



**KLAIPĖDOS SIMONO DACHO PROGIMNAZIJOS  
DIREKTORIUS**

**ĮSAKYMAS  
DĖL ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ POLITIKOS PATVIRTINIMO**

2021 m. gegužės 5 d. Nr. V1-49  
Klaipėda

Vadovaudamasis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrojo duomenų apsaugos reglamentu) (OL 2016 L 119, p. 1) ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu:

1. T v i r t i n u Klaipėdos Simono Dacho progimnazijos asmens duomenų saugumo pažeidimų politiką (pridedama).
2. P a v e d u raštinės administratori Simonai Jasinevičienei pasirašytinai supažindinti darbuotojus su Klaipėdos Simono Dacho progimnazijos asmens duomenų saugumo pažeidimų politika.
3. S k i r i u atsakingu už asmens duomenų saugumo pažeidimų tyrimą pavaduotoją ugdymui Daivą Šulcienę.

Direktorė

Daiva Marozienė

PATVIRTINTA  
Klaipėdos Simono Dachso progimnazijos  
direktoriaus 2021 m. gegužės 5 d.  
įsakymu Nr. V1-49

## KLAIPĖDOS SIMONO DACHO PROGIMNAZIJOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ POLITIKA

### I SKYRIUS BENDROSIOS NUOSTATOS

1. Klaipėdos Simono Dachso progimnazijos (toliau – Progimnazija arba **Duomenų valdytojas**) asmens duomenų saugumo pažeidimų politikos (toliau - Politika) tikslas – nustatyti asmens duomenų saugumo pažeidimo Progimnazijoje, pranešimų kompetentingai priežiūros institucijai (o tam tikrais atvejais ir duomenų subjektams) apie juos ir dokumentavimo tvarką siekiant įgyvendinti atskaitomybės principą.

2. Ši Politika visais atvejais taikoma Progimnazijos vykdomoje veikloje ir yra privaloma visiems Progimnazijos darbuotojams.

3. Šioje Politikoje vartojamos sąvokos atitinka apibrėžimus, nustatytus Lietuvos Respublikos įstatymuose ir Europos Sąjungos teisės aktuose.

4. Politikoje vartojamos sąvokos:

4.1. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (pavyzdžiui, vardas ir pavardė, asmens identifikavimo numeris, buvimo vietos duomenys ir interneto identifikatorius arba vienas ar keli to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymiai).

4.2. **Saugumo pažeidimas** – asmens duomenų saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų bei leidimo gaunama prieiga.

4.3. **Duomenų subjektas** – fizinis asmuo, kurio asmens duomenis Progimnazija tvarko.

4.4. **Duomenų tvarkymas** – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimasis arba sunaikinimas.

4.5. **Duomenų tvarkytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri Duomenų valdytojo vardu tvarko asmens duomenis.

4.6. **Priežiūros institucija** – Valstybinė duomenų apsaugos inspekcija (toliau -VDAI).

4.7. **Reglamentas** – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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).

### II SKYRIUS ASMENS DUOMENŲ TVARKYMO SAUGUMAS

5. Progimnazija, taikydama tinkamas technines ir organizacines priemones, užtikrina, kad asmens duomenys būtų tvarkomi tokiu būdu, kad būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo neteisėto duomenų tvarkymo ir atsitiktinio sunaikinimo, sugadinimo ar praradimo.

6. Progimnazija, atsižvelgdama į techninių galimybių išsivystymo lygį Progimnazijoje, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant, jei reikia:

6.1. pseudonimų suteikimą asmens duomenims ir jų šifravimą;

6.2. gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;

6.3. gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju;

6.4. reguliarių techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą;

6.5. Kitas Progimnazijos ir konkrečių informacijos sistemų naudojimo tvarkas, numatančias asmens duomenų privatumo užtikrinimo ir informacinės saugos priemones.

7. Nustatydamą tinkamo lygio saugumą, Progimnazija įvertina pavojus, kurie gali kilti dėl asmens duomenų tvarkymo, visų pirma dėl tvarkomų asmens duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo ar neteisėtos prieigos prie jų.

### **III SKYRIUS DUOMENŲ SAUGUMO PAŽEIDIMŲ KLASIFIKAVIMAS**

8. Saugumo pažeidimai, kurie yra skirstomi pagal tris informacijos saugumo principus, gali būti klasifikuojami į:

8.1. Konfidencialumo pažeidimas – kai yra be leidimo (nesankcionuotai) ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

8.2. Prieinamumo pažeidimas – kai netyčia arba neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;

8.3. Vientisumo pažeidimas – kai asmens duomenys pakeičiami be leidimo (nesankcionuotai) ar netyčiais naudotojų veiksmais.

9. Priklausomai nuo aplinkybių, Pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

### **IV SKYRIUS REAGAVIMAS Į SAUGUMO PAŽEIDIMUS**

10. Kiekvienas Progimnazijos darbuotojas, įtaręs, supratęs ar sužinojęs, jog buvo padarytas ar įvykęs saugumo pažeidimas, nedelsiant apie tokį pažeidimą privalo informuoti Progimnazijos vadovo paskirtą už saugumo pažeidimų tyrimą atsakingą darbuotoją.

11. Už saugumo pažeidimų tyrimą atsakingas darbuotojas:

11.1. privalo imtis visų reikiamų techninių ir organizacinių priemonių, kad nedelsiant būtų nustatyta, buvo padarytas/įvyko saugumo pažeidimas ar nebuvo. Tais atvejais, kai šis darbuotojas negali identifikuoti, ar buvo padarytas/įvyko saugumo pažeidimas, šiam klausimui išspręsti turi būti inicijuotas kompetentingos komisijos sudarymas;

11.2. turi įvertinti riziką, kurią gali patirti Progimnazija, duomenų subjektai bei kiti susiję asmenys;

11.3. privalo nedelsiant imtis visų įmanomų techninių ir organizacinių saugumo priemonių, kad būtų suvaldytas saugumo pažeidimas ir sumažinti neigiami padariniai;

11.4. apie saugumo pažeidimą, tame tarpe ir dar neįvykusį, o tik galimą, privalo nedelsiant informuoti Progimnazijos vadovą.

12. Progimnazijos vadovas arba jo įgaliotas asmuo privalo informuoti kompetentingą priežiūros instituciją, VDAI (o tam tikrais atvejais ir duomenų subjektus) apie saugumo pažeidimą Politikos 13 ir 19 punktuose nustatyta tvarka.

**V SKYRIUS**  
**PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI**  
**APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

13. Saugumo pažeidimo atveju Progimnazijos vadovas arba jo įgaliotas asmuo nepagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 (septyniasdešimt dviem) valandoms nuo tada, kai už duomenų saugumo pažeidimų tyrimą atsakingas darbuotojas sužinojo apie saugumo pažeidimą, apie tai praneša priežiūros institucijai (VDAI) 2 priedas.

14. Išimtiniais atvejais, kai Progimnazijos vadovas ir už duomenų saugumo pažeidimų tyrimą atsakingas darbuotojas, įvertinę (galimo) saugumo pažeidimo pobūdį ir keliamą riziką, nusprendžia, kad saugumo pažeidimas nekelia ir ateityje nesukels pavojaus duomenų subjektų teisėms ir laisvėms, apie tokį saugumo pažeidimą galima ir nepranešti.

15. Jeigu priežiūros institucijai apie saugumo pažeidimą nepranešama per 72 (septyniasdešimt dvi) valandas nuo tada, kai Progimnazija sužinojo apie saugumo pažeidimą, prie pranešimo turi būti pridėdamos vėlavimo priežastys.

16. Politikos 13 punkte nurodytame pranešime apie saugumo pažeidimą turi būti bent:

16.1. aprašytas saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;

16.2. nurodyta duomenų subjekto paskirto atsakingo Progimnazijos darbuotojo, galinčio suteikti daugiau informacijos, vardas bei pavardė ir kontaktiniai duomenys;

16.3. aprašytos tikėtinos saugumo pažeidimo pasekmės;

16.4. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis Progimnazija, kad būtų pašalintas saugumo pažeidimas, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti.

17. Jeigu visos 16 punkte nurodytos informacijos Progimnazija negali pateikti priežiūros institucijai pranešimo pateikimo metu, informacija apie saugumo pažeidimą toliau nepagrįstai nedelsiant gali būti teikiama etapais. Informacijos teikimas etapais yra pateisinamas sudėtingesnių pažeidimų atveju (pavyzdžiui, kai kuriems kibernetinio saugumo incidentams), kai gali būti reikalingas nuodugnus tyrimas, siekiant išsamiai nustatyti saugumo pažeidimo pobūdį ir tai, kokių mastu asmens duomenys buvo pažeisti.

18. Pateikusi pradinį pranešimą Progimnazija bet kuriuo metu gali informuoti priežiūros instituciją (VDAI) apie tolesniame tyrime atskleistus įrodymus, jog jokie saugumo pažeidimo faktiškai nebuvo. Tokiu atveju ši papildoma informacija yra įtraukiama į pradinę informaciją, kuri jau buvo pateikta priežiūros institucijai, ir incidentas atitinkamai nėra laikomas saugumo pažeidimu.

**VI SKYRIUS**  
**PRANEŠIMAS DUOMENŲ SUBJEKTUI**  
**APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

19. Tais atvejais, kai dėl saugumo pažeidimo gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, Progimnazijos vadovas ar jo įgaliotas asmuo, nepagrįstai nedelsdamas turi pranešti apie tokį saugumo pažeidimą ir patiekti duomenų subjektams, kad šie galėtų imtis visų įmanomų priemonių apsisaugoti nuo neigiamų padarinių.

20. Politikos 19 punkte nurodytame pranešime duomenų subjektams aiškia ir paprasta kalba aprašomas saugumo pažeidimo pobūdis ir pateikiama bent Politikos 16.2-16.4 punktuose nurodyta informacija ir priemonės.

21. Politikos 19 punkte nurodyto pranešimo duomenų subjektams nereikalaujama, jeigu įvykdomos bet kurios toliau nurodytos sąlygos:

21.1. Progimnazija įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems saugumo pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad neturint leidimo susipažinti su asmens duomenimis nebūtų galimybės juos panaudoti (pavyzdžiui, naudojant šifravimą (pseudonimizaciją));

21.2. Progimnazija toliau ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

21.3. tai pareikalautų neproporcingai daug pastangų. Tokiu atveju apie tai paskelbiama viešai (pavyzdžiui, naujienų portale, Progimnazijos internetiniame puslapyje ar kitomis žiniasklaidos formomis) arba darbuotojui informuoti taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai (pavyzdžiui, el. paštu ar trumposiomis SMS žinutėmis).

22. Jeigu Progimnazija dar nėra pranešusi duomenų subjektams apie saugumo pažeidimą, tačiau priežiūros institucija, apsvarsčiusi, kokia yra tikimybė, kad dėl saugumo pažeidimo kils didelis pavojus, pareikalauja tai padaryti, Progimnazija praneša duomenų subjektams 19 punkte nustatyta tvarka.

## **VII SKYRIUS SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS**

23. Visi pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, registruojami asmens duomenų saugumo pažeidimų registravimo žurnale (toliau - Žurnalas). Informacija apie pažeidimą į Žurnalą įvedama nedelsiant, kai tik nustatomas pažeidimo faktas ir įvertinama rizika (per 5 darbo dienas). Žurnale esanti informacija papildoma ir (ar) koreguojama.

24. Prie kiekvieno saugumo pažeidimo kortelės turi būti pridedama įvykusio saugumo pažeidimo analizė, kurioje nurodomi veiksmai, kuriuos vykdant siekiama išvengti analogiškų saugumo pažeidimų ateityje.

25. Žurnale nurodomi:

25.1. Visi su pažeidimu susiję faktai – pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

25.2. Pažeidimo poveikis ir pasekmės;

25.3. Taisomieji veiksmai (techninės priemonės), kurių buvo imtasi;

25.4. Priežastys dėl su pažeidimu susijusių sprendimų priėmimo;

25.5. Pranešimo VDAI pateikimo vėlavimo priežastys (jeigu pranešimą vėluojama pateikti ar pranešimas teikiamas etapais);

25.6. Informacija, susijusi su pranešimu duomenų subjektui;

25.7. Kita reikšminga informacija susijusi su pažeidimu.

26. Žurnalas tvarkomas raštu, įskaitant elektroninę formą, ir saugomas trejus metus pagal patvirtintą dokumentų saugojimo tvarką.

## **VIII SKYRIUS ATSAKOMYBĖ**

27. Jei dėl saugumo pažeidimo laiku nesiimama tinkamų priemonių, duomenų subjektai gali patirti materialinę ar nematerialinę žalą, pavyzdžiui, prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai atstatyta pradinė informacija panaikinus šifravimą, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

28. Progimnazijos nustatytų taisyklių, nustatančių reagavimo į saugumo pažeidimus nesilaikymas yra laikomas darbo tvarkos pažeidimu, už kurį darbuotojui gali būti taikoma atsakomybė.

29. Darbuotojams, kurie pažeidžia Reglamentą ar kitus teisės aktus, reglamentuojančius reagavimo į saugumo pažeidimus taisykles, gali būti taikomos minėtuose teisės aktuose numatytos atsakomybės priemonės.

## **IX SKYRIUS BAIGIAMOSIOS NUOSTATOS**

30. Šios Politikos laikymosi stebėseną ir kontrolę atliekama nuolat.

31. Nustačius šios Politikos pažeidimą, nedelsiant atliekamas pažeidimo aplinkybių, priežasčių bei pasekmių tyrimas ir neigiamų pasekmių šalinimas, taip pat imamasi neatidėliotinų priemonių, kad tokie pažeidimai nepasikartotų ateityje.

32. Ši Politika peržiūrima ne rečiau kaip kartą per dvejus metus arba atitinkamoms institucijoms, kaip kad VDAI priėmus naujus reglamentuojančius teisės aktus.

33. Ši Politika taikoma nuo jos patvirtinimo datos.

34. Ši Politika gali būti pakeista ar panaikinta bet kuriuo metu atskiru Progimnazijos direktoriaus įsakymu.

35. Darbuotojai supažindinami su šia Politika pasirašytinai ir tuo įsipareigoja laikytis šioje Politikoje nustatytų taisyklių.

---



## KLAIPĖDOS SIMONO DACHO PROGIMNAZIJA

Savivaldybės biudžetinė įstaiga, Kuršių a. 3, 92127 Klaipėda, tel. (8 46) 41 09 55, el. p. [info@dachas.lt](mailto:info@dachas.lt)  
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 190439336

Valstybinei duomenų 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 visus tinkamus):

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

1.3. Asmens duomenų saugumo pažeidimo aplinkybės (pažymėti visus tinkamus):

- 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 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 narysę 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 (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 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 prieiti, pavyzdžiui, prie asmens sveikatos istorijų ir teikti pacientams sveikatos paslaugų, arba įgyvendinti duomenų subjekto teises)
  - 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 sumažinti asmens duomenų saugumo pažeidimo pasekmes**

---

---

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)

\_\_\_\_\_

