Kauno rajono savivaldybės
administracijos
asmens duomenų apsaugos
politikos
3 priedas

POVEIKIO DUOMENŲ APSAUGAI VERTINIMO PROCEDŪRA

I. SĄVOKOS

1. Duomenų saugumo pažeidimas reiškia pažeidimą, 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.

2. Administracija – Kauno rajono savivaldybės administracija, juridinio asmens kodas: 188756386, buveinės adresas: Savanorių pr. 371, Kaunas.

3. Poveikio duomenų apsaugai vertinimo procedūra (toliau – PDAV) reiškia poveikio duomenų apsaugai vertinimą.

4. Priežiūros institucija reiškia valstybės narės pagal BDAR 51 straipsnį įsteigtą nepriklausomą valdžios instituciją. Lietuvos Respublikos atveju tokia institucija yra Valstybinė duomenų apsaugos inspekcija.

5. Procedūra reiškia šią Poveikio duomenų apsaugai vertinimo procedūrą.

6. Projekto vadovas (toliau – PV) reiškia asmenį, kuris yra atsakingas už projektą, kurio metu sukuriama nauja ar iš esmės atnaujinama Administracijos vykdomo automatinio duomenų tvarkymo sistema.

II. APIMTIS

7. Šis dokumentas taikomas PDAV procedūroms, kurias Duomenų valdytojas vykdo naujos ar atnaujintos automatinio duomenų tvarkymo sistemos kūrimo pradžioje ir jos metu.

III. PROCESAS

8. PDAV tikslas yra sistemiškai identifikuoti rizikas ir galimą Asmens duomenų rinkimo, saugojimo ir skleidimo poveikį ir ištirti bei įvertinti alternatyvius duomenų tvarkymo procesus tam, kad būtų galima sušvelninti galimas privatumo grėsmes.

9. PDAV atlikimas yra privalomas tada, jei tam tikro pobūdžio duomenų tvarkymas gali kelti didelį pavojų, visų pirma tada, kai naudojamos naujos technologijos, atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms.

10. PDAV turėtų būti įgyvendintas prieš tvarkymą. Atitinkamai, PDAV turėtų prasidėti taip anksti, kaip yra praktiška kuriant 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.

11. Kai duomenų tvarkymas tikėtinai gali kelti didelę riziką fizinių asmenų teisėms ir laisvėms, Administracija kaip duomenų valdytojas turi atlikti PDAV tam, kad būtų įvertinta visų pirma to pavojaus kilmė, pobūdis, specifika ir rimtumas.

12. Kiekvienam projektui, kurio metu planuojama sukurti naujas ar iš esmės atnaujinti esamas Administracijos valdomas automatinio duomenų tvarkymo sistemas, turi būti priskiriamas Darbuotojas, veikiantis kaip PV ir atitinkamai esantis atsakingas už tokio projekto vykdymą.

13. PDAV atliekamas PV bendradarbiaujant su atitinkamomis suinteresuotomis šalimis ir duomenų apsaugos pareigūnu.

14. Vienas PDAV gali įvertinti keletą panašių tvarkymo operacijų, keliančių panašias dideles rizikas.

15. 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.

IV. 1 ETAPAS – POREIKIO ATLIKTI PDAV NUSTATYMAS

16. Šio etapo metu PV atsako į atrankos klausimus.

17. Atrankos klausimai skirti nustatyti, ar yra reikalingas PDAV. Jei atsakymas į bet kurį iš šių klausimų yra „taip“, PDAV turėtų būti atliekamas:

17.1. Ar sistema tikėtinai gali kelti didelę riziką fizinių asmenų teisėms ir laisvėms?

17.2. Ar sistema apima sistemingą ir išsamų su fiziniais asmenimis susijusių asmeninių aspektų vertinimą, 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?

17.3. Ar ši sistema apima specialių kategorijų duomenų, atitinkamai (a) asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, (b) genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją ar (c) asmens duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymą dideliu mastu?

17.4. Ar šia sistema naudojantis bus atliekamas sistemingas viešos vietos stebėjimas dideliu mastu?

17.5. Ar šia sistema atliekamos tvarkymo operacijos, kurioms taikomas reikalavimas atlikti PDAV pagal Priežiūros institucijos parengtą tokių operacijų sąrašą?

18. Kiti kriterijai kurie turėtų būti įvertinti kaip galintys lemti duomenų tvarkymo operacijų „didelę riziką“, dėl kurios reikėtų atlikti PDAV, yra tokie:

18.1. Ar duomenys yra tvarkomi dideliu mastu? Į žemiau įvardytus faktorius turėtų būti atsižvelgta sprendžiant, ar tvarkymas atliekamas dideliu mastu:

18.1.1. Paveikiamų duomenų subjektų skaičius kaip konkretus skaičius arba kaip proporcija iš atitinkamos populiacijos;

18.1.2. Duomenų kiekį ir/ar tvarkomų skirtingų duomenų spektrą;

18.1.3. Duomenų tvarkymo veiksmų trukmę arba pastovumą;

18.1.4. Tvarkymo veiksmų geografinę apimtį.

18.2. Ar duomenų rinkiniai buvo suderinti arba sujungti tada, kai, pavyzdžiui, jie kilo iš dviejų ar daugiau skirtingų duomenų tvarkymo veiklų, atliktų skirtingais tikslais ir/arba skirtingų duomenų valdytojų, tokiu būdu, kuris peržengtų pagrįstus duomenų subjekto lūkesčius?

18.3. Ar tvarkomi duomenys susiję su labiau pažeidžiamais duomenų subjektais (vaikais, darbuotojais, pacientais ir t.t.)?

18.4. Ar tvarkymas vykdomas pritaikant inovatyvius technologinius ar organizacinius sprendimus?

18.5. Ar duomenys bus perduodami už Europos Sąjungos ribų?

18.6. Ar pats duomenų tvarkymas gali apriboti duomenų subjektų galimybės įgyvendinti savo teises arba naudotis paslaugomis ar sudaryti sutartį?

19. Kuo daugiau iš aukščiau 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 PV visais atvejais privalo išsamiai aprašyti savo sprendimą nevykdyti PDAV.

20. Jei pagal atsakymus į aukščiau nurodytus klausimus arba egzistuojant kitiems „didelės rizikos“ egzistavimo pagrindams PDAV turėtų būti atliekamas, tada PV tęsia pagal Procedūros 2 etapą.

21. Procedūra pakartojama tada, jei atliekami esminiai vertinto duomenų tvarkymo pakeitimai.

V. 2 ETAPAS – PASIRUOŠIMAS

22. PV parengia sistematišką planuojamų tvarkymo procedūrų ir jų tikslų aprašymą įskaitant, kur tai tinkama, Administracijos, kaip duomenų valdytojo, siekiamus teisėtus interesus.

23. Tuo atveju, jei teisėtų interesų siekimas yra taikomas kaip teisėto duomenų tvarkymo pagrindas, Administracija taip pat turėtų išsiaiškinti duomenų subjektų ar jų atstovų nuomonę apie numatytą duomenų tvarkymą. Jei Administracija tokiu atveju priima sprendimą nesiaiškinti duomenų subjektų nuomonės arba jos galutinis sprendimas skiriasi nuo duomenų subjektų išreikštos nuomones, tokių sprendimų pateisinimas turi būti aprašomas.

VI. 3 ETAPAS – DUOMENŲ RINKIMAS

24. Šiame etape PV kritiškai išanalizuoja asmens duomenų tvarkymo situacijas, nustatytas 2 etapo metu.

25. DV privalo išanalizuoti ir aprašyti esmines su asmens duomenimis susijusias sritis atsakydamas į šiuos klausimus:

25.1. Kokie duomenys bus tvarkomi?

25.2. Koks yra duomenų tvarkymo tikslas(-ai)?

25.3. Kaip vyksta duomenų tvarkymo procesas (aprašyti, kaip duomenų tvarkymas vyksta nuo duomenų gavimo iki sunaikinimo)?

25.4. Ar duomenų subjektui bus pateikiama visa reikiama informacija?

25.5. Ar visi tvarkomi asmens duomenys būtini duomenų tvarkymui vykdyti (pagrįsti būtinumą)?

25.6. Ar duomenys yra tikslūs ir esant poreikiui atnaujinami?

25.7. Kiek laiko saugomi duomenys?

25.8. Kaip duomenų subjektai informuojami apie duomenų tvarkymą?

25.9. Jei duomenys tvarkomi remiantis sutikimu, kokiu būdu jis gaunamas?

25.10. Kaip duomenų subjektai gali įgyvendinti savo teises?

25.11. Jei pasitelkiamas duomenų tvarkytojas ar tvarkytojai, ar jų pareigos tinkamai aprašytos susitarime pagal BDAR reikalavimus?

25.12. Jei duomenys teikiami už Europos Sąjungos ribų, ar duomenys yra tinkamai apsaugomi?

25.13. Kokias saugumo priemones Administracija įgyvendins siekdama apsaugoti asmens duomenis?

VII. 4 ETAPAS – RIZIKOS NUSTATYMAS

26. Kai nustatomos tvarkymo situacijos ir susijusių asmens duomenų pobūdis, PV įvertina grėsmes duomenų subjektų teisėms ir laisvėms.

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

27.1. Konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama prieiga tam teisės neturintiems asmenims;

27.2. Pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami;

27.3. Vientisumo pažeidimas – netyčia ar neteisėtai atliekami nepageidaujami asmens duomenų pakeitimai.

28. Įvardijęs grėsmes, PV jas aprašo atsakydamas į šiuos klausimus:

28.1. Kokios tikėtinos pasekmės duomenų subjektams tada, jei įvyktų pažeidimas?

28.2. Kokie veiksmai/įvykiai galėtų sudaryti sąlygas tokiam pažeidimui įvykti?

28.3. Kokie yra grėsmės šaltiniai (asmenys ar aplinkybes, dėl kurių tyčia ar atsitiktinai gali įvykti pažeidimas)?

29. PV įvertina sistemos atitiktį reikalavimams, nustatytiems BDAR ir atitinkamuose įstatymuose ir kituose teisės aktuose.

VIII. 5 ETAPAS – RIZIKOS VALDYMO PRIEMONIŲ NUSTATYMAS

30. Šio etapo metu PV turi aprašyti, kokios esamos ar planuojamos techninės (fizinio ir kibernetinio saugumo) bei organizacinės priemonės padės suvaldyti nustatytas grėsmes duomenų subjektų teisėms ir laisvėms. Pirmenybė teikiama reikšmingiausioms nustatytoms saugumo grėsmėms ir jų valdymo priemonėms, tačiau turi būti pagrindžiamas tam tikrų grėsmių ignoravimas.

31. Aprašius rizikos valdymo priemones, turi būti nurodoma, kokio rimtumo ir tikėtinumo grėsmė išlieka atsižvelgiant į taikomas ar planuojamas taikyti priemones, skirtas jo išvengti.

IX. 6 ETAPAS – REZULTATŲ ATASKAITOS TEIKIMAS

32. Šiame etape PV parengia ataskaitą apie PDAV rezultatus.

33. Ataskaitoje turi būti aprašomi ankstesnių etapų eiga ir rezultatai, nurodomi konkretūs veiksmai, kurių reikia imtis siekiant suvaldyti kylančias grėsmes, jei esamų rizikos valdymo priemonių tam nepakanka.

34. Kai iš PDAV paaiškėja, kad duomenų tvarkymo operacijos kelia didelį pavojų duomenų subjektų teisėms ir laisvėms, o duomenų valdytojas jo negali sumažinti tinkamomis rizikos valdymo priemonėmis, atsižvelgiant į turimas technologijas ir įgyvendinimo sąnaudas, prieš pradedant duomenų tvarkymą turi būti konsultuojamasi su Priežiūros institucija.

35. Duomenų tvarkymo veiklos kūrimo procesui tęsiantis, PDAV turėtų būti peržiūrėtas, patikslintas ir atnaujintas jei projekto raida ar įgyvendinimas daro naują įtaką privatumui, kuri anksčiau nebuvo įvertinta.