PATVIRTINTA
Rektoriaus 2021-12-15
įsakymu Nr. 1-044

KLAIPĖDOS UNIVERSITETO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REAGAVIMO TVARKOS APRAŠAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Šis asmens duomenų saugumo pažeidimų reagavimo tvarkos aprašas (toliau tekste – **Aprašas**) parengtas įgyvendinant 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (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 tekste – **BDAR**), taip pat vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau tekste – **ADTAĮ**), 2017 m. spalio 3 d. 29 straipsnio duomenų apsaugos darbo grupės patvirtintomis gairėmis dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą 2016/679, 2018 m. liepos 2 d. Valstybinės duomenų apsaugos inspekcijos (toliau tekste – **Inspekcija**) rekomendacija dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos, 2018 m. liepos 27 d. Inspekcijos direktoriaus įsakymo Nr. 1T-72(1.12.E) Dėl pranešimo apie asmens duomenų saugumo pažeidimą pateikimo valstybinei duomenų apsaugos inspekcijai tvarkos aprašu bei kitais asmens duomenų apsaugą reglamentuojančiais teisės aktais ir jų išaiškinimais.
2. Apraše naudojamos sąvokos:
2.1. **Įstaiga –** VšĮ „Klaipėdos universitetas“, juridinio asmens kodas 211951150;
2.2. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra 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;
2.3. **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;
2.4. **Duomenų apsaugos pareigūnas –** asmuo, įstaigoje paskirtas atsakingu už duomenų apsaugą ir kurio statusą reglamentuoja BDAR 37-39 straipsniai;
2.5. **Kontaktinis asmuo** – paskirtas asmuo, palaikantis kontaktą su duomenų apsaugos pareigūnu ir padedantis jam spręsti visus įvykusius ADSP;
2.6. **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 (toliau tekste – **ADSP**);
2.7. **Kibernetinė ataka** – elektroninėje erdvėje pavienių asmenų arba organizacijų vykdomas informacinių sistemų, infrastruktūros objektų, kompiuterių tinklų, asmeninių kompiuterių puolimas įvairiomis kenkėjiškomis priemonėmis.
3. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos BDAR bei kituose asmens duomenų tvarkymą ir apsaugą reglamentuojančiuose teisės aktuose.

II SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

4. ADSP yra laikomi, įskaitant, bet neapsiribojant, šie atvejai:

4.1. informacijos, kurioje yra asmens duomenų, atskleidimas asmeniui, neturinčiam teisės jos žinoti (pavyzdžiui.: *per pietų pertrauką darbuotojas A papasakojo darbuotojui B tam tikrą darbo metu sužinotą informaciją, kartu atskleidžiant ir trečiojo asmens vardą, pavardę bei gyvenamąją vietą, kuri buvo aktuali žinoti tik darbuotojui A pagal jo darbines funkcijas*);

4.2. informacijos, kurioje yra asmens duomenų, per klaidą išsiuntimas ne tam adresatui (pavyzdžiui.: *darbuotojas per klaidą išsiuntė tam tikrus dokumentus, kuriuose buvo asmens duomenų, ne savo kolegai, o trečiajam asmeniui*);

4.3. informacijos sunaikinamas ar pakeitimas, neturint tam leidimo ar atliekant tai pažeidžiant teisės aktų ar įstaigos vidaus tvarkų reikalavimus (pavyzdžiui.: *darbuotojas ištrynė darbiniame kompiuteryje saugotą informaciją, kurioje buvo asmens duomenų ir kurios naikinti jis neturėjo teisės*);

4.4. duomenų laikmenos arba bet kokios kitos duomenims laikyti skirtos įrangos praradimas, kai šiuose įrenginiuose esama bet kokių su įstaigos veikla susijusių asmens duomenų (pavyzdžiui.: *darbuotojas pametė įstaigos USB atmintuką, kuriame buvo asmens duomenų*);

4.5. popierinių dokumentų, kuriuose buvo asmens duomenų, praradimas arba vagystė (pavyzdžiui.: *iš įstaigos patalpų buvo pavogti dokumentai, kuriuose buvo įstaigos darbuotojų asmens duomenų*);

4.6. aptikimas kibernetinės atakos, įskaitant virusų egzistavimo, požymių, dėl ko įvyksta ADSP (pavyzdžiui.: *darbuotojas darbo metu pastebėjo, kad jo kompiuteris veikia gerokai lėčiau nei turėtų, todėl atliko papildomą antivirusinės programos skanavimą jo kompiuteryje, kurio metu buvo aptikti pavojingi virusai*);

4.7. aptikimas langų, durų ar kitų vietų, pro kurias galima patekti į patalpas, kuriose yra saugomi svarbiausi įstaigos veiklos asmens duomenys, sugadinimus ar kitokias modifikacijas bei pakeitimus, dėl kurių būtų apsunkintas arba padaromas neįmanomas priėjimas prie asmens duomenų (pavyzdžiui.: *kabineto, kuriame buvo saugomi svarbiausi įstaigos asmens duomenys, durų spynos sugadinimas*);

4.8. kiti veiksmai ar neveikimas, kuriais būtų padaromi informacijos konfidencialumo pažeidimai (kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų), prieinamumo pažeidimai (kai netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba jie yra sunaikinami) ar vientisumo pažeidimai (kai asmens duomenys pakeičiami be leidimo ar netyčia). Priklausomai nuo konkrečių aplinkybių, ADSP tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

5. Įstaigos darbuotojas, pastebėjęs ADSP ar pats padaręs veiką, dėl kurios įvyko ADSP, privalo nedelsdamas, tačiau ne vėliau nei per 2 valandas nuo sužinojimo apie šį ADSP ar jo padarymo, informuoti apie tai savo tiesioginį vadovą ir duomenų apsaugos pareigūną (šie subjektai nustatę, kad iš tiesų įvyko duomenų apsaugos pažeidimas, informuoja apie tai įstaigos rektorių). Įvykus ADSP, atliekamas šio incidento tyrimas, dokumentavimas bei priimamas sprendimas ar informuoti apie šį ADSP Inspekciją bei duomenų subjektą.

6. Duomenų apsaugos pareigūno kontaktiniai duomenys, kuriais būtų galima informuoti duomenų apsaugos pareigūną apie nutikusį ADSP, yra nurodomi įstaigos privatumo politikoje, kuri yra viešai skelbiama įstaigos internetinėje svetainėje.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS

7. Duomenų apsaugos pareigūnas, spręsdamas įvykusi ADSP, bendradarbiauja su kontaktiniu asmeniu, taip pat su kitais įstaigos darbuotojais, tiesiogiai ar netiesiogiai susijusiais su šiuo pažeidimu ar gebančiais užkirsti ar sumažinti dėl jo nutikimo galinčių kilti pasekmių mastą ar

kitaip padėti jį spręsti. Nepriklausomai nuo šių darbuotojų vykdomų tiesioginių darbo funkcijų, jie privalo bendradarbiauti su duomenų apsaugos pareigūnu, teikiant jam visą reikalingą pagalbą ADSP sprendimo eigoje.

8. Priklausomai nuo pažeidimo pobūdžio, atliekant pirminį tyrimą bei siekiant nustatyti, ar ADSP iš tiesų įvyko, privaloma išsaugoti visus esamos situacijos įrodymus.
9. Duomenų apsaugos pareigūnas, vertindamas riziką, kuri gali atsirasti dėl nutikusio ADSP, turi atsižvelgti į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę bei rimtumą, taip pat įvertinti žemiau nurodytas aplinkybes:
9.1. pažeidimo tipą (koks būtent ADSP įvyko);
9.2. Asmens duomenų pobūdį bei apimtis (ar tai buvo paprasti, ar specialių kategorijų asmens duomenys, kiek duomenų buvo prarasta ir panašiai);
9.3. kaip lengvai identifikuojamas fizinis asmuo (ar po nutikusio ADSP neįmanoma atsekti kokių fizinių asmenų duomenys buvo prarasti ar tiesiog pasunkėja šių asmenų identifikavimas, tačiau atsekamumas įmanomas);
9.4. pasekmių rimtumą (vertinami įvairūs scenarijai, kas galėtų nutikti, jeigu duomenys patektų į „blogas rankas“);
9.5. specialias fizinio asmens savybes (ar duomenys susiję su vaikais, ar kitais labiau pažeidžiamais asmenimis);
9.6. nukentėjusių fizinių asmenų skaičių;
9.7. specialias duomenų valdytojo savybes (veiklos pobūdį).
10. Atlikus rizikos vertinimą, turėtų būti laikoma, kad ADSP gali kelti pavojų asmenų teisėms ir laisvėms tuomet, jeigu dėl jo nesiėmus tinkamų saugumo priemonių fiziniai asmenys gali patirti kūno sužalojimus (pavyzdžiui.: *informacija apie fizinį asmenį patenka į rankas asmenims, ketinantiems šį fizinį asmenį reketuoti ir to pasėkoje galimai sužaloti, siekiant iš to gauti turtinę naudą*), materialinę žalą (pavyzdžiui.: *prarandami prisijungimai prie banko sąskaitų*) ar neturtinę žalą (pavyzdžiui.: *buvo neteisėtai atskleista informacija apie fizinio asmens sveikatos būklę, kurią fizinis asmuo slėpė nuo visuomenės*).
11. Po atlikto ADSP vertinimo, duomenų apsaugos pareigūnas, esant įstaigos rektoriaus pritarimui, privalo priimti sprendimą koks būtent ADSP įvyko. Žemiau pateikiami trys pažeidimų laipsniai, kurių konstatavimas sukelia skirtingas pasekmes:
11.1. ***žema rizikos tikimybė*** – ADSP neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Konstatavus šį ADSP laipsnį, apie ADSP nei Inspekcijai, nei duomenų subjektams pranešimai nėra teikiami;
11.2. ***vidutinė rizikos tikimybė*** **-** ADSP kelia nedidelį pavojų fizinių asmenų teisėms ir laisvėms. Konstatavus šį ADSP laipsnį, apie ADSP yra informuojama Inspekcija;
11.3. ***didelė rizikos tikimybė*** **-** ADSP kelia didelį pavojų fizinių asmenų teisėms ir laisvėms. Konstatavus šį ADSP laipsnį, apie ADSP yra informuojama ir Inspekcija, ir duomenų subjektai, kurių teisėms ir laisvėms iškilo grėsmė dėl įvykusio ADSP.
12. Atsižvelgiant į tai, koks buvo priimtas sprendimas dėl įvykusio ADSP laipsnio, t. y. ar buvo nustatyta žema rizikos tikimybė, ar buvo nustatyta vidutinė rizikos tikimybė, ar buvo nustatyta didelė rizikos tikimybė, duomenų apsaugos pareigūnas vadovaujasi tolimesniais šio Aprašo skyriais bei vykdo juose nustatytas procedūras, įskaitant privalomą kiekvieno įvykusio ADSP dokumentavimą ADSP registravimo žurnale (Priedas Nr. 2).

IV SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

13. Tuo atveju, jeigu duomenų apsaugos pareigūnas, turėdamas įstaigos rektoriaus pritarimą, nustato, jog įstaigoje įvyko žemos rizikos ADSP, šis ADSP yra dokumentuojamas Aprašo V skyriuje nustatyta tvarka ir apie jį nėra informuojama nei Inspekcija, nei duomenų subjektai.
14. Tuo atveju, jeigu duomenų apsaugos pareigūnas, turėdamas įstaigos rektoriaus pritarimą, nustato, jog įstaigoje įvyko vidutinės rizikos ADSP, šis ADSP yra dokumentuojamas V

skyriuje nustatyta tvarka ir apie jį yra pranešama Inspekcijai, pateikiant pranešimą pagal prie šio Aprašo pridėtą formą (Priedas Nr. 1).

15. Tuo atveju, jeigu duomenų apsaugos pareigūnas, turėdamas įstaigos rektoriaus pritarimą, nustato, jog įstaigoje įvyko didelės rizikos ADSP, šis ADSP yra dokumentuojamas V skyriuje nustatyta tvarka ir apie jį yra pranešama ir Inspekcijai, pateikiant pranešimą pagal prie šio Aprašo pridėtą formą (Priedas Nr. 1), ir duomenų subjektams, pateikiant jiems laisva forma (elektroniniu paštu, registruotu paštu ar kitokiu pasirinktu būdu) šią informaciją:

15.1. aprašomas ADSP pobūdis;

15.2. nurodomas duomenų apsaugos pareigūno vardas, pavardė ir kiti kontaktiniai duomenys;

15.3. aprašomos tikėtinos ADSP pasekmės;

15.4. aprašomos priemonės, kurių buvo ar bus imtasi, kad būtų pašalintos arba sumažintos šio pažeidimo sukeltos neigiamos pasekmės.

16. Įvykus didelės rizikos ADSP, pranešimo duomenų subjektams teikti nereikia, jeigu yra įvykdoma bet kuri iš žemiau nurodytų sąlygų:

16.1. duomenų valdytojas 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;

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

16.3. 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.

17. Parengtą pranešimą Inspekcijai, duomenų apsaugos pareigūnas privalo iš anksto suderinti su įstaigos rektoriumi ir, tik gavęs jo pritarimą, jį pasirašyti ir išsiųsti Inspekcijai kuo anksčiau, tačiau ne vėliau nei per 72 valandas nuo tada, kai buvo sužinota apie ADSP. Jeigu yra vėluojama Inspekcijai pateikti informaciją apie ADSP, tuomet pranešime yra nurodomos šio vėlavimo priežastys.

18. Jeigu Inspekcijai pranešimu yra pateikiama ne visa informacija iš karto, susijusi su įvykusiu ADSP, tuomet duomenų apsaugos pareigūnas nurodo to priežastis, taip pat nurodo, kada bus pateikta likusi su pažeidimu susijusi informacija.

19. Jeigu Inspekcija paprašo papildyti, patikslinti ar paaiškinti tam tikrą pateiktą informaciją, duomenų apsaugos pareigūnas privalo nepagrįstai nedelsdamas tai padaryti.

20. Pranešimai Inspekcijai yra teikiami vienu iš žemiau nurodytu būdu:

20.1. naudojantis el. siuntų sistema E.pristatymas;

20.2. elektroniniu parašu pasirašyti dokumentai siunčiami Inspekcijos elektroniniu paštu ada@ada.lt;

20.3. registruotu paštu;

20.4. įteikiami vietoje Inspekcijos buveinės adresu.

21. Tuo atveju, jeigu žinoma ar numanoma, kad ADSP įvyko dėl kažkieno galimai nusikalstamų veiksmų, duomenų apsaugos pareigūnas, turint įstaigos rektoriaus pritarimą, apie šį incidentą informuoja ir policiją.

V SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

22. Nepriklausomai nuo nustatyto ADSP rizikos laipsnio (žema, vidutinė arba didelė), visi ADSP privalo būti dokumentuojami ADSP registravimo žurnale (Priedas Nr. 2). Šis žurnalas privalo būti užpildytas kuo anksčiau, tačiau ne vėliau nei per 5 dienas nuo ADSP nutikimo.

23. ADSP registravimo žurnalą pildo duomenų apsaugos pareigūnas, o padaręs atitinkamą įrašą, persiunčia šį žurnalą peržiūrai įstaigos rektoriui, kuris arba patvirtina atliktą įrašą, arba nurodo pastabas ir duoda papildomą terminą atliktam įrašui pataisyti. Atlikus pataisymą, duomenų apsaugos pareigūnas vėl siunčią šį žurnalą įstaigos rektoriui patvirtinimui. Gavus patvirtinimą, atliktas įrašas yra laikomas tinkamu ir teisingu.

24. ADSP registravimo žurnalą duomenų apsaugos pareigūnas peržiūri ne rečiau nei 1 kartą per metus, ko pasėkoje yra įvertinami metų eigoje įvykę ADSP, peržiūrimos jau taikomos prevencinės priemonės bei priimami sprendimai dėl papildomų prevencinių priemonių taikymo. Peržiūrėjus šį žurnalą, duomenų apsaugos pareigūnas turi kreiptis į įstaigos rektorių su ataskaita, kurioje būtų trumpai aptariami jau įvykę ADSP bei teikiami pasiūlymai dėl naujų prevencinių priemonių taikymo, jeigu duomenų apsaugos pareigūno nuomone jų reiktų. Įstaigos rektorius šią ataskaitą įvertina savo nuožiūra ir priima galutinį sprendimą dėl naujų prevencinių priemonių taikymo.
25. ADSP registravimo žurnale yra saugomi ne senesni nei per 3 metus įvykę ADSP.