

**ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO FIKSAVIMO, DOKUMENTAVIMO,
PRANEŠIMO APIE PAŽEIDIMĄ PATEIKIMO IR PAŽEIDIMO PAŠALINIMO PRIENŲ
„ŽIBURIO“ GIMNAZIJOJE TVARKOS APRAŠAS**

**I SKYRIUS
BENDROSIOS NUOSTATOS**

1. Asmens duomenų saugumo pažeidimo fiksavimo, dokumentavimo, pranešimo apie pažeidimą pateikimo ir pažeidimo pašalinimo Prienų „Žiburio“ gimnazijoje (toliau - Mokykla) tvarkos aprašas (toliau – Aprašas) nustato asmens duomenų saugumo pažeidimo fiksavimo, dokumentavimo bei pranešimo apie asmens duomenų saugumo pažeidimo turinį, procedūrą, pateikimo duomenų subjektui ir Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) tvarką.

2. Aprašas taikomas Gimnazijoje tvarkant duomenų subjektų asmens duomenis ir juridiniams asmenims, veikiančiams kaip Gimnazijoje valdomų duomenų tvarkytojams.

3. 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, kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas), Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82 (1.12E) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“.

4. Apraše vartojamos sąvokos:

4.1. **Asmens duomenys** – bet kokia informacija arba jos visuma apie fizinį asmenį, pagal kurią galima nustatyti fizinio asmens tapatybę. Tokia informacija gali būti vardas ir pavardė, asmens kodas, buvimo vietos duomenys, elektroninis paštas, fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės duomenys.

4.2. **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami gauti, saugomi arba kitaip tvarkomi duomenys arba prie jų be leidimo gaunama prieiga.

4.3. **Darbuotojas** – Gimnazijos darbuotojas, dirbantis pagal darbo sutartį.

4.4. **Duomenų apsaugos pareigūnas** – Gimnazijoje tvarkomų duomenų apsaugos specialistas.

4.5. **Duomenų subjektas** – fizinis asmuo, kurio duomenis tvarko Gimnazija.

5. Kitos apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (toliau – ADTI) ir kituose teisės aktuose, reglamentuojančiuose asmens duomenų apsaugą.

**II SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO FIKSAVIMO, DOKUMENTAVIMO,
PRANEŠIMO APIE PAŽEIDIMĄ PATEIKIMO IR PAŽEIDIMO PAŠALINIMO
PROCEDŪRA**

6. Gimnazijos darbuotojas, sužinojęs, kad nebuvo užtikrintas asmens duomenų saugumas:

6.1. nedelsdamas, bet ne vėliau kaip per 4 darbo valandas nuo asmens duomenų saugumo

pažeidimo paaiškėjimo momento, elektroniniu paštu, telefonu arba žodžiu informuoja savo tiesioginį vadovą ir duomenų apsaugos pareigūną;

6.2. imasi priemonių asmens duomenų saugumo pažeidimui pašalinti ir priemonių galimoms neigiamoms jo pasekmėms sumažinti;

6.3. užpildo Aprašo 1 priede nurodytos formos Pranešimą apie asmens duomenų saugumo pažeidimą ir nedelsdamas perduoda jį duomenų apsaugos pareigūnui.

7. Duomenų tvarkytojai, sužinoję apie asmens duomenų saugumo pažeidimą, ne vėliau kaip per 1 darbo dieną apie tai praneša Gimnazijos duomenų apsaugos pareigūnui, pateikdami pranešimą.

8. Duomenų apsaugos pareigūnas, gavęs Gimnazijos darbuotojo užpildytą pranešimą ar duomenų tvarkytojo pranešimą:

8.1. nedelsdamas pradeda nagrinėti pranešime nurodytas aplinkybes;

8.2. prireikus pasitelkia kitus Gimnazijos darbuotojus;

8.3. įvertina, ar buvo padarytas asmens duomenų saugumo pažeidimas;

8.4. jei asmens duomenų saugumo pažeidimas padarytas, nustato asmens duomenų kategorijas, įskaitant specialių kategorijų asmens duomenis, kurios buvo susijusios su pažeidimu, pažeidimo priežastis, lėmusias asmens duomenų saugumo pažeidimą, apimtis (duomenų subjektų kategorijos ir skaičius), asmeniui padarytą žalą;

8.5. nustato, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas (pvz., naudoti atsargines kopijas, siekiant atkurti prarastus ar sugadintus duomenis);

8.6. nustato, ar būtina nedelsiant pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą;

8.7. nustato, ar būtina pranešti Inspekcijai apie asmens duomenų saugumo pažeidimą.

9. Duomenų tvarkytojai pateikia visą duomenų apsaugos pareigūno prašomą informaciją, susijusią su informavimu apie asmens duomenų saugumo pažeidimą ir jo tyrimu, per duomenų apsaugos pareigūno nurodytą terminą.

10. Duomenų apsaugos pareigūnas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, surašo aprašo 2 priede nurodytos formos Asmens duomenų saugumo pažeidimo ataskaitą.

11. Asmens duomenų saugumo pažeidimo ataskaita yra pateikiama Gimnazijos direktoriui.

12. Atsižvelgiant į asmens duomenų saugumo pažeidimo ataskaitą, prireikus Sporto centro direktorius tvirtina priemonių planą – jame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl asmens duomenų saugumo pažeidimo, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus.

13. Tuo atveju, jei yra nustatoma, kad dėl įvykusio asmens duomenų saugumo pažeidimo duomenų tvarkytojas turi imtis papildomų veiksmų ar užtikrinti papildomas asmens duomenų saugumo priemones, Gimnazijos direktorius duoda privalomus nurodymus duomenų tvarkytojui, jei asmens duomenų saugumo pažeidimas susijęs su duomenų tvarkytojo tvarkomomis informacinėmis sistemomis.

14. Duomenų apsaugos pareigūnas, nustatęs, kad asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, nedelsdamas ir, jei įmanoma, nepraėjus 72 valandoms nuo to laiko, kai buvo sužinota apie asmens duomenų saugumo pažeidimą, informuoja Inspekciją, pateikdamas užpildytą Aprašo 1 priede nurodytos formos Pranešimą apie asmens duomenų saugumo pažeidimą.

15. Tuo atveju, kai duomenų apsaugos pareigūnas nustato, kad asmens duomenų saugumo pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms, apie padarytą asmens duomenų saugumo pažeidimą Inspekcija nėra informuojama.

16. Duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, nepraėjus 72 valandoms nuo to laiko, kai buvo sužinota apie asmens duomenų saugumo pažeidimą, praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui elektroniniu paštu, raštu ar kitu būdu, kai dėl asmens duomenų

saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms.

17. Tuo atveju, kai yra įtariama, kad asmens duomenų saugumo pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą.

18. Darbuotojai privalo Gimnazijos duomenų apsaugos pareigūnui pateikti visą informaciją, susijusią su asmens duomenų saugos pažeidimais ir kitais jų kompetencijai priskirtais būdais padėti sustabdyti asmens duomenų saugos pažeidimą ir (arba) sumažinti jo sukeltus padarinius.

19. Duomenų apsaugos pareigūnas informaciją apie asmens duomenų saugumo pažeidimą įrašo į Aprašo 3 priede nurodytos formos Asmens duomenų saugumo pažeidimų registravimo žurnalą.

20. Asmens duomenų saugumo pažeidimų registravimo žurnalą ir Asmens duomenų saugumo pažeidimo ataskaitas saugo Gimnazijos asmens duomenų apsaugos pareigūnas.

21. Duomenų apsaugos pareigūnas dokumentuoja visus asmens duomenų saugumo pažeidimus, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kurių buvo imtasi.

III SKYRIUS

PRANEŠIMAS INSPEKCIJAI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

22. Asmens duomenų saugumo pažeidimo atveju duomenų apsaugos pareigūnas nepagrįstai nedelsdamas, bet ne vėliau kaip per 72 valandas nuo tada, kai sužinojo apie asmens duomenų saugumo pažeidimą, apie tai praneša Inspekcijai, kuri yra kompetentinga pagal Reglamento 55 straipsnį, nebent asmens duomenų saugumo pažeidimas nekeltų pavojaus fizinių asmenų teisėms ir laisvėms. Jeigu Inspekcijai apie asmens duomenų saugumo pažeidimą nepranešama per 72 valandas, prie pranešimo pridedamos vėlavimo priežastys.

23. Duomenų tvarkytojas, sužinojęs apie asmens duomenų saugumo pažeidimą, nedelsdamas apie tai praneša duomenų valdytojui.

24. Aprašo 22 punkte nurodytame pranešime Inspekcijai turi būti nurodyta:

24.1. Duomenų valdytojo duomenys:

24.1.1. juridinio asmens pavadinimas, kodas, buveinės adresas, telefono ryšio numeris ir (ar) elektroninio pašto adresas, ir (ar) elektroninės siuntos pristatymo dėžutės adresas;

24.1.2. fizinio asmens vardas, pavardė, asmens kodas, gimimo data (jeigu asmuo neturi asmens kodo), asmens duomenų tvarkymo vieta, telefono ryšio numeris ir (ar) elektroninio pašto adresas, ir (ar) elektroninės siuntos pristatymo dėžutės adresas;

24.1.3. duomenų valdytojo atstovo, jeigu jis yra įgaliotas pagal Reglamento 27 straipsnį, pavadinimas, kodas, buveinės adresas, telefono ryšio numeris ir (ar) elektroninio pašto adresas, ir (ar) elektroninės siuntos pristatymo dėžutės adresas;

24.2. duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, duomenys:

24.2.1. vardas ir pavardė;

24.2.2. telefono ryšio numeris ir (ar) elektroninio pašto adresas;

24.2.3. pareigos;

24.2.4. darbovietės pavadinimas ir adresas;

24.3. asmens duomenų saugumo pažeidimo apibūdinimas:

24.3.1. asmens duomenų saugumo pažeidimo data, laikas ir vieta;

24.3.2. asmens duomenų saugumo pažeidimo nustatymo data ir laikas;

24.3.3. asmens duomenų saugumo pažeidimo aplinkybės (asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas), asmens duomenų vientisumo praradimas

(neautorizuotas asmens duomenų pakeitimas), asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas);

24.3.4. apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius ir kategorijos;

24.3.5. apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius ir kategorijos;

24.3.6. tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

24.3.7. kita, duomenų valdytojo nuomone, reikšminga informacija;

24.4. aprašytos priemonės, kurių ėmėsi arba siūlo imtis duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas arba kad būtų sumažintos jo sukeltos pasekmės;

24.5. informacija apie tai, ar apie asmens duomenų saugumo pažeidimą informuoti duomenų subjektai, jeigu duomenų subjektai neinformuojami, nurodomos priežastys;

24.6. pranešimo vėlavimo priežastys, jeigu apie asmens duomenų saugumo pažeidimą pranešama vėliau nei per 72 valandas nuo tada, kai duomenų valdytojas sužinojo apie asmens duomenų saugumo pažeidimą.

25. Duomenų apsaugos pareigūnas, pranešdamas apie asmens duomenų saugumo pažeidimą, Aprašo 24.1–24.5 papunkčiuose nurodytą informaciją pateikia visą iš karto arba keliais etapais, jeigu nurodytos informacijos neįmanoma pateikti tuo pačiu metu. Duomenų apsaugos pareigūnas informaciją keliais etapais teikia nepagrįstai nedelsdamas.

26. Pranešimą apie asmens duomenų saugumo pažeidimą pasirašo Gimnazijos direktorius.

27. Pranešimas apie asmens duomenų saugumo pažeidimą Inspekcijai teikiamas vienu iš šių būdų:

27.1. per Inspekcijos interneto svetainę www.ada.lt naudojantis elektronine paslaugų sistema;

27.2. elektroninio pašto adresu ada@ada.lt;

27.3. paštu Inspekcijos buveinės adresu;

27.4. Inspekcijos faksu;

27.5. pateikiant pranešimą apie asmens duomenų saugumo pažeidimą Inspekcijoje.

28. Inspekcija, nustačiusi, kad pranešime pateikta ne visa aprašo 24 punkte nurodyta informacija arba pateikta netiksli ar neišsami informacija, nedelsiant, bet ne vėliau kaip per 5 darbo dienas nuo pranešimo gavimo dienos, informuoja apie tai duomenų valdytoją ir paprašo ne vėliau kaip kitą darbo dieną nuo prašymo pateikimo dienos pranešimą papildyti, patikslinti ir (ar) ištaisyti. Ši nuostata netaikoma, kai duomenų valdytojas informaciją apie asmens duomenų saugumo pažeidimą teikia etapais.

IV SKYRIUS

PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

29. Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, duomenų valdytojas nepagrįstai nedelsdamas praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui.

30. Pranešime duomenų subjektui aiškia ir paprasta kalba aprašomas asmens duomenų saugumo pažeidimo pobūdis ir pateikiama ši informacija:

30.1. nurodytas duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas ir pavardė (pavadinimas) ir kontaktiniai duomenys;

30.2. aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

30.3. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti.

31. Pranešimo duomenų subjektui nereikalaujama, jeigu įvykdomos bet kurios toliau nurodytos sąlygos:

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

31.2. Gimnazija ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;

31.3. pranešimas pareikalautų neproporcingai didelių pastangų. Tokiu atveju apie pažeidimą viešai paskelbiama Gimnazijos interneto svetainėje arba taikoma panaši (viešo paskelbimo) priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

32. Jei Inspekcija, apsvarsčiusi tikimybę, kad dėl pažeidimo kils didelis pavojus, pareikalauja, kad Gimnazija informuotų duomenų subjektą apie asmens duomenų saugumo pažeidimą, nedelsiant praneša duomenų subjektui apie asmens duomenų saugumo pažeidimą.

33. Duomenų tvarkytojai suteikia Gimnazijai pagalbą, kurios reikia, kad būtų tinkamai pranešta apie asmens duomenų saugumo pažeidimą duomenų subjektui.

V SKYRIUS BAIGIAMOSIOS NUOSTATOS

34. Gimnazijos darbuotojai su Aprašu supažindinami pasirašytinai.

35. Gimnazijos darbuotojai, pažeidę Aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.
