PALOMENĖS KULTŪROS CENTRAS

ĮSAKYMAS
DĖL ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO PALOMENĖS KULTŪROS CENTRE TVARKOS APRAŠO PATVIRTINIMO

2024 m. vasario 5 d. Nr. V- 6
Kaišiadorys

Vadovaudamasis 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, kuriuo panaikinama Direktyva 95/46/EB ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu:

1. T v i r t i n u Asmens duomenų saugumo pažeidimų valdymo Palomenės kultūros centre tvarkos aprašą (pridedama).

2. S k i r i u Palomenės kultūros centro administratorę Janiną Seliutienę būti atsakingu už duomenų apsaugą.

3. N u r o d a u kultūrinių veiklų koordinatorei ir organizatorei Kristinai Ulanavičienei šį įsakymą paskelbti Palomenės kultūros centro interneto svetainėje.

4. P a v e d u Palomenės kultūros centro administratorei Janinai Seliutienei su šiuo įsakymu pasirašytinai supažindinti darbuotojus.

Direktorė Virginija Kudaševičienė

PATVIRTINTA
Palomenės kultūros centre direktoriaus
2024 m. vasario 5 d. įsakymu Nr. V- 6

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO PALOMENĖS KULTŪROS CENTRE TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo Palomenės kultūros centre tvarkos aprašas (toliau – Aprašas) nustato asmens duomenų saugumo pažeidimų (toliau – pažeidimas) ir jų priežasčių klasifikavimą, pranešimo apie pažeidimus Palomenės kultūros centre (toliau – Centras), Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) ir duomenų subjektams, pažeidimų tyrimo, ir jų pasekmių pašalinimo ir mažinimo, pažeidimų prevencijos ir dokumentavimo tvarką.

2. Aprašas taikomas visiems Centro darbuotojams tvarkantiems asmens duomenis, kurių duomenų valdytojas yra Palomenės kultūros centras

3. Aprašas parengtas vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 (toliau -Reglamentas (ES) 2016/679), dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB.

4. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679 ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.

II SKYRIUS
PAŽEIDIMŲ IR JŲ PRIEŽASČIŲ KLASIFIKAVIMAS

5. Pažeidimai pagal pobūdį (tipą) yra:

5.1. konfidencialumo pažeidimas – netyčinis arba neteisėtas asmens duomenų laikinas ar nuolatinis atskleidimas ar prieigos prie asmens duomenų suteikimas asmenims, kurie neturi teisės susipažinti su asmens duomenimis;

5.2. prieinamumo pažeidimas – neteisėtas, laikinas ar nuolatinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas;

5.3. vientisumo pažeidimas – neteisėtas asmens duomenų laikinas ar nuolatinis pakeitimas;

5.4. mišraus pobūdžio (tipo) pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių Aprašo 5.1–5.3 papunkčiuose nurodytų pažeidimų derinys.

6. Pažeidimai gali būti nulemti šių priežasčių:

6.1. 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 ir kt.);

6.2. tyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas sąmoningai turint tikslą tai padaryti (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, asmens duomenų vagystė, neteisėtas naudojimasis kito Centro darbuotojo teisėmis ir kt.);

6.3. *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 6.1 papunktyje, ir kt.).

III SKYRIUS
PRANEŠIMAS APIE GALIMĄ PAŽEIDIMĄ IR JO NAGRINĖJIMAS

7. Centro darbuotojas, sužinojęs ar pats nustatęs galimą pažeidimą, arba kai informacija apie galimą pažeidimą gaunama, žiniasklaidos ar kito šaltinio (toliau – galimo pažeidimo paaiškėjimas), privalo:

7.1. tą pačią darbo dieną ne vėliau kaip per 2 darbo valandas nuo galimo pažeidimo paaiškėjimo momento informuoti žodžiu, raštu ar elektroninėmis priemonėmis savo tiesioginį vadovą ir Centro direktoriaus paskirtą už duomenų apsaugą atsakingą darbuotoją;

7.2. užpildyti Aprašo 1 priede nustatytos formos pranešimą apie galimą asmens duomenų saugumo pažeidimą (toliau – pranešimas), kuris registruojamas Dokumentų valdymo sistemoje (toliau – DVS), ir nedelsdamas, bet ne vėliau kaip per 4 darbo valandas nuo galimo pažeidimo paaiškėjimo momento, perduoti jį per DVS ir el. paštu janina.seliutiene@gmail.com, Centro darbuotojui atsakingam už duomenų apsaugą;

7.3. jei įmanoma, imtis priemonių pašalinti galimą pažeidimą ir priemonių galimoms neigiamoms jo pasekmėms sumažinti.

8. Centro darbuotojas atsakingas už duomenų apsaugą, gavęs užpildytą darbuotojo pranešimą apie galimą asmens duomenų saugumo pažeidimą privalo:

8.1. atlikti pažeidimo tyrimą Aprašo IV skyriaus nustatyta tvarka;

8.2. pasitelkti Centro direktoriaus įgaliotus asmenis pagal kompetenciją.

8.3. asmens duomenų, tvarkomų saugumo galimo pažeidimo atveju, kai galimas pažeidimas yra susijęs su kibernetiniu incidentu, informaciją apie galimą pažeidimą kartu su informacija apie kibernetinį incidentą pateikti Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytoms valstybės institucijoms Lietuvos Respublikos kibernetinio saugumo įstatymo nustatyta tvarka ir atvejais;

8.4. informaciją apie galimą pažeidimą fiksuoti Asmens duomenų saugumo pažeidimų registracijos žurnale (toliau – Žurnalas) (Aprašo 2 priedas);

8.5. bendradarbiauti su Inspekcija dėl pažeidimų;

8.6. teikti rekomendacijas Centro darbuotojams, atsakingiems už pažeidimo ir (ar) jo pasekmių pašalinimą ir (ar) sumažinimą, dėl tinkamų techninių ir organizacinių priemonių, kad pažeidimas būtų išsamiai ištirtas ir jis ir (ar) jo pasekmės būtų pašalintos ir (ar) sumažintos ir pažeidimas ateityje nepasikartotų, taikymo ir (arba) pats imtis šių veiksmų;

8.7. stebėti, kaip vykdomos Reglamente (ES) 2016/679 ir Apraše nustatytos Centro pareigos, susijusios su pažeidimų valdymu.

8.8. Centro darbuotojas atsakingas už duomenų apsaugą, gali konsultuotis su duomenų apsaugos pareigūnu.

9. Kai yra įtariama, kad pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, teisės aktų, reguliuojančių tokios informacijos teikimą, nustatyta tvarka.

IV SKYRIUS
PAŽEIDIMO TYRIMAS

10. Centro darbuotojas, atsakingas už duomenų apsaugą nedelsdamas, bet ne vėliau kaip per 24 valandas nuo pranešimo gavimo momento, išnagrinėja pranešime nurodytas aplinkybes, įvertina, ar padarytas pažeidimas, jei pažeidimas padarytas, nustato, kokio pobūdžio (tipo) pažeidimas padarytas, asmens duomenų, kurių saugumas pažeistas, kategorijas, įskaitant specialių kategorijų asmens duomenis, pažeidimo priežastis, pažeidimo apimtis (duomenų subjektų kategorijos ir jų skaičius), esamas ir (ar) galimas pasekmes ir žalą, padarytą duomenų subjektui (-ams), įvertina pavojų duomenų subjekto teisėms ir laisvėms (toliau – rizika), kuris gali atsirasti dėl galimo pažeidimo, Aprašo 12 ir 13 punktuose nustatyta tvarka ir pateikia Centro direktoriui (ar jo įgaliotam asmeniui) išvadą dėl pažeidimo buvimo ir rizikos.

11. Pažeidimo tyrimo metu Centro darbuotojai pagal kompetenciją privalo bendradarbiauti ir operatyviai teikti Centro darbuotojui, atsakingam už duomenų apsaugą, visą jo prašomą su pažeidimu susijusią informaciją ir dokumentus.

12. Rizika vertinama objektyviai įvertinus pažeidimo aplinkybes ir atsižvelgiant į:

12.1. pažeidimo pobūdį (tipą);

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

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

12.4. padarinių duomenų subjektui sunkumą. Vertinant riziką turi būti laikoma, kad 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 jis yra susijęs su specialių kategorijų asmens duomenimis;

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

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

12.7. duomenų valdytojo savybes (pvz., veiklos pobūdį).

13. Įvertinus riziką nustatoma, kad yra:

13.1. maža rizika, kai nustatoma, kad pavojaus duomenų subjekto teisėms ir laisvėms nėra;

13.2. vidutinė rizika, kai nustatoma, kad dėl asmens duomenų saugumo pažeidimo yra arba gali kilti nedidelis pavojus duomenų subjektų teisėms ir laisvėms;

13.3. didelė rizika, kai nustatoma, kad dėl asmens duomenų saugumo pažeidimo yra arba gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms.

14. Jeigu per 24 val. nuo pranešimo gavimo momento dėl objektyvių priežasčių nebuvo nustatytos visos aplinkybės, nurodytos Aprašo 12 punkte, Centro darbuotojas atsakingas už duomenų apsaugą atlieka tolesnį pažeidimo tyrimą. Šiame punkte nurodytas tyrimas turi būti atliktas ir Aprašo 3 priede nustatytos formos Asmens duomenų saugumo pažeidimo ataskaita parengta ir pateikta Centro direktoriui ne vėliau kaip per 20 darbo dienų nuo pažeidimo paaiškėjimo dienos.

15. Jeigu išvadoje dėl pažeidimo buvimo ir rizikos nurodyta, kad rizikos nėra, tačiau Aprašo 14 punkte nurodyto pažeidimo tyrimo metu nustatoma, kad rizika gali kilti, arba pažeidimo metu pasikeitė rizikos laipsnis, Centro darbuotojas atsakingas už duomenų apsaugą turi riziką vertinti iš naujo Aprašo 12 ir 13 punktuose nustatyta tvarka.

V SKYRIUS
PRANEŠIMAS INSPEKCIJAI

16. Aprašo 13.2 ir 13.3 papunkčiuose nurodytais atvejais asmens duomenų, tvarkomų Centro saugumo pažeidimo atveju Centro darbuotojas atsakingas už duomenų apsaugą ne vėliau kaip per 72 valandas nuo galimo pažeidimo paaiškėjimo momento Inspekcijos nustatyta tvarka ir sąlygomis praneša apie pažeidimą Inspekcijai (Aprašo 4 priedas) ir pranešimo kopiją pateikia Centro direktoriui. Jeigu abejojama dėl rizikos priskyrimo Aprašo 13.2 ar 13.3 papunkčiuose nurodytam rizikos lygiui, vis tiek apie pažeidimą pranešama Inspekcijai.

17. Kai sužinojus apie galimai įvykusį pažeidimą nėra objektyvių galimybių per 72 valandas nustatyti, ar pažeidimas tikrai įvyko, Inspekcijai per 72 valandas nuo sužinojimo apie galimai įvykusį pažeidimą būtina pateikti pranešimą apie pažeidimą, nurodant tiek informacijos, kiek tuo metu yra žinoma. Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie pažeidimą Inspekcijai, būtina pranešti.

18. Jeigu atliekamas Aprašo 14 punkte nurodytas tyrimas, Inspekcijai informacija gali būti teikiama etapais. Apie informacijos teikimą etapais Centras informuoja Inspekciją.

19. Jeigu po pranešimo Inspekcijai pateikimo, atlikus Aprašo 14 punkte nurodytą tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir nebuvo pažeidimo, apie tai ne vėliau kaip per 3 darbo dienas nuo šios informacijos paaiškėjimo momento Centras informuoja Inspekciją ir pažymi Žurnale.

VI SKYRIUS

PRANEŠIMAS DUOMENŲ SUBJEKTUI

20. Aprašo 13.3 papunktyje nurodytu atveju asmens duomenų, tvarkomų Centro saugumo pažeidimo atveju Centro darbuotojas atsakingas už duomenų apsaugą, privalo nedelsdamas (rekomenduojama per 72 val. nuo galimo pažeidimo paaiškėjimo momento) apie tai raštu (Aprašo 5 priedas) pranešti duomenų subjektui, kurio teisėms ir laisvėms dėl šio pažeidimo kyla didelė rizika. Pranešimas rengiamas ir teikiamas šio skyriaus ir Aprašo V skyriaus *mutatis mutandis* nustatyta tvarka.

21. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama:

21.1. pažeidimo pobūdžio aprašymas;

21.2. Centro darbuoto atsakingo už duomenų apsaugą, pavardė (pavadinimas) ir kontaktiniai duomenys;

21.3. galimų pažeidimo pasekmių aprašymas;

21.4. priemonių, kurių ėmėsi Centras arba siūlo imtis duomenų subjektui, kad būtų pašalintas pažeidimas ir (ar) pašalintos ar sumažintos galimos neigiamos jo pasekmės, aprašymas (pvz., kad apie pažeidimą yra informuota Inspekcija ir kad yra gautas patarimas dėl pažeidimo pasekmių pašalinimo ar sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);

21.5. kita reikšminga informacija, susijusi su pažeidimu, kuri, Centro manymu, turėtų būti pateikta duomenų subjektui.

22. Pranešimo pateikimo būdas pasirenkamas atsižvelgiant į tai, kokius duomenų subjekto kontaktinius duomenis tvarko Centras ir į tai, kuris būdas geriausiai užtikrintų, kad pranešimas pasiektų adresatą. Šis pranešimas turi būti atskirtas nuo kitos siunčiamos informacijos, tokios kaip nuolatiniai atnaujinimai, naujienlaiškiai ar standartiniai pranešimai. Gali būti taikomi keli pranešimo duomenų subjektui apie pažeidimą būdai.

23. Pranešimas duomenų subjektui apie pažeidimą neteikiamas, išskyrus, jei teikti pranešimą reikalauja Inspekcija, šiais atvejais:

23.1. Centras įgyvendino tinkamas technines ir organizacines asmens duomenų apsaugos priemones, kurios užtikrino, kad įvykus pažeidimui nekils rizika, ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio (pvz., asmens duomenys buvo šifruoti);

23.2. iš karto po pažeidimo Centras ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti rizika;

23.3. reikėtų neproporcingai daug pastangų susisiekti su duomenų subjektais (pvz., kai jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba nežinomi). Tokiu atveju Aprašo 21 punkte nurodyta informacija apie pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai, pvz., pranešimas interneto svetainėje, spaudoje ar pan.

24. Jeigu Centras pranešimo duomenų subjektui apie pažeidimą neteikė, Centras turi pagrįsti Inspekcijai, kad įvykdė vieną iš Aprašo 23 punkte nurodytų sąlygų.

VII SKYRIUS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRACIJOS ŽURNALO TVARKYMAS

25. Centras asmens duomenų saugumo pažeidimo atveju, tvarko asmens duomenų saugumo pažeidimų registracijos Žurnalą.

26. Žurnale nurodoma:

26.1. visi su pažeidimu susiję faktai – pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

26.2. pažeidimo poveikis ir pasekmės;

26.3. taisomieji veiksmai (techninės priemonės), kurių buvo imtasi;

26.4. su pažeidimu susijusių sprendimų priėmimo priežastys (pvz., kodėl duomenų valdytojas nusprendė nepranešti apie pažeidimą Inspekcijai ir (ar) duomenų subjektui, t. y. kodėl nusprendė, kad rizika žema, arba kokią Aprašo 23 punkte nurodytą sąlygą įvykdė);

26.5. pranešimo Inspekcijai pateikimo vėlavimo priežastys (jeigu pranešimą vėluojama pateikti ar pranešimas teikiamas etapais);

26.6. informacija, susijusi su pranešimu duomenų subjektui (pvz., ar buvo pranešta, kodėl nepranešta ir pan.);

26.7. kita reikšminga informacija, susijusi su pažeidimu (pvz., kad tyrimo metu nustatyta, jog Pažeidimo nebuvo, o buvo tik saugumo incidentas).

27. Už Žurnalo pildymą ir saugojimą atsakingas Centro darbuotas atsakingas už duomenų apsaugą. Žurnale registruojami visi pažeidimai, nepaisant to, ar apie juos pranešta Inspekcijai ir (ar) duomenų subjektui, ar tokie pažeidimai kelia riziką. Žurnalas gali būti popierinės arba elektroninės formos. Užpildytas Žurnalas saugomas 5 metus nuo paskutinio įrašo Žurnale datos.

28. Informacija apie pažeidimą į Žurnalą turi būti įrašoma nedelsiant, kai tik paaiškėja galimas pažeidimas, bet ne ilgiau kaip per 5 darbo dienas nuo galimo pažeidimo paaiškėjimo momento. Kai pasikeičia Žurnale nurodyta informacija arba paaiškėja nauja informacija, Žurnale esanti informacija turi būti papildoma ir (ar) koreguojama.

29. Žurnalas yra pateikiamas Inspekcijai jai pareikalavus.

30. Centro darbuotas atsakingas už duomenų apsaugą kartą per ketvirtį peržiūri Žurnale esančius įrašus ir pasiūlo Centro direktoriui, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip turėtų būti kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje tokie patys pažeidimai nesikartotų.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

31. Centro darbuotojai 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.) būtų galima tirti pažeidimą.

32. Prireikus Centre gali būti sudaryta darbo grupė pažeidimams (įskaitant jų priežastis, pasekmes) tirti bei pasiūlymams Centro direktoriui, kaip išvengti pažeidimų ateityje, teikti. Centras nuolat tobulina vidinius procesus, atsižvelgdama į nustatytas pažeidimų priežastis.

33. Atsižvelgiant į Ataskaitą, prireikus rengiamas Centro direktoriaus tvirtinamas priemonių planas, kuriame numatomos būtinos techninės, organizacinės, administracinės ir kitos priemonės, reikalingos užkirsti kelią pažeidimams, jų pasekmėms pašalinti ar sumažinti, nurodomi atsakingi priemonių vykdytojai ir įgyvendinimo terminai.

Susipažinau Janina Šeliutienė

33. Atsižvelgiant į Ataskaitą, prireikus rengiamas Centro direktoriaus tvirtinamas priemonių planas, kuriame numatomos būtinos techninės, organizacinės, administracinės ir kitos priemonės, reikalingos užkirsti kelią pažeidimams, jų pasekmėms pašalinti ar sumažinti, nurodomi atsakingi priemonių vykdytojai ir įgyvendinimo terminai.

____

Susipažinau · Janina Šeliutienė