Vilniaus universitetas

POVEIKIO VERTINIMAS IR ADA VEIKLOS ĮRAŠŲ REGITRAS VILNIAUS UNIVERSITETE

Parengė Vilniaus universiteto duomenų apsaugos pareigūnas Viktoras Bulavas

Vilniaus universitetas

Vilniaus universitetas

Poveikio duomenų apsaugai vertinimas

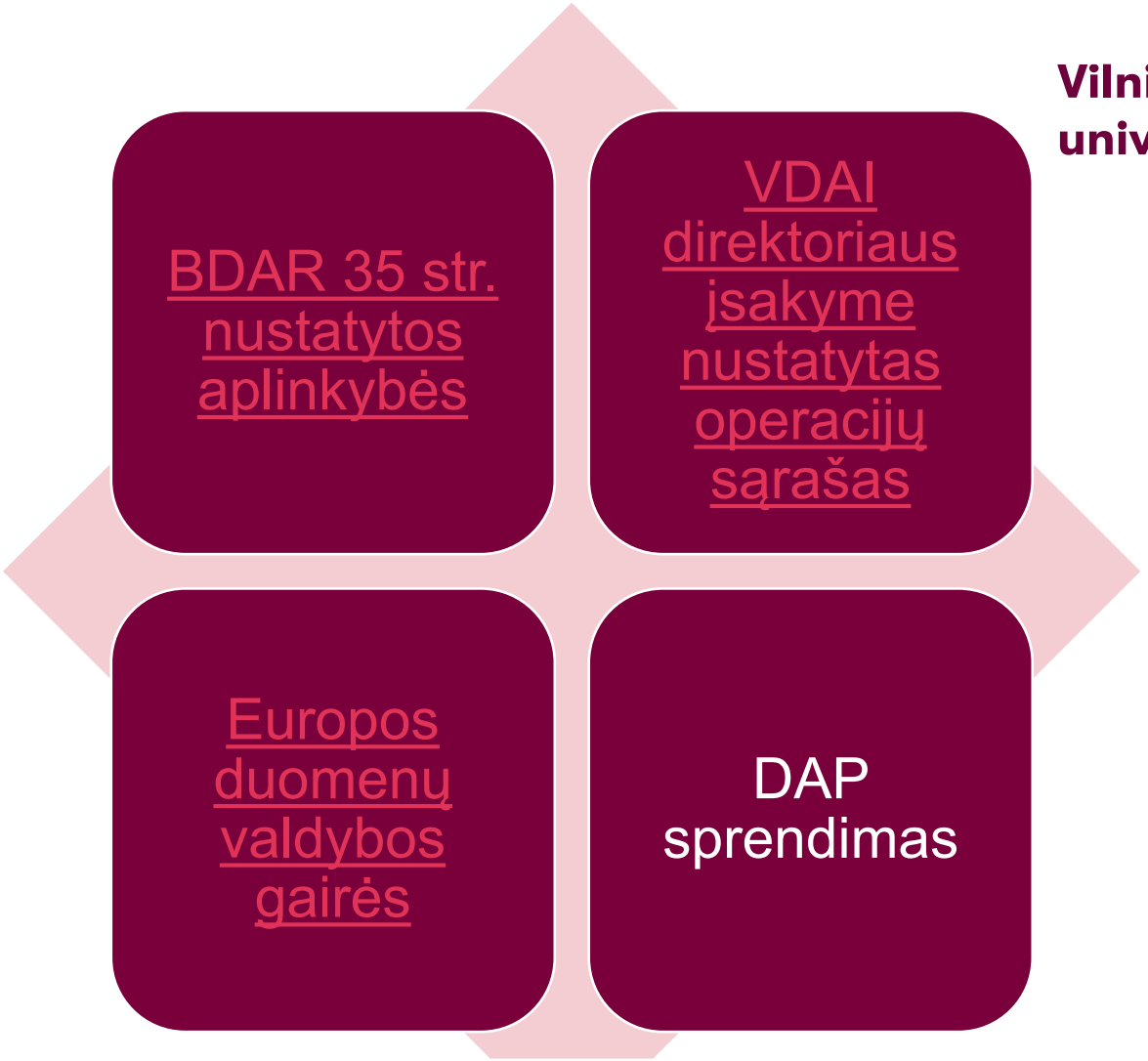
Vilniaus universitetas

Kada reikia atlikti vertinimą?

BDAR 35 str. Kai duomenų tvarkymo operacija galimai kelia didelį pavojų asmens teisėms ir laisvėms

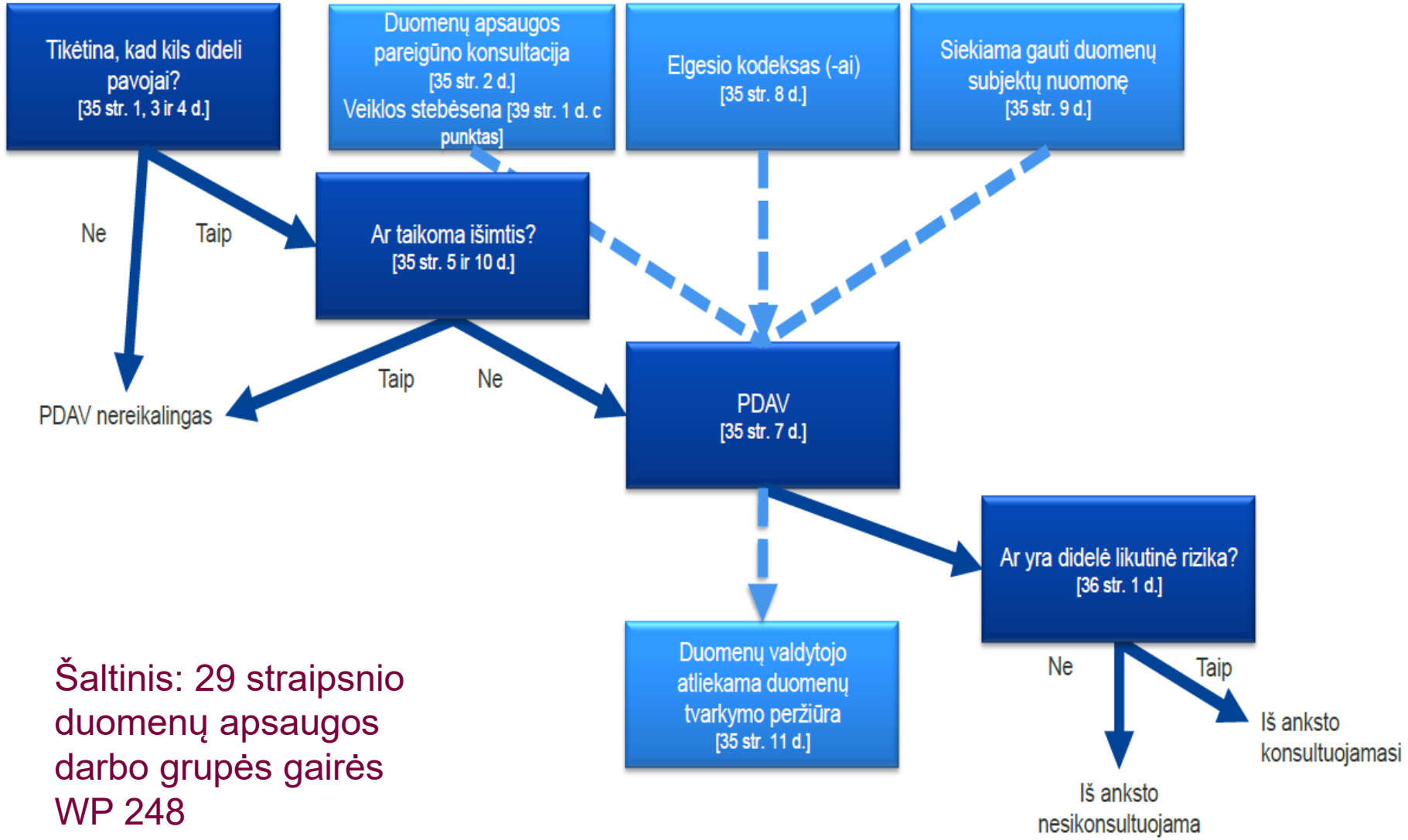
Vilniaus universitetas

Kada reikia atlikti vertinimą?



Būtų klaida nedaryti vertinimo, jei poveikis gali būti didelis, tačiau tvarkymo pobūdis tiesiogiai neįvardintas VDAI direktoriaus įsakyme

Toliau pateiktoje diagramoje parodyti pagrindiniai principai, susiję su BDAR nurodytu PDAV.



Šaltinis: 29 straipsnio duomenų apsaugos darbo grupės gairės WP 248

Vilniaus universitetas

Kada reikia atlikti vertinimą?

Prieš duomenų tvarkymą*

Kai reikia užtikrinti peržiūrą - yra naujos informacijos ar pasikeitimų

*VDAI DUK

Vilniaus universitetas

Kada dar reikia atlikti vertinimą?

Negalime įrodyti, kad:

- tvarkymas nekelia didelio pavojaus
- tvarkymas bus atliekamas nedideliu mastu

Vilniaus universitetas

DIDELIS PAVOJUS FIZINIŲ ASMENŲ TEISĖMS BEI LAISVĖMS

Tai situacija, kai dėl duomenų tvarkymo arba dėl galimo duomenų saugumo pažeidimo pažeidžiama ne tik asmens teisė į privatumą bet ir kitos pagrindinės teisės (žodžio, minties, judėjimo laisvės, teisė į laisvę, sąžinės ir tikėjimo laisvės ir pan.) ir duomenų subjektas dėl to, pvz., gali patirti atskirtį arba diskriminaciją, finansinius nuostolius, gali būti pakenkta jo reputacijai arba atsirasti kitokie rimti padariniai kasdieniam fizinio asmens gyvenimui.

Poveikio duomenų apsaugai vertinimas turi būti atliekamas prieš pradedant asmens duomenų tvarkymą. Jei poveikio vertinimo rezultatai parodytų, kad gali kilti didelis pavojus fizinių asmenų teisėms bei laisvėms, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti, turi būti konsultuojamasi su Valstybine duomenų inspekcija (BDAR 36 straipsnis).

Vilniaus universitetas

BDAR 35 str 1-2

1. 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 poveikio asmens duomenų apsaugai vertinimą.

    Panašius didelius pavojus keliančių duomenų tvarkymo operacijų sekai išnagrinėti galima atlikti vieną vertinimą.

2. Atlikdamas poveikio duomenų apsaugai vertinimą duomenų valdytojas konsultuojasi su duomenų apsaugos pareigūnu, jei toks yra paskirtas.

BDAR 35 str 3

Vilniaus universitetas

3. 1 dalyje nurodytas poveikio duomenų apsaugai vertinimas visų pirma turi būti atliekamas šiuo atveju:

a) 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;

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

c) sistemingas viešos vietos stebėjimas dideliu mastu.

BDAR 35 str 4-5

Vilniaus universitetas

4. Priežiūros institucija sudaro ir viešai paskelbia tų rūšių duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą pagal 1 dalį, sąrašą. Priežiūros institucija šiuos sąrašus pateikia 68 straipsnyje nurodytai Valdybai.

5. Priežiūros institucija taip pat gali sudaryti ir viešai paskelbti tų rūšių duomenų tvarkymo operacijų, kurioms netaikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašą. Priežiūros institucija šiuos sąrašus pateikia Valdybai.

BDAR 35 str 10: išimtys

Vilniaus universitetas

10. Jeigu duomenų tvarkymas pagal 6 straipsnio 1 dalies c arba e punktą turi teisinį pagrindą Sąjungos arba valstybės narės teisėje, kuri yra taikoma duomenų valdytojui, ir tokia teisė reglamentuoja atitinkamą konkrečią duomenų tvarkymo operaciją ar operacijų seką, o poveikio duomenų apsaugai vertinimas jau buvo atliktas kaip dalis bendro poveikio vertinimo priimant tą teisinį pagrindą, 1–7 dalys netaikomos, išskyrus atvejus, kai valstybės narės mano, kad prieš pradedant duomenų tvarkymo veiklą būtina atlikti tokį vertinimą.

Vilniaus universitetas

PROCESSING FOR SCIENTIFIC OR HISTORICAL PURPOSES WITHOUT CONSENT

The Board is of the opinion (EDPB Opinion 13/2018) that the processing of personal data for scientific or historical purposes on its own is not necessarily likely to represent a high risk. However, the processing of personal data for scientific or historical purpose in conjunction with at least one other criterion does require a DPIA to be carried out. The list submitted by the Lithuanian Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when there is a processing of personal data for scientific or historical purpose on its own.

The Board requests the Lithuanian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of personal data for scientific or historical purpose requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

Vilniaus universitetas

Kuo dar naudinga atlikti PDAV?

PDAV yra atskaitomybės priemonė, padedanti įrodyti, kad siekiant užtikrinti atitiktį BDAR, buvo vertintos rizikos, įvertintos ir pritaikytos organizacinės bei techninės priemonės

BDAR principai: 5 str.

Vilniaus universitetas

1. Asmens duomenys turi būti:

a) duomenų subjekto atžvilgiu tvarkomi teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas);

b) b) renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu; tolesnis duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais pagal 89 straipsnio 1 dalį nėra laikomas nesuderinamu su pirminiais tikslais (tikslo apribojimo principas);

BDAR principai: 5 str.

Vilniaus universitetas

c) adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (duomenų kiekio mažinimo principas);

d) tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi (tikslumo principas);

e) laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi; asmens duomenis galima saugoti ilgesnius laikotarpius, jeigu asmens duomenys bus tvarkomi tik archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais pagal 89 straipsnio 1 dalį, įgyvendinus atitinkamas technines ir organizacines priemones, kurių reikalaujama šiuo reglamentu siekiant apsaugoti duomenų subjekto teises ir laisves (saugojimo trukmės apribojimo principas);

BDAR principai: 5 str.

Vilniaus universitetas

f) tvarkomi tokiu būdu, kad taikant atitinkamas technines ar 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 (vientisumo ir konfidencialumo principas).

2. Duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi 1 dalies, ir turi sugebėti įrodyti, kad jos laikomasi (atskaitomybės principas).

Vilniaus universitetas

Operacijų sąrašas

Pagal Europos duomenų apsaugos valdybos pastabas patikslintas Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašas patvirtintas Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. kovo 14 d. įsakymu Nr. 1T- 35 (1.12.E).

VDAI DĮ 1T- 35 (1.12.E)

Vilniaus universitetas

1. Asmens duomenų tvarkymas vykdomas mokslinių ar istorinių tyrimų tikslais bent vienu iš žemiau nurodytų atvejų:

1.1. kai be duomenų subjekto sutikimo tvarkomi specialių kategorijų asmens duomenys arba asmens duomenų tvarkymas vykdomas susiejant ar derinant duomenų rinkinius;

1.2. kai tvarkomi nepilnamečių asmenų duomenys;

1.3. kai tvarkomas asmens kodas.

<2>

VDAI DĮ 1T- 35 (1.12.E)

Vilniaus universitetas

3 Asmens duomenų tvarkymas, kai duomenų gavėjų, kuriems buvo atskleisti asmens duomenys, informavimas apie asmens duomenų ištaisymą, ištrynimą arba tvarkymo apribojimą pagal Reglamento (ES) 2016/679 19 straipsnį, nėra įmanomas arba pareikalautų neproporcingų pastangų.

<4,5>

VDAI DĮ 1T- 35 (1.12.E)

Vilniaus universitetas

6. Asmens vaizdo duomenų tvarkymas, kai vaizdo stebėjimas vykdomas bent vienu iš žemiau nurodytų atvejų:

6.1. patalpose ir (ar) teritorijose, kurios nėra duomenų valdytojo valdomos nuosavybės ar kitais teisėtais pagrindais, kai vaizdo stebėjimas vykdomas laikantis Reglamento (ES) 2016/679 5 straipsnyje nustatytų su asmens duomenų tvarkymu susijusių principų;

6.2. sveikatos priežiūros, socialinės globos, įkalinimo įstaigose ir kitose įstaigose, kuriose paslaugos yra teikiamos pažeidžiamiems asmenims;

6.3. kartu su garso įrašymu.

7. Pokalbių telefonu įrašymas.

8. Asmens duomenų tvarkymas naudojant inovatyvias technologijas arba egzistuojančias technologijas panaudojant nauju būdu, kai tvarkomi pažeidžiamų duomenų subjektų asmens duomenys.

9. Vaikų asmens duomenų tvarkymas tiesioginės rinkodaros tikslais, vaikų asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, arba kai vaikams tiesiogiai yra siūlomos informacinės visuomenės paslaugos.

Nustatytos VDAI formos

Vilniaus universitetas

VDAI poveikio vertinimo forma

VDAI išankstinių konsultacijų forma

Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams

ISO standartuose numatyta metodika

Pildomi asmens duomenų veiklos tvarkymo įrašai

Vertinimo turinys

Vilniaus universitetas

PAVYZDINĖ POVEIKIO DUOMENŲ APSAUGAI ATLIKIMO FORMA

1. Priežastys, dėl kurių būtina atlikti poveikio duomenų apsaugai vertinimą

Planuojamos vykdyti veiklos aprašymas, jos tikslai ir planuojamos atlikti asmens duomenų tvarkymo operacijos. Paaiškinimas, kodėl būtina atlikti poveikio duomenų apsaugai vertinimą. Jei reikia, prie formos pridedami susiję dokumentai.

2. Asmens duomenų tvarkymo aprašymas

Aprašomi asmens duomenų rinkimo, naudojimo, saugojimo ir naikinimo veiksmai, nurodoma, iš kokių šaltinių bus renkami duomenys, kam bus teikiami (galima pateikti asmens duomenų tvarkymo veiksmų schemą). Aprašoma, kokie asmens duomenų tvarkymo veiksmai gali kelti pavojų fizinių asmenų teisėms ir laisvėms.

Vilniaus universitetas

Vilniaus universitetas

Asmens duomenų tvarkymo veiklų registras

Vilniaus universitetas

Asmens duomenų tvarkymo veiklos įrašai

- Bendrojo duomenų apsaugos reglamento (BDAR) 30 straipsnis numato duomenų valdytojams ir duomenų tvarkytojams pareigą tvarkyti duomenų tvarkymo veiklos įrašus, kuriuose būtų detaliai aprašytas atliekamas asmens duomenų tvarkymas.
- Veiklos įrašų tvarkymas Vilniaus Universitete:
  - Veiklos įrašus tvarko ir už jo turinį bei tikslumą atsako konkretų duomenų tvarkymo tikslą Universitete įgyvendinantis **padalinys**
  - **Duomenų apsaugos pareigūnas** valdo veiklos įrašų registrą, konsultuoja
  - Tvarkytojams – padaliniams – įrašus įvesti į registrą talkina įrašų registro IS tiekėjas

Asmens duomenų tvarkymo Vilniaus universitete taisyklės

Vilniaus universitetas

80. Duomenų tvarkymo veiklos įrašus tvarko ir už jo turinį bei tikslumą atsako konkretų duomenų tvarkymo tikslą Universitete įgyvendinantis **padalinys**.

13. **Duomenų apsaugos pareigūnas**:

13.1. kontroliuoja, kaip Universiteto darbuotojai ir kiti Universiteto asmens duomenų tvarkytojai vykdo šiame Apraše nustatytas asmens duomenų tvarkymo pareigas ir tvarko asmens duomenis;

...

13.8. konsultuoja asmens duomenų tvarkytojus asmens duomenų tvarkyme taikytinų organizacinių ir techninių priemonių parinkimo ir kitais asmens duomenų apsaugos klausimais;

13.9. koordinuoja duomenų tvarkymo veiklos įrašų parengimą;

Vilniaus
universitetas

Asmens duomenų tvarkymas: ką svarbu žinoti?

Vilniaus universitetas

Kas yra asmens duomenys?

Bet kuri informacija,

susijusi su fiziniu asmeniu,

kurio tapatybė gali būti nustatyta

Pavyzdžiai:

Vilniaus universitetas

Vardas, pavardė, asmens kodas, gyvenamosios vietos adresas, telefono ryšio numeris, elektroninio pašto adresas, pilietybė, socialinio draudimo numeris, gimimo data, banko kortelės numeris, išsilavinimo duomenys (baigta mokykla, diplomų ir sertifikatų duomenys), darbovietė, pajamos ir darbo užmokestis, duomenys apie turimą turtą (žemę, automobilį, butą, vertybinius popierius), duomenys apie sveikatą (sveikatos būklę, kraujo grupė ir kt.), vaizdo duomenys, biometriniai duomenys, šeimos narių duomenys (jei jie siejami su duomenų subjektu), pomėgiai, pirkimo ir pirkinių istorija, asmens lankomi interneto puslapiai, atsitiktinai sugeneruotas telefono ryšio numeris, buvimo vietos duomenys (pvz., buvimo vietos duomenys mobiliajame telefone), interneto protokolo (IP) adresas ir kt.

SVARBU! Nėra asmens duomenų baigtinio sąrašo.

Kas nėra laikoma asmens duomenimis?

Vilniaus universitetas

- Duomenys apie mirusį asmenį, išskyrus atvejus, kai duomenų tvarkymas gali pakenkti kitų asmenų teisėms ir laisvėms, numatytus valstybių narių teisėje (pavyzdžiui – asmeninė korespondencija LR CK 2.23 straipsnis 1 p., Po asmens mirties tokį sutikimą gali duoti jo sutuoktinis, tėvai ar vaikai.)
- Duomenys, kuriuos tvarko fizinis asmuo, užsiimdamas išimtinai asmenine ar namų ūkio veikla
- Duomenys apie juridinį asmenį (pvz., juridinio asmens kodas, el. pašto adresas- info@imone.lt)
- Anoniminiai duomenys (pvz., nuasmeninti duomenys, šifruoti duomenys, statistiniai duomenys ir pan.)

Vilniaus universitetas

Išimtys po mirties (LR CK 2.23 straipsnis. Teisė į privatų gyvenimą ir jo slaptumą

1. Fizinio asmens privatus gyvenimas neliečiamas. Informacija apie asmens privatų gyvenimą gali būti skelbiama tik jo sutikimu. Po asmens mirties tokį sutikimą gali duoti jo sutuoktinis, tėvai ar vaikai.
2. Privataus gyvenimo pažeidimu laikomas neteisėtas įėjimas į asmens gyvenamąsias ir kitokias patalpas, aptvertą privačią teritoriją, neteisėtas asmens stebėjimas, neteisėtas asmens ar jo turto apieškojimas, asmens telefoninių pokalbių, susirašinėjimo ar kitokios korespondencijos bei asmeninių užrašų ir informacijos konfidencialumo pažeidimas, duomenų apie asmens sveikatos būklę paskelbimas pažeidžiant įstatymų nustatytą tvarką bei kitokie neteisėti veiksmai.
3. Draudžiama rinkti informaciją apie privatų asmens gyvenimą pažeidžiant įstatymus.

Ar aš tvarkau asmens duomenis?

Vilniaus universitetas

Duomenų tvarkymas – sąvoka, apimanti **visus** įmanomus veiksmus su asmens duomenimis pvz.:

- rinkimas, įrašymas;
- rūšiavimas, sisteminimas;
- saugojimas;
- adaptavimas ar keitimas;
- susipažinimas, naudojimas;
- atskleidimas;
- ištrynimas, sunaikinimas ir pan.

Pavyzdžiai:

Vilniaus universitetas

- Personalo valdymas ir darbo užmokesčio administravimas;
- Prieiga prie kontaktų duomenų bazės;
- Tiesioginės rinkodaros (reklaminių) elektroninių laiškų siuntimas;
- Dokumentų, kuriuose yra asmens duomenų, naikinimas;
- Prekyba elektroninėje erdvėje (el. parduotuvė);
- Asmens nuotraukos skelbimas interneto svetainėje;
- Vaizdo įrašymas (apsauginė vaizdo stebėjimo sistema);
- Duomenų saugojimas duomenų bazėje, „Excel“ lentelėje, informacinėje sistemoje, popieriniame žurnale;
- Duomenų gavimas iš registrų, bankų ar kt.;
- Duomenų teikimas kurjerių tarnyboms, draudimo įmonėms;
- Duomenų paskelbimas skelbimų lentoje, internete;
- Telefoninių pokalbių įrašymas ir saugojimas ir kt.

Vilniaus universitetas

Asmens duomenų tvarkymo veiklos įrašų registras

Informacinių išteklių įstatyme:

....

6. **Registras** – teisinių, organizacinių, techninių ir programinių priemonių visuma, skirta registro objektui registruoti ir registro duomenims, registro informacijai, registrui pateiktiems dokumentams ir (arba) jų kopijoms tvarkyti ir naudoti.

7. **Registro duomenys** – registro objekto duomenys, surinkti iš objektui registruoti pateiktų duomenų, informacijos, dokumentų ir (arba) jų kopijų, papildyti registro objekto identifikavimo kodu, susijusio registro perduotais ir registravimo procedūrų duomenimis.

8. **Registro informacija** – su registro objektu susijusi informacija, surinkta iš registrui pateiktų duomenų, informacijos, dokumentų ir (arba) jų kopijų (išskyrus registro duomenis).

Vilniaus universitetas

Asmens duomenų tvarkymo veiklos įrašų registras

Informacinių išteklių įstatyme:

....

9. **Registro objektas** – registre registruojamas asmuo, veikla, daiktas, daikto buvimo vieta, daiktinė teisė, teisės suvaržymas, juridinis faktas, dokumentas, teritorija, gamtos išteklius, kultūros vertybė, intelektinė (pramoninė) nuosavybė, komunikacijų priemonė ir (arba) kitas objektas.

10. **Registro objekto įregistravimas** – registro objektui registruoti pateiktų duomenų, informacijos, dokumentų ir (arba) jų kopijų įvertinimas, sprendimo registruoti registro objektą priėmimas, identifikavimo kodo registro objektui suteikimas, registro duomenų ir registro informacijos sudarymas ir įrašymas į registro duomenų bazę, papildymas registravimo procedūrų ir susijusio registro perduotais duomenimis ir teisės aktų nustatytais atvejais ir tvarka dokumento, kuriuo patvirtinamas registro objekto registravimo registre faktas, išdavimas, jeigu toks dokumentas yra išduodamas.

Veiklos įrašo struktūra

Vilniaus universitetas

Duomenų tvarkymo tikslas
Duomenų subjekto aprašymas
Asmens duomenų kategorijos
Duomenų gavėjai
Asmens duomenų perdavimas į trečiąją valstybę ar tarptautinę organizaciją
Numatomi asmens duomenų saugojimo ir ištrynimo terminai
... ir t.t.

Saugumo priemonės

Saugumo priemonės

Vilniaus universitetas

VDAI yra pateikusi rekomendacijas dėl saugumo priemonių:

- Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams (3 versija, 2020 06 18)

Saugumo priemonės : organizacinės ir techninės

- Saugumo priemonių sąrašas ir kontrolinis klausimynas perkelti į veiklos įrašų registrą naudotojams.

Saugumo priemonės

Vilniaus universitetas

Organizacinės saugumo priemonės

- Asmens duomenų saugumo politika ir procedūros;
- Vaidmenys ir atsakomybės;
- Prieigos valdymo politika;
- IT išteklių ir turto valdymas;
- IT pakeitimų valdymas;
- Duomenų tvarkytojai;
- Asmens duomenų saugumo pažeidimai ir incidentai;
- Veiklos tęstinumas;
- Personalo konfidencialumas;
- Mokymai

Techninės saugumo priemonės

- Prieigų kontrolė ir autentifikavimas;
- Techninių žurnalų įrašai ir stebėsena
- Tarnybinių stočių, duomenų bazių apsauga
- Darbo stočių apsauga
- Tinklo ir komunikacijos sauga
- Atsarginės kopijos
- Mobilieji, nešiojami įrenginiai
- Programinės įrangos sauga
- Duomenų naikinimas, šalinimas
- Fizinė sauga

Vilniaus universitetas

KONTAKTAI

Viktoras Bulavas, duomenų apsaugos pareigūnas

+370 5 236 6200 dap@vu.lt

Zita Ambrutytė, veiklos įrašų įvedimo registre klausimais,

+370 616 51951, zita.ambrutyte@bsas.lt