29 STRAIPSNIO DUOMENŲ APSAUGOS DARBO GRUPĖ

17/LT

WP 248, 1-oji peržiūrėta versija

Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų

Priimta 2017 m. balandžio 4 d.

Paskutinį kartą peržiūrėta ir priimta 2017 m. spalio 4 d.

Ši darbo grupė įkurta pagal Direktyvos 95/46/EB 29 straipsnį. Tai nepriklausomas Europos patariamasis organas duomenų apsaugos ir privatumo klausimais. Jo užduotys aprašytos Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 2002/58/EB 15 straipsnyje.

Sekretoriato funkcijas atlieka Europos Komisijos Teisingumo generalinio direktorato C direktoratas (Pagrindinės teisės ir ES pilietybė), esantis adresu B-1049 Brussels, Belgium (kabineto Nr. MO-59 03/075).

Interneto svetainė http://ec.europa.eu/justice/data-protection/index_en.htm

DARBO GRUPĖ ASMENŲ APSAUGAI TVARKANT ASMENS DUOMENIS,

įkurta 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB,

atsižvelgdama į minėtos direktyvos 29 ir 30 straipsnius,

atsižvelgdama į savo Darbo tvarkos taisykles,

PRIĖMĖ ŠIAS GAIRES:

Turinys

I. ĮŽANGINIS ŽODIS 4

II. GAIRIŲ TAIKYMO SRITIS 5

III. PDAV. REGLAMENTO PAAIŠKINIMAS 7

A. KOKIE KLAUSIMAI SPRENDŽIAMI PDAV? VIENA DUOMENŲ TVARKYMO OPERACIJA AR PANAŠIŲ DUOMENŲ TVARKYMO OPERACIJŲ RINKINYS. 8

B. DĖL KURIŲ DUOMENŲ TVARKYMO OPERACIJŲ REIKIA ATLIKTI PDAV? TAIS ATVEJAIS, KAI JOS „GALI KELTI DIDELĮ PAVOJŲ“, IŠSKYRUS IŠIMTIS. 9

a) Kada PDAV privaloma atlikti? Kai dėl duomenų tvarkymo „gali kilti didelis pavojus“. 9

b) Kokiais atvejais nereikia atlikti PDAV? Tais atvejais, kai dėl duomenų tvarkymo negali „kilti didelis pavojus“ arba kai yra atliktas panašus PDAV, arba duomenis tvarkyti leista iki 2018 m. gegužės mėn., arba duomenys tvarkomi remiantis teisiniu pagrindu, arba duomenų tvarkymas įtrauktas į duomenų tvarkymo operacijų, kurių PDAV nereikalaujama atlikti, sąrašą. 14

C. KĄ GALIMA PASAKYTI APIE JAU VYKDOMAS DUOMENŲ TVARKYMO OPERACIJAS? TAM TIKRAIS ATVEJAIS REIKALAUJAMA ATLIKTI PDAV. 15

D. KAIP ATLIKTI PDAV? 16

a) Kada reikėtų atlikti PDAV? Prieš duomenų tvarkymą. 16

b) Kas turi pareigą atlikti PDAV? Duomenų valdytojas kartu su duomenų apsaugos pareigūnu ir duomenų tvarkytojais. 16

c) Kokia metodika taikoma atliekant PDAV? Skirtinga metodika, tačiau bendri kriterijai. 17

d) Ar privaloma skelbti PDAV? Ne, tačiau santraukos paskelbimas galėtų padidinti pasitikėjimą, o išsamus PDAV turi būti perduotas priežiūros institucijai, jei su ja anksčiau buvo konsultuojamasi arba jei to prašo duomenų apsaugos institucija. 20

E. KADA REIKĖTŲ KONSULTUOTIS SU PRIEŽIŪROS INSTITUCIJA? KAI YRA DIDELĖ LIKUTINĖ RIZIKA. 20

IV. IŠVADOS IR REKOMENDACIJOS 21

1 PRIEDAS. ESAMŲ ES PDAV SISTEMŲ PAVYZDŽIAI 23

2 PRIEDAS. PRIIMTINO PDAV KRITERIJAI 24

I. Įžanginis žodis

Reglamentas 2016/679[1] (toliau – BDAR) bus taikomas nuo 2018 m. gegužės 25 d. BDAR 35 straipsnyje nustatyta poveikio duomenų apsaugaivertinimo (toliau – PDAV[2]) sąvoka, kuri taip pat įtvirtinta Direktyvoje 2016/680[3].

PDAV – tai procesas, skirtas duomenų tvarkymui aprašyti ir tokio tvarkymo reikalingumui ir proporcingumui įvertinti, padedantis valdyti pavojų, kuris fizinių asmenų teisėms ir laisvėms kyla dėl asmens duomenų tvarkymo[4], jį įvertinant ir nustatant šio pavojaus pašalinimo priemones. PDAV yra svarbi atskaitomybės priemonė, nes padeda duomenų valdytojams ne tik laikytis BDAR, bet ir įrodyti, kad, siekiant užtikrinti atitiktį Reglamentui, buvo imtasi tinkamų priemonių (taip pat žr. 24 straipsnį)[5]. Kitaip tariant, **PDAV – tai atitikties užtikrinimo ir įrodymo procesas**.

BDAR nustatyta, kad nesilaikant PDAV reikalavimų kompetentinga priežiūros institucija gali skirti baudas. Jeigu PDAV neatliekamas tais atvejais, kai dėl duomenų tvarkymo jį reikia atlikti (35 straipsnio 1 dalis ir 3–4 dalys), jei PDAV atliekamas neteisingai (35 straipsnio 2 dalis ir 7–9 dalys) arba jei nesikonsultuojama su kompetentinga priežiūros institucija, kai to reikalaujama (36 straipsnio 3 dalies e punktas), gali būti skiriama administracinė bauda iki 10 mln. EUR arba, įmonės atveju, iki 2 proc. bendros pasaulinės metinės apyvartos, gautos ankstesniais finansiniais metais; visada skiriama didesnė bauda.

---

[1] 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).

[2] Terminas „poveikio privatumui vertinimas“ (PPV) kitomis aplinkybėmis dažnai vartojamas kalbant apie tą pačią sąvoką.

[3] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo 27 straipsnyje taip pat nurodyta, kad poveikio privatumui vertinimas yra reikalingas, kai „dėl duomenų tvarkymo <...> gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms“.

[4] BDAR nėra formalios PDAV sąvokos apibrėžties, bet:

- nurodomas būtinas PDAV turinys, kurį pagal 35 straipsnio 7 dalį sudaro:
    - „a) sistemingas numatytų duomenų tvarkymo operacijų aprašymas ir duomenų tvarkymo tikslai, įskaitant, kai taikoma, teisėtus interesus, kurių siekia duomenų valdytojas;
    - b) duomenų tvarkymo operacijų reikalingumo ir proporcingumo, palyginti su tikslais, vertinimas;
    - c) 1 dalyje nurodytas duomenų subjektų teisėms ir laisvėms kylančių pavojų vertinimas; ir
    - d) pavojams pašalinti numatytos priemonės, įskaitant apsaugos priemones, saugumo priemones ir mechanizmus, kuriais užtikrinama asmens duomenų apsauga ir įrodoma, kad laikomasi šio reglamento, atsižvelgiant į duomenų subjektų ir kitų susijusių asmenų teises ir teisėtus interesus“;
- PDAV reikšmė ir paskirtis 84 konstatuojamojoje dalyje paaiškinti taip: „siekiant užtikrinti, kad šio reglamento būtų geriau laikomasi, kai vykdant duomenų tvarkymo operacijas gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas turėtų būti atsakingas už poveikio duomenų apsaugai vertinimo atlikimą, kad būtų įvertinta visų pirma to pavojaus kilmė, pobūdis, specifika ir rimtumas.“

[5] Taip pat žr. 84 konstatuojamąją dalį: „Į šio vertinimo rezultatus turėtų būti atsižvelgta nustatant tinkamas priemones, kurių būtų imtasi siekiant įrodyti, kad asmens duomenų tvarkymas vykdomas laikantis šio reglamento.“

II. Gairių taikymo sritis

Šiose gairėse atsižvelgiama į:

- 29 straipsnio duomenų apsaugos darbo grupės (toliau – 29 straipsnio darbo grupė) pareiškimą Nr. 14/EN WP 218[6];
- 29 straipsnio darbo grupės gaires Nr. 16/EN WP 243 dėl duomenų apsaugos pareigūno[7];
- 29 straipsnio darbo grupės nuomonę Nr. 13/EN WP 203 dėl tikslo ribojimo principo[8];
- tarptautinius standartus[9].

Laikantis BDAR įtvirtinto rizika pagrįsto požiūrio, nebūtina atlikti kiekvienos duomenų tvarkymo operacijos PDAV. PDAV reikalaujama atlikti tik kai dėl duomenų tvarkymo „fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus“ (35 straipsnio 1 dalis). Siekiant užtikrinti nuoseklų aplinkybių, kuriomis PDAV yra privalomas (35 straipsnio 3 dalis), aiškinimą, šiose gairėse visų pirma siekiama paaiškinti šią sąvoką ir pateikti kriterijus, kuriais remiantis sudaromi 35 straipsnio 4 dalyje nurodyti sąrašai, kuriuos turi patvirtinti duomenų apsaugos institucijos

Pagal 70 straipsnio 1 dalies e punktą Europos duomenų apsaugos valdyba galės teikti gaires, rekomendacijas ir skelbti geriausią patirtį, siekdama skatinti nuoseklų BDAR taikymą. Šio dokumento tikslas – pasirengti tokiam būsimam Europos duomenų apsaugos valdybos darbui, taigi ir paaiškinti atitinkamas BDAR nuostatas siekiant padėti duomenų valdytojams laikytis teisės aktų ir užtikrinti duomenų valdytojų, kurie turi atlikti PDAV, teisinį tikrumą.

Šiomis gairėmis taip pat siekiama skatinti rengti:

- bendrą Europos Sąjungos duomenų tvarkymo operacijų, kurių PDAV atlikti būtina, sąrašą (35 straipsnio 4 dalis);
- bendrą ES duomenų tvarkymo operacijų, kurių PDAV atlikti būtina, sąrašą (35 straipsnio 5 dalis);
- bendrus PDAV atlikimo metodikos kriterijus (35 straipsnio 5 dalis);
- bendrus kriterijus, kuriuose būtų nurodyta, kada būtina konsultuotis su priežiūros institucija (36 straipsnio 1 dalis);
- rekomendacijas, kurios, kai įmanoma, būtų pagrįstos ES valstybių narių įgyta patirtimi.

---

[6] 2014 m. gegužės 30 d. priimtas 29 straipsnio darbo grupės pareiškimas Nr. 14/EN WP 218 dėl duomenų apsaugos teisinėse sistemose taikomo rizika pagrįsto požiūrio (angl. *On the role of a risk-based approach to data protection legal frameworks*)
(http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532).

[7] 2016 m. gruodžio 13 d. priimtos 29 straipsnio darbo grupės gairės Nr. 16/EN WP 243 dėl duomenų apsaugos pareigūno (angl. *On Data Protection Officer*)
(http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A).

[8] 2013 m. balandžio 2 d. priimta 2013 m. kovo mėn. 29 straipsnio darbo grupės nuomonė Nr. 13/EN WP 203 dėl tikslo ribojimo principo (angl. *Opinion on Purpose limitation*)
(http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409).

[9] Pavyzdžiui, ISO 31000:2009, *Rizikos valdymas – principai ir rekomendacijos*, Tarptautinė standartizacijos organizacija (ISO); ISO/IEC 29134 (projektas), *Informacinės technologijos – saugumo būdai – poveikio privatumui vertinimas – rekomendacijos*, Tarptautinė standartizacijos organizacija (ISO).

III. PDAV. Reglamento paaiškinimas

BDAR reikalaujama, kad duomenų valdytojai, be kita ko, atsižvelgdami į „įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms“ (24 straipsnio 1 dalis), įgyvendintų tinkamas priemones, kuriomis užtikrintų ir galėtų įrodyti atitiktį BDAR. Duomenų valdytojų pareiga tam tikromis aplinkybėmis atlikti PDAV turėtų būti vertinama atsižvelgiant į jų bendrą pareigą tinkamai valdyti pavojus[10], kurie kyla dėl asmens duomenų tvarkymo.

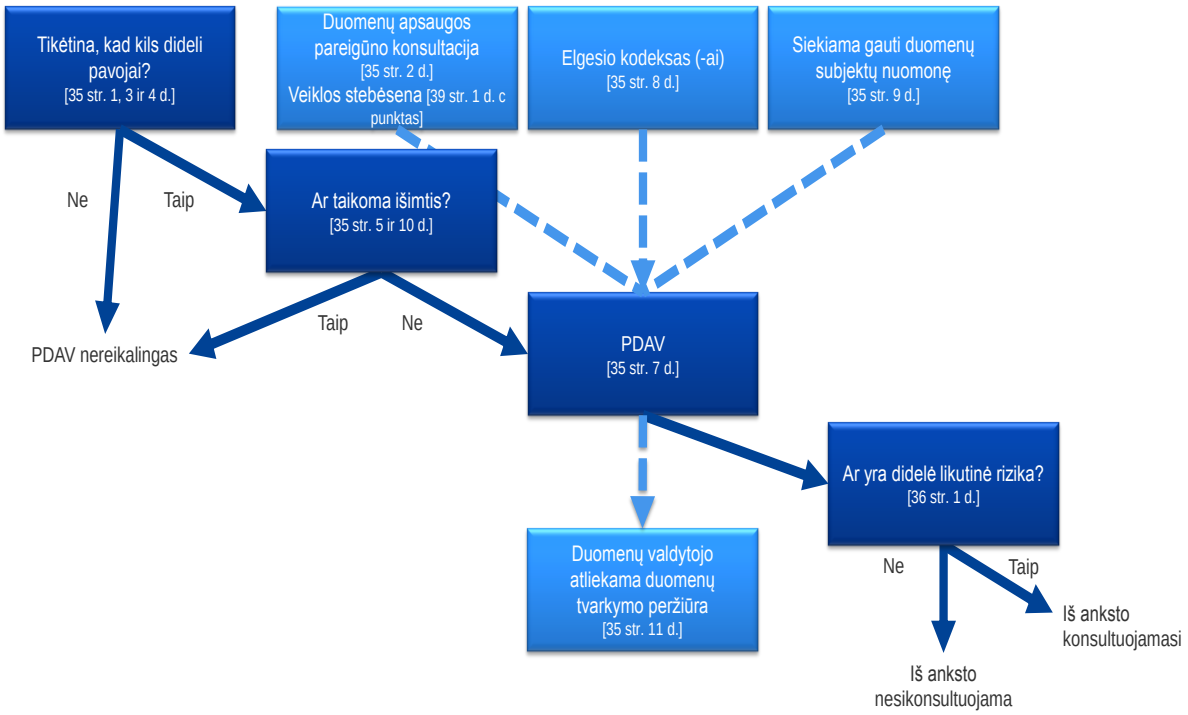
Pavojus – tai scenarijus, kuriame aprašomas įvykis ir jo padariniai, įvertinti atsižvelgiant į jų rimtumą ir tikimybę. Be to, pavojaus valdymas gali būti apibrėžiamas kaip koordinuoti veiksmai, kuriais organizacijos veiklą, susijusią su tuo pavojumi, siekiama nukreipti tam tikra linkme ir kontroliuoti.

35 straipsnyje pateikiama nuoroda į didelį pavojų, galintį kilti „fizinių asmenų teisėms bei laisvėms“. Kaip nurodyta 29 straipsnio duomenų apsaugos darbo grupės pareiškime dėl duomenų apsaugos teisinėse sistemose taikomo rizika pagrįsto požiūrio, nuoroda į duomenų subjektų „teises bei laisves“ visų pirma yra susijusi su teisėmis į duomenų apsaugą ir privatumą, tačiau taip pat gali apimti kitas pagrindines teises, pvz., žodžio laisvę, minties laisvę, judėjimo laisvę, diskriminacijos draudimą, teisę į laisvę, sąžinės ir tikėjimo laisvę.

Laikantis BDAR įtvirtinto rizika pagrįsto požiūrio, nebūtina atlikti kiekvienos duomenų tvarkymo operacijos PDAV. PDAV reikalaujama atlikti tik kai dėl duomenų tvarkymo rūšies „fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus“ (35 straipsnio 1 dalis). Tačiau vien faktas, kad sąlygos, dėl kurių atsiranda pareiga atlikti PDAV, nėra tenkinamos, nereiškia, kad sumažėja duomenų valdytojų bendra pareiga įgyvendinti priemones, kuriomis būtų tinkamai valdomi duomenų subjektų teisėms ir laisvėms kylantys pavojai. Praktiškai tai reiškia, kad duomenų valdytojai privalo nuolat vertinti dėl jų vykdomos duomenų tvarkymo veiklos kylančius pavojus, kad nustatytų atvejus, kai dėl duomenų tvarkymo rūšies „fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus“.

[10] Taip pat būtina pažymėti, kad, siekiant valdyti fizinių asmenų teisėms ir laisvėms kylančius pavojus, juos reikia reguliariai nustatyti, analizuoti, apskaičiuoti, įvertinti, spręsti (pvz., sumažinti ir pan.) ir peržiūrėti. Duomenų valdytojai negali išvengti atsakomybės įtraukdami pavojus į draudimo liudijimus.

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



A. <u>Kokie klausimai sprendžiami PDAV? Viena duomenų tvarkymo operacija ar panašių duomenų tvarkymo operacijų rinkinys.</u>

PDAV gali būti susijęs su viena duomenų tvarkymo operacija. Tačiau 35 straipsnio 1 dalyje nustatyta, kad „[p]anašius didelius pavojus keliančių duomenų tvarkymo operacijų sekai išnagrinėti galima atlikti vieną vertinimą.“ 92 konstatuojamojoje dalyje pridedama, kad „tam tikromis aplinkybėmis gali būti protinga ir ekonomiška atlikti platesnio masto poveikio duomenų apsaugai vertinimą, o ne susieti jį su vienu konkrečiu projektu, pavyzdžiui, kai valdžios institucijos ar įstaigos siekia sukurti bendrą taikomąją programą ar duomenų tvarkymo platformą arba kai keli duomenų valdytojai ketina tam tikroje pramonės šakoje, jos sektoriuje arba plačiai paplitusioje horizontalioje veikloje pradėti taikyti bendrą taikomąją programą ar duomenų tvarkymo aplinką“.

Vienas PDAV galėtų būti naudojamas vertinant įvairias duomenų tvarkymo operacijas, kurios yra panašios atsižvelgiant į jų pobūdį, aprėptį, kontekstą, tikslą ir pavojus. Tiesą sakant, PDAV siekiama sistemingai tirti naujas situacijas, kuriose galėtų kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, todėl PDAV nereikia atlikti tais atvejais, kurie jau buvo ištirti (t. y. konkrečiomis aplinkybėmis ir konkrečiu tikslu atliktos duomenų tvarkymo operacijos). Taip gali būti tuo atveju, kai tos pačios rūšies duomenims, kurie bus naudojami tuo pačiu tikslu, rinkti pasitelkiama panaši technologija. Pavyzdžiui, grupė savivaldybės institucijų, kurių kiekviena įrenginėja panašią apsauginę vaizdo stebėjimo sistemą (AVSS), galėtų atlikti vieną PDAV, kuriame aptartų, kaip šie atskiri duomenų valdytojai tvarko duomenis, arba geležinkelio operatorius (vienas duomenų valdytojas) galėtų, atlikdamas vieną PDAV, įvertinti vaizdo stebėjimo sistemų naudojimą visose savo geležinkelio stotyse. Ši taisyklė taip pat gali būti taikoma panašioms duomenų tvarkymo operacijoms, kurias vykdo įvairūs duomenų valdytojai. Tokiais atvejais reikėtų pasidalyti pavyzdiniu PDAV arba paskelbti jį viešai, būtina įgyvendinti PDAV aprašytas priemones ir pagrįsti, kodėl buvo atliktas vienas PDAV.

Kai duomenų tvarkymo operacijoje dalyvauja keletas duomenų valdytojų, jie turi tiksliai apibrėžti savo atitinkamas pareigas. Jų PDAV reikėtų nurodyti, kuri šalis yra atsakinga už įvairias priemones, kuriomis siekiama šalinti pavojus ir apsaugoti duomenų subjektų teises ir laisves. Kiekvienas duomenų valdytojas turėtų nurodyti savo poreikius ir pasidalyti naudinga informacija nesukeldamas pavojaus paslaptims (pvz., komercinių paslapčių, intelektinės nuosavybės, konfidencialios verslo informacijos apsaugai) ir neparodydamas pažeidžiamų vietų.

PDAV taip pat gali būti naudingas vertinant duomenų apsaugos poveikį technologiniam produktui, pvz., konkrečiai aparatinei ar programinei įrangai, kai tikėtina, kad jį įvairūs duomenų valdytojai naudos atlikdami skirtingas duomenų tvarkymo operacijas. Žinoma, produktą diegiantis duomenų valdytojas išlaiko pareigą atlikti atskirą PDAV, susijusį su konkrečiu įgyvendinimo būdu, tačiau šiuo atveju jis, jei tinkama, gali remtis produkto tiekėjo parengtu PDAV. Kaip pavyzdį būtų galima paminėti išmaniųjų skaitiklių gamintojų ir komunalines paslaugas teikiančių įmonių santykius. Kiekvienas produkto tiekėjas arba perdirbėjas turėtų pasidalyti naudinga informacija nesukeldamas pavojaus paslaptims ar pavojaus saugumui, parodęs pažeidžiamas vietas.

B. Dėl kurių duomenų tvarkymo operacijų reikia atlikti PDAV? Tais atvejais, kai jos „gali kelti didelį pavojų“, išskyrus išimtis.

Šioje skiltyje aprašomi atvejai, kai PDAV atlikti būtina, ir atvejai, kai to daryti nereikia.

Išskyrus atvejus, kai duomenų tvarkymo operacija atitinka išimties reikalavimus (III skyriaus B dalies a punktas), PDAV turi būti atliekamas tais atvejais, kai duomenų tvarkymo operacija „gali kelti didelį pavojų“ (III skyriaus B dalies b punktas).

a) Kada PDAV privaloma atlikti? Kai dėl duomenų tvarkymo „gali kilti didelis pavojus“.

Pagal BDAR nereikalaujama, kad PDAV būtų atliekamas dėl kiekvienos duomenų tvarkymo operacijos, dėl kurios gali kilti pavojus fizinių asmenų teisėms ir laisvėms. PDAV atlikti privaloma tik tuomet, kai dėl duomenų tvarkymo „fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus“ (35 straipsnio 1 dalis, pavyzdžiai pateikiami 35 straipsnio 3 dalyje, papildoma informacija pateikiama 35 straipsnio 4 dalyje). Tai ypač svarbu tais atvejais, kai pradedama naudoti nauja duomenų tvarkymo technologija[11].

Tais atvejais, kai neaišku, ar PDAV būtina atlikti, 29 straipsnio darbo grupė rekomenduoja šį vertinimą atlikti, nes PDAV yra naudinga priemonė, padedanti duomenų valdytojams laikytis duomenų apsaugos teisės aktų.

Nepaisant to, kad PDAV gali būti reikalaujama kitomis aplinkybėmis, 35 straipsnio 3 dalyje pateikta keletas pavyzdžių, kai dėl duomenų tvarkymo operacijos „gali kilti didelis pavojus“:

- „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[12];

[11] Žr. 89 ir 91 konstatuojamąsias dalis ir 35 straipsnio 1 ir 3 dalis, kuriose pateikiama daugiau pavyzdžių.

[12] Žr. 71 konstatuojamąją dalį: „visų pirma nagrinėjami arba prognozuojami su asmens darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu susiję aspektai“.

- 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[13]
- c) sistemingas viešos vietos stebėjimas dideliu mastu.“

Kaip matyti iš BDAR 35 straipsnio 3 dalies įžanginiame sakinyje vartojamų žodžių „visų pirma“, tai yra neišsamus sąrašas. Gali būti „didelį pavojų“ keliančių duomenų tvarkymo operacijų, kurių šis sąrašas neapima, tačiau kurios vis tiek kelia panašų didelį pavojų. Tokių duomenų tvarkymo operacijų PDAV taip pat turėtų būti atliktas. Todėl toliau išdėstytų kriterijų kartais negalima paprastai paaiškinti remiantis trijų BDAR 35 straipsnio 3 dalyje pateiktų pavyzdžių turiniu.

Siekiant nustatyti tikslesnį duomenų tvarkymo operacijų, dėl kurių, atsižvelgiant į joms būdingą didelį pavojų, reikia atlikti PDAV, rinkinį, atsižvelgiant į 35 straipsnio 1 dalyje bei 35 straipsnio 3 dalies a–c punktuose nustatytus konkrečius elementus ir sąrašą, kuris nacionaliniu lygmeniu turi būti tvirtinamas pagal 35 straipsnio 4 dalį ir 71, 75 ir 91 konstatuojamąsias dalis, bei kitas BDAR nuorodas į duomenų tvarkymo operacijas, dėl kurių „gali kilti didelis pavojus“[14], turėtų būti įvertinti toliau nurodyti devyni kriterijai.

1. Vertinimas arba balų skyrimas, įskaitant profiliavimą ir prognozavimą, visų pirma remiantis „aspekt[ais], susijusi[ais] su duomenų subjekto darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu“ (71 ir 91 konstatuojamosios dalys). Šiuo atveju kaip pavyzdį būtų galima nurodyti finansų įstaigą, kuri tikrina savo klientų duomenis kredito informacinėje duomenų bazėje, kovos su pinigų plovimu ir terorizmo finansavimu (AML / CTF) arba sukčiavimo duomenų bazėje, arba biotechnologijų bendrovę, kuri tiesiogiai vartotojams siūlo atlikti genetinius tyrimus, siekiant įvertinti ir prognozuoti su liga susijusį ir (arba) sveikatai gresiantį pavojų, arba bendrovę, kuri, remdamasi jos svetainės naudojimu arba naršymu joje, kuria elgesio arba rinkodaros profilius.
2. Automatizuotas sprendimų, sukeliančių teisinį arba panašų rimtą poveikį, priėmimas: duomenų tvarkymas, kuriuo siekiama priimti sprendimus dėl duomenų subjektų, darančius „su fiziniu asmeniu susij[usį] teisin[į] poveik[į]“ arba „panašų didelį poveikį fiziniam asmeniui“ (35 straipsnio 3 dalies a punktas). Pavyzdžiui, duomenų tvarkymas gali lemti asmenų atskirtį arba diskriminaciją. Duomenų tvarkymas, kai fiziniams asmenims daromas mažas poveikis arba apskritai nedaroma jokio poveikio, neatitinka šio konkretaus kriterijaus. Išsamesni šių sąvokų paaiškinimai bus pateikti būsimose 29 straipsnio darbo grupės profiliavimo gairėse.
3. Sisteminga stebėsena: duomenų tvarkymas, kuris naudojamas duomenų subjektų stebėsenos arba kontrolės tikslais, įskaitant tinkluose surinktus duomenis arba „sisteming[ą] viešos vietos stebėjim[ą] dideliu mastu“ (35 straipsnio 3 dalies c punktas)[15]. Šios rūšies stebėsena laikytina

[13] Žr. 75 konstatuojamąją dalį: „kai tvarkomi asmens duomenys, kurie atskleidžia rasinę arba etninę kilmę, politines pažiūras, religiją ar filosofinius įsitikinimus, priklausymą profesinėms sąjungoms, taip pat tvarkant genetinius duomenis, sveikatos duomenis ar duomenis apie lytinį gyvenimą, arba apkaltinamuosius nuosprendžius ir nusikalstamas veikas, arba susijusias saugumo priemones“.

[14] Žr., pvz., 75, 76, 92, 116 konstatuojamąsias dalis.

[15] 29 straipsnio darbo grupė sąvoką *sistemingas* aiškina kaip reiškiančią vieną ar daugiau toliau nurodytų aplinkybių (žr. 29 straipsnio darbo grupės gaires Nr. 16/EN WP 243 dėl duomenų apsaugos pareigūno):

- vykdoma pagal sistemą;
- vykdoma pagal iš anksto nustatytą, organizuotą arba metodinę tvarką;

kriterijumi, nes asmens duomenys gali būti renkami aplinkybėmis, kuriomis duomenų subjektai gali nežinoti, kas renka jų duomenis ir kaip jie bus panaudoti. Be to, fiziniai asmenys gali neišvengti tokio duomenų tvarkymo viešojoje (-siose) arba viešai prieinamoje (-ose) erdvėje (-ėse).

4. Neskelbtini duomenys arba labai asmeniški duomenys: jie apima specialių kategorijų asmens duomenis, kaip apibrėžta 9 straipsnyje (pvz., informaciją apie fizinių asmenų politines pažiūras), taip pat asmens duomenis, susijusius su apkaltinamaisiais nuosprendžiais ar nusikalstamomis veikomis, kaip apibrėžta 10 straipsnyje. Kaip pavyzdį būtų galima paminėti ligoninėje saugomus bendruosius paciento medicinos dokumentus arba privataus tyrėjo saugomus nusikaltėlių duomenis. Be šių BDAR nuostatų, yra tam tikrų kategorijų duomenų, kuriems gali kilti didesnis pavojus, susijęs su fizinių asmenų teisėmis ir laisvėmis. Šie asmens duomenys laikomi neskelbtinais duomenimis (atsižvelgiant į bendrą šio termino prasmę), nes jie susiję su namų ūkiu ir privačia veikla (pvz., elektroniniai ryšiai, kurių konfidencialumas turi būti apsaugotas) arba daro poveikį pagrindinės teisės įgyvendinimui (pvz., vietos duomenys, kurių rinkimas gali reikšti judėjimo laisvės apribojimą), arba jų pažeidimas yra aiškiai susijęs su rimtais padariniais kasdieniam duomenų subjekto gyvenimui (pvz., finansiniai duomenys, kurie gali būti panaudoti atliekant su sukčiavimu susijusį mokėjimą). Šiuo klausimu gali būti svarbu tai, ar duomenis jau viešai paskelbė duomenų subjektas arba trečiosios šalys. Faktas, kad asmens duomenys yra viešai prieinami, gali būti laikomas veiksniu vertinant, ar buvo tikėtina, kad duomenys gali būti toliau naudojami tam tikriems tikslams. Šis kriterijus taip pat gali apimti tokius duomenis kaip asmeniniai dokumentai, e. laiškai, dienoraščiai, e. dokumentuose, kuriuose naudojamos pastabų pateikimo funkcijos, skaitytojų užrašytos pastabos ir ypač asmeninio pobūdžio informacija, pateikta asmeninio turinio taikomosiose programose.
5. Didelio masto duomenų tvarkymas. BDAR neapibrėžiama, ką reiškia tvarkyti duomenis dideliu mastu, tačiau 91 konstatuojamojoje dalyje galima rasti tam tikrų nurodymų. Bet kuriuo atveju 29 straipsnio darbo grupė rekomenduoja nustatant, ar duomenys tvarkomi dideliu mastu, atsižvelgti visų pirma į toliau nurodytus veiksnius[16]:
    a. susijusių duomenų subjektų skaičių; tai gali būti konkretus skaičius arba atitinkamų gyventojų dalis;
    b. tvarkomų duomenų kiekį ir (arba) skirtingų tvarkomų duomenų įvairovę;
    c. duomenų tvarkymo veiklos trukmę arba pastovumą;
    d. geografinį duomenų tvarkymo mastą.
6. Duomenų rinkinių siejimas ir derinimas , kurį, pvz., lemia dvi ar daugiau duomenų tvarkymo operacijos, kurios skirtingais tikslais ir (arba) skirtingų duomenų valdytojų atliktos taip, kad viršija pagrįstus duomenų subjekto lūkesčius[17].
7. Su pažeidžiamais duomenų subjektais susiję duomenys (75 konstatuojamoji dalis). Šios rūšies duomenų tvarkymas – tai kriterijus, nes nėra didesnės duomenų subjektų ir duomenų valdytojo galios pusiausvyros, o tai reiškia, kad fiziniai asmenys gali neturėti galimybės lengvai sutikti su savo duomenų tvarkymu, jam prieštarauti arba įgyvendinti savo teises.

- vykdoma kaip sudedamoji bendro duomenų rinkimo plano dalis;
- vykdoma kaip strategijos dalis.

29 straipsnio darbo grupė sąvoką *vieša vieta* aiškina kaip reiškiančią bet kurią visuomenės nariui atvirą vietą, pvz., aikštę, prekybos centrą, gatvę, turgavietę, traukinių stotį arba viešąją biblioteką.

[16] Žr. 29 straipsnio darbo grupės gaires Nr. 16/EN WP 243 dėl duomenų apsaugos pareigūno.

[17] Žr. paaiškinimą 29 straipsnio darbo grupės nuomonėje Nr. 13/EN WP 203 dėl tikslo ribojimo principo, p. 24.

Pažeidžiamiems duomenų subjektams gali priklausyti vaikai (juos galima laikyti negalinčiais sąmoningai ir apgalvotai prieštarauti savo duomenų tvarkymui arba sutikti su duomenų tvarkymu), darbuotojai, pažeidžiamesni gyventojų, kuriems reikalinga speciali apsauga, segmentai (psichiškai nesveiki asmenys, prieglobsčio prašytojai arba vyresnio amžiaus asmenys, pacientai ir pan.), ir visais atvejais, kai galima nustatyti nelygiaverčius duomenų subjekto ir duomenų valdytojo santykius.

8. Naujoviškas naudojimas arba naujų technologinių ar organizacinių sprendimo būdų taikymas, pvz., pirštų atspaudų naudojimo ir veido atpažinimo derinimas siekiant užtikrinti geresnę fizinės prieigos kontrolę ir pan. BDAR aiškiai nurodyta (35 straipsnio 1 dalyje ir 89 bei 91 konstatuojamosiose dalyse), kad naujos technologijos, *apibrėžtos „atsižvelgiant į pasiektą technologinių žinių lygį*“ (91 konstatuojamoji dalis), naudojimas gali reikšti, jog būtina atlikti PDAV. Taip yra dėl to, kad naudojant tokias technologijas gali būti taikomos naujos duomenų rinkimo ir naudojimo formos, dėl kurių gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms. Tiesą sakant, su naujos technologijos diegimu susiję asmeniniai ir socialiniai padariniai gali būti nežinomi. PDAV duomenų valdytojui padės suprasti ir valdyti tokius pavojus. Pavyzdžiui, tam tikros daiktų interneto taikomosios programos galėtų daryti didelį poveikį kasdieniam fizinių asmenų gyvenimui ir privatumui, todėl reikia atlikti jų PDAV.
9. Atvejis, kai dėl paties duomenų tvarkymo „duomenų subjektams užkertamas kelias naudotis savo teisėmis, paslaugomis arba sudaryti sutartis“ (22 straipsnis ir 91 konstatuojamoji dalis). Jis apima duomenų tvarkymo operacijas, kuriomis siekiama duomenų subjektams leisti pasinaudoti paslauga arba sudaryti sutartį, pakeisti tokį leidimą arba atsisakyti jį suteikti. Taip, pvz., gali būti tuo atveju, kai bankas tikrina savo klientus kredito informacinėje duomenų bazėje, kad nuspręstų, ar suteikti jam paskolą.

Dažniausiai duomenų valdytojas gali manyti, kad, PDAV turėtų būti atliktas, kai duomenų tvarkymas atitinka du kriterijus. Apskritai 29 straipsnio darbo grupė mano, kad kuo daugiau kriterijų atitinka duomenų tvarkymo operacija, tuo labiau tikėtina, kad dėl jos kils didelis pavojus duomenų subjektų teisėms ir laisvėms, todėl, nepaisant priemonių, kurias numato taikyti duomenų valdytojas, būtina atlikti PDAV.

Tačiau tam tikrais atvejais **duomenų valdytojas gali manyti, kad PDAV būtina atlikti net jeigu tenkinamas tik vienas iš šių kriterijų.**

Toliau pateiktuose pavyzdžiuose atsispindi, kaip kriterijus reikėtų taikyti siekiant įvertinti, ar dėl konkrečios duomenų tvarkymo operacijos reikia atlikti PDAV.

Duomenų tvarkymo pavyzdžiai	**Galimi susiję kriterijai**	**Ar gali prireikti atlikti PDAV?**
Savo pacientų genetinius ir sveikatos duomenis tvarkanti ligoninė (ligoninės informacinė sistema).	- Neskelbtini duomenys arba labai asmeniški duomenys. - Su pažeidžiamais duomenų subjektais susiję duomenys. - Vykdomas didelio masto duomenų tvarkymas.	Taip
Vaizdo kamerų sistemos naudojimas siekiant stebėti	- Sisteminga stebėsena.	

Duomenų tvarkymo pavyzdžiai	Galimi susiję kriterijai	Ar gali prireikti atlikti PDAV?
elgesį greitkeliuose. Duomenų valdytojas planuoja naudoti išmanią vaizdo analizės sistemą, kad atrinktų automobilius ir automatiškai atpažintų registracijos numerius.	- Naujoviškas technologinių arba organizacinių sprendimo būdų naudojimas arba taikymas.	
Įmonė sistemingai stebi savo darbuotojų veiklą, įskaitant darbuotojų darbo vietos stebėseną, veiklą internete ir pan.	- Sisteminga stebėsena. - Su pažeidžiamais duomenų subjektais susiję duomenys.	
Viešų socialinės žiniasklaidos priemonėse pateikiamų duomenų rinkimas siekiant sukurti profilius.	- Vertinimas arba balų skyrimas. - Vykdomas didelio masto duomenų tvarkymas. - Duomenų rinkinių siejimas ir derinimas. - Neskelbtini duomenys arba labai asmeniški duomenys.	
Institucija nacionaliniu lygmeniu sukuria kredito reitingavimo arba sukčiavimo duomenų bazę.	- Vertinimas arba balų skyrimas. - Automatizuotas sprendimų, turinčių teisinį arba panašų rimtą poveikį, priėmimas. - Duomenų subjektui užkertamas kelias pasinaudoti teise arba paslauga arba sudaryti sutartį. - Neskelbtini duomenys arba labai asmeniški duomenys.	
Pseudoniminių neskelbtinų asmens duomenų, susijusių su tyrimų projektuose arba klinikiniuose tyrimuose dalyvaujančiais pažeidžiamais duomenų subjektais, saugojimas.	- Neskelbtini duomenys. - Su pažeidžiamais duomenų subjektais susiję duomenys. - Duomenų subjektams užkertamas kelias pasinaudoti teise arba paslauga arba sudaryti sutartį.	
„Atskirų gydytojų, kitų sveikatos priežiūros specialistų pacientų arba teisininko klientų asmens duomenų“ tvarkymas (91 konstatuojamoji dalis).	- Neskelbtini duomenys arba labai asmeniški duomenys. - Su pažeidžiamais duomenų subjektais susiję duomenys.	Ne
Internetinis laikraštis, kuriame naudojamas e. adresų sąrašas siekiant kasdien prenumeratoriams siųsti bendro pobūdžio santraukas.	- Vykdomas didelio masto duomenų tvarkymas.	
E. prekybos svetainė, kurioje rodomos senovinių automobilių detalių reklamos, susijusios su ribotu profiliavimu, pagrįstu toje svetainėje peržiūrėtomis arba įsigytomis detalėmis.	- Vertinimas arba balų skyrimas.	

Priešingai – duomenų tvarkymo operacija gali būti susijusi su minėtais atvejais, ir duomenų valdytojas vis tiek gali manyti, kad dėl jos negali „kilti didelis pavojus“. Tokiais atvejais duomenų valdytojas turėtų pagrįsti ir dokumentuoti priežastis, dėl kurių jis neatlieka PDAV, taip pat įtraukti ir (arba) užfiksuoti duomenų apsaugos pareigūno nuomonę.

Be to, kalbant apie atskaitomybės principą, pažymėtina, kad kiekvienas duomenų valdytojas „tvarko duomenų tvarkymo veiklos, už kurią jis atsako, įrašus“, įskaitant *inter alia* duomenų tvarkymo tikslus, duomenų kategorijų aprašymą ir duomenų gavėjus ir „kai įmanoma, bendr[ą] 32 straipsnio 1 dalyje nurodytų techninių ir organizacinių saugumo priemonių aprašym[ą]“ (30 straipsnio 1 dalis), ir privalo įvertinti, ar kyla didelis pavojus, net jeigu jis galiausiai nusprendžia neatlikti PDAV.

Pastaba. Reikalaujama, kad priežiūros institucijos nustatytų, viešai paskelbtų ir Europos duomenų apsaugos valdybai perduotų duomenų tvarkymo operacijų, kurių PDAV reikia atlikti, sąrašą (35 straipsnio 4 dalis)[18]. Pirmiau išdėstyti kriterijai gali padėti priežiūros institucijoms sudaryti tokį sąrašą, į kurį, jei tinkama, būtų įtraukta konkretesnė informacija. Pavyzdžiui, bet kurios rūšies biometrinių duomenų tvarkymas arba vaikų duomenų tvarkymas taip pat gali būti laikomi svarbiais pagal 35 straipsnio 4 dalį rengiant sąrašą.

b) Kokiais atvejais nereikia atlikti PDAV? Tais atvejais, kai dėl duomenų tvarkymo negali „kilti didelis pavojus“ arba kai yra atliktas panašus PDAV, arba duomenis tvarkyti leista iki 2018 m. gegužės mėn., arba duomenys tvarkomi remiantis teisiniu pagrindu, arba duomenų tvarkymas įtrauktas į duomenų tvarkymo operacijų, kurių PDAV nereikalaujama atlikti, sąrašą.

29 straipsnio darbo grupė mano, kad PDAV nereikia atlikti šiais atvejais:

- **kai duomenų tvarkymas negali kelti didelio pavojaus „fizinių asmenų teisėms bei laisvėms“** (35 straipsnio 1 dalis);
- **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 (35 straipsnio 1 dalis[19]);
- kai konkrečiomis sąlygomis, kurios nepasikeitė, vykdomas duomenų tvarkymo operacijas iki 2018 m. gegužės mėn. patikrino priežiūros institucija[20] (žr. III skyriaus C dalį);
- **kai duomenų tvarkymo operacijos** pagal 6 straipsnio 1 dalies c arba e punktą **teisinis pagrindas nustatytas** ES arba valstybės narės teisės akte, kai pagal teisės aktą reglamentuojama konkreti duomenų tvarkymo operacija **ir kai PDAV jau atliktas** nustačius tą teisinį pagrindą (35 straipsnio 10 dalis)[21], išskyrus atvejus, kai valstybė narė nurodė, kad PDAV būtina atlikti prieš tvarkymo veiklą;
- **kai duomenų tvarkymas įtrauktas į neprivalomą duomenų tvarkymo operacijų sąrašą (kurį nustatė priežiūros institucija)** ir dėl šių operacijų nereikia atlikti PDAV (35 straipsnio

[18] Šiomis aplinkybėmis „kompetentinga priežiūros institucija taiko 63 straipsnyje nurodytą nuoseklumo užtikrinimo mechanizmą, kai tokiuose sąrašuose nurodoma duomenų tvarkymo veikla, kuri yra susijusi su prekių ar paslaugų siūlymu duomenų subjektams arba su duomenų subjektų elgesio stebėjimu keliose valstybėse narėse, arba kurią vykdant gali būti padarytas didelis poveikis laisvam asmens duomenų judėjimui Sąjungoje“ (35 straipsnio 6 dalis).

[19] „Panašius didelius pavojus keliančių duomenų tvarkymo operacijų sekai išnagrinėti galima atlikti vieną vertinimą.“

[20] „Remiantis Direktyva 95/46/EB priimti Komisijos sprendimai ir priežiūros institucijų suteikti leidimai toliau galioja tol, kol iš dalies pakeičiami, pakeičiami naujais arba panaikinami“ (171 konstatuojamoji dalis).

[21] Kai PDAV atliekamas rengiant teisės aktą, kuriame nustatytas duomenų tvarkymo teisinis pagrindas, tikėtina, kad prieš pradedant duomenų tvarkymo operacijas jį bus būtina peržiūrėti, nes priimtas teisės aktas gali skirtis nuo pasiūlymo savo poveikiu privatumo ir duomenų apsaugai. Be to, gali trūkti išsamių techninių duomenų, susijusių su faktiniu duomenų tvarkymu priimant teisės aktą, net jeigu prie jo buvo pridėtas PDAV. Tokiais atvejais prieš pradedant faktiškai tvarkyti duomenis vis tiek gali reikėti atlikti konkretų PDAV.

5 dalis). Tokiame sąraše gali būti numatyta duomenų tvarkymo veikla, atitinkanti sąlygas, kurias ši institucija nustatė visų pirma gairėse, konkrečiuose sprendimuose ar leidimuose, atitikties taisyklėse ir pan. (pvz., Prancūzijoje tokios sąlygos nustatomos leidimuose, nuostatose dėl išimties, supaprastintose taisyklėse, atitikties rinkiniuose ir pan.). Tokiais atvejais ir atsižvelgiant į pakartotinį kompetentingos priežiūros institucijos vertinimą, PDAV atlikti nereikalaujama, tačiau tik tuo atveju, jeigu duomenų tvarkymas griežtai patenka į sąraše paminėtos susijusios procedūros taikymo sritį ir toliau visiškai atitinka visus susijusius BDAR reikalavimus.

C. Ką galima pasakyti apie jau vykdomas duomenų tvarkymo operacijas? Tam tikrais atvejais reikalaujama atlikti PDAV.

Reikalavimas atlikti PDAV taikomas esamoms duomenų tvarkymo operacijoms, dėl kurių gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms ir kurių keliamas pavojus pasikeitė, atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus.

PDAV nereikia atlikti dėl duomenų tvarkymo operacijų, kurias patikrino priežiūros institucija arba duomenų apsaugos pareigūnas pagal Direktyvos 95/46/EB 20 straipsnį ir kurios atliekamos taip pat, kaip ir prieš atliekant patikrinimą. Iš tikrųjų „[r]emiantis Direktyva 95/46/EB priimti Komisijos sprendimai ir priežiūros institucijų suteikti leidimai toliau galioja tol, kol iš dalies pakeičiami, pakeičiami naujais arba panaikinami“ (171 konstatuojamoji dalis).

Priešingai, tai reiškia, kad kiekvienos duomenų tvarkymo operacijos, kurios įgyvendinimo sąlygos (aprėptis, tikslas, renkami asmens duomenys, duomenų valdytojų arba gavėjų tapatybė, duomenų saugojimo laikotarpis, techninės ir organizacinės priemonės ir pan.) nuo išankstinio patikrinimo, kurį atliko priežiūros institucija arba duomenų apsaugos pareigūnas, pasikeitė ir tikėtina, kad toks pasikeitimas gali kelti didelį pavojų, PDAV turėtų būti atliekamas.

Be to, PDAV gali būti reikalaujama atlikti pasikeitus duomenų tvarkymo operacijų keliamiems pavojams[22], pvz., dėl to, kad buvo pradėta naudoti nauja technologija arba dėl to, kad asmens duomenys naudojami kitu tikslu. Duomenų tvarkymo operacijos gali greitai vystytis, o vykstant šiam procesui gali atsirasti naujų pažeidžiamų vietų. Todėl reikėtų atkreipti dėmesį į tai, kad PDAV peržiūra naudinga ne tik nuolatinio tobulinimo tikslais, bet ir yra labai svarbi siekiant išlaikyti tam tikrą duomenų apsaugos lygį ilgainiui besikeičiančiomis aplinkybėmis. PDAV taip pat gali prireikti atlikti dėl pasikeitusių organizacinių arba visuomeninių aplinkybių, susijusių su duomenų tvarkymo veikla, nes, pvz., tam tikri automatizuoti sprendimai sukelia rimtesnius padarinius arba naujų kategorijų duomenų subjektai gali patirti diskriminaciją. Kiekvienas iš šių pavyzdžių galėtų būti aplinkybė, lemianti pavojaus, kuris kyla dėl atitinkamos duomenų tvarkymo veiklos, pasikeitimą.

Priešingai, dėl tam tikrų pakeitimų pavojus taip pat galėtų sumažėti. Pavyzdžiui, duomenų tvarkymo operacija gali būti pakeista taip, kad sprendimai nebebūtų priimami automatizuotai, arba tuo atveju, jeigu nebevykdoma sistemingos stebėsenos veikla. Tuomet peržiūrėjus atliktą rizikos analizę gali paaiškėti, kad PDAV nebereikia atlikti.

[22] Pavojus kylantis pasikeitusioms aplinkybėms, surinktiems duomenims, tikslams, funkcijoms, tvarkomiems asmens duomenims, gavėjams, duomenų kombinacijoms, pavojams (pagalbinių priemonių, rizikos šaltinių, galimo poveikio, grėsmių ir pan.), saugumo priemonėms ir tarptautiniam duomenų perdavimui.

Geros praktikos tikslais**PDAV turėtų būti nuolat peržiūrimas ir reguliariai vertinamas.** Todėl net jeigu PDAV nereikalaujama atlikti 2018 m. gegužės 25 d., atitinkamu laiku duomenų valdytojas privalės atlikti tokį PDAV atsižvelgdamas į savo bendrus atskaitomybės įsipareigojimus.

D. Kaip atlikti PDAV?

a) Kada reikėtų atlikti PDAV? Prieš duomenų tvarkymą.

PDAV turėtų būti atliktas „prieš pradedant duomenų tvarkymą“ (35 straipsnio 1 dalis ir 35 straipsnio 10 dalis, 90 ir 93 konstatuojamosios dalys)[23]. Tai atitinka pritaikytosios ir standartizuotosios duomenų apsaugos principus (25 straipsnis ir 78 konstatuojamoji dalis). Į PDAV reikėtų žiūrėti kaip į priemonę, padedančią priimti sprendimus dėl duomenų tvarkymo.

PDAV turėtų būti pradėtas kuo anksčiau ir kai tai praktiškai įmanoma pritaikant duomenų tvarkymo operaciją, net jeigu tam tikros duomenų tvarkymo operacijos dar nėra žinomos. PDAV atnaujinimas projekto gyvavimo metu padės užtikrinti, kad būtų paisoma duomenų apsaugos ir privatumo ir paskatins kurti sprendimo būdus, padedančius laikytis reikalavimų. Progresuojant kūrimo procesui, taip pat gali prireikti pakartoti atskirus vertinimo etapus, nes tam tikrų techninių ar organizacinių priemonių pasirinkimas gali daryti poveikį duomenų tvarkymo keliamų pavojų rimtumui ar tikimybei.

Faktas, kad PDAV gali tekti atnaujinti faktiškai pradėjus tvarkyti duomenis, nėra pagrįsta priežastis atidėti PDAV arba jo neatlikti. PDAV yra tęstinis procesas, visų pirma tais atvejais, kai duomenų tvarkymo operacija yra dinamiška ir nuolat kinta. **PDAV atlikimas yra tęstinis procesas, o ne vienkartinis veiksmas.**

b) Kas turi pareigą atlikti PDAV? Duomenų valdytojas kartu su duomenų apsaugos pareigūnu ir duomenų tvarkytojais.

Duomenų valdytojas turi pareigą užtikrinti, kad būtų atliktas PDAV (35 straipsnio 2 dalis). PDAV gali atlikti kas nors kitas, dirbantis organizacijos viduje ar už jos ribų, tačiau už šios pareigos vykdymą galiausiai atsako duomenų valdytojas.

Duomenų valdytojas taip pat turi stengtis konsultuotis su duomenų apsaugos pareigūnu, kai jis yra paskirtas (35 straipsnio 2 dalis), o ši konsultacija ir duomenų valdytojo priimti sprendimai turėtų būti įtraukti į PDAV dokumentaciją. Duomenų apsaugos pareigūnas taip pat turėtų stebėti, kaip atliekamas PDAV (39 straipsnio 1 dalies c punktas). Daugiau rekomendacijų pateikta 29 straipsnio darbo grupės gairėse dėl duomenų apsaugos pareigūno 16/EN WP 243.

Jeigu duomenų tvarkymą visiškai arba iš dalies atlieka duomenų tvarkytojas, **jis turėtų padėti duomenų valdytojui atlikti PDAV** ir suteikti bet kurią būtiną informaciją (pagal 28 straipsnio 3 dalies f punktą).

Duomenų valdytojas privalo „atitinkamais atvejais <...> išsiaiškinti duomenų subjektų ar jų atstovų nuomonę“ (35 straipsnio 9 dalis). 29 straipsnio darbo grupė mano, kad:

- šias nuomones galima būtų gauti įvairiomis priemonėmis, priklausomai nuo konteksto (pvz., bendro pobūdžio tyrimas, susijęs su duomenų tvarkymo operacijos tikslu ir priemonėmis,

[23] Išskyrus atvejus, kai duomenys jau tvarkomi ir tokį tvarkymą anksčiau patikrino priežiūros institucija, tuomet PDAV turėtų būti atliekamas prieš įvykdant svarbius pakeitimus.

klausimas darbuotojų atstovams arba įprastos apklausos, kurios siunčiamos būsimiems duomenų valdytojo klientams), kuriomis užtikrinama, kad duomenų valdytojas turėtų teisėtą bet kokių asmens duomenų, susijusių su tokių nuomonių gavimu, tvarkymo pagrindą. Vis dėlto reikėtų pažymėti, kad sutikimas su duomenų tvarkymu, savaime suprantama, nėra būdas siekti gauti duomenų subjektų nuomones;

- jeigu duomenų valdytojo galutinis sprendimas skiriasi nuo duomenų subjektų nuomonių, šio sprendimo tolesnio įgyvendinimo arba neįgyvendinimo motyvus taip pat reikėtų dokumentuoti;
- duomenų valdytojas taip pat turėtų dokumentuoti priežastis, dėl kurių jis nesiekia išsiaiškinti duomenų subjektų nuomonių, jei nusprendžia, kad tai nėra tinkama, pvz., jei tai pažeistų įmonių verslo planų konfidencialumą arba būtų neproporcinga ar nepraktiška.

Galiausiai gera praktika yra apibrėžti ir dokumentuoti kitus konkrečius vaidmenis ir pareigas, priklausomai nuo vidaus politikos, procesų ir taisyklių, pvz.,

- tais atvejais, kai konkretūs verslo padaliniai gali pasiūlyti atlikti PDAV, tuomet jie turėtų pateikti su PDAV susijusius duomenis ir dalyvauti PDAV patvirtinimo procese;
- kai tinkama, rekomenduojama pabandyti konsultuotis su nepriklausomais įvairių profesijų ekspertais[24] (teisininkais, IT specialistais, saugumo ekspertais, sociologais, etikos specialistais ir pan.).
- duomenų tvarkytojų vaidmenys ir pareigos turi būti nustatomos sutartyje, be to, PDAV turi būti atliekamas padedant duomenų tvarkytojui ir atsižvelgiant į duomenų tvarkymo pobūdį bei duomenų tvarkytojui prieinamą informaciją (28 straipsnio 3 dalies f punktas);
- vyriausiasis informacijos saugumo pareigūnas (angl. CISO), jei jis paskirtas, taip pat duomenų apsaugos pareigūnas galėtų pasiūlyti duomenų valdytojui atlikti konkrečios duomenų tvarkymo operacijos PDAV, be to, jie turėtų padėti suinteresuotiesiems subjektams metodikos klausimais, padėti įvertinti pavojaus vertinimo kokybę ir nustatyti, ar likutinė pavojaus rizika yra priimtina, taip pat padėti tobulinti su duomenų valdytojo veiklos aplinkybėmis susijusias konkrečias žinias;
- vyriausiasis informacijos saugumo pareigūnas (CISO), jei jis paskirtas, ir (arba) IT departamentas turėtų suteikti pagalbą duomenų valdytojui, ir, priklausomai nuo saugumo arba veiklos poreikių, galėtų pasiūlyti atlikti konkrečios duomenų tvarkymo operacijos PDAV.

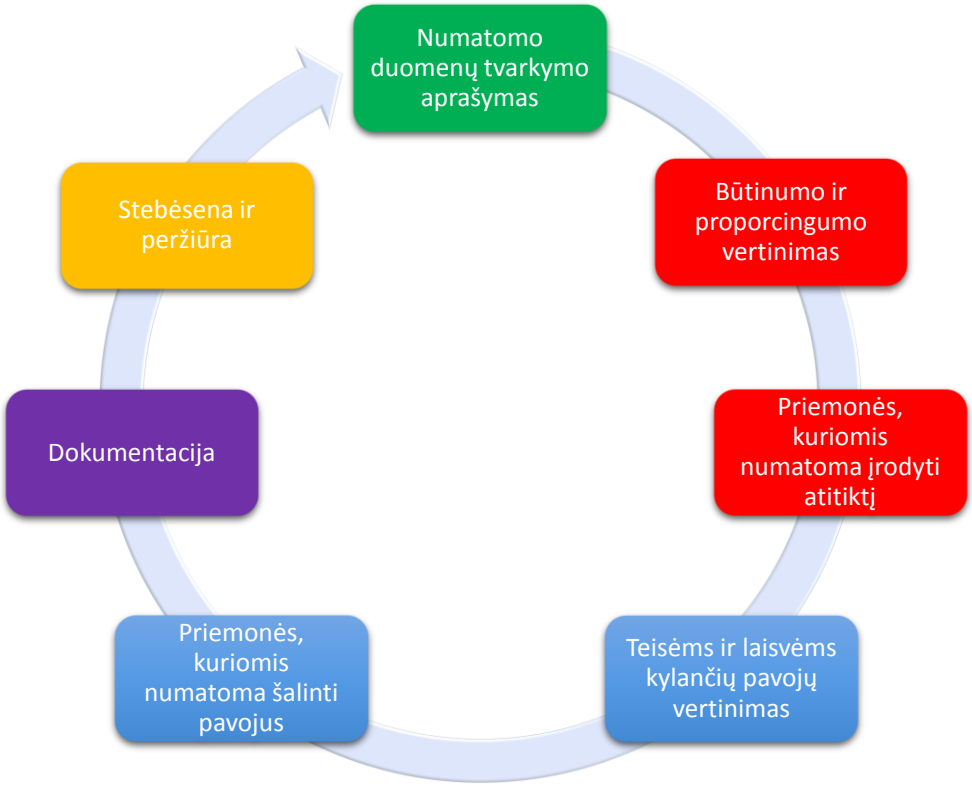
c) Kokia metodika taikoma atliekant PDAV? Skirtinga metodika, tačiau bendri kriterijai.

[24] *Rekomendacijos dėl Europos Sąjungos poveikio privatumui vertinimo sistemos, D3 rezultatas:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

BDAR nustatyti minimalūs PDAV požymiai (35 straipsnio 7 dalis ir 84 ir 90 konstatuojamosios dalys):

- „numatytų duomenų tvarkymo operacijų aprašymas ir duomenų tvarkymo tikslai“;
- „duomenų tvarkymo operacijų reikalingumo ir proporcingumo <...> vertinimas“;
- „duomenų subjektų teisėms ir laisvėms kylančių pavojų vertinimas“;
- numatomas priemones:
    - „pavojams pašalinti“;
    - kuriomis „įrodoma, kad laikomasi šio reglamento“.

Toliau pateiktame paveiksle pavaizduotas bendro pobūdžio pasikartojantis PDAV atlikimo procesas[25]:



Vertinant duomenų tvarkymo operacijos poveikį, būtina atsižvelgti į (35 straipsnio 8 dalis) elgesio kodeksą (40 straipsnis). Tai gali būti naudinga siekiant parodyti, kad buvo pasirinktos arba nustatytos tinkamos priemonės, jeigu elgesio kodeksas yra tinkamas tai duomenų tvarkymo operacijai. Siekiant įrodyti, kad duomenų valdytojų ir tvarkytojų tvarkymo operacijos atitinka BDAR, taip pat reikėtų atsižvelgti į sertifikatus, antspaudus ir ženklus (42 straipsnis), taip pat į įmonei privalomas taisykles.

Visi BDAR nustatyti susiję reikalavimai sudaro plataus masto, bendrą sistemą, pagal kurią PDAV yra pritaikomas ir atliekamas. Praktinis PDAV įgyvendinimas priklausys nuo BDAR nustatytų reikalavimų, kuriuos gali papildyti išsamesnės praktinės rekomendacijos. Todėl PDAV įgyvendinimo mastą galima keisti. Tai reiškia, kad net ir nedidelis duomenų valdytojas gali pritaikyti ir atlikti PDAV, kuris atitiktų jo duomenų tvarkymo operacijas.

[25] Reikėtų pažymėti, kad čia pavaizduotas procesas yra pasikartojantis: praktiškai tikėtina, kad kiekvienas etapas prieš užbaigiant PDAV bus peržiūrėtas keletą kartų.

BDAR 90 konstatuojamojoje dalyje pateikti įvairūs PDAV komponentai, kurie sutampa su gerai apibrėžtais rizikos valdymo komponentais (pvz., ISO 31000[26]). Rizikos valdymo požiūriu PDAV siekiama „valdyti“ fizinių asmenų teisėms ir laisvėms kylančius „pavojus“ naudojant toliau nurodytus procesus:

- nustatant aplinkybes: atsižvelgiant į „duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus bei pavojaus šaltinius“;
- įvertinant riziką: įvertinant „didelio pavojaus konkrečią tikimybę ir rimtumą“;
- valdant riziką: sumažinant „tą pavojų“ ir užtikrinant „asmens duomenų apsaugą“, ir parodant, „kad laikomasi šio reglamento“.

Pastaba. Pagal BDAR PDAV yra duomenų subjektų teisėms kylančių pavojų valdymo priemonė, todėl PDAV atsižvelgiama į jų padėtį, kaip tai daroma tam tikrose srityse (pvz., visuomenės saugumo). Rizikos valdymas kitose srityse (pvz., informacijos saugumo), priešingai, yra orientuotas į organizaciją.

BDAR numatytos lanksčios nuostatos, kurios leidžia duomenų valdytojams nustatyti tikslią PDAV struktūrą ir formą taip siekiant sudaryti sąlygas nustatyti esamą darbo praktiką atitinkančią PDAV struktūrą. ES ir pasauliniu mastu sukurta daug įvairių procesų, kuriuose atsižvelgiama į 90 konstatuojamojoje dalyje aprašytus komponentus. Tačiau, nepaisant formos, PDAV turi būti tikras pavojų vertinimas, leidžiantis duomenų valdytojams imtis priemonių jiems pašalinti.

Siekiant padėti įgyvendinti BDAR nustatytus pagrindinius reikalavimus, galima naudoti įvairią metodiką (žr. 1 priedą, kuriame pateikiami poveikio duomenų apsaugai ir privatumui vertinimo metodikų pavyzdžiai). Siekiant sudaryti sąlygas egzistuoti šiems skirtingiems metodams kartu leidžiant duomenų valdytojams laikytis BDAR, buvo nustatyti bendri kriterijai (žr. 2 priedą). Juose paaiškinami pagrindiniai reglamento reikalavimai, tačiau suteikiama pakankamai erdvės skirtingų formų įgyvendinimui. Šie kriterijai gali būti naudojami siekiant parodyti, kad konkreti PDAV metodika atitinka standartus, kurių reikalaujama laikytis pagal BDAR. **Metodiką pasirenka duomenų valdytojas, tačiau ji turėtų atitikti 2 priede nustatytus kriterijus.**

29 straipsnio darbo grupė ragina sukurti konkretiems sektoriams pritaikytas PDAV sistemas. Taip yra todėl, kad jie gali remtis konkrečiomis sektoriaus žiniomis, o tai reiškia, kad PDAV galima aptarti specifinius konkrečios duomenų tvarkymo operacijos aspektus (pvz., konkrečių rūšių duomenys, įmonės turtas, galimas poveikis, grėsmės, priemonės). Tai reiškia, kad PDAV galima aptarti konkrečiame ekonomikos sektoriuje kylančius klausimus arba klausimus, kurie kyla naudojant konkrečias technologijas arba vykdant konkrečių rūšių duomenų tvarkymo operaciją.

Galiausiai prireikus „duomenų valdytojas atlieka peržiūrą, kad įvertintų, ar duomenys tvarkomi laikantis poveikio duomenų apsaugai vertinimo, bent tais atvejais, kai pakinta tvarkymo operacijų keliamas pavojus“ (35 straipsnio 11 dalis[27]).

[26] Rizikos valdymo procesai: bendravimas ir konsultacijos, konteksto nustatymas, rizikos vertinimas, rizikos valdymas, stebėsena ir peržiūra (žr. ISO 31000 terminus ir apibrėžtis ir turinį (peržiūrėti galima adresu https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

[27] 35 straipsnio 10 dalyje numatyta tik 35 straipsnio 1–7 dalių taikymo išimtis.

d) Ar privaloma skelbti PDAV? Ne, tačiau santraukos paskelbimas galėtų padidinti pasitikėjimą, o išsamus PDAV turi būti perduotas priežiūros institucijai, jei su ja anksčiau buvo konsultuojamasi arba jei to prašo duomenų apsaugos institucija.

PDAV paskelbimas nėra BDAR nustatytas teisinis reikalavimas, šiuo klausimu sprendimą priima duomenų valdytojas. Tačiau duomenų valdytojai turėtų įvertinti galimybę paskelbti bent jau tokias dalis kaip jų atlikto PDAV santrauka arba išvada.

Tokio proceso tikslas būtų padėti didinti pasitikėjimą duomenų valdytojo atliekamomis duomenų tvarkymo operacijomis ir įrodyti, kad laikomasi atskaitomybės ir skaidrumo principų. Gera praktika laikomas PDAV paskelbimas, kai duomenų tvarkymo operacija turi poveikį visuomenės nariams. Tai visų pirma galėtų būti tais atvejais, kai PDAV atlieka valdžios institucija.

Paskelbtame PDAV neturi būti pateiktas visas vertinimas, ypač tais atvejais, kai PDAV galėtų būti pateikta konkreti informacija, susijusi su duomenų valdytojui kylančia rizika arba atskleidžianti komercines paslaptis arba neskelbtiną komercinę informaciją. Tokiu atveju paskelbtą versiją galėtų sudaryti tik pagrindinių PDAV išvadų santrauka arba tiesiog pareiškimas, kad PDAV buvo atliktas.

Be to, tais atvejais, kai PDAV nustatoma didelė likutinė rizika, duomenų valdytojas turės iš anksto konsultuotis dėl duomenų tvarkymo su priežiūros institucija (36 straipsnio 1 dalis). Šiuo atveju turi būti pateiktas visas PDAV (36 straipsnio 3 dalies e punktas). Priežiūros institucija gali pateikti savo rekomendacijas[28] ir neatskleis prekybos paslapčių arba pažeidžiamų saugumo vietų ir laikysis kiekvienoje valstybėje narėje taikomų principų, pagal kuriuos visuomenei suteikiama galimybė susipažinti su oficialiais dokumentais.

E. <u>Kada reikėtų konsultuotis su priežiūros institucija? Kai yra didelė likutinė rizika.</u>

Kaip paaiškinta pirmiau:

- PDAV reikalaujama atlikti kai dėl duomenų tvarkymo operacijos „ fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus“ (35 straipsnio 1 dalis, žr. III skyriaus B dalies a punktą). Pavyzdžiui, sveikatos duomenų tvarkymas dideliu mastu gali kelti didelį pavojų ir dėl jo reikia atlikti PDAV:
- tuomet duomenų valdytojas privalo įvertinti duomenų subjektų teisėms ir laisvėms kylančius pavojus ir nustatyti priemones[29], kuriomis numatoma sumažinti šiuos pavojus iki priimtino lygmens ir įrodyti atitiktį BDAR (35 straipsnio 7 dalis, žr. III skyriaus C dalies c punktą). Kaip pavyzdį galima paminėti asmens duomenų saugojimą nešiojamuosiuose kompiuteriuose, tinkamų techninių ir organizacinių saugumo priemonių naudojimą (veiksmingas viso disko šifravimas, griežtas rakto valdymas, tinkama prieigos kontrolė, apsaugotos atsarginės kopijos ir pan.) greta esamų politinių priemonių (pranešimas, sutikimas, prieigos teisė, teisė prieštarauti ir pan.).

Kalbant apie pirmiau minėtą nešiojamojo kompiuterio pavyzdį: jeigu duomenų valdytojas nusprendė, kad pavojai buvo pakankamai sumažinti ir atsižvelgiant į 36 straipsnio 1 dalies ir 84 ir 94 konstatuojamųjų dalių formuluotes, manytina, kad duomenys gali būti tvarkomi nesikonsultuojant su

[28] Rašytinė duomenų valdytojo konsultacija yra būtina tik kai priežiūros institucija laikosi nuomonės, kad numatomas duomenų tvarkymas neatitinka 36 straipsnio 2 dalyje nustatytos tvarkos.

[29] Taip pat atsižvelgti į esamas Europos duomenų apsaugos valdybos ir priežiūros institucijų rekomendacijas ir techninių galimybių išsivystymo lygį ir įgyvendinimo išlaidas, kaip nustatyta 35 straipsnio 1 dalyje.

priežiūros institucija. Duomenų valdytojas privalo konsultuotis su priežiūros institucija būtent tais atvejais, kai duomenų valdytojas negali tinkamai pašalinti nustatytų pavojų (t. y. likutinė rizika išlieka didelė).

Nepriimtinos didelės likutinės rizikos pavyzdžiai apima atvejus, kai duomenų subjektai gali susidurti su rimtomis arba net neištaisomomis pasekmėmis, kurių jie negali pašalinti (pvz., neteisėta prieiga prie duomenų, dėl kurios kyla pavojus duomenų subjektų gyvybei, jie gali būti atleisti iš darbo, jiems gresia finansinis pavojus) ir (arba) kai atrodo akivaizdu, kad pavojus taps realus (pvz., nes negalima sumažinti žmonių, turinčių prieigos prie duomenų, skaičiaus atsižvelgiant į jų dalijimosi, naudojimo arba paskirstymo būdus, arba kai neužkamšoma gerai žinoma spraga).

Tais atvejais, kai duomenų valdytojas negali rasti priemonių, kurių pakaktų pavojui sumažinti iki priimtino lygio (t. y. likutinė rizika vis dar yra didelė), reikalaujama konsultuotis su priežiūros institucija[30].

Be to, duomenų valdytojas turės konsultuotis su priežiūros institucija tais atvejais, kai pagal valstybės narės teisę reikalaujama, kad duomenų valdytojai konsultuotųsi su priežiūros institucija dėl duomenų valdytojo vykdomos duomenų tvarkymo operacijos, kuria siekiama vykdyti su viešuoju interesu susijusią užduotį, įskaitant duomenų tvarkymą siekiant užtikrinti socialinę apsaugą ir visuomenės sveikatą, arba gautų išankstinį priežiūros institucijos leidimą (36 straipsnio 5 dalis).

Tačiau reikėtų pareikšti, kad, nepaisant to, ar, remiantis likutinės rizikos lygiu, reikalinga konsultuotis su priežiūros institucija, pareigos išlaikyti PDAV įrašą ir tinkamai atnaujinti PDAV lieka galioti toliau.

IV. Išvados ir rekomendacijos

PDAV yra naudingas būdas, kurį naudodami duomenų valdytojai gali įdiegti BDAR atitinkančias duomenų valdymo sistemas, be to, PDAV gali būti privaloma atlikti dėl tam tikrų rūšių duomenų tvarkymo operacijų. PDAV gali būti nevienodo masto ir skirtingų formų, tačiau BDAR nustatyti pagrindiniai veiksmingo PDAV reikalavimai. Duomenų valdytojai turėtų vertinti PDAV atlikimą kaip naudingą ir teigiamą veiklą, kuri padeda užtikrinti teisinę atitiktį.

24 straipsnio 1 dalyje nustatyta bendroji duomenų valdytojo atsakomybė laikytis BDAR: „[a]tsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos.“

PDAV yra pagrindinis reglamento laikymosi aspektas tais atvejais, kai planuojama vykdyti didelį pavojų keliančias duomenų tvarkymo operacijas arba jos yra vykdomos. Tai reiškia, kad duomenų valdytojai turėtų naudoti šiame dokumente nustatytus kriterijus, kad išsiaiškintų, ar reikia atlikti PDAV. Duomenų valdytojo vidaus politikos nuostatose be BDAR teisinių reikalavimų gali būti nustatyti ir kiti papildomi reikalavimai. Tai turėtų padėti užtikrinti didesnį duomenų subjektų ir kitų duomenų valdytojų pasitikėjimą.

[30] Pastaba. „*Pseudonimų suteikimas asmens duomenims ir jų šifravimas*“ (taip pat duomenų minimzavimas, priežiūros mechanizmai ir pan.) nebūtinai yra tinkamos priemonės. Tai tik pavyzdžiai. Tinkamos priemonės priklauso nuo konteksto ir pavojų, būdingų duomenų tvarkymo operacijoms.

Tais atvejais, kai planuojama atlikti duomenų tvarkymo operacijas, kurios gali kelti didelį pavojų, duomenų valdytojas privalo:

- pasirinkti PDAV metodiką (pavyzdžiai pateikiami 1 priede), kuri atitinka 2 priede nurodytus kriterijus, arba nustatyti ir įgyvendinti sistemingo PDAV procesą:
  - kuris atitinka 2 priedo reikalavimus;
  - kuris yra integruotas į esamus pritaikymo, plėtojimo, keitimo , pavojaus ir veiklos peržiūros procesus laikantis vidaus procedūrų, aplinkybių ir kultūros;
  - kuriame dalyvauja atitinkamos suinteresuotosios šalys ir kuriame aiškiai apibrėžtos jų pareigos (duomenų valdytojas, duomenų apsaugos pareigūnas, duomenų subjektai ar jų atstovai, įmonės, techninės tarnybos, duomenų tvarkytojai, informacijos saugumo pareigūnai ir pan.);
- kurio metu rengiama kompetentingai priežiūros institucijai skirta PDAV ataskaita, kai jos reikalaujama;
- kurio metu konsultuojamasi su priežiūros institucija, kai duomenų valdytojui nepavyksta nustatyti pakankamų priemonių dideliems pavojams sumažinti;
- kuriame numatyta periodinė PDAV ir per jį vertinamo duomenų tvarkymo peržiūra bent jau tais atvejais, kai gali pasikeisti duomenų tvarkymo operacijos keliamas pavojus;
- kurioje dokumentuojamas priimtas sprendimas.

1 priedas. Esamų ES PDAV sistemų pavyzdžiai

BDAR konkrečiai nenurodyta, kuriais PDAV procesais reikia vadovautis, tačiau jame duomenų valdytojams leidžiama nustatyti jų susiklosčiusią darbo praktiką papildančią sistemą, jeigu joje atsižvelgiama į 35 straipsnio 7 dalyje aprašytus aspektus. Tokia sistema duomenų valdytojui gali būti parengta pagal specialų užsakymą arba galioti konkrečiame sektoriuje. Anksčiau paskelbtos sistemos, kurias parengė ES duomenų apsaugos institucijos, ir ES sektorinės sistemos apima (sąrašas neišsamus):

bendro pobūdžio ES sistemų pavyzdžiai:

- DE: Standartinis duomenų apsaugos modelis, V.1.0 – bandomoji versija, 2016[31]. (https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf).
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014 (https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf).
- FR: Poveikio privatumui vertinimas (PPV), *Commission nationale de l'informatique et des libertés* (CNIL), 2015 (https://www.cnil.fr/fr/node/15798).
- UK: Poveikio privatumui vertinimo atlikimo praktikos kodeksas, Informacijos komisaro biuras (angl. ICO), 2014 (https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf).

Konkrečių ES sektorių sistemų pavyzdžiai:

- Radijo dažninio atpažinimo paraiškų poveikio privatumuiir duomenų apsaugai vertinimo sistema[32]. (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf).
- Pažangiųjų tinklų ir pažangiųjų apskaitos sistemų poveikio duomenų apsaugai vertinimo formos[33] (http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf).

Tarptautiniame standarte taip pat pateikiamos rekomendacijos dėl PDAV atlikimo metodikos (ISO/IEC 29134[34]).

---

[31] Jai vieningai pritarė 92 nariai (Bavarija susilaikė). 2016 m. lapkričio 9–10 d. Kiūlungsborne įvykusi federalinės administracijos ir žemių administracijų nepriklausomų duomenų apsaugos institucijų konferencija

[32] Taip pat žr.

- 2009 m. gegužės 12 d. Komisijos rekomendaciją dėl privatumo ir duomenų apsaugos principų įgyvendinimo taikomosiose priemonėse, kurių naudojimas pagrįstas radijo dažniniu atpažinimu (https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles);
- Nuomonę 9/2011 dėl peržiūrėto pramonės atstovų pasiūlymo sukurti RDA taikomųjų priemonių poveikio privatumui ir duomenų apsaugai vertinimo sistemą (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_lt.pdf).

[33] Taip pat žr. Nuomonę 07/2013 dėl pažangiųjų tinklų ir pažangiųjų apskaitos sistemų poveikio duomenų apsaugai vertinimo formos (PDAV šablonas), kurią parengė Komisijos Europos pažangiųjų tinklų darbo grupės 2-a ekspertų grupė (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_lt.pdf).

2 priedas. Priimtino PDAV kriterijai

29 straipsnio darbo grupė siūlo toliau nurodytus kriterijus, kuriais remdamiesi duomenų valdytojai gali įvertinti, ar PDAV arba PDAV atlikimo metodika yra pakankamai išsami, kad atitiktų BDAR:

- ☐ pateiktas sisteminiss duomenų tvarkymo operacijų aprašymas (35 straipsnio 7 dalies a punktas):
  - ☐ atsižvelgiama į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus (90 konstatuojamoji dalis);
  - ☐ registruojami asmens duomenys, gavėjai ir asmens duomenų saugojimo laikotarpis;
  - ☐ pateikiamas funkcinis duomenų tvarkymo operacijos aprašymas;
  - ☐ nustatomas turtas, kuris naudojamas tvarkant asmens duomenis (aparatinė įranga, programinė įranga, tinklai, žmonės, spausdinti dokumentaiarba spausdintų dokumentų siuntimo kanalai);
  - ☐ atsižvelgiama į atitiktį patvirtintiems elgesio kodeksams (35 straipsnio 8 dalis);
- ☐ įvertinamas būtinumas ir proporcingumas (35 straipsnio 7 dalies b punktas):
  - ☐ nustatomos priemonės, kuriomis numatoma užtikrinti atitiktį reglamentui (35 straipsnio 7 dalies d punktas ir 90 konstatuojamoji dalis), atsižvelgiant į:
    - ☐ priemones, kuriomis prisidedama prie duomenų tvarkymo proporcingumo ir būtinumo remiantis:
      - ☐ konkrečiu (-iais), aiškiu (-iais) ir teisėtu (-ais) tikslu (-ais) (5 straipsnio 1 dalies b punktas);
      - ☐ tvarkymo teisėtumu (6 straipsnis);
      - ☐ adekvačiais, tinkamais ir tik tokiais, kurių reikia siekiant tikslų, duomenimis (5 straipsnio 1 dalies c punktas);
      - ☐ ribota saugojimo trukme (5 straipsnio 1 dalies e punktas);
    - ☐ priemones, padedančias užtikrinti duomenų subjektų teises:
      - ☐ duomenų subjektui teikiama informacija (12, 13 ir 14 straipsniai);
      - ☐ teisė susipažinti su duomenimis ir teisė į duomenų perkeliamumą (15 ir 20 straipsniai);
      - ☐ teisė ištaisyti ir ištrinti duomenis (16, 17 ir 19 straipsniai);
      - ☐ teisė prieštarauti duomenų tvarkymui ir teisė apriboti duomenų tvarkymą (18, 19 ir 21 straipsniai);
      - ☐ santykiai su duomenų tvarkytojais (28 straipsnis);
      - ☐ su tarptautiniu (-iais) perdavimu (-ais) susijusios apsaugos priemonės (V skyrius);
      - ☐ išankstinės konsultacijos (36 straipsnis).
- ☐ valdomi duomenų subjektų teisėms ir laisvėms kylantys pavojai (35 straipsnio 7 dalies c punktas):
  - ☐ įvertinama pavojų kilmė, pobūdis, specifika ir rimtumas (plg. 84 konstatuojamąją dalį) arba konkrečiau tariant, įvertinamas kiekvienas pavojus (neteisėta prieiga prie duomenų, nepageidaujamas duomenų pakeitimas ir duomenų pradanginimas) iš duomenų subjektų perspektyvos:
    - ☐ atsižvelgiama į pavojų šaltinius (90 konstatuojamoji dalis);
    - ☐ nustatomas galimas poveikis duomenų subjektų teisėms ir laisvėms tam tikrais atvejais, kai, pavyzdžiui, prieiga prie duomenų yra neteisėta, duomenys nepageidaujamai pakeičiami arba pradanginami;
    - ☐ nustatomos grėsmės, dėl kurių gali būti gaunama neteisėta prieiga prie duomenų, jie gali būti nepageidaujamai pakeičiami arba pradanginami;
    - ☐ įvertinama tikimybė ir rimtumas (90 konstatuojamoji dalis);

[34] ISO/IEC 29134 (projektas), *Informacinės technologijos – Saugumo būdai – Poveikio privatumui vertinimas – rekomendacijos*, Tarptautinė standartizacijos organizacija (ISO).

- ☐ nustatomos priemonės, kuriomis planuojama šalinti šiuos pavojus (35 straipsnio 7 dalies d punktas ir 90 konstatuojamoji dalis);

☐ dalyvauja suinteresuotosios šalys:

- ☐ siekiama konsultuotis su duomenų apsaugos pareigūnu (35 straipsnio 2 dalis);
- ☐ kai tinkama, siekiama išsiaiškinti duomenų subjektų arba jų atstovų nuomones (35 straipsnio 9 dalis).