

## **PANEVĖŽIO R. PAŽAGIELIŲ MOKYKLOS-DARŽELIO DARBUOTOJŲ ASMENS DUOMENŲ SAUGOJIMO POLITIKA**

### **I SKYRIUS DARBUOTOJŲ ASMENS DUOMENŲ SAUGOJIMO POLITIKA**

1. Darbuotojų asmens duomenų saugojimo politika (toliau – Politika) reglamentuoja darbuotojų asmens duomenų rinkimo, naudojimo ir saugojimo principus, nustato darbuotojų asmens duomenų tvarkymo tikslus ir priemones, nustato, kas ir kokiais tikslais, gali susipažinti su darbuotojų asmens duomenimis.

Atsakingas asmuo – fizinis ar juridinis asmuo pagal paslaugų ar kitą sutartį, išskyrus darbo sutartį, įstaigos paskirtas tvarkyti darbuotojų asmens duomenis;

Įstaiga – Panevėžio r. Pažagielių mokykla-darželis;

2. Kitos šioje politikoje vartojamos sąvokos yra suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir kituose asmens duomenų tvarkymą reglamentuojančiuose teisės aktuose.

### **II SKYRIUS DARBUOTOJŲ ASMENS DUOMENŲ TVARKYMO PRINCIPAI**

3. Įstaiga, tvarkydama darbuotojų asmens duomenis, vadovaujasi šiais principais:

3.1. darbuotojų asmens duomenis Įstaiga tvarko tik teisėtiems ir šioje politikoje apibrėžtiems tikslams pasiekti;

3.2. darbuotojų asmens duomenys yra tvarkomi tiksliai, sąžiningai ir teisėtai, laikantis teisės aktų reikalavimų;

3.3. Įstaiga darbuotojų asmens duomenis tvarko taip, kad asmens duomenys būtų tikslūs ir esant jų pasikeitimui nuolat atnaujinami;

3.4. Įstaiga atlieka darbuotojų asmens duomenų tvarkymą tik ta apimtimi, kuri yra reikalinga darbuotojų asmens duomenų tvarkymo tikslams pasiekti;

3.5. darbuotojų asmens duomenys saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi.

### **III SKYRIUS DARBUOTOJŲ ASMENS DUOMENŲ TVARKYMO TIKSLAI**

4. Darbuotojų asmens duomenys yra tvarkomi šiais tikslais:

4.1. darbo sutarčių sudarymo, vykdymo ir apskaitos;

4.2. Įstaigos kaip darbdavio pareigų, nustatytų teisės aktuose, tinkamam vykdymui;

4.3. tinkamai komunikacijai su darbuotojais ne darbo metu palaikyti;

4.4. tinkamoms darbo sąlygoms užtikrinti.

5. Darbo sutarčių sudarymo, vykdymo ir apskaitos tikslais yra tvarkomi darbuotojų vardai ir pavardės, gyvenamosios vietos adresai, gimimo datos, banko sąskaitų numeriai (darbuotojui sutikus), į kurias yra vedamas darbo užmokestis, socialinio draudimo numeris.

6. Įstaigos kaip darbdavio pareigų, nustatytų teisės aktuose, tinkamo vykdymo tikslu yra tvarkomi darbuotojų asmens kodai, informacija apie darbuotojų šeimines padėtis.

7. Tinkamos komunikacijos su darbuotojais ne darbo metu tikslu su darbuotojų sutikimu yra tvarkomi darbuotojų gyvenamosios vietos adresai, asmeniniai telefono numeriai, asmeniniai elektroninio pašto adresai.

8. Tinkamų darbo sąlygų užtikrinimo tikslu darbdavys su darbuotojo sutikimu tvarko informaciją, susijusią su darbuotojo sveikatos būkle, kuri tiesiogiai daro įtaką darbuotojo darbo funkcijoms ir galimybei jas vykdyti teisės aktų nustatyta tvarka.

9. Darbuotojų asmens duomenys yra saugomi tik ta apimtimi ir tiek laiko, kiek yra reikalinga nustatytiems tikslams pasiekti.

#### **IV SKYRIUS DARBUOTOJŲ ASMENS DUOMENŲ RINKIMAS IR TVARKYMAS**

10. Naujai priimto darbuotojo vardas, pavardė, asmens kodas, gimimo data yra surenkami iš darbuotojo pateikto asmens dokumento (asmens tapatybės kortelės ar paso).

11. Naujai priimto darbuotojo gyvenamosios vietos adresas, atsiskaitomosios sąskaitos numeris, socialinio draudimo numeris, asmeninis kontaktinis telefono numeris ir elektroninio pašto adresas darbuotojui sutikus yra surenkami iš darbuotojo.

12. Darbuotojų asmens duomenis turi teisę tvarkyti tik tie asmenys, kuriems jie yra būtini funkcijų vykdymui, ir tik tuomet, kai tai yra būtina atitinkamiems tikslams pasiekti.

13. Šioje Tvarkoje yra nustatyti darbuotojai ir atsakingi asmenys, kurie turi teisę tvarkyti darbuotojų asmens duomenis, taip pat, kokius darbuotojų asmens duomenis atitinkamas asmuo turi teisę tvarkyti.

14. Darbuotojai ar kiti atsakingi asmenys, kuriems yra suteikta teisė tvarkyti darbuotojų asmens duomenis, laikosi konfidencialumo principo ir laiko paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino vykdydami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas. Pareiga saugoti asmens duomenų paslaptį galioja taip pat ir perėjus dirbti į kitas pareigas, pasibaigus darbo ar sutartiniams santykiams.

15. Darbuotojų asmens duomenys, kurie yra atitinkamų dokumentų (sutartys, įsakymai, prašymai ir kt.) tekstuose, yra saugomi Lietuvos Respublikos teisės aktuose nustatytais terminais. Kiti darbuotojų ir buvusių darbuotojų asmens duomenys yra saugomi ne ilgiau nei tai yra reikalinga šioje tvarkoje numatytiems tikslams pasiekti. Atskirų darbuotojų asmens duomenų saugojimo terminus nustato Įstaigos vadovas.

#### **V SKYRIUS ASMENS DUOMENŲ SUBJEKTO TEISĖS**

16. Įstaiga paskiria atsakingą asmenį, kuris užtikrina, kad darbuotojų, kaip duomenų subjektų, teisės būtų užtikrintos, tinkamai įgyvendinamos ir visa informacija būtų pateikiama tinkamai, laiku ir darbuotojams priimtina forma.

17. Darbuotojų, kaip duomenų subjektų, teisės ir jų įgyvendinimo priemonės:

17.1. žinoti apie savo asmens duomenų rinkimą. Darbdavys, rinkdamas darbuotojo asmens duomenis, privalo informuoti darbuotoją, kokius asmens duomenis darbuotojas turi pateikti, koku tikslu atitinkami duomenys yra renkami, kam ir koku tikslu jie gali būti teikiami ir kokios asmens duomenų nepateikimo pasekmės. Darbuotojas turi teisę susipažinti su savo asmens duomenimis, reikalauti ištaisyti, patikslinti ar papildyti neteisingus ar neišsamius jo asmens duomenis. Darbuotojas taip pat gali nesutikti, kad būtų tvarkomi tam tikri neprivalomi jo asmens duomenys;

17.2. susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi. Darbuotojas turi teisę kreiptis į Įstaigos vadovą su prašymu (1 priedas) pateikti informaciją apie tai, kokie ir kokių tikslu jo asmens duomenys yra tvarkomi. Vieną kartą per metus darbuotojui ši informacija pateikiama nemokamai. Jeigu darbuotojas kreipiasi daugiau nei vieną kartą per metus dėl tokios informacijos pateikimo, mokestis už šios informacijos pateikimą negali viršyti tokios informacijos pateikimo sąnaudų;

17.3. reikalauti ištaisyti, sunaikinti savo asmens duomenis arba sustabdyti savo asmens duomenų tvarkymą;

17.4. nesutikti, kad būtų tvarkomi darbuotojo asmens duomenys. Darbuotojas turi teisę nesutikti, kad būtų tvarkomi tam tikri neprivalomi jo asmens duomenys. Toks nesutikimas gali būti išreikštas neužpildant tam tikrų darbuotojo anketos ar kitų pildomų dokumentų skilčių, taip pat vėliau pateikiant prašymą dėl neprivalomai tvarkomų asmens duomenų tvarkymo nutraukimo. Įstaiga suteikia darbuotojui informaciją raštu, kokie jo asmens duomenys yra tvarkomi neprivalomai. Įstaiga, gavusi prašymą nutraukti neprivalomai tvarkomų asmens duomenų tvarkymą, nedelsiant nutraukia tokį tvarkymą, nebent tai prieštarauja teisės aktų reikalavimams, ir apie tai informuoja darbuotoją.

## **VI SKYRIUS**

### **ASMENS DUOMENŲ SAUGUMO UŽTIKRINIMO PRIEMONĖS**

18. Prieigos teisės prie asmens duomenų ir įgaliojimai tvarkyti asmens duomenis suteikiami, naikinami ir keičiami Įstaigos vadovo įsakymu.

19. Įstaiga, saugodama asmens duomenis, įgyvendina ir užtikrina tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

20. Įstaiga užtikrina tinkamą dokumentų bei duomenų rinkmenų saugojimą, imasi priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui. Dokumentų kopijos, kuriose nurodomi darbuotojų asmens duomenys, turi būti sunaikintos taip, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio.

21. Įstaigoje su darbuotojų asmens duomenimis turi teisę susipažinti tik tie asmenys, kurie buvo įgalioti susipažinti su tokiais duomenimis, ir tik tuomet, kai tai yra būtina šioje politikoje numatytiems tikslams pasiekti.

22. Įstaiga užtikrina patalpų, kuriose laikomi asmens duomenys, saugumą, tinkamą techninės įrangos išdėstymą ir peržiūrą, priešgaisrinės saugos taisyklių laikymąsi, tinkamą tinklo valdymą, informacinių sistemų priežiūrą bei kitų techninių priemonių, būtinų asmens duomenų apsaugai užtikrinti, įgyvendinimą.

23. Įstaiga imasi priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, saugodama jai patikėtus dokumentus bei duomenų rinkmenas tinkamai ir saugiai.

24. Jei darbuotojas ar kitas atsakingas asmuo abejoja įdiegtų saugumo priemonių patikimumu, jis turi kreiptis į tiesioginį savo vadovą, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir įdiegimas.

25. Darbuotojai ar kiti atsakingi asmenys, kurie automatinio būdu tvarko asmens duomenis arba iš kurių kompiuterių galima patekti į vietinio tinklo sritis, kuriose yra saugomi asmens duomenys, naudoja pagal atitinkamas taisykles sukurtus slaptažodžius. Slaptažodžiai yra keičiami periodiškai, ne rečiau kaip kartą per tris mėnesius, taip pat susidarius tam tikroms aplinkybėms (pvz.: pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims, ir pan.).

26. Darbuotojas, dirbantis konkrečiu kompiuteriu, gali žinoti tik savo slaptažodį. Darbuotojas slaptažodį užklijuotame voke perduoda Įstaigos įgaliotam atsakingam asmeniui. Slaptažodžiai saugomi seife ar kitoje saugioje vietoje ir naudojami tik būtinu atveju.

27. Nustačius asmens duomenų saugumo pažeidimus, Įstaiga imasi neatidėliotųjų priemonių užkertant kelią neteisėtam asmens duomenų tvarkymui pagal patvirtintą reagavimo į asmens duomenų saugumo pažeidimus procedūrą (priedas2).

28. Šios politikos nesilaikymas atsižvelgiant į pažeidimo sunkumą gali būti laikomas darbo drausmės pažeidimu, už kurį darbuotojams gali būti taikoma atsakomybė, numatyta Lietuvos Respublikos darbo kodekse.

## **VII SKYRIUS BAIGIAMOSIOS NUOSTATOS**

29. Ši politika peržiūrima ir atnaujinama ne dažniau kaip kartą per metus arba pasikeitus teisės aktams, kurie reglamentuoja asmens duomenų tvarkymą.

30. Darbuotojai ir kiti atsakingi asmenys su šia politika yra supažindinami pasirašytinai arba elektroninėmis priemonėmis ir privalo laikytis joje nustatytų įpareigojimų bei atlikdami savo darbo funkcijas vadovautis šioje politikoje nustatytais principais.

31. Įstaiga turi teisę iš dalies arba visiškai pakeisti šią politiką. Su pakeitimais darbuotojai ir kiti atsakingi asmenys yra supažindinami pasirašytinai arba elektroninėmis priemonėmis.

---

Asmens duomenų tvarkymo ir duomenų subjektų teisių įgyvendinimo Pažagienių mokyklos-darželio tvarkos aprašo 1 priedas

**(Prašymo susipažinti su tvarkomais asmens duomenimis forma)**

\_\_\_\_\_  
(duomenų subjekto (fizinio asmens) vardas, pavardė, asmens kodas)

\_\_\_\_\_  
(kontakcinė informacija: gyvenamoji vieta, telefono ryšio numeris, elektroninio pašto adresas)

Panevėžio r. Pažagienių mokyklos-darželio  
Direktoriui

**PRAŠYMAS  
SUSIPAŽINTI SU TVARKOM AIS ASMENS DUOMENIMIS**

\_\_\_\_\_  
(data)

\_\_\_\_\_  
(prašymo sudarymo vieta)

Vadovaudamasis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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) 15 straipsniu:

1. P r a š a u informuoti, ar tvarkote mano asmens duomenis Pažagienių mokykloje-darželyje:

\_\_\_\_\_  
(nurodykite Jus dominančių registrų ir (ar) informacinių sistemų pavadinimus)

2. Jei mano asmens duomenys tvarkomi, prašau pateikti informaciją apie tvarkomus asmens duomenis pagal: vardas – \_\_\_\_\_, pavardė – \_\_\_\_\_, asmens kodas – \_\_\_\_\_ arba gimimo data – \_\_\_\_\_.

3. Prašau pateikti informaciją apie duomenų gavėjus, kuriems buvo atskleisti mano tvarkomi asmens duomenys per laikotarpį nuo \_\_\_\_\_ iki \_\_\_\_\_.

4. Parengtą dokumentą (*pažymėkite tinkamą langelį*):

atsiimsiu asmeniškai Pažagienių mokykloje-darželyje (Švyturio g. 31, Pažagienių k., Panevėžio r.);

prašau išsiųsti \_\_\_\_\_ pašto adresu:

prašau išsiųsti elektroniniu paštu: \_\_\_\_\_.

PRIDEDAMA. Asmens tapatybės dokumento, patvirtinto teisės aktų nustatyta tvarka, kopija (*pildoma, kai prašymas siunčiamas paštu*) \_\_\_\_\_.

(dokumento pavadinimas)

\_\_\_\_\_  
(Duomenų subjekto vardas, pavardė, parašas)

—  
Teikiant prašymą asmeniškai, Pažagienių mokyklos-darželio darbuotojas, priimantis duomenų subjekto prašymą, nurodo asmens tapatybei patvirtinti duomenų subjekto pateiktą asmens tapatybę patvirtinantį dokumentą:

Pasas  Asmens tapatybės kortelė

\_\_\_\_\_  
(Darbuotojo vardas ir pavardė, parašas)

Pažagienių mokyklos-darželio  
asmens duomenų saugojimo apsaugos politikos  
2 priedas

## REAGAVIMO Į ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪRA

### I SKYRIUS

#### SĄVOKOS

1. **Duomenų saugumo pažeidimas** reiškia pažeidimą, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami tvarkomi Asmens duomenys arba prie jų be leidimo gaunama prieiga.
2. **Administracija** – Panevėžio r. Pažagienių mokyklos-darželio administracija, juridinio asmens kodas: 191429544, buveinės adresas: Švyturio g. 31, Pažagienių k., Panevėžio r.
3. **Už duomenų saugą atsakingas asmuo** – Pažagienių mokyklos-darželio direktoriaus paskirtas Darbuotojas, turintis kompetenciją imtis reagavimo į Duomenų saugumo pažeidimą procedūros vykdymo.
4. **Priežiūros institucija** reiškia valstybės narės pagal BDAR 51 straipsnį įsteigtą nepriklausomą valdžios instituciją. Lietuvos Respublikos atveju tokia institucija yra Valstybinė duomenų apsaugos inspekcija.
5. **Procedūra** reiškia šią Reagavimo į asmens duomenų saugumo pažeidimus procedūrą.

### II SKYRIUS

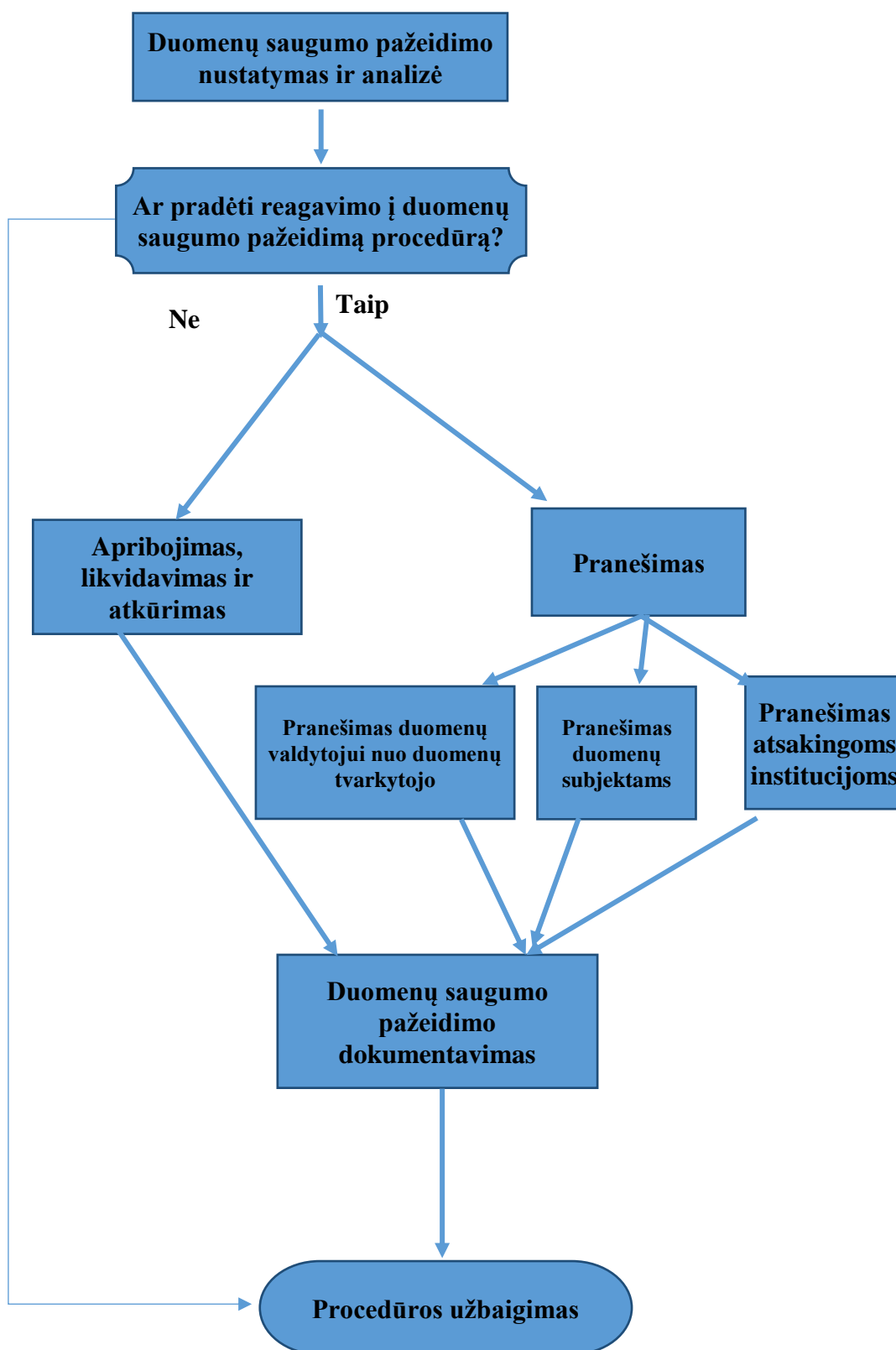
#### APIMTIS

6. Ši procedūra taikoma įvykus asmens duomenų saugumo pažeidimui pagal BDAR 33 straipsnį ir 34 straipsnį.
7. Šiame dokumente išdėstyta procedūra turėtų būti vadovaujama reaguojant į duomenų saugumo pažeidimą, atsižvelgiant į konkrečios situacijos faktines aplinkybes.

### III SKYRIUS

#### ATSAKOMYBĖ

8. Visi asmenys, turintys prieigą prie Administracijos tvarkomų asmens duomenų privalo žinoti ir vadovautis šia Procedūra duomenų saugumo pažeidimo atveju.



1 pav. Reagavimo į duomenų saugumo pažeidimus schema



#### **IV SKYRIUS**

### **PROCEDŪRA – DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMAS IR ANALIZĖ**

9. Kaip ir galima spręsti iš Procedūros 1 punkte nurodyto apibrėžimo, saugumo pažeidimu laikomas toks saugumo incidentas, dėl kurio įvyksta (konkretus pažeidimas gali patekti į daugiau nei vieną kategoriją):

9.1. Konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama prieiga tam teisės neturintiems asmenims. Tokio pobūdžio pažeidimo pavyzdžiais galėtų būti duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio paviešinimas ir pan.;

9.2. Pasiiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami. Tokio pobūdžio pažeidimu galėtų būti duomenų bazės ištrynimasis nesant atsarginės kopijos, iš kurios būtų galima atkurti prarastus duomenis. Pasiiekiamumo pažeidimu, kuris turėtų būti aprašytas, būtų ir laikinas įprastinę Administracijos veiklą sutrikdęs prieigos prie duomenų praradimas;

9.3. Vientisumo pažeidimas – netyčia ar neteisėtai atliekami asmens duomenų pakeitimai. Tai galėtų būti trečiojo asmens, įgijusio neteisėtą prisijungimą prie duomenų bazės, įvykdyti joje esančių įrašų pakeitimai.

10. Kai yra nustatomas duomenų saugumo pažeidimas, jį nustatęs Darbuotojas turi kuo skubiau informuoti už duomenų saugą atsakingą asmenį asmeniškai, el. paštu, telefonu, ir / arba kitomis komunikacijos priemonėmis.

11. Už duomenų saugą atsakingas asmuo atlieka pradinį vertinimą tam, kad nuspręstų dėl tinkamo veiksmų plano. Šis vertinimas turėtų apimti šiuos pagrindinius veiksniai:

11.1. Poveikio informacinių technologijų (toliau – IT) infrastruktūrai apimtis;

11.2. Informaciniai išteklių, kuriems gali kilti arba yra kilęs pavojus (kokios duomenų bazės yra arba gali būti paveiktos);

11.3. Tikėtina duomenų saugumo pažeidimo trukmė (kada prasidėjo ir kada buvo sustabdytas pažeidimas arba kaip skubiai tikėtina galima būtų tai padaryti);

11.4. Paveikti duomenų subjektai ir poveikio jiems apimtis (ar paveikti tik konkrečios duomenų subjektų grupės duomenys, kokia konkrečios grupės dalis yra paveikta ir pan.);

11.5. Pradiniai duomenų saugumo pažeidimo pasekmių požymiai (tai galėtų būti prieigos prie duomenų praradimas, nustatyti neteisėti duomenų pakeitimai, rasti paviešinti duomenys ir pan.).

12. Aukščiau nurodyta informacija turėtų būti fiksuojama tokiu būdu, kad atliekant vėlesnę peržiūrą būtų galima susidaryti aiškų chronologišką suvokimą apie situacijos eigą ir priemones, kurių buvo imtasi.

13. Atsižvelgdamas į aukščiau aprašytą pradinę analizę, Už duomenų saugą atsakingas asmuo pagal Procedūros 11 punkte nurodytus kriterijus įvertina, ar duomenų saugumo pažeidimo apimtis ir faktinis ar galimas poveikis lemia Reagavimo į duomenų saugumo pažeidimus procedūros pradėjimą.

#### **V SKYRIUS**

### **PROCEDŪRA – REAGAVIMO Į DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS PRADĖJIMAS**

14. Formalus reagavimas į Duomenų saugumo pažeidimą visais atvejais turėtų būti pradėtas tada, jei nustatytos bet kurios iš toliau nurodytų aplinkybių:

14.1. prarastas arba gali būti prarastas reikšmingas kiekis asmens duomenų;

14.2. duomenų pažeidimas tikėtina gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms;

14.3. daromas poveikis dideliam duomenų subjektų skaičiui;

14.4. bet kokia kita situacija, kuri gali sukelti reikšmingą poveikį Administracijai ir / arba duomenų subjektams.

15. Jei nusprendžiama nepradėti Procedūros, tada Procedūros 11 punkte aprašytas vertinimas turi būti tinkamai dokumentuotas už duomenų saugą atsakingo asmens ir ši Procedūra užbaigta.

## **VI SKYRIUS PROCEDŪRA – DUOMENŲ SAUGUMO PAŽEIDIMO APRIBOJIMAS, LIKVIDAVIMAS IR ATKŪRIMAS**

16. Pirmasis žingsnis sprendžiant duomenų saugumo pažeidimo klausimą yra jo apribojimas. Konkretūs veiksmai, atliktini norint tai pasiekti priklauso nuo konkretaus pažeidimo aplinkybių, bet tai galėtų būti tokie veiksmai kaip:

16.1. duomenų ištrynimasis nuotoliniu būdu iš pamesto ar pavogto įrenginio;

16.2. kuo skubesis kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti duomenys, su prašymu neatidarinėti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;

16.3. atskleisto tretiesiems asmenims prisijungimo prie duomenų bazės slaptažodžio pakeitimas;

16.4. prarastų duomenų atkūrimas iš turimos atsarginės kopijos.

17. Vykdamas šią procedūrą reikia imtis atsargumo priemonių tam, kad būtų užtikrinta, jog būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį duomenų saugumo pažeidimą (pavyzdžiui, užfiksuojama, kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės, kam konkrečiai buvo per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su duomenimis).

18. Veiksmai, skirti atitaisyti žalą, sukeltą duomenų saugumo pažeidimo, turėtų būti nukreipti ne vien į esamo pažeidimo priežasties pašalinimą, bet ir skirti neleisti duomenų saugumo pažeidimui pasikartoti. Turėtų būti nustatytas bet koks pažeidžiamumas, kuris gali būti išnaudotas siekiant įvykdyti pažeidimą.

19. Prireikus gali būti pasitelkiama IT specialistų ar teisininkų pagalba.

20. Atkūrimo stadijoje sistemos turėtų būti pagal galimybes atstatytos į ankstesnę būklę, tačiau turėtų būti imamasi būtinų veiksmų tam, kad būtų atsižvelgta į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdamas duomenų saugumo pažeidimą.

## **VII SKYRIUS PROCEDŪRA – DUOMENŲ VALDYTOJO PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ**

21. Administracija, kaip duomenų valdytojas, nedelsdama privalo informuoti Priežiūros instituciją apie duomenų saugumo pažeidimą tada, jei už duomenų saugą atsakingas asmuo nustato, kad duomenų saugumo pažeidimas tikėtina gali kelti pavojų duomenų subjektų, paveiktų duomenų saugumo pažeidimo, teisėms ir laisvėms. Pavojų keliančiu laikytinas toks pažeidimas, dėl kurio duomenų subjektas galėtų patirti kūno sužalojimą, materialinę ar nematerialinę žalą, teisių apribojimą, diskriminaciją, galėtų būti pavogta ar suklastota asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesinė paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala.

22. Jei duomenų saugumo pažeidimas kelia pavojų duomenų subjektų teisėms ir laisvėms, už duomenų saugą atsakingas asmuo ne vėliau kaip per 72 valandas nuo Administracijos sužinojimo apie pažeidimą Priežiūros institucijai pateikia tokią informaciją:

22.1. duomenų saugumo pažeidimo pobūdį, įskaitant, jeigu įmanoma, atitinkamai paveiktų duomenų subjektų kategorijas ir apytikslių skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslių skaičių;

22.2. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis;

22.3. tikėtinų duomenų saugumo pažeidimo pasekmių aprašymą;

22.4. priemonės, kurių ėmėsi arba planuoja imtis Administracija tam, kad būtų pašalintas duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti.

23. Jeigu visos informacijos neįmanoma pateikti tuo pačiu metu, tolesnė informacija nepagrįstai nedelsiant gali būti teikiama etapais.

## **VIII SKYRIUS**

### **PROCEDŪRA – DUOMENŲ VALDYTOJO PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ**

24. Kai dėl duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, Administracija nepagrįstai nedelsdama praneša apie asmens duomenų saugumo pažeidimą duomenų subjektams. Didelį pavojų keliančiu gali būti laikytinas bet kuris 21 punkte nurodytų pasekmių riziką keliantis pažeidimas tada, jei tokios pažeidimo pasekmės yra labai tikėtinos, tvarkomi jautrūs asmens duomenys (pavyzdžiui, duomenys apie sveikatą), pažeidimas turi neigiamą poveikį dideliame duomenų subjektų skaičiui ir pan.

25. Už duomenų saugą atsakingas asmuo duomenų subjektui aiškia ir paprasta kalba aprašo duomenų saugumo pažeidimo pobūdį ir pateikia bent jau žemiau nurodytą informaciją:

25.1. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis;

25.2. tikėtinų duomenų saugumo pažeidimo pasekmių aprašymą;

25.3. priemonės, kurių ėmėsi arba planuoja imtis Administracija tam, kad būtų pašalintas duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti.

26. Šios Procedūros 25 punkte nurodytas komunikavimas su duomenų subjektu nebus reikalingas tada, jei egzistuoja bet kuri iš šių aplinkybių:

26.1. Administracija įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems duomenų saugumo pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su Asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės;

26.2. Administracija vėliau ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

26.3. tai pareikalautų neproporcingai daug pastangų. Tokiu atveju apie įvykusį duomenų saugumo pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

27. Priežiūros institucija, apsvarsčiusi, kokia yra tikimybė, kad dėl duomenų saugumo pažeidimo kils didelis pavojus, gali pareikalauti, kad Administracija informuotų duomenų subjektus apie duomenų saugumo pažeidimą. Už duomenų saugą atsakingas asmuo gavęs tokią nurodymą turi nedelsdamas jį vykdyti.

**IX SKYRIUS**  
**DUOMENŲ SAUGUMO PAŽEIDIMO DOKUMENTAVIMAS IR PROCEDŪROS**  
**UŽBAIGIMAS**

28. Už duomenų saugą atsakingas asmuo, gavęs supažindinto su duomenų saugumo pažeidimo ir jo pašalinimo aplinkybėmis Pažagienių mokyklos-darželio direktoriaus pritarimą, priima sprendimą užbaigti Procedūrą tada, kai duomenų saugumo pažeidimas laikytinas pašalintu, o visoms reikalingoms šalims apie pažeidimą yra pranešta.

29. Visi veiksmai, kurių imamasi Procedūros metu turi būti aprašomi ir visi susiję įrašai apie duomenų saugumo pažeidimą peržiūrimi tam, kad būtų užtikrintas jų išbaigtumas, tikslumas ir atitiktis atitinkamam teisiniam reguliavimui.

---