



VILNIAUS SOFIJOS KOVALEVSKAJOS PROGIMNAZIJOS
DIREKTORIAUS

ĮSAKYMAS
DĖL ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠO
PATVIRTINIMO

2021 m. kovo 26 d. Nr. V-*42*
Vilnius

Vadovaudamasi 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų duomenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) 24 straipsnio 1 dalimi:

1. tvirtinu Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašą (pridedama).

Direktorė



Galina Kirilova

PATVIRTINTA

Vilniaus Sofijos Kovalevskajos progimnazijos

direktorius 2021 m. kovo 26 d.

įsakymu Nr. V-42

**ASMENS DUOMENŲ SAUGUMO
PAŽEIDIMŲ VALDYMO TVARKOS
APRAŠAS**

I SKYRIUS

BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pašalinimo ir pranešimo apie juos Vilniaus Sofijos Kovalevskajos progimnazijoje (toliau – progimnazija) tvarką.

2. 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas (ES) 2016/679).

3. Apraše vartojamos sąvokos atitinka Reglamente (ES) 2016/679 apibrėžtas sąvokas.

4. Galimi šie asmens duomenų saugumo pažeidimai:

4.1. konfidentialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie jų suteikimas;

4.2. vientisumo pažeidimas – neleistinas arba netyčinis asmens duomenų pakeitimas;

4.3. prieinamumo pažeidimas – neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas.

5. Atsižvelgiant į aplinkybes, saugumo pažeidimas vienu metu gali būti susijęs su asmens duomenų konfidentialumu, vientisu su prieinamumu, taip pat su bet kokiui jų deriniu.

6. Asmens duomenų saugumo pažeidimas gali įvykti dėl šių priežasčių:

6.1. žmogiškoji klaida (pvz., asmens duomenys persiųsti ne tam adresatui, kuriam jie buvo skirti; ne saugojimui skirtoje vietoje palikti dokumentai, kuriuose yra asmens duomenų; pamesti nešiojami / mobilūs įrenginiai (telefonas, nešiojamas kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys ir kt.);

6.2. vagystė (pvz., pavogti nešiojami / mobilūs įrenginiai, kuriuose saugomi asmens duomenys; pavogtos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų ir kt.);

6.3. kibernetinė ataka (pvz., duomenų bazėje ar informacinėje sistemoje esantys asmens duomenys užšifravomi, naudojant išpirkos reikalaujančią programą; internete paskelbiami informacinių sistemų naudotojų vardai ir slaptažodžiai ir kt.);

6.4. neleistina (neautorizuota) prieiga prie asmens duomenų (pvz., įgaliojimų neturintys asmenys patenka į patalpas, kuriose saugomos bylos su asmens duomenimis; įgaliojimų neturintys asmenys prisijungia prie duomenų bazių ar informacinių sistemų ir kt.);

6.5. įrenginių ar programinės įrangos gedimas, saugos sistemos spragos (pvz., energijos tiekimo nutrūkimas, dėl kurio negalima prieiga prie asmens duomenų; programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas informacinių sistemų naudotojams, klaida ir kt.);

6.6. nenumatyto (force majeure) aplinkybės ir kitos priežastys (gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys ir kt.).

7. Asmens duomenų saugumo pažeidimas, galintis kelti pavojų asmenų teisėms ir laisvėms yra tokis, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą (pvz., asmuo gali patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, pakenkta jo reputacijai, prarastas duomenų, kurie laikomi profesine paslaptimi, konfidencialumas ir kt.).

8. Šis Aprašas skirtas užtikrinti, kad progimnazijos darbuotojai, dirbantys pagal darbo sutartį (toliau – progimnazijos darbuotojai), sugebėtų laiku nustatyti galimus asmens duomenų saugumo pažeidimus bei suprastų, kokie veiksmai privalo būti atlikti valdant juos.

9. Aprašo privalo laikytis visi progimnazijos darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino.

II SKYRIUS

PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

10. Progimnazijos darbuotojas, nustatęs galimą asmens duomenų saugumo pažeidimą, arba gavęs informaciją apie galimą saugumo pažeidimą iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio:

10.1. nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo asmens duomenų saugumo pažeidimo paaiškėjimo momento, žodžiu (tiesiogiai ar telefonu) arba elektroniniu paštu informuoja tiesioginį vadovą.

10.2. užpildo Pranešimą apie asmens duomenų saugumo pažeidimą (Aprašo 1 priedas) ir nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo saugumo pažeidimo paaiškėjimo momento, perduoda jį progimnazijos vadovui.

10.3. jei jmanoma, imasi priemonių pašalinti saugumo pažeidimą ir (ar) priemonių sumažinti jo sukeltas neigiamas pasekmes.

III SKYRIUS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

11. Progimnazijos vadovas, gavęs darbuotojo pranešimą apie asmens duomenų saugumo pažeidimą:

11.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

11.2. konsultuoja su Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) duomenų apsaugos pareigūnu;

11.3. jei saugumo pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkia progimnazijos ar duomenų tvarkytojo IT specialistus ir informacinių sistemų saugos specialistus;

11.4. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

11.5. jei asmens duomenų saugumo pažeidimas padarytas, nustato pažeidimo pobūdį, pričastis, asmens duomenų kategorijas, jų pobūdį ir kiekj, duomenų subjektų kategorijas ir jų kiekj, įvertina padarytą žalą fiziniam asmenims bei tiketinas pažeidimo pasekmes;

11.6. įvertina, kokių skubij ir tinkamų priemonių būtina imtis, kad būtų pašalintas saugumo pažeidimas (pvz., naudoti atsargines kopijas, siekiant atkirti prarastus ar sugadintus duomenis ar kt.);

11.7. nustato, ar apie saugumo pažeidimą būtina pranešti VDAI;

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

12. Progimnazijos darbuotojai, atsakingi už asmens duomenų tvarkymą, pateikia progimnazijos duomenų apsaugos pareigūnui visą jo prašomą informaciją, susijusią su asmens duomenų saugumo pažeidimu ir tyrimu, per jo nurodytą terminą.

13. Atliekant asmens duomenų saugumo pažeidimo tyrimą ir siekiant nustatyti, ar pažeidimas iš tikrujų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas.

14. Vertinant rizikos lygį, atsižvelgiama į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:

14.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis, nuo kurio gali priklausyti pavojaus duomenų subjektams dydis;

14.2. asmens duomenų pobūdis, jautumas ir kiekis – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavoju;

14.3. galimybė identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiemis asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiemis asmenims, todėl pažeidimas padarys mažesnį poveikį duomenų subjektams);

14.4. fizinio asmens specifiniai ypatumai – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavoju, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalią turintys asmenys), tuo didesnį poveikį pažeidimas gali jiems padaryti;

14.5. nukentėjusių duomenų subjektų skaičius – nustatomas nukentėjusių asmenų skaičius: kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnis žalos pavoju;

14.6. pasekmės, sukeltos fiziniams asmenims – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumas; taip pat atsižvelgiant į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis.

15. Įvertinus riziką nustatomas vienas iš trijų rizikos tikimybių lygių – mažas, vidutinis ar didelis rizikos tikimybės lygis.

16. Progimnazijos vadovas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, užpildo Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (Aprašo 2 priedas).

17. Atsižvelgiant į Asmens duomenų saugumo pažeidimo tyrimo ataskaitą, progimnazijos direktorius, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl saugumo pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

18. Sprendžiant asmens duomenų saugumo pažeidimo pašalinimo klausimą bei tvirtinant priemonių planą, priklausomai nuo konkrečių pažeidimo aplinkybių pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą: ištinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamo / mobiliaus įrenginio (telefono, nešiojamo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuo skubiau kreiptis į jį su prašymu ištinti atsiūstus asmens duomenis be galimybės juos atkurti; pakeisti prisijungimo prie duomenų bazės ar informacinės sistemos vardus ir slaptažodžius, jeigu jie tapo žinomi tretiesiems asmenims; atkuriant prarastus ar sugadintus asmens duomenis, naudoti atsargines kopijas ir kt.

19. Siekiant apriboti ar sustabdyti asmens duomenų saugumo pažeidimą, būtina kiek įmanoma tiksliau surinkti duomenis ir įrodymus apie įvykusį saugumo incidentą (pvz., kas, kada ir

iš kokio įrenginio jungësi prie duomenų bazës ar informacinës sistemos, kam per klaidą išsiusti asmens duomenys, kokiomis aplinkybëmis buvo prarastas įrenginys su asmens duomenimis ir kt.).

20. Priemonių plane turi būti numatytos prevencinës ir kitos priemonës, užtikrinančios, kad pažeidimas nepasikartotų.

IV SKYRIUS

PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

21. Tyrimo metu nustačius, kad asmens duomenų saugumo pažeidimas buvo, progimnazijos vadovas nedelsdamas ir, jei jmanoma, praëjus ne daugiau kaip 72 valandoms nuo tada, kai tapo žinoma apie pažeidimą, apie tai informuoja VDAI, išskyrus atvejus, kai saugumo pažeidimas nekelia pavojaus fizinių asmenų teisëms ir laisvëms.

22. VDAI informuojama Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto VDAI direktoriaus 2018 m. liepos 27 d. įsakymu Nr. 1T-72(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“, nustatyta tvarka ir sąlygomis, užpildant Pranešimo apie asmens duomenų saugumo pažeidimo formą, patvirtintą VDAI direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“ (toliau – pranešimas).

23. Jeigu įvertinus riziką abejojama, ar asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisëms ir laisvëms, apie pažeidimą pranešama VDAI.

24. Jeigu įvertinus riziką nustatoma, kad apie saugumo pažeidimą VDAI pranešti nereikia, tačiau po kurio laiko situacija pasikeičia, saugumo pažeidimas bei jo keliamas pavojus fizinių asmenų teisëms ir laisvëms turi būti vertinamas iš naujo ir, jeigu reikia, pranešama VDAI (pvz., pamesta USB atmintinė, kurioje saugomi užšifruoti asmens duomenys taikant pažangų algoritmą. Jeigu yra atsarginës duomenų kopijos ir nera pavojaus šifro saugumui, apie tokį saugumo pažeidimą pranešti VDAI nereikia, tačiau jei vëliau paaiškëja, kad gali kilti pavojus šifro saugumui, pažeidimo keliamas pavojus turi būti vertinamas iš naujo ir apie tokį pažeidimą reikia pranešti VDAI).

25. Tuo atveju, kai pagal pažeidimo pobûdį bûtina atlkti išsamesnį tyrimą, tačiau per 72 valandas dël objektyvių priežasčių ištirti padarytą pažeidimą nera jmanoma, informacija VDAI teikiama etapais, nurodant vélavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminj pranešimą.

26. Jeigu pateikus VDAI pranešimą ir atlikus tolesnį tyrimą yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo asmens duomenų saugumo pažeidimo, apie tai nedelsiant informuojama VDAI.

27. Tuo atveju, kai yra įtariama, kad asmens duomenų saugumo pažeidimas turi nusikalstamas veikos požymį, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybės institucijoms, įgaliotomis atliliki ikiteisminį tyrimą.

V SKYRIUS

PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

28. Tyrimo metu nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, progimnazijos vadovas, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo to laiko, kai buvo sužinota apie pažeidimą, praneša apie tai duomenų subjektui, kurio teisėms ir laisvėms gali kilti didelis pavojus.

29. Duomenų subjektas informuojamas tiesiogiai, t. y. siunčiant jam pranešimą paštu, elektroniniu paštu, trumpajai žinute (SMS) ar kitu būdu. Pranešimas duomenų subjektui siunčiamas atskirai nuo kitos siunčiamos informacijos, tokios kaip naujienlaiškiai ar standartiniai pranešimai.

30. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jis turėtų imtis, kad apsaugotų nuo neigiamų pažeidimo pasekmisi. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama ši informacija:

30.1. asmens duomenų saugumo pažeidimo pobūdžio ir tiketinų pažeidimo pasekmisi aprašymas;

30.2. priemonių, kurių ēmési progimnazija, kad būtų pašalintas saugumo pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti aprašymas;

30.3. Progimnazijos vadovo arba kito kontaktinio asmens, galinčio sutekti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

30.4. kita reikšminga informacija, susijusi su pažeidimu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsaugoti nuo galimų neigiamų pažeidimo pasekmisi.

31. Pranešimo apie asmens duomenų saugumo pažeidimą duomenų subjektams teikti nereikia, jeigu:

31.1. Progimnazija įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikyto asmens duomenims, kuriems pažeidimas turėjo poveikio, visų pirmą tąs priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su duomenimis, jie būtų nesuprantami (pvz., asmens duomenų šifravimo priemonės);

31.2. iš karto po pažeidimo progimnazija ēmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojuς duomenų subjektų teisėms ir laisvėms;

32. Jeigu įvertinus riziką nustatoma, kad apie saugumo pažeidimą duomenų subjektui pranešti nereikia, tačiau po kurio laiko situacija pasikeitė, todėl pažeidimas bei jo keliamas pavojuς fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdama kibernetinė ataka, naudojant išpirkos reikalaujančią programą, – duomenų bazėje esantys asmens duomenys užšifruojami). Jei atlikus tyrimą paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenis ir jokio kito kenksmingo poveikio duomenų bazei nėra, apie saugumo pažeidimą reikės pranešti tik VDAI, tačiau jei vėliau paaiškėja, kad prarastas ne tik duomenų prieinamumas, bet ir konfidencialumas, saugumo pažeidimo keliamas pavojuς bus vertinamas iš naujo bei sprendžiama, ar atsižvelgiant į tiketinas saugumo pažeidimo pasekmes reikia apie jį pranešti duomenų subjektams).

33. Progimnazija, atsižvelgdama į esamas pagrįstas aplinkybes ir teisėtus teisėsaugos institucijų reikalavimus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą iki to laiko, kol tai netrukdytys saugumo pažeidimo tyrimui.

VI SKYRIUS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

34. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale (Apaščio 3 priedas).

35. Informacija apie pažeidimą registruojama nedelsiant, kai tik nustatomas pažeidimo faktas ir įvertinama rizika, bet ne vėliau kaip per 5 darbo dienas.

36. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

36.1. pažeidimo nustatymo aplinkybės (pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);

36.2. pažeidimo aplinkybės (pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

36.3. tiketinos pažeidimo pasekmės ir pavojuς duomenų subjekto teisėms ir laisvėms;

36.4. priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, išskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;

36.5. informacija apie pranešimą ar nepranešimą VDAI;

36.5.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta VDAI, nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta VDAI, nurodoma pranešimo data ir numeris, taip pat, ar pranešimas teikiamas etapais;

36.5.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti VDAI, nurodomos tokio vėlavimo priežastys:

36.6. informacija apie pranešimą ar nepranešimą duomenų subjektui (subjektams):

36.6.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);

36.6.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodomos tokio vėlavimo priežastys;

36.7. kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

37. Asmens duomenų saugumo pažeidimų registravimo žurnalas yra tvarkomas ir saugomas pagal patvirtintą progimnazijos dokumentacijos planą.

38. Už Asmens duomenų saugumo pažeidimų registravimo žurnalo tvarkymą ir saugojimą atsakingas progimnazijos vadovas.

VII SKYRIUS

BAIGIAMOSIOS NUOSTATOS

39. Progimnazijos darbuotojai su šiuo Aprašu bei jo pakeitimais supažindinami dokumentų valdymo sistemos priemonėmis; darbuotojai, kurie neturi prieigos prie dokumentų valdymo sistemos, su Aprašu supažindinami pasirašytinai.

40. Progimnazijos darbuotojai, pažeidę šio Aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
I priedas

VILNIAUS SOFIJOS KOVALEVSKAJOS PROGIMNAZIJA

(pareigų pavadinimas)

(vardas, pavardė)

**PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

Nr.
(data, dokumento numeris)

Vilnius

Informuoju apie asmens duomenų saugumo pažeidimą, pateikdamas turimą informaciją:

1. Asmens duomenų saugumo pažeidimo nustatymo data, laikas ir vieta:

2. Asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta:

3. Asmens duomenų saugumo pažeidimo esmė ir aplinkybės:

4. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (pvz., įstaigos darbuotojai, asmenys, pateikę prašymus, skundus ir kt.) ir apytikslis jų skaičius (jei žinoma):

5. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us)):

- Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.)
- Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.)
- Asmens kontaktiniai duomenys (gyvenamosios vienos adresas, telefono numeris, elektroninio pašto adresas ir kt.)
- Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniiais, filosofiniaijs įsitikinimais ar naryste profesinėse sajungose, duomenys susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.)
- Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas
- Kiti asmens duomenys (jrašyti):

6. Aptykslis asmens duomenų, kurių saugumas pažeistas, skaičius:

7. Kokį veiksmų (priemonių) buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti prisijungimo prie informaciniés sistemos slaptažodžiai, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimui skirtoje vietoje palikti dokumentai su asmens duomenimis ir kt.):

(pareigos)

(parašas)

(vardas ir pavardė)

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
2 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO ATASKAITA

Nr.

(data, dokumento numeris)

1. Asmens duomenų saugumo pažeidimo aprašymas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:

Asmens duomenų saugumo pažeidimo data _____, laikas _____.

Asmens duomenų saugumo pažeidimo nustatymo data _____, laikas _____.

1.2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us)):

- Informacinė sistema
- Duomenų bazė
- Tarnybinė stotis
- Interneto svetainė
- Debesų kompiuterijos paslaugos
- Nešiojami / mobilūs įrenginiai
- Neautomatiniu būdu susistemintos bylos (archyvas)
- Kita (jrašyti):

1.3. Asmens duomenų saugumo pažeidimo pobūdis (pažymėti tinkamą (-us)):

- Konfidencialumo pažeidimas (neautorizuota prieiga ar atskleidimas)
- Vientisumo pažeidimas (neautorizuotas asmens duomenų pakaitimas)
- Prieinamumo pažeidimas (asmens duomenų praradimas, sunaikinimas)

1.4. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us) ir aprašyti):

- Asmens tapatybę patvirtinančios duomenys (vardas, pavardė, gimimo data, lytis ir kt.):

- Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.):

Asmens kontaktiniai duomenys (gyvenamosios vietas adresas, telefono numeris, elektroninio pašto adresas ir kt.):

Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniai, filosofiniai įsitikinimais ar naryste profesinėse sajungose, duomenys susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.):

Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

Kiti asmens duomenys:

1.5. Aptykslis asmens duomenų, kurių saugumas pažeistas, skaičius:

1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (Įstaigos darbuotojai, asmenys, pateikę prašymus, skundus ir kt.):

1.7. Aptykslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:

1.8. Darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, įstaigos struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas, telefono numeris, elektroninio pašto adresas):

1.9. Duomenų tvarkytojas, pranešęs apie asmens duomenų saugumo pažeidimą (pavadinimas, kontaktinio asmens duomenys (vardas, pavardė, telefono numeris, elektroninio pašto adresas):

2. Asmens duomenų saugumo pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms įvertinimas

2.1. Specifiniai fizinių asmenų, kurių asmens duomenų saugumas buvo pažeistas, ypatumai (vaikai, asmenys su negalia ir kt.):

2.2. Galimybė identifikuoti fizinių asmenų (pvz., iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užšifruoti, anonimizuoti, arba iki saugumo pažeidimo asmens duomenims šifravimas nebuvo taikomas ir kt.):

2.3. Kas gavo prieigą prie asmens duomenų, kurių saugumas pažeistas?

2.4. Ar buvo kokių kitų įvykių ar aplinkybių, turėjusių poveikį asmens duomenų saugumo pažeidimo padarymui?

2.5. Kokia žala padaryta fiziniam asmenim (duomenų subjektams)?

2.6. Galimos asmens duomenų saugumo pažeidimo pasekmės:

2.6.1. Konfidentialumo pažeidimo atveju (pažymėti tinkamą (-us):

Asmens duomenų išplėtimas ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pvz., asmenys duomenys išplito internete)

Skirtingos informacijos susiejimas (pvz., gyvenamosios vienos adreso susiejimas su asmenys buvimo vieta realiu laiku)

Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pvz., komerciniai tikslai, asmenys tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)

Kita:

2.6.2. Vientisumo pažeidimo atveju (pažymėti tinkamą (-us)):

- Paketimas į neteisingus duomenis, dėl ko asmuo gali netekti galimybės naudotis paslaugomis
- Paketimas į kitus duomenis, kad asmens duomenų tvarkymas būtų nukreiptas tam tikra linkme (pvz., pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)
- Kita:

2.6.3. Prieinamumo pažeidimo atveju (pažymėti tinkamą (-us)):

- Dėl asmens duomenų trūkumo negalima teikti paslaugų (pvz., administracinių procesų sutrikdymas, dėl ko negalima prieiti prie tvarkomų asmens duomenų ir įgyvendinti duomenų subjekto teisę susipažinti su jo tvarkomais asmens duomenimis)
- Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pvz., tam tikra informacija iš informacinės sistemos išnyko, dėl ko negalima tinkamai suteikti administracinių paslaugos)
- Kita:

2.7. Asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis:

- Žema rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms)
- Vidutinė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra / gali kilti pavojuς fizinių asmenų teisėms ir laisvėms)
- Didelė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra / gali kilti didelis pavojuς fizinių asmenų teisėms ir laisvėms)

2.8. Kokių veiksmų / priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?

2.9. Kokios taikytos priemonės, siekiant sumažinti neigiamą poveikį duomenų subjektams?

2.10. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?

2.11. Techninės ir / ar organizacinės saugumo priemonės, kurios įgyvendintos dėl asmens duomenų saugumo pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų:

2.12. Techninės ir / ar organizacinės saugumo priemonės, kurios ketinamos įgyvendinti dėl asmens duomenų saugumo pažeidimo, išskaitant ir priemones sumažinti asmens duomenų saugumo pažeidimo pasiekmes:

3. Pranešimų apie asmens duomenų saugumo pažeidimą pateikimas

3.1. Ar pranešta Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) apie asmens duomenų saugumo pažeidimą?

Taip

Pranešimo VDAI data _____ numeris _____

Ne (nurodomos nepranešimo VDAI priežastys):

Apie duomenų saugumo pažeidimą pranešta VDAI vėliau nei per 72 valandas (nurodomos vėlavimo pranešti VDAI priežastys):

3.2. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą?

Taip

Pranešimo duomenų subjektui data _____ numeris _____ (jeigu pranešimas užregistruotas)

Pranešimo duomenų subjektui būdas (pažymėti tinkamą (-us)):

paštu elektroniniu paštu trumpaja žinute (SMS) kitais būdais

Informuotų duomenų subjektų skaičius:

Pranešimo duomenų subjektui turinys:

Ne (nurodomos nepranešimo duomenų subjektui priežastys):

Apie duomenų saugumo pažeidimą duomenų subjektams pranešta vėliau nei per 72 valandas (nurodomos vėlavimo pranešti duomenų subjektui priežastys):

Apie saugumo pažeidimą pranešta viešai (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta):

3.3. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymiu (jeigu taip, nurodoma rašto data ir numeris):

Asmens Vadovas:

(parašas)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Asmens duomenų saugumo pažėdinių
valdymo tvarkos aprašo
3 priedas

