PATVIRTINTA
Prezidento Antano Smetonos gimnazijos direkotriaus
2022 m. rugsėjo 1 d. įsakymu Nr. V - 87

PREZIDENTO ANTANO SMETONOS GIMNAZIJOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Prezidento Antano Smetonos gimnazijos asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) nustato asmens duomenų saugumo pažeidimų valdymo, pranešimų asmens duomenų priežiūros institucijai bei duomenų subjektams teikimo tvarką Prezidento Antano Smetonos gimnazijoje (toliau – Gimnazija) bei Gimnazijos duomenų tvarkytojų pareigas kilus asmens duomenų saugumo pažeidimui.

2. Aprašo tikslas – užtikrinti efektyvų Gimnazijos ir jos duomenų tvarkytojų reagavimą į galimą asmens duomenų saugumo pažeidimą, nustatyto asmens duomenų saugumo pažeidimo valdymą ir operatyvų jo sukeltų padarinių šalinimą siekiant kiek įmanoma sumažinti riziką duomenų subjektų teisėms ir laisvėms.

3. Pagrindinės Apraše vartojamos sąvokos:

3.1. **asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti;

3.2. **asmens duomenų saugumo pažeidimas** – 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;

3.3. **duomenų subjektas** – fizinis asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius;

3.4. **duomenų tvarkytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis;

3.5. **duomenų valdytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones;

3.6. **Reglamentas** – Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. Reglamentas (ES) 2016/679;

3.7. **VDAI –** Valstybinė duomenų apsaugos inspekcija;

3.8. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679 ir kituose teisės aktuose, reglamentuojančiuose asmens duomenų apsaugą.

4. Asmens duomenų saugumo pažeidimai yra skirstomi į 3 tipus:

4.1. konfidencialumo pažeidimas – be Gimnazijos leidimo ar neteisėtai tretiesiems asmenims atskleidžiami asmens duomenys arba suteikiama prieiga prie šių duomenų;

4.2. prieinamumo pažeidimas – dėl neatsargumo arba neteisėtai prarandama prieiga prie Administracijos ar jos duomenų tvarkytojų tvarkomų asmens duomenų arba pastarieji asmens duomenys dėl neatsargumo arba neteisėtai yra sunaikinami;

4.3. vientisumo pažeidimas – Gimnazijos ar jos duomenų tvarkytojų tvarkomi asmens duomenys neteisėtai ar dėl neatsargumo yra pakeičiami be Gimnazijos leidimo.

5. Vienas asmens duomenų saugumo pažeidimas gali atitikti kelis tipus.

6. Reagavimo į galimą asmens duomenų saugumo pažeidimą, nustatyto asmens duomenų saugumo pažeidimo valdymo ir šalinimo procese dalyvauja ir Gimnazijos duomenų apsaugos pareigūnas / duomenų apsaugos pareigūno funkcijas atliekanti įmonė, teikdamas / teikdama pasiūlymus dėl asmens duomenų saugumo pažeidimo tyrimo ir nustatymo, valdymo, jo sukeltų padarinių šalinimo.

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ PAŽEIDIMĄ GIMNAZIJOS VIDUJE

7. Bet kuris Gimnazijos darbuotojas ar valstybės tarnautojas, pastebėjęs ar sužinojęs apie neteisėtą Gimnazijos tvarkomų asmens duomenų perdavimą arba neteisėtą prieigos prie šių asmens duomenų suteikimą tretiesiems asmenims, asmens duomenų perdavimą arba prieigos suteikimą tretiesiems asmenims be Gimnazijos direktoriaus ar jo įgalioto asmens leidimo, dėl neatsargumo ar neteisėtai prarastą prieigą prie Gimnazijos tvarkomų asmens duomenų, dėl neatsargumo ar neteisėtai sunaikintus, pakeistus asmens duomenis, taip pat pakeistus asmens duomenis be Gimnazijos direktoriaus ar jo įgalioto asmens leidimo, privalo nedelsiant pranešti asmenims, atsakingiems už asmens duomenų saugumo pažeidimų tyrimą, nustatymą ir valdymą bei sukeltų padarinių šalinimą (toliau – Atsakingas asmuo).

8. Atsakingą asmenį skiria Gimnazijos direktorius.

9. Apie galimą asmens duomenų saugumo pažeidimą Atsakingas asmuo informuojamas elektroniniu paštu saulius.peckauskas@pasmetonosgimnazija.lt .

III SKYRIUS
GALIMO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS

10. Atsakingas asmuo, gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą, privalo nedelsiant pradėti tyrimą dėl galimo asmens duomenų saugumo pažeidimo. Tyrimo metu yra įvertinama gauta informacija, jos pakankamumas, patikimumas ir teisingumas. Vykdantis tyrimą asmuo gali pareikalauti Gimnazijos darbuotojo ar valstybės tarnautojo, pateikusio informaciją, pateikti papildomus paaiškinimus, apklausti kitus Gimnazijos darbuotojus ir pedagogus, galinčius turėti informacijos apie galimą asmens duomenų saugumo pažeidimą, apklausti asmenį, dėl kurio veiksmų galimai kilo asmens duomenų saugumo pažeidimas, jei su šiuo asmeniu yra galimybė susisiekti, patikrinti fizinę vietą ar skaitmeninę erdvę, kurioje pastebėtas asmens duomenų saugumo pažeidimas arba apie jį sužinota.

11. Tyrimo pabaigoje Atsakingas asmuo surašo Galimo asmens duomenų saugumo pažeidimo tyrimo išvadą (1 priedas), kurioje pažymima, ar buvo nustatytas asmens duomenų saugumo pažeidimas. Jei asmens duomenų saugumo pažeidimas nebuvo nustatytas, tyrimas nutraukiamas. Jei asmens duomenų saugumo pažeidimas nustatomas, tyrimą atlikęs asmuo privalo papildomai įvertinti asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygį.

12. Rizikos lygiai skirstomi į žemą, vidutinį ir didelį. Vertinant, kokio lygio rizika kyla duomenų subjekto teisėms ir laisvėms, reikia vadovautis protingumo principu ir atsižvelgti į tai, kokie padariniai atsiranda dėl asmens duomenų saugumo pažeidimo.

13. Tyrimas privalo būti atliktas ir išvada pateikta per 48 val. nuo informacijos apie galimą asmens duomenų saugumo pažeidimą gavimo momento.

IV SKYRIUS
NUSTATYTO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO VALDYMAS IR ŠALINIMAS

14. Gimnazija asmens duomenų saugumo pažeidimą valdo ir pažeidimo sukeltus neigiamus padarinius šalina įgyvendindama tinkamas organizacines ir technines apsaugos priemones. Gimnazijos taikomos organizacinės ir techninės apsaugos priemonės turi kiek įmanoma labiau sumažinti šiuos padarinius.

V SKYRIUS
PRANEŠIMAS VDAI APIE NUSTATYTĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

15. Jei tyrimo išvadoje buvo nustatyta, kad atitinkamas asmens duomenų saugumo pažeidimas kelia didelę riziką duomenų subjektų teisėms ir laisvėms, Gimnazija pateikia VDAI pranešimą apie Gimnazijoje nustatytą asmens duomenų saugumo pažeidimą. Apie asmens duomenų saugumo pažeidimą VDAI pranešama užpildant VDAI patvirtintą Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamą formą ir ją pateikiant internetu ar kitais VDAI nustatytais būdais.

16. Apie asmens duomenų saugumo pažeidimą VDAI informuojama ne vėliau kaip per 72 val. nuo sužinojimo apie galimą asmens duomenų saugumo pažeidimą momento. Jei, atsižvelgiant į asmens duomenų saugumo pažeidimo sudėtingumą, šio pažeidimo tyrimo bei įgyvendinamų organizacinių ir techninių apsaugos priemonių apimtis ir kitas objektyvias aplinkybes, VDAI informuoti per 72 val. nėra galimybės, Gimnazija gali informuoti VDAI vėliau pranešime pateikdama vėlavimo priežastis.

VI SKYRIUS
PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE NUSTATYTĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

17. Jei tyrimo išvadoje buvo nustatyta, kad atitinkamas asmens duomenų saugumo pažeidimas kelia didelę riziką duomenų subjektų teisėms ir laisvėms, Gimnazija privalo pateikti duomenų subjektams, kurių teisėms ir laisvėms kyla didelė rizika, pranešimą apie Gimnazijoje nustatytą asmens duomenų saugumo pažeidimą. Pranešime turi būti nurodoma ši informacija:

17.1. nustatyto asmens duomenų saugos pažeidimo aprašymas;

17.2. Gimnazijos duomenų apsaugos pareigūno ar duomenų apsaugos pareigūno funkcijas atliekanti įmonė ir Atsakingo asmens, atlikusio tyrimą, vardas, pavardė ir kontaktiniai duomenys;

17.3. asmens duomenų saugumo pažeidimo neigiami padariniai, keliantys didelę riziką duomenų subjekto teisėms ir laisvėms;

17.4. organizacinių ir techninių apsaugos priemonių, kurios padėtų pašalinti arba kiek įmanoma sumažinti neigiamus padarinius duomenų subjekto teisėms ir laisvėms, aprašymas;

17.5. kita, Gimnazijos manymu, su asmens duomenų saugumo pažeidimu susijusi informacija, kuri turėtų būti pateikiama duomenų subjektui.

18. Pranešimas duomenų subjektui siunčiamas duomenų subjekto turimais kontaktiniais duomenimis.

19. Apie asmens duomenų saugumo pažeidimą duomenų subjektas informuojamas ne vėliau kaip per 72 val. nuo sužinojimo apie galimą asmens duomenų saugumo pažeidimą momento. Jei, atsižvelgiant į asmens duomenų saugumo pažeidimo sudėtingumą, šio pažeidimo tyrimo bei įgyvendinamų organizacinių ir techninių apsaugos priemonių apimtis ir kitas objektyvias aplinkybes, duomenų subjekto informuoti per 72 val. nėra galimybės, Gimnazija gali informuoti duomenų subjektą vėliau pranešime pateikdama vėlavimo priežastis.

20. Pranešimo duomenų subjektui teikti Gimnazija neprivalo, jei egzistuoja bent viena iš žemiau nurodytų sąlygų:

20.1. Gimnazija įgyvendino tinkamas organizacines ir technines apsaugos priemones, kurios pašalino nustatyto asmens duomenų saugumo pažeidimo keliamus neigiamus padarinius duomenų subjekto teisėms ir laisvėms arba sumažino nustatyto asmens duomenų saugumo pažeidimo keliamą didelę riziką iki vidutinės ar žemos rizikos;

20.2. pranešimo teikimas duomenų subjektui iš Gimnazijos pareikalautų neproporcingų pastangų dėl asmens duomenų saugumo pažeidimo sudėtingumo, pažeidimo tyrimo bei įgyvendinamų organizacinių ir techninių apsaugos priemonių apimties, duomenų subjektų, kurių teisėms ir laisvėms kilo didelė rizika, didelio skaičiaus ir kitų objektyvių aplinkybių. Tokiu atveju duomenų subjektui pranešimas yra teikiamas ne asmeniškai, o viešai, pasitelkiant žiniasklaidos ir kitas informacijos sklaidos priemones.

VII SKYRIUS
DUOMENŲ TVARKYTOJŲ PAREIGOS ĮVYKUS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUI

21. Bet kuris Gimnazijos duomenų tvarkytojo darbuotojas, pastebėjęs ar kitaip sužinojęs apie galimą duomenų tvarkytojo tvarkomų asmens duomenų saugumo pažeidimą, privalo nedelsiant apie tai informuoti duomenų tvarkytojo įgaliotus asmenis, atsakingus už asmens duomenų saugumo pažeidimų tyrimą, valdymą ir šalinimą. Duomenų tvarkytojo įgalioti asmenys apie galimą asmens duomenų saugumo pažeidimą atitinkamai turi informuoti Gimnaziją.

22. Duomenų tvarkytojas, nustatęs asmens duomenų saugumo pažeidimą, taip pat privalo imtis visų reikalingų organizacinių ir techninių apsaugos priemonių, kad pašalintų, o jei pašalinti neįmanoma, kad sumažintų riziką, kylančią duomenų subjektų teisėms ir laisvėms.

VIII SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMAS

23. Gimnazija registruoja visus asmens duomenų saugumo pažeidimus: tiek nustatytus, tiek nenustatytus. Asmens duomenų saugumo pažeidimai registruojami Asmens duomenų saugumo pažeidimų registracijos žurnale (2 priedas).

24. Gimnazijoje Asmens duomenų saugumo pažeidimų registracijos žurnalas yra tvarkomas elektroniniu būdu.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

25. Visi Gimnazijos darbuotojai, pedagogai ir Gimnazijos duomenų tvarkytojai, paskirti tvarkyti Gimnazijos asmens duomenis, privalo laikytis šiame Apraše nustatytų reikalavimų.

_____

Prezidento Antno Smetonos gimnazijos asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo 1 priedas

GALIMO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO IŠVADA

20___ m. _____ d. Nr. ___

_____

(surašymo vieta)

Atlikto tyrimo metu asmens duomenų saugumo pažeidimas buvo _____ *(nustatytas / nenustatytas).*

Nr.	**Sąlyga**	**Išvados**
1.	Asmens duomenų saugumo pažeidimo tipas	
2.	Asmens duomenų saugumo pažeidimo aprašymas	
3.	Asmens duomenų saugumo pažeidimo paaiškėjimo data	
4.	Apytikslis asmens duomenų saugumo pažeidimo paaiškėjimo laikas	
5.	Fizinė vieta arba skaitmeninė erdvė, kurioje užfiksuotas asmens duomenų saugumo pažeidimas	
6.	Duomenų subjektų, kurių teisėms ir laisvėms asmens duomenų saugumo pažeidimas sukėlė ar galėjo sukelti neigiamų padarinių, kategorijos ir sąrašas	
7.	Asmens duomenų, kurie buvo paveikti asmens duomenų saugumo pažeidimo, kategorijos ir sąrašas	

8.	Asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis (nenustatytas, žemas, vidutinis, didelis)	
9.	Nustatyti asmens duomenų saugumo pažeidimo sukelti arba tikėtini padariniai duomenų subjektų teisėms ir laisvėms	
10.	Priežastys, kodėl asmens duomenų saugumo pažeidimas nekelia rizikos duomenų subjektų teisėms ir laisvėms (praleisti, jei pateikta išvada dėl sąlygos Nr. 9)	
11.	Pasiūlymai dėl organizacinių ir techninių apsaugos priemonių, kurios padėtų pašalinti arba kiek įmanoma sumažinti neigiamus padarinius duomenų subjektų teisėms ir laisvėms	
12.	Pasiūlymai dėl prevencijos priemonių, padėsiančių ateityje išvengti tokių pačių ar panašių asmens duomenų saugumo pažeidimų	
13.	Kitos tyrimo metu nustatytos aplinkybės	

(Pareigos) (Parašas) (Vardas ir pavardė)

Prezidento Antano Smetonos gimnazijos asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo 2 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRACIJOS ŽURNALAS

Reg. Nr.	Data	Apytikslis laikas	Asmens duomenų saugumo pažeidimo tipas	Pažeidimo vieta (fizinė / skaitmeninė)	Asmens duomenų saugumo pažeidimas nustatytas (taip / ne)

_____