ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO ATASKAITA

202 __ m. _____ mėn. ___ d.
Nr. _____

DUOMENŲ VALDYTOJAS	
Vilniaus darželis-mokykla „Saulutė", juridinio asmens kodas:190022061. Buveinės ir korespondencijos adresas: Miglos g.1. LT-08101 Vilnius. Tel. Nr.: +370 5 275 6056, el. paštas: rastine@saulute.vilnius.lm.lt	
1. Asmens duomenų saugumo pažeidimo apibūdinimas	
1.1. Asmens duomenų saugumo pažeidimo data ir laikas *(valandų ir minučių tikslumu)*:	
1.2. Asmens duomenų saugumo pažeidimo nustatymo data ir laikas *(valandų ir minučių tikslumu)*:	
1.3. Subjektas arba šaltinis, iš kurio gauta informacija apie asmens duomenų saugumo pažeidimą: *(Pranešėjo vardas, pavardė, kito šaltinio pavadinimas ir kontaktiniai duomenys)*	
1.4. Asmens duomenų saugumo pažeidimo vieta: a) Informacinė sistema; b) Duomenų bazė; c) Tarnybinė stotis; d) Internetinė svetainė; e) Debesų kompiuterijos paslaugos; f) Nešiojamieji / mobilieji įrenginiai; g) Neautomatiniu būdu susistemintos bylos (archyvas); h) Kita	
1.5. Asmens duomenų saugumo pažeidimo pobūdis, esmė ir aplinkybės: a) asmens duomenų konfidencialumo praradimas *(neautorizuota prieiga ar atskleidimas);* b) asmens duomenų vientisumo praradimas *(neautorizuotas asmens duomenų pakeitimas);* c) asmens duomenų prieinamumo praradimas *(asmens duomenų praradimas, sunaikinimas)*; d) Kita.	
1.6. Nukentėjusių ar galinčių nukentėti duomenų subjektų kategorijos ir jų skaičius: a) Darbuotojai; b) Duomenų tvarkytojo darbuotojai; c) Klientai; d) Vaikai; e) Vaikų tėvai ar globotiniai; f) Kiti duomenų subjektai.	

1.7. Duomenų subjektų asmens duomenų kategorijos, susijusios su asmens duomenų saugumo pažeidimu: a) asmens tapatybę patvirtinantys asmens duomenys *(vardas, pavardė, amžius, gimimo data, asmens kodas, lytis ir kt.);* b) finansiniai duomenys *(Banko sąskaitos Nr. ir kt).*; c) prisijungimo prie IT sistemų duomenys ir (ar) asmens identifikaciniai numeriai *(pvz., asmens kodas, mokėtojo kodas, slaptažodžiai)*; d) specialių kategorijų asmens duomenys *(pvz., 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)*; e) kiti duomenys ir informacija.	
1.8. Apytikslis nukentėjusių ar galinčių nukentėti duomenų subjektų skaičius:	
1.9. Kaip ilgai tęsėsi asmens duomenų saugumo pažeidimas?	
2. Asmens duomenų saugumo pažeidimo rizikos įvertinimas	
2.1. Priežastys, lėmusios asmens duomenų saugumo pažeidimą *(pvz., duomenų ar įrangos, kurioje yra saugomi asmens duomenys, vagystė, netinkamos prieigos kontrolės priemonės, leidžiančios neteisėtai naudotis asmens duomenimis, įrangos gedimas, žmogiška klaida, įsilaužimo ataka ir pan.).*	
2.2. Asmens duomenų saugumo pažeidimo tikėtinos pasekmės nukentėjusiems ar galintiems nukentėti duomenų subjektams: *(Nurodyti yra arba nėra, ar gali kilti pasekmės ir aprašyti, koks pasekmių sunkumo laipsnis (mažas, vidutinis, didelis, kritinis)*	
2.3. Išsamiai pagrįsti tikėtinos pasekmės nukentėjusiems ar galintiems nukentėti duomenų subjektams rizikos lygį, aprašant, kaip asmens duomenų saugumo pažeidimas daro poveikį duomenų subjektų teisėms ir interesams: *- asmens duomenys išplito internete ir galimas asmens duomenų panaudojimas neteisėtais tikslais;* *- asmens duomenys yra prarasti ar sunaikinti atsitiktinai arba neteisėtai;* *- asmens duomenys yra atsitiktinai arba neteisėtai pakeisti be duomenų subjekto sutikimo;* *- asmens duomenys yra atskleisti be duomenų subjekto sutikimo ir sudaryta galimybė naudotis jo asmens duomenimis;* *- asmens duomenys pakeisti į neteisingus duomenis, dėl ko duomenų subjektas gali netekti galimybės naudotis teikiamomis paslaugomis;* *- dėl asmens duomenų trūkumo ir padarytų klaidų asmens duomenų tvarkymo procesuose toliau nėra galimybės teikti tinkamas paslaugas;* *- kitos tikėtinos pasekmės nukentėjusiems ar galintiems nukentėti duomenų subjektams.*	

2.4. Kokia žala buvo padaryta duomenų subjektams dėl asmens duomenų saugumo pažeidimo? (*Pvz., grėsmė fiziniam saugumui, grėsmė emocinei gerovei, žala reputacijai, finansinė žala, kita žala)*	
2.5. Kas turėjo prieigą prie pažeistų asmens duomenų iki asmens duomenų saugumo pažeidimo padarymo?	
2.6. Ar iki asmens duomenų saugumo pažeidimo padarymo buvo fiksuota kitų įvykių, kurie galėjo turėti poveikį asmens duomenų saugumo pažeidimo padarymui?	
2.7. Ar tai yra sisteminė klaida ir/ar vienetinis įvykis (incidentas)?	
2.8. Ar iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai apsaugoti ir tvarkomi? *(Pvz., užkoduoti, anonimizuoti ar kitaip lengvai neprieinami prie IT sistemos)*	
3. Priemonės, kurių imtasi, kad būtų pašalintas asmens duomenų saugumo pažeidimas ar būtų sumažintos jo neigiamos pasekmės ir kad asmens duomenų saugumo pažeidimas nepasikartotų ateityje	
3.1. Kokių veiksmų / priemonių buvo imtasi, siekiant pašalinti asmens duomenų saugumo pažeidimą ar sumažinti jo pasekmes?	
3.2. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, siekiant užkirsti kelią analogiškiems ir panašiems pažeidimams ateityje?	
3.3. Kokios organizacinės priemonės buvo taikomos, siekiant užkirsti kelią analogiškiems ir panašiems pažeidimams ateityje ir užtikrinti asmens duomenų saugumą ?	
3.4. Kokios techninės ir/ar organizacinės priemonės siūlomos, siekiant sumažinti įvykusio asmens duomenų saugumo pažeidimo pasekmes?	
4. Pranešimų pateikimas Valstybinei duomenų apsaugos inspekcijai	
4.1. Kada buvo pateiktas pranešimas Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų saugumo pažeidimą (pranešimo data ir numeris)? *(Atsižvelgiant į tyrimo metų nustatytos rizikos duomenų subjektui (subjektams) lygį, per 72 val. nuo sužinojimo apie asmens duomenų saugumo pažeidimą privaloma pranešti VDAI pagal nustatytą formą (Priedas Nr. 1.); kai nėra rizikos arba kitais atvejais priimtas sprendimas nepranešti apie pažeidimą VDAI, būtina nurodyti, kas priėmė tokį sprendimą)*	
4.2. Nepranešimo apie asmens duomenų saugumo pažeidimą Valstybinei duomenų apsaugos inspekcijai priežastys. *(Kai asmens duomenų saugumo pažeidimo tyrimo metu nėra nustatytos rizikos arba priimtas sprendimas nepranešti apie pažeidimą VDAI, būtina nurodyti, kas ir kada priėmė tokį sprendimą)*	

4.3. Vėlavimo pranešti inspekcijai apie asmens duomenų saugumo pažeidimą priežastys. *(Nurodyti, kas ir kada priėmė tokį sprendimą)*	
5. Pranešimų pateikimas duomenų subjektams	
5.1. Kada buvo pateiktas pranešimas duomenų subjektui (subjektams) apie asmens duomenų saugumo pažeidimą? *(Nurodykite pranešimo datą ir numerį)*	
5.2. Duomenų subjektų apie asmens duomenų saugumo pažeidimą ir rizikas informavimo būdas: *(Paštu, el. pašto pranešimu ar SMS pranešimu ir kt.)*	
5.3. Informuotų apie asmens duomenų saugumo pažeidimą duomenų subjektų skaičius:	
5.4. Neinformavimo apie asmens duomenų saugumo pažeidimą duomenų subjektų priežastys: a) bus informuotas vėliau; b) duomenų subjektas tokią informaciją jau turi; c) nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms *(nurodomos priežastys)*; d) įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms *(nurodomos, kokios)*; e) nes tai pareikalautų neproporcingai daug pastangų ir apie tai yra viešai paskelbta *(nurodoma, kada ir kur paskelbta informacija viešai, arba, jei taikyta kita priemonė, nurodoma, kokia ir kada taikyta)*; f) nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas.	

Už asmens duomenų saugumo pažeidimų tyrimą ir valdymą atsakingas duomenų valdytojo darbuotojas:

_____

(vardas, pavardė, parašas)