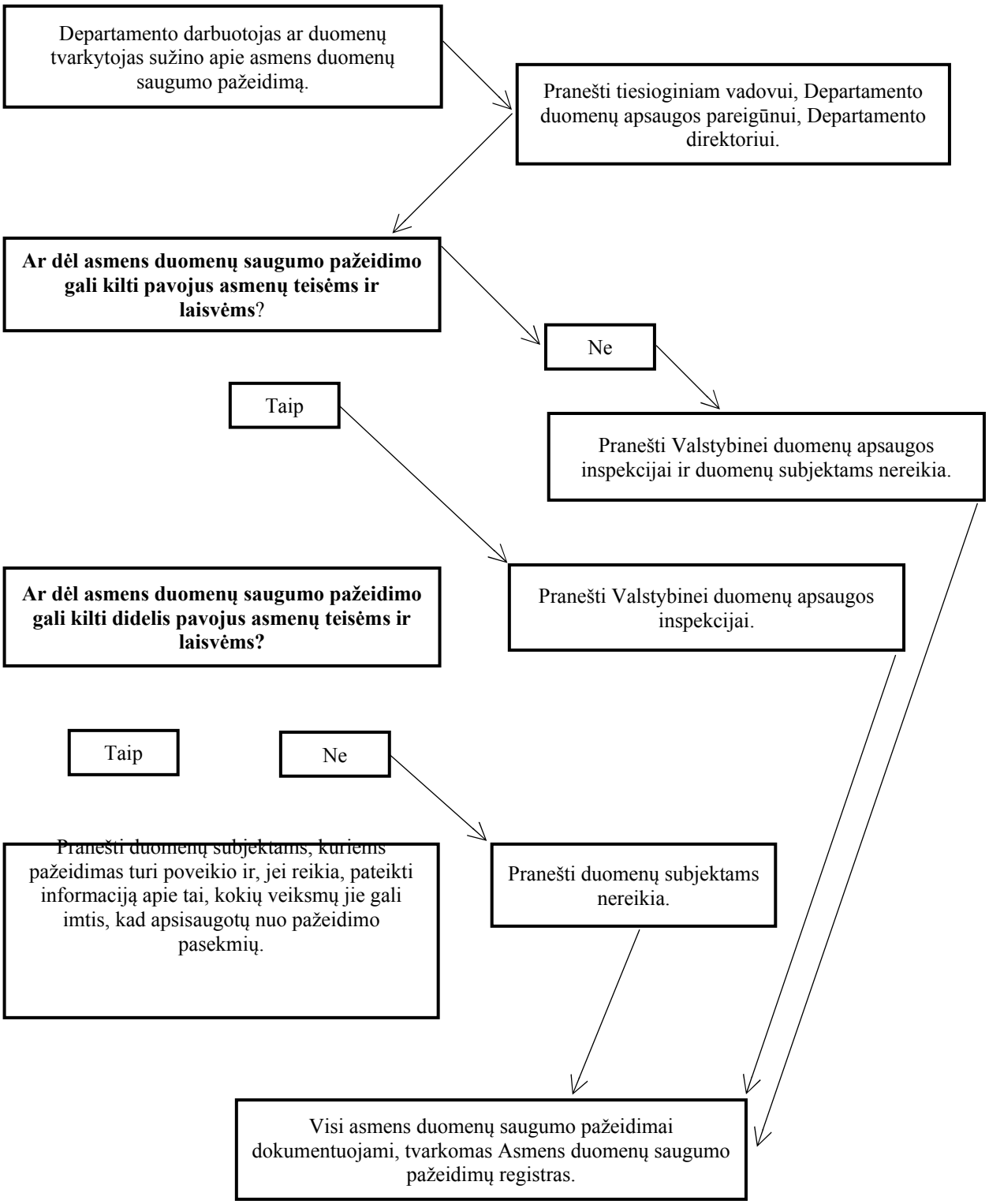
VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

42. Departamento darbuotojai, pažeidę šio Tvarkos prašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____

Asmens duomenų saugumo pažeidimų valdymo Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos tvarkos aprašo
1 priedas

REIKALAVIMŲ PRANEŠTI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ VYKDYMO SCHEMA



_____

Asmens duomenų saugumo pažeidimų valdymo Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos tvarkos aprašo 2 priedas

(Pranešimo apie asmens duomenų saugumo pažeidimą forma)

PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTAS
PRIE VIDAUS REIKALŲ MINISTERIJOS

_____
(struktūrinio padalinio pavadinimas)

_____
(pareigų pavadinimas)

_____
(vardas, pavardė)

Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriui

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ
_____ Nr. _____

(data, dokumento numeris)

(sudarymo viet)

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., Departamento darbuotojai, asmenys, pateikę prašymus, skundus 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.)

☐ Specialiųjų 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 Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos tvarkos aprašo
3 priedas

(Asmens duomenų saugumo pažeidimo tyrimo ataskaitos forma)

PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTAS PRIE VIDAUS REIKALŲ MINISTERIJOS

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 / mobilieji 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.):

☐ Specialiųjų 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 (administracijos darbuotojai, asmenys, pateikę prašymus, skundus ir kt.):

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

____

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

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):

Departamento duomenų apsaugos pareigūnas _____ _____

(Parašas) (Vardas ir pavardė)

Asmens duomenų saugumo pažeidimų valdymo
Priešgaisrinės apsaugos ir gelbėjimo departamente
prie Vidaus reikalų ministerijos tvarkos aprašo
4 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ PRIEŠGAISRINĖS APSAUGOS IR GELBĖJIMO DEPARTAMENTE PRIE VIDAUS REIKALŲ MINISTERIJOS REGISTRAVIMO ŽURNALAS

Eil. Nr.	**Pažeidimo nustatymo data, laikas ir vieta**	**Departamento darbuotojas ar duomenų tvarkytojas, pranešęs apie pažeidimą (vardas,**	**Pažeidimo padarymo data ir vieta**	**linkybės Pažeidimo pobūdis, priežastys ir kitos**	**Duomenų subjektų, kurių asmens duomenų**	**Asmens duomenų, kurių saugumas pažeistas,**	**ns Tikėtinos pažeidimo pasekmės bei pavojus**	**mo Priemonės, kurių buvo imtasi pažeidimui**	**Informacija, ar apie pažeidimą buvo pranešta**	**Informacija, ar apie pažeidimą buvo pranešta duomenų subjektui (subjektams), priimto**	**Kita informacija, susijusi su asmens duomenų**
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Vidaus reikalų ministerijos, Švitrigailos g. 18, LT-03223 Vilnius, Lietuva (2024-12-02 15:06:38)
Dokumento pavadinimas (antraštė)	Dėl Asmens duomenų saugumo pažeidimų valdymo Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos tvarkos aprašo patvirtinimo
Dokumento registracijos data ir numeris	2022-07-14 Nr. 1-426
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Vizavimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Arnoldas Silius, Patarėjas
Parašo sukūrimo data ir laikas	2022-07-13 10:40:33 (GMT+03:00)
Parašo formatas	Xades-C
Laiko žymoje nurodytas laikas	2022-07-13 10:40:35 (GMT+03:00)
Informacija apie sertifikavimo paslaugos teikėją	ADIC CA-A,Asmens dokumentu israsymo centras prie LR VRM,2.5.4.97=#160931383837373833313 5,LT
Sertifikato galiojimo laikas	2020-02-20 11:36:52–2023-02-19 11:36:52
Parašo paskirtis	Suderinimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Nadežda Bakučionienė, Vedėja
Parašo sukūrimo data ir laikas	2022-07-13 11:09:18 (GMT+03:00)
Parašo formatas	Xades-XL
Laiko žymoje nurodytas laikas	2022-07-13 11:09:32 (GMT+03:00)
Informacija apie sertifikavimo paslaugos teikėją	RCSC IssuingCA,VI Registru centras - i.k. 124110246,RCSC,LT
Sertifikato galiojimo laikas	2021-12-21 12:14:46–2023-12-21 12:14:46
Parašo paskirtis	Suderinimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Jūratė Bareišienė, Vedėja
Parašo sukūrimo data ir laikas	2022-07-13 12:40:06 (GMT+03:00)
Parašo formatas	Xades-XL
Laiko žymoje nurodytas laikas	2022-07-13 12:40:14 (GMT+03:00)
Informacija apie sertifikavimo paslaugos teikėją	RCSC IssuingCA,VI Registru centras - i.k. 124110246,RCSC,LT
Sertifikato galiojimo laikas	2021-12-02 16:47:16–2023-12-02 16:47:16
Parašo paskirtis	Suderinimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Jūratė Bareišienė, Vedėja
Parašo sukūrimo data ir laikas	2022-07-13 12:40:54 (GMT+03:00)
Parašo formatas	Xades-XL
Laiko žymoje nurodytas laikas	2022-07-13 12:41:02 (GMT+03:00)
Informacija apie sertifikavimo paslaugos teikėją	RCSC IssuingCA,VI Registru centras - i.k. 124110246,RCSC,LT
Sertifikato galiojimo laikas	2021-12-02 16:47:16–2023-12-02 16:47:16
Parašo paskirtis	Suderinimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Giedrius Sakalinskas, Direktoriaus pavaduotojas

Parašo sukūrimo data ir laikas	2022-07-14 13:17:39 (GMT+03:00)
Parašo formatas	Xades-XL
Laiko žymoje nurodytas laikas	2022-07-14 13:17:45 (GMT+03:00)
Informacija apie sertifikavimo paslaugos teikėją	RCSC IssuingCA,VI Registru centras - i.k. 124110246,RCSC,LT
Sertifikato galiojimo laikas	2021-08-10 09:40:37–2023-08-10 09:40:37
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Mindaugas Kanapickas, Direktoriaus pavaduotojas
Parašo sukūrimo data ir laikas	2022-07-14 13:20:36 (GMT+03:00)
Parašo formatas	Xades-XL
Laiko žymoje nurodytas laikas	2022-07-14 13:20:43 (GMT+03:00)
Informacija apie sertifikavimo paslaugos teikėją	RCSC IssuingCA,VI Registru centras - i.k. 124110246,RCSC,LT
Sertifikato galiojimo laikas	2021-08-03 09:53:58–2023-08-03 09:53:58
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Ieva Raminta Bagdonienė, Vyriausioji specialistė
Parašo sukūrimo data ir laikas	2022-07-14 14:07:55 (GMT+03:00)
Parašo formatas	Xades-C
Laiko žymoje nurodytas laikas	2022-07-14 14:08:05 (GMT+03:00)
Informacija apie sertifikavimo paslaugos teikėją	RCSC IssuingCA,VI Registru centras - i.k. 124110246,RCSC,LT
Sertifikato galiojimo laikas	2021-12-21 13:58:58–2023-12-21 13:58:58
Parašo paskirtis	Susipažinimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Tatjana Jeriomina, Buhalterė
Parašo sukūrimo data ir laikas	2022-07-14 14:44:41 (GMT+03:00)
Parašo formatas	Xades-C
Laiko žymoje nurodytas laikas	2022-07-14 14:44:58 (GMT+03:00)
Informacija apie sertifikavimo paslaugos teikėją	ADIC CA-B,Asmens dokumentu israsymo centras prie LR VRM,2.5.4.97=#160931383837373833313 5,LT
Sertifikato galiojimo laikas	2021-12-16 10:30:34–2024-12-15 10:30:34
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	5
Pagrindinio dokumento pridedamų dokumentų skaičius	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	DocLogix v11.0.0.0
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Tikrinant dokumentą nenustatyta jokių klaidų (2024-12-02 15:06:39)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2024-12-02 15:06:39 atspausdino Giedrė Pesliakienė
Paieškos nuoroda	-
Papildomi metaduomenys	-