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

KLAIPĖDOS UNIVERSITETO POVEIKIO DUOMENŲ APSAUGAI VERTINIMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šis poveikio duomenų apsaugai vertinimo tvarkos aprašas (toliau tekste – **Aprašas**) yra 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. balandžio 4 d. 29 straipsnio duomenų apsaugos darbo grupės poveikio duomenų apsaugai vertinimo gairėmis, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų, 2019 m. kovo 14 d. Valstybinės duomenų apsaugos inspekcijos (toliau tekste – **Inspekcija**) direktoriaus įsakymu Nr. 1T-35(1.12.E) dėl duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo 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. **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, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas;
2.4. **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;
2.5. **Poveikio duomenų apsaugai vertinimas** - tai procesas, skirtas duomenų tvarkymui aprašyti ir tokio tvarkymo reikalingumui ir proporcingumui įvertinti, padedantis valdyti pavojų, kuris fizinių asmenų teisėms ir laisvėms kyla dėl asmens duomenų tvarkymo, jį įvertinant ir nustatant šio pavojaus pašalinimo priemones. Poveikio duomenų apsaugai vertinimas yra svarbi atskaitomybės priemonė, nes padeda duomenų valdytojams ne tik laikytis BDAR, bet ir įrodyti, kad, siekiant užtikrinti atitiktį BDAR, buvo imtasi tinkamų priemonių (toliau tekste – **PDAV**);
2.6. **Pavojus** – tai scenarijus, kuriame aprašomas įvykis ir jo padariniai, įvertinti atsižvelgiant į jų rimtumą ir tikimybę;
2.7. **Kontaktinis asmuo** – paskirtas asmuo, palaikantis kontaktą su duomenų apsaugos pareigūnu ir padedantis jam atlikti PDAV;

2.8. **Duomenų apsaugos pareigūnas –** asmuo, įstaigoje paskirtas atsakingu už duomenų apsaugą ir kurio statusą reglamentuoja BDAR 37-39 straipsniai.

3. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos BDAR bei kituose asmens duomenų tvarkymą ir apsaugą reglamentuojančiuose teisės aktuose.

II SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

4. Tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, duomenų valdytojas, prieš pradėdamas tvarkyti duomenis, atlieka numatytų duomenų tvarkymo operacijų PDAV. Nuoroda į duomenų subjektų teises ir laisves visų pirma yra susijusi su teisėmis į duomenų apsaugą ir privatumą, tačiau taip pat gali apimti ir kitas pagrindines teises (pavyzdžiui.: *žodžio laisvę, minties laisvę, judėjimo laisvę, diskriminacijos draudimą*).

5. Tam tikromis aplinkybėmis gali būti protinga ir ekonomiška atlikti platesnio masto PDAV, o ne susieti jį su vienu konkrečiu projektu (pavyzdžiui,: *kai valdžios institucijos ar įstaigos siekia sukurti bendrą taikomąją programą ar duomenų tvarkymo platformą arba kai keli duomenų valdytojai ketina tam tikroje pramonės šakoje, jos sektoriuje arba plačiai paplitusioje horizontalioje veikloje pradėti taikyti bendrą taikomąją programą ar duomenų tvarkymo aplinką*).

6. PDAV visų pirma turi būti atliktas šiais atvejais:

6.1. sistemingas ir išsamus su fiziniais asmenimis susijusių asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, ir kuriuo remiantis priimami sprendimai, kuriais padaromas su fiziniu asmeniu susijęs teisinis poveikis arba kurie daro panašų didelį poveikį fiziniam asmeniui;

6.2. BDAR 9 straipsnio 1 dalyje nurodytų specialių kategorijų duomenų arba 10 straipsnyje nurodytų asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu;

6.3. sistemingas viešos vietos stebėjimas dideliu mastu.

7. Inspekcija, vadovaudamasi BDAR 35 straipsnio 4 dalimi, parengė operacijų sąrašą, kurioms yra būtina atlikti PDAV. Šis sąrašas yra patvirtintas Inspekcijos direktoriaus 2019 m. kovo 14 d. įsakymu Nr. 1T-35 (1.12.E). Šiuo sąrašu, įskaitant visus jo pakeitimus ir papildymus, privaloma vadovautis nustatant, ar konkrečiu atveju privalu atlikti PDAV.

8. 29 straipsnio duomenų apsaugos darbo grupė yra išsakiusi nuomonę, jog PDAV turi būti atliktas, jeigu duomenų valdytojas atlieka operacijas, kurios atitinka bent du iš žemiau paminėtų kriterijų (kartais pakanka ir vieno kriterijaus):

8.1. egzistuoja vertinimas arba balų skyrimas, įskaitant profiliavimą ir prognozavimą;

8.2. egzistuoja automatizuotų sprendimų, sukeliančių teisinį arba panašų rimtą poveikį, priėmimas;

8.3. egzistuoja sisteminga stebėsena;

8.4. tvarkomi neskelbtini arba labai asmeniški duomenys;

8.5. duomenys yra tvarkomi dideliu mastu;

8.6. esti duomenų rinkinių siejimas ir derinimas;

8.7. tvarkomi pažeidžiamų duomenų subjektų duomenys;

8.8. duomenys naudojami naujovišku būdu arba taikomos naujos technologijos ar organizaciniai sprendimo būdai;

8.9. dėl duomenų tvarkymo duomenų subjektams užkertamas kelias naudotis savo teisėmis, paslaugomis arba sudaryti sutartį.

9. Tais atvejais, kai įstaigoje su asmens duomenimis yra ketinama atlikti naujas operacijas (pavyzdžiui,: *diegiama nauja duomenų valdymo sistema*), taip pat jeigu nusprendžiama tvarkyti naujus, iki šiol netvarkytus, asmens duomenis, darbuotojas, kuris inicijavo naujų operacijų atlikimą ar naujų duomenų valdymo būtinybę, privalo nedelsdamas apie tai informuoti įstaigos rektorių ir duomenų apsaugos pareigūną. Įstaigos rektorius, gavęs šią informaciją, pasitaręs su

duomenų apsaugos pareigūnu, priima sprendimą dėl PDAV atlikimo būtinybės. Tais atvejais, kai nėra aišku, ar reikia PDAV atlikti, jis turėtų būti atliekamas.

10. PDAV gali būti atliekamas ir esamoms duomenų tvarkymo operacijoms, jei tose operacijose atsirastų reikšmingų pokyčių (pavyzdžiui,: *iš esmės perdaroma duomenų valdymo sistema, gebanti atlikti naujas funkcijas*).
11. PDAV turi būti atliktas prieš pradedant duomenų tvarkymą.
12. Vienu PDAV gali būti įvertintos ir kelios duomenų tvarkymo operacijos, jeigu jos yra glaudžiai susijusios ir kelia panašų pavojų.
13. PDAV yra siekiama ištirti tik naujas situacijas, dėl kurių gali kilti pavojus duomenų subjektų teisėms ir laisvėms, todėl PDAV nereikia atlikti tais atvejais, kurie jau buvo ištirti (pavyzdžiui,: *tos pačios rūšies duomenims, kurie bus naudojami tuo pačiu tikslu, rinkti pasitelkiama panaši technologija*).

III SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMO ATLIKIMAS, DOKUMENTAVIMAS IR KONSULTAVIMASIS SU INSPEKCIJA

14. PDAV yra atliekamas pagal prie šio Aprašo pridėtą formą (Priedas Nr. 1).
15. PDAV atlieka duomenų apsaugos pareigūnas, jeigu įstaigos rektorius nepaskiria kito už tai atsakingo asmens.
16. Duomenų apsaugos pareigūnas, atlikdamas PDAV, bendradarbiauja su kontaktiniu asmeniu, taip pat su kitais įstaigos darbuotojais, galinčiais duomenų apsaugos pareigūnui suteikti PDAV atlikti reikalingą informaciją. Visi įstaigos darbuotojai, nepriklausomai nuo jų vykdomų tiesioginių darbo funkcijų, privalo bendradarbiauti su duomenų apsaugos pareigūnu, teikiant jam visą reikalingą pagalbą ir informaciją PDAV atlikimo eigoje.
17. Atlikus PDAV, nurodoma bent ši informacija:

17.1. sistemingas numatytų duomenų tvarkymo operacijų aprašymas ir duomenų tvarkymo tikslai, įskaitant, kai taikoma, teisėtus interesus, kurių siekia įstaiga;
17.2. duomenų tvarkymo operacijų reikalingumo ir proporcingumo, palyginti su tikslais, vertinimas;
17.3. koks gali kilti pavojus duomenų subjektų teisėms ir laisvėms;
17.4. pavojams pašalinti numatytos priemonės, įskaitant apsaugos priemones, saugumo priemones ir mechanizmus, kuriais užtikrinama asmens duomenų apsauga ir įrodoma, kad laikomasi šio reglamento, atsižvelgiant į duomenų subjektų ir kitų susijusių asmenų teises ir teisėtus interesus.

18. Tais atvejais, kuomet po atlikto PDAV iš esmės ar dalinai keičiasi duomenų tvarkymo operacija dėl kurios ir buvo atliktas PDAV, PDAV privalo būti atliktas iš naujo.
19. Įstaiga privalo konsultuotis su Inspekcija, jeigu atlikus PDAV buvo nustatyta, jog tvarkant duomenis kiltų didelis pavojus, jei įstaiga nesiimtų priemonių pavojui sumažinti.
20. Konsultuojantis su Inspekcija, įstaiga Inspekcijai privalo pateikti bent šią informaciją:

20.1. kai taikoma, atitinkamas duomenų tvarkymo procese dalyvaujančio duomenų valdytojo, bendrų duomenų valdytojų ir duomenų tvarkytojų atsakomybės sritis, visų pirma, kai duomenys tvarkomi įstaigų grupėje;
20.2. numatyto duomenų tvarkymo tikslus ir priemones;
20.3. nustatytas priemones bei apsaugos priemones duomenų subjektų teisėms ir laisvėms apsaugoti pagal BDAR;
20.4. duomenų apsaugos pareigūno kontaktinius duomenis;
20.5. BDAR 35 straipsnyje numatytą poveikio duomenų apsaugai vertinimą;
20.6. bet kokią kitą priežiūros institucijos prašomą informaciją.

21. Duomenų apsaugos pareigūnas privalo įgyvendinti iš Inspekcijos gautus patarimus ar nurodytas pastabas per Inspekcijos nurodytą terminą, taip pat įvykdyti kitus nurodymus, jeigu tokie yra pateikiami.
22. Atlikti PDAV yra saugomi 5 metus.