

PATVIRTINTA  
Alytaus Senamiesčio pradinės mokyklos  
direktoriaus 2020 m. sausio 6 d.  
įsakymu Nr. V-3(1.2.)

## ALYTAUS SENAMIESČIO PRADINĖS MOKYKLOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

### I SKYRIUS BENDROSIOS NUOSTATOS

1. Alytaus Senamiesčio pradinės mokyklos asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo (toliau – Aprašas) tikslas – nustatyti duomenų tvarkymo metu įvykusių asmens duomenų saugumo pažeidimų valdymo, tyrimo, pašalinimo ir pranešimų apie įvykusį Pažeidimą (toliau – Pranešimas) Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI arba priežiūros institucija) ir (ar) duomenų subjektams įgyvendinimo tvarką Alytaus Senamiesčio pradinėje mokykloje (toliau – Mokykla), užtikrinti, kad Mokyklos darbuotojai sugebėtų laiku nustatyti galimus Pažeidimus bei suprastų, kokie veiksmai privalo būti atlikti valdant juos.

2. Pagrindinės taisyklėse vartojamos sąvokos:

2.1. **Asmens duomenų saugumo pažeidimas** (neatitiktis) (toliau – Pažeidimas) – duomenų 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;

2.2. **Informacijos saugumo incidentas** – vienas ar daugiau nepageidaujamų ir netikėtų informacijos saugumo įvykių, turinčių didelę tikimybę pakenkti veiklai ir keliančių grėsmę informacijos saugumui;

2.3. **Duomenų apsaugos pareigūnas** (toliau – Pareigūnas) – Mokyklos vadovo paskirtas darbuotojas ar paslaugų teikėjas, atliekantis BDAR nustatytas duomenų apsaugos pareigūno funkcijas;

2.4. **Įgaliotas (-i) darbuotojas (-ai)** – Mokyklos vadovo paskirtas darbuotojas (-ai) atsakingas(-i) už Pažeidimų tyrimą, pašalinimą ir pranešimą apie juos priežiūros institucijai ir duomenų subjektams.

3. Tiriant galimus Pažeidimus ir teikiant Pranešimus vadovaujamosi 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 teisinės apsaugos įstatymu (toliau – ADTAĮ) ir kitais teisės aktais, kurie nustato šių procedūrų atlikimo tvarką.

4. Kitos, aukščiau nenurodytos Apraše vartojamos sąvokos atitinka ADTAĮ ir BDAR vartojamas sąvokas.

### II SKYRIUS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMAS

5. Galimi šie Pažeidimai pagal pobūdį (tipą):

5.1. konfidencialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie jų suteikimas (pavyzdžiui, atskleisti duomenys ir jie tapo prieinami tretiesiems asmenims, suteikiant prieigą, tinkamai nešifruojant, kt.);

5.2. duomenų pasiekiamumo / prieinamumo – neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas (pavyzdžiui, prarasti duomenys ir neturima atsarginių kopijų);

5.3. duomenų vientisumo pažeidimas – neleistinas arba netyčinis asmens duomenų pakeitimas (pavyzdžiui, prarasti vaikų duomenys, turima tik dalis atsarginių kopijų, dėl ko neįmanoma „atkurti“ visos su vaiku bendravimo istorijos);

5.4. mišraus pobūdžio (tipo) pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių aukščiau nurodytų pažeidimų derinys.

6. Pažeidimas gali įvykti dėl šių priežasčių:

6.1. žmogiškoji klaida (pvz., asmens duomenys persiųsti ne tam adresatui, kuriam jie buvo skirti; ne saugojimui skirtoje vietoje palikti dokumentai, kuriuose yra asmens duomenų; pamesti nešiojami / mobilūs įrenginiai (telefonas, nešiojamas kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys ir kt.);

6.2. vagystė (pvz., pavogti nešiojami / mobilūs įrenginiai, kuriuose saugomi asmens duomenys; pavogtos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų ir kt.);

6.3. 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.);

6.4. 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.);

6.5. 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.);

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

7. 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.

### **III SKYRIUS**

#### **PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

8. Mokyklos darbuotojas, pastebėjęs, nustatęs, gavęs informaciją apie galimą Pažeidimą iš duomenų tvarkytojo ar kito šaltinio, privalo:

8.1. nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo galimo Pažeidimo paaiškėjimo momento informuoti žodžiu, raštu ar elektroninėmis priemonėmis Mokyklos vadovo įgaliotą darbuotoją ir Pareigūną;

8.2. užpildyti Pranešimą apie asmens duomenų saugumo pažeidimą (toliau – Pranešimas) (Aprašo priedas Nr. 1) ir nedelsiant, bet ne vėliau kaip per 4 darbo valandas nuo galimo Pažeidimo paaiškėjimo momento perduoti jį Mokyklos vadovo įgaliotam darbuotojui, o jo kopiją – Pareigūnui;

8.3. jei įmanoma, imtis priemonių pašalinti galimą Pažeidimą ir imtis priemonių galimoms neigiamoms jo pasekmėms sumažinti.

### **IV SKYRIUS**

#### **ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS**

9. Mokyklos vadovo įgaliotas darbuotojas, gavęs Pranešimą apie Pažeidimą, privalo:

9.1. atlikti Pažeidimo tyrimą ir nedelsdamas, bet ne vėliau kaip per 24 valandas nuo Pranešimo gavimo momento nagrinėti Pranešime nurodytas aplinkybes;

9.2. įvertinti, ar padarytas Pažeidimas;

9.3. konsultuotis su Pareigūnu;

9.4. jei Pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkti Mokyklos ar duomenų tvarkytojo IT specialistus, informacinių sistemų saugos įgaliotinį;

9.5. jei Pažeidimas padarytas, nustatyti, kokio pobūdžio (tipo) Pažeidimas padarytas, asmens duomenų, kurių saugumas pažeistas, kategorijas, įskaitant specialių kategorijų asmens duomenis, Pažeidimo priežastis, Pažeidimo apimtį (duomenų subjektų kategorijos ir jų skaičius), esamas ir (ar) galimas pasekmės ir žalą, padarytą duomenų subjektui (-ams), įvertinti pavojų duomenų subjekto teisėms ir laisvėms (toliau – rizika), kuris gali atsirasti dėl galimo Pažeidimo, pateikti užpildytą

Pareigūnui Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (toliau – Ataskaita) (Aprašo priedas Nr. 2) dėl pažeidimo buvimo ir rizikos;

9.6. teikti rekomendacijas Mokyklos darbuotojams, atsakingiems už Pažeidimo ir (ar) jo pasekmių pašalinimą ir (ar) sumažinimą, ir (ar) duomenų tvarkytojui dėl tinkamų techninių ir organizacinių priemonių, kad Pažeidimas būtų išsamiai ištirtas ir jis ir (ar) jo pasekmės būtų pašalintos ir (ar) sumažintos ir pažeidimas ateityje nepasikartotų, taikymo ir (arba) pats imtis šių veiksmų;

9.7. įvertinti, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas Pažeidimas;

9.8. nustatyti, ar apie Pažeidimą būtina pranešti VDAI;

9.9. nustatyti, ar apie Pažeidimą būtina pranešti duomenų subjektams.

10. Pareigūnas, gavęs Pranešimą privalo:

10.1. Mokyklos vadovo įgaliotam asmeniui patarti dėl Pažeidimo tyrimo ir teikti išvadas dėl Pranešimo teikimo VDAI ir (ar) duomenų subjektui;

10.2. bendradarbiauti su VDAI dėl pažeidimų;

10.3. stebėti, kaip vykdomos BDAR ir Apraše nustatytos Mokyklos pareigos, susijusios su Pažeidimų valdymu.

11. Atliekant Pažeidimo tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas.

12. Pažeidimo tyrimo metu darbuotojai ir duomenų tvarkytojas privalo operatyviai teikti Mokyklos vadovo įgaliotam asmeniui visą jo paprašytą su Pažeidimu susijusią informaciją ir dokumentus.

13. 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:

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

13.2. 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;

13.3. galimybė identifikuoti fizinį asmenį – įvertinama, ar neį galiojantiems 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 neįgaliojantiems asmenims, todėl pažeidimas padarys mažesnę poveikį duomenų subjektams);

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

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

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

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

15. Ataskaita yra pateikiama Mokyklos vadovui ir duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

16. Atsižvelgiant į Ataskaitą, Mokyklos vadovas jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl Pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

17. Sprendžiant Pažeidimo pašalinimo klausimą, bei tvirtinant priemonių planą, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą. Priklausomai nuo konkrečių Pažeidimo aplinkybių, turėtų būti atlikti tokie veiksmai, kaip: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamo / mobilaus įrenginio (telefono, nešiojamo 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.

18. Siekiant apriboti ar sustabdyti 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.).

19. Priemonių plane turi būti numatyti veiksmai, nukreipti ne vien į esamo Pažeidimo priežasties pašalinimą, pavojaus fizinių asmenų teisėms ir laisvėms sumažinimą ar pašalinimą, bet taip pat skirti neleisti pasikartoti Pažeidimui. Būtina atsižvelgti į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant Pažeidimą bei imtis priemonių tuos trūkumus pašalinti.

## **V SKYRIUS**

### **PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI**

20. Tyrimo metu nustatė, kad Pažeidimas buvo, Mokyklos vadovui priėmus sprendimą dėl Pranešimo priežiūros institucijai pateikimo būtinybės, Mokyklos vadovo įgaliotas darbuotojas privalo nedelsiant, bet ne vėliau nei kaip per 72 val. nuo tada, kai tapo žinoma apie Pažeidimą, apie tai informuoti VDAI, išskyrus atvejus, kai Pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms.

21. VDAI informuojama Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto VDAI direktoriaus 2018 m. liepos 27 d. įsakymu Nr. 1T-72(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“ (su visais aktualiais pakeitimais), nustatyta tvarka ir sąlygomis, užpildant Pranešimo apie asmens duomenų saugumo pažeidimo formą, patvirtintą VDAI direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“ (Aprašo priedas Nr. 3).

22. Jeigu įvertinus riziką, abejojama, ar Pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.

23. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie Pažeidimą VDAI pranešti nereikia, po kurio laiko situacija gali pasikeisti, todėl Pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., pamesta USB atmintinė, kurioje saugomi asmens duomenys, užšifruoti taikant pažangų algoritmą – jeigu yra atsarginės duomenų kopijos ir nėra pavojaus šifro saugumui, apie tokį saugumo pažeidimą pranešti VDAI nereikia, tačiau jei vėliau paaiškėja, kad gali kilti pavojus šifro saugumui, pažeidimo keliamas pavojus bus vertinamas iš naujo ir apie tokį pažeidimą reikės pranešti VDAI).

24. 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.

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

26. Tuo atveju, kai yra įtariama, kad Pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, teisės aktų, reguliuojančių tokios informacijos teikimą, nustatyta tvarka.

## **VI SKYRIUS**

### **PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI**

27. Tyrimo metu nustatė, kad dėl Pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Mokyklos vadovo įgaliotas darbuotojas 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.

28. Duomenų subjektas informuojamas tiesiogiai, t. y. siunčiant jam pranešimą paštu, elektroniniu paštu, trumpąja žinute (SMS) ar kitu būdu. Pranešimas duomenų subjektui siunčiamas atskirai nuo kitos siunčiamos informacijos, kaip naujienlaiškiai ar standartiniai pranešimai.

29. 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:

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

29.2. priemonių, kurių ėmėsi Mokykla, kad būtų pašalintas saugumo pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti aprašymas;

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

29.4. kita reikšminga informacija, susijusi su pažeidimu, kuri, Mokyklos vadovo įgalioto darbuotojo manymu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

30. Pranešimo apie Pažeidimą duomenų subjektams teikti nereikia jeigu:

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

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

30.3. 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 Mokyklos 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).

31. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie Pažeidimą duomenų subjektams pranešti nereikia, po kurio laiko situacija gali pasikeisti, todėl Pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą ir duomenų bazėje esantys asmens duomenys užšifruojami – jei atlikus tyrimą, paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenis ir jokio kito kenksmingo poveikio duomenų bazei nėra, apie saugumo pažeidimą reikės pranešti tik VDAI, tačiau jei vėliau paaiškėja, kad prarastas ne tik duomenų prieinamumas, bet ir konfidencialumas, saugumo pažeidimo keliamas pavojus bus vertinamas iš naujo bei sprendžiama, ar atsižvelgiant į tikėtinas saugumo pažeidimo pasekmes reikia apie jį pranešti duomenų subjektams).

32. Tam tikromis aplinkybėmis, kai tai yra pagrįsta, Mokykla pasitarusi su teisėsaugos institucijomis ir atsižvelgdama į teisėtus teisėsaugos interesus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą apie saugumo pažeidimą iki to laiko, kai tai netrukdytų saugumo pažeidimo tyrimams.

## **VII SKYRIUS**

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

33. Visi Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI ir (ar) duomenų subjektui, ar tokie pažeidimai kelia riziką, registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale (Aprašo priedas Nr. 4) (toliau – Žurnalas).

34. Informacija apie Pažeidimą į Žurnalą turi būti įvedama nedelsiant, kai tik paaiškėja galimas Pažeidimas, bet ne vėliau kaip per 5 darbo dienas nuo galimo pažeidimo paaiškėjimo momento. Kai pasikeičia Žurnale nurodyta informacija arba paaiškėja nauja informacija, Žurnale esanti informacija turi būti papildoma ir (ar) koreguojama.

35. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

35.1. pažeidimo nustatymo aplinkybės (pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);

35.2. pažeidimo aplinkybės (pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

- 35.3. tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;
- 35.4. priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;
- 35.5. informacija apie pranešimą VDAI apie asmens duomenų saugumo pažeidimą;
- 35.6. jei apie asmens duomenų saugumo pažeidimą nebuvo pranešta VDAI, nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta VDAI, nurodoma pranešimo data ir numeris, taip pat, ar pranešimas teikiamas etapais;
- 35.7. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti VDAI, nurodomos tokio vėlavimo priežastys;
- 35.8. informacija apie pranešimą duomenų subjektui (subjektams) apie asmens duomenų saugumo pažeidimą;
- 35.9. jei apie asmens duomenų saugumo pažeidimą nebuvo pranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);
- 35.10. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodomos tokio vėlavimo priežastys;
- 35.11. kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.
36. Už Žurnalo pildymą ir saugojimą atsakingas Mokyklos raštinės administratorius. Žurnalas gali būti popierinės arba elektroninės formos. Užpildytas Žurnalas saugomas 5 metus nuo paskutinio įrašo Žurnale padarymo dienos.
37. Žurnalas yra pateikiamas VDAI jai pareikalavus.

## **VIII SKYRIUS BAIGIAMOSIOS NUOSTATOS**

38. Aprašas skirtas užtikrinti, kad Mokyklos darbuotojai sugebėtų laiku nustatyti galimus Pažeidimus bei suprastų, kokie veiksmai privalo būti atlikti valdant juos.
39. Aprašo privalo laikytis visi Mokyklos darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino.
40. Šio Aprašo rekomenduojama laikytis juridiniams asmenims, esantiems Mokyklos duomenų tvarkytojams, kuriems pagal BDAR 33 str. 2 d. yra nustatyta prievolė pranešti Mokyklai apie kiekvieną Pažeidimą.
41. Mokyklos darbuotojai ir duomenų tvarkytojai privalo išsaugoti esamos situacijos, susijusios su galimu Pažeidimu, įrodymus, kad vėliau naudojant technines ir organizacines priemones (pvz., duomenų srauto ir prisijungimų analizės įrankius ar kt.) galima būtų tirti Pažeidimą.
42. Mokyklos darbuotojai su šiuo Aprašu bei jo pakeitimais supažindinami pasirašytinai.
43. Mokyklos darbuotojai, pažeidę šio Aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.
44. Aprašo priedai, jeigu tokių yra, tampa neatsiejama šio Aprašo dalimi.

**(Pranešimo apie asmens duomenų saugumo pažeidimą forma Įstaigos viduje)**

\_\_\_\_\_

(juridinio asmens pavadinimas)

\_\_\_\_\_

(struktūrinio padalinio pavadinimas)

\_\_\_\_\_

(pareigų pavadinimas)

\_\_\_\_\_

(vardas, pavardė)

**PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

\_\_\_\_\_ Nr. \_\_\_\_\_

(data, dokumento numeris)

\_\_\_\_\_

(miestas)

Informuoju apie asmens duomenų saugumo pažeidimą, pateikdamas turimą informaciją:

1. Asmens duomenų saugumo pažeidimo nustatymo data, laikas ir vieta:
2. Asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta:
3. Asmens duomenų saugumo pažeidimo esmė ir aplinkybės:
4. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (pvz., Įmonės darbuotojai, asmenys, pateikę prašymus, skundus, asmenys, užsisakę Įmonės naujienlaiškius ir kt.) ir apytikslis jų skaičius:
5. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us):
  - Asmens tapatybę patvirtinantis duomenys (vardas, pavardė, gimimo data, lytis ir kt.)
  - Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.)
  - Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.)
  - Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.)
  - Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas
  - Kiti asmens duomenys (įrašyti):
6. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

7. Kokių veiksmų (priemonių) buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti prisijungimo prie informacinės sistemos slaptažodžiai, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimui skirtose vietose palikti dokumentai su asmens duomenimis ir kt.):

---

(pareigos)

(parašas)

---

(vardas ir pavardė)



(Asmens duomenų saugumo pažeidimo tyrimo ataskaitos forma)

**ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO ATASKAITA**

\_\_\_\_\_ Nr. \_\_\_\_\_

(data, dokumento numeris)

**1. Asmens duomenų saugumo pažeidimo aprašymas**

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 (įrašyti):

---

1.3. Asmens duomenų saugumo pažeidimo pobūdis (pažymėti tinkamą (-us)):

- Konfidencialumo pažeidimas (neautorizuota prieiga ar atskleidimas)
- Vientisumo pažeidimas (neautorizuotas asmens duomenų pakeitimas)
- Prieinamumo pažeidimas (asmens duomenų praradimas, sunaikinimas)

1.4. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us) ir aprašyti):

- Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.):
- Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.):
- Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.):
- Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilmė, duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.):
- Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:
- Kiti asmens duomenys:

1.5. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (Administracijos darbuotojai, asmenys, pateikę prašymus, skundus, asmenys, užsisakę Savivaldybės naujienlaiškius ir kt.):

1.7. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:

1.8. Darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, Administracijos struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas, telefono numeris, elektroninio pašto adresas):

---

1.9. Duomenų tvarkytojas, pranešęs apie asmens duomenų saugumo pažeidimą (pavadinimas, kontaktinio asmens duomenys (vardas, pavardė, telefono numeris, elektroninio pašto adresas):

---

## **2. Asmens duomenų saugumo pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms įvertinimas**

2.1. Specifiniai fizinių asmenų, kurių asmens duomenų saugumas buvo pažeistas, ypatumai (vaikai, asmenys su negalia ir kt.):

---

2.2. Galimybė identifikuoti fizinį asmenį (pvz., iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užšifruoti, anonimizuoti, arba iki saugumo pažeidimo asmens duomenims šifravimas nebuvo taikomas ir kt.):

---

2.3. Kas gavo prieigą prie asmens duomenų, kurių saugumas pažeistas?

---

2.4. Ar buvo kokių kitų įvykių ar aplinkybių, turėjusių poveikį asmens duomenų saugumo pažeidimo padarymui?

