

POVEIKIO DUOMENŲ APSAUGAI VERTINIMO ROKIŠKIO LOPŠELYJE- DARŽELYJE „VARPELIS“ TVARKOS APRAŠAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Poveikio duomenų apsaugai vertinimo tvarkos aprašas (toliau – Aprašas) nustato duomenų tvarkymo operacijų poveikio duomenų apsaugai vertinimo Rokiškio lopšelyje-darželyje „Varpelis“ (toliau – Darželis) atlikimo pagrindus, eigą, procedūrą ir reikalavimus, 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 (Bendrojo duomenų apsaugos reglamento) (OL 2016 L 119, p. 1) (toliau – Reglamentas (ES) 2016/679) laikymąsi ir įgyvendinimą.

2. Aprašu vadovaujama šiais atvejais, kai dėl numatomo duomenų tvarkymo, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms ir laisvėms gali kilti didelis pavojus.

3. Šiame Apraše vartojamos sąvokos:

3.1. **Didelis pavojus fizinių asmenų teisėms ir laisvėms** – atvejais, kai dėl asmens duomenų tvarkymo arba dėl galimo asmens duomenų saugumo pažeidimo duomenų subjektams gali būti sunkiau naudotis savo teisėmis ir laisvėmis, duomenų subjektas gali patirti atskirtį arba diskriminaciją, finansinių nuostolių, gali būti pakenkta jo reputacijai arba atsirasti kitokių rimtų padarinių kasdieniam fizinio asmens gyvenimui.

3.2. **Duomenų apsaugos pareigūnas** – įstaigoje asmens duomenų apsaugos pareigūno funkcijas atliekantis asmuo, kuris vykdo jam pagal Reglamentą (ES) 2016/679 pavestas užduotis.

3.3. **Duomenų tvarkymo operacija** – vienas ar keli duomenų tvarkymo veiksmai.

3.4. **Fizinių asmenų teisės ir laisvės** – teisės į duomenų apsaugą ir privatumą, taip pat kitos pagrindinės teisės ir laisvės, pavyzdžiui, žodžio laisvė, minties laisvė, judėjimo laisvė, diskriminacijos draudimas, teisė į laisvę, sąžinės ir tikėjimo laisvę ir kt.

3.5. **Pavojus** – įvykis ir jo padariniai (žala), įvertinti atsižvelgiant į jų rimtumą ir tikimybę.

3.6. **Poveikio duomenų apsaugai vertinimas** (toliau – PDAV) – procesas, skirtas duomenų tvarkymo operacijai aprašyti ir tokios duomenų tvarkymo operacijos reikalingumui ir proporcingumui įvertinti, padedantis valdyti pavojų, kuris fizinių asmenų teisėms ir laisvėms kyla dėl asmens duomenų tvarkymo, apimantis pavojaus įvertinimą ir jo pašalinimo priemonių nustatymą. PDAV atlikimas schemiškai pavaizduotas šio Aprašo I priede.

3.7. **Darželio darbuotojas** – darbuotojas, dirbantis pagal darbo sutartį.

3.8. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679.

3.9. Poreikio atlikti PDAV nustatymą ir PDAV atlieka projekto, kurį įgyvendinus būtų atliekama duomenų tvarkymo operacija, kuriai taikomas reikalavimas atlikti PDAV, įstaigos vadovas arba kitas paskirtas darbuotojas (toliau – PDAV koordinatorius).

II SKYRIUS POVEIKIO DUOMENŲ APSAUGAI VERTINIMO PAGRINDAI

4. Poveikio duomenų apsaugai vertinimas (toliau-PDAV) atliekamas šiais atvejais:

4.1. kai duomenų tvarkymo operacija yra įtraukta į Valstybinės duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti PDAV, sąrašą;

4.2. kai planuojama rinkti arba kitaip tvarkyti naujus asmens duomenis (pavyzdžiui, sisteminga Darželio darbuotojų veiklos, darbuotojų darbo vietos, veiklos internete ir pan. stebėsena) ir dėl asmens duomenų tvarkymo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, vertinant asmens duomenų tvarkymą pagal šio Aprašo III skyriuje nurodytus kriterijus;

4.3. kai keičiasi jau tvarkomų asmens duomenų tvarkymo procesas (būdas, tikslas ir pan.) arba aplinka (pavyzdžiui, diegiama nauja informacinių technologijų sistema, teikiama nauja paslauga, atsiranda naujas procesas, naujos rizikos, susijusios su įvykdytomis kibernetinėmis atakomis ir pan.) ir dėl asmens duomenų tvarkymo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, vertinant asmens duomenų tvarkymą pagal šio Aprašo III skyriuje nurodytus kriterijus;

4.4. gavus priežiūros institucijos (Valstybinės duomenų apsaugos inspekcijos, administracinės veiklos priežiūrą atliekančio subjekto ir pan.), duomenų apsaugos pareigūno rekomendaciją atlikti PDAV.

5. PDAV gali būti neatliekamas šiais atvejais:

5.1. kai duomenų tvarkymas negali kelti didelio pavojaus fizinių asmenų teisėms ir laisvėms, vertinant asmens duomenų tvarkymą pagal šio Aprašo III skyriuje nurodytus kriterijus;

5.2. kai duomenų tvarkymo pobūdis, aprėptis, kontekstas ir tikslai yra labai panašūs į duomenų tvarkymą, kurio PDAV buvo atliktas (tokiais atvejais galima pasinaudoti dėl panašaus duomenų tvarkymo atliktu PDAV);

5.3. kai konkrečiomis sąlygomis, kurios nepasikeitė, vykdomas duomenų tvarkymo operacijas planiškai patikrino priežiūros institucija;

5.4. kai Darželio administracija asmens duomenis tvarko vadovaudamasi Reglamento (ES)2016/679 6 straipsnio 1 dalies c punktu arba e punktu ir PDAV buvo atliktas nustatant teisinį pagrindą.

6. PDAV turi būti atliktas prieš pradėdant tvarkyti asmens duomenis arba kai tvarkant asmens duomenis atsiranda objektyvi būtinybė atlikti PDAV, atsižvelgiant į šio Aprašo 4 punkte nurodytus atvejus.

7. PDAV gali būti atliekamas dėl kelių duomenų tvarkymo operacijų, kurios panašios savo pobūdžiu, apimtimi, kontekstu, tikslu ir kylančiais pavojais asmens duomenų saugumui.

III SKYRIUS

KRITERIJAI, KURIAIS REMIANTIS NUSTATOMA AR DĖL DUOMENŲ TVARKYMO OPERACIJOS GALI KILTI DIDELIS PAVOJUS FIZINIŲ ASMENŲ TEISĖMS IR LAISVĖMS

8. Siekiant nustatyti duomenų tvarkymo operacijas, dėl kurių reikia atlikti PDAV, atsižvelgiama į Reglamento (ES) 2016/679 35 straipsnio 1 dalyje bei 35 straipsnio 3 dalies a–c punktuose nustatytus konkrečius elementus, Valstybinės duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti PDAV, sąrašą, Reglamento (ES) 2016/679 71, 75, 91 konstatuojamąsias dalis bei kitas Reglamento (ES) 2016/679 nuorodas į duomenų tvarkymo operacijas, dėl kurių gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, bei įvertinami šie kriterijai:

8.1. atliekamas su fiziniais asmenimis susijusių asmeninių aspektų vertinimas arba balų skyrimas, įskaitant profiliavimą ir prognozavimą, visų pirma remiantis aspektais, susijusiais su duomenų subjekto darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu (pavyzdžiui, naudotojo elgesio profilio sudarymas, remiantis interneto svetainės naudojimu, ir pan.);

8.2. automatizuotai (technologinėmis priemonėmis, be jokio žmogaus įsikišimo) priimami sprendimai, duomenų subjektams sukeltiantys teisinį arba panašų rimtą poveikį (pavyzdžiui, duomenų tvarkymas gali lemti asmenų atskirtį arba diskriminaciją);

8.3. atliekama sisteminga stebėseną, t. y. duomenų tvarkymas, kuris reikalingas duomenų subjektų stebėsenos arba kontrolės tikslais, įskaitant tinkluose surinktus duomenis arba sistemingą viešos vietos stebėjimą dideliu mastu;

8.4. tvarkomi neskelbtini duomenys arba labai asmeniški duomenys (pavyzdžiui, specialių kategorijų asmens duomenys, duomenys apie apkaltinamuosius nuosprendžius ar nusikalstamas veikas, vietos nustatymo duomenys ir pan.);

8.5. 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);

8.6. 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.);

8.7. 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);

8.8. naudojamosi inovatyviais organizaciniais-techniniais sprendimais (pavyzdžiui, pirštų atspaudų ir veido atpažinimo derinimas siekiant užtikrinti geresnę fizinės prieigos kontrolę);

8.9. kai dėl paties duomenų tvarkymo duomenų subjektas negali įgyvendinti savo teisių, pasinaudoti paslaugomis arba sudaryti sutartis.

IV SKYRIUS

POREIKIO ATLIKTI POVEIKIO DUOMENŲ APSAUGAI VERTINIMĄ NUSTATYMAS

9. Poreikį atlikti PDAV paprastai nustato PDAV koordinatorius užpildydamas nustatytos formos poreikio atlikti PDAV nustatymo klausimyną.

10. Jei duomenų tvarkymo operacija nėra įtraukta į Valstybinės duomenų apsaugos inspekcijos sudarytą duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti PDAV, sąrašą, tokios duomenų tvarkymo operacijos PDAV paprastai atliekamas, kai planuojamas duomenų tvarkymas atitinka bent du iš šio Aprašo 8.1–8.9 papunkčiuose nurodytų kriterijų. Kuo daugiau kriterijų, nurodytų šio Aprašo 8.1–8.9 papunkčiuose, atitinka planuojamas duomenų tvarkymas, tuo labiau tikėtina, kad dėl duomenų tvarkymo operacijos gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms ir yra pagrindas atlikti PDAV. PDAV gali būti atliekamas ir tais atvejais, kai planuojamas duomenų tvarkymas atitinka tik vieną iš šio Aprašo 8.1–8.9 papunkčiuose nurodytų kriterijų.

11. Užpildytas poreikio atlikti PDAV nustatymo klausimynas pateikiamas įstaigos vadovui, kuris, įvertinęs klausimyne užfiksuotą informaciją, priima sprendimą dėl PDAV atlikimo.

12. Jei Darželio administracija, kaip duomenų valdytoja, nusprendžia neatlikti PDAV šio Aprašo 4 punkte nurodytais atvejais, manydamas, kad dėl duomenų tvarkymo negali kilti didelis pavojus fizinio asmens teisėms ir laisvėms, toks sprendimas turi būti pagrįstas, nurodant priežastis, dėl kurių nuspręsta neatlikti PDAV, taip pat įtraukiant ir (arba) užfiksuojant duomenų tvarkyme dalyvaujančių Darželio administracijos darbuotojų ir (arba) duomenų apsaugos pareigūno nuomonę.

V SKYRIUS

POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

13. Darželio vadovas, priėmęs sprendimą atlikti PDAV, organizuoja PDAV atlikimą, įvertindamas poreikio atlikti PDAV nustatymo klausimyne nurodytą siūlymą dėl Darželio administracijos darbuotojų, kurių dalyvavimas atliekant PDAV būtų reikšmingas pagal jų turimas kompetencijas ir atliekamas asmens duomenų tvarkymo funkcijas.

14. PDAV atlieka PDAV koordinatorius. PDAV atlikti gali būti pavesta Darželio administracijos darbuotojų grupei, kuri paprastai sudaroma iš PDAV koordinatoriaus, Darželio IT specialisto, bei kitų asmenų, kurie atliks duomenų tvarkymo operacijas ir (arba) yra su jomis susiję.

15. Darželio vadovo sprendimu PDAV atlikti gali būti pasitelkti išorės konsultantai, specialistai, ekspertai (teisininkai, informacinių technologijų specialistai, saugumo ekspertai, etikos specialistai ir pan.), jeigu Darželio administracijos žmogiškųjų ir (ar) laiko išteklių nepakanka PDAV tinkamai atlikti.

16. PDAV atlikimo rezultatai fiksuojami nustatytos formos PDAV atlikimo ataskaitoje.

17. 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 (pavojaus poveikio), kuri duomenų subjektams gali kilti dėl asmens duomenų tvarkymo arba galimo asmens duomenų saugumo pažeidimo, tikimybę ir sunkumą (žala gali būti fizinė, materialinė ir (arba) nematerialinė).

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

18.1. 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);

18.2. vidutinis (kai dėl asmens duomenų tvarkymo arba dėl galimo asmens duomenų saugumo pažeidimo duomenų subjektams gali būti sunkiau laikinai naudotis savo teisėmis ir laisvėmis, pasinaudoti Darželio administracijos teikiamomis paslaugomis, gali atsirasti kitokių neigiamų padarinių kasdieniam fizinio asmens gyvenimui);

18.3. 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).

19. Pavojaus įvertinimas ir bendro pavojaus lygio nustatymas atliekamas vadovaujantis pavojaus įvertinimo ir bendro pavojaus lygio nustatymo lentele.

20. Priemonės, kurių galima imtis siekiant sumažinti ar pašalinti pavojus (pavyzdžiui, saugumo priemonės, kuriomis užtikrinama asmens duomenų apsauga ir įrodoma, kad laikomasi Reglamento (ES) 2016/679 reikalavimų: duomenų šifravimas ir kitos techninės priemonės, reikšmingas asmenų, turinčių prieigą prie tam tikrų asmens duomenų, rato apribojimas, reikalavimų prieigos teisės turinčių vartotojų identifikavimui sugriežtinimas ir pan.), nustatomos atsižvelgiant į pavojaus mažinimo ir šalinimo priemonių rekomendacijas, kurios pateiktos šio.

21. Jei planuojamos pavojaus fizinių asmenų teisėms ir laisvėms mažinimo ir šalinimo priemonės yra imlios finansiniu ir laiko atžvilgiu, jų įgyvendinimui reikalingas tarpinstitucinis bendradarbiavimas ir (ar) keli vykdytojai ir pan., šios priemonės bei informacija apie jų įgyvendinimą gali būti fiksuojama atskirame pavojaus, kylančio fizinių asmenų teisėms ir laisvėms, mažinimo ir šalinimo priemonių plane.

22. Darželio vadovas užtikrina, kad būtų atliktas pavojaus, kylančio fizinių asmenų teisėms ir laisvėms, mažinimo ir šalinimo priemonių plane (jei toks planas buvo rengtas) nustatytų priemonių įgyvendinimo veiksmingumo vertinimas. Asmuo, įgyvendinęs plane numatytas priemones, negali vertinti jų veiksmingumo. Įgyvendinus numatytas priemones, iš naujo atliekamas pavojaus vertinimas (paprastai jį atlieka PDAV koordinatorius).

23. Darželio administracija, kaip duomenų valdytoja, gali nuspręsti, kad kai kurie pavojai (net ir dideli) yra priimtini, įvertinus planuojamo asmens duomenų tvarkymo naudą bei neproporcingas pavojų mažinimo ir šalinimo priemonių įgyvendinimo sąnaudas.

24. Jei atliekant PDAV paaiškėja, kad tvarkant asmens duomenis kiltų didelis pavojus duomenų subjektų teisėms ir laisvėms, jei Darželio administracija, kaip duomenų valdytoja, nesiimtų priemonių pavojui sumažinti, Darželio administracija, prieš pradėdama tvarkyti asmens duomenis, privalo iš anksto konsultuotis su Valstybine duomenų apsaugos inspekcija. Darželio

administracija, kreipdamasi dėl išankstinės konsultacijos, Valstybinei duomenų apsaugos inspekcijai pateikia Reglamento (ES) 2016/679 36 straipsnio 3 dalyje nurodytą informaciją.

25. Atliekant PDAV, Darželio darbuotojai, kuriems yra pavesta atlikti naujas duomenų tvarkymo operacijas ir (arba) yra su jomis susiję, privalo PDAV koordinatorius teikti visą informaciją, kurios pagrindu yra pildoma PDAV ataskaita bei pavojaus, kylančio fizinių asmenų teisėms ir laisvėms, mažinimo ir šalinimo priemonių planas (jei reikia), ir bendradarbiauti atliekant PDAV (paprastai, pateikti papildomą informaciją ir (ar) dokumentus, pagal kompetenciją teikti konsultacijas ir pan.).

26. PDAV koordinatoriui išreiškus poreikį, duomenų apsaugos pareigūnas PDAV atlikimo metu jam teikia konsultacijas ir metodinę informaciją dėl Reglamento (ES) 2016/679 nuostatų taikymo. PDAV koordinatoriaus prašymai dėl šiame Aprašo punkte nurodytų konsultacijų ir (ar) metodinės informacijos pateikimo bei duomenų apsaugos pareigūno atsakymai į juos teikiami elektroniniu paštu.

27. Atlikus PDAV, PDAV koordinatorius ne vėliau kaip per 5 darbo dienas po atlikto PDAV duomenų apsaugos pareigūnui elektroniniu paštu pateikia Darželio administracijos direktoriaus patvirtintos PDAV atlikimo ataskaitos, pavojaus, kylančio fizinių asmenų teisėms ir laisvėms, mažinimo ir šalinimo priemonių plano (jei planas buvo patvirtintas) bei Valstybinės duomenų apsaugos inspekcijos pateiktų rekomendacijų (jei atliekant PDAV buvo kreiptasi dėl išankstinių konsultacijų) nuorašus arba skaitmenines kopijas.

VI SKYRIUS DARBUOTOJŲ ATSAKOMYBĖ

28. Darželio vadovas užtikrina, kad prireikus būtų atlikta PDAV peržiūra ir įvertinta, ar asmens duomenys tvarkomi laikantis PDAV atlikimo ataskaitoje nurodytų išvadų ir sprendimų.

29. Už Aprašo nuostatų pažeidimą Darželio darbuotojams taikoma įstatymuose numatyta atsakomybė.

VII SKYRIUS BAIGIAMOSIOS NUOSTATOS

30. Jei atlikus PDAV iš esmės pasikeičia asmens duomenų tvarkymo pobūdis, aprėptis, kontekstas ir (ar) tikslai, turi būti atliekamas naujas PDAV.

31. Visi PDAV dokumentai (poreikio atlikti PDAV nustatymo klausimynas, PDAV atlikimo ataskaita, pavojaus, kylančio fizinių asmenų teisėms ir laisvėms, mažinimo ir šalinimo priemonių planas ir kt.) registruojami ir saugomi byloje pagal Darželio dokumentacijos planą.

32. PDAV atlikimo ataskaita arba jos santrauka gali būti skelbiama Darželio interneto svetainėje.
