VAIKO GEROVĖS IR GLOBOS CENTRAS
DIREKTORIUS

ĮSAKYMAS
DĖL VAIKO GEROVĖS IR GLOBOS CENTRO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠO PATVIRTINIMO

2024 m. gruodžio d. Nr. V-
Šilutė

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

1. T v i r t i n u Vaiko gerovės ir globos centro asmens duomenų saugumo pažeidimų valdymo tvarkos aprašą (pridedama).

2. N u s t a t a u Kad ši tvarka įsigalioja nuo 2024 m. gruodžio 20 d.

3. N u r o d a u atsakingą asmenį supažindinti visus įstaigos darbuotojus su šia tvarka per dokumentų valdymo sistemą DVS „Kontora”.

Direktorė Audronė Čekanskienė

Parengė

Sigita Olberkienė
2024-12-20

PATVIRTINTA
Vaiko gerovės ir globos centro
direktoriaus 2024 m. gruodžio d.
įsakymu Nr. V-

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pašalinimo ir pranešimo apie juos Vaiko gerovės ir globos centre (toliau – Centras) tvarką.

2. Aprašas parengtas vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR).

3. Apraše vartojamos sąvokos:

3.1. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti.

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

3.3. **Neįgaliotas asmuo** – asmuo, neturintis teisės prieiti prie Centro turimų asmens duomenų.

3.4. **Duomenų subjektas** – fizinis asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

4. Kitos Apraše vartojamos sąvokos atitinka BDAR apibrėžtas sąvokas.

5. Galimi šie asmens duomenų saugumo pažeidimai:

5.1. **konfidencialumo pažeidimas** – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie jų suteikimas;

5.2. **vientisumo pažeidimas** – neleistinas arba netyčinis asmens duomenų pakeitimas;

5.3. **prieinamumo pažeidimas** – neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas.

6. Atsižvelgiant į aplinkybes, saugumo pažeidimas vienu metu gali būti susijęs su asmens duomenų konfidencialumu, vientisumu ir prieinamumu, taip pat su bet kokiu jų deriniu.

7. Asmens duomenų saugumo pažeidimas gali įvykti dėl šių priežasčių:

7.1. **žmogiškoji klaida** (pvz., asmens duomenys persiųsti ne tam adresatui, kuriam jie buvo skirti; ne saugojimui skirtoje vietoje palikti dokumentai, kuriuose yra asmens duomenų; pamesti nešiojamieji ar mobilieji įrenginiai (telefonas, nešiojamasis kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys, ir kt.);

7.2. **vagystė** (pvz., pavogti nešiojamieji ar mobilieji įrenginiai, kuriuose saugomi asmens duomenys; pavogtos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų, ir kt.);

7.3. **kibernetinė ataka** (pvz., duomenų bazėje ar informacinėje sistemoje esantys asmens duomenys užšifruojami, naudojant išpirkos reikalaujančią programą; internete paskelbiami informacinių sistemų naudotojų vardai ir slaptažodžiai ir kt.);

7.4. **neleistina (neautorizuota) prieiga prie asmens duomenų** (pvz., įgaliojimų neturintys asmenys patenka į patalpas, kuriose saugomos bylos su asmens duomenimis; įgaliojimų neturintys asmenys prisijungia prie duomenų bazių ar informacinių sistemų ir kt.);

7.5. **įrenginių ar programinės įrangos gedimas, saugos sistemos spragos** (pvz., energijos tiekimo nutrūkimas, dėl kurio negalima prieiga prie asmens duomenų; programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas informacinių sistemų naudotojams, klaida ir kt.);

7.6. **nenumatytos (*force majeure*) aplinkybės ir kitos priežastys** (gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys, ir kt.).

8. Asmens duomenų saugumo pažeidimas, galintis kelti pavojų asmenų teisėms ir laisvėms yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą (pvz., asmuo gali patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, pakenkta jo reputacijai, prarastas duomenų, kurie laikomi profesine paslaptimi, konfidencialumas ir kt.).

9. Aprašu siekiama užtikrinti, kad Centro darbuotojai sugebėtų laiku nustatyti galimus asmens duomenų saugumo pažeidimus ir suprastų, kokie veiksmai privalo būti atlikti valdant juos.

10. Aprašo privalo laikytis visi Centro darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino.

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

11. Centro darbuotojas, nustatęs galimą asmens duomenų saugumo pažeidimą arba kai informacija apie galimą saugumo pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio:

11.1. nedelsdamas, bet ne vėliau kaip per 1 darbo valandą nuo pažeidimo paaiškėjimo momento, žodžiu (tiesiogiai ar telefonu) arba elektroniniu paštu informuoja tiesioginį vadovą ir (arba) Centro duomenų apsaugos pareigūną (toliau – duomenų apsaugos pareigūnas);

11.2. užpildo Pranešimą apie asmens duomenų saugumo pažeidimą (Aprašo 1 priedas) ir nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo saugumo pažeidimo paaiškėjimo momento, perduoda jį duomenų apsaugos pareigūnui;

11.3. jei įmanoma, imasi priemonių pašalinti saugumo pažeidimą ir (ar) priemonių sumažinti jo sukeltas neigiamas pasekmes.

12.Centro duomenų tvarkytojas, nustatęs galimą asmens duomenų saugumo pažeidimą, nedelsdamas, bet ne vėliau kaip per 24 valandas nuo pažeidimo paaiškėjimo momento, apie tai praneša Centrui, pateikdamas užpildytą Pranešimą apie asmens duomenų saugumo pažeidimą (Aprašo 1 priedas).

13. Tuo atveju, jei terminas nuo momento, kai duomenų tvarkytojui tapo žinoma apie saugumo pažeidimą, iki pranešimo Centrui yra ilgesnis nei 24 valandos, duomenų tvarkytojas kartu su pranešimu pateikiaCentrui paaiškinimą dėl uždelsto informacijos pateikimo.

14. Duomenų tvarkytojas pateikia visą Centro prašomą informaciją, susijusią su saugumo pažeidimu ir jo tyrimu, per 12 punkte nurodytą laiką.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

15. Duomenų apsaugos pareigūnas, gavęs Centro darbuotojo ar duomenų tvarkytojo pateiktą pranešimą apie asmens duomenų saugumo pažeidimą:

15.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

15.2. jei saugumo pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkia Centro ar duomenų tvarkytojo informacinių technologijų specialistus, informacinių sistemų saugos įgaliotinį;

15.3. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

15.4. jei asmens duomenų saugumo pažeidimas padarytas, nustato pažeidimo pobūdį, priežastis, asmens duomenų kategorijas, jų pobūdį ir kiekį, duomenų subjektų kategorijas ir jų kiekį, įvertina padarytą žalą fiziniams asmenims bei tikėtinas pažeidimo pasekmes;

15.5. įvertina, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas saugumo pažeidimas;

15.6. nustato, ar apie saugumo pažeidimą būtina pranešti Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI);

15.7. nustato, ar apie saugumo pažeidimą būtina pranešti duomenų subjektams.

16. Atliekant asmens duomenų saugumo pažeidimo tyrimą ir siekiant nustatyti, ar pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas.

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

18. Vertinant rizikos lygį, atsižvelgiama į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:

18.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis: nuo padaryto pažeidimo pobūdžio gali priklausyti pavojaus duomenų subjektams dydis;

18.2. asmens duomenų pobūdis, jautrumas ir kiekis – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautrumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavojus;

18.3. galimybė identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiems asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, todėl pažeidimas padarys mažesnį poveikį duomenų subjektams);

18.4. fizinio asmens specifiniai ypatumai – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavojus, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalią turintys asmenys), tuo didesnį poveikį pažeidimas gali jiems padaryti;

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

18.6. pasekmės, sukeltos fiziniams asmenims, – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumas; taip pat atsižvelgiama į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis.

19. Įvertinus riziką nustatomas vienas iš trijų rizikos tikimybių lygių – maža, vidutinė ar didelė rizikos tikimybė.

20. Duomenų apsaugos pareigūnas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, užpildo Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (Aprašo 2 priedas).

21. Saugumo pažeidimo tyrimo ataskaita yra pateikiama Centro direktoriui jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

22. Atsižvelgdamas į saugumo pažeidimo tyrimo ataskaitą, Centro direktorius, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl saugumo pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

23. Sprendžiant asmens duomenų saugumo pažeidimo pašalinimo klausimą ir tvirtinant priemonių planą, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą. Priklausomai nuo konkrečių pažeidimo aplinkybių, reikia atlikti tokius veiksmus, kaip: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamojo ar mobiliojo įrenginio

(telefono, nešiojamojo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuriam jie buvo skirti, kuo skubiau kreiptis į jį su prašymu ištrinti atsiųstus asmens duomenis be galimybės juos atkurti; pakeisti prisijungimo prie duomenų bazės ar informacinės sistemos vardus ir slaptažodžius, jeigu jie tapo žinomi tretiesiems asmenims; atkuriant prarastus ar sugadintus asmens duomenis, naudoti atsargines kopijas ir kt.

24. Siekiant apriboti ar sustabdyti asmens duomenų saugumo pažeidimą, būtina kiek įmanoma tiksliau surinkti duomenų ir įrodymų apie įvykusį saugumo incidentą (pvz., kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės ar informacinės sistemos, kam per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su asmens duomenimis ir kt.).

25. Priemonių plane turi būti numatyti veiksmai, skirti ne vien esamo saugumo pažeidimo priežasčiai pašalinti, pavojui fizinių asmenų teisėms ir laisvėms sumažinti ar pašalinti, bet taip pat skirti neleisti pasikartoti pažeidimui. Būtina atsižvelgti į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant saugumo pažeidimą, ir imtis priemonių tiems trūkumams pašalinti.

IV SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

26. Tyrimo metu nustačius, kad asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai tapo žinoma apie pažeidimą, apie tai informuoja VDAI.

27. VDAI informuojama užpildant VDAI direktoriaus įsakymu patvirtintos galiojančios formos pranešimą apie asmens duomenų saugumo pažeidimą.

28. Jeigu įvertinus riziką abejojama, ar asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, duomenų apsaugos pareigūnas kartu su Centro direktoriumi sprendžia, ar apie pažeidimą turėtų būti pranešta VDAI.

29. Jeigu įvertinus riziką nustatoma, kad tuo metu apie saugumo pažeidimą VDAI pranešti nereikia, bet po kurio laiko situacija gali pasikeisti, tada saugumo pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo.

30. Tuo atveju kai, priklausomai nuo pažeidimo pobūdžio, būtina atlikti išsamesnį tyrimą, nustatyti visus svarbius faktus, susijusius su pažeidimu, ir per 72 valandas dėl objektyvių priežasčių nėra įmanoma ištirti padarytą pažeidimą, informacija VDAI teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminį pranešimą.

31. Jeigu po pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai asmens duomenų saugumo pažeidimo nebuvo, apie tai nedelsiant informuojama VDAI.

32. Tuo atveju, kai yra įtariama, kad asmens duomenų saugumo pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą.

V SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

33. Tyrimo metu nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo to laiko, kai buvo sužinota apie pažeidimą, praneša apie tai duomenų subjektui, kurio teisėms ir laisvėms gali kilti didelis pavojus.

34. Duomenų subjektas informuojamas siunčiant jam pranešimą paštu, elektroniniu paštu, telefonu ar kitu būdu.

35. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jis turėtų imtis, kad apsisaugotų nuo neigiamų pažeidimo pasekmių. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama ši informacija:

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

35.2. priemonių, kurių ėmėsi Centras, kad būtų pašalintas saugumo pažeidimas;

35.3. duomenų apsaugos pareigūno arba kito atsakingo asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

35.4. kita reikšminga informacija, susijusi su pažeidimu, kuri, duomenų apsaugos pareigūno manymu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

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

36.1. Centras įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio, visų pirma tos priemonės,
kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su duomenimis, jie būtų nesuprantami (pvz., asmens duomenų šifravimo priemonės);

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

36.3. tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai didelių pastangų, pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi. Tokiu atveju apie pažeidimą viešai paskelbiama Centro interneto svetainėje,

spaudoje, pasitelkiami ne vienas, o keli informavimo būdai arba taikomos panašios priemonės, kuriomis duomenų subjektai būtų efektyviai informuojami (pvz., vien tik pranešimas interneto svetainėje nėra efektyvi informavimo priemonė).

VI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMAS

37. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, registruojami Asmens duomenų saugumo pažeidimų registracijos žurnale (3 priedas).

38. Centro Asmens duomenų saugumo pažeidimų registracijos žurnalas yra tvarkomas elektroniniu būdu.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

39. Centro darbuotojai su Aprašu ir jo pakeitimais supažindinami elektroninėmis dokumentų valdymo sistemos priemonėmis per DVS „Kontora".

40. Centro darbuotojai, pažeidę Aprašo reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

Asmens duomenų saugumo pažeidimų valdymo
Vaiko gerovės ir globos centre tvarkos aprašo
1 priedas

(Pranešimo apie galimą asmens duomenų saugumo pažeidimą forma)

_____ (juridinio asmens pavadinimas)

_____
(struktūrinio padalinio pavadinimas)

_____
(pareigų pavadinimas)

_____
(vardas, pavardė)

PRANEŠIMAS
APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____
Šilutė

Informuoju apie galimą asmens duomenų saugumo pažeidimą, pateikdamas man turimą informaciją apie jį:

1. Galimo asmens duomenų saugumo pažeidimo nustatymo data, valanda (minučių tikslumu) ir vieta:
_____

2. Galimo asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta: _____
_____

3. Galimo asmens duomenų saugumo pažeidimo pobūdis, esmė ir aplinkybės _____
_____
_____

4. Duomenų subjektų, kurių asmens duomenų saugumas galimai pažeistas, kategorijos (pvz., darbuotojai, asmenys, pateikę prašymus, skundus ir pan.) ir jų skaičius (jei žinoma)) _____
_____
_
_____
_

5. Asmens duomenų kategorijos, susijusios su galimu asmens duomenų saugumo pažeidimu:
5.1. Asmens duomenys

Vardas	
Pavardė	
Asmens kodas	
Adresas	
Telefono ryšio numeris	
Elektroninio pašto adresas	
Banko sąskaitos numeris	
Banko kortelės numeris	

Prisijungimo duomenys (vartotojo vardas, slaptažodis)	
Asmens dokumento (-ų) duomenys	
Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas	
Kiti duomenys	

5.2. Specialių kategorijų asmens duomenys

Duomenys, susiję su asmens sveikata	
Biometriniai duomenys	
Duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais	
Duomenys, susiję su asmens naryste profesinėse sąjungose	
Duomenys, susiję su asmens rasine ar etnine kilme	
Duomenys, susiję su asmens lytiniu gyvenimu ir lytine orientacija	

6. Kokių veiksmų / priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti kompiuterio slaptažodžiai, nutraukta neteisėta prieiga prie tvarkomų asmens duomenų, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimui skirtoje vietoje palikti dokumentai su asmens duomenimis ir pan.)

_____

_____

_

_____

_____

(pareigos) (parašas) (vardas ir pavardė)

Asmens duomenų saugumo pažeidimų valdymo
Vaiko gerovės ir globos centre tvarkos aprašo
2 priedas

(Asmens duomenų saugumo pažeidimų registracijos žurnalo forma)

VAIKO GEROVĖS IR GLOBOS CENTRO
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRACIJOS ŽURNALAS

Eil. Nr.	Pažeidimo nustatymo data, valanda (minučių tikslumu) ir vieta	Darbuotojas ar kitas subjektas, pranešęs apie pažeidimą (vardas, pavardė, pareigos)	Pažeidimo padarymo data ir vieta	Pažeidimo pradžia ir pabaiga, pobūdis, tipas, aplinkybės	Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius	Asmens duomenų, kurių saugumas pažeistas, kategorijos ir apimtis	Tikėtinos pažeidimo pasekmės bei pavojus fizinių asmenų teisėms ir laisvėms	Priemonės, kurių buvo imtasi pažeidimui pašalinti ir (ar) neigiamoms pažeidimo pasekmėms sumažinti	Darbuotojas, ar kitas subjektas, pašalinęs pažeidimą (vardas, pavardė, pareigos)	Informacija, ar apie pažeidimą buvo pranešta Valstybinei duomenų apsaugos inspekcijai, ir priimto sprendimo motyvai	Informacija, ar apie pažeidimą buvo pranešta duomenų subjektui (-ams), ir priimto sprendimo motyvai
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											

Asmens duomenų saugumo pažeidimų valdymo
Vaiko gerovės ir globos centro tvarkos aprašo
3 priedas

(Asmens duomenų saugumo pažeidimo ataskaitos forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

_____ Nr. _____

1. Asmens duomenų saugumo pažeidimo (toliau – pažeidimas) aprašymas	
1.1. Pažeidimo nustatymo data, laikas (minučių tikslumu) ir vieta	
1.2. Darbuotojas, pranešęs apie pažeidimą (vardas, pavardė, Biuro struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas, telefono Nr., elektroninio pašto adresas)	
1.3. Duomenų valdytojo, pranešusio apie pažeidimą, pavadinimas, jo kontaktinio asmens duomenys (vardas, pavardė, telefono Nr., elektroninio pašto adresas)	
1.4. Pažeidimo padarymo data ir vieta	
1.5. Pažeidimo pobūdis (tipas), esmė ir aplinkybės	
1.5.1. Konfidencialumo pažeidimas	
1.5.2. Vientisumo pažeidimas	
1.5.3. Prieinamumo pažeidimas	
1.5.4. Mišraus pobūdžio (tipo) pažeidimas	
1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir jų skaičius	
1.7. Kaip ilgai tęsėsi pažeidimas?	

1.8. Asmens duomenų kategorijos, susijusios su pažeidimu:	
1.8.1. Asmens duomenys	
1.8.2. Specialių kategorijų asmens duomenys	
1.9. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius	
2. Pažeidimo rizikos įvertinimas	
2.1. Priežastys, lėmusios pažeidimą, ar įvykiai, kurie galėjo turėti įtakos pažeidimo padarymui	
2.2. Pažeidimo pasekmės:	
2.2.1. Sunaikinti asmens duomenys	
2.2.2. Prarasti asmens duomenys	
2.2.3. Pakeisti asmens duomenys	
2.2.4. Be duomenų subjekto sutikimo atskleisti asmens duomenys	
2.2.5. Sudaryta galimybė naudotis asmens duomenimis	
2.2.6. Asmens duomenys, išplitę labiau nei tai yra būtina, ir prarasta duomenų subjekto kontrolė savo asmens duomenų atžvilgiu	
2.2.7. Asmens duomenų susiejimas	
2.2.8. Asmens duomenų panaudojimas neteisėtais tikslais	
2.2.9. Dėl asmens duomenų trūkumo negalima teikti paslaugų	
2.2.10. Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamų paslaugų	
2.2.11. Kita	
2.3. Dėl pažeidimo nėra pavojaus duomenų subjektų teisėms ir laisvėms (maža rizika)	
2.4. Dėl pažeidimo yra / gali kilti pavojus duomenų subjektų teisėms ir laisvėms (būtina pranešti Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) (vidutinė rizika)	

2.5. Dėl pažeidimo yra / gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms (būtina pranešti Inspekcijai ir duomenų subjektams) (didelė rizika)	
2.6. Kas turėjo prieigą prie pažeistų asmens duomenų iki asmens duomenų saugumo pažeidimo padarymo?	
2.7. Kas gavo prieigą prie pažeistų asmens duomenų (jei pažeidimas yra, ar apima asmens duomenų prieinamumo pažeidimą)?	
2.8. Ar iki pažeidimo asmens duomenys buvo tinkamai užkoduoti, anonimizuoti ar kitaip lengvai neprieinami?	
2.9. Informacinės sistemos, įrenginiai, įranga, įrašai, susiję su pažeidimu	
2.10. Ar pažeidimas yra sisteminė klaida, ar vienetinis incidentas?	
2.11. Kokia žala buvo padaryta duomenų subjektams, kurių asmens duomenų saugumas pažeistas, ar Biuras?	
2.12. Kokių veiksmų / priemonių buvo imtasi sužinojus apie padarytą pažeidimą?	
2.13. Kokios taikytos priemonės, siekiant sumažinti ir (ar) pašalinti pažeidimo pasekmes duomenų subjektams?	
2.14. Kokios techninės ir (ar) organizacinės priemonės buvo taikomos pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?	
2.15. Techninės ir (ar) organizacinės priemonės, kurios įgyvendintos dėl pažeidimo, siekiant, kad pažeidimas nepasikartotų	
2.16. Techninės ir (ar) organizacinės priemonės, kurios ketinamos įgyvendinti dėl pažeidimo, įskaitant ir priemones sumažinti pažeidimo pasekmes	
3. Pranešimų pateikimas	
3.1. Ar pranešta duomenų subjektui apie pažeidimą:	
3.1.1. Taip	(Pranešimo turinys ir data)

3.1.2. Ne	
3.2. Jei buvo teikiamas pranešimas duomenų subjektams:	
3.2.1. Pranešimo duomenų subjektui būdas (paštu, elektroninio pašto pranešimu ar SMS pranešimu ir kt.)	
3.2.2. Informuotų duomenų subjektų skaičius	
3.2.3. Vėlavimo pranešti duomenų subjektui apie pažeidimą priežastys	
3.3. Nepranešimo apie pažeidimą duomenų subjektui priežastys:	
3.3.1. Nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos priežastys)	
3.3.2. Biuras įgyvendino tinkamas technines ir organizacines asmens duomenų apsaugos priemones, kurios užtikrino, kad įvykus pažeidimui nekils rizika, ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio (nurodoma, kokios)	
3.3.3. iš karto po pažeidimo Biuras ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti rizika (nurodoma, kokios)	
3.3.4. Reikėtų neproporcingai daug pastangų susisiekti su duomenų subjektais. Informacija apie pažeidimą buvo paskelbta viešai arba taikyta panaši priemonė, kuria duomenų subjektai buvo informuoti taip pat efektyviai (nurodoma, kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma, kokia ir kada taikyta)	
3.3.5. Dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas	
3.4. Ar pranešta Inspekcijai apie asmens duomenų saugumo pažeidimą:	
3.4.1. Taip	(rašto data ir numeris)
3.4.2. Ne	
3.5. Vėlavimo pranešti Inspekcijai apie pažeidimą priežastys	

3.6. Nepranešimo apie pažeidimą Inspekcijai priežastys	
3.7. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie pažeidimą, galimai turintį nusikalstamos veikos požymių:	
3.7.1. Taip	(rašto data ir numeris, adresatas)
3.7.2. Ne	
3.8. Ar pranešta valstybės institucijoms, nurodytoms Lietuvos Respublikos kibernetinio saugumo įstatyme, apie kibernetinį incidentą, susijusį su pažeidimu:	
3.8.1. Taip	(rašto data ir numeris, adresatas)
3.8.2. Ne	
Biuro darbuotojas atsakingas už duomenų apsaugą	(vardas, pavardė, parašas)

_____

Asmens duomenų saugumo pažeidimų valdymo Vaiko gerovės ir globos centre tvarkos aprašo
4 priedas

(Pranešimo apie asmens duomenų saugumo pažeidimą forma)

(duomenų valdytojo (juridinio asmens) pavadinimas)

(juridinio asmens kodas ir buveinės adresas, asmens duomenų tvarkymo vieta)

_____

(telefono ryšio nr. 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. 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 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, mokėtojo 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 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 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 pridėtas pranešimo duomenų subjektui kopija):

_____ 5.4. Būdas, kokiu 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 (darbuotojas atsakingas už duomenų apsaugą 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

Asmens duomenų saugumo pažeidimų valdymo
Vaiko gerovės ir globos centre tvarkos aprašo
5 priedas

(Pranešimo duomenų subjektui apie asmens duomenų saugumo pažeidimą forma)

PRANEŠIMAS DUOMENŲ SUBJEKTUI
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____

Šilutė

Vaiko gerovės ir globos centras (toliau – Centras) praneša apie įvykusį asmens duomenų saugumo pažeidimą ir pateikia šią informaciją:

1. Asmens duomenų saugumo pažeidimo pobūdžio aprašymas	
2. Asmens, galinčio suteikti daugiau informacijos, vardas, pavardė, kontaktiniai duomenys ir (ar) atsakingo už duomenų apsaugą darbuotojo vardas, pavardė, kontaktiniai duomenys	
3. Tikėtinų asmens duomenų saugumo pažeidimo pasekmių aprašymas (tikėtinų pasekmių duomenų subjektui aprašymas)	
4. Priemonės, kurių ėmėsi arba planuoja imtis Centras) tam, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti	*(pvz., apie įvykusį pažeidimą yra pranešta Inspekcijai ir yra gautas patarimas dėl pažeidimo tvarkymo ir jo poveikio sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodį ir kt.);*

_____ _____
(pareigos) (vardas, pavardė)

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Vaiko gerovės ir globos centras
Dokumento pavadinimas (antraštė)	Įsakymas Dėl vaiko gerovės ir globos centro asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo patvirtinimo
Dokumento registracijos data ir numeris	2024-12-20 Nr. V-107 (1.6. E)
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Audronė Čekanskienė Direktorė
Parašo sukūrimo data ir laikas	2024-12-20 09:49
Parašo formatas	Einamojo galiojimo (XAdES-EPES)
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	RCSC IssuingCA
Sertifikato galiojimo laikas	2023-06-28 14:26 - 2025-06-27 14:26
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Sigita Olberkienė Administratorė-Personalo specialistė
Parašo sukūrimo data ir laikas	2024-12-20 09:55
Parašo formatas	Einamojo galiojimo (XAdES-EPES)
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016
Sertifikato galiojimo laikas	2024-01-30 21:22 - 2027-01-30 21:22
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Sigita Olberkienė Administratorė-Personalo specialistė
Parašo sukūrimo data ir laikas	2024-12-20 09:56
Parašo formatas	Einamojo galiojimo (XAdES-EPES)
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016
Sertifikato galiojimo laikas	2024-01-30 21:22 - 2027-01-30 21:22
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	0
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	asmens-duomenų-saugumo-pažeidimų-valdymo-tvarkos-aprašas.docx
Pridedamo dokumento registracijos data ir numeris	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elpako v.20241217.3
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Tikrinant dokumentą nenustatyta jokių klaidų (2024-12-20)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2024-12-20 nuorašą suformavo Sigita Olberkienė
Paieškos nuoroda	-
Papildomi metaduomenys	-