PATVIRTINTA
Vilniaus technologijų ir inžinerijos mokymo centro direktoriaus 2025 m. kovo 27 d. įsakymu Nr. V1-155

VILNIAUS TECHNOLOGIJŲ IR INŽINERIJOS MOKYMO CENTRO REAGAVIMO Į ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS TVARKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Vilniaus technologijų ir inžinerijos mokymo centro reagavimo į asmens duomenų saugumo pažeidimus tvarkos (toliau – Tvarka) tikslas – nustatyti asmens duomenų saugumo pažeidimo, pranešimo apie jį kompetentingai priežiūros institucijai (o tam tikrais atvejais ir duomenų subjektams) ir dokumentavimo tvarką Vilniaus technologijų ir inžinerijos mokymo centre (toliau – TECHIN/Mokymo centras), siekiant įgyvendinti atskaitomybės principą.

2. Tvarka parengta 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 (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR).

3. Ši Tvarka taikoma Mokymo centro vykdomoje veikloje ir yra privaloma visiems darbuotojams.

4. Tvarkoje vartojamos sąvokos:

4.1. **Asmens duomenys** - bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (pavyzdžiui, vardas ir pavardė, asmens identifikavimo numeris, buvimo vietos duomenys ir interneto identifikatorius arba vienas ar keli to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymiai).

4.2. **Saugumo pažeidimas** - asmens duomenų 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.

4.3. **Duomenų subjektas** - fizinis asmuo, kurio asmens duomenis Mokymo centras tvarko.

4.4. **Duomenų tvarkymas** - bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.

4.5. **Duomenų tvarkytojas** - fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri Mokymo centro vardu tvarko asmens duomenis.

4.6. **Priežiūros institucija** - Valstybinė duomenų apsaugos inspekcija (toliau -VDAI).

II SKYRIUS
DUOMENŲ SAUGUMO PAŽEIDIMŲ IR JŲ PRIEŽASČIŲ KLASIFIKAVIMAS

5. Saugumo pažeidimai, kurie yra skirstomi pagal tris informacijos saugumo principus, klasifikuojami į:

5.1. Konfidencialumo pažeidimas – kai yra be leidimo (nesankcionuotai) ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

5.2. Prieinamumo pažeidimas – kai netyčia arba neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;

5.3. Vientisumo pažeidimas – kai asmens duomenys pakeičiami be leidimo (nesankcionuotai) ar netyčiniais naudotojų veiksmais.

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

7. Pažeidimai gali būti nulemti šių priežasčių:

7.1. netyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas neturint tikslo tai padaryti (dėl duomenų tvarkymo klaidos, informacijos laikmenų, duomenų įrašų ištrynimo, sunaikinimo ar sistemų sutrikimų dėl elektros tiekimo nutrūkimo, įvykusio dėl asmens veiklos, kompiuterinio viruso, paskleisto dėl asmens veiklos, vidaus taisyklių pažeidimo, sistemos priežiūros trūkumo, programinės įrangos testų atlikimo, netinkamos duomenų laikmenų priežiūros, netinkamo ryšio linijų pajėgumo ir apsaugos nustatymo, kompiuterių integravimo į tinklą, netinkamos kompiuterinių programų apsaugos parinkimo ir kt.);

7.2. tyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas sąmoningai turint tikslą tai padaryti (neteisėtas įsibrovimas į asmens duomenų tvarkytojo patalpas, asmens duomenų laikmenų saugyklas, informacines sistemas, kompiuterių tinklą, tyčinis nustatytų taisyklių tvarkant asmens duomenis pažeidimas, sąmoningas kompiuterinio viruso platinimas, asmens duomenų vagystė, neteisėtas naudojimasis kito Mokymo centro darbuotojo teisėmis ir kt.);

7.3. *force majeure* ir kiti netikėti įvykiai, kurių negalima kontroliuoti, numatyti ir užkirsti kelio jų atsiradimui (žaibas, gaisras, potvynis, užliejimas, audros, elektros instaliacijos degimas, temperatūros ir (ar) drėgmės pakitimų poveikis, purvo, dulkių ir magnetinių laukų įtaka, techninės avarijos ir kt.).

III SKYRIUS
REAGAVIMAS Į SAUGUMO PAŽEIDIMUS

8. Kiekvienas Mokymo centro darbuotojas, įtaręs, supratęs ar sužinojęs, jog buvo padarytas ar įvykęs saugumo pažeidimas, nedelsiant:

8.1. tą pačią darbo dieną ne vėliau kaip per 2 darbo valandas nuo galimo pažeidimo paaiškėjimo momento žodžiu, raštu ar elektroninėmis priemonėmis informuoja savo tiesioginį vadovą;

8.2. užpildo „Pranešimą apie galimą asmens duomenų saugumo pažeidimą“ Priedas Nr.1, ir nedelsdamas, bet ne vėliau kaip per 4 darbo valandas nuo galimo pažeidimo paaiškėjimo momento, perduoti jį per DVS ir elektroniniu paštu Mokymo centro direktoriui ir duomenų apsaugos pareigūnui.

8.3. Nurodytame pranešime turi būti:

8.3.1. įvardinti kokie asmens duomenys buvo pažeisti;

8.3.2. 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;

8.3.3. nurodyta kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė ir kontaktiniai duomenys;

8.3.4. aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

8.3.5. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis Mokymo centras, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant priemones galimoms neigiamoms jo pasekmėms sumažinti;

8.4. jei įmanoma, imasi priemonių pašalinti saugumo pažeidimą ir (ar) priemonių sumažinti jo sukeltas neigiamas pasekmes.

IV SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

9. Mokymo centro direktorius, gavęs darbuotojo pranešimą apie asmens duomenų saugumo pažeidimą, nedelsdamas nagrinėja pranešime nurodytas aplinkybes ir sudaro darbo grupę asmens duomenų saugumo pažeidimui tirti.

10. Darbo grupė, tirdama asmens duomenų saugumo pažeidimą:

10.1. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

10.2. jei saugumo pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkia mokyklos IT specialistus ir/ar informacinių sistemų saugos specialistus;

10.3. jei asmens duomenų saugumo pažeidimas padarytas, nustato pažeidimo pobūdį, priežastis, asmens duomenų kategorijas, jų pobūdį ir kiekį, duomenų subjektų kategorijas ir jų kiekį, įvertina padarytą žalą fiziniams asmenims bei tikėtinas pažeidimo pasekmes;

10.4. įvertina, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas saugumo pažeidimas (pvz., naudoti atsargines kopijas, siekiant atkurti prarastus ar sugadintus duomenis ar kt.);

10.5. nustato, ar apie saugumo pažeidimą būtina pranešti VDAI;

10.6. nustato, ar būtina nedelsiant pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą.

11. Mokymo centro darbuotojai, atsakingi už asmens duomenų tvarkymą, pateikia darbo grupei visą jos prašomą informaciją, susijusią su asmens duomenų saugumo pažeidimu ir tyrimu, per jos nurodytą terminą.

12. Atliekant asmens duomenų saugumo pažeidimo tyrimą ir siekiant nustatyti, ar pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas.

13. Vertinant rizikos lygį, atsižvelgiama į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:

13.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis, nuo kurio gali priklausyti pavojaus duomenų subjektams dydis;

13.2. asmens duomenų pobūdis, jautrumas ir kiekis – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautrumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavojus;

13.3. galimybė identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiems asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, todėl pažeidimas padarys mažesnį poveikį duomenų subjektams);

13.4. fizinio asmens specifiniai ypatumai – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavojus, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalią turintys asmenys), tuo didesnį poveikį pažeidimas gali jiems padaryti;

13.5. nukentėjusių duomenų subjektų skaičius – nustatomas nukentėjusių asmenų skaičius: kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnis žalos pavojus;

13.6. pasekmės, sukeltos fiziniams asmenims – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumas; taip pat atsižvelgiama į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis.

14. Įvertinus riziką nustatomas vienas iš trijų rizikos lygių – mažas, vidutinis ar didelis rizikos tikimybės lygis:

14.1. maža rizika, kai nustatoma, kad pavojaus duomenų subjekto teisėms ir laisvėms nėra;

14.2. vidutinė rizika, kai nustatoma, kad dėl asmens duomenų saugumo pažeidimo yra arba gali kilti nedidelis pavojus duomenų subjektų teisėms ir laisvėms;

14.3. didelė rizika, kai nustatoma, kad dėl asmens duomenų saugumo pažeidimo yra arba gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms.

15. Mokymo centro darbo grupė, atlikusi asmens duomenų saugumo pažeidimo tyrimą, užpildo Asmens duomenų saugumo pažeidimo tyrimo ataskaitą, Priedas Nr.2.

16. Išvadą dėl pažeidimo buvimo ir rizikos fizinių asmenų teisėms bei laisvėms įvertinimo darbo grupė pateikia Mokymo centro direktoriui, kuris priima sprendimą dėl tolimesnių veiksmų, susijusių su pažeidimu.

17. Atsižvelgiant į Asmens duomenų saugumo pažeidimo tyrimo ataskaitą, Mokymo centro direktorius, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl saugumo pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

18. Sprendžiant asmens duomenų saugumo pažeidimo pašalinimo klausimą ir tvirtinant priemonių planą, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą. Priklausomai nuo konkrečių pažeidimo aplinkybių, reikia atlikti tokius veiksmus, kaip: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamojo ar mobiliojo įrenginio (telefono, nešiojamojo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuriam jie buvo skirti, kuo skubiau kreiptis į jį su prašymu ištrinti atsiųstus asmens duomenis be galimybės juos atkurti; pakeisti prisijungimo prie duomenų bazės ar informacinės sistemos vardus ir slaptažodžius, jeigu jie tapo žinomi tretiesiems asmenims; atkuriant prarastus ar sugadintus asmens duomenis, naudoti atsargines kopijas ir kt.

19. Siekiant apriboti ar sustabdyti asmens duomenų saugumo pažeidimą, būtina kiek įmanoma tiksliau surinkti duomenis ir įrodymus apie įvykusį saugumo incidentą (pvz., kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės ar informacinės sistemos, kam per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su asmens duomenimis ir kt.).

20. Priemonių plane turi būti numatytos prevencinės ir kitos priemonės, užtikrinančios, kad pažeidimas nepasikartotų.

V SKYRIUS
PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

21. Saugumo pažeidimo atveju Mokymo centro direktorius arba jo įgaliotas už duomenų saugumo pažeidimų tyrimą atsakingas darbuotojas/duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 (septyniasdešimt dviem) valandoms nuo tada, kai sužinojo apie saugumo pažeidimą, apie tai praneša priežiūros institucijai (VDAI). Informacija apie pranešimo būdus bei pranešimo forma pasiekiama adresu: https://vdai.lrv.lt/lt/adsp-ir-dap/pranesimas-apie-asmens-duomenu-saugumo-pazeidima/

22. Tais atvejais, kai Mokymo centro direktorius ir už duomenų saugumo pažeidimų tyrimą atsakingas darbuotojas/duomenų apsaugos pareigūnas, įvertinę (galimo) saugumo pažeidimo pobūdį ir keliamą riziką, nusprendžia, kad saugumo pažeidimas nekelia ir ateityje nesukels pavojaus duomenų subjektų teisėms ir laisvėms, apie tokį saugumo pažeidimą priežiūros institucijai nepranešama.

23. Jeigu priežiūros institucijai apie saugumo pažeidimą nepranešama per 72 (septyniasdešimt dvi) valandas nuo tada, kai Mokymo centras sužinojo apie saugumo pažeidimą, prie pranešimo turi būti pridedamos vėlavimo priežastys.

24. Tvarkos 21 punkte nurodytame pranešime apie saugumo pažeidimą turi būti bent:

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

24.2. nurodyta Mokymo centro paskirto atsakingo darbuotojo, galinčio suteikti daugiau informacijos, vardas bei pavardė ir kontaktiniai duomenys;

24.3. aprašytos tikėtinos saugumo pažeidimo pasekmės;

24.4. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis Mokymo centras, kad būtų pašalintas saugumo pažeidimas, įskaitant, priemones galimoms neigiamoms jo pasekmėms sumažinti.

25. Jeigu visos 24 punkte nurodytos informacijos Mokymo centras negali pateikti priežiūros institucijai pranešimo pateikimo metu, informacija apie saugumo pažeidimą toliau nedelsiant gali būti teikiama etapais. Informacijos teikimas etapais yra pateisinamas sudėtingesnių pažeidimų atveju (pavyzdžiui, kai kuriems kibernetinio saugumo incidentams), kai gali būti reikalingas nuodugnus

tyrimas, siekiant išsamiai nustatyti saugumo punktuose nustatyta tvarka pažeidimo pobūdį ir tai, kokiu mastu asmens duomenys buvo pažeisti.

26. Pateikęs pradinį pranešimą Mokymo centras bet kuriuo metu gali informuoti priežiūros instituciją (VDAI) apie tolesniame tyrime atskleistus įrodymus, jog jokio saugumo pažeidimo faktiškai nebuvo. Tokiu atveju ši papildoma informacija yra įtraukiama į pradinę informaciją, kuri jau buvo pateikta priežiūros institucijai, ir incidentas atitinkamai nėra laikomas saugumo pažeidimu.

VI SKYRIUS
PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

27. Tais atvejais, kai dėl saugumo pažeidimo gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, Mokymo centro direktorius ar jo įgaliotas asmuo/duomenų apsaugos pareigūnas nedelsdamas turi pranešti apie tokį saugumo pažeidimą ir patiems duomenų subjektams (paštu, elektroniniu paštu, telefonu ar kitu būdu), kad šie galėtų imtis visų įmanomų priemonių apsisaugoti nuo neigiamų padarinių. Laikoma, kad didelis pavojus duomenų subjektų teisėms gali kilti tuomet, jei dėl incidento duomenų subjektai gali patirti materialinę ar nematerialinę žalą, pavyzdžiui, prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai atstatyta pradinė informacija panaikinus pseudonimus, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

28. Tvarkos 27 punkte nurodytame pranešime duomenų subjektams aiškiai aprašomas saugumo pažeidimo pobūdis ir pateikiama bent Tvarkos 24.2-24.4 punktuose nurodyta informacija ir priemonės.

30. Tvarkos 27 punkte nurodyto pranešimo duomenų subjektams nereikalaujama, jeigu įvykdomos bet kurios toliau nurodytos sąlygos:

31.1. Mokymo centras įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems saugumo pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad neturint leidimo susipažinti su asmens duomenimis nebūtų galimybės juos panaudoti (pavyzdžiui, naudojant šifravimą);

31.2. Mokymo centras toliau ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

31.3. tai pareikalautų neproporcingai daug pastangų. Tokiu atveju apie tai paskelbiama viešai (pavyzdžiui, naujienų portale, Mokymo centro interneto svetainėje ar kitomis žiniasklaidos priemonėmis) arba duomenų subjektui informuoti taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai (pavyzdžiui, el. paštu ar trumposiomis SMS žinutėmis).

32. Jeigu Mokymo centras dar nėra pranešęs duomenų subjektams apie saugumo pažeidimą, tačiau priežiūros institucija, apsvarsčiusi, kokia yra tikimybė, kad dėl saugumo pažeidimo kils didelis pavojus, pareikalauja tai padaryti, Mokymo centras praneša duomenų subjektams 27 punkte nustatyta tvarka.

VII SKYRIUS
SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

33. Visi pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, registruojami asmens duomenų saugumo pažeidimų registravimo žurnale (toliau - Žurnalas), Priedas Nr.3. Informacija apie pažeidimą į Žurnalą įvedama nedelsiant, kai tik nustatomas pažeidimo faktas ir įvertinama rizika. Žurnale esanti informacija papildoma ir/ar koreguojama.

34. Prie kiekvieno saugumo pažeidimo kortelės turi būti pridedama įvykusio saugumo pažeidimo analizė, kurioje nurodomi veiksmai, kuriuos vykdant siekiama išvengti analogiškų saugumo pažeidimų ateityje.

35. Žurnale nurodomi:

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

35.2. Pažeidimo poveikis ir pasekmės;

35.3. Taisomieji veiksmai (techninės priemonės), kurių buvo imtasi;

35.4. Priežastys dėl su pažeidimu susijusių sprendimų priėmimo;

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

35.6. Informacija, susijusi su pranešimu duomenų subjektui;

35.7. Kita reikšminga informacija susijusi su pažeidimu.

36. Žurnalas tvarkomas raštu, įskaitant elektroninę formą, ir saugomas 5 (penkis) metus pagal patvirtintą dokumentų saugojimo tvarką. Žurnalą tvarkant elektronine forma, naikinami senesni nei 5 (penkerių) metų įrašai.

VIII SKYRIUS
ATSAKOMYBĖ

37. Jei dėl saugumo pažeidimo laiku nesiimama tinkamų priemonių, duomenų subjektai gali patirti materialinę ar nematerialinę žalą, pavyzdžiui, prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai atstatyta pradinė informacija panaikinus pseudonimus, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

38. Mokymo centro nustatytos tvarkos, nustatančios reagavimo į saugumo pažeidimus nesilaikymas, yra laikomas darbo tvarkos pažeidimu, už kurį darbuotojui gali būti taikoma atsakomybė.

39. Darbuotojams, kurie pažeidžia Reglamentą ar kitus teisės aktus, reglamentuojančius reagavimo į saugumo pažeidimus, gali būti taikomos minėtuose teisės aktuose numatytos atsakomybės priemonės.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

40. Šios Tvarkos laikymosi stebėsena ir kontrolė atliekama nuolat.

41. Ši Tvarka peržiūrima ne rečiau kaip kartą per 2 (dvejus) metus arba atitinkamoms institucijoms, kaip kad VDAI priėmus naujus reglamentuojančius teisės aktus.

42. Ši Tvarka gali būti pakeista ar panaikinta bet kuriuo metu atskiru Mokymo centro direktoriaus įsakymu.

43. Darbuotojai supažindinami su šia Tvarka ir pakeitimais skelbiant ją Mokymo centro svetainėje.

Reagavimo į asmens duomenų saugumo pažeidimus tvarkos
1 priedas

(Pranešimo apie galimą asmens duomenų saugumo pažeidimą forma)

_____
(juridinio asmens / strultūrinio padalinio pavadinimas)

_____
(pareigų pavadinimas)

_____
(vardas, pavardė)

PRANEŠIMAS
APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____
Vilnius

Informuoju apie galimą asmens duomenų saugumo pažeidimą, pateikdamas man turimą informaciją apie jį:

1. Galimo asmens duomenų saugumo pažeidimo nustatymo data, valanda (minučių tikslumu) ir vieta: _____
2. Galimo asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta: _____
_____
3. Galimo asmens duomenų saugumo pažeidimo pobūdis, esmė ir aplinkybės _____
_____
_____
4. Duomenų subjektų, kurių asmens duomenų saugumas galimai pažeistas, kategorijos (pvz., darbuotojai, asmenys, pateikę prašymus, skundus ir pan.) ir jų skaičius (jei žinoma) _____
_____
_____
5. Asmens duomenų kategorijos, susijusios su galimu asmens duomenų saugumo pažeidimu:

5.1. Asmens duomenys:

Vardas	
Pavardė	
Asmens kodas	
Adresas	
Telefono ryšio numeris	
Elektroninio pašto adresas	
Banko sąskaitos numeris	
Banko kortelės numeris	
Prisijungimo duomenys (vartotojo vardas, slaptažodis)	
Asmens dokumento (-ų) duomenys	
Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas	
Kiti duomenys	

5.2. Specialių kategorijų asmens duomenys

Duomenys, susiję su asmens sveikata	
Biometriniai duomenys	
Duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais	
Duomenys, susiję su asmens naryste profesinėse sąjungose	
Duomenys, susiję su asmens rasine ar etnine kilme	
Duomenys, susiję su asmens lytiniu gyvenimu ir lytine orientacija	

6. Kokių veiksmų/priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti kompiuterio slaptažodžiai, nutraukta neteisėta prieiga prie tvarkomų asmens duomenų, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimui skirtoje vietoje palikti dokumentai su asmens duomenimis ir pan.) _____
_____
_____
_____

_____ _____ _____
(pareigos) (parašas) (vardas ir pavardė)

Reagavimo į asmens duomenų saugumo pažeidimus tvarkos
2 priedas

(Asmens duomenų saugumo pažeidimo ataskaitos forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

_____ Nr. _____

1. Asmens duomenų saugumo pažeidimo (toliau – pažeidimas) aprašymas	
1.1. Pažeidimo nustatymo data, laikas (minučių tikslumu) ir vieta	
1.2. Darbuotojas, pranešęs apie pažeidimą (vardas, pavardė, struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas, telefono Nr., elektroninio pašto adresas)	
1.3. Duomenų tvarkytojo, pranešusio apie pažeidimą, pavadinimas, jo kontaktinio asmens duomenys (vardas, pavardė, telefono Nr., elektroninio pašto adresas)	
1.4. Pažeidimo padarymo data ir vieta	
1.5. Pažeidimo pobūdis (tipas), esmė ir aplinkybė	
1.5.1. Konfidencialumo pažeidimas	
1.5.2. Vientisumo pažeidimas	
1.5.3. Prieinamumo pažeidimas	
1.5.4. Mišraus pobūdžio (tipo) pažeidimas	
1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir jų skaičius	
1.7. Kaip ilgai tęsėsi pažeidimas?	
1.8. Asmens duomenų kategorijos, susijusios su pažeidimu:	
1.8.1. Asmens duomenys	
1.8.2. Specialių kategorijų asmens duomenys	
1.9. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius	
2. Pažeidimo rizikos įvertinimas	
2.1. Priežastys, lėmusios pažeidimą, ar įvykiai, kurie galėjo turėti įtakos pažeidimo padarymui	
2.2. Pažeidimo pasekmės:	
2.2.1. Sunaikinti asmens duomenys	
2.2.2. Prarasti asmens duomenys	
2.2.3. Pakeisti asmens duomenys	
2.2.4. Be duomenų subjekto sutikimo atskleisti asmens duomenys	
2.2.5. Sudaryta galimybė naudotis asmens duomenimis	
2.2.6. Asmens duomenys, išplitę labiau nei tai yra būtina, ir prarasta duomenų subjekto kontrolė savo asmens duomenų atžvilgiu	
2.2.7. Asmens duomenų susiejimas	
2.2.8. Asmens duomenų panaudojimas neteisėtais tikslais	
2.2.9. Dėl asmens duomenų trūkumo negalima teikti paslaugų	
2.2.10. Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamų paslaugų	
2.2.11. Kita	
2.3. Dėl pažeidimo nėra pavojaus duomenų subjektų teisėms ir laisvėms (maža rizika)	
2.4. Dėl pažeidimo yra / gali kilti pavojus duomenų subjektų teisėms ir laisvėms (būtina pranešti Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) (vidutinė rizika)	
2.5. Dėl pažeidimo yra / gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms (būtina pranešti Inspekcijai ir duomenų subjektams) (didelė rizika)	
2.6. Kas turėjo prieigą prie pažeistų asmens duomenų iki asmens duomenų saugumo pažeidimo padarymo?	

2.7. Kas gavo prieigą prie pažeistų asmens duomenų (jei pažeidimas yra, ar apima asmens duomenų prieinamumo pažeidimą)?	
2.8. Ar iki pažeidimo asmens duomenys buvo tinkamai užkoduoti, anonimizuoti ar kitaip lengvai neprieinami?	
2.9. Informacinės sistemos, įrenginiai, įranga, įrašai, susiję su pažeidimu	
2.10. Ar pažeidimas yra sisteminė klaida, ar vienetinis incidentas?	
2.11. Kokia žala buvo padaryta duomenų subjektams, kurių asmens duomenų saugumas pažeistas, ar Mokymo centrui?	
2.12. Kokių veiksmų / priemonių buvo imtasi sužinojus apie padarytą pažeidimą?	
2.13. Kokios taikytos priemonės, siekiant sumažinti ir (ar) pašalinti pažeidimo pasekmes duomenų subjektams?	
2.14. Kokios techninės ir (ar) organizacinės priemonės buvo taikomos pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?	
2.15. Techninės ir (ar) organizacinės priemonės, kurios įgyvendintos dėl pažeidimo, siekiant, kad pažeidimas nepasikartotų	
2.16. Techninės ir (ar) organizacinės priemonės, kurios ketinamos įgyvendinti dėl pažeidimo, įskaitant ir priemones sumažinti pažeidimo pasekmes	
3. Pranešimų pateikimas	
3.1. Ar pranešta duomenų subjektui apie pažeidimą:	
3.1.1. Taip	(Pranešimo turinys ir data)
3.1.2. Ne	
3.2. Jei buvo teikiamas pranešimas duomenų subjektams:	
3.2.1. Pranešimo duomenų subjektui būdas (paštu, elektroninio pašto pranešimu ar SMS pranešimu ir kt.)	
3.2.2. Informuotų duomenų subjektų skaičius	
3.2.3. Vėlavimo pranešti duomenų subjektui apie pažeidimą priežastys	
3.3. Nepranešimo apie pažeidimą duomenų subjektui priežastys:	
3.3.1. Nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos priežastys)	
3.3.2. TECHIN ir (ar) duomenų tvarkytojas įgyvendino tinkamas technines ir organizacines asmens duomenų apsaugos priemones, kurios užtikrino, kad įvykus pažeidimui nekils rizika, ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio (nurodoma, kokios)	
3.3.3. iš karto po pažeidimo TECHIN ir (ar) duomenų tvarkytojas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti rizika (nurodoma, kokios)	
3.3.4. Reikėtų neproporcingai daug pastangų susisiekti su duomenų subjektais. Informacija apie pažeidimą buvo paskelbta viešai arba taikyta panaši priemonė, kuria duomenų subjektai buvo informuoti taip pat efektyviai (nurodoma, kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma, kokia ir kada taikyta)	
3.3.5. Dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas	
3.4. Ar pranešta Inspekcijai apie asmens duomenų saugumo pažeidimą:	
3.4.1. Taip	(rašto data ir numeris)
3.4.2. Ne	
3.5. Vėlavimo pranešti Inspekcijai apie pažeidimą priežastys	
3.6. Nepranešimo apie pažeidimą Inspekcijai priežastys	

3.7. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie pažeidimą, galimai turintį nusikalstamos veikos požymių:	
3.7.1. Taip	(rašto data ir numeris, adresatas)
3.7.2. Ne	
3.8. Ar pranešta valstybės institucijoms, nurodytoms Lietuvos Respublikos kibernetinio saugumo įstatyme, apie kibernetinį incidentą, susijusį su pažeidimu:	
3.8.1. Taip	(rašto data ir numeris, adresatas)
3.8.2. Ne	
Mokymo centro duomenų apsaugos pareigūnas	(vardas, pavardė, parašas)

_____

Reagavimo į asmens duomenų saugumo
pažeidimus tvarkos
3 priedas

Asmens duomenų saugumo pažeidimų registravimo žurnalas

Eil. Nr.	Asmens duomenų saugumo pažeidimas[1]	Asmens duomenų saugumo pažeidimo poveikis[2]	Taisomieji veiksmai[3]	Informacija, ar buvo pateiktas pranešimas Valstybinei duomenų inspekcijai ir duomenų subjektams[4]	Priežastys ir argumentai, kodėl pranešimas Valstybinei duomenų inspekcijai ir (ar) duomenų subjektams nebuvo pateiktas[5]

[1] Šioje skiltyje pateikiama: 1) laikas ir data, kada pažeidimas įvyko, kada pažeidimas buvo užfiksuotas, kada apie pažeidimą sužinojo Techin, 2) pažeidimo faktinės aplinkybės, 3) pažeidimo pobūdis, 4) pažeidimo priežastys.

[2] Šioje skiltyje pateikiama: 1) asmens duomenų ir asmens duomenų subjektų kategorija, susijusi su pažeidimu, 2) asmens duomenų, susijusių su pažeidimu, apimtis, 3) realus ar galimas pažeidimo poveikis ir jo padariniai duomenų subjektų teisėms ir laisvėms (fiziniai, materialiniai ir nematerialiniai padariniai).

[3] Šioje skiltyje pateikiama: 1) priemonės ir veiksmai, kurių buvo imtasi siekiant ištaisyti asmens duomenų pažeidimą ir jo padarinius, 2) priemonės ir veiksmai, kurių buvo imtasi siekiant užkirsti kelią ar sumažinti pažeidimo poveikį duomenų subjektams, 3) priemonėmis ir veiksmais pasiekti rezultatai.

[4] Šioje skiltyje pateikiama: 1) ar buvo teiktas pranešimas Valstybinei duomenų inspekcijai ir duomenų subjektams, 2) pranešimo data, (3) pranešimo pateikimo būdas.

[5] Ši skiltis pildoma tuomet, jeigu Valstybinei duomenų inspekcijai ir (ar) duomenų subjektui nebuvo teiktas pranešimas dėl asmens duomenų saugumo pažeidimo. Šioje skiltyje nurodomos priežastys, argumentai, nuorodos į dokumentus ir tyrimo rezultatus, kurie pagrindžia, kad: 1) asmens duomenų saugumo pažeidimas nekelia pavojaus duomenų subjektų teisėms ir laisvėms – kai pranešimas nėra teikiamas nei Valstybinei duomenų inspekcijai, nei duomenų subjektams, 2) asmens duomenų saugumo pažeidimas negali sukelti didelio pavojaus duomenų subjektų teisėms ir laisvėms – kai pranešimas yra teikiamas Inspekcijai, bet nėra teikiamas duomenų subjektams.