PATVIRTINTA
Marijampolės profesinio rengimo centro
direktoriaus 2019 m. lapkričio 22 d.
įsakymu Nr. V1–146

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO IR REAGAVIMO Į JUOS TVARKOS APRAŠAS

I SKYRIUS. BENDROSIOS NUOSTATOS

1. Marijampolės profesinio rengimo centro (toliau – Marijampolės PRC), asmens duomenų saugumo pažeidimų valdymo ir reagavimo į juos tvarkos aprašo (toliau – Aprašas) tikslas – užtikrinti efektyvų Marijampolės PRC ir jo duomenų tvarkytojų reagavimą į galimą asmens duomenų saugumo pažeidimą, nustatyto asmens duomenų saugumo pažeidimo valdymą ir jo sukeltų padarinių šalinimą, siekiant kiek įmanoma sumažinti riziką duomenų subjektų teisėms ir laisvėms.

2. Aprašas parengtas vadovaujantis 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, BDAR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – ADTAĮ), kitais Lietuvos Respublikos teisės aktais, reglamentuojančiais saugų asmens duomenų tvarkymą ir apsaugą.

3. Apraše vartojamos sąvokos:

3.1. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti;

3.2. **Duomenų tvarkytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis.

3.3. **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;

3.4. **Duomenų subjektas** – fizinis asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius;

3.5. **VDAI** – Valstybinė asmens duomenų inspekcija;

3.6. **Atsakingas asmuo** – Marijampolės PRC direktoriaus įsakymu paskirtas Marijampolės PRC darbuotojas, kuris atsakingas už duomenų pažeidimų valdymą.

4. Kitos Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente, ADTAĮ ir kituose teisės aktuose, reguliuojančiuose asmens duomenų tvarkymą ir apsaugą.

II SKYRIUS. PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ PAŽEIDIMĄ MARIJAMPOLĖS PRC

5. Darbuotojai, turintys prieigos teisę prie asmens duomenų, sužinoję ar patys nustatę galimą asmens duomenų saugumo pažeidimą nedelsdami, bet ne vėliau kaip pažeidimo paaiškėjimo dieną, informuoja tiesioginį vadovą ir atsakingą už duomenų pažeidimų valdymą asmenį, suteikdami visą informaciją, susijusią su galimu pažeidimu. Pranešimas apie galimą pažeidimą pateikiamas žodžiu (tiesiogiai ar telefonu), raštu ar elektroniniu būdu. Nepagrįstas delsimas informuoti apie asmens duomenų saugumo pažeidimą laikomas šiurkščiu darbo pareigų pažeidimu.

6. Galimi asmens duomenų pažeidimo tipai:

6.1. konfidencialumo pažeidimas – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

6.2. prieinamumo pažeidimas – kai netyčia arba neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;

6.3. vientisumo pažeidimas – kai asmens duomenys pakeičiami be leidimo ar netyčia.

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

III SKYRIUS. GALIMO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS

8. Atsakingas asmuo, gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą, privalo nedelsiant:

8.1. apie galimą pažeidimą informuoti duomenų apsaugos pareigūną;

8.2. pradėti pirminį tyrimą dėl galimo asmens duomenų saugumo pažeidimo.

9. Atsakingas asmuo privalo imtis visų tinkamų techninių ir organizacinių priemonių, kad pažeidimas būtų išsamiai ištirtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų.

10. Galimi pažeidimo tipai:

10.1. konfidencialumo pažeidimas – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

10.2. prieinamumo pažeidimas – kai netyčia arba neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;

10.3. vientisumo pažeidimas – kai asmens duomenys pakeičiami be leidimo ar netyčia. Priklausomai nuo aplinkybių, pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

11. Tyrimo metu yra įvertinama gauta informacija, jos pakankamumas, patikimumas ir teisingumas. Vykdantis tyrimą Atsakingas asmuo gali pareikalauti darbuotojo, pateikusio informaciją, pateikti papildomus paaiškinimus, apklausti kitus darbuotojus, galinčius turėti informacijos apie galimą asmens duomenų saugumo pažeidimą, apklausti asmenį, dėl kurio veiksmų galimai kilo asmens duomenų saugumo pažeidimas, jei su šiuo asmeniu yra galimybė susisiekti, patikrinti fizinę vietą ar skaitmeninę erdvę, kurioje pastebėtas asmens duomenų saugumo pažeidimas arba apie jį sužinota.

12. 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.).

13. Vertinant riziką, kuri gali atsirasti dėl pažeidimo, turėtų būti atsižvelgiama į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą.

14. Rizika turėtų būti vertinama remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus:

14.1. pažeidimo tipą;

14.2. asmens duomenų pobūdį, apimtis (pavyzdžiui, specialių kategorijų asmens duomenys);

14.3. kaip lengvai identifikuojamas fizinis asmuo;

14.4. pasekmių rimtumą fiziniams asmenims;

14.5. specialias fizinio asmens savybes (pavyzdžiui, duomenys susiję su pažeidžiamais asmenimis);

14.6. nukentėjusiųjų fizinių asmenų skaičių;

14.7. specialias duomenų valdytojo savybes (pavyzdžiui, veiklos pobūdį).

15. 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, 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 fiziniam asmeniui.

16. Įvertinus riziką rekomenduotina nustatyti, kad yra:

16.1. žema rizikos tikimybė;

16.2. vidutinė rizikos tikimybė;

16.3. didelė (aukšta) rizikos tikimybė.

17. Tyrimas turi būti atliktas per 72 valandas nuo informacijos apie galimą asmens duomenų saugumo pažeidimą gavimo momento.

18. Baigus tyrimą, surašoma Galimo asmens duomenų saugumo pažeidimo tyrimo išvada (toliau tyrimo išvada), kurios pavyzdinė forma patvirtinta Aprašo 1 priede.

19. Išvadą dėl pažeidimo buvimo ir rizikos fizinių asmenų teisėms bei laisvėms įvertinimo Atsakingas asmuo privalo pateikti Marijampolės PRC direktoriui. Marijampolės PRC direktorius ar jo įgaliotas asmuo turi priimti sprendimą dėl tolimesnių veiksmų, susijusių su pažeidimu.

20. Reagavimo į galimą asmens duomenų saugumo pažeidimą, nustatyto asmens duomenų saugumo pažeidimo valdymo ir šalinimo procese dalyvauja ir duomenų apsaugos pareigūnas, pateikdamas pasiūlymus dėl asmens duomenų saugumo pažeidimo tyrimo ir nustatymo, valdymo, jo sukeltų padarinių šalinimo.

IV SKYRIUS. NUSTATYTO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO VALDYMAS IR ŠALINIMAS

21. Duomenų saugumo pažeidimai valdomi ir pažeidimo sukelti neigiami padariniai šalinami įgyvendinant tinkamas organizacines ir technines apsaugos priemones, pasiūlytas tyrimo išvadoje.

22. Jei asmens duomenų saugumo pažeidimo sukeltų padarinių pašalinti neįmanoma, taikomos organizacinės ir techninės apsaugos priemonės turi kiek įmanoma labiau sumažinti šiuos padarinius.

V SKYRIUS. PRANEŠIMAS VDAI APIE NUSTATYTĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

23. Jei tyrimo išvadoje buvo nustatyta, kad atitinkamas asmens duomenų saugumo pažeidimas kelia bet kurio lygio riziką duomenų subjektų teisėms ir laisvėms, Atsakingas asmuo nedelsdamas, bet ne vėliau kaip per 72 valandas, vadovaudamasis Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos apraše, patvirtintame Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. liepos 27 d. įsakymu Nr. 1T-72(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“, nustatyta tvarka ir sąlygomis, praneša Valstybinei duomenų apsaugos inspekcijai, pateikdamas užpildytą pranešimą pagal Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamą formą, patvirtintą Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“ (toliau – Pranešimas).

24. Jeigu, priklausomai nuo pažeidimo pobūdžio, yra būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su pažeidimu (pavyzdžiui, dar nėra

išsiaiškinta pažeidimo apimtis), ir per 72 valandas nuo sužinojimo apie pažeidimą dėl objektyvių aplinkybių pranešimo per nurodytą laikotarpį pateikti neįmanoma, Pranešimui reikalinga informacija turi būti teikiama etapais. Apie informacijos teikimą etapais, VDAI turėtų būti informuota teikiant pirminį Pranešimą.

25. 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.

26. Pranešimas VDAI nėra teikiamas, jeigu asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms.

27. Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie pažeidimą VDAI, pranešti vis vien privaloma.

28. Jeigu centras, veikdamas kaip duomenų tvarkytojas, sužino apie asmens duomenų saugumo pažeidimus, nedelsdami apie tai raštu praneša duomenų valdytojui. Marijampolės PRC, veikdamas kaip duomenų tvarkytojas, teikia pranešimą VDAI ir (ar) duomenų subjektams, jeigu turi duomenų valdytojo įgaliojimą arba jeigu tokia pareiga nustatyta sutartyje, kurios pagrindu duomenys yra tvarkomi.

VI SKYRIUS. PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE NUSTATYTĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

29. Jei tyrimo išvadoje buvo nustatyta, kad atitinkamas asmens duomenų saugumo pažeidimas kelia didelę riziką duomenų subjektų teisėms ir laisvėms, Atsakingas darbuotojas privalo pateikti duomenų subjektams, kurių teisėms ir laisvėms kyla didelė rizika, pranešimą apie Centre nustatytą asmens duomenų saugumo pažeidimą.

30. Pranešime duomenų subjektui aiškia ir paprasta kalba nurodoma ši informacija:

30.1. nustatyto asmens duomenų saugos pažeidimo aprašymas;

30.2. Centro duomenų apsaugos pareigūno ir Atsakingo asmens, atlikusio tyrimą, vardas pavardė ir kontaktiniai duomenys;

30.3. asmens duomenų saugumo pažeidimo neigiami padariniai, keliantys didelę riziką duomenų subjekto teisėms ir laisvėms;

30.4. organizacinių ir techninių apsaugos priemonių, kurios padėtų pašalinti arba kiek įmanoma sumažinti neigiamus padarinius duomenų subjekto teisėms ir laisvėms, aprašymas;

30.5. kita Marijampolės PRC manymu su asmens duomenų saugumo pažeidimu susijusi informacija, kuri turėtų būti pateikiama duomenų subjektui.

31. Pranešimas duomenų subjektui siunčiamas duomenų subjekto turimais kontaktiniais duomenimis.

32. Apie asmens duomenų saugumo pažeidimą duomenų subjektas informuojamas ne vėliau kaip per 72 valandas nuo sužinojimo apie galimą asmens duomenų saugumo pažeidimą momento. Jei, atsižvelgiant į asmens duomenų saugumo pažeidimo sudėtingumą, šio pažeidimo tyrimo bei įgyvendinamų organizacinių ir techninių apsaugos priemonių apimtis ir kitas objektyvias aplinkybes, duomenų subjekto informuoti per 72 valandas nėra galimybės, Atsakingas darbuotojas gali informuoti duomenų subjektą vėliau pranešime pateikdama vėlavimo priežastis.

33. Pranešimo duomenų subjektui teikti neprivaloma, jei egzistuoja bent viena iš žemiau nurodytų sąlygų:

33.1. Marijampolės PRC buvo įgyvendintos tinkamos organizacinės ir techninės apsaugos priemonės, kurios pašalino nustatyto asmens duomenų saugumo pažeidimo keliamus neigiamus padarinius duomenų subjekto teisėms ir laisvėms arba sumažino nustatyto asmens duomenų saugumo pažeidimo keliamą didelę riziką iki vidutinės ar žemos rizikos;

33.2. pranešimo teikimas duomenų subjektui iš Marijampolės PRC pareikalautų neproporcingų pastangų dėl asmens duomenų saugumo pažeidimo sudėtingumo, pažeidimo

tyrimo bei įgyvendinamų organizacinių ir techninių apsaugos priemonių apimties, duomenų subjektų, kurių teisėms ir laisvėms kilo didelė rizika, didelio skaičiaus ir kitų objektyvių aplinkybių. Tokiu atveju duomenų subjektui pranešimas yra teikiamas ne asmeniškai, o viešai, pasitelkiant žiniasklaidos ir kitas informacijos sklaidos priemones.

34. Dėl informavimo pareigos tinkamo vykdymo konsultuojamasi su duomenų apsaugos pareigūnu.

VII SKYRIUS. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMAS

35. Atsakingas darbuotojas visus asmens duomenų pažeidimus, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, registruoja Asmens duomenų saugumo pažeidimų registracijos žurnale (toliau – Žurnalas), kurio pavyzdinė forma pateikta Aprašo 2 priede.

36. Informacija apie pažeidimą į Žurnalą turėtų būti įvedama nedelsiant, bet ne vėliau kaip per 5 darbo dienas kai tik nustatomas pažeidimo faktas ir įvertinama rizika.

37. Esant būtinybei, Žurnale esanti informacija turėtų būti papildoma ir (ar) koreguojama.

38. Žurnale turi būti nurodoma:

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

38.2. pažeidimo poveikis ir pasekmės;

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

38.4. priežastys dėl su pažeidimu susijusių sprendimų priėmimo (pavyzdžiui, kodėl priimtas sprendimas nepranešti apie pažeidimą VDAI ir (ar) duomenų subjektui, t. y. kodėl nuspręsta, kad tikėtina, jog pažeidimas negali sukelti pavojaus fizinių asmenų teisėms ir laisvėms, arba kokia sąlyga įvykdyta, kuomet pranešti apie pažeidimą duomenų subjektui nereikia);

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

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

38.7. kita reikšminga informacija susijusi su pažeidimu (pavyzdžiui, kad tyrimo metu nustatyta, jog faktiškai pažeidimo nebuvo, o buvo tik saugumo incidentas).

39. Žurnalas Marijampolės PRC yra tvarkomas elektronine forma ir saugomas pagal centre patvirtintą dokumentų saugojimo tvarką.

VIII SKYRIUS. BAIGIAMOSIOS NUOSTATOS

40. Visi Marijampolės PRC darbuotojai, įgalioti tvarkyti asmens duomenis, ir Marijampolės PRC asmens duomenų tvarkytojai ir jų darbuotojai, paskirti tvarkyti Marijampolės PRC asmens duomenis, privalo laikytis šiame Apraše nustatytų reikalavimų.

_____

PRITARTA
Marijampolės profesinio rengimo centro
darbo tarybos pirmininkė

Aušra Krupavičienė
2019-11-

Asmens duomenų saugumo pažeidimų
Valdymo ir reagavimo į juos tvarkos
aprašo 1 priedas

MARIJAMPOLĖS PROFESINIO RENGIMO CENTRAS

GALIMO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO IŠVADA

20___ m. _____ d. Nr. ___

_____

(surašymo vieta)

Atlikto tyrimo metu asmens duomenų saugumo pažeidimas buvo (nustatytas/nenustatytas):

Eil. Nr.	**Sąlyga**	**Išvados**	**Pastabos**
1.	Asmens duomenų saugumo pažeidimo data ir laikas		
2.	Asmens duomenų saugumo pažeidimo nustatymo data ir laikas		
3.	Asmens duomenų saugumo pažeidimo tipas		
4.	Fizinė vieta arba skaitmeninė erdvė, kurioje užfiksuotas asmens duomenų saugumo pažeidimas		
5.	Asmens duomenų saugumo pažeidimo aprašymas		
6.	Duomenų subjektų, kurių teisėms ir laisvėms asmens duomenų saugumo pažeidimas sukėlė ar galėjo sukelti neigiamų padarinių, kategorijos ir sąrašas		
7.	Asmens duomenų, kurie buvo paveikti asmens duomenų saugumo pažeidimo, kategorijos ir sąrašas		

8.	Asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis (nenustatytas, žemas, vidutinis, didelis)		
9.	Nustatyti asmens duomenų saugumo pažeidimo sukelti arba tikėtini padariniai duomenų subjektų teisėms ir laisvėms		
10.	Priežastys, kodėl asmens duomenų saugumo pažeidimas nekelia rizikos duomenų subjektų teisėms ir laisvėms		
11.	Pasiūlymai dėl organizacinių ir techninių apsaugos priemonių, kurios padėtų pašalinti arba kiek įmanoma sumažinti neigiamus padarinius duomenų subjektų teisėms ir laisvėms		
12.	Pasiūlymai dėl prevencijos priemonių, padėsiančių ateityje išvengti tokių pačių ar panašių asmens duomenų saugumo pažeidimų		
13.	Kitos tyrimo metu nustatytos aplinkybės		

_____

(Tyrimo išvadą parengusio asmens vardas, pavardė, parašas)

Asmens duomenų saugumo pažeidimų
valdymo ir reagavimo į juos tvarkos aprašo
2 priedas

(Asmens duomenų saugumo pažeidimų žurnalo forma)

MARIJAMPOLĖS PROFESINIO RENGIMO CENTRAS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRACIJOS ŽURNALAS

Eil. Nr.	Pažeidimo nustatymo data, valanda ir vieta	Darbuotojas ar kitas subjektas, pranešęs apie pažeidimą (vardas, pavardė, pareigos)	Pažeidimo padarymo data ir vieta	Pažeidimo pobūdis, tipas, aplinkybės	Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius	Asmens duomenų, kurių saugumas pažeistas, kategorijos ir apimtis	Tikėtinos pažeidimo pasekmės bei pavojus fizinių asmenų teisėms ir laisvėms	Priemonės, kurių buvo imtasi pažeidimui pašalinti ir (ar) neigiamoms pažeidimo pasekmėms sumažinti	Darbuotojas, ar kitas subjektas, pašalinęs pažeidimą (vardas, pavardė, pareigos)	Informacija, ar apie pažeidimą buvo pranešta Valstybinei duomenų apsaugos inspekcijai, ir priimto sprendimo motyvai	Informacija, ar apie pažeidimą buvo pranešta duomenų subjektui (-ams), ir priimto sprendimo motyvai
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											

_____