

# PAŽEIDIMŲ APTIKIMO, SUSTABDYMO (PAŠALINIMO) IR PRANEŠIMO APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS BENDRUOMENINIAME PAGALBOS VAIKAMS CENTRE TVARKOS APRAŠAS

## I SKYRIUS BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie asmens duomenų saugumo pažeidimus Bendruomeniniame Pagalbos vaikams centre (toliau – Centras, Duomenų valdytojas) tvarkos aprašas (toliau – Aprašas) nustato pažeidimų tyrimo, pranešimo apie juos ir dokumentavimo Bendruomeniniame pagalbos vaikams centre tvarką ir sąlygas.
2. Pranešimai apie asmens duomenų saugumo pažeidimus teikiami Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) ir duomenų subjektams, vadovaujantis 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 straipsniais ir Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo (toliau – Įstatymas) 29 ir 30 straipsniais.
3. Apraše vartojamos sąvokos atitinka BDAR ir Įstatyme vartojamas sąvokas. Asmens duomenų saugumo pažeidimas šiuose teisės aktuose apibrėžiamas kaip:
  - 3.1. **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiūsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (BDAR 4 straipsnio 12 punktą);
  - 3.2. **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio neatsargiai arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiūsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (Įstatymo 2 straipsnio 2 dalis).
4. VDAI apie asmens duomenų saugumo pažeidimą (toliau – Pažeidimas) Centras privalo pranešti pateikdamas pranešimą apie asmens duomenų saugumo pažeidimą (toliau – Pranešimas), išskyrus, kai tikėtina, kad toks Pažeidimas nekels pavojaus asmenų teisėms ir laisvėms. Kai dėl Pažeidimo pobūdžio ir rizikos rimtumo kyla didelė grėsmė fizinių asmenų teisėms ir laisvėms, Centras apie Pažeidimą privalo pranešti ir duomenų subjektui.

## II SKYRIUS PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

5. Duomenų valdytojas privalo informuoti darbuotojus apie jų pareigą pranešti apie galimus Pažeidimus ir supažindinti juos su nustatyta pranešimų apie Pažeidimus pateikimo tvarka.
6. Centro darbuotojas, sužinojęs ar pats nustatęs galimą Pažeidimą arba kai informacija apie galimą Pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio, privalo nedelsdamas (ne ilgiau kaip per 24 val.) apie tai informuoti Duomenų valdytoją. Pranešimas gali būti pateikiamas raštu ar elektroninėmis priemonėmis.

7. Duomenų valdytojas nedelsiant (ne ilgiau kaip per 24 val.) informuoja Centro duomenų apsaugos pareigūną ir suteikia jam visą informaciją, susijusią su galimu Pažeidimu.
8. Duomenų apsaugos pareigūnas informaciją apie Pažeidimą įveda į Centro asmens duomenų pažeidimų žurnalą (toliau – Žurnalas) nedelsiant, kai tik nustatomas Pažeidimo faktas ir įvertinama rizika.

### III SKYRIUS

#### ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS

9. Duomenų apsaugos pareigūnas, sužinojęs apie galimą Pažeidimą, turėtų kaip įmanoma greičiau atlikti pirminį tyrimą, išsiaiškinti ir nustatyti, ar Pažeidimas iš tikrųjų įvyko, bei kokios galimos pasekmės asmenims (t. y. įvertinti riziką).
10. Galimi Pažeidimo tipai:
  - 10.1. „*Konfidencialumo Pažeidimas*“ – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;
  - 10.2. „*Prieinamumo Pažeidimas*“ – kai netyčia arba neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;
  - 10.3. „*Vientisumo Pažeidimas*“ – kai asmens duomenys pakeičiami be leidimo ar netyčia.
11. Priklausomai nuo aplinkybių, Pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.
12. Priklausomai nuo Pažeidimo tipo, atliekant pirminį tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, turi būti išsaugomi esamos situacijos įrodymai bei vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės, pvz., duomenų srauto ir prisijungimų analizės įrankiai bei kt.
13. Vertinant riziką, kuri gali atsirasti dėl Pažeidimo, turi būti atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika turi būti vertinama remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus:
  - 13.1. pažeidimo tipą;
  - 13.2. asmens duomenų pobūdį, apimtį (pvz., specialių kategorijų asmens duomenys);
  - 13.3. kaip lengvai identifikuojamas fizinis asmuo;
  - 13.4. pasekmių rimtumą fiziniams asmenims;
  - 13.5. specialias fizinio asmens savybes (pvz., duomenys susiję su vaikais ar kitais pažeidžiamais asmenimis);
  - 13.6. nukentėjusiųjų fizinių asmenų skaičių;
  - 13.7. specialias duomenų valdytojo savybes (pvz., veiklos pobūdį).
14. Vertinant riziką, turi būti laikoma, kad 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., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.
15. Įvertinus riziką rekomenduotina nustatyti, kad yra:
  - 15.1. žema rizikos tikimybė;

- 15.2. vidutinė rizikos tikimybė;
- 15.3. didelė (aukšta) rizikos tikimybė.
- 16. Išvadą dėl Pažeidimo buvimo ir rizikos fizinių asmenų teisėms bei laisvėms įvertinimo duomenų apsaugos pareigūnas pateikia Centro vadovui. Centro vadovas turi priimti sprendimą dėl tolimesnių veiksmų, susijusių su Pažeidimu.
- 17. Už kompiuterių priežiūrą atsakingas darbuotojas ar kompiuterių/sistemų priežiūros paslaugas teikiantis subjektas visų pirma turėtų imtis visų tinkamų techninių, o Duomenų apsaugos pareigūnas organizacinių priemonių, kad Pažeidimas būtų išsamiai ištirtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų ir tuomet pateikti Pranešimą VDAI.

#### **IV SKYRIUS PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI**

- 18. Nustačius, kad Pažeidimas buvo ir, kad yra rizika fizinių asmenų teisėms ir laisvėms, Duomenų valdytojas nedelsdamas, **ne vėliau kaip per 72 val.** nuo sužinojimo apie Pažeidimą, turi pranešti apie tai VDAI (Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie Pažeidimą VDAI, **rekomenduotina pranešti**).
- 19. Pranešimas apie asmens duomenų saugumo pažeidimą VDAI teikiamas vienu iš šių būdų:
  - 19.1. per VDAI interneto svetainę [www.ada.lt](http://www.ada.lt) naudojantis elektronine paslaugų sistema;
  - 19.2. elektroninio pašto adresu [ada@ada.lt](mailto:ada@ada.lt);
  - 19.3. paštu VDAI buveinės adresu;
  - 19.4. VDAI faksu;
  - 19.5. pateikiant pranešimą apie asmens duomenų saugumo pažeidimą VDAI.
- 20. Jeigu, priklausomai nuo Pažeidimo pobūdžio, duomenų valdytojui yra būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su Pažeidimu (pvz., dar nėra išsiaiškinta Pažeidimo apimtis), ir per 72 val. nuo sužinojimo apie Pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, Pranešimui reikalinga informacija gali būti teikiama etapais. Apie informacijos teikimą etapais, VDAI turi būti informuota teikiant pirminį Pranešimą.
- 21. Jeigu po Pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo jokio Pažeidimo, apie tai nedelsiant turėtų būti informuojama VDAI ir pažymėta Žurnale.

#### **V SKYRIUS PRANEŠIMAS DUOMENŲ SUBJEKTUI**

- 22. Nustačius, kad Pažeidimas buvo ir, kad yra didelė rizika fizinių asmenų teisėms ir laisvėms, duomenų apsaugos pareigūnas nedelsdamas (rekomenduojama per 72 val.) apie tai turi pranešti duomenų subjektui, kurio teisėms ir laisvėms dėl šio Pažeidimo gali kilti didelis pavojus.
- 23. VDAI informavimas apie Pažeidimą neatleidžia Duomenų valdytojo nuo pareigos informuoti duomenų subjektą.
- 24. Pranešime duomenų subjektui aiškia ir paprasta kalba turėtų būti pateikiama:
  - 24.1. pažeidimo pobūdžio aprašymas;
  - 24.2. duomenų apsaugos pareigūno vardas, pavardė ir kontaktiniai duomenys;
  - 24.3. tikėtinų Pažeidimo pasekmių aprašymas;

- 24.4. priemonių, kurių ėmėsi arba pasiūlė imtis Duomenų valdytojas, kad būtų pašalintas Pažeidimas, įskaitant (kai tinkama) priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas (pvz., kad apie Pažeidimą yra informuota VDAI ir, kad yra gautas patarimas dėl Pažeidimo tvarkymo ir jo poveikio sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);
- 24.5. kita reikšminga informacija, susijusi su Pažeidimu, kuri, Duomenų valdytojo manymu, turėtų būti pateikta duomenų subjektui.
25. Duomenų subjektai apie Pažeidimą turėtų būti informuoti tiesiogiai, pvz., siunčiant jiems pranešimą el. paštu, SMS, paštu ar pan.
26. Kai tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai daug pastangų, vietoj to apie įvykusį Pažeidimą gali būti paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai, pvz., pranešimas žinomos interneto svetainės antraštėje ar pranešimuose, žinomos reklamos spausdintoje žiniasklaidoje ar pan.
27. Turėtų būti pasirinkti tokie pranešimo duomenų subjektui būdai, kurie maksimaliai didintų galimybę tinkamai pranešti informaciją visiems nukentėjusiems asmenims. Gali būti pasirinkti keli pranešimo duomenų subjektui apie Pažeidimą būdai.
28. Esant Pažeidimui, pranešimo duomenų subjektui teikti nereikia, jeigu:
- 28.1. duomenų valdytojas įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikio;
- 28.2. iš karto po Pažeidimo duomenų valdytojas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus asmenų teisėms ir laisvėms;
- 28.3. tai pareikalautų neproporcingai daug pastangų susisiekti su asmenimis (pvz., kai jų kontaktiniai duomenys buvo prarasti dėl Pažeidimo arba pirma nežinomi). Tokiu atveju vietoj to apie Pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.
29. Duomenų valdytojas turėtų gebėti įrodyti VDAI, kad jis įvykdė vieną ar daugiau 28 punkte nurodytų sąlygų.
30. Jeigu tiriant Pažeidimą pradžioje nustatoma, kad nėra pavojaus fizinių asmenų teisėms ir laisvėms, tačiau detalesnio Pažeidimo tyrimo metu nustatoma, kad toks pavojus gali kilti, Duomenų valdytojas turėtų riziką vertinti iš naujo.

## **VI SKYRIUS**

### **ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS**

31. Visi Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, turi būti registruojami Duomenų valdytojo Žurnale.
32. Informacija apie Pažeidimą į Žurnalą turi būti įvedama nedelsiant, kai tik nustatomas Pažeidimo faktas ir įvertinama rizika (ne ilgiau kaip per 5 darbo dienas). Esant būtinybei, Žurnale esanti informacija turėtų būti papildoma ir (ar) koreguojama.
33. Žurnale turi būti nurodoma:
- 33.1. visi su Pažeidimu susiję faktai – Pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;
- 33.2. pažeidimo poveikis ir pasekmės;
- 33.3. taisomieji veiksmai (techninės priemonės), kurių buvo imtasi;

- 33.4. priežastys dėl su Pažeidimu susijusių sprendimų priėmimo (pvz., kodėl Duomenų valdytojas nusprendė nepranešti apie Pažeidimą VDAI ir (ar) duomenų subjektui, t. y. kodėl nusprendė, kad tikėtina, jog Pažeidimas negali sukelti pavojaus fizinių asmenų teisėms ir laisvėms, arba kokią sąlygą įvykdė, kuomet pranešti apie Pažeidimą duomenų subjektui nereikia);
  - 33.5. pranešimo VDAI pateikimo vėlavimo priežastys (jeigu Pranešimą vėluojama pateikti ar Pranešimas teikiamas etapais);
  - 33.6. informacija, susijusi su pranešimu duomenų subjektui (pvz., ar buvo pranešta, kodėl nepranešta ir pan.);
  - 33.7. kita reikšminga informacija susijusi su Pažeidimu (pvz., kad tyrimo metu nustatyta, jog faktiškai Pažeidimo nebuvo, o buvo tik saugumo incidentas).
34. Žurnalas tvarkomas raštu ir saugomas pagal Duomenų valdytojo patvirtintą dokumentų saugojimo tvarką.

## **VII SKYRIUS**

### **BAIGIAMOSIOS NUOSTATOS**

- 35. VDAI apie Pažeidimą Duomenų valdytojas privalo pranešti pateikdamas Pranešimą (teisinė prievolė pranešti VDAI).
  - 36. Duomenų valdytojas, nepateikęs Pranešimo VDAI atsako BDAR nustatyta tvarka.
  - 37. Tvarkos įgyvendinimo kontrolę vykdo duomenų apsaugos pareigūnas.
  - 38. Visi Centro darbuotojai su Tvarka supažindinami pasirašytinai. Tvarka skelbiama Centro internetinėje svetainėje adresu [www.atokvepis.lt](http://www.atokvepis.lt).
-

Pažeidimų aptikimo, sustabdymo (pašalinimo)  
ir pranešimo apie asmens duomenų saugumo  
pažeidimus Bendruomeniniame pagalbos  
vaikams centre taisyklių aprašo  
1 priedas

*(Pranešimo apie asmens duomenų saugumo pažeidimą forma)*



## BENDRUOMENINIS PAGALBOS VAIKAMS CENTRAS

Biudžetinė įstaiga, Laisvės g. 8, LT-89223, Mažeikiai  
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 304405337,  
Bendruomeninio pagalbos vaikams centro duomenys: Laisvės g.83, Mažeikiai, tel. (8-443) 20110, el.p. info@atokvepis.lt

Valstybinei duomenų apsaugos inspekcijai

\_\_\_\_\_ Nr. \_\_\_\_\_  
(data) (rašto numeris)

### PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

#### 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 / mobilūs 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 patvirtinantys 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, 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 biometriniiais 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 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, 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)

\_\_\_\_\_