KULTŪROS PAVELDO DEPARTAMENTO PRIE KULTŪROS MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ KULTŪROS PAVELDO DEPARTAMENTE PRIE KULTŪROS MINISTERIJOS VALDYMO TVARKOS APRAŠO PATVIRTINIMO

2021 m. d. Nr.
Vilnius

Vadovaudamasis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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) (OL 2016 L 119, p. 1) 24 straipsnio 1 dalimi:

1. T v i r t i n u Asmens duomenų saugumo pažeidimų Kultūros paveldo departamente prie Kultūros ministerijos valdymo tvarkos aprašą (pridedama).

2. P a v e d u :

2.1. Kultūros paveldo departamento prie Kultūros ministerijos (toliau – Departamentas) Teisės ir personalo skyriaus patarėjui per Departamento dokumentų valdymo sistemą organizuoti Departamento valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, supažindinimą su šiuo įsakymu;

2.2. Departamento Išteklių valdymo ir viešųjų pirkimų skyriaus vedėjui ne vėliau kaip per 3 darbo dienas po šio įsakymo įsigaliojimo dienos užtikrinti jo paskelbimą Departamento interneto svetainėje.

Direktorius Vidmantas Bezaras

PATVIRTINTA
Kultūros paveldo departamento prie
Kultūros ministerijos direktoriaus
2021 m. d.
įsakymu Nr.

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ KULTŪROS PAVELDO DEPARTAMENTE PRIE KULTŪROS MINISTERIJOS VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų Kultūros paveldo departamente prie Kultūros ministerijos valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pašalinimo ir pranešimo apie juos Kultūros paveldo departamente prie Kultūros ministerijos (toliau – Departamentas) 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) (OL 2016 L 119, p. 1) (toliau – Reglamentas (ES) 2016/679).

3. Apraše vartojamos sąvokos:

3.1. **asmens duomenų saugumo pažeidimas** (toliau – 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;

3.2. **darbuotojas –** Departamento valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį;

3.3. **atsakingas asmuo** – Departamento direktoriaus paskirtas darbuotojas, atliekantis konkretaus pažeidimo tyrimą, pranešantis apie pažeidimą Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) ir asmens duomenų subjektams.

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

5. Aprašas taikomas duomenų valdytojui – Departamentui, tvarkančiam asmens duomenis, ir Departamento pasitelktiems juridiniams ir fiziniams asmenims, tvarkantiems asmens duomenis Departamento vardu ir pagal jo nurodymus (toliau – duomenų tvarkytojai), kuriems pagal Reglamento (ES) 2016/679 33 straipsnio 2 dalį yra nustatyta prievolė pranešti Departamentui apie pažeidimą.

II SKYRIUS
PAŽEIDIMŲ, JŲ PRIEŽASČIŲ, KELIAMŲ RIZIKŲ KLASIFIKAVIMAS

6. Asmens duomenų saugumo pažeidimai pagal pobūdį (tipą) yra:

6.1. konfidencialumo pažeidimas – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

6.2. vientisumo pažeidimas – asmens duomenų pakeitimas be leidimo ar netyčia;

6.3. prieinamumo pažeidimas – netyčinis arba neteisėtas prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas;

6.4. mišraus pobūdžio pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių Aprašo 6.1–6.3 papunkčiuose nurodytų pažeidimų derinys.

7. Pažeidimai gali būti nulemti šių priežasčių:

7.1. netyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas neturint tikslo tai padaryti (dėl duomenų tvarkymo klaidos, informacijos laikmenų, duomenų įrašų ištrynimo, sunaikinimo ar sistemų sutrikimų dėl elektros tiekimo nutrūkimo, įvykusio dėl asmens veiklos, kompiuterinio viruso, paskleisto dėl asmens veiklos, vidaus taisyklių pažeidimo, sistemos priežiūros

trūkumo, programinės įrangos testų atlikimo, netinkamos duomenų laikmenų priežiūros, netinkamo ryšio linijų pajėgumo ir apsaugos nustatymo, kompiuterių integravimo į tinklą, netinkamos kompiuterinių programų apsaugos parinkimo, asmens duomenų persiuntimo ne tam adresatui, ne saugojimui skirtoje vietoje paliktų dokumentų, pamestų nešiojamų įrenginių (telefono, nešiojamo kompiuterio, išorinės duomenų laikmenos) ir kt.);

7.2. tyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas sąmoningai turint tikslą tai padaryti (kibernetinė ataka, vagystė, neteisėtas įsibrovimas į asmens duomenų tvarkytojo patalpas, asmens duomenų laikmenų saugyklas, informacines sistemas, kompiuterių tinklą, tyčinis nustatytų taisyklių tvarkant asmens duomenis pažeidimas, sąmoningas kompiuterinio viruso platinimas, neteisėtas naudojimasis kito darbuotojo teisėmis ir kt.);

7.3. force majeure ir kiti netikėti įvykiai, kurių negalima kontroliuoti, numatyti ir užkirsti kelio jų atsiradimui (žaibas, gaisras, potvynis, užliejimas, audros, elektros instaliacijos degimas, temperatūros ir (ar) drėgmės pakitimų poveikis, purvo, dulkių ir magnetinių laukų įtaka, techninės avarijos, išskyrus nurodytas Aprašo 7.1 papunktyje, ir kt.).

8. Pažeidimas, galintis kelti pavojų duomenų subjektų teisėms ir laisvėms, yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, kyla grėsmė duomenų subjektų sveikatai ir (ar) gyvybei ar grėsmė patirti materialinę ar nematerialinę žalą, pvz., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala. Preziumuojama, kad pažeidimas kelia riziką, kai pažeidimas yra susijęs su specialių kategorijų asmens duomenimis.

9. Pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis skirstomas:

9.1. žema rizikos tikimybė (dėl pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms): fizinis asmuo gali susidurti su tam tikrais nepatogumais (pvz., sugaištas laikas iš naujo suvedant informaciją, susierzinimas, nepasitenkinimas ir pan.);

9.2. vidutinė rizikos tikimybė (dėl pažeidimo yra/gali kilti nedidelis pavojus fizinių asmenų teisėms ir laisvėms): fizinis asmuo gali patirti nepatogumų, kuriuos jis galės įveikti nepaisant tam tikrų sunkumų (pvz., papildomos išlaidos, prieigos prie reikalingų išteklių praradimas, stresas, nedideli fiziniai negalavimai ir kt.);

9.3. didelė rizikos tikimybė (dėl pažeidimo yra/gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms): fizinis asmuo gali patirti reikšmingas pasekmes ir norint jas ištaisyti, pašalinti reikės susidurti su rimtais sunkumais (pvz., lėšų praradimas, asmens įtraukimas į finansinių institucijų juodąjį sąrašą, turto nuostoliai (žala), darbo vietos praradimas, teisminiai procesai, sveikatos būklės pablogėjimas ir pan.) arba dideles ar negrįžtamas pasekmes, kurių negalės ištaisyti, pašalinti (pvz., negalėjimas dirbti, ilgalaikiai psichiniai ar fiziniai negalavimai, mirtis ir pan.).

III SKYRIUS
PRANEŠIMO APIE PAŽEIDIMĄ PATEIKIMAS

10. Darbuotojas, nustatęs arba kitaip sužinojęs apie galimą pažeidimą arba kai informacija apie galimą pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio:

10.1. nedelsdamas, bet ne vėliau kaip per 2 valandas nuo galimo pažeidimo paaiškėjimo momento, žodžiu (tiesiogiai ar telefonu) arba elektroniniu paštu informuoja Departamento direktorių, savo tiesioginį vadovą ir valstybės tarnautoją, atliekantį duomenų apsaugos pareigūno funkcijas Departamente (toliau – duomenų apsaugos pareigūnas);

10.2. užpildo Aprašo 1 priede nurodytos formos Pranešimą apie asmens duomenų saugumo pažeidimą, kuris registruojamas dokumentų valdymo sistemoje (toliau – DVS) ir nedelsiant, bet ne vėliau kaip per 2 valandas nuo asmens duomenų saugumo pažeidimo paaiškėjimo momento perduodamas per DVS ir elektroniniu paštu Departamento direktoriui, darbuotojo tiesioginiam vadovui ir duomenų apsaugos pareigūnui;

10.3. tuo atveju, jei terminas nuo momento, kai darbuotojui tapo žinoma apie pažeidimą iki pranešimo Departamento direktoriui, tiesioginiam vadovui ir duomenų apsaugos pareigūnui, yra ilgesnis nei 2 valandos, Departamento darbuotojas kartu su Pranešimu apie asmens duomenų saugumo pažeidimą pateikia paaiškinimą dėl uždelsto informacijos pateikimo priežasčių;

10.4. jei įmanoma, pagal kompetenciją imasi priemonių pašalinti pažeidimą ir (ar) priemonių sumažinti jo sukeltas neigiamas pasekmes.

11. Duomenų tvarkytojas, nustatęs galimą pažeidimą, nedelsdamas, bet ne vėliau kaip per 24 valandas nuo pažeidimo paaiškėjimo momento, apie tai praneša Departamento el. pašto adresu centras@kpd.lt, pateikdamas užpildytą Aprašo 1 priede nurodytos formos Pranešimą apie asmens duomenų saugumo pažeidimą.

12. Tuo atveju, jei terminas nuo momento, kai duomenų tvarkytojui tapo žinoma apie pažeidimą iki pranešimo Departamentui yra ilgesnis nei 24 valandos, duomenų tvarkytojas kartu su pranešimu pateikia Departamentui paaiškinimą dėl uždelsto informacijos pateikimo priežasčių.

13. Duomenų tvarkytojas pateikia visą Departamento prašomą informaciją, susijusią su pažeidimu ir jo tyrimu, per Departamento nurodytą laiką.

IV SKYRIUS
PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

14. Departamento direktorius, sužinojęs apie pažeidimą, rašytine rezoliucija arba įsakymu paskiria atsakingą asmenį, kuris pradeda pažeidimo tyrimą ir imasi šių veiksmų:

14.1. nagrinėja Pranešime apie asmens duomenų saugumo pažeidimą nurodytas aplinkybes ir įvertina, ar įvyko pažeidimas;

14.2. kiek įmanoma tiksliau surenka duomenis ir įrodymus apie įvykusį pažeidimą (pvz., kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės ar informacinės sistemos, kam per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su asmens duomenimis ir kt.);

14.3. dokumentuoja pažeidimo tyrimą (apžiūros aktai, specialistų išvados, liudytojų parodymai, fotofiksacija ir kt.);

14.4. konsultuojasi su duomenų apsaugos pareigūnu (jeigu atsakingas asmuo kartu nėra ir duomenų apsaugos pareigūnas); esant būtinybei, pagal kompetenciją konsultuojasi su kitais Departamento specialistais;

14.5. imasi kitų veiksmų, kurie yra būtini pažeidimui nustatyti ir (ar) galimoms neigiamoms jo pasekmėms sumažinti.

15. Darbuotojai ir duomenų tvarkytojai privalo išsaugoti esamos situacijos, susijusios su galimu pažeidimu, įrodymus, kad vėliau naudojant technines ir organizacines priemones (pvz., duomenų srauto ir prisijungimų analizės įrankius ar kt.) galima būtų tirti pažeidimą.

16. Tyrimo metu objektyviai įvertinamos pažeidimo aplinkybės ir atsižvelgiama į:

16.1. pažeidimo pobūdį (tipą);

16.2. asmens duomenų pobūdį, kategoriją (pvz., specialių kategorijų asmens duomenys), asmens duomenų, kurių saugumas pažeistas pažeidimu, apimtį;

16.3. duomenų subjekto identifikavimo galimybę tiesiogiai ar netiesiogiai pasinaudojant pažeidimo objektu esančiais duomenimis;

16.4. pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygį;

16.5. duomenų subjekto savybes (pvz., vaikas ar kitas pažeidžiamas asmuo);

16.6. duomenų subjektų, kurių asmens duomenų saugumas buvo pažeistas, skaičių;

16.7. kitas reikšmingas aplinkybes.

17. Atsakingas asmuo atlikto pažeidimo tyrimo rezultatus įformina Asmens duomenų saugumo pažeidimo tyrimo ataskaitoje (Aprašo 2 priedas), kuri registruojama DVS.

18. Asmens duomenų saugumo pažeidimo tyrimo ataskaita yra perduodama Departamento direktoriui rezoliucijai įrašyti ir duomenų apsaugos pareigūnui, kuris šias ataskaitas kaupia ir saugo.

Atsakingas asmuo perduoda Asmens duomenų saugumo pažeidimo tyrimo ataskaitą susipažinti duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

19. Atsižvelgiant į Asmens duomenų saugumo pažeidimo tyrimo ataskaitą, Departamento direktorius, konsultuodamasis su duomenų apsaugos pareigūnu:

19.1. priima sprendimą apie pažeidimą pranešti VDAI, kai dėl pažeidimo yra arba gali kilti pavojus fizinių asmenų teisėms ir laisvėms;

19.2. priima sprendimą apie pažeidimą nepranešti VDAI, kai pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms;

19.3. priima sprendimą apie pažeidimą pranešti duomenų subjektams, kai dėl pažeidimo yra arba gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms;

19.4. priima sprendimą apie pažeidimą nepranešti duomenų subjektams, kai dėl pažeidimo nekyla arba negali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms;

19.5. priima sprendimą dėl tolesnių veiksmų, susijusių su pažeidimu, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

20. Sprendžiant pažeidimo pašalinimo klausimą bei tvirtinant priemonių planą, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti pažeidimą. Priklausomai nuo konkrečių pažeidimo aplinkybių, turėtų būti atlikti tokie veiksmai, kaip: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamo / mobilaus įrenginio (telefono, nešiojamo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuriam jie buvo skirti, kuo skubiau kreiptis į jį su prašymu ištrinti atsiųstus asmens duomenis be galimybės juos atkurti ir patvirtinti ištrynimo faktą; pakeisti prisijungimo prie duomenų bazės ar informacinės sistemos vardus ir slaptažodžius; naudoti atsargines kopijas, siekiant atkurti prarastus, sugadintus ar pakeistus duomenis ir kt.).

21. Priemonių plane turi būti numatyti veiksmai, nukreipti ne vien į esamo pažeidimo priežasties pašalinimą, pavojaus fizinių asmenų teisėms ir laisvėms sumažinimą ar pašalinimą, bet taip pat skirti neleisti pasikartoti pažeidimui. Būtina atsižvelgti į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant pažeidimą bei imtis priemonių tuos trūkumus pašalinti.

V SKYRIUS
PRANEŠIMAS APIE PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

22. Tyrimo metu nustačius, kad pažeidimas įvyko, atsakingas asmuo Departamento direktoriaus pavedimu nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai tapo žinoma apie pažeidimą, apie tai informuoja VDAI, išskyrus Aprašo 19.2 punkte nustatytą atvejį.

23. VDAI informuojama Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, tvirtinamo VDAI direktoriaus, nustatyta tvarka ir sąlygomis, užpildant VDAI direktoriaus tvirtinamą Pranešimo apie asmens duomenų saugumo pažeidimo formą.

24. Jeigu, įvertinus riziką, abejojama, ar pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.

25. Jeigu įvertinus riziką, nustatoma, kad apie pažeidimą VDAI pranešti nereikia, pasikeitus situacijai, pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., pamesta USB atmintinė, kurioje saugomi asmens duomenys, užšifruoti taikant pažangų algoritmą, yra atsarginės duomenų kopijos ir nėra pavojaus šifro saugumui, tačiau vėliau paaiškėjus, kad gali kilti pavojus šifro saugumui, pažeidimo keliamas pavojus bus vertinamas iš naujo ir sprendžiama dėl pranešimo VDAI).

26. Tuo atveju kai, priklausomai nuo pažeidimo pobūdžio, būtina atlikti išsamesnį tyrimą, nustatyti visus svarbius faktus, susijusius su pažeidimu, ir per 72 valandas dėl objektyvių priežasčių nėra įmanoma ištirti pažeidimą, informacija VDAI teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminį pranešimą.

27. Jeigu po pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad pažeidimo nebuvo, apie tai nedelsiant informuojama VDAI.

28. Tuo atveju, kai yra įtariama, kad pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybinėms institucijoms, įgaliotoms atlikti ikiteisminį tyrimą.

VI SKYRIUS
PRANEŠIMAS APIE PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

29. Tyrimo metu nustačius, kad dėl pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, atsakingas asmuo Departamento direktoriaus pavedimu nedelsdamas ir, 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.

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

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

31.1. pažeidimo pobūdžio (tipo) ir tikėtinų pažeidimo pasekmių aprašymas;

31.2. priemonių, kurių ėmėsi Departamentas, kad būtų pašalintas pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas;

31.3. duomenų apsaugos pareigūno, atsakingo asmens arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

31.4. kita reikšminga informacija, susijusi su pažeidimu, kuri, atsakingo asmens manymu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

32. Pranešimo apie pažeidimą duomenų subjektams teikti nereikia jeigu:

32.1. Departamentas įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su duomenimis, jie būtų nesuprantami (pvz., asmens duomenų šifravimo priemonės);

32.2. iš karto po pažeidimo Departamentas ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;

32.3. tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai didelių pastangų, pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi. Tokiu atveju apie pažeidimą viešai paskelbiama Departamento interneto svetainėje, spaudoje, pasitelkiami ne vienas, o keli informavimo būdai arba taikomos panašios priemonės, kuriomis duomenų subjektai būtų efektyviai informuojami (pvz., vien tik pranešimas interneto svetainėje tam tikrais atvejais gali būti nepakankama priemonė).

33. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie pažeidimą duomenų subjektams pranešti nereikia, po kurio laiko situacija gali pasikeisti, todėl pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą ir duomenų bazėje esantys asmens duomenys užšifruojami, tačiau atlikus tyrimą, paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenis ir jokio kito kenksmingo poveikio duomenų bazei ir asmens duomenims nėra; tačiau, jei vėliau paaiškėja, kad prarastas ne tik duomenų prieinamumas,

bet ir konfidencialumas, pažeidimo keliamas pavojus bus vertinamas iš naujo bei sprendžiama, ar atsižvelgiant į tikėtinas pažeidimo pasekmes apie jį reikia pranešti duomenų subjektams).

34. Tam tikromis aplinkybėmis, kai tai yra pagrįsta, Departamentas pasitaręs su teisėsaugos institucijomis ir atsižvelgdamas į teisėtus teisėsaugos interesus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą apie pažeidimą iki to laiko, kai tai netrukdys pažeidimo tyrimui.

VII SKYRIUS
PAŽEIDIMŲ DOKUMENTAVIMAS

35. Atsakingas asmuo pildo Pranešimų apie asmens duomenų saugumo pažeidimą pateikimo ataskaitą, kuri registruojama DVS (Aprašo 3 priedas). Ataskaita yra perduodama susipažinti Departamento direktoriui ir duomenų apsaugos pareigūnui, kuris šias ataskaitas kaupia ir saugo. Atsakingas asmuo perduoda Pranešimų apie asmens duomenų saugumo pažeidimą pateikimo ataskaitą susipažinti duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

36. Visi pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale (Aprašo 4 priedas).

37. Informacija apie pažeidimą į Asmens duomenų saugumo pažeidimų registravimo žurnalą įvedama nedelsiant, kai tik paaiškėja galimas pažeidimas, bet ne vėliau kaip per 5 darbo dienas nuo galimo pažeidimo paaiškėjimo momento. Kai pasikeičia Asmens duomenų saugumo pažeidimų registravimo žurnale nurodyta informacija arba paaiškėja nauja informacija, Asmens duomenų saugumo pažeidimų registravimo žurnale esanti informacija turi būti papildoma ir (ar) koreguojama.

38. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

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

38.2. 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);

38.3. tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;

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

38.5. informacija apie pranešimo apie pažeidimą pateikimą VDAI:

38.5.1. jei apie pažeidimą nebuvo pranešta VDAI, nurodomi tokio sprendimo motyvai; jei apie pažeidimą buvo pranešta VDAI, nurodoma pranešimo data ir numeris, taip pat, ar pranešimas teikiamas etapais;

38.5.2. jeigu apie pažeidimą buvo vėluojama pranešti VDAI, nurodomos tokio vėlavimo priežastys;

38.6. informacija apie pranešimą duomenų subjektui (subjektams) apie pažeidimą:

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

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

38.6.3. kita reikšminga informacija, susijusi su pažeidimu.

39. Asmens duomenų saugumo pažeidimų registravimo žurnalas yra tvarkomas elektronine forma ir saugomas pagal patvirtintą Departamento dokumentacijos planą.

40. Asmens duomenų saugumo pažeidimų registravimo žurnalą pildo ir tvarko duomenų apsaugos pareigūnas.

41. Kai padarytas pažeidimas yra susijęs su kibernetiniu incidentu, informacija apie kibernetinį incidentą, susijusį su pažeidimu, pateikiama Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytoms valstybės institucijoms šio įstatymo nustatyta tvarka ir atvejais.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

42. Darbuotojai su Aprašu bei jo pakeitimais supažindinami DVS priemonėmis.

43. Aprašas duomenų apsaugos pareigūno peržiūrimas periodiškai, ne rečiau kaip kartą per metus arba įvykus organizaciniams, sisteminiams ar kitiems pokyčiams, arba pasikeitus teisės aktų reikalavimams.

44. Darbuotojai, pažeidę Aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____

Asmens duomenų saugumo pažeidimų
Kultūros pavelde departamente prie Kultūros
ministerijos valdymo tvarkos aprašo
1 priedas

(Pranešimo apie asmens duomenų saugumo pažeidimą forma)

_____
(juridinio asmens pavadinimas)

_____
(struktūrinio padalinio pavadinimas)

_____
(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., Departamento darbuotojai, asmenys, pateikę prašymus, skundus ir kt.) ir apytikslis jų skaičius:

_____
_____

_____

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 vietos 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, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys, susiję su asmens lytiniu gyvenimu ir lytine orientacija)

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas

☐ Jautresni duomenys ir duomenys apie pažeidžiamus asmenis: finansinė informacija, duomenys apie vaikus ir pan.:

☐ Kiti asmens duomenys (įrašyti):

_____

_____

_____

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

_____

_____

7. Kokių veiksmų (priemonių) buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti prisijungimo prie informacinės 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
Kultūros pavelde departamente prie
Kultūros ministerijos valdymo tvarkos aprašo
2 priedas

(Asmens duomenų saugumo pažeidimo tyrimo ataskaitos forma)

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 ir laikas ☐

Asmens duomenų saugumo pažeidimo nustatymo data ir laikas ☐

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

☐ Informacinė sistema
☐ Duomenų bazė
☐ Tarnybinė stotis
☐ Internetinė svetainė
☐ Debesų kompiuterijos paslaugos
☐ Nešiojami / mobilūs įrenginiai
☐ Neautomatiniu būdu susistemintos bylos (archyvas)
☐ Kita (įrašyti):

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

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

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

☐ 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 vietos 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, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.):

_____
_____
_____

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

_____
_____
_____

☐ Kiti asmens duomenys:

1.5. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius: ☐

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

1.7. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius: ☐

1.8. Darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, Departamento 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 fizinį asmenį (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 fiziniams asmenims (duomenų subjektams)?

2.6. Galimos asmens duomenų saugumo pažeidimo pasekmės:

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

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

☐ Skirtingos informacijos susiejimas (pvz., gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)

☐ Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pvz., komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)

☐ Kita:

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

☐ Pakeitimas į neteisingus duomenis, dėl ko asmuo gali netekti galimybės naudotis paslaugomis

☐ Pakeitimas 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 administracinės 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 pavojus fizinių asmenų teisėms ir laisvėms)

☐ Didelė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra / gali kilti didelis pavojus 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, įskaitant ir priemones sumažinti asmens duomenų saugumo pažeidimo pasekmes:

Atsakingas asmuo:

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

Susipažino valstybės tarnautojas, atliekantis duomenų apsaugos pareigūno funkcijas:

_____	_____
(parašas)	(vardas ir pavardė)

Asmens duomenų saugumo pažeidimų
Kultūros pavelde departamente prie
Kultūros ministerijos valdymo tvarkos aprašo
3 priedas

(Pranešimų apie asmens duomenų saugumo pažeidimą pateikimo ataskaitos forma)

PRANEŠIMŲ APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PATEIKIMO ATASKAITA

_____ Nr. _____
(data, dokumento numeris)

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

☐ Taip

Pranešimo VDAI data ir numeris ____

☐ Ne (nurodomos nepranešimo VDAI priežastys):

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

---

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

☐ Taip

Pranešimo duomenų subjektui data ir numeris (jeigu pranešimas užregistruotas) ____

Pranešimo duomenų subjektui būdas (pažymėti tinkamą (-us): ☐ paštu ☐ elektroniniu paštu ☐ trumpąja 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. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių (jeigu taip, nurodoma rašto data ir numeris):

Atsakingas asmuo:

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

Susipažino Departamento direktorius:

_____	_____
(parašas)	(vardas ir pavardė)

Susipažino valstybės tarnautojas, atliekantis duomenų apsaugos pareigūno funkcijas:

_____	_____
(parašas)	(vardas ir pavardė)

Asmens duomenų saugumo pažeidimų
Kultūros pavelde departamente prie
Kultūros ministerijos valdymo tvarkos aprašo
4 priedas

(Asmens duomenų saugumo pažeidimų registravimo žurnalo forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Pažeidimo nustatymo data, laikas ir vieta	Darbuotojas ar duomenų tvarkytojas, pranešęs apie pažeidimą (vardas, pavardė,	Pažeidimo padarymo data ir vieta	Pažeidimo pobūdis, priežastys ir kitos aplinkybės	Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir	Asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis	Tikėtinos pažeidimo pasekmės bei pavojus fizinių asmenų teisėms ir	Priemonės, kurių buvo imtasi pažeidimui pašalinti ir (ar) neigiamoms	Informacija, ar apie pažeidimą buvo pranešta Valstybinei duomenų	Informacija, ar apie pažeidimą buvo pranešta duomenų subjektui	Kita informacija, susijusi su asmens duomenų saugumo pažeidimu

		pareigos ar pavadinimas)			**apytikslis skaičius**	**skaičius**	**laisvėms**	**pažeidimo pasekmėms sumažinti**	**apsaugos inspekcijai, priimto sprendimo motyvai**	**(subjektams), priimto sprendimo motyvai**	
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Kultūros paveldo departamentas prie Kultūros ministerijos 188692688, Šnipiškių g. 3, Vilnius
Dokumento pavadinimas (antraštė)	DĖL ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ KULTŪROS PAVELDO DEPARTAMENTE PRIE KULTŪROS MINISTERIJOS VALDYMO TVARKOS APRAŠO PATVIRTINIMO
Dokumento registracijos data ir numeris	2021-06-25 Nr. Į-166
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Vidmantas Bezaras, Direktorius
Sertifikatas išduotas	VIDMANTAS BEZARAS, Kultūros paveldo departamentas prie Kultūros ministerijos LT
Parašo sukūrimo data ir laikas	2021-06-24 22:47:06 (GMT+03:00)
Parašo formatas	XAdES-X-L
Laiko žymoje nurodytas laikas	2021-06-24 22:47:17 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA-A, Asmens dokumentu israsymo centras prie LR VRM LT
Sertifikato galiojimo laikas	2018-12-06 09:44:13 – 2021-12-05 09:44:13
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA, VI Registru centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Kultūros paveldo departamentas prie KM, į.k.188692688 LT", sertifikatas galioja nuo 2018-12-27 13:50:17 iki 2021-12-26 13:50:17
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.34
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2021-06-26 01:25:23)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2021-06-26 01:25:23 Dokumentų valdymo sistema Avilys