PATVIRTINTA
Viešosios įstaigos Kelmės rajono pirminės sveikatos priežiūros centro direktoriaus 2022 m. lapkričio 7 d. įsakymu Nr. 05-03-171

DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau - Aprašas) reglamentuoja duomenų saugumo pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie juos įgyvendinimo tvarką viešojoje įstaigoje Kelmės rajono pirminės sveikatos priežiūros centre (toliau - Centras).

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 (toliau - Reglamentas) bei Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau - ADTAĮ), o Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente, ADTAĮ ir kituose Lietuvos Respublikos teisės aktuose.

3. Aprašas taikomas įgyvendinant Centro asmens duomenų saugumo pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie juos tvarką.

II SKYRIUS
DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

4. Asmens duomenų saugumo pažeidimu yra laikoma 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.

5. Centro darbuotojas, sužinojęs ar pats nustatęs galimą pažeidimą arba kai informacija apie galimą pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio, privalo nedelsdamas visais įmanomais būdais (įskaitant, tačiau neapsiribojant, žodžiu, raštu, telefonu, elektroniniu paštu) apie tai informuoti Centro informacinių technologijų specialistą (jeigu pažeidimas susijęs su elektroninės formos asmens duomenų tvarkymu bei Centro naudojamomis informacinėmis programomis) arba Centro sveikatos statistiką (jeigu pažeidimas susijęs su rašytinės formos asmens duomenų tvarkymu), kuris siekdamas nustatyti, ar iš tikrųjų įvyko asmens duomenų saugumo pažeidimas bei kokios galimos pasekmės duomenų subjektams, privalo imtis atitinkamų ir adekvačių

priemonių galimo duomenų saugumo pažeidimo tyrimui ir apie įvykusį asmens duomenų saugumo pažeidimą bei jo tyrimo rezultatus nedelsiant visais įmanomais būdais informuoti Centro direktorių bei duomenų apsaugos pareigūną (toliau - **Pareigūnas**).

6. Galimi asmens duomenų saugumo pažeidimo tipai: **konfidencialumo pažeidimas** (kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų), **prieinamumo pažeidimas** (kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba sunaikinami asmens duomenys) ir **vientisumo pažeidimas** (kai asmens duomenys pakeičiami be leidimo ar netyčia). Priklausomai nuo aplinkybių asmens duomenų saugumo pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

7. Priklausomai nuo asmens duomenų saugumo pažeidimo pobūdžio (tipo), atliekant pirminį tyrimą ir siekiant nustatyti, ar pažeidimas iš tikrųjų įvyko, turi būti išsaugomi esamos situacijos įrodymai bei vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės (pavyzdžiui, duomenų srauto ir prisijungimų analizės įrankiai bei kita).

8. Vertinant riziką, kuri gali atsirasti dėl asmens duomenų saugumo pažeidimo, turi būti atsižvelgiama į konkrečias asmens duomenų saugumo pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika turi būti vertinama remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus: asmens duomenų saugumo pažeidimo tipą bei pobūdį (pavyzdžiui, ypatingi asmens duomenys), apimtis, kaip lengvai identifikuojamas duomenų subjektas, pasekmių rimtumą duomenų subjektams, specialias duomenų subjekto savybes (pavyzdžiui, duomenys, susiję su vaikais ar kitais pažeidžiamais asmenimis), nukentėjusiųjų duomenų subjektų skaičių, Centro veiklos pobūdį.

9. Vertinant riziką, turi būti laikoma, kad asmens duomenų saugumo pažeidimas, galintis kelti pavojų duomenų subjektų teisėms ir laisvėms, yra toks, dėl kurio laiku nesiėmus tinkamų priemonių, duomenų subjektai gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą (pavyzdžiui, 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 laikomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam duomenų subjektui).

10. Įvertinus riziką, nustatoma: žema rizikos tikimybė, vidutinė rizikos tikimybė arba didelė (aukšta) rizikos tikimybė.

11. Už duomenų saugumo pažeidimų valdymą Centre atsakingi asmenys (t. y. Centro informacinių technologijų specialistas), visų pirma, turi imtis visų tinkamų techninių ir organizacinių priemonių, kad su Pareigūno pagalba asmens duomenų saugumo pažeidimas būtų išsamiai ištirtas ir

pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų.

12. Išvadą dėl asmens duomenų saugumo pažeidimo buvimo ir rizikos duomenų subjektų teisėms bei laisvėms įvertinimo atsakingas asmuo (t. y. Centro informacinių technologijų specialistas) turi nedelsiant pateikti Centro direktoriui bei Pareigūnui, kurie turi priimti sprendimą dėl tolimesnių veiksmų, susijusių su asmens duomenų saugumo pažeidimu.

13. Nustačius asmens duomenų saugumo pažeidimą, Centras imasi neatidėliotinų adekvačių priemonių užkertant kelią neteisėtam asmens duomenų tvarkymui. Įvertinus riziką, Centro direktorius, asmens duomenų saugumo pažeidimo atveju nepagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai sužino apie asmens duomenų saugumo pažeidimą, apie tai praneša Centro Pareigūnui bei Valstybinei duomenų apsaugos inspekcijai (toliau - Priežiūros institucija) ir / ar duomenų subjektams, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Jeigu Priežiūros institucijai apie asmens duomenų saugumo pažeidimą nepranešama per 72 valandas, pranešime nurodomos vėlavimo priežastys ir, jei įmanoma, pridedami nurodytas aplinkybes pagrindžiantys dokumentai. Pranešti apie asmens duomenų saugumo pažeidimą Priežiūros institucijai reikia net ir tuo atveju, jeigu įvertinus riziką yra abejojama, ar rizika yra ir ar reikia apie tai pranešti Priežiūros institucijai.

14. Pareigūnui sužinojus apie įvykusį asmens duomenų saugumo pažeidimą ar kitą incidentą, Pareigūnas nedelsiant įvertina su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgdamas į duomenų tvarkymo pobūdį, apimtį, kontekstą ir tikslus, bendradarbiaudamas kartu su Centro informacinių technologijų specialistu ir / ar Centro sveikatos statistiku pasiūlo Centrui sprendimus dėl priemonių, reikiamų asmens duomenų apsaugos pažeidimui ir jo padariniams pašalinti.

15. Centras fiksuoja bei dokumentuoja visus asmens duomenų saugumo pažeidimus, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kurių buvo imtasi taip, kad remdamasi tais dokumentais, Priežiūros institucija galėtų patikrinti, ar laikomasi šio reikalavimo.

16. Įvykusius duomenų saugumo pažeidimus Centro direktoriaus patvirtintos formos asmens duomenų saugumo pažeidimų registravimo žurnale registruoja Pareigūnas. Centro asmens duomenų saugumo pažeidimų registravimo žurnalas (1 priedas) yra pildomas elektronine forma, o jame esantys duomenų saugumo pažeidimų įrašai elektronine forma Centre yra saugomi 3 (trejus) metus po duomenų saugumo pažeidimo tyrimo pabaigos.

17. Asmens duomenų saugumo pažeidimų registravimo žurnale turi būti registruojami visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta Priežiūros institucijai ar ne. Informacija apie asmens duomenų saugumo pažeidimą į asmens duomenų saugumo pažeidimų registravimo žurnalą turi būti įvedama nedelsiant, bet ne vėliau kaip per 5 (penkias) darbo

dienas, kai tik nustatomas asmens duomenų saugumo pažeidimo faktas ir įvertinama rizika. Esant būtinybei, asmens duomenų saugumo pažeidimų registravimo žurnale esanti informacija turi būti papildoma ir / arba koreguojama.

18. Asmens duomenų saugumo pažeidimų registravimo žurnale turi būti nurodomi visi su asmens duomenų saugumo pažeidimu susiję faktai - pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti, pažeidimo poveikis ir pasekmės, taisomieji veiksmai (techninės priemonės), kurių buvo imtasi, priežastys dėl su asmens duomenų saugumo pažeidimu susijusių sprendimų priėmimo (pavyzdžiui, kodėl Centras nusprendė nepranešti apie asmens duomenų saugumo pažeidimą Priežiūros institucijai ir / ar duomenų subjektui), pranešimo Priežiūros institucijai pateikimo vėlavimo priežastys (jeigu pranešimą vėluojama pateikti arba pranešimas yra teikiamas etapais), informacija, susijusi su pranešimu duomenų subjektui (pavyzdžiui, ar buvo pranešta, kodėl nepranešta ir pan.), kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

19. Centras privalo periodiškai, bet ne rečiau kaip kartą per 1 (vienerius) metus, peržiūrėti asmens duomenų saugumo pažeidimų registravimo žurnale esančius įrašus ir numatyti, kokios prevencinės priemonės turi būti įgyvendinamos, kad ateityje analogiški asmens duomenų saugumo pažeidimai nesikartotų.

20. Pranešime Priežiūros institucijai apie asmens duomenų saugumo pažeidimą turi būti bent:

20.1. aprašytas asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;

20.2. nurodyta Pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;

20.3. aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

20.4. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis Centras, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones, galimoms neigiamoms jo pasekmėms sumažinti (pavyzdžiui, nurodyti, kad apie asmens duomenų saugumo pažeidimą yra informuota Priežiūros institucija ir kad yra gautas patarimas dėl asmens duomenų saugumo pažeidimo tvarkymo ir jo poveikio sumažinimo, duomenų subjektui buvo pasiūlyta pasikeisti slaptažodį ir pan.).

21. Kai ir jeigu informacijos neįmanoma pateikti Priežiūros institucijai tuo pačiu metu arba, priklausomai nuo asmens duomenų saugumo pažeidimo pobūdžio, Centrui yra būtina atlikti išsamesnį tyrimą ir nustatyti visas svarbias asmens duomenų saugumo pažeidimo aplinkybes ir per 72 valandas nuo sužinojimo apie asmens duomenų saugumo pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, pranešimui reikalinga informacija toliau nepagrįstai nedelsiant gali būti teikiama etapais. Esant galimybei, Centras privalo pateikti Priežiūros institucijai pirminį pranešimą bei informuoti apie tai, kad informacija apie asmens duomenų saugumo pažeidimą bus teikiama etapais.

22. Jeigu po pranešimo Priežiūros institucijai pateikimo, atlikus išsamesnį tyrimą yra nustatoma, kad asmens duomenų saugumo incidentas buvo sustabdytas ir faktiškai nebuvo jokio asmens duomenų saugumo pažeidimo, apie tai nedelsiant turi būti informuojama Priežiūros institucija ir tai pažymėta asmens duomenų saugumo pažeidimų registravimo žurnale.

23. Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, Centras nedelsiant turi pranešti apie tai ir duomenų subjektui. Pranešime duomenų subjektui aiškia ir paprasta kalba aprašomas asmens duomenų saugumo pažeidimo pobūdis ir pateikiama bent Aprašo 20 punkte nurodyta informacija ir priemonės bei kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu, kuri, Centro manymu, turėtų būti pateikta duomenų subjektui. Priežiūros institucijos informavimas apie asmens duomenų saugumo pažeidimą, neatleidžia Centro nuo pareigos informuoti duomenų subjektą.

24. Duomenų subjektai apie asmens duomenų saugumo pažeidimą turi būti informuoti tiesiogiai (pavyzdžiui, siunčiant jiems pranešimą elektroniniu paštu, trumpąją žinute, paštu ar pan.). Šis pranešimas turi būti atskirtas nuo kitos siunčiamos informacijos (pavyzdžiui, naujienlaiškiai ar standartiniai pranešimai).

25. Kai tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai daug pastangų, vietoj to, apie įvykusį asmens duomenų saugumo pažeidimą gali būti paskelbiama viešai visuomenės informavimo priemonėmis (pavyzdžiui, žiniasklaidoje, Centro interneto svetainėje ar pan.) pasirenkant tokį informavimo būdą, kuris maksimaliai didintų galimybę tinkamai pranešti informaciją visiems nukentėjusiems asmenims. Centras gali pasirinkti vieną arba kelis duomenų subjektų informavimo apie asmens duomenų saugumo pažeidimą būdus.

26. Pranešimas duomenų subjektui gali būti neteikiamas, jeigu įvykdomos bet kurios toliau nurodytos sąlygos:

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

26.2. Centras vėliau ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

26.3. tai pareikalautų neproporcingai daug pastangų; tokiu atveju vietoj to apie tai viešai paskelbiama arba taikoma panaši priemonė, kuria Duomenų subjektai būtų informuojami taip pat efektyviai.

27. Prireikus Centras turi sugebėti įrodyti Priežiūros institucijai, kad jis įvykdė bent vieną Aprašo 26 punkte nurodytų sąlygų.

28. Jeigu tiriant duomenų saugumo pažeidimą pradžioje nustatoma, kad nėra pavojaus

duomenų subjektų teisėms ir laisvėms, tačiau detalesnio duomenų saugumo pažeidimo tyrimo metu nustatoma, kad toks pavojus gali kilti, Centras privalo riziką vertinti iš naujo.

III SKYRIUS
BAIGIAMOSIOS NUOSTATOS

29. Už duomenų saugumo pažeidimų valdymą (įskaitant, tačiau neapsiribojant pirminį duomenų saugumo pažeidimo tyrimą (kada ir koks pažeidimas įvyko, kokie duomenys buvo pažeisti, kokie galimi neigiami padariniai, siūlomos priemonės pažeidimo padariniams sumažinti ir kt.) bei Pareigūno informavimą) Centre atsakingi informacinių technologijų specialistas (jeigu pažeidimas susijęs su elektroninės formos asmens duomenų tvarkymu bei Centro naudojamomis informacinėmis programomis) ir sveikatos statistikas (jeigu pažeidimas susijęs su rašytinės formos asmens duomenų tvarkymu).

30. Už asmens duomenų saugumo pažeidimų registravimo žurnalo pildymą Centre atsakingas Pareigūnas.

31. Už duomenų saugumo pažeidimų valdymą bei asmens duomenų saugumo pažeidimų registravimo žurnalo pildymą Centre atsakingi asmenys su Aprašu yra supažindinami pasirašytinai arba elektroninėmis priemonėmis ir privalo laikytis j o nuostatų bei atlikdami savo darbo funkcijas vadovautis Apraše nustatyta duomenų saugumo pažeidimų valdymo Centre tvarka.

32. Centras turi teisę iš dalies arba visiškai pakeisti Aprašą. Su Aprašo nuostatų pakeitimais už duomenų saugumo pažeidimų valdymą bei asmens duomenų saugumo pažeidimų registravimo žurnalo pildymą Centre atsakingi asmenys yra supažindinami pasirašytinai arba elektroninėmis priemonėmis.

ASMENS DUOMENŲ PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Su pažeidimu susiję faktai - pažeidimo priežastis (kas įvyko ir kokie asmens duomenys pažeisti)	Pažeidimo poveikis ir pasekmės	Taisomieji veiksmai (techninės priemonės), kurių buvo imtasi	Priežastys dėl su pažeidimu susijusių sprendimų priėmimo	Pranešimo VDAI pateikimo data arba pranešimo VDAI pateikimo vėlavimo priežastys	Informacija, susijusi su pranešimu duomenų subjektui	Kita informacija, susijusi su pažeidimu