|  |  |
| --- | --- |
| **KAS YRA POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS?****KADA IR KAIP JIS ATLEIKAMAS?** |  |

 Dėl sparčios skaitmeninių technologinių priemonių plėtros ir jų panaudojimo galimybių renkant asmens duomenis nuolat auga asmens duomenų rinkimo ir keitimosi jais mastas. Technologijos leidžia institucijoms vykdant savo veiklą naudoti asmens duomenis (toliau – AD) dideliu mastu. Siekiant užtikrinti fizinių asmenų teisių ir laisvių apsaugą tvarkant AD reikia imtis tinkamų techninių ir organizacinių priemonių siekiant užtikrinti, kad būtų laikomasi 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 – BDAR) reikalavimų.

 Kai vykdant AD tvarkymo operacijas gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas privalo atlikti poveikio duomenų apsaugai vertinimą (toliau – PADV), kad būtų įvertinta visų pirma to pavojaus kilmė, pobūdis, specifika ir rimtumas.

 PADV turi būti numatytos priemonės, kuriomis duomenų valdytojas užtikrins aukštą asmens duomenų apsaugos lygį, bei nebus pažeistas tvarkomų (persiunčiamų) asmens duomenų prieinamumas, autentiškumas, vientisumas ir konfidencialumas.

 Valstybinė duomenų apsaugos inspekcija pažymi, kad PADV turi būti atliekamas ne tik kai duomenų valdytojas pradeda naujai tvarkyti AD, bet ir jau iki BDAR įsigaliojimo duomenų valdytoja jau pradėjęs vykdyti AD rinkimo operacijas, kurių sąrašas patvirtintas Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. kovo 14 d. įsakymu Nr. 1T-35 (1.12.E) „Dėl duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“ (toliau – sąrašas) <https://vdai.lrv.lt/lt/naujienos/veiklos-del-kuriu-tures-buti-atliekamas-poveikio-duomenu-apsaugai-vertinimas> . Sąraše numatyta, kad PADV privalomas, kai vykdomas vaizdo stebėjimas, pokalbių telefonu įrašymas vaizdo ir (ar) garso duomenų tvarkymas darbo vietoje ir etc.

***Kaip atliekamas PADV?***

**Poveikio duomenų apsaugai vertinimas (toliau – PDAV)** – poveikio duomenų apsaugai vertinimo procedūra, kurios metu nustatoma koks ir kiek rizikingas poveikis kils duomenų subjektams, jei bus pradedama vykdyti nauja ar iš esmės atnaujinama vykdoma duomenų tvarkymo operacija.

****PDAV tikslas yra sistemiškai identifikuoti rizikas ir galimą asmens duomenų tvarkymo poveikį ir ištirti bei įvertinti alternatyvius duomenų tvarkymo procesus tam, kad būtų galima sušvelninti galimas privatumo grėsmes.

PDAV turi būti įgyvendintas prieš asmens duomenų tvarkymo operacijos vykdymo pradžią. Atitinkamai, PDAV turi prasidėti taip anksti, kaip yra praktiška kuriant arba atnaujinant tvarkymo operaciją, net jei tam tikri jos aspektai vis dar nėra žinomi. Tai, kad gali prireikti atnaujinti PDAV, kai tvarkymas jau bus prasidėjęs, nėra pateisinama priežastis atidėti ar nevykdyti PDAV.

Sistemoms, kurios niekaip neidentifikuoja asmenų, įprastai nekeliamas reikalavimas atlikti PDAV.

Tačiau būtina atsižvelgti į tai, kad tai, kas gali atrodyti nuasmenintais duomenimis, iš tikro gali būti identifikuojantys naudojant juos kartu su kita informacija, taigi nuasmeninti duomenys turėtų būti atidžiai įvertinti, siekiant įsitikinti, kad jais nebus identifikuojami individai.

**Nuo ko pradėti?**

**Įprastai kartu su duomenų apsaugos pareigūnu (toliau - DAP) įvertinami šie kriterijai:**

* + - ar automatizuotai (technologinėmis priemonėmis, be jokio žmogaus įsikišimo) priimami sprendimai, duomenų subjektams sukeliantys teisinį arba panašų rimtą poveikį (pavyzdžiui, duomenų tvarkymas gali lemti asmenų atskirtį arba diskriminaciją);
		- ar atliekama sisteminga stebėsena, t. y. duomenų tvarkymas, kuris reikalingas duomenų subjektų stebėsenos arba kontrolės tikslais, įskaitant tinkluose surinktus duomenis arba sistemingą viešos vietos stebėjimą dideliu mastu;
		- ar tvarkomi neskelbtini duomenys arba labai asmeniški duomenys (pavyzdžiui, specialių kategorijų asmens duomenys, duomenys apie apkaltinamuosius nuosprendžius ar nusikalstamas veikas, vietos nustatymo duomenys ir pan.);
		- ar duomenys tvarkomi dideliu mastu (vertinant, ar duomenys tvarkomi dideliu mastu, turi būti atsižvelgiama į susijusių duomenų subjektų skaičių (konkretų skaičių arba atitinkamą gyventojų dalį), tvarkomų duomenų kiekį ir intervalą ir (arba) skirtingų tvarkomų duomenų įvairovę, duomenų tvarkymo veiklos trukmę arba pastovumą, geografinį duomenų tvarkymo veiklos mastą);
		- ar atliekamos sudėtingos duomenų tvarkymo operacijos (pavyzdžiui, keli asmens duomenų tvarkymo tikslai ir (ar) duomenų valdytojai, duomenų rinkinių siejimas ir derinimas, kai duomenų tvarkymo operacijos atliekamos taip, kad viršija pagrįstus duomenų subjekto lūkesčius, ir pan.);
		- ar tvarkomi duomenys, susiję su pažeidžiamais duomenų subjektais (pavyzdžiui, vaikais, darbuotojais, labiau pažeidžiamais gyventojais, kuriems reikalinga speciali apsauga, ir visais atvejais, kai galima nustatyti nelygiaverčius duomenų subjekto ir duomenų valdytojo santykius);

 Kuo daugiau iš klausimyne nurodytų kriterijų atitinka tvarkymas, tuo labiau tikėtina, kad jis kelia didelę grėsmę duomenų subjektų teisėms bei laisvėms ir atitinkamai reikalauja PDAV.

 Tvarkymas, atitinkantis mažiau nei du kriterijus, įprastai nereikalaus PDAV dėl žemesnės rizikos, tačiau būtina racionaliai įvertinti faktinę situaciją. Atitinkamai asmens duomenų rinkimo iniciatorius visais atvejais privalo konsultuotis su DAP.

Kai nustatomos tvarkymo situacijos ir susijusių asmens duomenų pobūdis, asmens duomenų rinkimo iniciatorius (projekto vadovas) įvertina grėsmes duomenų subjektų teisėms ir laisvėms.

 Esminiai duomenų subjektams kylančių grėsmių tipai, atitinkantys duomenų saugumo pažeidimų rūšis, yra šie:

|  |  |  |
| --- | --- | --- |
| Konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama prieiga tam teisės neturintiems asmenims. | Pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami. | Vientisumo pažeidimas – netyčia ar neteisėtai atliekami nepageidaujami asmens duomenų pakeitimai. |

Nustatant pavojus fizinių asmenų teisėms ir laisvėms ir juos vertinant turi būti atsižvelgiama į pavojų kilmę, pobūdį, specifiką ir rimtumą, t. y. į kiekvieną pavojų (neteisėtą prieigą prie asmens duomenų, nepageidaujamą asmens duomenų pakeitimą ir asmens duomenų praradimą) iš duomenų subjektų perspektyvos, taip pat į žalos (žala gali būti fizinė, materialinė ir (arba) nematerialinė), kuri duomenų subjektams gali kilti dėl asmens duomenų tvarkymo arba galimo asmens duomenų saugumo pažeidimo, tikimybę ir sunkumą.

Pavojus fizinių asmenų teisėms ir laisvėms, atsižvelgiant į pavojaus ir pavojaus poveikio fiziniam asmeniui pobūdį, gali būti:

|  |  |  |
| --- | --- | --- |
| Mažas (kai asmens duomenų tvarkymas arba galimas asmens duomenų saugumo pažeidimas duomenų subjektų teisėms ir laisvėms įtakos neturės arba padariniai kasdieniam fizinio asmens gyvenimui bus mažareikšmiai). | Vidutinis (kai dėl asmens duomenų tvarkymo arba dėl galimo asmens duomenų saugumo pažeidimo duomenų subjektams gali būti sunkiau laikinai naudotis savo teisėmis ir laisvėmis, gali atsirasti kitokių neigiamų padarinių kasdieniam fizinio asmens gyvenimui). | Didelis (kai dėl asmens duomenų tvarkymo arba dėl galimo asmens duomenų saugumo pažeidimo duomenų subjektams gali būti sunku arba neįmanoma pasinaudoti savo teisėmis ir laisvėmis, duomenų subjektas gali patirti atskirtį ar diskriminaciją, finansinių nuostolių, gali būti pakenkta jo reputacijai arba atsirasti kitokių rimtų neigiamų padarinių kasdieniam fizinio asmens gyvenimui). |

Jei atliekant PDAV paaiškėja, kad tvarkant asmens duomenis kiltų didelis pavojus duomenų subjektų teisėms ir laisvėms, duomenų valdytojas, prieš pradėdamas tvarkyti asmens duomenis, privalo iš anksto konsultuotis su Valstybine duomenų apsaugos inspekcija.

Jei atlikus PDAV iš esmės pasikeičia asmens duomenų tvarkymo pobūdis, aprėptis, kontekstas ir (ar) tikslai arba duomenų rinkimo/projekto raida ar įgyvendinimas daro naują įtaką privatumui, kuri anksčiau nebuvo įvertinta, turi būti atliekamas naujas PDAV.

*Pateikiu viešai skelbiamų PADV:*

[*https://e-seimas.lrs.lt/rs/lasupplement/TAK/83f65610a57411eaa51db668f0092944/ed195081a57411eaa51db668f0092944/format/ISO\_PDF/*](https://e-seimas.lrs.lt/rs/lasupplement/TAK/83f65610a57411eaa51db668f0092944/ed195081a57411eaa51db668f0092944/format/ISO_PDF/)

[*https://vilniausmiesto.teismas.lt/data/public/uploads/2020/06/doc06879020200617100728.pdf*](https://vilniausmiesto.teismas.lt/data/public/uploads/2020/06/doc06879020200617100728.pdf)

*PADV forma:* [*https://vdai.lrv.lt/uploads/vdai/documents/files/Pavyzd\_PDAV\_forma.docx*](https://vdai.lrv.lt/uploads/vdai/documents/files/Pavyzd_PDAV_forma.docx)

*Šaltiniai:*

*2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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)*

*<https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679>*

[*https://am.lrv.lt/uploads/am/documents/files/wp248\_PDAV\_gaires\_2017-04-04.pdf*](https://am.lrv.lt/uploads/am/documents/files/wp248_PDAV_gaires_2017-04-04.pdf)