Prienų r. Jiezno gimnazijos bendrųjų, mokinių ir ugdytinių bei jų atstovų
asmens duomenų tvarkymo taisyklių
5 priedas

POVEIKIO ASMENS DUOMENŲ APSAUGAI VERTINIMO PROCEDŪRA

I. SĄVOKOS

1. Asmens duomenų saugumo pažeidimas reiškia pažeidimą, 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. Poveikio asmens duomenų apsaugai vertinimo procedūra (toliau – PADAV) reiškia poveikio asmens duomenų apsaugai vertinimą.
3. Priežiūros institucija reiškia valstybės narės pagal BDAR 51 straipsnį įsteigtą nepriklausomą valdžios instituciją. Lietuvos Respublikos atveju tokia institucija yra Valstybinė duomenų apsaugos inspekcija.
4. Procedūra reiškia šią Poveikio asmens duomenų apsaugai vertinimo procedūrą.
5. Projekto vadovas (toliau – PV) reiškia asmenį, kuris yra atsakingas už projektą, kurio metu sukuriama nauja ar iš esmės atnaujinama Prienų r. Jiezno gimnazijos vykdomo asmens duomenų tvarkymo sistema.

II. APIMTIS

6. Šis dokumentas taikomas PADAV procedūroms, kurias asmens duomenų valdytojas vykdo naujos ar atnaujintos automatinio asmens duomenų tvarkymo sistemos kūrimo pradžioje ir jos metu.

III. PROCESAS

7. PADAV tikslas yra sistemiškai identifikuoti rizikas ir galimą asmens duomenų rinkimo, saugojimo ir skleidimo poveikį ir ištirti bei įvertinti alternatyvius asmens duomenų tvarkymo procesus tam, kad būtų galima sušvelninti galimas privatumo grėsmes.
8. PADAV atlikimas yra privalomas tada, jei tam tikro pobūdžio asmens duomenų tvarkymas gali kelti didelį pavojų, visų pirma tada, kai naudojamos naujos technologijos, atsižvelgiant į asmens duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms.
9. PADAV turėtų būti įgyvendintas prieš tvarkymą. Atitinkamai, PADAV turėtų prasidėti taip anksti, kaip yra praktiška kuriant tvarkymo operaciją, net jei tam tikri jos aspektai vis dar nėra žinomi. Tai, kad gali prireikti atnaujinti PADAV kai tvarkymas jau bus prasidėjęs nėra pateisinama priežastis atidėti ar nevykdyti PADAV.
10. Kai asmens duomenų tvarkymas tikėtinai gali kelti didelę riziką fizinių asmenų teisėms ir laisvėms, asmens duomenų valdytojas turi atlikti PADAV tam, kad būtų įvertinta visų pirma to pavojaus kilmė, pobūdis, specifika ir rimtumas.
11. Kiekvienam projektui, kurio metu planuojama sukurti naujas ar iš esmės atnaujinti esamas Prienų „Ąžuolo“ progimnazijos valdomas asmens duomenų tvarkymo sistemas, turi būti priskiriamas Darbuotojas, veikiantis kaip PV ir atitinkamai esantis atsakingas už tokio projekto vykdymą.
12. PADAV atliekamas PV bendradarbiaujant su atitinkamomis suinteresuotomis šalimis ir asmens duomenų apsaugos pareigūnu.
13. Vienas PADAV gali įvertinti keletą panašių tvarkymo operacijų, keliančių panašias dideles rizikas.
14. Sistemoms, kurios niekaip neidentifikuoja asmenų, įprastai nekeliamas reikalavimas atlikti PADAV. Tačiau būtina atsižvelgti į tai, kad tai, kas gali atrodyti nuasmenintais asmens duomenimis, iš

tikro gali būti identifikuojantys naudojant juos kartu su kita informacija, taigi nuasmeninti asmens duomenys turėtų būti atidžiai įvertinti siekiant įsitikinti, kad jais nebus identifikuojami individai.

IV. 1 ETAPAS – POREIKIO ATLIKTI PDAV NUSTATYMAS

15. Šio etapo metu PV atsako į atrankos klausimus.

16. Atrankos klausimai skirti nustatyti, ar yra reikalingas PADAV. Jei atsakymas į bet kurį iš šių klausimų yra „taip“, PADAV turėtų būti atliekamas:

16.1. Ar sistema tikėtinai gali kelti didelę riziką fizinių asmenų teisėms ir laisvėms?

16.2. Ar sistema apima sistemingą ir išsamų su fiziniais asmenimis susijusių asmeninių aspektų vertinimą, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, ir kuriuo remiantis priimami sprendimai, kuriais padaromas su fiziniu asmeniu susijęs teisinis poveikis arba kurie daro panašų didelį poveikį fiziniam asmeniui?

16.3. Ar ši sistema apima specialių kategorijų duomenų, atitinkamai (a) asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, (b) genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją ar (c) asmens duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymą dideliu mastu?

16.4. Ar šia sistema naudojantis bus atliekamas sistemingas viešos vietos stebėjimas dideliu mastu?

16.5. Ar šia sistema atliekamos tvarkymo operacijos, kurioms taikomas reikalavimas atlikti PADAV pagal Priežiūros institucijos parengtą tokių operacijų sąrašą?

17. Kiti kriterijai kurie turėtų būti įvertinti kaip galintys lemti duomenų tvarkymo operacijų „didelę riziką“, dėl kurios reikėtų atlikti PADAV, yra tokie:

17.1. Ar asmens duomenys yra tvarkomi dideliu mastu? Į žemiau įvardytus faktorius turėtų būti atsižvelgta sprendžiant, ar tvarkymas atliekamas dideliu mastu:

17.1.1. Paveikiamų asmens duomenų subjektų skaičius kaip konkretus skaičius arba kaip proporcija iš atitinkamos populiacijos;

17.1.2. Asmens duomenų kiekį ir/ar tvarkomų skirtingų duomenų spektrą;

17.1.3. Asmens duomenų tvarkymo veiksmų trukmę arba pastovumą;

17.1.4. Tvarkymo veiksmų geografinę apimtį.

17.2. Ar asmens duomenų rinkiniai buvo suderinti arba sujungti tada, kai, pavyzdžiui, jie kilo iš dviejų ar daugiau skirtingų asmens duomenų tvarkymo veiklų, atliktų skirtingais tikslais ir/arba skirtingų asmens duomenų valdytojų, tokiu būdu, kuris peržengtų pagrįstus asmens duomenų subjekto lūkesčius?

17.3. Ar tvarkomi asmens duomenys susiję su labiau pažeidžiamais duomenų subjektais (vaikais, darbuotojais, pacientais ir t.t.)?

17.4. Ar tvarkymas vykdomas pritaikant inovatyvius technologinius ar organizacinius sprendimus?

17.5. Ar asmens duomenys bus perduodami už Europos Sąjungos ribų?

17.6. Ar pats asmens duomenų tvarkymas gali apriboti asmens duomenų subjektų galimybės įgyvendinti savo teises arba naudotis paslaugomis ar sudaryti sutartį?

18. Kuo daugiau iš aukščiau nurodytų kriterijų atitinka tvarkymas, tuo labiau tikėtina, kad jis kelia didelę grėsmę asmens duomenų subjektų teisėms bei laisvėms ir atitinkamai reikalauja PADAV. Tvarkymas, atitinkantis mažiau nei du kriterijus, įprastai nereikalaus PADAV dėl žemesnės rizikos, tačiau būtina racionaliai įvertinti faktinę situaciją. Atitinkamai PV visais atvejais privalo išsamiai aprašyti savo sprendimą nevykdyti PADAV.

19. Jei pagal atsakymus į aukščiau nurodytus klausimus arba egzistuojant kitiems „didelės

rizikos“ egzistavimo pagrindams PADAV turėtų būti atliekamas, tada PV tęsia pagal Procedūros 2 etapą.

20. Procedūra pakartojama tada, jei atliekami esminiai vertinto asmens duomenų tvarkymo pakeitimai.

V. 2 ETAPAS – PASIRUOŠIMAS

21. PV parengia sistematišką planuojamų tvarkymo procedūrų ir jų tikslų aprašymą įskaitant, kur tai tinkama, Prienų r. Jiezno gimnazijos, kaip asmens duomenų valdytojo, siekiamus teisėtus interesus.

22. Tuo atveju, jei teisėtų interesų siekimas yra taikomas kaip teisėto asmens duomenų tvarkymo pagrindas, Prienų r. Jiezno gimnazija taip pat turėtų išsiaiškinti asmens duomenų subjektų ar jų atstovų nuomonę apie numatytą asmens duomenų tvarkymą.

23. Jei Prienų r. Jiezno gimnazija priima sprendimą nesiaiškinti asmens duomenų subjektų nuomonės arba jos galutinis sprendimas skiriasi nuo asmens duomenų subjektų išreikštos nuomones, tokių sprendimų pateisinimas turi būti aprašomas.

VI. 3 ETAPAS – DUOMENŲ RINKIMAS

24. Šiame etape PV kritiškai išanalizuoja asmens duomenų tvarkymo situacijas, nustatytas 2 etapo metu.

25. DV privalo išanalizuoti ir aprašyti esmines su asmens duomenimis susijusias sritis atsakydamas į šiuos klausimus:

25.1. Kokie asmens duomenys bus tvarkomi?

25.2. Koks yra asmens duomenų tvarkymo tikslas(-ai)?

25.3. Kaip vyksta asmens duomenų tvarkymo procesas (aprašyti, kaip asmens duomenų tvarkymas vyksta nuo asmens duomenų gavimo iki sunaikinimo)?

25.4. Ar asmens duomenų subjektui bus pateikiama visa reikiama informacija?

25.5. Ar visi tvarkomi asmens duomenys būtini duomenų tvarkymui vykdyti (pagrįsti būtinumą)?

25.6. Ar asmens duomenys yra tikslūs ir esant poreikiui atnaujinami?

25.7. Kiek laiko saugomi asmens duomenys?

25.8. Kaip asmens duomenų subjektai informuojami apie asmens duomenų tvarkymą?

25.9. Jei asmens duomenys tvarkomi remiantis sutikimu, kokiu būdu jis gaunamas?

25.10. Kaip asmens duomenų subjektai gali įgyvendinti savo teises?

25.11. Jei pasitelkiamas asmens duomenų tvarkytojas ar tvarkytojai, ar jų pareigos tinkamai aprašytos susitarime pagal BDAR reikalavimus?

25.12. Jei asmens duomenys teikiami už Europos Sąjungos ribų, ar asmens duomenys yra tinkamai apsaugomi?

25.13. Kokias saugumo priemones Prienų r. Jiezno gimnazija įgyvendins siekdama apsaugoti asmens duomenis?

VII.4 ETAPAS – RIZIKOS NUSTATYMAS

26. Kai nustatomos tvarkymo situacijos ir susijusių asmens duomenų pobūdis, PV įvertina grėsmes asmens duomenų subjektų teisėms ir laisvėms.

27. Esminiai asmens duomenų subjektams kylančių grėsmių tipai, atitinkantys asmens duomenų saugumo pažeidimų rūšis, yra šie:

27.1. Konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie asmens duomenų suteikiama prieiga tam teisės neturintiems asmenims;

27.2. Pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba asmens duomenys yra sunaikinami;

27.3. Vientisumo pažeidimas – netyčia ar neteisėtai atliekami nepageidaujami asmens duomenų pakeitimai.

28. Įvardijęs grėsmes, PV jas aprašo atsakydamas į šiuos klausimus:

28.1. Kokios tikėtinos pasekmės asmens duomenų subjektams tada, jei įvyktų pažeidimas?

28.2. Kokie veiksmai/įvykiai galėtų sudaryti sąlygas tokiam pažeidimui įvykti?

28.3. Kokie yra grėsmės šaltiniai (asmenys ar aplinkybes, dėl kurių tyčia ar atsitiktinai gali įvykti pažeidimas)?

29. PV įvertina sistemos atitiktį reikalavimams, nustatytiems BDAR ir atitinkamuose įstatymuose ir kituose teisės aktuose.

VIII. 5 ETAPAS – RIZIKOS VALDYMO PRIEMONIŲ NUSTATYMAS

30. Šio etapo metu PV turi aprašyti, kokios esamos ar planuojamos techninės (fizinio ir kibernetinio saugumo) bei organizacinės priemonės padės suvaldyti nustatytas grėsmes asmens duomenų subjektų teisėms ir laisvėms. Pirmenybė teikiama reikšmingiausioms nustatytoms saugumo grėsmėms ir jų valdymo priemonėms, tačiau turi būti pagrindžiamas tam tikrų grėsmių ignoravimas.

31. Aprašius rizikos valdymo priemones, turi būti nurodoma, kokio rimtumo ir tikėtinumo grėsmė išlieka atsižvelgiant į taikomas ar planuojamas taikyti priemones, skirtas jo išvengti.

IX. 6 ETAPAS – REZULTATŲ ATASKAITOS TEIKIMAS

32. Šiame etape PV parengia ataskaitą apie PADAV rezultatus.

33. Ataskaitoje turi būti aprašomi ankstesnių etapų eiga ir rezultatai, nurodomi konkretūs veiksmai, kurių reikia imtis siekiant suvaldyti kylančias grėsmes, jei esamų rizikos valdymo priemonių tam nepakanka.

34. Kai iš PADAV paaiškėja, kad asmens duomenų tvarkymo operacijos kelia didelį pavojų asmens duomenų subjektų teisėms ir laisvėms, o asmens duomenų valdytojas jo negali sumažinti tinkamomis rizikos valdymo priemonėmis, atsižvelgiant į turimas technologijas ir įgyvendinimo sąnaudas, prieš pradedant duomenų tvarkymą turi būti konsultuojamasi su Priežiūros institucija.

35. asmens duomenų tvarkymo veiklos kūrimo procesui tęsiantis, PDAV turėtų būti peržiūrėtas, patikslintas ir atnaujintas jei projekto raida ar įgyvendinimas daro naują įtaką privatumui, kuri anksčiau nebuvo įvertinta.

_____

POVEIKIO ASMENS DUOMENŲ APSAUGAI VERTINIMO ATASKAITA

Duomenų valdytojas:			
Duomenų valdytojo (jei taikoma, ir bendro duomenų valdytojo) pavadinimas (jei fizinis asmuo – vardas ir pavardė)			
adresas	*tel. nr.*	*el. p.*	*kitos ryšių priemonės*
Duomenų apsaugos pareigūnas (jei taikoma)**:**			
Duomenų apsaugos pareigūno vardas ir pavardė			
adresas	*tel. nr.*	*el. p.*	*kitos ryšių priemonės*
Priežastys, dėl kurių būtina atlikti poveikio asmens duomenų apsaugai vertinimą:			
Planuojamos vykdyti veiklos aprašymas, jos tikslai ir planuojamos atlikti asmens duomenų tvarkymo operacijos. Paaiškinimas, kodėl būtina atlikti poveikio duomenų apsaugai vertinimą. Jei reikia, prie formos pridedami susiję dokumentai.			
Asmens duomenų tvarkymo aprašymas			
Aprašomi asmens duomenų rinkimo, naudojimo, saugojimo ir naikinimo veiksmai, nurodoma, iš kokių šaltinių bus renkami duomenys, kam bus teikiami (galima pateikti asmens duomenų tvarkymo veiksmų schemą). Aprašoma, kokie asmens duomenų tvarkymo veiksmai gali kelti pavojų fizinių asmenų teisėms ir laisvėms.			
Aprašomas tvarkymo mastas: kokių kategorijų asmens duomenys bus tvarkomi; ar bus tvarkomi specialių kategorijų asmens duomenys arba duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas; kiek duomenų, kaip dažnai bus renkama ir naudojama; kaip ilgai bus saugomi asmens duomenys; nurodomas apytikslis duomenų subjektų skaičius bei geografinė duomenų tvarkymo aprėptis.			
Aprašomas duomenų tvarkymo pobūdis: kokio pobūdžio santykiai sieja Jūsų įmonę su duomenų subjektais; ar duomenų subjektai turės galimybę kontroliuoti duomenų tvarkymą; ar duomenų subjektai gali numatyti, kad jų asmens duomenys bus tvarkomi šiuo būdu; ar bus tvarkomi vaikų ir kitų pažeidžiamų asmenų duomenys; įvertinama, ar toks duomenų tvarkymas yra saugus; ar duomenų tvarkymo technologijos yra naujos, ar egzistuojančios technologijos bus panaudotos kitokiu būdu; koks yra technologijų išsivystymo lygis šioje srityje; ar yra kokių nors visuomeninių ar pan. problemų ar klausimų, į kuriuos būtina atsižvelgti; nurodoma, ar yra įsipareigojimas laikytis patvirtinto elgesio kodekso ar patvirtinto sertifikavimo mechanizmo.			

Aprašomi asmens duomenų tvarkymo tikslai: kokį rezultatą siekiama gauti; kokį poveikį tai turės fiziniams asmenims; kokia yra tokio duomenų tvarkymo nauda Jūsų įmonei bei kitiems asmenims.
Konsultacijos
Aprašoma, kaip planuojama sužinoti suinteresuotų asmenų nuomonę arba pagrindžiama, kodėl to daryti nebūtina: kokių asmenų nuomonę planuojama gauti; kokie asmenys bus pasitelkti Jūsų įmonėje, ar bus pasitelkti duomenų tvarkytojai; ar planuojama konsultuotis su duomenų saugos ekspertais ar kitokių sričių ekspertais.
Būtinumo ir proporcingumo įvertinimas
Aprašomas asmens duomenų tvarkymo teisėtumas ir tvarkymo proporcingumas: nurodomas teisėto tvarkymo pagrindas; įvertinama, ar tvarkant asmens duomenis bus pasiektas Jūsų tikslas; ar tą patį rezultatą įmanoma pasiekti kitokiu būdu; kokiu būdu bus išvengta veiklos sutrikimų; kaip bus užtikrinta duomenų kokybė ir įgyvendintas duomenų kiekio mažinimo principas; kokia informacija bus pateikta duomenų subjektams; kaip Jūsų įmonė planuoja įgyvendinti duomenų subjektų teises; kokiu būdu bus užtikrinta, kad duomenų tvarkytojas laikytųsi reikalavimų; kokiu būdu bus užtikrintas į užsienio valstybes teikiamų asmens duomenų saugumas.

Pavojų nustatymas ir įvertinimas

Aprašomas pavojaus ir poveikio fiziniam asmeniui pobūdis. Jei būtina, aprašoma susijusi verslo rizika.	**Žalos tikimybė**	**Žalos sunkumas**	**Bendras pavojaus lygis**
	Mažai tikėtina, tikėtina ar labai tikėtina	Minimali, reikšminga ar sunki	Žemas, vidutinis ar aukštas

Priemonių sumažinti pavojų nustatymas

Nurodomos papildomos priemonės, kurių galima imtis siekiant sumažinti ar panaikinti aukšto ar vidutinio lygio pavojus.

Pavojus	**Priemonės sumažinti ar pašalinti pavojų**	**Priemonės pritaikymo rezultatas**	**Likęs pavojus**	**Priemonė patvirtinta**
		Pašalinta, sumažinta, priimtina rizika	Žemas, vidutinis ar aukštas	Taip, ne

Išvados ir sprendimai		
Nurodomos priemonės ir įvardijamas likęs pavojus	*Vardas, pavardė, data, parašas*	*Pastabos*
Priemonės patvirtintos:		Įtraukti numatytas priemones į veiklos planą, nustatant atlikimo terminą ir atsakingus asmenis
Likęs pavojus pripažintas priimtina rizika:		Jei priimtina rizika pripažintas aukšto lygio pavojus priimtinas, privaloma kreiptis dėl išankstinės konsultacijos į Valstybinę duomenų apsaugos inspekciją
Duomenų apsaugos pareigūno nuomonė		
Duomenų apsaugos pareigūno nuomonė turi būti pateikta dėl asmens duomenų tvarkymo teisėtumo, planuojamų priemonių pavojams mažinti ar pašalinti bei dėl galimybės toliau tvarkyti asmens duomenis.		
Nurodoma duomenų apsaugos pareigūno nuomonė:		
		Vardas, pavardė, data, parašas
Nurodoma, ar atsižvelgta į duomenų apsaugos pareigūno nuomonę		
Jeigu atmesta, pagrindžiama, kodėl.		
		Vardas, pavardė, data, parašas
Gautos kitų asmenų nuomonės		
Trumpai aprašomos kitų asmenų nuomonės ir nurodoma, ar į jas atsižvelgta. Jeigu sprendimas skiriasi nuo susijusių asmenų nuomonės, pagrindžiama, kodėl.		
		Vardas, pavardė, data, parašas
Už šio poveikio duomenų apsaugai vertinimo priežiūrą paskirtas atsakingas asmuo		
Trumpai aprašomos kitų asmenų nuomonės ir nurodoma, ar į jas atsižvelgta. Jeigu sprendimas skiriasi nuo susijusių asmenų nuomonės, pagrindžiama, kodėl.		
		Vardas, pavardė, data, parašas