PATVIRTINTA
Vilniaus lopšelio–darželio „Varpelis“
Direktoriaus
2025 m. spalio 3 d. įsakymu Nr. V-84

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

Vilnius
2025

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šis Vilniaus lopšelio-darželio „Varpelis“ (toliau – Įstaiga) asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja asmens duomenų saugumo pažeidimų nustatymą, tyrimą, pašalinimą ir pranešimą apie juos Įstaigoje. Aprašas parengtas vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 (Bendruoju duomenų apsaugos reglamentu, toliau **BDAR**). Vartojamos sąvokos atitinka BDAR apibrėžimus.

2. Šio Aprašo tikslas – užtikrinti, kad visi Įstaigos darbuotojai, dirbantys pagal darbo sutartį (toliau – Darbuotojai), sugebėtų laiku nustatyti galimus asmens duomenų saugumo pažeidimus ir suprastų, kokie veiksmai privalo būti atlikti jiems valdyti. Aprašo privalo laikytis visi Darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino.

II SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ APIBRĖŽIMAS

3. Galimi šie asmens duomenų saugumo pažeidimai:

- **Konfidencialumo pažeidimas:** neleistinas arba netyčinis asmens duomenų atskleidimas ar prieigos prie jų suteikimas.
- **Vientisumo pažeidimas:** neleistinas arba netyčinis asmens duomenų pakeitimas.
- **Prieinamumo pažeidimas:** neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas.

4. Asmens duomenų saugumo pažeidimas gali būti susijęs su viena ar visomis šiomis kategorijomis:

- **Žmogiškosios klaidos:** neteisingam adresatui persiųsti duomenys, palikti dokumentai viešose vietose, pamesti mobilieji įrenginiai.
- **Vagystės:** nešiojamų įrenginių, kuriuose saugomi asmens duomenys, ar popierinių bylų vagystė.
- **Kibernetinės atakos:** duomenų šifravimas kenkėjiškomis programomis, slaptažodžių paviešinimas.
- **Neleistina prieiga:** įgaliotų asmenų patekimas į patalpas, kuriose saugomi duomenys, ar prisijungimas prie informacinių sistemų be leidimo.
- **Techniniai gedimai:** energijos tiekimo sutrikimas, programinės įrangos klaidos, saugumo spragos.
- **Nenumatytos aplinkybės:** gaisras ar vandens užliejimas.

5. Saugumo pažeidimas, galintis kelti pavojų asmenų teisėms ir laisvėms, yra toks, dėl kurio fiziniai asmenys gali patirti žalą, pvz., teisių apribojimą, diskriminaciją, finansinius nuostolius ar reputacijos pakenkimą.

III SKYRIUS
VEIKSMAI GAVUS INFORMACIJA ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

6. Pastebėjęs galimą duomenų saugumo pažeidimą, ar gavęs informacijos apie jį iš išorinių šaltinių, Darbuotojas privalo:

- **Nedelsiant pranešti tiesioginiam vadovui:** tai turi būti atlikta žodžiu (tiesiogiai arba telefonu) arba elektroniniu paštu ne vėliau kaip per **2 darbo valandas** nuo pažeidimo paaiškėjimo momento.
- **Užpildyti pranešimą:** nedelsiant užpildyti "Pranešimą apie asmens duomenų saugumo pažeidimą" ir perduoti jį Įstaigos vadovui ne vėliau kaip per **2 darbo valandas**.
- **Imtis skubių priemonių:** jei įmanoma, Darbuotojas turi imtis priemonių pašalinti pažeidimą ir sumažinti jo neigiamas pasekmes.

IV SKYRIUS
PAŽEIDIMO TYRIMAS IR VALDYMAS

7. Įstaigos vadovas, gavęs Įstaigos darbuotojo pranešimą apie asmens duomenų saugumo pažeidimą:
- **Nagrinėti aplinkybes:** įvertinti, ar padarytas duomenų saugumo pažeidimas, nedelsiant išnagrinėti aplinkybes, apklausti su incidentu susijusius asmenis, surinkti kitą informaciją.
- **Perduoti informaciją** asmens duomenų apsaugos pareigūnui.
- **Konsultuotis:** nustatyti, ar apie pažeidimą būtina pranešti VDAI, jei pažeidimo mastas didelis – konsultuotis su Valstybinės duomenų apsaugos inspekcija (toliau – VDAI).
- **Sprendimas dėl pranešimo:** nustatyti, ar apie pažeidimą būtina pranešti nedelsiant duomenų subjektui.
- **Pasitelkti specialistus:** jei pažeidimas susijęs su elektroninės informacijos saugumu, kompiuterine ar kita IT technika, pasitelkti IT specialistą, ar informacinę sistemą aptarnaujantį administratorių.
- **Įvertinti pažeidimą:** nustatyti, ar pažeidimas įvyko, koks jo pobūdis, priežastys, paveiktų duomenų ir subjektų kategorijos, bei įvertinti padarytą žalą ir galimas pasekmes.
- **Nustatyti priemones:** įvertinti, kokių skubių ir tinkamų priemonių būtina imtis pažeidimui pašalinti (pvz., atkurti duomenis iš atsarginių kopijų).

8. Atliekant tyrimą, Darbuotojai, atsakingi už asmens duomenų tvarkymą, privalo pateikti visą prašomą informaciją asmens apsaugos pareigūnui, taip pat jei dalyvauja Valstybinės duomenų apsaugos inspekcijai.

9. Visi įrodymai turi būti dokumentuojami ir užtikrinamas jų atsekamumas ir pateikimas per numatytą (kuo trumpesnį) periodą.

10. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:
- **Pažeidimo tipas ir mastas:** konfidencialumo užtikrinimo, duomenų vientisumo, IT sistemos ar tinklų sutrikdymo, techninės įrangos pažeidimo, fizinių duomenų vagystės pažeidimas.
- **Duomenų pobūdis ir jautrumas:** ar pažeidimas susijęs su ypatingais asmens duomenimis (pvz., sveikatos duomenys).
- **Panaudotos apsaugos priemonės:** ar duomenys buvo šifruoti ar pseudonimizuoti.
- **Pasekmės duomenų subjektams:** ar pažeidimas sukėlė žalą, pakenkė reputacijai ar sukėlė diskriminaciją.
- **Duomenų kiekis ir skaičius:** kiek duomenų ir duomenų subjektų buvo paveikta.
- **Kiti veiksniai:** pvz., ar duomenys buvo paviešinti.

11. Įstaigos vadovas, konsultuodamasis su asmens duomenų apsaugos pareigūnu, priklausomai nuo konkrečių pažeidimo veiksnių, priima spendimą dėl asmens duomenų pažeidimo pašalinimo žingsnių. Pirmiausia organizuojami veiksmai siekiant sustabdyti tolimesnes galimybes duomenų naudojimui, viešinimui, nutekėjimui, poveikiui, ar kitiems elementams. Tam tikslui gali

būti pasitelkiamas tiek prisijungimo saugos priemonių keitimas, tiek fizinė apsaugą, tiek IT infrastruktūros keitimai, tiek kontaktas su pažeidimo dalyviais, siekiant atgauti, ištrinti ar kitaip apriboti patekimą prie informacijos.

V SKYRIUS
PRANEŠIMAS VDAI IR DUOMENŲ SUBJEKTAMS

12. Įstaiga privalo nedelsdama, bet ne vėliau kaip per 72 valandas nuo pažeidimo paaiškėjimo momento, pranešti VDAI apie asmens duomenų saugumo pažeidimą, nebent pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms. Pranešimas turi būti pateiktas pagal VDAI nustatytą formą ir jame turi būti nurodyta:

- Pažeidimo pobūdis, įskaitant asmens duomenų kategorijas ir apytikrį skaičių.
- Duomenų apsaugos pareigūno kontaktiniai duomenys.
- Galimos pažeidimo pasekmės.
- Siūlomos ir taikomos priemonės pažeidimui pašalinti ir neigiamoms pasekmėms sumažinti.

13. Įstaiga privalo nedelsdama informuoti duomenų subjektą apie asmens duomenų saugumo pažeidimą, jei jis gali sukelti didelę riziką duomenų subjekto teisėms ir laisvėms. Pranešime turi būti aprašyta aiškia ir paprasta kalba. Pranešimas duomenų subjektams nebūtinas, jei:

- Įstaiga jau yra ėmusi tinkamų apsaugos techninių ir organizacinių priemonių, dėl kurių duomenys tapo nesuprantami (pvz., šifravimas).
- Po pažeidimo buvo imtasi priemonių, kurios užtikrino, kad didelė rizika nebeegzistuotų.
- Būtų neproporcingos pastangos informuoti kiekvieną subjektą atskirai (tokiu atveju skelbiamas viešas pranešimas).

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

14. Visi asmens duomenų saugumo pažeidimai registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale.
15. Žurnalas saugomas pagal Įstaigos patvirtintą dokumentacijos planą.
16. Už žurnalo tvarkymą ir saugojimą atsakingas Įstaigos vadovas.
17. Šio Aprašo pažeidimas yra prilyginamas darbo drausmės pažeidimui.