PATVIRTINTA
BĮ „Adakavo socialinių paslaugų namai“
direktoriaus
2023 m. kovo 13 d. įsakymu Nr. V-37

POVEIKIO DUOMENŲ APSAUGAI VERTINIMO PROCEDŪRA

I. BENDROSIOS NUOSTATOS

1. Poveikio duomenų apsaugai vertinimo (toliau – PDAV) procedūra skirta įvertinti asmens duomenų tvarkymo reikalingumą ir proporcingumą. Ši procedūra padeda numatyti, kokioms fizinių asmenų teisėms ir laisvėms kyla pavojus dėl asmens duomenų tvarkymo.

2. 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 sumažinti kylančias grėsmes.

3. PDAV atlikimas yra privalomas operacijoms ar jų grupėms, nurodytoms Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) paskelbtame sąraše, taip pat toms, kurios 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.

4. PDAV reikėtų atlikti prieš duomenų tvarkymą arba kuo anksčiau, jei duomenų tvarkymas jau yra pradėtas.

II. POREIKIO ATLIKTI PDAV IDENTIFIKAVIMAS

5. Siekiant įvertinti potencialią riziką ir PDAV poreikį, reikia atsakyti į šiuos klausimus:

5.1. Ar buvo pradėtos naudoti naujos technologijos, operacinės sistemos?

5.2. 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?

5.3. Ar yra tvarkomos dideliu mastu specialios asmens duomenų kategorijos:

5.3.1. atskleidžiančios rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose,

5.3.2. genetiniai duomenys, biometriniai duomenys, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenys arba duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.

5.4. Ar yra tvarkomi dideliu mastu asmens duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas?

5.5. Ar bus atliekamas sistemingas viešos vietos stebėjimas dideliu mastu?

5.6. Ar tvarkomi pažeidžiamų duomenų subjektų duomenys, (pvz. vaikų, asmenų, kuriems reikalinga speciali apsauga ir t.t.)?

5.7. Ar duomenys yra perduodami už Europos Sąjungos ribų?

5.8. Ar asmens duomenys bus tvarkomi tokiu būdu, kurio duomenų subjektas negalėtų numatyti?

6. Siekiant įvertinti ar asmens duomenų tvarkymas vyksta dideliu mastu, reikia atsižvelgti į šiuos faktorius:

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

6.2. Duomenų tvarkymo veiksmų trukmę arba pastovumą;

6.3. Tvarkymo veiksmų geografinę apimtį.

7. Kuo daugiau buvo atsakyta teigiamai į pateiktus atrankos klausimus, tuo labiau tikėtina, kad asmens duomenų tvarkymas 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 atsakingas asmuo visais atvejais privalo išsamiai aprašyti ir pagrįsti savo sprendimą nevykdyti PDAV.

III. DUOMENŲ TVARKYMO BŪTINUMAS IR PROPORCINGUMAS

8. Jei įvertinus PDAV poreikį, nustatoma, kad tam tikroms asmens duomenų tvarkymo operacijoms ar jų grupėms yra reikalingas PDAV, toliau analizuojamas tvarkymo operacijų ar jų grupių būtinumas ir proporcingumas, rizika duomenų subjektų teisėms ir laisvėms, nustatomos organizacinės ir techninės apsaugos priemonės rizikos pašalinimui arba sumažinimui.

9. Atsakingas asmuo turi išanalizuoti ir aprašyti su asmens duomenimis susijusias sritis atsakydamas į šiuos klausimus:

9.1. Kokie duomenys bus tvarkomi?

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

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

9.4. Ar duomenų subjektui bus pateikiama visa reikiama informacija?

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

9.6. Ar duomenys yra tikslūs ir esant poreikiui atnaujinami?

9.7. Kiek laiko saugomi duomenys?

9.8. Kokiu būdu duomenų subjektai yra informuojami apie duomenų tvarkymą?

9.9. Jei duomenys tvarkomi su duomenų subjekto sutikimu, kokiu būdu jis gaunamas?

9.10. Kaip duomenų subjektai gali įgyvendinti savo teises?

9.11. Jei pasitelkiamas duomenų tvarkytojas ar tvarkytojai, ar jų pareigos tinkamai aprašytos sutartyje ir atitinka BDAR reikalavimus?

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

9.13. Kokios saugumo priemonės yra įgyvendinamos siekiant apsaugoti asmens duomenis?

IV. RIZIKOS IR JOS VALDYMO PRIEMONIŲ NUSTATYMAS

10. Atsakingas asmuo turėtų įvertinti galimą grėsmę duomenų subjektų teisėms ir laisvėms, kuomet yra nustatomos duomenų tvarkymo situacijos ir susijusių asmens duomenų pobūdis.

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

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

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

11.3. Vientisumo pažeidimas – netyčia ar neteisėtai atliekami nepageidaujami

asmens duomenų pakeitimai.

12. Įvardinus grėsmes, jos turi būti aprašytos atsakant į tolesnius klausimus:

12.1. Kokios tikėtinos pasekmės duomenų subjektams, jei įvyktų pažeidimas?

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

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

13. Toliau, turi būti aprašytos kokios esamos ar planuojamos techninės (fizinio ir kibernetinio saugumo) bei organizacinės priemonės, kurios padėtų sumažinti kylančias grėsmės duomenų subjektų teisėms ir laisvėms.

14. Įvertinus galimas grėsmes, nustatomas sprendimo būdas, kylančių grėsmių pašalinimui, o jei pašalinti neįmanoma, sumažinimui.

V. BAIGIAMOSIOS NUOSTATOS

15. Atlikus PDAV, turi būti parengta ataskaita, kurioje nurodoma PDAV eiga, rezultatai ir konkretūs veiksmai, kurių reikia imtis siekiant suvaldyti kylančias grėsmes, jei esamų rizikos valdymo priemonių tam nepakanka

16. Kylant abejonėms dėl rizikos valdymo priemonių efektyvumo, duomenų subjektų teisių ir laisvių užtikrinimo, turi būti konsultuojamasi su VDAI.

17. Visi, kurie dalyvauja duomenų tvarkymo procese, turi būti supažindinti su rizikos ataskaita ir jos išvadomis.

18. PDAV turi būti peržiūrimas, ir esant reikalui patikslinamas ir atnaujinamas.

_____