PATVIRTINTA
Kelmės krašto muziejaus direktoriaus
2020 m. liepos 30 d. įsakymu Nr. V-20

REAGAVIMO Į ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Reagavimo į asmens duomenų saugumo pažeidimus procedūros aprašas (toliau – Aprašas) nustato biudžetinės įstaigos, Kelmės krašto muziejaus, įstaigos kodas 288208070, registracijos adresas Dvaro g. 15, LT-86111 Kelmė (toliau – Įstaiga) darbuotojų, dirbančių pagal darbo sutartis, veiksmus, įvykus duomenų saugumo pažeidimui, jų išaiškinimo, pranešimo priežiūros institucijai, duomenų subjektams tvarką, pažeidimo prevencinio plano sudarymo bei kitus atvejus, įgyvendinant 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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 – BDAR) 33 ir 34 straipsnių reikalavimus.

2. Aprašu privalo vadovautis:

2.1. Įstaigos darbuotojai, dirbantys pagal darbo ar kitas sutartis (toliau – darbuotojai);

3. Apraše vartojamos sąvokos:

3.1. **duomenų saugumo pažeidimas** – bet koks įvykis, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga;

3.2. **priežiūros institucija** – valstybės narės pagal BDAR 51 straipsnį įsteigta nepriklausoma valdžios institucija. Įstaigos atžvilgiu tai Valstybinė duomenų apsaugos inspekcija (įmonės kodas 188607912, A. Juozapavičiaus g. 6, 09310 Vilnius, el. paštas ada@ada.lt);

3.3. kitos Apraše vartojamos sąvokos atitinka BDAR įtvirtintas sąvokas.

II SKYRIUS
I ETAPAS: DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMAS IR ANALIZĖ

4. Duomenų saugumo pažeidimu (toliau – Pažeidimas) laikomas bet koks saugumo incidentas, dėl kurio įvyksta vienas arba keli toliau numatyti pažeidimai:

4.1. konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama (gaunama) prieiga tam teisės neturintiems asmenims, pavyzdžiui, duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio paviešinimas, praradimas, atskleidimas kitam darbuotojui, nešiojamojo kompiuterio, kuriame sukaupti duomenys, praradimas, popierinių dokumentų praradimas, vagystė ir pan.;

4.2. pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami. Tokio pobūdžio pažeidimu galėtų būti laikomas

duomenų bazės ištrynimas, praradimas (vagystė), sunaikinimas, pavyzdžiui, gaisro, liūties atveju ir nesant atsarginės kopijos, iš kurios būtų galima atkurti prarastus duomenis. Pasiekiamumo pažeidimu laikytinas ir įprastinę Įstaigos veiklą sutrikdęs prieigos prie duomenų praradimas;

4.3. vientisumo pažeidimas – netyčia ar neteisėtai atlikti asmens duomenų pakeitimai. Tai galėtų būti trečiojo asmens, įgijusio neteisėtą prisijungimą prie duomenų bazės, įvykdyti joje esančių įrašų pakeitimai, taip pat programinės įrangos ar kitokie procedūrų sutrikimai, dėl kurių atsiranda duomenų netikslumų arba pasikeitimų.

5. Kai yra nustatomas arba įtariamas Pažeidimas, atitinkantis Aprašo 4 punkto reikalavimus, jį nustatęs darbuotojas asmeniškai el. paštu, telefonu ir (arba) kitomis komunikacijos priemonėmis turi kuo skubiau informuoti savo tiesioginį vadovą ir Įstaigos duomenų apsaugos pareigūną (toliau – pareigūnas).

6. Darbuotojas Įstaigos direktoriui ir pareigūnui pateikia jam žinomą Pažeidimo nustatymui būtiną informaciją:

6.1. poveikio informacinių technologijų (toliau – IT) infrastruktūrai mastą;

6.2. informacinius išteklius, kuriems gali kilti arba yra kilęs pavojus (kokios duomenų bazės yra arba gali būti paveiktos);

6.3. žinomą arba tikėtiną Pažeidimo trukmę (kada įvyko ir kada buvo sustabdytas arba kada, tikėtina, galima būtų tai padaryti);

6.4. paveiktus arba galimai paveiktus duomenų subjektus ir poveikio jiems mastą (ar paveikti tik konkrečios duomenų subjektų grupės duomenys, kokia konkrečios grupės dalis yra paveikta ir pan.);

6.5. pradinius Pažeidimo pasekmių požymius (pavyzdžiui, prieigos prie duomenų praradimas, nustatyti neteisėti duomenų pakeitimai, rasti paviešinti duomenys ir pan.).

7. Nustatant Pažeidimą ir vykdant jo analizę darbuotojai Pažeidimo tyrimo komisijai arba pareigūnui privalo teikti visapusišką, išsamią, tikslią ir operatyvią informaciją dėl galimo Pažeidimo.

8. Nustačius Pažeidimą, atliekamas pirminis įvykusio galimo Pažeidimo vertinimas ir nustatoma, ar egzistuoja šios aplinkybės:

8.1. prarastas arba gali būti prarastas reikšmingas kiekis asmens duomenų, ypač kai Pažeidimas susijęs su specialių kategorijų duomenimis arba jautresniais duomenimis, pavyzdžiui, sveikatos duomenimis, religiniais, filosofiniais įsitikinimais, naryste profesinėse sąjungose, lytine orientacija, asmenų teistumu, finansine informacija ir pan. Nereikšmingu kiekiu gali būti laikomas vienkartinis, atsitiktinis duomenų praradimas, pavyzdžiui, elektroninio laiško išsiuntimas ne tam adresatui, popieriaus lapo, bylos praradimas (pametimas);

8.2. Pažeidimas tikėtinai gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms;

8.3. daromas poveikis dideliam duomenų subjektų skaičiui, ypač kai poveikis daromas labiau pažeidžiamiems duomenų subjektams, pavyzdžiui, vaikams;

8.4. susiklostė bet kokia kita situacija, kuri gali sukelti reikšmingą poveikį duomenų subjektams ir (arba) Įstaigai.

9. Jeigu nustatoma, kad turimais duomenimis Pažeidimas atitinka Aprašo 4 ir 8 punktų kriterijus, pradedama reagavimo į asmens duomenų saugumo pažeidimus procedūra ir Įstaigos direktoriaus įsakymu sudaroma Pažeidimo tyrimo komisija (toliau – Komisija).

10. Komisiją sudaro pareigūnas ir kiti darbuotojai, atsakingi už Pažeidimą arba turintys informacijos apie įvykusį Pažeidimą ir (ar) galintys padėti jį sustabdyti, taip pat kiti Pažeidimui svarbūs asmenys. Paprastai Komisija sudaroma iš Įstaigos direktoriaus arba jo įgaliojo asmens, pareigūno.

11. Jeigu Pažeidimas neatitinka Aprašo 4 ir (ar) 8 punkto reikalavimų, Komisija nesudaroma ir vykdoma supaprastinta reagavimo į asmens duomenų saugumo pažeidimus procedūra (toliau – Supaprastinta procedūra). Vykdant Supaprastintą procedūrą visus Pažeidimo išaiškinimo, apribojimo ir kitus būtinus atlikti veiksmus koordinuoja pareigūnas. Atlikus visus būtinus veiksmus Supaprastinta procedūra dokumentuojama ir užpildžius Biudžetinės įstaigos, Kelmės krašto muziejus, įstaigos kodas 288208070, asmens duomenų saugumo pažeidimų žurnalą (toliau – Žurnalas), kurio forma nustatyta Aprašo 1 priede, užbaigiama.

12. Vykdant Supaprastintą procedūrą ir nustačius, kad įvykęs Pažeidimas atitinka Aprašo 4 ir 8 punktų kriterijus, pareigūnas teikia siūlymą Įstaigos direktoriui Pažeidimo tyrimui sudaryti Komisiją.

13. Visa gauta, renkama informacija fiksuojama tokiu būdu, kad atliekant vėlesnę peržiūrą būtų galima nustatyti aiškią chronologinę veiksmų seką ir situacijos eigą bei priemones, kurių buvo imtasi.

III SKYRIUS

II ETAPAS: DUOMENŲ SAUGUMO PAŽEIDIMO APRIBOJIMAS, LIKVIDAVIMAS IR ATKŪRIMAS

14. Nustačius, kad įvyko Pažeidimas pirmiausia būtina imtis priemonių, kad Pažeidimas būtų kuo skubiau apribotas (sustabdytas, nutrauktas, pašalintas). Konkretūs veiksmai Pažeidimui apriboti atliekami įvertinus konkretaus Pažeidimo aplinkybes, mastą, specifiką ir pan. Siekiant Pažeidimą apriboti, gali būti imamasi šių priemonių:

14.1. duomenų ištrynimas nuotoliniu būdu iš pamesto, pavogto ar kitaip prarasto įrenginio;

14.2. duomenų užšifravimas nuotoliniu būdu pamestame, pavogtame ar kitaip prarastame įrenginyje;

14.3. skubus kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti ar kitaip atskleisti duomenys, su prašymu neatidaryti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;

14.4. atskleisto tretiesiems asmenims prisijungimo prie duomenų bazės slaptažodžio pakeitimas;

14.5. prarastų duomenų atkūrimas iš turimos atsarginės kopijos.

15. Šiame etape būtina imtis atsargumo priemonių siekiant užtikrinti, kad būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį Pažeidimą (pavyzdžiui, užfiksuojama, kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės, kam konkrečiai buvo per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su duomenimis).

16. Veiksmai, skirti ištaisyti arba sumažinti žalą duomenų subjektui, sukeltą Pažeidimo, turėtų būti nukreipti ne vien į esamo Pažeidimo priežasties pašalinimą, bet ir siekiant neleisti Pažeidimui pasikartoti. Turėtų būti nustatytos bent vykdomų procesų, naudojamų sistemų pažeidimo priežastys, dėl kurių ir toliau gali įvykti Pažeidimų arba kurios savaime sudaro prielaidas įvykti Pažeidimui.

17. Esant būtinybei, Įstaiga gali informuoti visuomenę apie Pažeidimo tyrimą, jo rezultatus, priemones, kurių imamasi Pažeidimui apriboti ir pan. Visuomenės informavimą vykdo viešųjų ryšių specialistas, suderinęs poziciją su pareigūnu ir (ar) kitais Komisijos nariais.

18. Atkūrimo stadijoje sistemos turėtų būti pagal galimybes atkurtos į ankstesnę būklę, siekiant užtikrinti Įstaigos veiklos tęstinumą.

IV SKYRIUS
III ETAPAS: DUOMENŲ VALDYTOJO PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

19. Įstaiga, kaip duomenų valdytoja, nedelsdama privalo informuoti Valstybinę duomenų apsaugos inspekciją (toliau – VDAI), jeigu Komisija arba pareigūnas nustato, kad Pažeidimas kelia arba tikėtinai gali kelti pavojų duomenų subjektų, paveiktų Pažeidimo, teisėms ir laisvėms. Pavojų keliančiu laikytinas toks Pažeidimas, dėl kurio, laiku nesiėmus tinkamų priemonių, duomenų subjektas galėtų patirti kūno sužalojimą, materialinę ar nematerialinę žalą, teisių apribojimą, diskriminaciją, galėtų būti pavogta ar suklastota asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta jo reputacijai, prarastas asmens duomenų, kurie laikomi profesine paslaptimi, konfidencialumas arba padaryta kita turtinė, neturtinė ar socialinė žala.

20. Vertinant pavojų duomenų subjektui atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Pavojus turėtų būti vertinamas remiantis objektyviai ir atsižvelgiant į šiuos kriterijus:

20.1. Pažeidimo tipą;

20.2. asmens duomenų kategorijas (pavyzdžiui, specialių kategorijų asmens duomenys, duomenys apie apkaltinamuosius nuosprendžius, jautresni duomenys, finansiniai duomenys);

20.3. kaip lengvai gali būti identifikuojamas duomenų subjektas;

20.4. pasekmių rimtumą duomenų subjektams;

20.5. specialias duomenų subjekto savybes (pavyzdžiui, duomenys, susiję su vaikais ar kitais pažeidžiamais asmenimis);

20.6. paveiktų duomenų subjektų skaičių;

20.7. specialias duomenų valdytojo savybes (pavyzdžiui, veiklos pobūdį).

21. Įvertinus riziką duomenų subjekto teisėms ir laisvėms nustatomos šios rizikos rūšys:

21.1. nėra rizikos;

21.2. maža;

21.3. vidutinė;

21.4. didelė.

22. Išvadą dėl Pažeidimo buvimo ir rizikos fizinių asmenų teisėms ir laisvėms egzistavimo Komisija arba pareigūnas pateikia Įstaigos direktoriui (ar jo įgaliotam asmeniui), kuris sprendžia dėl tolesnių veiksmų. Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie Pažeidimą VDAI, rekomenduotina pranešti. Pranešimo priežiūros institucijai forma nustatyta Aprašo 2 priede.

23. Jei Pažeidimas kelia pavojų (riziką) duomenų subjektų teisėms ir laisvėms, pareigūnas ne vėliau kaip per 72 valandas nuo Įstaigos sužinojimo (nustatymo) apie Pažeidimą momento VDAI pateikia tokią informaciją:

23.1. Pažeidimo pobūdį, įskaitant, jeigu įmanoma, atitinkamai paveiktų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;

23.2. tikėtinų Pažeidimo pasekmių aprašymą;

23.3. priemones, kurių ėmėsi arba planuoja imtis Įstaiga tam, kad būtų pašalintas Pažeidimas;

23.4. priemones galimoms neigiamoms Pažeidimo pasekmėms duomenų subjektui sumažinti;

23.5. informaciją, ar apie įvykusį Pažeidimą pranešta duomenų subjektams;

23.6. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis.

24. Jeigu visos informacijos VDAI neįmanoma pateikti vienu metu arba aiškinamasi Pažeidimo priežastis, tolesnė informacija nepagrįstai nedelsiant gali būti teikiama etapais. Apie tai, kad informacija bus teikiama etapais, VDAI informuojama pirminiame pranešime.

25. Jeigu po pranešimo VDAI pateikimo atlikus tolesnį tyrimą yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo jokio Pažeidimo, apie tai nedelsiant informuojama VDAI ir tai pažymima Žurnale.

26. Jeigu Pažeidimas paveikia arba gali paveikti duomenų subjektų duomenis daugiau negu vienoje valstybėje narėje ir yra reikalinga pranešti priežiūros institucijai, Įstaiga turėtų pranešti vadovaujančiai priežiūros institucijai (BDAR preambulės 55 punktas). Jeigu abejojama, kuri priežiūros institucija yra vadovaujanti, bet Pažeidimas įvyko Lietuvos Respublikoje, tuomet pranešama VDAI. Šiuo atveju, teikiant pranešimą, rekomenduotina nurodyti, ar toks Pažeidimas apima ir kitose valstybėse narėse esančias duomenų valdytojo buveines ir kuriose valstybėse narėse esančius duomenų subjektus Pažeidimas galėjo paveikti.

V SKYRIUS
IV ETAPAS: DUOMENŲ VALDYTOJO PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

27. Kai nustatoma, kad įvyko Pažeidimas, atitinkantis Aprašo 4 ir 8 punktų reikalavimus, ir dėl jo gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, Įstaiga nepagrįstai nedelsdama, bet ne vėliau kaip per 72 valandas nuo Pažeidimo paaiškėjimo momento informuoja duomenų subjektus, kurių teisėms ir laisvėms gali kilti didelis pavojus.

28. Didelį pavojų keliančiu gali būti laikomas bet kuris 19 punkte nurodytų pasekmių riziką keliantis Pažeidimas tada, jei tokios Pažeidimo pasekmės yra labai tikėtinos, tvarkomi jautrūs asmens duomenys (pavyzdžiui, duomenys apie sveikatą), Pažeidimas turi neigiamą poveikį dideliam duomenų subjektų skaičiui ir pan.

29. Įstaiga, informuodama duomenų subjektus, teikia pranešimą, kurio forma nustatyta Aprašo 3 priede, ir aiškia, paprasta kalba aprašo Pažeidimo pobūdį bei pateikia bent jau toliau nurodytą informaciją:

29.1. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis arba pareigūno kontaktus;

29.2. Pažeidimo aprašymą;

29.3. tikėtinų Pažeidimo pasekmių duomenų subjektui aprašymą;

29.4. priemones, kurių ėmėsi arba planuoja imtis Įstaiga tam, kad būtų pašalintas Pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti;

29.5. kitą reikšmingą informaciją, susijusią su Pažeidimu, kuri gali būti reikšminga duomenų subjektui.

30. Pranešimas duomenų subjektui neprivalomas, jei egzistuoja bet kuri iš šių aplinkybių:

30.1. Įstaiga įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikį, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės;

30.2. Įstaiga, įvykus Pažeidimui, ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

30.3. pranešimas duomenų subjektams apie įvykusi Pažeidimą pareikalautų neproporcingai didelių pastangų. Tokiu atveju apie Pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

31. Gavusi priežiūros institucijos reikalavimą informuoti duomenų subjektus apie Pažeidimą, Įstaiga nedelsdama jį vykdo.

VI SKYRIUS
PRANEŠIMAS DUOMENŲ VALDYTOJUI NUO DUOMENŲ TVARKYTOJO

32. Jeigu Įstaiga duomenis tvarko kaip duomenų tvarkytoja, o ne valdytoja, tuomet Įstaiga laikosi visų Aprašo II ir III skyriuose nustatytų reikalavimų ir, jeigu sutartyje su duomenų valdytoju nenumatyta kitaip, informuoja duomenų valdytoją apie įvykusį Pažeidimą.

33. Informuojant duomenų valdytoją apie Pažeidimą pateikiama visa Aprašo 23 punkte nurodyta informacija. Duomenų valdytojui reikalaujant, teikiama visa kita su Pažeidimo tyrimu susijusi informacija, galinti padėti duomenų valdytojui įgyvendinti pareigą pranešti priežiūros institucijai ir (ar) duomenų subjektams.

34. Duomenų valdytojo prašymu Įstaigos darbuotojai privalo bendradarbiauti, teikti visą reikiamą informaciją ir vykdyti visus duomenų valdytojo teikiamus nurodymus duomenų tvarkymo sutartyje nustatyta tvarka.

VII SKYRIUS
V ETAPAS: DUOMENŲ SAUGUMO PAŽEIDIMO DOKUMENTAVIMAS IR PROCEDŪROS UŽBAIGIMAS

35. Kai Pažeidimas laikytinas pašalintu, o visiems reikiamiems asmenims apie Pažeidimą yra pranešta arba nustatyta ir dokumentuota, kodėl ši pareiga Įstaigai netaikoma, Komisijos įgaliotas asmuo arba pareigūnas sudaro prevencinių veiksmų planą, kuriuo būtų siekiama ateityje užkirsti kelią analogiškam ar panašiam Pažeidimui įvykti, ir jis pateikiamas Įstaigos direktoriui spręsti dėl jo įgyvendinimo.

36. Sudarius ir Įstaigos direktoriui patvirtinus prevencinių veiksmų planą, taip pat Pažeidimą užfiksavus Žurnale, Procedūra laikoma baigta.

37. Procedūros dokumentai turi būti saugomi teisės aktų nustatyta tvarka.

38. Reagavimo į duomenų saugumo pažeidimus procedūros schema nustatyta 4 priede.

VIII SKYRIUS
ATSAKOMYBĖ

39. Visi darbuotojai privalo būti supažindinti ir vadovautis Aprašu Pažeidimo atveju.

40. Aprašo 19, 25, 27, 29 ir 32 punktuose nurodytą Įstaigos pareigą informuoti VDAI, duomenų subjektus arba duomenų valdytojus įgyvendina pareigūnas arba kitas Komisijos įgaliotas asmuo.

41. Asmenys, nesilaikantys arba pažeidę Aprašo reikalavimus, atsako teisės aktų nustatyta tvarka.