

VIEŠOSIOS ĮSTAIGOS ROKIŠKIO RAJONO LIGONINĖS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKA

I. BENDROSIOS NUOSTATOS

1. Viešosios įstaigos Rokiškio rajono ligoninės asmens duomenų saugumo pažeidimų valdymo tvarka (toliau – **Tvarka**) reglamentuoja asmens duomenų saugumo pažeidimų identifikavimo, tyrimo ir kontrolės tvarką Įstaigoje ir yra taikoma visiems Įstaigos darbuotojams, dirbantiems su asmens duomenimis.
2. Ši Tvarka parengta remiantis Įstaigos asmens duomenų apsaugos politika ir yra neatsiejama jos dalis.
3. Visi Tvarkoje naudojami terminai ir sutrumpinimai yra suprantami taip, kaip jie yra išaiškinti Įstaigos asmens duomenų apsaugos politikoje.

II. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMAS IR ĮVERTINIMAS

4. Kiekvienas Įstaigos darbuotojas, kuris pastebėjo Informacijos saugumo incidentą, privalo nedelsdamas apie tai pranešti DAP ir Proceso šeimininkui, kuriam papildomai pateikiama su Informacijos saugumo incidentu susijusi informacija. Toks pranešimas turi pirmenybę prieš visas kitas atliekamas darbo funkcijas.
5. Jei gavus pirminę informaciją iš Duomenų subjekto, darbuotojo, žiniasklaidos, kito šaltinio arba tuo atveju, kai Įstaiga pati nustatė Informacijos saugumo incidentą, nėra aišku, ar asmens duomenys buvo pažeisti, tai yra, ar įvyko asmens duomenų saugumo pažeidimas, Proceso šeimininkas nedelsdamas ir per kuo trumpesnę laiką atlieka pradinį tyrimą, siekdamas nustatyti, ar asmens duomenys iš tikrųjų buvo pažeisti. Tyrimo laikotarpis nėra įskaitomas į terminą, nuo kurio tapo žinoma apie asmens duomenų saugumo pažeidimą.
6. Proceso šeimininkas gavęs pirminę informaciją apie Informacijos saugumo incidentą ir su juo susijusią reikšmingą informaciją:
 - 6.1. nedelsdamas inicijuoja pradinį Informacijos saugumo incidento tyrimo atlikimą, kad būtų surinkti reikiami įrodymai, ar Informacijos saugumo incidento metu galėjo kilti grėsmė asmens duomenų saugumui ir įvertinta rizika duomenų subjektų teisėms ir laisvėms bei pagal poreikį formuoja vidinę Informacijos saugumo incidento tyrimo bei padarinių šalinimo komandą;
 - 6.2. imasi visų įmanomų veiksmų (atsižvelgiant į technologines bei finansines galimybes) siekiant susigrąžinti prarastus asmens duomenis ir (arba) sumažinti Informacijos saugumo incidento metu asmens duomenims padarytą žalą;
 - 6.3. pagal poreikį kreipiasi į kitas valstybės institucijas (pavyzdžiui, Ryšių reguliavimo tarnybą);

6.4. pagal poreikį kreipiasi į trečiuosius asmenis, kurie galėtų suteikti pagalbą suvaldant Informacijos saugumo incidento padarinius (pavyzdžiui, informacinių technologijų įmones, apsaugos įmones, patalpų bei technikos priežiūros įmones);

6.5. ne vėliau kaip per 48 (keturiasdešimt aštuonias) valandas nuo tada, kai buvo sužinota apie Asmens duomenų saugumo pažeidimą, pateikia DAP pranešimą apie šį pažeidimą bei informaciją apie Asmens duomenų saugumo pažeidimą.

7. Laikoma, kad Įstaiga sužino apie Asmens duomenų saugumo pažeidimą, kai Įstaiga atlieka vidinį tyrimą ir konstatuoja Informacijos saugumo incidento buvimo faktą bei identifikuoja, kad jo metu buvo pažeistas Asmens duomenų saugumas.

8. DAP, gavęs Proceso šeimininko pateiktą pranešimą apie Asmens duomenų saugumo pažeidimą:

8.1. įvertina nustatytas aplinkybes ir Asmens duomenų saugumo pažeidimo pobūdį, prireikus, gauna papildomus paaiškinimus ir informaciją iš Proceso šeimininko;

8.2. vertina riziką Duomenų subjektų teisėms ir laisvėms ir atitinkamai identifikuoja poreikį apie šį pažeidimą pranešti Priežiūros institucijai ir Duomenų subjektams;

8.3. teikia rekomendacijas Įstaigos vadovybei dėl sprendimo pranešti apie Asmens duomenų saugumo pažeidimą Priežiūros institucijai ir Duomenų subjektams poreikio;

8.4. rengia pranešimus ir bendradarbiauja su Priežiūros institucija bei Duomenų subjektais;

8.5. registruoja visus Asmens duomenų saugumo pažeidimus registre.

III. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ RIZIKOS VERTINIMAS

9. Kai dėl Asmens duomenų saugumo pažeidimo gali kilti pavojus fizinių asmenų teisėms ir laisvėms, turi būti pranešama Priežiūros institucijai. Kai dėl Asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, papildomai turi būti pranešama ir Duomenų subjektui. Jeigu Asmens duomenų saugumo pažeidimas nekeltų pavojaus fizinių asmenų teisėms ir laisvėms, pranešimas dėl šio pažeidimo Priežiūros institucijai gali būti neteikiamas.

10. Pavojaus Duomenų subjekto teisėms ir laisvėms tikimybė ir rimtumas turėtų būti nustatomi atsižvelgiant į Asmens duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus. Pavojus turėtų būti vertinamas remiantis objektyviu įvertinimu, kurio metu nustatoma, ar Asmens duomenų tvarkymo operacijos yra susijusios su pavojumi arba dideliu pavojumi. Atliekant rizikos vertinimą reikėtų vertinti:

10.1. Asmens duomenų saugumo pažeidimo pobūdį (pavyzdžiui, prarasta prieiga prie Asmens duomenų ar prarasti patys Asmens duomenys);

10.2. Asmens duomenų pobūdį, jautrumą, apimtį (pavyzdžiui, kuo jautresni Asmens duomenys, tuo, tikėtina, kad rizika bus didesnė);

10.3. galimybę pagal Asmens duomenis identifikuoti asmenį (pavyzdžiui, susiejant juos su kitais duomenimis);

10.4. galimas pasekmes (pavyzdžiui, gali būti suklastotas asmens tapatybės dokumentas, prarastas Asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas);

10.5. Duomenų subjektų kategoriją (pavyzdžiui, kai Duomenų subjektai yra nepilnamečiai asmenys);

10.6. Duomenų subjektų kiekį (tikėtina, kad kuo didesnis paveiktų asmenų skaičius, tuo yra didesnė neigiamų pasekmių tikimybė).

11. Pasikeitus tam tikroms aplinkybėms, rizikos pobūdis ir poreikis atitinkamą riziką įvertinti bei priimti sprendimus dėl pranešimo Priežiūros institucijai ir Duomenų subjektams gali pasikeisti.

IV. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

12. Visi Asmens duomenų saugumo pažeidimai Įstaigoje turi būti dokumentuoti. Asmens duomenų saugumo pažeidimai registruojami nepriklausomai nuo to, ar apie Asmens duomenų saugumo pažeidimą bus pranešama Priežiūros institucijai ir Duomenų subjektams. Už Asmens duomenų saugumo pažeidimų registro pildymą yra atsakingas DAP. Asmens duomenų saugumo pažeidimo registre nurodoma ši informacija:

12.1. su Asmens duomenų saugumo pažeidimu susiję faktai;

12.2. Asmens duomenų saugumo pažeidimo poveikis;

12.3. veiksmai, kurių buvo imtasi, ir tokių sprendimų pagrindimas;

12.4. informacija, ar pranešta Priežiūros institucijai, jei nepranešta- tokio sprendimo pagrindimas;

12.5. informacija, ar pranešta Duomenų subjektui, jei nepranešta- tokio sprendimo pagrindimas;

12.6. Asmens duomenų saugumo pažeidimų pranešimų vėlavimo priežastys (jeigu vėluojama);

12.7. kita reikšminga informacija.

13. DAP ne rečiau kaip 1 (vieną) kartą per metus turi peržiūrėti įvykusius Asmens duomenų saugumo pažeidimus bei teikti Įstaigos vadovybei rekomendacijas dėl papildomų priemonių, kurių Įstaiga galėtų imtis tam, kad būtų užtikrintas didesnis Asmens duomenų saugumas.

V. PRANEŠIMŲ PRIEŽIŪROS INSTITUCIJAI TEIKIMO TVARKA

14. DAP privalo užtikrinti, kad apie Asmens duomenų saugumo pažeidimą būtų pranešama Priežiūros institucijai ne vėliau kaip per 72 (septyniasdešimt dvi) valandas nuo tada, kai Įstaigoje buvo sužinota apie Asmens duomenų saugumo pažeidimą.

15. Jei per trumpą laiką patiriami keli panašaus pobūdžio Asmens duomenų saugumo pažeidimai vienu metu paveikiant daug Duomenų subjektų, įvertinus šių pažeidimų mastą, gali būti rengiamas vienas bendras pranešimas apie šiuos pažeidimus, susijusius su tais pačiais Duomenų subjektais. Priežiūros institucijai turi būti nurodoma ši informacija:

15.1. aprašytas Asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų Duomenų subjektų kategorijas (pavyzdžiui, darbuotojai, klientai) ir apytikslį jų skaičių, taip pat Asmens duomenų kategorijas (pavyzdžiui, asmens tapatybės dokumentuose esantys duomenys, finansiniai duomenys);

15.2. nurodyti DAP bei kito asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

15.3. aprašytos tikėtinos Asmens duomenų saugumo pažeidimo pasekmės;

15.4. aprašytos priemonės, kurių Įstaiga ėmėsi arba planuoja imtis, kad būtų pašalintas Asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemonės Asmens duomenų saugumo pažeidimo galimoms neigiamoms pasekmėms sumažinti;

15.5. jeigu vėluojama pranešti per 72 (septyniasdešimt dvi) valandas nuo tada, kai buvo Įstaigoje buvo sužinota apie Asmens duomenų saugumo pažeidimą, nurodomos vėlavimo priežastys;

15.6. jeigu informacijos neįmanoma pateikti tuo pačiu metu, nurodoma, kad informacija bus teikiama etapais arba papildoma informacija bus pateikta vėliau;

15.7. pateikiama kita reikšminga informacija, pavyzdžiui, informacija apie Duomenų tvarkytojus.

VI. PRANEŠIMŲ DUOMENŲ SUBJEKTUI TEIKIMO TVARKA

16. Kai Asmens duomenų saugumo pažeidimas gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms, Duomenų valdytojas privalo nedelsdamas parengti pranešimą bei informuoti Duomenų subjektą apie Asmens duomenų saugumo pažeidimą, kad jis galėtų imtis reikiamų priemonių apsaugoti save ir savo Asmens duomenis.

17. Pranešime apie Asmens duomenų saugumo pažeidimą turėtų būti:

17.1. aprašytas Asmens duomenų saugumo pažeidimo pobūdis;

17.2. nurodyti DAP arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

17.3. aprašytos tikėtinos Asmens duomenų saugumo pažeidimo pasekmės;

17.4. aprašytos priemonės, kurių Įstaiga ėmėsi arba planuoja imtis, kad būtų pašalintas Asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemonės galimoms Asmens duomenų saugumo pažeidimo neigiamoms pasekmėms sumažinti;

17.5. pateiktos Duomenų subjektui skirtos rekomendacijos, kurios galėtų sumažinti neigiamą poveikį (pavyzdžiui, tam tikrų elektroninio pašto adresų siunčiamų laiškų blokavimas, slaptažodžių pakeitimas ir kiti veiksmai).

18. Duomenų subjekto informuoti nebūtina, jeigu Įstaiga įgyvendino tinkamas priemonės Asmens duomenims, kurių saugumas buvo pažeistas; Įstaiga po įvykusio Asmens duomenų saugumo pažeidimo ėmėsi priemonių, kuriomis užtikrino, kad pavojus nebekils; Duomenų subjekto informavimas pareikalautų neproporcingai daug pastangų ar resursų.

19. Duomenų subjektai, su kurių Asmens duomenimis susijęs Asmens duomenų saugumo pažeidimas, apie šį pažeidimą turi būti informuojami tiesiogiai, išskyrus atvejus, kai toks informavimas pareikalautų neproporcingai daug pastangų. Tokiu atveju gali būti naudojama vieša komunikacija. Pranešimai apie Asmens duomenų saugumo pažeidimus turi būti rengiami kaip atskiri pranešimai ir pateikiami Duomenų subjektui atskirai nuo kitų bet kokio pobūdžio pranešimų, kurie tuo pat metu yra teikiami Duomenų subjektui.

20. Priežiūros institucijos pranešimo apie Asmens duomenų saugumo pažeidimą rekomenduojama forma pateikiama Tvarkos priede Nr. 1.

VII. BAIGIAMOSIOS NUOSTATOS

21. Tvarka yra peržiūrima ir atnaujinama ne rečiau kaip 1 (vieną) kartą per metus arba pasikeitus teisės aktams, kurie reglamentuoja Asmens duomenų tvarkymą.

22. Įstaigos darbuotojai su šia Tvarka yra supažindinami pasirašytinai arba, esant techninėms galimybės, supažindinamas elektroninėmis priemonėmis ir privalo laikytis jos nuostatų.

23. Įstaiga turi teisę iš dalies arba visiškai pakeisti Tvarką. Su pakeitimais darbuotojai yra supažindinami pasirašytinai arba, esant techninėms galimybės, supažindinamas elektroninėmis priemonėmis.

(Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojama forma)

(duomenų valdytojo (juridinio asmens) pavadinimas, duomenų valdytojo atstovo pavadinimas,
duomenų valdytojo (fizinio asmens) vardas, pavardė)

(juridinio asmens kodas ir buveinės adresas arba fizinio asmens kodas, gimimo data (jeigu asmuo
neturi asmens kodo) ir asmens duomenų tvarkymo vieta)

(telefono ryšio numeris ir (ar) elektroninio pašto adresas, ir (ar) elektroninės siuntos pristatymo
dėžutės adresas)

Valstybinei duomenų apsaugos inspekcijai

**PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

_____ Nr. _____
(data) (rašto numeris)

1. Asmens duomenų saugumo pažeidimo apibūdinimas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:

Asmens duomenų saugumo pažeidimo:

Data _____ Laikas _____

Asmens duomenų saugumo pažeidimo nustatymo:

Data _____ 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

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

- Asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas)
- Asmens duomenų vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas)
- Asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas)

1.4. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:

1.5. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (atskiriamos pagal jai būdingą požymį):

1.6. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-as):

Asmens tapatybę patvirtinantis asmens duomenys (vardas, pavardė, amžius, gimimo data, lytis ir kt.):

Specialių kategorijų asmens duomenys (duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, sveikatos duomenys, duomenys apie lytinį gyvenimą ir lytinę orientaciją):

Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai (pavyzdžiui, asmens kodas, mokėtojo kodas, slaptažodžiai):

Kiti:

Nežinomi (pranešimo teikimo metu)

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

1.8. Kita duomenų valdytojo nuomone reikšminga informacija apie asmens duomenų saugumo pažeidimą:

2. Galimos asmens duomenų saugumo pažeidimo pasekmės

2.1. Konfidencialumo praradimo atveju:

- Asmens duomenų išplitimas labiau nei yra būtina ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pavyzdžiui, asmens duomenys išplito internete)
 - Skirtingos informacijos susiejimas (pavyzdžiui, gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)
 - Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pavyzdžiui, komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)
 - Kita
-
-
-
-

2.2. Vientisumo praradimo atveju:

- Pakeitimas į neteisingus duomenis dėl ko asmuo gali netekti galimybės naudotis paslaugomis
 - Pakeitimas į galiojančius duomenis, kad asmens duomenų tvarkymas būtų nukreiptas (pavyzdžiui, pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniiais duomenimis)
 - Kita
-
-
-
-

2.3. Duomenų prieinamumo praradimo atveju:

- Dėl asmens duomenų trūkumo negalima teikti paslaugų (pavyzdžiui, administracinių procesų sutrikdymas, dėl ko negalima prieiti, pavyzdžiui, prie asmens sveikatos istorijų ir teikti pacientams sveikatos paslaugų, arba įgyvendinti duomenų subjekto teises)
 - Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pavyzdžiui, asmens sveikatos istorijoje neliko informacijos apie asmens alergijas, tam tikra informacija iš mokesčių deklaracijos išnyko, dėl ko negalima tinkamai apskaičiuoti mokesčių ir pan.)
 - Kita
-
-
-
-

2.4. Kita:

3. Priemonės, kurių imtasi siekiant pašalinti pažeidimą ar sumažinti jo pasekmes

3.1. Taikytos priemonės siekiant sumažinti poveikį duomenų subjektams:

3.2. Taikytos priemonės siekiant pašalinti asmens duomenų saugumo pažeidimą:

3.3. Taikytos priemonės siekiant, kad pažeidimas nepasikartotų:

3.4. Kita:

4. Siūlomos priemonės sumažinti asmens duomenų saugumo pažeidimo pasekmėms

5. Duomenų subjektų informavimas apie asmens duomenų saugumo pažeidimą

5.1. Duomenys apie informavimo faktą:

- Taip, duomenų subjektai informuoti (nurodoma data) _____
- Ne, bet jie bus informuoti (nurodoma data) _____
- Ne

5.2. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, neinformavimo priežastys:

- Ne, nes nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodoma kodėl)
- Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami (nurodomos kokios)

Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos kokios)

Ne, nes tai pareikalautų neproporcingai daug pastangų ir apie tai viešai paskelbta (arba taikyta panaši priemonė) (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta)

Ne, nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas

5.3. Informacija, kuri buvo pateikta duomenų subjektams (gali būti pridėtas pranešimo duomenų subjektui kopija):

5.4. Būdas, koku duomenų subjektai buvo informuoti:

Paštu

Elektroniniu paštu

Kitu būdu _____

5.5. Informuotų duomenų subjektų skaičius _____

6. Asmuo galintis suteikti daugiau informacijos apie asmens duomenų saugumo pažeidimą (duomenų apsaugos pareigūnas ar kitas kontaktinis asmuo)

6.1. Vardas ir pavardė _____

6.2. Telefono ryšio numeris _____

6.3. Elektroninio pašto adresas _____

6.4. Pareigos _____

6.5. Darbovietės pavadinimas ir adresas _____

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

8. Kita reikšminga informacija

(vardas, pavardė, pareigos, parašas)