PATVIRTINTA
Kėdainių pagalbos šeimai centro
Direktoriaus 2018 m. lapkričio 29 d.
įsakymu Nr. V-135
Pakeista
2020 m. birželio 10 d. direktoriaus
įsakymu V-192

PAŽEIDIMŲ APTIKIMO, SUSTABDYMO (PAŠALINIMO) IR PRANEŠIMO APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS KĖDAINIŲ PAGALBOS ŠEIMAI CENTRE TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie asmens duomenų saugumo pažeidimus Kėdainių pagalbos šeimai centre (toliau – Centras) tvarkos aprašas (toliau – Aprašas) nustato pažeidimų tyrimo, pranešimo apie juos ir dokumentavimo Kėdainių pagalbos šeimai centre tvarką ir sąlygas.

2. Pagal Aprašą Kėdainių pagalbos šeimai centro direktoriui (toliau - Duomenų valdytojas) teikiami pranešimai apie asmens duomenų saugumo pažeidimus (toliau – Pažeidimus), vykdant 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 – Reglamentas (ES) 2016/679) 33 straipsnyje numatytą pareigą (toliau – Pranešimas).

3. Šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679:

3.1. **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (BDAR 4 straipsnio 12 punktas).

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

4. Duomenų valdytojas ir duomenų tvarkytojas privalo informuoti darbuotojus apie jų pareigą pranešti apie galimus Pažeidimus ir supažindinti juos su nustatyta Pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie asmens duomenų saugumo pažeidimus Centre tvarka.

5. Procesai, kurių reikia laikytis įvykus ar pastebėjus Pažeidimus: (pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie asmens duomenų saugumo pažeidimus Centre taisyklių 2 priedas);

5.1. duomenų valdytojo ir duomenų tvarkytojo darbuotojas, sužinojęs ar pats nustatęs galimą Pažeidimą arba kai informacija apie galimą Pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio, privalo nedelsdamas (rekomenduotina ne ilgiau kaip per 24 val.) apie tai informuoti Duomenų valdytoją. Pranešimas gali būti pateikiamas raštu ar elektroninėmis priemonėmis. Pažeidimą pastebėjęs/padaręs darbuotojas užpildo Centro bendrųjų asmens duomenų apsaugos taisyklių 1 priede nustatytą informavimo apie pažeidimą formą.

5.2. Duomenų valdytojas nedelsiant (rekomenduotina ne ilgiau kaip per 24 val.) informuoja Centro Duomenų apsaugos pareigūną ir suteikia jam visą informaciją, susijusią su galimu Pažeidimu.

5.3. Duomenų apsaugos pareigūnas informaciją apie Pažeidimą įveda į Centro asmens duomenų pažeidimų žurnalą (toliau – Žurnalas) nedelsiant, kai tik nustatomas Pažeidimo faktas ir įvertinama rizika, raštu, įskaitant elektroninę formą (Kėdainių pagalbos šeimai centro bendrųjų asmens duomenų apsaugos taisyklių 1 priedas).

5.4. Duomenų apsaugos pareigūnas, įforminęs Pažeidimą ir tyrimo rezultatus, kartu su Duomenų valdytoju vykdo Pažeidimo analizę ir prevencijos priemonių įgyvendinimo kontrolę, t.y. peržiūrimi Žurnale esantys įrašai, atliekama Pažeidimų analizė ir prevencijos priemonių įgyvendinimas.

5.5. Nustačius, kad Pažeidimas buvo ir, kad yra rizika fizinių asmenų teisėms ir laisvėms, Duomenų valdytojas nedelsdamas, ne vėliau kaip per 72 val. nuo sužinojimo apie Pažeidimą, turi pranešti apie tai Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI).

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO EIGA

6. Duomenų apsaugos pareigūnas, sužinojęs apie galimą Pažeidimą, turėtų kaip įmanoma greičiau atlikti pirminį tyrimą, išsiaiškinti ir nustatyti, ar Pažeidimas iš tikrųjų įvyko, bei kokios galimos pasekmės asmenims (t. y. įvertinti riziką).

7. Galimi Pažeidimo tipai:

7.1. „Konfidencialumo Pažeidimas“ – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

7.2. „Prieinamumo Pažeidimas“ – kai netyčia arba neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;

7.3. „Vientisumo Pažeidimas“ – kai asmens duomenys pakeičiami be leidimo ar netyčia.

8. Priklausomai nuo aplinkybių, Pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

9. Priklausomai nuo Pažeidimo tipo, atliekant pirminį tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, turėtų būti išsaugomi esamos situacijos įrodymai bei vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės, pvz., duomenų srauto ir prisijungimų analizės įrankiai bei kt.

10. Vertinant riziką, kuri gali atsirasti dėl Pažeidimo, turėtų būti atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika turėtų būti vertinama atsižvelgiant į šiuos kriterijus:

10.1. pažeidimo tipą;

10.2. asmens duomenų pobūdį, apimtis (pvz., specialių kategorijų asmens duomenys);

10.3. kaip lengvai identifikuojamas fizinis asmuo;

10.4. pasekmių rimtumą fiziniams asmenims;

10.5. specialias fizinio asmens savybes (pvz., duomenys susiję su vaikais ar kitais pažeidžiamais asmenimis);

10.6. nukentėjusiųjų fizinių asmenų skaičių;

10.7. specialias duomenų valdytojo savybes (pvz., veiklos pobūdį).

11. Vertinant riziką, turėtų būti laikoma, kad Pažeidimas, galintis kelti pavojų asmenų teisėms ir laisvėms yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, 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, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

12. Įvertinus riziką rekomenduotina nustatyti, kad yra:

12.1. žema rizikos tikimybė;

12.2. vidutinė rizikos tikimybė;

12.3. didelė (aukšta) rizikos tikimybė.

13. Išvadą dėl Pažeidimo buvimo ir rizikos fizinių asmenų teisėms bei laisvėms įvertinimo duomenų apsaugos pareigūnas turėtų pateikti Duomenų valdytojui. Duomenų valdytojas turi priimti sprendimą dėl tolimesnių veiksmų, susijusių su Pažeidimu.

14. Už kompiuterių priežiūrą atsakingas darbuotojas (ar) kompiuterių/sistemų priežiūros paslaugas teikiantis subjektas visų pirma turėtų imtis visų tinkamų techninių, o Duomenų apsaugos pareigūnas organizacinių priemonių, kad Pažeidimas būtų išsamiai ištirtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų ir tuomet pateikti Pranešimą VDAI.

IV SKYRIUS
PRANEŠIMAS VALSTYBINEI DUOMENŲ APSAUGOS INSPEKCIJAI

15. Nustačius, kad Pažeidimas buvo ir, kad yra rizika fizinių asmenų teisėms ir laisvėms, Duomenų valdytojas nedelsdamas, **ne vėliau kaip per 72 val.** nuo sužinojimo apie Pažeidimą, turėtų pranešti apie tai VDAI.

16. Pranešimas apie asmens duomenų saugumo pažeidimą VDAI teikiamas vienu iš šių būdų:

16.1. per VDAI interneto svetainę www.vdai.lrv.lt naudojantis elektronine paslaugų sistema;

16.2. elektroninio pašto adresu ada@ada.lt;

16.3. paštu VDAI buveinės adresu;

16.4. VDAI faksu;

16.5. pateikiant pranešimą apie asmens duomenų saugumo pažeidimą VDAI.

17. Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie Pažeidimą VDAI, **rekomenduotina pranešti**.

18. Jeigu, priklausomai nuo Pažeidimo pobūdžio, Duomenų valdytojui yra būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su Pažeidimu (pvz., dar nėra išsiaiškinta Pažeidimo apimtis), ir per 72 val. nuo sužinojimo apie Pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, Pranešimui reikalinga informacija galėtų būti teikiama etapais. Esant galimybei, apie informacijos teikimą etapais, VDAI turėtų būti informuota teikiant pirminį Pranešimą.

19. Jeigu po Pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo jokio Pažeidimo, apie tai nedelsiant turėtų būti informuojama VDAI ir tai pažymėta Žurnale.

V SKYRIUS
PRANEŠIMAS DUOMENŲ SUBJEKTUI

20. Nustačius, kad Pažeidimas buvo ir, kad yra didelė rizika fizinių asmenų teisėms ir laisvėms, Duomenų apsaugos pareigūnas nedelsdamas (rekomenduojama per 72 val.) apie tai turėtų pranešti duomenų subjektui, kurio teisėms ir laisvėms dėl šio Pažeidimo gali kilti didelis pavojus.

21. VDAI informavimas apie Pažeidimą neatleidžia duomenų valdytojo nuo pareigos informuoti duomenų subjektą.

22. Pranešime duomenų subjektui aiškia ir paprasta kalba turėtų būti pateikiama (pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie asmens duomenų saugumo pažeidimus Centre taisyklių 3 priedas); :

22.1. pažeidimo pobūdžio aprašymas;

22.2. duomenų apsaugos pareigūno asmens vardas, pavardė ir kontaktiniai duomenys;

23.3. tikėtinų Pažeidimo pasekmių aprašymas;

23.4. priemonių, kurių ėmėsi arba pasiūlė imtis Duomenų valdytojas, kad būtų pašalintas Pažeidimas, įskaitant (kai tinkama) priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas (pvz., kad apie Pažeidimą yra informuota VDAI ir, kad yra gautas patarimas dėl Pažeidimo tvarkymo ir jo poveikio sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);

23.5. kita reikšminga informacija, susijusi su Pažeidimu, kuri, duomenų valdytojo manymu, turėtų būti pateikta duomenų subjektui.

24. Duomenų subjektai apie Pažeidimą turėtų būti informuoti tiesiogiai, pvz., siunčiant jiems pranešimą el. paštu, SMS, paštu ar pan.

25. Kai tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai daug pastangų, vietoj to apie įvykusį Pažeidimą gali būti paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai, pvz., pranešimas žinomos interneto svetainės antraštėje ar pranešimuose ar pan.

26. Duomenų valdytojas turėtų pasirinkti tokius pranešimo duomenų subjektui būdus, kurie maksimaliai didintų galimybę tinkamai pranešti informaciją visiems nukentėjusiems asmenims.

27. Esant Pažeidimui, pranešimo Duomenų subjektui teikti nereikia, jeigu:

27.1. Duomenų valdytojas įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikio;

27.2. iš karto po Pažeidimo duomenų valdytojas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus asmenų teisėms ir laisvėms;

27.3. tai pareikalautų neproporcingai daug pastangų susisiekti su asmenimis (pvz., kai jų kontaktiniai duomenys buvo prarasti dėl Pažeidimo arba pirma nežinomi). Tokiu atveju vietoj to apie Pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

VI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

28. Visi Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, turėtų būti registruojami Duomenų valdytojo Žurnale.

29. Informacija apie Pažeidimą į Žurnalą turėtų būti įvedama nedelsiant, kai tik nustatomas Pažeidimo faktas ir įvertinama rizika (rekomenduotina ne ilgiau kaip per 5 darbo dienas). Esant būtinybei, Žurnale esanti informacija turėtų būti papildoma ir (ar) koreguojama.

30. Žurnale turėtų būti nurodoma:

30.1. visi su Pažeidimu susiję faktai – Pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

30.2. pažeidimo poveikis ir pasekmės;

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

30.4. priežastys dėl su Pažeidimu susijusių sprendimų priėmimo (pvz., kodėl Duomenų valdytojas nusprendė nepranešti apie Pažeidimą VDAI ir (ar) duomenų subjektui, t. y. kodėl nusprendė, kad tikėtina, jog Pažeidimas negali sukelti pavojaus fizinių asmenų teisėms ir laisvėms, arba kokią sąlygą įvykdė, kuomet pranešti apie Pažeidimą duomenų subjektui nereikia);

30.5. pranešimo VDAI pateikimo vėlavimo priežastys (jeigu Pranešimą vėluojama pateikti ar Pranešimas teikiamas etapais);

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

30.7. žurnalas turėtų būti tvarkomas raštu, įskaitant elektronine formą, ir saugomas pagal duomenų valdytojo patvirtintą dokumentų saugojimo tvarką.

31. Rekomenduotina periodiškai peržiūrėti Žurnale esančius įrašus ir numatyti, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip bus kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje analogiški Pažeidimai nesikartotų.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

32. Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) apie asmens duomenų saugumo pažeidimą (toliau – Pažeidimas) Duomenų valdytojas privalo pranešti pateikdamas Pranešimą apie asmens duomenų saugumo pažeidimą (teisinė prievolė pranešti VDAI).

33. Duomenų valdytojas, nepateikęs pranešimo apie asmens duomenų saugumo pažeidimą VDAI atsako Reglamente (ES) 2016/679 nustatyta tvarka.

34. Tvarkos įgyvendinimo kontrolę vykdo Duomenų apsaugos pareigūnas.

35. Visi Centro darbuotojai su Tvarka supažindinami pasirašytinai. Tvarka skelbiama Centro internetinėje svetainėje adresu: https://kedainiupsc.lt

_____