

PATVIRTINTA
Klaipėdos „Aukuro“ gimnazijos
direktoriaus 2025 m. rugsėjo 3 d.
įsakymu Nr.V-126

KLAIPĖDOS „AUKURO“ GIMNAZIJOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REAGAVIMO TVARKA

I SKYRIUS BENDROSIOS NUOSTATOS

1. Klaipėdos „Aukuro“ gimnazija (toliau – **Gimnazija** arba **Duomenų valdytojas**) asmens duomenų saugumo pažeidimų Tvarkos (toliau - **Tvarka**) tikslas – nustatyti asmens duomenų saugumo pažeidimo Įstaigoje, pranešimų kompetentingai priežiūros institucijai (o tam tikrais atvejais ir duomenų subjektams) apie juos ir dokumentavimo tvarką siekiant įgyvendinti atskaitomybės principą.

2. Ši Tvarka visais atvejais taikoma Gimnazijos vykdomoje veikloje ir yra privaloma visiems Gimnazijos darbuotojams.

3. Šioje Tvarkoje vartojamos sąvokos atitinka apibrėžimus, nustatytus Lietuvos Respublikos įstatymuose ir Europos Sąjungos teisės aktuose.

4. Tvarkoje vartojamos sąvokos:

4.1. **Asmens duomenys** - bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (pavyzdžiui, vardas ir pavardė, asmens identifikavimo numeris, buvimo vietos duomenys ir interneto identifikatorius arba vienas ar keli to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymiai).

4.2. **Saugumo pažeidimas** - asmens duomenų saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų bei leidimo gaunama prieiga.

4.3. **Duomenų subjektas** - fizinis asmuo, kurio asmens duomenis Gimnazija tvarko.

4.4. **Duomenų tvarkymas** - bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimasis arba sunaikinimas.

4.5. **Duomenų tvarkytojas** - fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri Duomenų valdytojo vardu tvarko asmens duomenis.

4.6. **Priežiūros institucija** - Valstybinė duomenų apsaugos inspekcija (toliau - VDAI).

4.7. **Reglamentas** - 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendras duomenų apsaugos reglamentas).

II SKYRIUS ASMENS DUOMENŲ TVARKYMO SAUGUMAS

5. Gimnazija, taikydama tinkamas technines ir organizacines priemones, užtikrina, kad asmens duomenys būtų tvarkomi tokiu būdu, kad būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo neteisėto duomenų tvarkymo ir atsitiktinio sunaikinimo, sugadinimo ar praradimo.

6. Gimnazija, atsižvelgdama į techninių galimybių išsivystymo lygį Gimnazijoje, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant, jei reikia:

- 6.1. pseudonimų suteikimą asmens duomenims ir jų šifravimą;
 - 6.2. gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;
 - 6.3. gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju;
 - 6.4. reguliarių techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą;
 - 6.5. Kitas Gimnazijos ir konkrečių informacijos sistemų naudojimo tvarkas, numatančias asmens duomenų privatumo užtikrinimo ir informacinės saugos priemones.
7. Nustatydamą tinkamo lygio saugumą, Gimnazija įvertina pavojus, kurie gali kilti dėl asmens duomenų tvarkymo, visų pirmiausia dėl tvarkomų asmens duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo ar neteisėtos prieigos prie jų.

III SKYRIUS DUOMENŲ SAUGUMO PAŽEIDIMŲ KLASIFIKAVIMAS

8. Asmens duomenų saugumo pažeidimai pagal pažeidimo poveikį duomenims yra skirstomi į:
- 8.1. Konfidencialumo pažeidimas – kai yra be leidimo (nesankcionuotai) ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;
 - 8.2. Prieinamumo pažeidimas – kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba duomenys sunaikinami;
 - 8.3. Vientisumo pažeidimas – kai asmens duomenys pakeičiami be leidimo (nesankcionuotai) ar netyčiais naudotojų veiksmais.
9. Tuo pat metu priklausomai nuo aplinkybių dėl Pažeidimo gali būti paveiktas asmens duomenų konfidencialumas, prieinamumas ir vientisumas, bei gali pasitaikyti bet koks šių pažeidimo tipų derinys.

IV SKYRIUS REAGAVIMAS Į SAUGUMO PAŽEIDIMUS

10. Kiekvienas Gimnazijos darbuotojas, įtaręs, supratęs ar sužinojęs, jog buvo padarytas ar įvykęs saugumo pažeidimas, nedelsdamas apie tokį pažeidimą privalo informuoti Gimnazijos vadovo paskirtą už saugumo pažeidimų tyrimą atsakingą darbuotoją.
11. Už saugumo pažeidimų tyrimą atsakingas darbuotojas:
- 11.1. privalo imtis visų reikiamų techninių ir organizacinių priemonių, kad nedelsiant būtų nustatyta, buvo padarytas/įvyko saugumo pažeidimas ar nebuvo. Tais atvejais, kai šis darbuotojas negali identifikuoti, ar buvo padarytas/įvyko saugumo pažeidimas, šiam klausimui išspręsti turi būti inicijuotas kompetentingos komisijos sudarymas;
 - 11.2. turi įvertinti riziką, kurią gali patirti Gimnazija, duomenų subjektai bei kiti susiję asmenys;
 - 11.3. privalo nedelsiant imtis visų įmanomų techninių ir organizacinių saugumo priemonių, kad būtų suvaldytas saugumo pažeidimas ir sumažinti neigiami padariniai;
 - 11.4. apie saugumo pažeidimą, tame tarpe ir dar neįvykusį o tik galimą, privalo nedelsiant informuoti Gimnazijos vadovą.

12. Gimnazijos vadovas arba jo įgaliotas asmuo privalo informuoti kompetentingą priežiūros instituciją, VDAI (o tam tikrais atvejais ir duomenų subjektus) apie saugumo pažeidimą Tvarkos 13 ir 19 punktuose nustatyta tvarka.

V SKYRIUS

PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

13. Saugumo pažeidimo atveju Gimnazijos vadovas arba jo įgaliotas asmuo nepagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 (septyniasdešimt dviem) valandoms nuo tada, kai už duomenų saugumo pažeidimų tyrimą atsakingas darbuotojas sužinojo apie saugumo pažeidimą, apie tai praneša priežiūros institucijai (VDAI). Informacija apie pranešimo būdus bei pranešimo forma pasiekama adresu: <https://vdai.lrv.lt/lt/adsp-ir-dap/pranesimas-apie-asmens-duomeniu-saugumo-pazeidima>.

14. Tais atvejais, kai Gimnazijos vadovas ir už duomenų saugumo pažeidimų tyrimą atsakingas darbuotojas, įvertinę (galimo) saugumo pažeidimo pobūdį ir keliamą riziką, nusprendžia, kad saugumo pažeidimas nekelia ir ateityje nesukels pavojaus duomenų subjektų teisėms ir laisvėms, apie tokį saugumo pažeidimą priežiūros institucijai nepranešama.

15. Jeigu priežiūros institucijai apie saugumo pažeidimą nepranešama per 72 (septyniasdešimt dvi) valandas nuo tada, kai Gimnazija sužinojo apie saugumo pažeidimą, prie pranešimo turi būti pridedamos vėlavimo priežastys.

16. Tvarkos 13 punkte nurodytame pranešime apie saugumo pažeidimą turi būti bent:

16.1. aprašytas saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;

16.2. nurodyta duomenų subjekto paskirto atsakingo Gimnazijos darbuotojo, galinčio suteikti daugiau informacijos, vardas bei pavardė ir kontaktiniai duomenys;

16.3. aprašytos tikėtinos saugumo pažeidimo pasekmės;

16.4. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis Gimnazija, kad būtų pašalintas saugumo pažeidimas, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti.

17. Jeigu visos 16 punkte nurodytos informacijos Gimnazija negali pateikti priežiūros institucijai pranešimo pateikimo metu, informacija apie saugumo pažeidimą toliau nepagrįstai nedelsiant gali būti teikiama etapais. Informacijos teikimas etapais yra pateisinamas sudėtingesnių pažeidimų atveju (pavyzdžiui, kai kuriems kibernetinio saugumo incidentams), kai gali būti reikalingas nuodugnus tyrimas, siekiant išsamiai nustatyti saugumo pažeidimo pobūdį ir tai, koku mastu asmens duomenys buvo pažeisti.

18. Pateikusi pradinį pranešimą Gimnazija bet kuriuo metu gali informuoti priežiūros instituciją (VDAI) apie tolesniame tyrime atskleistus įrodymus, jog jokio saugumo pažeidimo faktiškai nebuvo. Tokiu atveju ši papildoma informacija yra įtraukiama į pradinę informaciją, kuri jau buvo pateikta priežiūros institucijai, ir incidentas atitinkamai nėra laikomas saugumo pažeidimu.

VI SKYRIUS

PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

19. Tais atvejais, kai dėl saugumo pažeidimo gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, Gimnazijos vadovas ar jo įgaliotas asmuo, nepagrįstai nedelsdamas turi pranešti apie tokį saugumo pažeidimą ir patiems duomenų subjektams, kad šie galėtų imtis visų įmanomų priemonių apsisaugoti nuo neigiamų padarinių.

20. Tvarkos 19 punkte nurodytame pranešime duomenų subjektams aiškia ir paprasta kalba aprašomas saugumo pažeidimo pobūdis ir pateikiama bent Tvarkos 16.2–16.4 punktuose nurodyta informacija ir priemonės.

21. Tvarkos 19 punkte nurodyto pranešimo duomenų subjektams nereikalaujama, jeigu įvykdomos bet kurios toliau nurodytos sąlygos:

21.1. Gimnazija įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems saugumo pažeidimas turėjo poveikio, visų pirma tas priemonės, kuriomis užtikrinama, kad neturint leidimo susipažinti su asmens duomenimis nebūtų galimybės juos panaudoti (pavyzdžiui, naudojant šifravimą, pseudonimizaciją);

21.2. Gimnazija toliau ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

21.3. tai pareikalautų neproporcingai daug pastangų. Tokiu atveju apie tai paskelbiama viešai (pavyzdžiui, naujienų portale, Gimnazijos internetiniame puslapyje ar kitomis žiniasklaidos formomis) arba darbuotojui informuoti taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai (pavyzdžiui, el. paštu ar trumposiomis SMS žinutėmis).

22. Jeigu Gimnazija dar nėra pranešusi duomenų subjektams apie saugumo pažeidimą, tačiau priežiūros institucija, apsvarsčiusi, kokia yra tikimybė, kad dėl saugumo pažeidimo kils didelis pavojus, pareikalauja tai padaryti, Gimnazija praneša duomenų subjektams 19 punkte nustatyta tvarka.

VII SKYRIUS SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

23. Visi Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, registruojami asmens duomenų saugumo pažeidimų registravimo žurnale (toliau - Žurnalas). Informacija apie Pažeidimą į Žurnalą įvedama nedelsiant, kai tik nustatomas Pažeidimo faktas ir įvertinama rizika (per 5 darbo dienas). Žurnale esanti informacija papildoma ir (ar) koreguojama.

24. Prie kiekvieno saugumo pažeidimo kortelės turi būti pridedama įvykusio saugumo pažeidimo analizė, kurioje nurodomi veiksmai, kuriuos vykdant siekiama išvengti analogiškų saugumo pažeidimų ateityje.

25. Žurnale nurodomi:

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

25.2. Pažeidimo poveikis ir pasekmės;

25.3. Taisomieji veiksmai (techninės ir organizacinės priemonės), kurių buvo imtasi;

25.4. Priežastys dėl su Pažeidimu susijusių sprendimų priėmimo;

25.5. Pranešimo VDAI pateikimo vėlavimo priežastys (jeigu Pranešimą vėluojama pateikti ar Pranešimas teikiamas etapais);

25.6. Informacija, susijusi su pranešimu duomenų subjektui;

25.7. Kita reikšminga informacija susijusi su Pažeidimu.

26. Žurnalas tvarkomas raštu, įskaitant elektroninę formą, ir saugomas 2 (du) metus pagal Lietuvos vyriausiojo archyvaro patvirtintą dokumentų saugojimo tvarką - Vidaus administravimo dokumentų saugojimo terminų rodyklę. Žurnalą tvarkant elektronine forma, naikinami senesni nei 2 (dviejų) metų įrašai.

VIII SKYRIUS ATSAKOMYBĖ

27. Jei dėl saugumo pažeidimo laiku nesiimama tinkamų priemonių, duomenų subjektai gali patirti materialinę ar nematerialinę žalą, pavyzdžiui, prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota asmens tapatybė, jam padaryta

finansinių nuostolių, neleistina atstatyti pradinę informaciją panaikinus pseudonimus, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesinė paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

28. Gimnazijoje nustatytų taisyklių, nustatančių reagavimo į saugumo pažeidimus nesilaikymas yra laikomas darbo tvarkos pažeidimu, už kurį darbuotojui gali būti taikoma atsakomybė.

29. Darbuotojams, kurie pažeidžia Reglamentą ar kitus teisės aktus, reglamentuojančius reagavimo į saugumo pažeidimus taisykles, gali būti taikomos minėtuose teisės aktuose numatytos atsakomybės priemonės.

IX SKYRIUS BAIGIAMOSIOS NUOSTATOS

30. Šios Tvarkos laikymosi stebėseną ir kontrolę atliekama nuolat.

31. Nustačius šios Tvarkos pažeidimą, nedelsiant atliekamas pažeidimo aplinkybių, priežasčių bei pasekmių tyrimas ir neigiamų pasekmių šalinimas, taip pat imamasi neatidėliotinų priemonių, kad tokie pažeidimai nepasikartotų ateityje.

32. Ši Tvarka peržiūrima ne rečiau kaip kartą per 2 (du) metus arba atitinkamoms institucijoms, kaip kad VDAI priėmus naujus reglamentuojančius teisės aktus.

33. Ši Tvarka taikoma nuo jos patvirtinimo datos.

34. Ši Tvarka gali būti pakeista ar panaikinta bet kuriuo metu atskiru Gimnazijos direktoriaus įsakymu.

35. Darbuotojai supažindinami su šia Tvarka pasirašytinai ir tuo įsipareigoja laikytis šioje Tvarkoje nustatytų taisyklių.
