PATVIRTINTA
Informacinės visuomenės plėtros komiteto
2023 m. vasario 1 d. įsakymu Nr. T-11(2023)

# ASMENS DUOMENŲ TVARKYMO INFORMACINĖS VISUOMENĖS PLĖTROS KOMITETE TAISYKLĖS

## I SKYRIUS
## BENDROSIOS NUOSTATOS

1. Asmens duomenų tvarkymo Informacinės visuomenės plėtros komitete taisyklių (toliau – Taisyklės) tikslas – reglamentuoti asmens duomenų tvarkymą Informacinės visuomenės plėtros komitete (toliau – Komitetas), nustatyti pagrindines asmens duomenų tvarkymo ir duomenų apsaugos technines bei organizacines priemones, siekiant užtikrinti 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 (ES) 2016/679), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ir kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir apsaugą, laikymąsi ir įgyvendinimą.

2. Šios Taisyklės privalomos visiems Komiteto valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau – Komiteto darbuotojams), kurie tvarko Komitete esančius asmens duomenis ir (arba) eidami savo pareigas sužino arba gali sužinoti asmens duomenis.

3. Komitetas, kaip asmens duomenų valdytojas, atlikdamas Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos valstybės informacinių išteklių įstatyme, Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatyme, Lietuvos Respublikos administracinių nusižengimų kodekse ir kituose teisės aktuose nustatytas funkcijas, turi teisę informaciją Komiteto kompetencijai priskirtais klausimais ir teisės aktų nustatyta tvarka tvarkyti asmens duomenis.

4. Šiose Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir kituose teisės aktuose.

5. Komitete asmens duomenys nėra tvarkomi tiesioginės rinkodaros tikslais bei jo veikloje nėra vykdomas profiliavimas.

6. Komiteto vykdoma asmens duomenų tvarkymo veikla yra aprašoma Duomenų tvarkymo veiklos įrašų žurnale, kurio pavyzdinė forma nustatyta šių Taisyklių 1 priede ir pildoma pagal Komiteto atsakingų struktūrinių padalinių pateiktą informaciją. Duomenų tvarkymo veiklos įrašų žurnalą pildo ir tvarko Duomenų apsaugos pareigūnas. Duomenų apsaugos pareigūnas turi peržiūrėti Duomenų tvarkymo veiklos įrašus pagal poreikį ir iškilus būtinybei, bet ne rečiau nei 1 kartą per metus.

## II SKYRIUS
## PAGRINDINIAI ASMENS DUOMENŲ TVARKYMO IR APSAUGOS REIKALAVIMAI

7. Komiteto darbuotojai, atlikdami savo funkcijas ir tvarkydami asmens duomenis, privalo laikytis pagrindinių asmens duomenų tvarkymo reikalavimų:

7.1. asmens duomenys renkami tik apibrėžtais tikslais ir tvarkomi su šiais tikslais suderintais būdais;

7.2. asmens duomenys duomenų subjekto atžvilgiu tvarkomi teisėtu, sąžiningu ir skaidriu būdu;

7.3. asmens duomenys turi būti tikslūs ir, jei reikia dėl asmens duomenų tvarkymo, nuolat atnaujinami; netikslūs ar neišsamūs duomenys turi būti ištaisyti, papildyti, ištrinti (sunaikinti) arba sustabdytas jų tvarkymas;

7.4. asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi;

7.5. asmens duomenys turi būti laikomi (saugomi) tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi;

7.6. asmens duomenys turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ir organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo;

7.7. asmens duomenys tvarkomi pagal Reglamente (ES) 2016/679, Asmens duomenų teisinės apsaugos įstatyme ir kituose atitinkamą veiklą reglamentuojančiuose teisės aktuose nustatytus asmens duomenų tvarkymo reikalavimus.

8. Asmens duomenys Komitete renkami tik teisės aktų nustatyta tvarka, juos gaunant tiesiogiai iš duomenų subjekto, gaunant iš kitų asmenų nustatyta tvarka ir pagrindais, taip pat oficialiai užklausiant reikalingą informaciją tvarkančių ir turinčių teisę ją teikti subjektų pagal prašymą (vienkartinio asmens duomenų rinkimo atveju) arba pagal asmens duomenų teikimo sutartį (daugkartinio asmens duomenų rinkimo atveju).

9. Asmens duomenų saugojimo terminus ir veiksmus, kurie atliekami pasibaigus šiam terminui, nustato teisės aktai, reglamentuojantys atitinkamų asmens duomenų tvarkymą. Asmens duomenys saugomi ne ilgiau, negu to reikalauja duomenų tvarkymo tikslai. Asmens duomenys, esantys dokumentuose, yra saugomi teisės aktų, reglamentuojančių šių dokumentų saugojimą, nustatyta tvarka ir terminais. Elektroninės informacijos (duomenų) atsarginės kopijos saugomos informacinės sistemos valdytojo tvirtinamuose informacinės sistemos saugos nuostatuose nustatyta tvarka ir terminais. Kai asmens duomenys nebereikalingi jų tvarkymo tikslams, jie yra sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduoti Lietuvos valstybės naujajam archyvui.

10. Komitetas užtikrina, kad visa reikalinga informacija, susijusi su duomenų tvarkymu, duomenų subjektui būtų pateikiama aiškiai ir suprantamai.

11. Teisės aktų nustatytais atvejais ir tvarka Komitetas teikia jo tvarkomus asmens duomenis valstybės registrų ir valstybės informacinių sistemų valdytojams ir (arba) tvarkytojams, valstybės ir savivaldybių institucijoms, įstaigoms, organizacijoms ir kitiems asmenims, kuriems asmens duomenis teikti Komitetą įpareigoja įstatymai ar kiti teisės aktai arba kuriems Komitetas, teisės aktų nustatyta tvarka vykdydamas savo funkcijas, teikia asmens duomenis, taip pat pagal duomenų gavėjų prašymus (vienkartinio teikimo atveju) arba Komiteto ir duomenų gavėjų sudarytas asmens duomenų teikimo sutartis (daugkartinio teikimo atveju). Sutartyje turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka ir teikiamų asmens duomenų apimtis. Prašyme turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo bei gavimo teisinis pagrindas ir prašomų pateikti asmens duomenų apimtis. Kai asmens duomenys tvarkomi automatiniu būdu ir taikomos tinkamos duomenų saugumą užtikrinančios priemonės, teikiant asmens duomenis pagal Komiteto ir duomenų gavėjo sudarytą asmens duomenų teikimo sutartį, prioritetas turi būti teikiamas automatiniam duomenų teikimui, o teikiant asmens duomenis pagal duomenų gavėjo prašymą, – duomenų teikimui elektroninėmis priemonėmis.

## III SKYRIUS
## SPECIALIEJI ASMENS DUOMENŲ TVARKYMO KOMITETE REIKALAVIMAI

12. Komitetas įgyvendina šiose Taisyklėse nurodytas organizacines ir technines asmens duomenų saugumo priemones, skirtas užtikrinti tinkamą asmens duomenų saugumą, taip pat apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo.

13. Pasikeitus duomenų subjektų asmens duomenims ir duomenų subjektams apie tai raštu informavus Komitetą, toks duomenų subjekto raštas įdedamas į bylą, o automatinėse duomenų rinkmenose ir duomenų bazėse duomenys atnaujinami.

14. Naikinant dokumentus, kurių saugojimo terminas yra pasibaigęs, Komiteto dokumentai, kuriuose nurodomi asmens duomenys, bei jų kopijos turi būti sunaikinti taip, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio.

15. Duomenų subjektų pateikti dokumentai bei jų kopijos, finansavimo, buhalterinės apskaitos ir atskaitomybės, archyvinės ar kitos bylos, kuriose yra asmens duomenų, saugomos rakinamose spintose, seifuose arba patalpose. Dokumentai, kuriuose yra asmens duomenų, neturi būti laikomi taip, kad neturintys teisės asmenys nekliudomai galėtų su jais susipažinti.

16. Archyviniam saugojimui perduoti dokumentai (bylos) iki perdavimo Lietuvos valstybės naujajam archyvui saugomos Komiteto archyve dokumentų saugykloje.

17. Vietinio tinklo sritys, kuriose yra saugomi asmens duomenys, privalo būti apsaugotos prieigos prie asmens duomenų slaptažodžiais arba turi būti apribotos prieigos teisės prie jų.

18. Komiteto kompiuterinė įranga turi būti apsaugota nuo kenksmingos programinės įrangos (antivirusinių programų įdiegimas, atnaujinimas ir pan.). Asmens duomenų tvarkymo keliamos rizikos vertinimo atlikimo tvarka ir saugumo pažeidimų valdymas, reagavimo į šiuos pažeidimus veiksmai, duomenų atsarginių kopijų darymo, saugojimo ir duomenų atkūrimo iš atsarginių duomenų kopijų tvarka nustatoma informacinių sistemų valdytojo tvirtinamuose informacinės sistemos saugos nuostatuose bei kituose saugos politiką įgyvendinančiuose teisės aktuose.

## IV SKYRIUS
## DUOMENŲ APSAUGOS PAREIGŪNO PASKYRIMAS IR JO VEIKLOS VYKDYMAS

19. Siekiant užtikrinti aukštą tvarkomų asmens duomenų apsaugos lygį Komitetas paskiria Duomenų apsaugos pareigūną.

20. Duomenų apsaugos pareigūnu skiriamas asmuo privalo turėti asmens duomenų apsaugos teisės ir praktikos ekspertines žinias, taip pat asmens duomenų saugumo užtikrinimo patirtį informacinių technologijų srityje.

21. Duomenų apsaugos pareigūno pagrindinės funkcijos:

21.1. vykdo stebėseną ar Komiteto atliekamas asmens duomenų tvarkymas atitinka asmens duomenų apsaugos teisės reikalavimus ir esant poreikiui informuoja Komiteto direktorių, jo įgaliotus asmenis, struktūrinių padalinių vadovus ir su asmens duomenų tvarkymu bei apsauga susijusius darbuotojus apie jų prievoles tvarkant asmens duomenis ir konsultuoja juos šiais klausimais;

21.2. konsultuoja Komiteto vadovybę, jo įgaliotus asmenis struktūrinių padalinių vadovus ir su asmens duomenų tvarkymu bei apsauga susijusius darbuotojus dėl vidinių teisės aktų, sutarčių ar kitų dokumentų projektų, kurie susiję su asmens duomenų apsauga bei teikia pastabas ir pasiūlymus dėl jų;

21.3. dalyvauja vertinant Komiteto pasitelkiamus duomenų tvarkytojus jų atitikties keliamiems duomenų apsaugos reikalavimams požiūriu, esant poreikiui atlieka jų vykdomos duomenų tvarkymo veiklos patikrinimą;

21.4. vykdo šių Taisyklių, kitų vidaus dokumentų, įstatymų ir kitų asmens duomenų tvarkymą reglamentuojančių teisės aktų įgyvendinimo Komitete priežiūrą bei teikia pasiūlymus Komiteto vadovybei dėl neatitikčių bei jų šalinimo;

21.5. šių taisyklių nustatyta tvarka pildo Duomenų tvarkymo veiklos įrašų žurnalą (Taisyklių 1 priedas);

21.6. organizuoja ir vykdo Komiteto darbuotojų švietimą ir mokymus asmens duomenų tvarkymo ir apsaugos klausimais;

21.7. teikia konsultacijas dėl Poveikio duomenų apsaugai vertinimo, vykdo vertinimo priežiūrą bei atlieka kitas šių Taisyklių VI skyriuje nurodytas funkcijas susijusias su Poveikio duomenų apsaugai vertinimo atlikimu;

21.8. atlieka kontaktinio asmens funkcijas bendradarbiaujant bei konsultuojantis su visomis suinteresuotomis šalimis - Valstybine asmens duomenų apsaugos inspekcija, Duomenų subjektais ir kitais Duomenų valdytojais, tvarkytojais bei subtvarkytojais;

21.9. šių Taisyklių VI skyriaus bei Komiteto direktoriaus patvirtinto Informacinės visuomenės plėtros komiteto asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo nustatyta tvarka dalyvauja asmens duomenų saugumo pažeidimų vertinime ir teikia rekomendacijas;

21.10. nagrinėja Duomenų subjektų tiesiogiai Duomenų apsaugos pareigūnui pateiktus prašymus, susijusius su jų asmens duomenų tvarkymu, siekiant užtikrinti jų teisių įgyvendinimą ir rengia atsakymus duomenų subjektams. Taip pat Komiteto direktoriaus sprendimu nagrinėja sudėtingus Komitete gautus Duomenų subjektų prašymus ir rengia atsakymus duomenų subjektams;

21.11. esant poreikiui konsultuoja Komiteto darbuotojus, nagrinėjančius Duomenų subjektų prašymus susijusius su jų teisių įgyvendinimu;

21.12. atlieka kitas šiose Taisyklėse ar kitais vidaus teisės aktais apibrėžtas funkcijas, kurių vykdymas tiesiogiai susijęs su pagalba Duomenų valdytojui užtikrinant atitiktį asmens duomenų apsaugos reikalavimams ir dėl kurių vykdymo nekiltų interesų konfliktas.

22. Duomenų apsaugos pareigūnas vykdydamas savo užduotis veikia nepriklausomai ir savarankiškai vadovaudamasis savo profesine kompetencija tinkamai vertina su asmens duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgdamas į duomenų tvarkymo pobūdį, kontekstą ir tikslus. Iškilus interesų konflikto tikimybei, Duomenų apsaugos pareigūnas privalo raštu nusišalinti ir apie tai informuoti Komiteto direktorių arba jo įgaliotą asmenį. Duomenų apsaugos pareigūną pavaduojančiu asmeniu gali būti skiriamas tik asmuo atitinkantis Duomenų apsaugos pareigūnui keliamus reikalavimus dėl kurio nekyla interesų konflikto tikimybės.

23. Duomenų apsaugos pareigūno teisės:

23.1. Duomenų apsaugos pareigūnas įgyvendindamas jam pavestas funkcijas turi teisę iš visų Komiteto darbuotojų gauti informaciją susijusią su asmens duomenų tvarkymu, teisę susipažinti su Komiteto vidaus ir kitais dokumentais susijusiais su asmens duomenų tvarkymu, gauti paaiškinimus ir kitą informaciją būtina jo tiesioginėms funkcijoms vykdyti;

23.2. Duomenų apsaugos pareigūnas, esant poreikiui, bet ne rečiau kaip kartą per tris mėnesius, turi teisę inicijuoti susitikimą su Komiteto vadovybe asmens duomenų apsaugos klausimams aptarti;

23.3. Duomenų apsaugos pareigūnas turi teisę būti įtrauktas į visų klausimų, susijusių su asmens duomenų apsauga, nagrinėjimą bei išsakyti savo pasiūlymus ir pastabas.

24. Duomenų apsaugos pareigūnas yra atskaitingas Komiteto direktoriui. Komiteto direktorius privalo užtikrinti, jog duomenų apsaugos pareigūnas būtų tinkamai ir laiku įtraukiamas į visų su asmens duomenų apsauga susijusių klausimų nagrinėjimą ir jam būti suteikti visi būtini ištekliai jo vykdomoms užduotims atlikti.

25. Duomenų apsaugos pareigūnas privalo užtikrinti konfidencialumą susijusį su jo užduočių vykdymu.

## V SKYRIUS
## REIKALAVIMAI ASMENIMS, TVARKANTIEMS ASMENS DUOMENIS

26. Prieiga prie asmens duomenų gali būti suteikta tik tam Komiteto darbuotojui, kuriam asmens duomenys yra reikalingi jo funkcijoms vykdyti.

27. Su asmens duomenimis galima atlikti tik tuos veiksmus, kuriuos būtina atlikti Komiteto darbuotojui vykdant savo funkcijas.

28. Komiteto darbuotojas, tvarkantis duomenų subjektų asmens duomenis, privalo:

28.1. laikytis pagrindinių asmens duomenų tvarkymo reikalavimų ir saugumo reikalavimų, įtvirtintų Reglamente (ES) 2016/679, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, šiose Taisyklėse ir kituose teisės aktuose;

28.2. laikytis konfidencialumo principo ir laikyti paslaptyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jis susipažino vykdydamas savo funkcijas, išskyrus, jeigu tokia informacija buvo vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas. Pareiga saugoti asmens duomenų paslaptį galioja ir perėjus dirbti į kitas pareigas ar pasibaigus įgaliojimams, valstybės tarnybos ar darbo santykiams Komitete;

28.3. laikytis šiose Taisyklėse nustatytų organizacinių ir techninių asmens duomenų saugumo priemonių, siekiant užkirsti kelią netyčiniam ar neteisėtam tvarkomų asmens duomenų sunaikinimui, praradimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, saugoti

dokumentus, duomenų rinkmenas bei duomenų bazėse saugomus duomenis ir vengti perteklinių jų kopijų darymo;

28.4. neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su asmens duomenimis asmeniui, kuris nėra įgaliotas tvarkyti asmens duomenų;

28.5. nedelsiant pranešti Komiteto direktoriui ar jo įgaliotam atsakingam asmeniui ir duomenų apsaugos pareigūnui apie bet kokią įtartiną situaciją, kuri gali kelti grėsmę Komiteto tvarkomų asmens duomenų saugumui;

28.6. laikytis kitų šiose Taisyklėse ir asmens duomenų apsaugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų.

29. Komiteto darbuotojas netenka teisės tvarkyti duomenų subjektų asmens duomenų, kai pasibaigia Komiteto darbuotojo įgaliojimai, valstybės tarnybos ar darbo santykiai su Komitetu, arba kai jam pavedama vykdyti su duomenų tvarkymu nesusijusias funkcijas.

30. Už asmens duomenų tvarkymą atsako Komiteto padalinių ir (ar) skyrių vadovai (vedėjai) toje apimtyje, kokioje yra numatytas asmens duomenų tvarkymas vykdant padalinio ir (ar) skyriaus funkcijas ir darbuotojų pareigas numatytas nuostatuose ir pareigybių aprašymuose.

## VI SKYRIUS
## POVEIKIO ASMENS DUOMENŲ APSAUGAI VERTINIMAS IR KONSULTACIJOS SU PRIEŽIŪROS INSTITUCIJA

31. Tais atvejais, kai, atsižvelgiant į asmens duomenų ir duomenų subjektų kategoriją, duomenų tvarkymo pobūdį, aprėptį, kontekstą, tikslus, duomenų subjektų teisėms bei laisvėms gali kilti didelis pavojus, Komitetas, prieš pradėdamas vykdyti duomenų tvarkymo operacijas (veiksmus) ir tvarkyti duomenis, atlieka numatytų duomenų tvarkymo operacijų poveikio duomenų apsaugai vertinimą.

32. Poveikis asmens duomenų apsaugai vertinamas, kai:

32.1. duomenų tvarkymo operacija patenka į Valstybinės duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų sąrašą, kurioms poveikio asmens duomenų apsaugai vertinimas yra privalomas;

32.2. duomenų tvarkymo operacija nepatenka į Valstybinės duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų sąrašą, kurioms poveikio asmens duomenų apsaugai vertinimo reikalavimas yra privalomas, tačiau Komitetas įvertina, kad asmens duomenų tvarkymo operacija, atsižvelgiant į Taisyklių 33 punkte įtvirtintus kriterijus, asmens duomenų subjektų teisėms bei laisvėms gali kelti didelį pavojų;

32.3. pasikeitus asmens duomenų tvarkymo operacijų (veiksmų) įgyvendinimo sąlygoms ir kai tai gali lemti didelį pavojų asmens duomenų subjektų teisėms ir laisvėms;

32.4. kitais šiose Taisyklėse įtvirtintais atvejais.

33. Ar asmens duomenų tvarkymo operacijos (veiksmai) gali kelti didelį pavojų duomenų subjektų teisėms ir laisvėms, sprendžiama kiekvieną kartą atsižvelgiant į šiuos kriterijus:

33.1. sisteminga asmens duomenų ar duomenų subjektų stebėsena;

33.2. neskelbtini duomenys arba labai asmeniški duomenys, pavyzdžiui, specialių kategorijų asmens duomenys;

33.3. didelio masto asmens duomenų tvarkymas (susijusių duomenų subjektų skaičius, tvarkomų duomenų kiekis, tvarkomų duomenų įvairovė, duomenų tvarkymo veiklos trukmė ir pastovumas, geografinis duomenų tvarkymo mastas);

33.4. asmens duomenų rinkinių siejimas ir derinimas;

33.5. su pažeidžiamais asmens duomenų subjektais susiję duomenys;

33.6. naujų technologijų ar organizacinių sprendimų būdų taikymas;

33.7. dėl duomenų tvarkymo duomenų subjektams užkertamas kelias naudotis savo teisėmis, paslaugomis arba sudaryti sutartis;

33.8. kitos aplinkybės, rodančios galimą didelį pavojų asmens duomenų subjektų teisėms ir laisvėms.

34. Kuo daugiau Taisyklių 33 punkte įtvirtintų kriterijų atitinka konkreti asmens duomenų tvarkymo operacija (veiksmai), tuo didesnė tikimybė, kad duomenų tvarkymo operacija (veiksmai)

gali kelti didelį pavojų duomenų subjektų teisėms ir laisvėms. Dėl poveikio asmens duomenų apsaugai atlikimo būtinybės visais atvejais konsultuojamasi su duomenų apsaugos pareigūnu.

35. Jeigu duomenų tvarkymo operacija (veiksmai) atitinka du ir daugiau 26 punkte išdėstytus kriterijus, tačiau padaroma išvada, kad tokia duomenų tvarkymo operacija (veiksmai) negali kelti didelio pavojaus asmens duomenų subjektų teisėms ir laisvėms, toks sprendimas ir jo argumentai išdėstomi raštu ir kartu su duomenų apsaugos pareigūno nuomone pateikiami Komiteto direktoriui arba jo paskirtam asmeniui.

36. Poveikio asmens duomenų apsaugai vertinimas turi būti atliktas prieš pradedant įgyvendinti duomenų tvarkymo operacijas (veiksmus).

37. Už poveikio asmens duomenų apsaugai vertinimą kiekvienu konkrečiu atveju atsakingas Komiteto padalinio, kuris tvarkys asmens duomenis, vadovas ar darbuotojas atsakingas už duomenų tvarkymą. Poveikio asmens duomenų vertinimui atlikti gali būti pasitelkti išorės konsultantai, specialistai, ekspertai (teisininkai, IT specialistai, saugumo ekspertai, etikos specialistai ir pan.), jeigu Komitetui žmogiškųjų, laiko išteklių nepakanka tinkamam poveikio asmens duomenų apsaugai vertinimui atlikti.

38. Atlikus poveikio asmens duomenų apsaugai vertinimą, asmuo ar asmenys, atlikę poveikio duomenų apsaugai vertinimą, užpildo poveikio asmens duomenų apsaugai vertinimo ataskaitą, kurio pavyzdinė forma nustatyta šių Taisyklių 2 priede. Panašių didelius pavojus keliančių duomenų tvarkymo operacijų sekai išnagrinėti galima atlikti vieną poveikio asmens duomenų apsaugai vertinimą.

39. Visais atvejais poveikio asmens duomenų apsaugai vertinimo ataskaita tarnybiniu pranešimu yra pateikiama Komiteto direktoriui ir/ar už sprendimo dėl vertinamos duomenų tvarkymo operacijos priėmimą bei jo įgyvendinimą atsakingam asmeniui.

40. Komitetas atlieka nuolatinę peržiūrą, kad įvertintų, ar asmens duomenys tvarkomi laikantis poveikio asmens duomenų apsaugai vertinimo, ypač tais atvejais, kai pakinta tvarkymo operacijų keliamas pavojus duomenų subjektų teisėms ir laisvėms.

41. Komitetas, prieš pradėdamas asmens duomenų tvarkymo operacijas (veiksmus), kurie gali kelti didelį pavojų asmens duomenų subjektų teisėms ir laisvėms, privalo konsultuotis su Valstybine duomenų apsaugos inspekcija šiais atvejais:

41.1. jeigu poveikio duomenų asmens apsaugai vertinimo ataskaitoje yra nustatyta, kad asmens duomenų tvarkymo veiksmai (operacijos) gali kelti didelį pavojų duomenų subjektų teisėms ir laisvėms ir numatytos priemonės nesumažina šios rizikos iki priimtino lygio;

41.2. jeigu pareiga konsultuotis dėl tam tikrų rūšių duomenų tvarkymo operacijų (veiksmų) įtvirtinta teisės aktuose arba šiose Taisyklėse.

42. Duomenų tvarkymo veiksmai, kurie gali sukelti didelį pavojų asmens duomenų subjektų teisėms ir laisvėms, gali būti vykdomi tik tada, kai Komitetas visiškai ir tinkamai įgyvendina Valstybinės duomenų apsaugos inspekcijos rekomendacijas, nurodymus ir priemonės, gautus konsultavimosi procedūros metu.

43. Kai duomenų tvarkymo apimtis, pobūdis, kontekstas ir tikslas yra labai panašūs į asmens duomenų tvarkymą, kurio poveikis asmens duomenų apsaugai buvo atliktas, galima iš naujo nevertinti poveikio asmens duomenų apsaugai, o pasinaudoti dėl panašaus asmens duomenų tvarkymo atliktu poveikio asmens duomenų apsaugai vertinimu.

## VII SKYRIUS
## PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

44. Komiteto direktorius ar jo įgaliotas atsakingas asmuo, sužinojęs apie asmens duomenų saugumo pažeidimą, nedelsiant organizuoja pažeidimo tyrimą, kad būtų nustatytas pažeidimo pobūdis, tipas (asmens duomenų konfidencialumo, vientisumo ir (arba) prieinamumo pažeidimas) aplinkybės, apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius, asmens duomenų, kurių saugumas pažeistas, kategorijos (asmens tapatybę patvirtinantys asmens duomenys, specialių kategorijų asmens duomenys, prisijungimo duomenys ir (arba) asmens identifikaciniai numeriai ir kt.) ir apimtis, tikėtinos asmens duomenų saugumo pažeidimo pasekmės, pavojus fizinių asmenų teisėms ir laisvėms, imasi priemonių pažeidimui pašalinti ir (arba)

neigiamoms pažeidimo pasekmėms sumažinti bei atlieka atitinkamus veiksmus, numatytus šiame Taisyklių skyriuje.

45. Komiteto direktorius ar jo įgaliotas atsakingas asmuo užtikrina, kad nepagrįstai nedelsiant ir, jei įmanoma, ne vėliau kaip per 72 valandas nuo sužinojimo apie asmens duomenų saugumo pažeidimą, apie tai būtų pranešta Valstybinei duomenų apsaugos inspekcijai, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Jeigu Valstybinei duomenų apsaugos inspekcijai nepranešama per 72 valandas, pranešime nurodomos vėlavimo priežastys. Pranešimas apie asmens duomenų saugumo pažeidimą pateikiamas Valstybinės duomenų apsaugos inspekcijos nustatyta tvarka.

46. Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms (gali būti padarytas kūno sužalojimas, turtinė ar neturtinė žala, gali kilti diskriminacija, būti pavogta ar suklastota tapatybė, būti padaryta finansinių nuostolių, pakenkta reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas, padaryta didelė ekonominė ar socialinė žala, kai duomenų subjektai gali netekti galimybės naudotis savo teisėmis ir laisvėmis ar jiems užkertamas kelias kontroliuoti savo asmens duomenis, gali būti paviešinti specialių kategorijų, pažeidžiamų fizinių asmenų asmens duomenys ir (ar) asmens duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas arba susijusias saugumo priemones ir kt.) Komiteto direktorius ar jo įgaliotas atsakingas asmuo užtikrina, kad apie asmens duomenų saugumo pažeidimą nepagrįstai nedelsiant būtų pranešta duomenų subjektui: duomenų subjektui aiškia ir paprasta kalba aprašomas duomenų saugumo pažeidimo pobūdis, nurodomas duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys (telefono numeris, elektroninio pašto adresas), aprašomos tikėtinos asmens duomenų saugumo pažeidimo pasekmės ir priemonės, kurių buvo imtasi arba pasiūlyta imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas, taip pat priemonės galimoms neigiamoms jo pasekmėms sumažinti bei pagal galimybes atitinkamam fiziniam asmeniui skirtos rekomendacijos, kaip sumažinti galimą neigiamą poveikį (pasikeisti prisijungimo slaptažodžius neteisėtos prieigos prie asmens duomenų atveju ir kt.).

47. Apie asmens duomenų saugumo pažeidimą duomenų subjektui pranešti neprivaloma, jei:

47.1. Komitetas įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio;

47.2. iš karto po asmens duomenų saugumo pažeidimo Komitetas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

47.3. tai pareikalautų neproporcingai daug pastangų. Tokiu atveju vietoj to apie asmens duomenų saugumo pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

48. Komiteto direktorius ar jo įgaliotas atsakingas asmuo užtikrina, kad būtų fiksuojami visi asmens duomenų saugumo pažeidimų atvejai ir kaupiama informacija apie tokių pažeidimų priežastis, jų poveikį ir pasekmes, priemones, kurių buvo imtasi, sprendimų dėl pranešimo (nepranešimo) Valstybinei duomenų apsaugos inspekcijai ir (ar) duomenų subjektui motyvus, vėlavimo pateikti pranešimą priežastis bei kitokio pobūdžio informaciją, kuri leistų patikrinti, kaip buvo laikomasi šio Taisyklių skyriaus nuostatų. Asmens duomenų saugumo pažeidimų valdymas vykdomas Komiteto direktoriaus patvirtinto Informacinės visuomenės plėtros komiteto asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo nustatyta tvarka.

## VIII SKYRIUS
## BAIGIAMOSIOS NUOSTATOS

49. Taisyklės skelbiamos Komiteto interneto svetainėje.

50. Už Taisyklių nuostatų laikymosi priežiūrą ir jose reglamentuotų nuostatų vykdymo kontrolę bei periodišką, ne rečiau kaip kartą per 1 metus, Taisyklių peržiūrėjimą atsakingas duomenų apsaugos pareigūnas, kuris, įvertinęs Taisyklių taikymo praktiką, esant poreikiui, inicijuoja Taisyklių atnaujinimą.

51. Komitete periodiškai, bet ne rečiau kaip kartą per 2 metus, vyksta Komiteto vykdomos asmens duomenų tvarkymo veiklos atitikties Reglamentui, Taisyklėms bei kitiems asmens duomenų apsaugą reglamentuojantiems teisės aktams patikra. Atliekant patikrą prioritetas skiriamas aukščiausią riziką keliančioms veiklos sritims, taip pat asmens duomenų tvarkymo operacijoms, kurios atitinka šių Taisyklių 33 punkte nurodytus kriterijus. Už patikros vykdymą yra atsakingas asmens duomenų apsaugos pareigūnas. Patikros rezultatai įforminami ataskaitoje, kurioje nurodomi nustatyti trūkumai, jei tokie nustatyti, bei rekomendacijos, kaip trūkumus ištaisyti ar pagerinti asmens duomenų tvarkymo veiklą. Ataskaita pateikiama Komiteto direktoriui, kuris yra atsakingas už ataskaitoje pateiktų rekomendacijų įgyvendinimo kontrolę ir kuris tvirtina ataskaitos rekomendacijų įgyvendinimo planą, kuriame nustatomos įgyvendinamos priemonės, jų įgyvendinimo terminai ir atsakingi vykdytojai.

52. Vykdant Komiteto veiklos stebėseną asmens duomenų apsaugos pareigūnas periodiškai, bet ne rečiau kaip kartą per tris mėnesius, organizuoja asmens duomenų tvarkymo veiklos aptarimą su Komiteto vadovybe.

53. Asmens duomenų apsaugos pareigūnas kasmet iki kovo 1 dienos pateikia Komiteto direktoriui veiklos metinę ataskaitą už praėjusius kalendorinius metus. Esant poreikiui, DAP veiklos ataskaitas Komiteto direktoriui gali teikti ir dažniau.

54. Komitetas nustatyta tvarka vykdo Komiteto darbuotojų mokymus siekiant užtikrinti, jog jų turimos žinios atitiktų įgyvendinamas asmens duomenų tvarkymo operacijas ir, esant galimybėms, sudaro sąlygas Komiteto darbuotojų kvalifikacijai kelti asmens duomenų teisinės apsaugos srityje.

55. Komiteto darbuotojai su šiomis taisyklėmis supažindinami pasirašytinai. Už taisyklių laikymosi priežiūrą ir kontrolę atsakingi Komiteto padalinių vadovai ir duomenų apsaugos pareigūnas.

56. Už Taisyklių nuostatų pažeidimą Komiteto darbuotojams taikoma įstatymuose numatyta atsakomybė.

57. Esant prieštaravimams ar neatitikimams tarp Taisyklių ir Reglamento (ES) 2016/679), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ar kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir apsaugą yra vadovaujamasi pastaraisiais.

_____

Asmens duomenų tvarkymo Informacinės visuomenės plėtros komitete taisyklių
1 priedas

**(Duomenų tvarkymo veiklos įrašų žurnalo forma)**

**INFORMACINĖS VISUOMENĖS PLĖTROS KOMITETO**
**DUOMENŲ TVARKYMO VEIKLOS ĮRAŠŲ ŽURNALAS**
Konstitucijos per. 15-89, 09319 Vilnius

**Duomenų apsaugos pareigūnas** – _____
*(vardas, pavardė, kontaktiniai duomenys)*

| **Eil. Nr.** | **AD šaltiniai (sistema, registras, aplikacija, laikmena, DB ir pan.)** | **AD šaltinio paskirtis (aprašymas)** | **AD tvarkymo teisinis pagrindas** | **AD tvarkymo tikslas (tikslai)** | **Duomenų kategorijos (asmens duomenys)** | **Specialių kategorijų duomenys** | **Subjektų kategorijos (subjektai)** | **Duomenų siuntėjų kategorijos (Valdytojai)** | **Duomenų gavėjų kategorijos (Tvarkytojai)*** | **Papildomų duomenų tvarkytojų kategorijos (Subtvarkytojai)*** | **AD tvarkymo terminai (saugojimas, ištrynimas)** | **Žurnalinių įrašų saugojimo terminas (angl. Log failai)** | **Naudotojai (darbuotojai ir kiti asmenys, kurie tvarko AD)** | **Administratoriai (pagrindinis ir pavaduojantys)** | **Atsakingas darbuotojas (AD šaltinio savininkas)** | **Atsakingas struktūrinis padalinys arba skyrius** | **Techninės ir organizacinės priemonės (pavadinimas ar aprašymas)** | **Informacijos įvedimo, keitimo data** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | | | | | | | | | | | | | | | | | | |
| 2. | | | | | | | | | | | | | | | | | | |
| 3. | | | | | | | | | | | | | | | | | | |
| 4. | | | | | | | | | | | | | | | | | | |
| 5. | | | | | | | | | | | | | | | | | | |

* Kai taikoma, asmens duomenų perdavimai į trečiąją valstybę arba tarptautinei organizacijai, įskaitant tos trečiosios valstybės arba tarptautinės organizacijos pavadinimą, ir Reglamento (ES) 2016/679 49 straipsnio 1 dalies antroje pastraipoje nurodytais duomenų perdavimų atvejais tinkamų apsaugos priemonių dokumentai.
Trumpinys: AD – asmens duomenys.

Asmens duomenų tvarkymo Informacinės visuomenės plėtros komitete taisyklių
2 priedas

**(Poveikio asmens duomenų apsaugai vertinimo ataskaitos forma)**

# POVEIKIO ASMENS DUOMENŲ APSAUGAI VERTINIMO ATASKAITA

_____

(vertinamos veiklos, sistemos, registro, aplikacijos, technologijos, duomenų bazės ar kito vertinamo objekto pavadinimas)

(data)

## 1. Priežastys, dėl kurių būtina atlikti poveikio asmens duomenų (toliau – AD) apsaugai vertinimą

| Planuojamos vykdyti (vykdomos) veiklos aprašymas, jos tikslai ir planuojamos atlikti AD tvarkymo operacijos (jei reikia, prie formos pridedami susiję dokumentai). | |
|---|---|
| -AD tvarkomi dideliu mastu<br>-vykdomas asmens savybių vertinimas<br>-vykdomas AD profiliavimas<br>-spec. kategorijų AD tvarkymas<br>-biometrinių duomenų tvarkymas<br>-vaikų AD tvarkymas | -tel. pokalbių įrašymas / vaizdo įrašymas /GPS<br>-įdiegta nauja IT sistema / įranga / technologija<br>-pradėta vykdyti naują AD tvarkymo operaciją<br>-įvyko incidentas (pvz. atskleisti duomenys, prarastos piniginės lėšos, sveikatos sutrikimai, sužalojimai)<br>-kita (aprašyti): |
| | |

## 2. AD tvarkymo aprašymas

| Rinkimo, naudojimo, saugojimo ir naikinimo veiksmai, nurodomi,AD rinkimo šaltiniai ir kam bus teikiami, galimi pavojai fizinių asmenų teisėms ir laisvėms (galima pateikti asmens duomenų tvarkymo veiksmų schemą). |
|---|
| Rinkimo veiksmai:<br>Naudojimo veiksmai:<br>Saugojimo veiksmai:<br>Naikinimo veiksmai:<br>AD šaltiniai:<br>Kam teikiami:<br>Veiksmai galintys kelti pavojų fizinio asmens teisėms (aprašyti): |
| |

| Tvarkymo mastas. |
|---|
| Specialių kategorijų AD: taip / ne<br>Duomenys apie apkaltinamuosius nuosprendžius: taip / ne<br>Asmens kodas: taip / ne<br>Tvarkomų AD kategorijos, terminai, apytikslis subjektų sk., geografinė tvarkymo aprėptis (aprašyti): |
| |

| Tvarkymo pobūdis. |
|---|
| Subjektų santykiai su Valdytoju: sutartis / kita<br>Subjektai gali kontroliuoti AD tvarkymą: taip / ne |

| |
|---|
| Subjektai gali numanyti jų AD tvarkymo būdą: taip / ne<br>Vaikų AD tvarkymas: taip / ne<br>Pažeidžiamų asmenų AD tvarkymas: taip / ne<br>Numatytas sertifikavimas: taip / ne<br>Numatytas patvirtintas elgesio kodeksas: taip / ne<br>AD tvarkymo praktika - galimos/žinomos problemos (aprašyti): |
| |

| |
|---|
| Tvarkymo tikslai ir poveikis. |
| Tikslai:<br>Rezultatai:<br>Poveikis subjektams:<br>Tvarkymo nauda organizacijai/įstaigai:<br>Tvarkymo nauda kitiems fiziniams arba juridiniams asmenims (aprašyti): |
| |

## 3. Konsultacijos

| |
|---|
| Suinteresuotų asmenų nuomonė apie AD tvarkymą ir konsultacijos. |
| Konsultacijos su AD apsaugos ekspertais planuojamos / ne:<br>Konsultacijos su kitų sričių ekspertais planuojamos / ne:<br>Konsultacijos su įstaigos/organizacijos specialistais planuojamos / ne:<br>Suinteresuotų asmenų nuomonė būtina / ne (aprašyti pagrindimą, jeigu nebūtina): |
| |

## 4. Būtinumo ir proporcingumo įvertinimas

| |
|---|
| AD tvarkymo teisėtumo ir proporcingumo principų užtikrinimas. |
| Tvarkymo pagrindas (teisėtumas):<br>Tvarkymo proporcingumas (apimtys):<br>AD apsaugos priemonės (techninės/organizacinės):<br>Subjektų informavimas apie AD tvarkymą (būdai):<br>Subjektų teisių užtikrinimas (būdai):<br>Tvarkytojų/subtvarkytojų AD apsaugos reikalavimų užtikrinimas (pažymėti): AD tvarkymo sutartis, AD susitarimas kaip priedas prie sutarties, sutarties atskiras skyrius<br>Numatytas tvarkytojų/subtvarkytojų auditas: taip / ne<br>AD teikimas į užsienio ne ES valstybes: taip /ne<br>Ar galima pasiekti tikslus netvarkant šių AD (aprašyti pagrindimą): taip / ne |
| |

## 5. Pavojų nustatymas ir įvertinimas

| Pavojaus ir poveikio fiziniam asmeniui pobūdis bei galima susijusi verslo rizika (aprašyti): | **Žalos tikimybė** | **Žalos sunkumas** | **Bendras pavojaus lygis** |
|---|---|---|---|
| | | | |

| | | | |
|---|---|---|---|
| | Mažai tikėtina<br>Tikėtina<br>Labai tikėtina | Minimali<br>Reikšminga<br>Sunki | Žemas<br>Vidutinis<br>Aukštas |

## 6. Priemonių sumažinti nustatymas

| Papildomos priemonės, kurios gali sumažinti ar panaikinti aukšto ar vidutinio lygio pavojus. | | | | |
|---|---|---|---|---|
| **Pavojus** | **Priemonės sumažinti ar pašalinti pavojų** | **Priemonės taikymo rezultatas** | **Likęs pavojus** | **Priemonė patvirtinta** |
| | | Pašalintas<br>Sumažintas<br>Priimtinas | Žemas<br>Vidutinis<br>Aukštas | Taip<br>Ne |

## 7. Išvados ir sprendimai

| **Priemonės ir likęs pavojus** | **Vardas, pavardė, data, parašas** | **Pastabos** |
|---|---|---|
| Priemonės patvirtintos: | | Įgyvendintos priemones pagal veiklos planą |
| Priemonės nepatvirtintos: | | Įtraukti numatytas priemones į veiklos planą, nustatant atlikimo terminą ir atsakingus asmenis |
| Likęs pavojus pripažintas priimtina rizika: | | Jei priimtina rizika pripažintas aukšto lygio pavojus priimtinas, privaloma kreiptis dėl išankstinės konsultacijos į Valstybinę duomenų apsaugos inspekciją |

## Duomenų apsaugos pareigūno nuomonė

| Nuomonė dėl AD tvarkymo teisėtumo, taikomų ir planuojamų priemonių bei galimybės tvarkyti AD: | |
|---|---|
| *Parašas, data* | *Vardas, pavardė,paraeigos* |

## Atsižvelgta į duomenų apsaugos pareigūno nuomonę

| Taip / ne (pagrindžiama, jeigu neatsižvelgta): | |
|---|---|
| *Parašas, data* | *Vardas, pavardė,pareigos* |

## Kitų asmenų nuomonės

| Nuomonės dėl AD tvarkymo teisėtumo, taikomų ir planuojamų priemonių | |
|---|---|
| *Paraša, datas* | *Vardas, pavardė,pareigos* |

## Atsižvelgta į kitų asmenų nuomones

| Taip / ne (pagrindžiama, jeigu neatsižvelgta): | |
|---|---|
| *Parašas, data* | *Vardas, pavardė, pareigos* |

## Už šio poveikio duomenų apsaugai vertinimo priežiūrą atsakingas asmuo

| Duomenų apsaugos pareigūnas ir atsakingo asmens tiesioginis vadovas turi būti informuoti apie AD tvarkymo atitiktį ataskaitoje nurodytoms išvadoms ir sprendimams | |
|---|---|
| *Parašas, data* | *Vardas, pavardė, pareigos* |