

## 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 vaikų ir jaunimo klubo „Šatrija“, juridinio asmens kodas 191664421, buveinės adresas Kalvarijų g. 156, LT-08207 Vilnius (toliau – Klubas), 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 tokių 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. Klubo darbuotojai, dirbantys pagal darbo ar kitas sutartis (toliau – darbuotojai);

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

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

4. Apraše vartojamos sąvokos:

4.1. **duomenų saugumo pažeidimas** – bet koks įvykis, dėl kurio netyčia 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. Klubo atžvilgiu tai Valstybinė duomenų apsaugos inspekcija (įmonės 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. konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama (gaunama) prieiga tam teisės neturintiems asmenims, pavyzdžiui, duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio pavišimas, 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 ištrynimasis, praradimas (vagystė), sunaikinimas, pavyzdžiui, gaisro, liūtis atveju ir nesant

atsarginės kopijos, iš kurios būtų galima atkurti prarastus duomenis. Pasiiekiamumo pažeidimu laikytinas ir įprastinę Klubo veiklą sutrikdęs prieigos prie duomenų praradimas;

5.3. vientisumo pažeidimas – netyčia ar neteisėtai atlikti 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 netikslumų arba pasikeitimų.

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 Klubo duomenų apsaugos pareigūną (toliau – pareigūnas).

7. Darbuotojas arba jo tiesioginis vadovas Klubo 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 pavojus (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 konkrečios duomenų subjektų grupės duomenys, kokia konkrečios grupės dalis yra paveikta ir pan.);

7.5. pradinius Pažeidimo pasekmių požymius (pavyzdžiui, 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 jautresniais duomenimis, pavyzdžiui, sveikatos duomenimis, religiniais, filosofiniais įsitikinimais, naryste profesinėse sąjungose, lytine orientacija, asmenų teistumu, finansine informacija ir pan. Nereikšmingu kiekiu gali būti laikomas vienkartinis, atsitiktinis duomenų praradimas, pavyzdžiui, elektroninio laiško išsiuntimas ne tam adresatui, popieriaus lapo, bylos praradimas (pametimas);

9.2. Pažeidimas tikėtina gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms;

9.3. daromas poveikis dideliame duomenų subjektų skaičiui, ypač kai poveikis daromas labiau pažeidžiamiems duomenų subjektams, pavyzdžiui, vaikams;

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

10. Jeigu nustatoma, kad turimais duomenimis Pažeidimas atitinka Aprašo 5 ir 9 punktų kriterijus, pradedama reagavimo į asmens duomenų saugumo pažeidimus procedūra ir Klubo 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 Klubo direktoriaus arba jo įgaliojo asmens, pareigūno, direktoriaus pavaduotojų ir kitų atsakingų darbuotojų.

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 Klubo asmens duomenų saugumo pažeidimų žurnalą (toliau – Žurnalas), kurio forma nustatyta Aprašo 1 priede, užbaigiama.

13. Vykdamas Supaprastintą procedūrą ir nustatius, kad įvykęs Pažeidimas atitinka Aprašo 5 ir 9 punktų kriterijus, pareigūnas teikia siūlymą Klubo 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 eigą bei priemones, kurių buvo imtasi.

### **III SKYRIUS**

#### **II ETAPAS: DUOMENŲ SAUGUMO PAŽEIDIMO APRIBOJIMAS, LIKVIDAVIMAS IR ATKŪRIMAS**

15. Nustatius, 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 imamasi šių priemonių:

15.1. duomenų ištrynimasis 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 ištrinti 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, Klubas gali informuoti Klubo bendruomenę apie Pažeidimo tyrimą, jo rezultatus, priemones, kurių imamasi Pažeidimui apriboti ir pan. Klubo bendruomenės informavimą vykdo komunikacijos projektų vadovas, suderinęs poziciją su Klubo direktoriumi, pareigūnu ir (ar) kitais Komisijos nariais.

19. Atkūrimo stadijoje sistemos turėtų būti pagal galimybes atkurtos į ankstesnę būklę, siekiant užtikrinti Klubo veiklos tęstinumą.

### **IV SKYRIUS**

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

20. Klubas, kaip duomenų valdytojas, nedelsdamas privalo informuoti Valstybinę duomenų apsaugos inspekciją (toliau – VDAI), jeigu Komisija arba pareigūnas nustato, kad Pažeidimas kelia arba tikėtina gali kelti pavojų duomenų subjektų, paveiktų Pažeidimo, teisėms ir laisvėms. Pavojų 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 pavojų duomenų subjektui atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Pavojus 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. pasekmių rimtumą duomenų subjektams;

21.5. specialias duomenų subjekto savybes (pavyzdžiui, duomenys, susiję su vaikais ar kitais pažeidžiamais asmenimis);

21.6. paveiktų 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 Klubo 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 pavojų (riziką) duomenų subjektų teisėms ir laisvėms, pareigūnas ne vėliau kaip per 72 valandas nuo Klubo sužinojimo (nustatymo) apie Pažeidimą momento VDAI pateikia tokią informaciją:

24.1. Pažeidimo pobūdį, įskaitant, jeigu įmanoma, atitinkamai paveiktų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;

24.2. tikėtinų Pažeidimo pasekmių aprašymą;

24.3. priemones, kurių ėmėsi arba planuoja imtis Klubas tam, kad būtų pašalintas Pažeidimas;

24.4. priemonės 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 pirminiame pranešime.

26. Jeigu po pranešimo VDAI pateikimo atlikus tolesnį tyrimą yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo 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, Klubas 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 esančius 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 pavojus duomenų subjektų teisėms ir laisvėms, Klubas nepagrįstai nedelsdamas, bet ne vėliau kaip per 72 valandas nuo Pažeidimo paaiškėjimo momento informuoja duomenų subjektus, kurių teisėms ir laisvėms gali kilti didelis pavojus.

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

30. Klubas, informuodamas 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 pasekmių duomenų subjektui aprašymą;

30.4. priemonės, kurių ėmėsi arba planuoja imtis Klubas tam, kad būtų pašalintas Pažeidimas, įskaitant 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. Klubas įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikį, visų pirma tas priemonės, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės;

31.2. Klubas, įvykus Pažeidimui, ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

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

32. Gavęs priežiūros institucijos reikalavimą informuoti duomenų subjektus apie Pažeidimą, Klubas nedelsdamas jį vykdo.

## **VI SKYRIUS**

### **PRANEŠIMAS DUOMENŲ VALDYTOJUI NUO DUOMENŲ TVARKYTOJO**

33. Jeigu Klubas duomenis tvarko kaip duomenų tvarkytojas, o ne valdytojas, tuomet Klubas laikosi visų Aprašo II ir III skyriuose nustatytų reikalavimų ir, jeigu sutartyje su duomenų valdytoju nenumatyta 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 Klubo 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 Klubui netaikoma, Komisijos įgaliotas asmuo arba pareigūnas sudaro prevencinių veikslių planą, kuriuo būtų siekiama ateityje užkirsti kelią analogiškam ar panašiam Pažeidimui įvykti, ir jis pateikiamas Klubo direktoriui spręsti dėl jo įgyvendinimo.

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

38. Procedūros dokumentai turi būti saugomi teisės 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 Klubo pareigą informuoti VDAI, duomenų subjektus arba duomenų valdytojus įgyvendina pareigūnas arba kitas Komisijos įgaliotas asmuo.

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

---



**(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 numeris 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
- Interneto svetainė
- Debesų kompiuterijos paslaugos
- Nešiojamieji / mobilieji įrenginiai
- Neautomatiniu būdu susistemintos bylos (archyvas)
- Kita \_\_\_\_\_

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

- Asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas)



- Asmens duomenų vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas)
- Asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas)

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

---

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

---

---

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

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

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

- Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:
- 
- 

- Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai (pavyzdžiui, asmens kodas, mokytojo kodas, slaptažodžiai):
- 
- 

- Kiti:
- 
- 

- Nežinomi (pranešimo teikimo metu)

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

---

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

---

---

---

---

---

## 2. Galimos asmens duomenų saugumo pažeidimo pasekmės

### 2.1. Konfidencialumo praradimo atveju:

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

---



---



---



---



---

### 2.2. Vientisumo praradimo atveju:

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

---



---



---



---



---

### 2.3. Duomenų prieinamumo praradimo atveju:

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

---



---



---



---



---

## 2.4. Kita:

---



---



---



---

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

## 3.1. Taikytos priemonės siekiant sumažinti poveikį duomenų subjektams:

---



---



---



---

## 3.2. Taikytos priemonės siekiant pašalinti asmens duomenų saugumo pažeidimą:

---



---



---



---

## 3.3. Taikytos priemonės siekiant, kad pažeidimas nepasikartotų:

---



---



---



---

## 3.4. Kita:

---



---



---



---



---

4. Siūlomos priemonės asmens duomenų saugumo pažeidimo pasekmėms sumažinti
--

---



---



---



---



---

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 pridėta pranešimo duomenų subjektui kopija):

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

5.4. Būdas, koku duomenų subjektai buvo informuoti:

- Paštu
- Elektroniniu paštu
- Kitu būdu \_\_\_\_\_

5.5. Informuotų duomenų subjektų skaičius \_\_\_\_\_

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

6.1. Vardas ir pavardė \_\_\_\_\_

6.2. Telefono ryšio numeris \_\_\_\_\_

6.3. Elektroninio pašto adresas \_\_\_\_\_

6.4. Pareigos \_\_\_\_\_

6.5. Darbovietės pavadinimas ir adresas \_\_\_\_\_

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

---

---

---

---

---

---

---

---

8. Kita reikšminga informacija

---

---

---

---

---

---

---

---

\_\_\_\_\_  
(pareigos)

\_\_\_\_\_  
(parašas)

\_\_\_\_\_  
(vardas, pavardė)

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*

Vilnius

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 miesto savivaldybės administracija
Duomenų tvarkytojas:	<input type="checkbox"/> Vilniaus miesto savivaldybės administracija

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

\_\_\_\_\_

(pareigos)

\_\_\_\_\_

(parašas)

\_\_\_\_\_

(vardas, pavardė)

Reagavimo į asmens duomenų saugumo  
pažeidimus procedūros aprašo  
4 priedas

**REAGAVIMO Į DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS SCHEMA**

