PATVIRTINTA
VšĮ Raseinių psichikos sveikatos centro
direktoriaus 2018 m. liepos 17 d.
įsakymu Nr. V-33

VIEŠOSIOS ĮSTAIGOS RASEINIŲ PSICHIKOS SVEIKATOS CENTRO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMO, SUSTABDYMO IR PRANEŠIMO APIE JUOS TVARKA

1. BENDROSIOS NUOSTATOS

1.1. Viešosios įstaigos Raseinių psichikos sveikatos centro (toliau – Centras) Asmens duomenų saugumo pažeidimų nustatymo, sustabdymo ir pranešimo apie juos tvarka (toliau – Tvarka) nustato reikalavimus, kaip Centre valdomi asmens duomenų saugumo pažeidimai.

1.2. Tvarka parengta vadovaujantis ES Bendrojo duomenų apsaugos reglamento Nr. (EU) 2016/679 (toliau – Reglamentas) ir kitų teisės aktų, reguliuojančių duomenų apsaugą ir tvarkymą, nuostatomis.

1.3. Tvarka taikoma ir yra privaloma Centrui bei visiems joje dirbantiems asmenims.

1.4. Tvarkoje vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Reglamente, ir kituose teisės aktuose.

1.5. Už asmens duomenų saugumo pažeidimų tyrimą, pranešimų Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektui teikimą, prevencinių priemonių įdiegimo kontrolę, asmens duomenų saugumo pažeidimų žurnalo pildymą ir kitų šioje tvarkoje numatytų funkcijų atlikimą Centre yra atsakingas IT specialistas (toliau – Atsakingas asmuo).

2. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI IR JŲ TYRIMAS

2.1. Asmens duomenų saugumo pažeidimu laikomas 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 (toliau – Pažeidimas).

2.2. Bet kuris Centro darbuotojas, sužinojęs ar pats nustatęs galimą Pažeidimą arba kai informacija apie galimą Pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio, privalo nedelsdamas apie tai informuoti Atsakingą asmenį. Informavimas gali būti atliekamas žodžiu, raštu ar elektroninėmis priemonėmis.

2.3. Atsakingas asmuo, sužinojęs apie galimą Pažeidimą, privalo nedelsiant atlikti pirminį tyrimą, išsiaiškinti ir nustatyti, ar Pažeidimas iš tikrųjų įvyko, bei kokios galimos pasekmės asmenims (t. y. įvertinti riziką).

2.4. Atlikęs pirminį Pažeidimo įvertinimą Atsakingas asmuo, atsižvelgdamas į pažeidimo rimtumą ir galimą poveikį duomenų subjekto teisėms, gali pasiūlyti Centre suformuoti pažeidimo tyrimo bei padarinių šalinimo komandą, į kurią galėtų būti įtraukti ir kiti darbuotojai, kurių darbo funkcijos susijusios su asmens duomenimis, kurių saugumas buvo pažeistas.

2.5. Priklausomai nuo Pažeidimo pobūdžio (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, pavyzdžiui, duomenų srauto ir prisijungimų analizės įrankiai bei kt.

2.6. 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 remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus:

2.6.1. Pažeidimo tipą;
2.6.2. Asmens duomenų pobūdį, apimtis (pavyzdžiui, specialių kategorijų asmens duomenys);
2.6.3. Kaip lengvai identifikuojamas duomenų subjektas;
2.6.4. Pasekmių rimtumą duomenų subjektams;
2.6.5. Specialias duomenų subjekto savybes (pavyzdžiui, duomenys susiję su vaikais ar kitais pažeidžiamais asmenimis);
2.6.6. Nukentėjusiųjų duomenų subjektų skaičių;
2.6.7. Asmens duomenų tvarkymo veiklos pobūdį.

2.7. Vertinant riziką, turėtų būti laikoma, kad Pažeidimas, galintis kelti pavojų asmenų 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 saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam duomenų subjektui.

2.8. Išvadą dėl Pažeidimo buvimo ir rizikos fizinių asmenų teisėms bei laisvėms įvertinimo Atsakingas asmuo turėtų pateikti Centro generaliniam direktoriui. Centro generalinis direktorius, pasitaręs su Atsakingu asmeniu ir duomenų apsaugos pareigūnu, turi priimti sprendimą dėl tolimesnių veiksmų, susijusių su Pažeidimu.

2.9. Atsakingas asmuo turėtų imtis visų tinkamų techninių ir organizacinių priemonių, kad Pažeidimas būtų išsamiai ištirtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų ir tuomet pateikti pranešimą Valstybinei duomenų apsaugos inspekcijai.

2.10. Atsakingas asmuo apie Pažeidimą turėtų informuoti duomenų apsaugos pareigūną bei laiku ir tinkamai teikti jam visą informaciją, susijusią su galimu Pažeidimu, taip pat konsultuojasi su duomenų apsaugos pareigūnu.

3. PRANEŠIMAS APIE PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

3.1. Nustačius, kad Pažeidimas buvo ir, kad yra rizika fizinių asmenų teisėms ir laisvėms, Atsakingas asmuo nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip per 72 valandoms nuo tada, kai buvo sužinota apie Pažeidimą, turėtų pranešti apie tai Valstybinei duomenų apsaugos inspekcijai.

3.2. Pranešime turi būti pateikiama ši informacija:

3.2.1. 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;
3.2.2. Nurodyta duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;
3.2.3. Aprašytos tikėtinos Pažeidimo pasekmės;
3.2.4. Aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis Centras, kad būtų pašalintas Pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

3.3. Jeigu, priklausomai nuo Pažeidimo pobūdžio, yra būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su Pažeidimu, ir per 72 valandas nuo sužinojimo apie Pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, Pranešimui reikalinga informacija galėtų būti teikiama etapais. Esant galimybei, apie informacijos teikimą etapais, Valstybinė duomenų apsaugos inspekcija turėtų būti informuota teikiant pirminį Pranešimą.

4. PRANEŠIMAS APIE PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

4.1. Nustačius, kad Pažeidimas buvo ir, kad yra didelė rizika fizinių asmenų teisėms ir laisvėms, Atsakingas asmuo nepagrįstai nedelsdamas apie Pažeidimą praneša duomenų subjektams, kurių teisėms ir laisvėms dėl šio Pažeidimo gali kilti didelis pavojus.
4.2. Pranešime duomenų subjektui aiškia ir paprasta kalba turėtų būti pateikiama:

4.2.1. Pažeidimo pobūdžio aprašymas;
4.2.2. Duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė (pavadinimas) ir kontaktiniai duomenys;
4.2.3. Tikėtinų Pažeidimo pasekmių aprašymas;
4.2.4. Priemonių, kurių ėmėsi arba pasiūlė imtis Centras, kad būtų pašalintas Pažeidimas, įskaitant (kai tinkama) priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas (pavyzdžiui, kad apie Pažeidimą yra informuota Valstybinė duomenų apsaugos inspekcija ir, kad yra gautas patarimas dėl Pažeidimo tvarkymo ir jo poveikio sumažinimo);
4.2.5. Kita reikšminga informacija, susijusi su Pažeidimu, kuri, Centro manymu, turėtų būti pateikta duomenų subjektui.

4.3. Duomenų subjektai apie Pažeidimą informuojami tiesiogiai, pavyzdžiui, siunčiant jiems pranešimą el. paštu, SMS, paštu ar pan. Šis pranešimas atskiriamas nuo kitos siunčiamos informacijos, tokios kaip nuolatiniai atnaujinimai, naujienlaiškiai ar standartiniai pranešimai.

4.4. Turėtų būti pasirinkami tokie pranešimo duomenų subjektui būdai, kurie maksimaliai didintų galimybę tinkamai pranešti informaciją visiems nukentėjusiems duomenų subjektams. Gali būti pasirenkami keli pranešimo duomenų subjektui apie Pažeidimą būdai.

4.5. Esant Pažeidimui, pranešimo duomenų subjektui teikti nereikia, jeigu:

4.5.1. Centras 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 asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemones;
4.5.2. Iš karto po Pažeidimo Centras ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus asmenų teisėms ir laisvėms;
4.5.3. Tai pareikalautų neproporcingai daug pastangų susisiekti su asmenimis (pavyzdžiui, 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.

4.6. Jeigu remiantis 4.5 punktu būtų nuspręsta nepranešti duomenų subjektams apie Pažeidimą, Centras turėtų turėti ir saugoti įrodymą apie 4.5 punkte numatytos sąlygos ar sąlygų egzistavimą.

5. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMAS

5.1. Visi Pažeidimai registruojami Asmens duomenų saugumo pažeidimų žurnale (toliau – Žurnalas), kurio forma pridedama prie šios Tvarkos kaip priedas Nr. 1.

5.2. Informacija apie Pažeidimą į Žurnalą įvedama nedelsiant, ne ilgiau kaip per 5 darbo dienas kai tik nustatomas Pažeidimo faktas ir įvertinama rizika, nebent egzistuotų pateisinamos priežastys informaciją įvesti per ilgesnį terminą. Esant būtinybei, Žurnale esanti informacija gali būti papildoma ir (ar) koreguojama.

5.3. Žurnale pateikiama ši informacija:

5.3.1. Informacijos įvedimo data;
5.3.2. Saugumo pažeidimo aprašymas – kas ir kada įvyko, priežastys, kokių duomenų subjektų ir kokių kategorijų duomenys pažeisti, pažeidimo poveikis ir pasekmės;
5.3.3. Pranešimas apie pažeidimą Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams – ar buvo pranešta, kodėl nepranešta, jeigu vėluojama – vėlavimo priežastys;
5.3.4. Taisomieji veiksmai, kurių imtasi pažeidimui ištaisyti, pavyzdžiui, techninės priemonės;
5.3.5. Kita su Pažeidimu susijusi reikšminga informacija.

5.4. Žurnale esantys įrašai reguliariai peržiūrimi siekiant įvertinti, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip bus kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje analogiški Pažeidimai nesikartotų.

6. BAIGIAMOSIOS NUOSTATOS

6.1. Šios Tvarkos sudėtinė dalis yra priedas Nr. 1 – Asmens duomenų saugumo pažeidimų žurnalas.

6.2. Pasikeitus šios Tvarkos nuostatoms, apie pakeitimus Centro darbuotojai informuojami elektroniniu paštu arba kitokia tvarka, nustatyta Centre.

6.3. Tvarka peržiūrima ir, reikalui esant, atnaujinama pasikeitus asmens duomenų apsaugą reglamentuojantiems teisės aktams ar jų įgyvendinimo praktikai, bet ne rečiau kaip kartą per vienerius metus.