PATVIRTINTA
Kauno lopšelio-darželio „Žuvintas“
direktoriaus 2019 m. gruodžio 31 d.
įsakymu Nr. V-106

KAUNO LOPŠELIO-DARŽELIO „ŽUVINTAS“ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ APTIKIMO, SUSTABDYMO (PAŠALINIMO) IR PRANEŠIMO APIE JUOS TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kauno lopšelio-darželio „Žuvintas“ asmens duomenų saugumo pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie juos tvarkos aprašas (toliau – Tvarkos aprašas) nustato Kauno lopšelio-darželio „Žuvintas“ (toliau – Įstaigos) procesus, kurių reikia laikytis įvykus pažeidimui, atsižvelgiant į atliekamus asmens duomenų tvarkymo veiksmus.

2. Tvarkos 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), 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 įstatymu (toliau - Įstatymas), kitais asmens duomenų saugą reglamentuojančiais teisės norminiais aktais.

3. Tvarkos 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 persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (BDAR 4 straipsnio 12 punktas);

3.2. **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio neatsargiai arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (Įstatymo 2 straipsnio 2 dalis).

4. Apie asmens duomenų saugumo pažeidimą (toliau – Pažeidimas) Įstaiga praneša Valstybinei duomenų apsaugos inspekcijai, pateikdama pranešimą apie asmens duomenų saugumo pažeidimą (toliau – Pranešimas), kurio rekomenduojamą formą patvirtino Valstybinės duomenų apsaugos inspekcijos direktorius 2018 m. gegužės 24 d. įsakymu Nr. 1T-53(1.12.), 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, Įstaiga apie Pažeidimą praneša ir duomenų subjektui.

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ PAŽEIDIMĄ

5. Įstaigos darbuotojai, tvarkantys asmens duomenis atitinkamose srityse, yra atsakingi už Pažeidimų valdymą (toliau – Atsakingi asmenys), pavyzdžiui, už Pažeidimų tyrimą, pranešimų

Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektui teikimą, prevencinių priemonių įdiegimo kontrolę ir pan.

6. Atsakingas asmuo, sužinojęs ar pats nustatęs galimą Pažeidimą arba kai informacija apie galimą Pažeidimą gaunama iš žiniasklaidos ar kito šaltinio, privalo nedelsdamas apie tai informuoti Įstaigos direktorių. Pranešimas galėtų būti pateikiamas žodžiu, raštu ar elektroninėmis priemonėmis.

7. Įstaiga apie Pažeidimą teisės norminių aktų nustatyta tvarka praneša Valstybinei duomenų apsaugos inspekcijai, išskyrus, kai tikėtina, kad toks Pažeidimas nekels pavojaus asmenų teisėms ir laisvėms.

III SKYRIUS
PAŽEIDIMŲ DOKUMENTAVIMAS

8. Visi Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta Valstybinei duomenų apsaugos inspekcijai, ar ne, turėtų būti registruojami Įstaigos Asmens duomenų saugumo pažeidimų registravimo žurnale (toliau – Žurnalas) (Priedas).

9. Informacija apie Pažeidimą į Žurnalą turėtų būti įvedama nedelsiant, ne ilgiau kaip per 5 darbo dienas, kai tik nustatomas Pažeidimo faktas ir įvertinama rizika. Esant būtinybei, Žurnale esanti informacija turėtų būti papildoma ir (ar) koreguojama.

10. Žurnale nurodoma:

10.1. Visi su Pažeidimu susiję faktai – Pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

10.2. Pažeidimo poveikis ir pasekmės;

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

10.4. Priežastys dėl su Pažeidimu susijusių sprendimų priėmimo (pavyzdžiui, kodėl Įstaiga nusprendė nepranešti apie Pažeidimą Valstybinei duomenų apsaugos inspekcijai 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);

10.5. Pranešimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys (jeigu Pranešimą vėluojama pateikti ar Pranešimas teikiamas etapais);

10.6. Informacija, susijusi su pranešimu duomenų subjektui (pavyzdžiui, ar buvo pranešta, kodėl nepranešta ir pan.);

10.7. Kita reikšminga informacija susijusi su Pažeidimu (pvz., kad tyrimo metu nustatyta, jog faktiškai Pažeidimo nebuvo, o buvo tik saugumo incidentas).

11. Žurnalas turėtų būti tvarkomas raštu, įskaitant elektronine formą, ir saugomas pagal Įstaigos patvirtintą dokumentų saugojimo tvarką.

12. Įstaigos direktorius paskiria asmenį (darbuotoją), atsakingą už Žurnalo pildymą.

13. Remdamasi Žurnale pateikta informacija, Valstybinė duomenų apsaugos inspekcija turi galimybę patikrinti, kaip įgyvendinama prievolė pranešti apie Pažeidimus.

14. Žurnale esantys įrašai periodiškai peržiūrimi ir Įstaiga numato, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip bus kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje analogiški Pažeidimai nesikartotų.

IV SKYRIUS
PAŽEIDIMO TYRIMAS

15. Atsakingas asmuo, 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).

16. Galimi Pažeidimo tipai:

16.1. „Konfidencialumo Pažeidimas“ – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

16.2. „Prieinamumo Pažeidimas“ – kai netyčia arba neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;

16.3. „Vientisumo Pažeidimas“ – kai asmens duomenys pakeičiami be leidimo ar netyčia.

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

17. Priklausomai nuo Pažeidimo pobūdžio (tipo), atliekant pirminį tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, turėtų būti išsaugomi esamos situacijos įrodymai bei vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės, pavyzdžiui, duomenų srauto ir prisijungimų analizės įrankiai bei kt.

18. Vertinant riziką, kuri gali atsirasti dėl Pažeidimo, turėtų būti atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika turėtų būti vertinama remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus:

18.1. Pažeidimo tipą;

18.2. Asmens duomenų pobūdį, apimtis (pavyzdžiui, specialių kategorijų asmens duomenys);

18.3. Kaip lengvai identifikuojamas fizinis asmuo;

18.4. Pasekmių rimtumą fiziniams asmenims;

18.5. Specialias fizinio asmens savybes (pavyzdžiui, duomenys susiję su vaikais ar kitais pažeidžiamais asmenimis);

18.6. Nukentėjusiųjų fizinių asmenų skaičių;

18.7. Specialias Įstaigos savybes (pavyzdžiui, veiklos pobūdį).

19. Vertinant riziką, turėtų 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, pavyzdžiui, 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 konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

20. Įvertinus riziką rekomenduotina nustatyti, kad yra:

20.1. Žema rizikos tikimybė;

20.2. Vidutinė rizikos tikimybė;

20.3. Didelė (aukšta) rizikos tikimybė.

21. Išvadą dėl Pažeidimo buvimo ir rizikos fizinių asmenų teisėms bei laisvėms įvertinimo Atsakingas asmuo pateikia Įstaigos direktoriui. Įstaigos direktorius turi priimti sprendimą dėl tolimesnių veiksmų, susijusių su Pažeidimu.

22. Atsakingas asmuo visų pirma turėtų imtis visų tinkamų techninių ir organizacinių priemonių, kad Pažeidimas būtų išsamiai ištirtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje

nepasikartotų. Tuomet Įstaiga pateikia Pranešimą Valstybinei duomenų apsaugos inspekcijai, išskyrus, kai tikėtina, kad toks Pažeidimas nekels pavojaus asmenų teisėms ir laisvėms.

V SKYRIUS
PRANEŠIMAS VALSTYBINEI DUOMENŲ APSAUGOS INSPEKCIJAI

23. Nustačius, kad Pažeidimas buvo ir, kad yra rizika fizinių asmenų teisėms ir laisvėms, Įstaiga nedelsdama, ne vėliau kaip per 72 val. nuo sužinojimo apie Pažeidimą, praneša apie tai Valstybinei duomenų apsaugos inspekcijai.

24. Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie Pažeidimą Valstybinei duomenų apsaugos inspekcijai, Įstaiga praneša.

25. Jeigu, priklausomai nuo Pažeidimo pobūdžio, Įstaigai yra būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su Pažeidimu (pavyzdžiui, dar nėra išsiaiškinta Pažeidimo apimtis), ir per 72 val. nuo sužinojimo apie Pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, Pranešimui reikalinga informacija galėtų būti teikiama etapais. Esant galimybei, apie informacijos teikimą etapais, Valstybinei duomenų apsaugos inspekcijai turėtų būti informuota teikiant pirminį Pranešimą.

26. Jeigu po Pranešimo Valstybinei duomenų apsaugos inspekcijai pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo jokio Pažeidimo, apie tai nedelsiant turėtų būti informuojama Valstybinei duomenų apsaugos inspekcija ir pažymėta Žurnale.

27. Jeigu Pažeidimas paveikia fizinių asmenų duomenis daugiau negu vienoje valstybėje narėje ir yra reikalinga pranešti Valstybinei duomenų apsaugos inspekcijai, Įstaiga praneša vadovaujančiai priežiūros institucijai (BDAR preambulės 55 punktas). Jeigu Įstaiga abejoja, kuri priežiūros institucija yra vadovaujanti, bet Pažeidimas įvyko Lietuvos Respublikoje, tuomet jis turėtų pranešti Valstybinei duomenų apsaugos inspekcijai. Šiuo atveju, teikiant Pranešimą, nurodoma, ar toks Pažeidimas apima ir kitose valstybėse narėse esančias duomenų valdytojo buveines, ir kuriose valstybėse narėse esančius duomenų subjektus Pažeidimas galėjo paveikti.

VI SKYRIUS
PRANEŠIMAS DUOMENŲ SUBJEKTUI

28. Nustačius, kad Pažeidimas buvo ir, kad yra didelė rizika fizinių asmenų teisėms ir laisvėms, Atsakingas asmuo nedelsdamas, ne vėliau kaip per 72 val., apie tai praneša duomenų subjektui, kurio teisėms ir laisvėms dėl šio Pažeidimo gali kilti didelis pavojus.

29. Valstybinės duomenų apsaugos inspekcijos informavimas apie Pažeidimą neatleidžia Įstaigos nuo pareigos informuoti duomenų subjektą.

30. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama:

30.1. Pažeidimo pobūdžio aprašymas;

30.2. Įstaigos kontaktinio asmens vardas, pavardė ir kontaktiniai duomenys;

30.3. Tikėtinų Pažeidimo pasekmių aprašymas;

30.4. Priemonių, kurių ėmėsi Įstaiga, kad būtų pašalintas Pažeidimas, įskaitant (kai tinkama) priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas (pavyzdžiui, kad apie Pažeidimą yra informuota Valstybinė duomenų apsaugos inspekcija ir, kad yra gautas patarimas dėl Pažeidimo tvarkymo ir jo poveikio sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);

30.5. Kita reikšminga informacija, susijusi su Pažeidimu, kuri, duomenų valdytojo manymu, turėtų būti pateikta duomenų subjektui.

31. Duomenų subjektai apie Pažeidimą informuojami tiesiogiai, siunčiant jiems pranešimą el. paštu, SMS, paštu ar pan. Šis pranešimas turėtų būti atskirtas nuo kitos siunčiamos informacijos, tokios kaip nuolatiniai atnaujinimai, naujienlaiškiai ar standartiniai pranešimai.

32. 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, pavyzdžiui, pranešimas žinomos interneto svetainės antraštėje ar pranešimuose, žinomos reklamos spausdintoje žiniasklaidoje ar pan.

33. Įstaiga pasirenka tokius pranešimo duomenų subjektui būdus, kurie maksimaliai didintų galimybę tinkamai pranešti informaciją visiems nukentėjusiems asmenims.

34. Įstaiga gali pasirinkti kelis pranešimo duomenų subjektui apie Pažeidimą būdus.

35. Esant Pažeidimui, pranešimo duomenų subjektui teikti nereikia, jeigu:

35.1. Įstaiga įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikio;

35.2. Iš karto po Pažeidimo Įstaiga ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus asmenų teisėms ir laisvėms;

35.3. Tai pareikalautų neproporcingai daug pastangų susisiekti su asmenimis (pavyzdžiui, 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.

36. Jeigu tiriant Pažeidimą pradžioje nustatoma, kad nėra pavojaus fizinių asmenų teisėms ir laisvėms, tačiau detalesnio Pažeidimo tyrimo metu nustatoma, kad toks pavojus gali kilti, Įstaiga riziką vertina iš naujo.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

37. Šis Tvarkos aprašas peržiūrimas ir atnaujinamas esant būtinybei, tačiau ne rečiau kaip kartą per du metus arba pasikeitus teisės norminiams aktams, kurie reglamentuoja asmens duomenų tvarkymą.

38. Darbuotojai ir kiti atsakingi asmenys su šiuo Tvarkos aprašu yra supažindinami pasirašytinai arba elektroninėmis priemonėmis ir privalo laikytis jame nustatytų įpareigojimų.

39. Įstaiga turi teisę iš dalies arba visiškai pakeisti šį Tvarkos aprašą. Su pakeitimais darbuotojai ir kiti atsakingi asmenys yra supažindinami pasirašytinai arba elektroninėmis priemonėmis.

_____

Kauno lopšelio - darželio "Žuvintas" asmens duomenų saugumo pažeidimų aptikimo, sustabdymo (pašalinimo) ir ir pranešimo apie juos tvarkos aprašo

Priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Pažeidimo nustatymo data, laikas ir vieta	Darbuotojas ar duomenų tvarkytojas, pranešęs apie pažeidimą (vardas, pavardė, pareigos ar pavadinimas)	Pažeidimo padarymo data ir vieta	Pažeidimo pobūdis, priežastys ir kitos aplinkybės	Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius	Asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius	Tikėtinos pažeidimo pasekmės bei pavojus fizinių asmenų teisėms ir laisvėms	Priemonės , kurių buvo imtasi pažeidimui pašalinti ir (ar) neigiamoms pažeidimo pasekmėms sumažinti	Informacija, ar apie pažeidimą buvo pranešta Valstybinei duomenų apsaugos inspekcijai, priimto sprendimo motyvai	Informacija, ar apie pažeidimą buvo pranešta duomenų subjektui/ams, priimto sprendimo motyvai	Kita informacija, susijusi su asmens duomenų saugumo pažeidimu