



**VILNIAUS LOPŠELIO-DARŽELIO „SAKALĖLIS“
DIREKTORIUS**

**JSAKYMAS
DĖL VILNIAUS LOPŠELIO-DARŽELIO „SAKALĖLIS“ REAGAVIMO Į ASMENS
DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS APRAŠO PATVIRTINIMO**

2023 m. kovo 8 d. Nr V- 13
Vilnius

Vadovaudamas Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu:

1. **T v i r t i n u** Vilniaus lopšelio-darželio „Sakalėlis“ reagavimo į asmens duomenų saugumo pažeidimus procedūros aprašą (pridedama).
2. **I p a r e i g o j u** direktoriaus pavaduotoją ugdymui su šiuo įsakymu ir aprašu supažindinti įstaigos darbuotojus.
3. **Įsakymo vykdymo kontrolę p a v e d u** direktoriaus pavaduotojai ugdymui.

Direktorius

Daiva Riškienė

PATVIRTINTA
Vilniaus lopšelio-darželio „Sakalėlis“
direktoriaus 2023 m. vasario kovo 8 d.
įsakymu Nr. V- 13

**VILNIAUS LOPŠELIO-DARŽELIO „SAKALĖLIS“
REAGAVIMO Į ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS
APRAŠAS**

**I SKYRIUS
BENDROSIOS NUOSTATOS**

1. Reagavimo į asmens duomenų saugumo pažeidimus procedūros aprašas (toliau – Aprašas) nustato Vilniaus lopšelio-darželio „Sakalėlis“, juridinio asmens kodas 190033314, registracijos adresas S. Stanevičiaus g. 86, LT-07105 Vilnius (toliau – Įstaiga) darbuotojų, dirbančių pagal darbo sutartis, veiksmus, įvykus duomenų saugumo pažeidimui, jų išaiškinimo, pranešimo priežiūros institucijai, duomenų subjektams tvarką, pažeidimo prevencinio plano sudarymo bei kitus atvejus, įgyvendinant 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokų duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR) 33 ir 34 straipsnių reikalavimus.

2. Aprašu privalo vadovautis:

2.1. Darbuotojai, dirbantys pagal darbo ar kitas sutartis (toliau – darbuotojai);

2.2. Įstaigos duomenų tvarkytojai, kuriems pavesta laikytis Aprašo duomenų tvarkymo sutartyje nustatyta tvarka ir apimtimi.

3. Darbuotojai privalo užtikrinti, kad Įstaigos pasitelkiami duomenų tvarkytojai, be kitų reikalavimų, numatyti BDAR 28 straipsnyje, būtų įpareigoti laikytis atitinkamų Apraše numatyti reikalavimų, užtikrinančių pareigą duomenų tvarkytojui tinkamai informuoti Įstaigą apie jos pavedimu tvarkomų duomenų pažeidimą, bendradarbiauti aiškinantis duomenų saugumo pažeidimo priežastis, teikti visą reikiamą informaciją, kad Įstaiga galėtų tinkamai įgyvendinti visas duomenų valdytojui tenkančias pareigas, numatytas BDAR.

4. Apraše vartojamos sąvokos:

4.1. **duomenų saugumo pažeidimas** – bet koks įvykis, dėl kurio netičia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga;

4.2. **priežiūros institucija** – valstybės narės pagal BDAR 51 straipsnį įsteigta nepriklausoma valdžios institucija. Įstaigos atžvilgiu tai Valstybinė duomenų apsaugos inspekcija (jmonės kodas 188607912, A. Juozapavičiaus g. 6, 09310 Vilnius, el. paštas ada@ada.lt);

4.3. kitos Apraše vartojamos sąvokos atitinka BDAR įtvirtintas sąvokas.

**II SKYRIUS
I ETAPAS: DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMAS IR ANALIZĖ**

5. Duomenų saugumo pažeidimu (toliau – Pažeidimas) laikomas bet koks saugumo incidentas, dėl kurio įvyksta vienas arba keli toliau numatyti pažeidimai:

5.1. konfidentialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama (gaunama) prieiga tam teisės neturintiems asmenims, pavyzdžiu, duomenų kopijos išsiuntimas trečiam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio paviešinimas, praradimas, atskleidimas kitam darbuotojui, nešiojamojo kompiuterio, kuriame sukaupti duomenys, praradimas, popierinių dokumentų praradimas, vagystė ir pan.;

5.2. pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami. Tokio pobūdžio pažeidimu galėtų būti laikomas duomenų bazės ištrynimas, praradimas (vagystė), sunaikinimas, pavyzdžiu, gaisro, liūties atveju ir nesant atsarginės kopijos, iš kurios būtų galima atkurti prarastus duomenis. Pasiekiamumo pažeidimu laikytinas ir įprastinė Įstaigos veiklą sutrikdės prieigos prie duomenų praradimas;

5.3. vientisumo pažeidimas – netyčia ar neteisėtai atliliki asmens duomenų pakeitimai. Tai galėtų būti trečiojo asmens, įgijusio neteisėtą prisijungimą prie duomenų bazės, įvykdyti joje esančių įrašų pakeitimai, taip pat programinės įrangos ar kitokie procedūrų sutrikimai, dėl kurių atsiranda duomenų netikslumą arba pasikeitimą.

6. Kai yra nustatomas arba įtariamas Pažeidimas, atitinkantis Aprašo 5 reikalavimus, jį nustatęs darbuotojas asmeniškai el. paštu, telefonu ir (arba) kitomis komunikacijos priemonėmis turi kuo skubiau informuoti savo tiesioginį vadovą ir Įstaigos duomenų apsaugos pareigūną (toliau – pareigūnas).

7. Darbuotojas arba jo tiesioginis vadovas Įstaigos direktoriui ir pareigūnui pateikia jam žinomą Pažeidimo nustatymui būtiną informaciją:

7.1. poveikio informacinių technologijų (toliau – IT) infrastruktūrai mastą;

7.2. informacinius išteklius, kuriems gali kilti arba yra kilęs pavoju (kokios duomenų bazės yra arba gali būti paveiktos);

7.3. žinomą arba tikėtiną Pažeidimo trukmę (kada įvyko ir kada buvo sustabdytas arba kada, tikėtina, galima būtų tai padaryti);

7.4. paveiktus arba galimai paveiktus duomenų subjektus ir poveikio jiems mastą (ar paveikti tik konkretios duomenų subjektų grupės duomenys, kokia konkretios grupės dalis yra paveikta ir pan.);

7.5. pradiniaus Pažeidimo pasekmių požymius (pavyzdžiu, prieigos prie duomenų praradimas, nustatyti neteisėti duomenų pakeitimai, rasti paviešinti duomenys ir pan.).

8. Nustatant Pažeidimą ir vykdant jo analizę darbuotojai Pažeidimo tyrimo komisijai arba pareigūnui privalo teikti visapusišką, išsamią, tikslią ir operatyvią informaciją dėl galimo Pažeidimo.

9. Nustačius Pažeidimą, atliekamas pirminis įvykusio galimo Pažeidimo vertinimas ir nustatoma, ar egzistuoja šios aplinkybės:

9.1. prarastas arba gali būti prarastas reikšmingas kiekis asmens duomenų, ypač kai Pažeidimas susijęs su specialių kategorijų duomenimis arba jautresniiais duomenimis, pavyzdžiu, sveikatos duomenimis, religiniai, filosofiniai įsitikinimai, naryste profesinėse sajungose, lytinė orientacija, asmenų teistumu, finansine informacija ir pan. Nereikšmingu kiekiu gali būti laikomas vienkartinis, atsitiktinis duomenų praradimas, pavyzdžiu, elektroninio laiško išsiuntimas ne tam adresatui, popieriaus lapo, bylos praradimas (pametimas);

9.2. Pažeidimas tikėtinai gali kelti didelį pavoju fizinių asmenų teisėms ir laisvėms;

9.3. daromas poveikis dideliams duomenų subjektų skaičiui, ypač kai poveikis daromas labiau pažeidžiamiems duomenų subjektams, pavyzdžiu, vaikams;

9.4. susiklostė bet kokia kita situacija, kuri gali sukelti reikšmingą poveikį duomenų subjektams ir (arba) Įstaigai.

10. Jeigu nustatoma, kad turimais duomenimis Pažeidimas atitinka Aprašo 5 ir 9 punktų kriterijus, pradedama reagavimo į asmens duomenų saugumo pažeidimus procedūra ir Įstaigos direktoriaus įsakymu sudaroma Pažeidimo tyrimo komisija (toliau – Komisija).

11. Komisiją sudaro pareigūnas ir kiti darbuotojai, atsakingi už Pažeidimą arba turintys informacijos apie įvykusį Pažeidimą ir (ar) galintys padėti jį sustabdyti, taip pat kiti Pažeidimui

svarbūs asmenys. Paprastai Komisija sudaroma iš Įstaigos direktoriaus arba jo įgalioto asmens, duomenų apsaugos pareigūno ir direktoriaus pavaduotojo ugdymui.

12. Jeigu Pažeidimas neatitinka Aprašo 5 ir (ar) 9 punkto reikalavimų, Komisija nesudaroma ir vykdoma supaprastinta reagavimo į asmens duomenų saugumo pažeidimus procedūra (toliau – Supaprastinta procedūra). Vykdant Supaprastintą procedūrą visus Pažeidimo išaiškinimo, apribojimo ir kitus būtinus atlikti veiksmus koordinuoja pareigūnas. Atlikus visus būtinus veiksmus Supaprastinta procedūra dokumentuojama ir užpildžius Įstaigos, asmens duomenų saugumo pažeidimų žurnalą (toliau – Žurnalas), kurio forma nustatyta Aprašo 1 priede, užbaigiamą.

13. Vykdant Supaprastintą procedūrą ir nustačius, kad įvykęs Pažeidimas atitinka Aprašo 5 ir 9 punktų kriterijus, pareigūnas teikia siūlymą Įstaigos direktoriui Pažeidimo tyrimui sudaryti Komisiją.

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

III SKYRIUS

II ETAPAS: DUOMENŲ SAUGUMO PAŽEIDIMO APRIBOJIMAS, LIKVIDAVIMAS IR ATKŪRIMAS

15. Nustačius, kad įvyko Pažeidimas pirmiausia būtina imtis priemonių, kad Pažeidimas būtų kuo skubiau apribotas (sustabdytas, nutrauktas, pašalintas). Konkretūs veiksmai Pažeidimui apriboti atliekami įvertinus konkretaus Pažeidimo aplinkybes, mastą, specifiką ir pan. Siekiant Pažeidimą apriboti, gali būti imamas šių priemonių:

15.1. duomenų ištrynimas nuotoliniu būdu iš pamesto, pavogto ar kitaip prarasto įrenginio;
15.2. duomenų užšifravimas nuotoliniu būdu pamestame, pavogtame ar kitaip prarastame įrenginyje;

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

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

15.5. prarastų duomenų atkūrimas iš turimos atsarginės kopijos.

16. Šiame etape būtina imtis atsargumo priemonių siekiant užtikrinti, kad būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį Pažeidimą (pavyzdžiui, užfiksuojama, kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės, kam konkrečiai buvo per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su duomenimis).

17. Veiksmai, skirti ištaisyti arba sumažinti žalą duomenų subjektui, sukeltą Pažeidimo, turėtų būti nukreipti ne vien į esamo Pažeidimo priežasties pašalinimą, bet ir siekiant neleisti Pažeidimui pasikartoti. Turėtų būti nustatytos bent vykdomų procesų, naudojamų sistemų pažeidimo priežastys, dėl kurių ir toliau gali įvykti Pažeidimų arba kurios savaime sudaro prielaidas įvykti Pažeidimui.

18. Esant būtinybei, Įstaiga gali informuoti visuomenę apie Pažeidimo tyrimą, jo rezultatus, priemones, kurių imamas Pažeidimui apriboti ir pan. Visuomenės informavimą vykdo direktoriaus pavaduotoja ugdymui, suderinus poziciją su direktoriumi, pareigūnu ir (ar) kitais Komisijos nariais.

19. Atkūrimo stadioje sistemos turėtų būti pagal galimybes atkurtos į ankstesnę būklę, siekiant užtikrinti Įstaigos veiklos tēstinumą.

IV SKYRIUS

III ETAPAS: DUOMENŲ VALDYTOJO PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

20. Istaiga, kaip duomenų valdytojas, nedelsdamas privalo informuoti Valstybinę duomenų apsaugos inspekciją (toliau – VDAI), jeigu Komisija arba pareigūnas nustato, kad Pažeidimas kelia arba tikėtinai gali kelti pavoju duomenų subjektą, paveiktą Pažeidimo, teisėms ir laisvėms. Pavoju keliančiu laikytinas toks Pažeidimas, dėl kurio, laiku nesiėmus tinkamų priemonių, duomenų subjektas galėtų patirti kūno sužalojimą, materialinę ar nematerialinę žalą, teisių apribojimą, diskriminaciją, galėtų būti pavogta ar suklastota asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta jo reputacijai, prarastas asmens duomenų, kurie laikomi profesine paslaptimi, konfidencialumas arba padaryta kita turtinė, neturtinė ar socialinė žala.

21. Vertinant pavoju duomenų subjektui atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Pavoju turėtų būti vertinamas remiantis objektyviai ir atsižvelgiant į šiuos kriterijus:

- 21.1. Pažeidimo tipą;
- 21.2. asmens duomenų kategorijas (pavyzdžiui, specialių kategorijų asmens duomenys, duomenys apie apkaltinamuosius nuosprendžius, jautresni duomenys, finansiniai duomenys);
- 21.3. kaip lengvai gali būti identifikuojamas duomenų subjektas;
- 21.4. pasekmį rimtumą duomenų subjektams;
- 21.5. specialias duomenų subjekto savybes (pavyzdžiui, duomenys, susiję su vaikais ar kitais pažeidžiamais asmenimis);
- 21.6. paveiktą duomenų subjektų skaičių;
- 21.7. specialias duomenų valdytojo savybes (pavyzdžiui, veiklos pobūdį).

22. Įvertinus riziką duomenų subjekto teisėms ir laisvėms nustatomos šios rizikos rūšys:

- 22.1. nėra rizikos;
- 22.2. maža;
- 22.3. vidutinė;
- 22.4. didelė.

23. Išvadą dėl Pažeidimo buvimo ir rizikos fizinių asmenų teisėms ir laisvėms egzistavimo Komisija arba pareigūnas pateikia Istaigos direktoriui (ar jo įgaliotam asmeniui), kuris sprendžia dėl tolesnių veiksmų. Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie Pažeidimą VDAI, rekomenduotina pranešti. Pranešimo priežiūros institucijai forma nustatyta Aprašo 2 priede.

24. Jei Pažeidimas kelia pavoju (riziką) duomenų subjektų teisėms ir laisvėms, pareigūnas ne vėliau kaip per 72 valandas nuo Istaigos sužinojimo (nustatymo) apie Pažeidimą momento VDAI pateikia tokią informaciją:

- 24.1. Pažeidimo pobūdį, išskaitant, jeigu įmanoma, atitinkamai paveiktą duomenų subjektų kategorijas ir apytkslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytkslį skaičių;
- 24.2. tikėtinų Pažeidimo pasekmį aprašymą;
- 24.3. priemones, kurių įmėsi arba planuoja imtis Istaiga tam, kad būtų pašalintas Pažeidimas;
- 24.4. priemones galimoms neigiamoms Pažeidimo pasekmėms duomenų subjektui sumažinti;
- 24.5. informaciją, ar apie įvykusį Pažeidimą pranešta duomenų subjektams;
- 24.6. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis.

25. Jeigu visos informacijos VDAI neįmanoma pateikti vienu metu arba aiškinamasi Pažeidimo priežastis, tolesnė informacija nepagrįstai nedelsiant gali būti teikiama etapais. Apie tai, kad informacija bus teikiama etapais, VDAI informuojama pirminiaime pranešime.

26. Jeigu po pranešimo VDAI pateikimo atlikus tolesnį tyrimą yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvvo jokio Pažeidimo, apie tai nedelsiant informuojama VDAI ir tai pažymima Žurnale.

27. Jeigu Pažeidimas paveikia arba gali paveikti duomenų subjektų duomenis daugiau negu vienoje valstybėje narėje ir yra reikalinga pranešti priežiūros institucijai, įstaiga turėtų pranešti vadovaujančiai priežiūros institucijai (BDAR preambulės 55 punktas). Jeigu abejojama, kuri priežiūros institucija yra vadovaujanti, bet Pažeidimas įvyko Lietuvos Respublikoje, tuomet pranešama VDAI. Šiuo atveju, teikiant pranešimą, rekomenduotina nurodyti, ar toks Pažeidimas apima ir kitose valstybėse narėse esančias duomenų valdytojo buveines ir kuriose valstybėse narėse esančius duomenų subjektus Pažeidimas galėjo paveikti.

V SKYRIUS

IV ETAPAS: DUOMENŲ VALDYTOJO PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

28. Kai nustatoma, kad įvyko Pažeidimas, atitinkantis Aprašo 5 ir 9 punktų reikalavimus, ir dėl jo gali kilti didelis pavojas duomenų subjektų teisėms ir laisvėms, įstaiga nepagrįstai nedelsdamas, bet ne vėliau kaip per 72 valandas nuo Pažeidimo paaiškėjimo momento informuoja duomenų subjektus, kurių teisėms ir laisvėms gali kilti didelis pavojas.

29. Didelį pavoju keliančiu gali būti laikomas bet kuris 20 punkte nurodytų pasekmį riziką keliantis Pažeidimas tada, jei tokios Pažeidimo pasekmės yra labai tikėtinos, tvarkomi jautrūs asmens duomenys (pavyzdžiui, duomenys apie sveikatą), Pažeidimas turi neigiamą poveikį dideliam duomenų subjektų skaičiui ir pan.

30. Įstaiga, informuodama duomenų subjektus, teikia pranešimą, kurio forma nustatyta Aprašo 3 priede, ir aiškia, paprasta kalba aprašo Pažeidimo pobūdį bei pateikia bent jau toliau nurodytą informaciją:

30.1. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis arba pareigūno kontaktus;

30.2. Pažeidimo aprašymą;

30.3. tikėtinų Pažeidimo pasekmį duomenų subjektui aprašymą;

30.4. priemones, kurių ēmësi arba planuoja imtis įstaiga tam, kad būtų pašalintas Pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti;

30.5. kitą reikšmingą informaciją, susijusią su Pažeidimu, kuri gali būti reikšminga duomenų subjektui.

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

31.1. Įstaiga įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytojas asmens duomenims, kuriems Pažeidimas turėjo poveikį, visų pirmą tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės;

31.2. Įstaiga, įvykus Pažeidimui, ēmësi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojas duomenų subjektų teisėms ir laisvėms;

31.3. pranešimas duomenų subjektams apie įvykusį Pažeidimą pareikalautų neproporcingai didelių pastangų. Tokiu atveju apie Pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

32. Gavusi priežiūros institucijos reikalavimą informuoti duomenų subjektus apie Pažeidimą, įstaiga nedelsdamas ji vykdo.

VI SKYRIUS
PRANEŠIMAS DUOMENŲ VALDYTOJUI NUO DUOMENŲ TVARKYTOJO

33. Jeigu Įstaiga duomenis tvarko kaip duomenų tvarkytoja, o ne valdytoja, tuomet Įstaiga laikosi visų Aprašo II ir III skyriuose nustatyti reikalavimų ir, jeigu sutartyje su duomenų valdytoju nenumatytą kitaip, informuoja duomenų valdytoją apie įvykusį Pažeidimą.

34. Informuojant duomenų valdytoją apie Pažeidimą pateikiama visa Aprašo 24 punkte nurodyta informacija. Duomenų valdytojui reikalaujant, teikiama visa kita su Pažeidimo tyrimu susijusi informacija, galinti padėti duomenų valdytojui įgyvendinti pareigą pranešti priežiūros institucijai ir (ar) duomenų subjektams.

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

VII SKYRIUS
V ETAPAS: DUOMENŲ SAUGUMO PAŽEIDIMO DOKUMENTAVIMAS IR
PROCEDŪROS UŽBAIGIMAS

36. Kai Pažeidimas laikytinas pašalintu, o visiems reikiamiems asmenims apie Pažeidimą yra pranešta arba nustatyta ir dokumentuota, kodėl ši pareiga Įstaigai netaikoma, Komisijos įgaliotas asmuo arba pareigūnas sudaro prevencinių veiksmų planą, kuriuo būtų siekiama ateityje užkirsti kelią analogiškam ar panašiam Pažeidimui įvykti, ir jis pateikiamas Įstaigos direktoriui spręsti dėl jo įgyvendinimo.

37. Sudarius ir Įstaigos direktoriui patvirtinus prevencinių veiksmų planą, taip pat Pažeidimą užfiksavus Žurnale, Procedūra laikoma baigta.

38. Procedūros dokumentai turi būti saugomi teisés aktų nustatyta tvarka.

39. Reagavimo į duomenų saugumo pažeidimus procedūros schema nustatyta 4 priede.

VIII SKYRIUS
ATSAKOMYBĖ

40. Visi darbuotojai privalo būti supažindinti ir vadovautis Aprašu Pažeidimo atveju.

41. Aprašo 20, 26, 28, 30 ir 33 punktuose nurodytą Įstaigos pareigą informuoti VDAI, duomenų subjektus arba duomenų valdytojus įgyvendina pareigūnas arba kitas Komisijos įgaliotas asmuo.

42. Asmenys, nesilaikantys arba pažeidę Aprašo reikalavimus, atsako teisés aktų nustatyta tvarka.

Reagavimo į asmens duomenų
saugumo pažeidimus procedūros
aprašo 1 priedas

Su pažeidimu susijusi informacija		Pažeidimo poveikis ir pasekmės		Taisomieji velksmai									
Pažei di mo dat a, tik slu nu sta ty mo lai kas	Eilės nr.	Kai P buv o duo men tik slu s subj ekt skai čius	P buv ie duo men o subj ekt skai čius	Kok ie duo men apraš ymas prie žasti s	Pažei idim duo men o subj ekt skai čius	Ar visi klient ai ir men duo men on nalo na subj ekt skai čius	Priem onės pažei darbu dimui jautr umas not men ys apie paže idim a?	VDAI infor mavi apsa ugos insp ekci ja sum žinti otojai buvo infor muoti ?	Ar duom enų subj ekt skai čius	Duome nų subjekt o neinf orma vimo / vėlav i ja sum žinti sum žinti buvo infor muoti ?	Ar duom enų subje ktai infor mavim vimo / vėlavim ja (tol mo au- VD AI) info rmu ota?	Priemo nės pažeidi mui išvengt i ateityje	Pasta bos
Pažei di mo dat a, tik slu nu sta ty mo lai kas	Eilės nr.	Kai P buv o duo men tik slu s subj ekt skai čius	P buv ie duo men o subj ekt skai čius	Kok ie duo men apraš ymas prie žasti s	Pažei idim duo men o subj ekt skai čius	Ar visi klient ai ir men duo men on nalo na subj ekt skai čius	Priem onės pažei darbu dimui jautr umas not men ys apie paže idim a?	VDAI infor mavi apsa ugos insp ekci ja sum žinti otojai buvo infor muoti ?	Ar duom enų subj ekt skai čius	Duome nų subjekt o neinf orma vimo / vėlav i ja sum žinti sum žinti buvo infor muoti ?	Ar duom enų subje ktai infor mavim vimo / vėlavim ja (tol mo au- VD AI) info rmu ota?	Priemo nės pažeidi mui išvengt i ateityje	Pasta bos

Reagavimo į asmens duomenų
saugumo pažeidimus
procedūros aprašo
2 priedas

PRANEŠIMO APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ FORMA

(duomenų valdytojo (juridinio asmens) pavadinimas, duomenų valdytojo atstovo pavadinimas,
duomenų valdytojo (fizinio asmens) vardas, pavardė)

(juridinio asmens kodas ir buveinės adresas arba fizinio asmens kodas, gimimo data (jeigu asmuo
neturi asmens kodo) ir asmens duomenų tvarkymo vieta

(telefono ryšio ir (ar) elektroninio pašto adresas, ir (ar) elektroninės siuntos pristatymo dėžutės
adresas)

Valstybinei duomenų apsaugos inspekcijai

PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

Nr. _____
(data) (rašto numeris)

1. Asmens duomenų saugumo pažeidimo apibūdinimas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:

Asmens duomenų saugumo pažeidimo :

Data _____ Laikas _____

Asmens duomenų saugumo pažeidimo nustatymo:

Data _____ Laikas _____

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

- Informacinė sistema
- Duomenų bazė
- Tarnybinė stotis
- Internetinė svetainė
- Debesų kompiuterijos paslaugos
- Nešiojami / mobilus įrenginiai
- Neautomatiniu būdu susistemintos bylos (archyvas)
- Kita _____

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

- Asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas)
- Asmens duomenų vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas)

- Asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas)

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

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

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

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

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

- Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:
-
-

- Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai (pavyzdžiu, asmens kodas, mokėtojo kodas, slaptažodžiai):
-
-

- Kiti:
-
-

- Nežinomi (pranešimo teikimo metu)

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

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

2. Galimos asmens duomenų saugumo pažeidimo pasekmės

2.1. Konfidencialumo praradimo atveju:

- Asmens duomenų išplėtimas labiau nei yra būtina ir duomenų subjekto praradimas savo asmens duomenų atžvilgiu (pavyzdžiu, asmens duomenys išplito interne)
 - Skirtingos informacijos susiejimas (pavyzdžiu, gyvenamosios vietas adreso susiejimas su asmens buvimo vieta realiu laiku)
 - Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pavyzdžiu, komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)
 - Kita
-
-
-

2.2. Vientisumo praradimo atveju:

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

2.3. Duomenų prieinamumo praradimo atveju:

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

2.4. Kita:

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

3.1. Taikytos priemonės siekiant sumažinti poveikį duomenų subjektams:

3.2. Taikytos priemonės siekiant pašalinti asmens duomenų saugumo pažeidimą:

3.3. Taikytos priemonės siekiant, kad pažeidimas nepasikartotų:

3.4. Kita:

4. Siūlomos priemonės sumažinti asmens duomenų saugumo pažeidimo pasekmėms

5. Duomenų subjektų informavimas apie asmens duomenų saugumo pažeidimą

5.1. Duomenys apie informavimo faktą:

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

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

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

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

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

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

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

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

5.4. Būdas, kokių duomenų subjektai buvo informuoti:

- Paštu
 Elektroniniu paštu
 Kitu būdu _____

5.5. Informuotų duomenų subjekto skaičius _____

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

6.1. Vardas ir pavardė _____

6.2. Telefono ryšio numeris _____

6.3. Elektroninio pašto adresas _____

6.4. Pareigos _____

6.5. Darbovietės pavadinimas ir adresas _____

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

8. Kita reikšminga informacija

(pareigos)

(parašas)

(vardas, pavardė)

Reagavimo į asmens duomenų
saugumo pažeidimus
procedūros aprašo
3 priedas

(Pranešimo duomenų subjektui apie įvykusį duomenų saugumo pažeidimą forma)

PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE ĮVYKUSĮ DUOMENŲ SAUGUMO PAŽEIDIMĄ

data

Vadovaudamiesi Bendrojo duomenų apsaugos reglamento 34 straipsniu, teikiame šį pranešimą apie asmens duomenų saugumo pažeidimo atvejį.

Pažymėti vieną langelį:

Duomenų valdytojas:	<input type="checkbox"/> Vilniaus lopšelis-darželis „Sakalėlis“
Duomenų tvarkytojas:	<input type="checkbox"/> Vilniaus lopšelis-darželis „Sakalėlis“

Nr.	Aprašymas
1.	Asmens duomenų saugumo pažeidimo pobūdis (incidento aprašymas)
2.	Duomenų apsaugos pareigūno (arba kito atsakingo asmens) vardas, pavardė, kontaktinė informacija
3.	Incidento vienos adresas
4.	Asmens duomenų saugumo pažeidimo pasekmės (tikėtinų pasekmių duomenų subjektui aprašymas)
5.	Priemonės asmens duomenų saugumo pažeidimui pašalinti (priemonių, kurių ėmėtės, aprašymas)

(pareigos)

(parašas)

(vardas, pavardė)

Reagavimo į asmens duomenų saugumo pažeidimus procedūros aprašo 4 priedas

Reagavimo į duomenų saugumo pažeidimus schema

