Gairės

Gairės Nr. 9/2022 dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal BDAR

2.0 versija

Priimta 2023 m. kovo 28 d.

This language version has not yet been proofread.

Informacija apie versijas

1.0 versija	2022 m. spalio 10 d.	Priimtos gairės (ankstesnių gairių WP250 (rev.01), kurias priėmė 29 straipsnio darbo grupė ir 2018 m. gegužės 25 d. patvirtino EDAV, atnaujinta versija) dėl tikslinių viešų konsultacijų.
2.0 versija	2023 m. kovo 28 d.	Po tikslinių viešų konsultacijų priimtos EEE neįsisteigusiems duomenų valdytojams skirtos gairės dėl pranešimo apie duomenų saugumo pažeidimus.

TURINYS

Europos duomenų apsaugos valdyba,

atsižvelgdama į 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 (toliau – BDAR), 70 straipsnio 1 dalies e ir l punktus,

atsižvelgdama į EEE susitarimą, ypač į jo XI priedą ir 37 protokolą, su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018[1],

atsižvelgdama į savo Darbo tvarkos taisyklių 12 ir 22 straipsnius,

atsižvelgdama į 29 straipsnio darbo grupės gaires dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal Reglamentą 2016/679, WP250 rev.01,

PRIĖMĖ ŠIAS GAIRES:

0 ĮVADAS

1. 2017 m. spalio 3 d. 29 straipsnio darbo grupė priėmė gaires dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal Reglamentą 2016/679 (WP250 rev.01)[2], kurias per pirmąjį plenarinį posėdį patvirtino Europos duomenų apsaugos valdyba (toliau – EDAV)[3]. Šis dokumentas – šiek tiek atnaujinta tų gairių versija. Bet kokia nuoroda į 29 straipsnio darbo grupės gaires dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal Reglamentą 2016/679 (WP250 rev.01) nuo šiol turėtų būti suprantama kaip nuoroda į šias EDAV gaires Nr. 9/2022.
2. EDAV pastebėjo, kad reikia patikslinti reikalavimus, taikomus pranešimui apie asmens duomenų saugumo pažeidimus ne ES buveinėse. Atitinkama dalis buvo peržiūrėta ir atnaujinta, o visas likęs dokumentas nepakeistas, išskyrus redakcines pataisas. Konkrečiai, buvo peržiūrėtas šio dokumento II.C.2 skirsnio 73 punktas.

ĮVADAS

3. BDAR nustatytas reikalavimas apie kiekvieną asmens duomenų saugumo pažeidimą (toliau – pažeidimas) pranešti kompetentingai nacionalinei priežiūros institucijai [4] (arba, jei pažeidimas tarpvalstybinio pobūdžio, vadovaujančiai institucijai) ir tam tikrais atvejais apie pažeidimą informuoti asmenis, kuriems jis turėjo poveikio.
4. Prievolės pranešti apie pažeidimus buvo taikomos tam tikroms organizacijoms, pvz., viešųjų elektroninių ryšių paslaugų teikėjams (kaip nurodyta Direktyvoje 2009/136/EB ir Reglamente (ES) Nr. 611/2013)[5]. Be to, kai kurios ES valstybės narės pačios buvo nustačiusios nacionalines prievoles pranešti apie pažeidimus. Pavyzdžiui, jomis galėjo būti įpareigota pranešti apie pažeidimus, susijusius

[1] Nuorodos į valstybes nares šiame dokumente turėtų būti suprantamos kaip nuorodos į EEE valstybes nares.
[2] 29 straipsnio darbo grupės gairės dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal Reglamentą 2016/679 (WP250 rev.01) (paskutinį kartą peržiūrėtos ir atnaujintos 2018 m. vasario 6 d.), paskelbtos adresu https://ec.europa.eu/newsroom/article29/items/612052.
[3] Žr. https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_lt.
[4] Žr. BDAR 4 straipsnio 21 punktą.
[5] Žr. http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex:32009L0136 ir http://eur-lex.europa.eu/legalcontent/LT/TXT/?uri=CELEX%3A32013R0611

ne tik su viešųjų elektroninių ryšių paslaugų tiekėjais, bet ir su tam tikrų kategorijų duomenų valdytojais (pvz., tokia prievolė nustatyta Vokietijoje ir Italijoje), arba apie visus pažeidimus, susijusius su asmens duomenimis (pvz., tokia prievolė nustatyta Nyderlanduose). Kitos valstybės narės turėjo atitinkamus praktikos kodeksus (pvz., Airija [6]). Įvairios ES duomenų apsaugos institucijos skatino duomenų valdytojus pranešti apie pažeidimus, tačiau Duomenų apsaugos direktyvoje 95/46/EB[7], kurią pakeitė BDAR, nebuvo nustatyta konkrečios prievolės pranešti apie pažeidimus, todėl daugeliui organizacijų šis reikalavimas buvo naujas. Pagal BDAR pranešti apie pažeidimus privalo visi duomenų valdytojai, nebent dėl pažeidimo neturėtų kilti pavojaus asmenų teisėms ir laisvėms[8]. Duomenų tvarkytojams taip pat tenka svarbus vaidmuo, apie kiekvieną pažeidimą jie privalo pranešti savo duomenų valdytojui[9].

5. EDAV mano, kad reikalavimas pranešti yra naudingas įvairiais atžvilgiais. Pranešę priežiūros institucijai, duomenų valdytojai gali gauti patarimą, ar reikia informuoti asmenis, kuriems pažeidimas turi poveikio. Priežiūros institucija gali ir liepti duomenų valdytojui informuoti tuos asmenis apie pažeidimą[10]. Pranešdamas asmenims apie pažeidimą, duomenų valdytojas gali pateikti informaciją apie pavojus, kurie kyla dėl pažeidimo, ir veiksmus, kurių tiek asmenys gali imtis, norėdami apsisaugoti nuo galimų to pažeidimo pasekmių. Be kokiu reagavimo į pažeidimą planu pirmiausia turėtų būti siekiama apsaugoti asmenis ir jų asmens duomenis. Todėl pranešimas apie pažeidimą turėtų būti vertinamas kaip priemonė, padedanti laikytis reikalavimų, susijusių su asmens duomenų apsauga. Kartu reikėtų pažymėti, kad asmens arba priežiūros institucijos neinformavus apie pažeidimą, duomenų valdytojui gali būti taikoma kuri nors iš BDAR 83 straipsnyje nustatytų sankcijų.

6. Todėl duomenų valdytojai ir duomenų tvarkytojai raginami iš anksto numatyti ir įgyvendinti procedūras, pagal kurias būtų galima nustatyti ir skubiai sustabdyti pažeidimą, įvertinti asmenims kilusį pavojų[11] ir tuomet nustatyti, ar apie pažeidimą būtina pranešti kompetentingai priežiūros institucijai ir, kai reikia, apie jį informuoti susijusius asmenis. Pranešimas priežiūros institucijai turėtų būti to reagavimo į incidentus plano sudedamoji dalis.

7. BDAR nustatyta, kada reikia pranešti apie pažeidimą, taip pat kam ir kokia informacija turėtų būti pateikta tame pranešime. Pranešant pateiktina informacija gali būti pateikiama etapais, tačiau bet kokiu atveju duomenų valdytojai į bet kokį pažeidimą turėtų reaguoti laiku.

8. Nuomonėje 03/2014 dėl pranešimo apie asmens duomenų saugumo pažeidimą[12] 29 straipsnio darbo grupė duomenų valdytojams pateikė gaires, kuriomis siekta padėti priimti sprendimą, ar apie pažeidimą pranešti duomenų subjektams. Šioje nuomonėje aptarta Direktyvoje 2002/58/EB elektroninių ryšių paslaugų teikėjams nustatyta prievolė ir, atsižvelgiant į tuometinį BDAR projektą, pateikta pavyzdžių iš įvairių sektorių ir visi duomenų valdytojai supažindinti su atitinkama gerąja praktika.

---

[6] Žr. https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm.

[7] Žr. http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex:31995L0046

[8] ES pagrindinių teisių chartijoje įtvirtintos teisės, žr. http://eurlex.europa.eu/legal-content/LT/TXT/?uri=CELEX:12012P/TXT

[9] Žr. BDAR 33 straipsnio 2 punktą. Ši nuostata panaši į Reglamento (ES) Nr. 611/2013 5 straipsnyje nustatytą principą, kad tuo atveju, kai teikėjas elektroninių ryšių paslaugą iš dalies teikia naudodamasis kito teikėjo (kuris su abonentais nėra tiesiogiai susietas sutartiniais santykiais) paslaugomis, pastarasis teikėjas asmens duomenų saugumo pažeidimo atveju privalo nedelsdamas informuoti teikėją, su kuriuo yra sudaręs paslaugos teikimo sutartį.

[10] Žr. BDAR 34 straipsnio 4 dalį ir 58 straipsnio 2 dalies e punktą.

[11] Tai galima užtikrinti vykdant reikalavimo dėl poveikio duomenų apsaugai vertinimo laikymosi stebėseną ir peržiūrą, kurios yra privalomos duomenų tvarkymo operacijoms, dėl kurių gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms (35 straipsnio 1 ir 11 dalys).

[12] Žr. 29 straipsnio darbo grupės nuomonę 03/2014 dėl pranešimo apie asmens duomenų saugumo pažeidimą http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf .

9. Šiose gairėse paaiškinami privalomi BDAR reikalavimai, susiję su pranešimu ir informavimu apie pažeidimus, ir kai kurie veiksmai, kurių duomenų valdytojai ir duomenų tvarkytojai gali imtis, norėdami įvykdyti šias prievoles. Gairėse taip pat pateikiama įvairaus pobūdžio pažeidimų pavyzdžių ir nurodoma, kam, atsižvelgiant į skirtingus scenarijus, apie juos turėtų būti pranešta.

I. PRANEŠIMŲ APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS TEIKIMAS PAGAL BDAR

A. Pagrindiniai saugumo aspektai

10. Vienas iš BDAR reikalavimų yra tas, kad asmens duomenys turėtų būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ir organizacines priemones, būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo, taip pat nuo netyčinio praradimo, sunaikinimo ar sugadinimo[13].

11. BDAR atitinkamai reikalaujama, kad duomenų valdytojai ir duomenų tvarkytojai įgyvendintų tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų tvarkomiems asmens duomenims atitinkančio lygio saugumas. Jie turėtų atsižvelgti į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms[14]. Be to, Bendrajame duomenų apsaugos reglamente reikalaujama įgyvendinti visas tinkamas technologines apsaugos ir organizacines priemones, kad nedelsiant būtų nustatyta, ar buvo padarytas pažeidimas, ir, atsižvelgiant į tai, ar taikoma prievolė pranešti[15].

12. Taigi vienas iš pagrindinių bet kokios duomenų saugumo politikos aspektų yra gebėjimas, kai įmanoma, užkirsti kelią pažeidimui, o tuo atveju, jei jis vis tiek padaromas, laiku į jį reaguoti.

B. Kas yra asmens duomenų saugumo pažeidimas?

1. Apibrėžtis

13. Kad galėtų pašalinti pažeidimą, duomenų valdytojas visų pirma turi gebėti jį atpažinti. BDAR 4 straipsnio 12 dalyje asmens duomenų saugumo pažeidimas apibrėžtas taip:

> *„saugumo pažeidimas, 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“.*

14. Asmens duomenų „sunaikinimo“ sąvoka yra pakankamai aiški: tai situacija, kai duomenų nebelieka arba jų nebelieka tokia forma, kad duomenų valdytojas juos galėtų naudoti. „Sugadinimas“ taip pat yra pakankamai aiški sąvoka: tai situacija, kai asmens duomenys pakeičiami, iškraipomi arba dalis duomenų dingsta. Asmens duomenų „praradimas“ turėtų būti suprantamas kaip situacija, kai duomenys galbūt tebėra, tačiau duomenų valdytojas jų nebevaldo, netenka prieigos prie jų arba nebegali jais disponuoti. Ir galiausiai dėl duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo pažymėtina, kad tai reiškia asmens duomenų atskleidimą (arba prieigos prie duomenų suteikimą) duomenų gavėjams, kurie neturi leidimo gauti (arba prieiti prie) duomenų arba duomenų tvarkymą bet kokia kita forma, kuria pažeidžiamas BDAR.

Pavyzdys

[13] Žr. BDAR 5 straipsnio 1 dalies f punktą ir 32 straipsnį.
[14] 32 straipsnis; taip pat žr. BDAR 83 konstatuojamąją dalį.
[15] Žr. BDAR 87 konstatuojamąją dalį.

Asmens duomenų praradimo pavyzdys gali būti atvejis, kai pametamas arba pavagiamas įrenginys, kuriame yra duomenų valdytojo klientų duomenų bazės kopija. Kitas praradimo pavyzdys gali būti atvejis, kai vienintelė asmens duomenų kopija užšifruojama naudojant išpirkos reikalaujančią programą arba kai duomenų valdytojas praranda raktą, kuriuo jis užšifravo vienintelę asmens duomenų kopiją.

15. Reikėtų aiškiai suvokti, kad pažeidimas yra saugumo incidento rūšis. Tačiau, kaip nurodyta 4 straipsnio 12 dalyje, BDAR taikomas tik tokiu atveju, kai pažeidimas yra susijęs su asmens duomenimis. Tokio pažeidimo pasekmė yra ta, kad duomenų valdytojas negalės užtikrinti atitikties BDAR 5 straipsnyje nustatytiems asmens duomenų tvarkymo principams. Iš to aiškiai matyti, kuo saugumo incidentas skiriasi nuo asmens duomenų saugumo pažeidimo: iš esmės, nors visi asmens duomenų saugumo pažeidimai yra saugumo incidentai, ne visi saugumo incidentai būtinai yra asmens duomenų saugumo pažeidimai[16].

16. Toliau aptariami galimi neigiami pažeidimų padariniai asmenims.

2. Asmens duomenų saugumo pažeidimų rūšys

17. Nuomonėje 03/2014 dėl pranešimo apie pažeidimą 29 straipsnio darbo grupė paaiškino, kad pažeidimai gali būti skirstomi pagal šiuos gerai žinomus informacijos saugumo principus[17]:

- **konfidencialumo pažeidimas** – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie asmens duomenų suteikimas;
- **vientisumo pažeidimas** – neleistinas arba netyčinis asmens duomenų pakeitimas;
- **prieinamumo pažeidimas** – netyčinis arba neleistinas prieigos [18] prie asmens duomenų praradimas arba asmens duomenų sunaikinimas.

18. Taip pat reikėtų pažymėti, kad, atsižvelgiant į aplinkybes, pažeidimas vienu metu gali būti susijęs su asmens duomenų konfidencialumu, vientisumu ir prieinamumu prie asmens duomenų, taip pat su bet kokiu šių savybių deriniu.

19. Nustatyti, ar buvo padarytas konfidencialumo arba vientisumo pažeidimas, yra palyginti nesunku, tačiau prieinamumo pažeidimai nėra tokie akivaizdūs. Prieinamumo pažeidimais visada laikomi tokie pažeidimai, kai asmens duomenys negrąžinamai prarandami arba sunaikinami.

Pavyzdys

Prieinamumo praradimo pavyzdžiai yra atvejai, kai duomenys panaikinami netyčia arba kai juos panaikina neįgaliotas tai daryti asmuo, arba, kalbant apie saugiai užšifruotus duomenis, atvejis, kai

[16] Reikėtų pažymėti, kad saugumo incidentai gali būti susiję ne tik su tokiais grėsmių modeliais, kai organizacija atakuojama iš išorės, bet taip pat apima incidentus, susijusius su duomenų tvarkymu organizacijos viduje pažeidžiant saugumo principus.

[17] Žr. 29 straipsnio darbo grupės nuomonę 03/2014.

[18] Visuotinai pripažįstama, kad prieiga yra esminis prieinamumo aspektas. Pavyzdžiui., žr. NIST SP80053 (4 red.), kurioje prieinamumas apibrėžtas taip: „patikimos galimybės gauti informaciją ir ja naudotis užtikrinimas tinkamu laiku“, skelbiama šiuo interneto adresu: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 taip pat minima „leidimą turinčio subjekto galimybė laiku ir patikimai gauti duomenis ir naudotis informacinėmis paslaugomis“. Žr. https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf. Standarte ISO/IEC 27000:2016 prieinamumas taip pat apibrėžtas kaip „galimybė leidimą turinčiam subjektui pateikus prašymą gauti informaciją ir ja naudotis“: https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:en

prarandamas iššifravimo raktas. Jei duomenų valdytojas negali atkurti prieigos prie duomenų, pvz., pasinaudodamas atsargine kopija, tai laikoma negrąžinamu prieinamumo praradimu.

Prieinamumas taip pat gali būti prarandamas, kai iš esmės sutrinka įprastas organizacijos paslaugų teikimas, pvz., nutrūksta elektros energijos tiekimui arba įvykdoma aptarnavimo perkrovos ataka ir dėl to asmens duomenys tampa neprieinami.

20. Gali kilti klausimas, ar laikinas asmens duomenų prieinamumo praradimas turėtų būti laikomas pažeidimu, o jei taip, ar apie jį reikia pranešti. BDAR 32 straipsnyje „Duomenų tvarkymo saugumas“ paaiškinta, kad įgyvendinant technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, be kitų dalykų, turėtų būti atsižvelgiama į *„gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą“* ir *„gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“*.

21. Taigi saugumo incidentas, dėl kurio asmens duomenys tam tikrą laiką tampa neprieinami, taip pat yra tam tikros rūšies pažeidimas, nes dėl prieigos prie duomenų nebuvimo gali būti padarytas didelis poveikis fizinių asmenų teisėms ir laisvėms. Aiškumo sumetimais pažymėtina, kad tuo atveju, kai asmens duomenys yra neprieinami dėl atliekamų numatytų sistemos techninės priežiūros darbų, tai nėra laikoma „saugumo pažeidimu“, kaip apibrėžta BDAR 4 straipsnio 12 dalyje.

22. Kaip ir negrąžinamo asmens duomenų praradimo arba sunaikinimo atveju (o išties – bet kokios rūšies pažeidimo atveju), pažeidimas, susijęs su laikinu prieinamumo praradimu, turėtų būti patvirtinamas dokumentais, kaip nustatyta BDAR 33 straipsnio 5 dalyje. Tai leidžia duomenų valdytojui patvirtinti atskaitomybę priežiūros institucijai, kuri gali paprašyti susipažinti su tais įrašais[19]. Tačiau atsižvelgdama į pažeidimo aplinkybes ji gali reikalauti pranešti priežiūros institucijai ir informuoti paveiktus asmenis arba to nedaryti. Duomenų valdytojui reikės įvertinti poveikio fizinių asmenų teisėms ir laisvėms, kuris gali būti padarytas dėl neprieinamumo prie asmens duomenų, tikimybę ir rimtumą. Pagal BDAR 33 straipsnį duomenų valdytojas turės pranešti apie pažeidimą, nebent dėl pažeidimo neturėtų kilti pavojaus asmenų teisėms ir laisvėms. Žinoma, tai, ar reikia pranešti, kiekvienu konkrečiu atveju įvertinama atskirai.

Pavyzdys

Jei ligoninei nebus prieinami – nors ir laikinai – svarbūs medicininiai duomenys apie pacientus, gali kiti pavojus asmenų teisėms ir laisvėms; pavyzdžiui, gali būti atšauktos operacijos ir kilti grėsmė žmonių gyvybei.

Ir atvirkščiai – jei kelias valandas neveiks (pvz., dėl elektros energijos nutrūkimo) žiniasklaidos bendrovės sistemos ir dėl to bendrovė negalės išsiųsti naujienlaiškių savo prenumeratoriams, pavojaus asmenų teisėms ir laisvėms veikiausiai nekils.

23. Reikėtų pažymėti, kad nors duomenų valdytojo sistemų prieinamumo praradimas gali būti tik laikinas ir nepadaryti poveikio asmenims, svarbu, kad duomenų valdytojas apsvarstytų visas galimas pažeidimo pasekmes, nes jam gali reikėti apie jį pranešti dėl kitų priežasčių.

Pavyzdys

Užsikrėtus išpirkos reikalaujančia programa (kenkimo programine įranga, kuri užšifruoja duomenų valdytojo duomenis ir jų neiššifruoja, kol nesumokama išpirka), prieinamumo praradimas gali būti laikinas, jei duomenis galima atkurti pasinaudojant atsargine kopija. Tačiau į tinklą jau buvo įsibrauta,

[19] Žr. BDAR 33 straipsnio 5 punktą.

todėl, jei incidentas laikomas konfidencialumo pažeidimu (t. y. įsilaužėlis gavo asmens duomenis) ir dėl to kyla pavojus asmenų teisėms ir laisvėms, gali reikėti pranešti apie tokį pažeidimą.

3. Galimos asmens duomenų saugumo pažeidimo pasekmės

24. Pažeidimas gali padaryti įvairų didelį neigiamą poveikį asmenims, dėl kurio gali būti padarytas kūno sužalojimas, materialinė arba nematerialinė žala. BDAR paaiškinta, kad dėl tokio pažeidimo gali būti prarasta savo asmens duomenų kontrolė, apribotos asmens teisės, kilti diskriminacija, būti pavogta ar suklastota tapatybė, būti padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas. Be to, tiems asmenims gali būti padaryta kitokia didelė ekonominė ar socialinė žala[20].

25. Be to, BDAR reikalaujama, kad duomenų valdytojas apie pažeidimą praneštų priežiūros institucijai, nebent pažeidimas neturėtų kelti pavojaus, kad bus padarytas toks neigiamas poveikis. BDAR reikalaujama, kad tuo atveju, kai tikėtina, kad kils didelis tokio neigiamo poveikio pavojus, duomenų valdytojas apie pažeidimą kaip galėdamas anksčiau praneštų asmenims, kuriems tas pažeidimas turi poveikio[21].

26. Bendrojo duomenų apsaugos reglamento 87 konstatuojamojoje dalyje pabrėžiama, kaip svarbu sugebėti nustatyti pažeidimą, įvertinti jo keliamą pavojų asmenis ir tuomet prireikus apie jį pranešti:

> *„turėtų būti įsitikinta, ar įgyvendintos visos tinkamos technologinės apsaugos ir organizacinės priemonės, kad nedelsiant būtų nustatyta, ar buvo padarytas asmens duomenų saugumo pažeidimas, ir skubiai apie tai būtų informuoti priežiūros institucija ir duomenų subjektas. Turėtų būti nustatytas faktas, kad pranešimas buvo pateiktas nepagrįstai nedelsiant, atsižvelgiant visų pirma į asmens duomenų saugumo pažeidimo pobūdį ir sunkumą, jo pasekmes ir neigiamą poveikį duomenų subjektui. Dėl tokio pranešimo priežiūros institucija gali imtis intervencinių veiksmų vykdydama šiame reglamente nustatytas užduotis ir įgaliojimus.“*

27. Išsamesnės neigiamo poveikio asmenims vertinimo gairės pateiktos IV skyriuje.

28. Jei duomenų valdytojai nepraneša priežiūros institucijai ir (arba) duomenų subjektams apie duomenų saugumo pažeidimą, net jei ir įvykdomi BDAR 33 ir (arba) 34 straipsnio reikalavimai, priežiūros institucijai suteikiama galimybė pasirinkti, kurią iš visų taisomųjų priemonių, kurių ji įgaliota imtis, įskaitant atitinkamos administracinės baudos skyrimą[22] kartu su kuria nors kita 58 straipsnio 2 dalyje nustatyta taisomąja priemone arba be jos, taikyti. Jei pasirenkama skirti administracinę baudą, jos dydis gali būti iki 10 000 000 EUR arba iki 2 proc. įmonės bendros metinės pasaulinės apyvartos, kaip nustatyta BDAR 83 straipsnio 4 dalies a punkte. Taip pat svarbu atminti, kad kai kuriais atvejais tai, jog nepranešta apie pažeidimą, gali reikšti, kad nėra įgyvendinta jokių saugumo priemonių arba kad jos yra netinkamos. 29 straipsnio darbo grupės išleistose administracinių baudų nustatymo ir taikymo gairėse nurodyta: *„jeigu konkrečiu atveju yra kartu padaryti keli skirtingi pažeidimai, priežiūros institucija gali veiksmingai, proporcingai ir atgrasomai skirti administracines baudas, numatytas už sunkiausią pažeidimą“.* Tokiu atveju priežiūros institucija taip pat galės taikyti sankcijas už, viena, nepranešimą arba neinformavimą apie pažeidimą (BDAR 33 ir 34 straipsniai) ir, antra, už (tinkamų) saugumo priemonių netaikymą (BDAR 32 straipsnis), nes tai yra du skirtingi pažeidimai.

---

[20] Taip pat žr. 85 ir 75 konstatuojamąsias dalis.

[21] Taip pat žr. BDAR 86 konstatuojamąją dalį.

[22] Išsamesnės informacijos pateikta 29 straipsnio darbo grupės išleistose administracinių baudų taikymo ir nustatymo gairėse, skelbiamose šiuo interneto adresu: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

II. 33 STRAIPSNIS. PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI

A. Kada pranešti

1. 33 straipsnio reikalavimai

29. BDAR 33 straipsnio 1 dalyje nustatyta:

> *„Asmens duomenų saugumo pažeidimo atveju duomenų valdytojas nepagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai jis sužino apie asmens duomenų saugumo pažeidimą, apie tai praneša priežiūros institucijai, kuri yra kompetentinga pagal 55 straipsnį, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Jeigu priežiūros institucijai apie asmens duomenų saugumo pažeidimą nepranešama per 72 valandas, prie pranešimo pridedamos vėlavimo priežastys.“*

30. BDAR 87 konstatuojamojoje dalyje nustatyta[23]:

> *„turėtų būti įsitikinta, ar įgyvendintos visos tinkamos technologinės apsaugos ir organizacinės priemonės, kad nedelsiant būtų nustatyta, ar buvo padarytas asmens duomenų saugumo pažeidimas, ir skubiai apie tai būtų informuoti priežiūros institucija ir duomenų subjektas. Turėtų būti nustatytas faktas, kad pranešimas buvo pateiktas nepagrįstai nedelsiant, atsižvelgiant visų pirma į asmens duomenų saugumo pažeidimo pobūdį ir sunkumą, jo pasekmes ir neigiamą poveikį duomenų subjektui. Dėl tokio pranešimo priežiūros institucija gali imtis intervencinių veiksmų vykdydama šiame reglamente nustatytas užduotis ir įgaliojimus.“*

2. Kada duomenų valdytojas „sužino“ (apie pažeidimą)?

31. Kaip jau minėta, Bendrajame duomenų apsaugos reglamente reikalaujama, kad duomenų valdytojas apie pažeidimą praneštų nepagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip per 72 valandoms nuo tada, kai apie jį sužinojo. Gali kilti klausimas, kada galima laikyti, kad duomenų valdytojas sužinojo apie pažeidimą. EDAV nuomone, duomenų valdytojas turėtų būti laikomas žinančiu apie pažeidimą, kai jis pakankamai patikimai įsitikina, kad įvyko saugumo incidentas, dėl kurio kilo pavojus asmens duomenų saugumui.

32. Tačiau, kaip nurodyta pirmiau, BDAR reikalaujama, kad duomenų valdytojas įgyvendintų visas technines apsaugos ir organizacines priemones, kad nedelsdamas nustatytų, ar buvo padarytas pažeidimas, ir skubiai informuotų priežiūros instituciją ir duomenų subjektus. Be to, jame teigiama, kad turėtų būti nustatytas faktas, kad pranešimas buvo pateiktas nepagrįstai nedelsiant, atsižvelgiant visų pirma į pažeidimo pobūdį ir sunkumą, jo pasekmes ir neigiamą poveikį duomenų subjektui[24]. Taip duomenų valdytojas įpareigojamas laiku sužinoti apie bet kokius pažeidimus, kad galėtų imtis atitinkamų veiksmų.

33. Tikslus momentas, kada duomenų valdytojas gali būti laikomas žinančiu apie tam tikrą pažeidimą, priklausys nuo konkretaus pažeidimo aplinkybių. Kai kuriais atvejais jau iš pradžių bus gana aišku, kad buvo padarytas pažeidimas, o kartais gali praeiti šiek tiek laiko, kol bus galima nustatyti, ar kilo pavojus asmens duomenų saugumui. Tačiau svarbiausia, kad būtų imamasi skubių veiksmų, kad incidentas būtų ištirtas ir būtų nustatyta, ar iš tikrųjų buvo padarytas asmens duomenų saugumo pažeidimas, ir, jeigu jis buvo padarytas, kad būtų imtasi taisomųjų veiksmų bei prireikus pranešta apie pažeidimą.

Pavyzdžiai

[23] Šiuo atžvilgiu taip pat svarbi 85 konstatuojamoji dalis.

[24] Žr. BDAR 87 konstatuojamąją dalį.

1. Pametus USB raktą su neužšifruotais asmens duomenimis, dažnai neįmanoma įsitikinti, ar neįgalioti asmenys įgijo prieigą prie tų duomenų. Nepaisant to, net jei duomenų valdytojas ir negali nustatyti, ar buvo padarytas konfidencialumo pažeidimas, apie atvejį turi būti pranešta, nes galima pakankamai patikimai teigti, kad buvo padarytas prieinamumo pažeidimas; tokiu atveju duomenų valdytojas sužino apie pažeidimą, kai pametamas USB raktas.

2. Trečioji šalis informuoja duomenų valdytoją, kad atsitiktinai gavo vieno iš savo klientų asmens duomenis, ir pateikia neleistino atskleidimo įrodymus. Kadangi duomenų valdytojui buvo pateikti aiškūs konfidencialumo pažeidimo įrodymai, nekyla abejonių, kad jis sužinojo apie pažeidimą.

3. Duomenų valdytojas nustato, kad galėjo būti įsibrauta į jo tinklą. Duomenų valdytojas patikrina savo sistemas, siekdamas nustatyti, ar kilo pavojus toje sistemoje laikomų duomenų saugumui ir, jei taip, tai patvirtina. Šiuo atveju duomenų valdytojas taip pat jau turi aiškius pažeidimo įrodymus, todėl nekyla abejonių, kad jis sužinojo apie pažeidimą.

4. Kibernetinis nusikaltėlis, įsilaužęs į duomenų valdytojo sistemą, susisiekia su duomenų valdytoju, norėdamas pareikalauti išpirkos. Tokiu atveju, duomenų valdytojas, patikrinęs savo sistemą, jog įsitikintų, kad jos atžvilgiu buvo įvykdyta ataka, gauna aiškių įrodymų, kad buvo padarytas pažeidimas, dėl to nekyla abejonių, kad jis sužinojo apie pažeidimą.

34. Duomenų valdytojas, asmens, žiniasklaidos organizacijos ar kito šaltinio informuotas apie galimą pažeidimą arba pats nustatęs saugumo incidentą, gali atlikti trumpą tyrimą, kad nustatytų, ar pažeidimas iš tikrųjų buvo padarytas. Šio tyrimo laikotarpiu valdytojas negali būti laikomas žinančiu apie pažeidimą. Tačiau, tikimasi, kad kuo skubiau bus pradėtas pirminis tyrimas ir pakankamai patikimai nustatyta, ar buvo padarytas pažeidimas; tada gali būti atliekamas išsamesnis tyrimas.

35. Duomenų valdytojui sužinojus apie pažeidimą, apie kurį turi būti pranešta, apie jį turi būti pranešta nepagrįstai nedelsiant, o jei įmanoma, ne vėliau kaip per 72 valandas. Per šį laikotarpį duomenų valdytojas turėtų įvertinti galimą pavojų asmenims, kad nustatytų, ar turi būti vykdomas reikalavimas pranešti, taip pat veiksmą (-us), reikalingą (-us) pažeidimui pašalinti. Tačiau duomenų valdytojas gali būti jau atlikęs pirminį pavojaus, kuris gali kilti dėl pažeidimo, vertinimą[25], kai, prieš atlikdamas susijusią duomenų tvarkymo operaciją, atliko poveikio duomenų apsaugai vertinimą. Tačiau poveikio duomenų apsaugai vertinimas gali būti gana bendro pobūdžio, palyginti su konkrečiomis kokio nors faktinio pažeidimo aplinkybėmis, todėl bet kokiu atveju reikės papildomo vertinimo, kurį atliekant būtų atsižvelgta į tas aplinkybes. Išsamesnė informacija apie pavojaus vertinimą pateikta IV skyriuje.

36. Daugeliu atvejų šie išankstiniai veiksmai turėtų būti baigti netrukus po to, kai buvo gautas pradinis pavojaus signalas (t. y. kai duomenų valdytojui arba duomenų tvarkytojui kilo įtarimas, kad įvyko saugumo incidentas, kuris gali būti susijęs su asmens duomenimis); ilgiau jie gali trukti tik išskirtiniais atvejais.

Pavyzdys

Asmuo informuoja duomenų valdytoją, kad nuo subjekto, kuris dedasi duomenų valdytoju, gavo el. laišką su savo asmens duomenimis, susijusiais su jo (tikrai) naudojama duomenų valdytojo paslauga, todėl mano, kad kilo pavojus duomenų valdytojo saugumui. Duomenų valdytojas atlieka trumpą tyrimą ir nustato, kad buvo įsibrauta į jo tinklą, ir randa neleistinos prieigos prie asmens duomenų įrodymų. Nuo to momento duomenų valdytojas laikomas „žinančiu“ apie pažeidimą ir privalo apie jį pranešti priežiūros institucijai, nebent tas pažeidimas neturėtų kelti pavojaus asmenų teisėms ir laisvėms. Duomenų valdytojas turės imtis atitinkamų taisomųjų veiksmų, kad pašalintų pažeidimą.

[25] Žr. 29 straipsnio darbo grupės išleistas poveikio duomenų apsaugai vertinimo (PDAV) gaires WP248, skelbiamas šiuo interneto adresu: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

37. Todėl duomenų valdytojas turi įgyvendinti vidaus procedūras, pagal kurias būtų galima nustatyti ir pašalinti pažeidimą. Pavyzdžiui, norėdamas rasti duomenų tvarkymo trūkumų, duomenų valdytojas arba duomenų tvarkytojas gali taikyti tam tikras technines priemones, pvz., duomenų srauto ir kompiuterinio žurnalo analizatorius, kuriomis, taikant kompiuterinio žurnalo duomenų koreliaciją, būtų galima nustatyti įvykius ir pavojaus signalus[26]. Svarbu, kad nustačius pažeidimą, apie jį būtų informuota atitinkama aukštesnio lygmens vadovybė, kad tą pažeidimą būtų galima pašalinti ir prireikus apie jį pranešti pagal 33 straipsnį ir, jei reikia, 34 straipsnį. Šios priemonės ir informavimo mechanizmai galėtų būti išsamiai aprašyti duomenų valdytojo incidentų valdymo planuose ir (arba) valdymo tvarkose. Taip duomenų valdytojui bus lengviau užtikrinti veiksmingą planavimą ir organizacijoje nustatyti funkcinę atsakomybę už pažeidimų valdymą bei nuspręsti, ar dėl incidento reikia imtis tolesnių veiksmų, o jei taip, taip kaip tai daryti.

38. Be to, duomenų valdytojas su duomenų tvarkytojais, kurių paslaugomis naudojasi, turi sudaryti susitarimus, kuriuose būtų nustatyta prievolė pranešti duomenų valdytojui apie kiekvieną pažeidimą (žr. toliau).

39. Nors duomenų valdytojai ir duomenų tvarkytojai privalo įgyvendinti tinkamas priemones, kuriomis būtų galima užtikrinti pažeidimų prevenciją, reaguoti į pažeidimus ir juos pašalinti, yra keletas praktiškų veiksmų, kurių turėtų būti imamasi visais atvejais.

    - Informacija apie visus su saugumu susijusius įvykius turėtų būti perduodama atsakingam asmeniui (-ims), kuriam (-iems) yra pavesta reaguoti į incidentus, nustatyti, ar buvo padarytas pažeidimas, ir įvertinti pavojų.
    - Paskui turėtų būti įvertintas pavojus, kuris kyla dėl pažeidimo (tikimybė, kad pavojaus nėra, kad pavojus yra arba kad kyla didelis pavojus), ir apie vertinimo rezultatus informuoti atitinkami organizacijos padaliniai.
    - Prireikus apie tai turėtų būti pranešama priežiūros institucijai ir galbūt informuojami asmenys, kuriems pažeidimas turi poveikio.
    - Tuo pat metu duomenų valdytojas turėtų imtis veiksmų, kad pažeidimas būtų sustabdytas ir būtų pašalinti jo padariniai. Išaiškinus pažeidimą, jis turėtų būti dokumentuojamas.

40. Taigi turėtų būti aišku, kad duomenų valdytojas, atsižvelgdamas į bet kokį pradinį pavojaus signalą, privalo imtis veiksmų ir nustatyti, ar pažeidimas išties buvo padarytas. Per šį trumpą laikotarpį galima atlikti tam tikrą tyrimą – duomenų valdytojas gali surinkti įrodymus ir kitą svarbią informaciją. Tačiau duomenų valdytojas, pakankamai patikimai nustatęs, kad pažeidimas buvo padarytas, ir atsižvelgdamas į tai, ar įvykdytos BDAR 33 straipsnio 1 dalyje nustatytos sąlygos, privalo nepagrįstai nedelsdamas, jei įmanoma, ne vėliau kaip po 72 valandų, apie jį pranešti priežiūros institucijai[27]. Jei duomenų valdytojas laiku nesiima veiksmų ir paaiškėja, kad pažeidimo nebuvo padaryta, tai gali būti laikoma reikalavimo pranešti pagal BDAR 33 straipsnį neįvykdymu.

41. BDAR 32 straipsnyje aiškiai nurodyta, kad duomenų valdytojas ir duomenų tvarkytojas turėtų įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas tinkamas asmens duomenų saugumo lygis: gebėjimas laiku nustatyti, pašalinti pažeidimą ir apie pranešti turėtų būti vertinami kaip esminiai šių priemonių aspektai.

---

[26] Reikėtų pažymėti, kad kompiuterinio žurnalo duomenys, pagal kuriuos lengviau patikrinti, pvz., ar duomenys yra saugomi, buvo pakeisti ar ištrinti, taip pat gali atitikti asmens duomenų, susijusių su asmeniu, inicijavusiu atitinkamą duomenų tvarkymo veiksmą, sąvoką.

[27] Žr. Reglamentą (EEB, Euratomas) Nr. 1182/71, nustatantį terminams, datoms ir laikotarpiams taikytinas taisykles, skelbiamą šiuo interneto adresu: http://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:31971R1182&from=EN

3. Bendri duomenų valdytojai

42. BDAR 26 straipsnyje kalbama apie bendrus duomenų valdytojus ir nurodoma, kad bendri duomenų valdytojai privalo išsiaiškinti atitinkamas savo prievoles, susijusias su BDAR laikymusi[28]. Tai reiškia, kad taip pat reikia nustatyti, kokia šalis bus atsakinga už BDAR 33 ir 34 straipsniuose nustatytų prievolių laikymąsi. EDAV rekomenduoja, kad bendrų duomenų valdytojų tarpusavio sutartimi įformintuose susitarimuose būtų nustatyta, kuris duomenų valdytojas imsis vadovaujančio vaidmens užtikrinant BDAR nustatytų prievolių pranešti apie pažeidimus laikymąsi arba prisiims atsakomybę už tai.

4. Duomenų tvarkytojo prievolės

43. Duomenų valdytojui paliekama bendra atsakomybė už asmens duomenų apsaugą, tačiau duomenų tvarkytojui tenka svarbus vaidmuo įgalinant duomenų valdytoją laikytis jam nustatytų prievolių; vienas iš jų – pranešti apie pažeidimus. Šiuo atžvilgiu pažymėtina, kad BDAR 28 straipsnio 3 dalyje nustatyta, jog duomenų tvarkytojo atliekamas duomenų tvarkymas turėtų būti reglamentuojamas sutartimi ar kitu teisės aktu. 28 straipsnio 3 dalies f punkte nustatyta, kad „sutartyje ar kitame teisės akte turi būti nustatoma, kad duomenų tvarkytojas padeda duomenų valdytojui užtikrinti 32–36 straipsniuose nustatytų prievolių laikymąsi, atsižvelgdamas į duomenų tvarkymo pobūdį ir duomenų tvarkytojo turimą informaciją“.

44. BDAR 33 straipsnio 2 dalyje aiškiai nurodyta, kad tuo atveju, jei duomenų valdytojas naudojasi duomenų tvarkytojo paslaugomis, duomenų tvarkytojas, sužinojęs apie asmens duomenų, kuriuos jis tvarko duomenų valdytojo vardu, saugumo pažeidimą, privalo nepagrįstai nedelsdamas apie tai pranešti duomenų valdytojui. Reikėtų pažymėti, kad duomenų tvarkytojas, prieš pranešdamas apie pažeidimą duomenų valdytojui, neprivalo iš pradžių įvertinti pavojaus, kuris kyla dėl pažeidimo; atlikti šį vertinimą privalo duomenų valdytojas, kai tik sužino apie pažeidimą. Duomenų tvarkytojas turi tik nustatyti, ar pažeidimas buvo padarytas, ir tada apie jį pranešti duomenų valdytojui. Duomenų tvarkytojo paslaugomis duomenų valdytojas naudojasi tam, kad pasiektų savo tikslus; todėl iš esmės turėtų būti laikoma, kad duomenų valdytojas sužino apie pažeidimą, kai jam apie jį praneša duomenų tvarkytojas. Duomenų tvarkytoją įpareigojant informuoti duomenų valdytoją, kuriam jis teikia paslaugas, duomenų valdytojui suteikiama galimybė pašalinti pažeidimą ir nustatyti, ar pagal 33 straipsnio 1 dalį apie jį reikia pranešti priežiūros institucijai ir pagal 34 straipsnio 1 dalį informuoti asmenis, kuriems pažeidimas turi poveikio. Be to, duomenų valdytojui gali reikėti ištirti pažeidimą, nes duomenų tvarkytojas gali nežinoti visų su nagrinėjamu atveju susijusių faktų, pvz., ar duomenų valdytojas tebeturi atsarginę sunaikintų arba duomenų tvarkytojo prarastų asmens duomenų kopiją. Nuo to gali priklausyti, ar duomenų valdytojui paskui reikės pranešti apie pažeidimą.

45. BDAR nėra nustatyta konkretaus laikotarpio, per kurį duomenų tvarkytojas privalo perspėti duomenų valdytoją, išskyrus tai, kad jis tai turi padaryti „nepagrįstai nedelsdamas“. Todėl EDAV rekomenduoja, kad duomenų tvarkytojas nedelsdamas praneštų duomenų valdytojui apie pažeidimą, o papildomą informaciją apie pažeidimą teiktų etapais, kai turės daugiau išsamių duomenų. Tai svarbu norint padėti duomenų valdytojui įvykdyti reikalavimą per 72 valandas apie pažeidimą pranešti priežiūros institucijai.

46. Kaip paaiškinta pirmiau, duomenų valdytojo ir duomenų tvarkytojo tarpusavio sutartyje turėtų būti nurodyta, kaip, be kitų BDAR nuostatų, turėtų būti vykdomi 33 straipsnio 2 dalies reikalavimai. Šiuo tikslu gali būti nustatyti reikalavimai, kad duomenų tvarkytojas kuo anksčiau praneštų apie pažeidimą, o tai savo ruožtu turėtų padėti duomenų valdytojui įvykdyti prievoles per 72 valandas apie pažeidimą pranešti priežiūros institucijai.

47. Jei duomenų tvarkytojas teikia paslaugas daugiau nei vienam duomenų valdytojui ir tas pats incidentas turi poveikio visiems tiems duomenų valdytojams, duomenų tvarkytojas apie incidentą turės pranešti kiekvienam duomenų valdytojui.

---

[28] Taip pat žr. BDAR 79 konstatuojamąją dalį.

48. Jei duomenų valdytojas duomenų tvarkytojui yra suteikęs tinkamą įgaliojimą ir jis yra įtrauktas į duomenų valdytojo ir duomenų tvarkytojo tarpusavio sutartimi įformintus susitarimus, duomenų tvarkytojas gali teikti pranešimus duomenų valdytojo vardu. Tokie pranešimai turi būti teikiami pagal BDAR 33 ir 34 straipsnius. Tačiau svarbu pažymėti, kad teisinė atsakomybė už pranešimą vis vien tenka duomenų valdytojui.

B. Informacijos teikimas priežiūros institucijai

1. Teiktina informacija

49. Dėl pranešimo, kurį duomenų valdytojas teikia priežiūros institucijai, BDAR 33 straipsnio 3 dalyje nurodyta, kad tame pranešime turėtų būti pateikta bent tokia informacija:

> *„a) aprašytas asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jei įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;*
>
> (b) *nurodyta duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;*
>
> (c) *aprašomos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;*
>
> (d) *aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti“.*

50. Bendrajame duomenų apsaugos reglamente nėra apibrėžta duomenų subjektų ar asmens duomenų įrašų kategorijų. Tačiau EDAV siūlo duomenų subjektus skirstyti pagal įvairius asmenų, kuriems pažeidimas turi poveikio, tipus: atsižvelgiant į naudojamus požymius, tai, bet kita ko, galėtų būti vaikai ir kitos pažeidžiamos grupės, žmonės su negalia, darbuotojai arba klientai. Asmens duomenų kategorijos taip pat gali būti sudaromos pagal įvairias įrašų, kuriuos duomenų valdytojai gali tvarkyti, rūšis, pvz., sveikatos duomenys, švietimo įrašai, socialinės rūpybos informacija, finansinė informacija, banko sąskaitų numeriai, paso numeriai ir t. t.

51. BDAR 85 konstatuojamojoje dalyje aiškiai nurodyta, kad vienas iš pranešimo tikslų yra sumažinti asmenų patiriamą žalą. Taigi, jei iš duomenų subjektų arba asmens duomenų pobūdžio matyti, kad dėl pažeidimo kyla tam tikras pavojus (pvz., tapatybės vagystė, finansiniai nuostoliai, profesinės paslapties atskleidimo grėsmė), tuomet pranešime svarbu nurodyti šias kategorijas. Tai susiję su reikalavimu apibūdinti galimas pažeidimo pasekmes.

52. Jei tikslios informacijos (pvz., tikslaus duomenų subjektų, kuriems pažeidimas turi poveikio, skaičiaus) neturima, tai neturėtų būti kliūtis laiku pranešti apie pažeidimą. BDAR leidžiama nurodyti apytikslį asmenų, kuriems pažeidimas turi poveikio, arba susijusių asmens duomenų įrašų skaičių. Daugiausia dėmesio turėtų būti skiriama pažeidimo neigiamo poveikio šalinimui, o ne tikslių skaičių pateikimui.

53. Taigi, kai išsiaiškinama, kad buvo padarytas pažeidimas, tačiau jo mastas dar nėra žinomas, tinkamas būdas įvykdyti reikalavimus pranešti apie pažeidimą yra apie jį pranešti etapais (žr. toliau).

54. BDAR 33 straipsnio 3 dalyje teigiama, kad duomenų valdytojas duomenų valdytojo pranešime „turi būti bent“ tam tikra informacija, taigi, jei reikia, duomenų valdytojas gali nuspręsti pateikti išsamesnę informaciją. Skirtingo pobūdžio (konfidencialumo, vientisumo arba prieinamumo) pažeidimų atveju, norint išsamiai paaiškinti kiekvieno atvejo aplinkybes, gali reikėti pateikti papildomą informaciją.

> **Pavyzdys**
>
> Jei pagrindinė pažeidimo priežastis yra susijusi su duomenų tvarkytojo veikla, pirmiausia – jei jam tvarkant duomenis įvyko incidentas, turėjęs įtakos daugelio kitų duomenų valdytojų, kurie naudojasi

to paties duomenų tvarkytojo paslaugomis, valdomiems asmens duomenims, teikiant pranešimą priežiūros institucijai, duomenų valdytojui gali būti naudinga įvardyti savo duomenų tvarkytoją.

55. Bet kokiu atveju priežiūros institucija, tirdama pažeidimą, gali pareikalauti pateikti išsamesnę informaciją.

2. Pranešimas etapais

56. Atsižvelgiant į pažeidimo pobūdį, duomenų valdytojui gali reikėti atlikti tolesnį tyrimą, kad būtų nustatyti visi su incidentu susiję svarbūs faktai. Todėl BDAR 33 straipsnio 4 dalyje nustatyta:

> *„Kai ir jeigu informacijos neįmanoma pateikti tuo pačiu metu, informacija toliau nepagrįstai nedelsiant gali būti teikiama etapais.“*

57. Tai reiškia, kad Bendrajame duomenų apsaugos reglamente pripažįstama, jog duomenų valdytojai ne visada per 72 valandas nuo to momento, kai sužino apie pažeidimą, surinks visą reikiamą informaciją apie tą pažeidimą, nes šiuo pradiniu laikotarpiu ne visada gali būti prieinama visa išsami informacija apie incidentą. Todėl pranešimą leidžiama teikti etapais. Tikėtina, kad toks principas bus taikytinas sudėtingesnių pažeidimų atveju, pvz., kai kurių rūšių kibernetinio saugumo incidentų atveju, kai pvz., norint tiksliai nustatyti pažeidimo pobūdį ir duomenų saugumui kilusio pavojaus mastą, gali reikėti atlikti nuodugnią teisminę ekspertizę. Todėl duomenų valdytojui dažnai reikės atlikti išsamesnį tyrimą ir vėliau pateikti daugiau informacijos. Tai leistina, jei duomenų valdytojas nurodo vėlavimo priežastis, kaip nustatyta BDAR 33 straipsnio 1 dalyje. EDAV rekomenduoja, kad tuo atveju, jei duomenų valdytojas dar neturi visos reikiamos informacijos, jis, pirmą kartą informuodamas priežiūros instituciją, jai tai nurodytų ir informuotų, kad išsamesnę informaciją pateiks vėliau. Priežiūros institucija turėtų patvirtinti papildomos informacijos pateikimo būdą ir laiką. Tai nereiškia, kad duomenų valdytojas, gavęs svarbios papildomos svarbios informacijos apie pažeidimą, kuri turi būti pateikta priežiūros institucijai, jos negali pateikti kuriame nors vėlesniame etape.

58. Reikalavimu pranešti pirmiausia siekiama paskatinti duomenų valdytojus skubiai reaguoti į pažeidimą, jį sustabdyti ir, jei įmanoma, atkurti asmens duomenis, kurių saugumui kilo pavojus, taip pat kreiptis atitinkamo patarimo į priežiūros instituciją. Priežiūros institucijos informavimas per pirmąsias 72 valandas duomenų valdytojui gali suteikti galimybę įsitikinti, kad sprendimai dėl asmenų informavimo arba neinformavimo yra teisingi.

59. Tačiau pranešimo priežiūros institucijai tikslas yra ne tik išsiaiškinti, ar reikia informuoti asmenis, kuriems pažeidimas turi poveikio. Akivaizdu, kad kai kuriais atvejais, atsižvelgiant į pažeidimo pobūdį ir pavojaus rimtumą, duomenų valdytojui reikės nedelsiant informuoti asmenis, kuriems pažeidimas turi poveikio. Pavyzdžiui, jei kyla tiesioginė tapatybės vagystės grėsmė arba internete atskleidžiami tam tikrų kategorijų asmens duomenys[29], duomenų valdytojas turėtų nedelsdamas imtis veiksmų, kad sustabdytų pažeidimą ir apie jį praneštų susijusiems asmenims (žr. III skyrių). Išskirtinėmis aplinkybėmis tai netgi gali būti atliekama prieš pranešant priežiūros institucijai. Apskritai pažymėtina, jog tai, kad buvo pranešta priežiūros institucijai, negali būti pagrindas apie pažeidimą nepranešti duomenų subjektui, kai to reikia.

60. Be to, turėtų būti aišku, kad, pateikęs pradinį pranešimą ir per tolesnį tyrimą nustatęs, kad saugumo incidentas buvo suvaldytas ir iš tikrųjų nebuvo padaryta jokio pažeidimo, duomenų valdytojas gali pateikti priežiūros institucijai atnaujintą informaciją. Tuomet ši informacija galėtų būti pridėta prie informacijos, kuri jau buvo pateikta priežiūros institucijai, o incidentas atitinkamai galėtų būti užregistruotas ne kaip pažeidimas. Už pranešimą apie incidentą, kuris, kaip galiausiai paaiškėja, nėra pažeidimas, nebaudžiama.

[29] Žr. BDAR 9 straipsnį.

Pavyzdys

Duomenų valdytojas per 72 valandas nuo pažeidimo nustatymo praneša priežiūros institucijai, kad prarado USB raktą su kai kurių savo klientų asmens duomenų kopija. Vėliau USB raktas duomenų valdytojo patalpose randamas padėtas ne vietoje ir susigrąžinamas. Duomenų valdytojas pateikia priežiūros institucijai atnaujintą informaciją ir paprašo iš dalies pakeisti pranešimą.

61. Reikėtų pažymėti, kad pranešimo etapais principas jau buvo taikomas pagal galiojančius įpareigojimus, nustatytus Direktyvoje 2002/58/EB, Reglamente (ES) Nr. 611/2013, ir savanoriškai pranešant apie kitus incidentus.

3. Pavėluoti pranešimai

62. BDAR 33 straipsnio 1 dalyje aiškiai nurodyta, kad tuo atveju, jei priežiūros institucijai apie asmens duomenų saugumo pažeidimą pranešama vėliau nei po 72 valandų, teikiant pranešimą turi būti nurodytos vėlavimo priežastys. Šia nuostata, kartu taikant pranešimo etapais principą, pripažįstama, kad duomenų valdytojas ne visada gali turėti galimybę pranešti per minėtą laikotarpį ir kad pranešimas gali būti pateikiamas vėliau.

63. Pavyzdžiui, toks scenarijus galimas tada, kai per trumpą laiką duomenų valdytojas susiduria su daug panašių konfidencialumo pažeidimų, turinčių tokios pat įtakos daugybei duomenų subjektų. Gali būti, kad duomenų valdytojas, sužinojęs apie pažeidimą ir pradėjęs tyrimą, prieš pranešdamas apie pažeidimą, nustatys daugiau panašių pažeidimų, padarytų dėl skirtingų priežasčių. Atsižvelgiant į aplinkybes, duomenų valdytojui gali reikėti šiek tiek laiko pažeidimų apimčiai nustatyti, o vietoje atskiro pranešimo apie kiekvieną pažeidimą duomenų valdytojas gali parengti prasmingą pranešimą dėl kelių labai panašių pažeidimų, kurių priežastys gali būti skirtingos. Dėl to priežiūros institucijai gali būti pranešta vėliau nei per 72 valandas nuo to momento, kai duomenų valdytojas pirmą kartą sužino apie šiuos pažeidimus.

64. Iš principo būtina pranešti apie kiekvieną pažeidimą. Tačiau, siekdamas išvengti pernelyg didelės naštos, duomenų valdytojas gali pateikti vieną bendrą pranešimą apie visus šiuos pažeidimus, jei tie pažeidimai yra susiję su tokio pat pobūdžio asmens duomenimis, jų saugumas buvo pažeistas tokiu pat būdu ir per palyginti trumpą laikotarpį. Jei padaroma daug pažeidimų, susijusių su skirtingo pobūdžio asmens duomenimis, ir tų duomenų saugumas pažeidžiamas skirtingais būdais, pranešimas turėtų būti teikiamas įprastu būdu, t. y. pagal 33 straipsnį turi būti pranešama apie kiekvieną pranešimą.

65. Nors BDAR pranešimą leidžiama pateikti šiek tiek vėliau, nereikėtų suprasti, kad tai galima daryti nuolat. Verta pažymėti, kad bendri pranešimai taip pat gali būti rengiami dėl kelių ar daugiau panašių pažeidimų, apie kuriuos turi būti pranešama per 72 valandas.

C. Tarpvalstybiniai pažeidimai ir pažeidimai, padaryti ne ES buveinėse

1. Tarpvalstybiniai pažeidimai

66. Jei asmens duomenys tvarkomi tarpvalstybiniu mastu[30], pažeidimas gali turėti įtakos daugiau nei vienos valstybės narės duomenų subjektams. BDAR 33 straipsnio 1 dalyje aiškiai nurodyta, kad pažeidimo atveju duomenų valdytojas apie jį turėtų pranešti pagal BDAR 55 straipsnį kompetentingai priežiūros institucijai[31]. BDAR 55 straipsnio 1 dalyje nurodyta:

„Kiekviena priežiūros institucija turi kompetenciją savo valstybės narės teritorijoje vykdyti pagal šį reglamentą jai pavestas užduotis ir naudotis pagal šį reglamentą jai suteiktais įgaliojimais.“

[30] Žr. BDAR 4 straipsnio 23 punktą.

[31] Taip pat žr. BDAR 122 konstatuojamąją dalį.

67. Tačiau BDAR 56 straipsnio 1 dalyje nustatyta:

> *„Nedarant poveikio 55 straipsniui, duomenų valdytojo arba duomenų tvarkytojo pagrindinės buveinės arba vienintelės buveinės priežiūros institucija turi kompetenciją veikti kaip vadovaujanti priežiūros institucija, kai tas duomenų valdytojas arba duomenų tvarkytojas vykdo tarpvalstybinį duomenų tvarkymą, vadovaujantis 60 straipsnyje nustatyta procedūra.“*

68. Taip pat BDAR 56 straipsnio 6 dalyje nustatyta:

> *„Vadovaujanti priežiūros institucija yra vienintelė institucija, su kuria duomenų valdytojas arba duomenų tvarkytojas palaiko ryšius, kai jie vykdo tarpvalstybinį duomenų tvarkymą.“*

69. Tai reiškia, kad kaskart, kai padaromas su tarpvalstybiniu duomenų tvarkymu susijęs pažeidimas, apie kurį turi būti pranešta, duomenų valdytojas turės apie jį pranešti vadovaujančiai priežiūros institucijai[32]. Todėl, rengdamas reagavimo į pažeidimus planą, duomenų valdytojas privalo įvertinti, kokia priežiūros institucija yra vadovaujanti priežiūros institucija, kuriai jis turės teikti pranešimą[33]. Tai duomenų valdytojui suteiks galimybę skubiai reaguoti į pažeidimą ir įvykdyti 33 straipsnyje jam nustatytas prievoles. Reikėtų aiškiai suvokti, kad su tarpvalstybiniu duomenų tvarkymu susijusio pažeidimo atveju pranešimas turi būti teikiamas vadovaujančiai priežiūros institucijai, nebūtinai esančiai toje šalyje, kurioje yra duomenų subjektai, kuriems pažeidimas turi poveikio, arba kurioje iš tikrųjų buvo padarytas pažeidimas. Teikdamas pranešimą vadovaujančiai priežiūros institucijai, duomenų valdytojas prireikus turėtų nurodyti, ar pažeidimas apima buveines, esančias kitose valstybėse narėse, ir kokiose šalyse esantiems duomenų subjektams pažeidimas, tikėtina, turėjo poveikio. Jei duomenų valdytojui kyla abejonių dėl vadovaujančios priežiūros institucijos tapatybės, jis turėtų pateikti pranešimą bent jau tos vietos, kurioje buvo padarytas pažeidimas, priežiūros institucijai.

2. Pažeidimai, padaryti ne ES buveinėse

70. BDAR 3 straipsnyje nustatyta BDAR teritorinė taikymo sritis, įskaitant susijusią su atvejais, kai asmens duomenis tvarko ES neįsisteigęs duomenų valdytojas arba duomenų tvarkytojas. Visų pirma, BDAR 3 straipsnio 2 dalyje nustatyta[34]:

> *„Šis reglamentas taikomas asmens duomenų tvarkymui, kai Sąjungoje esančių duomenų subjektų asmens duomenis tvarko Sąjungoje neįsisteigęs duomenų valdytojas arba duomenų tvarkytojas ir duomenų tvarkymo veikla yra susijusi su:*
>
> (a) *prekių arba paslaugų siūlymu tokiems duomenų subjektams Sąjungoje, nepaisant to, ar už šias prekes arba paslaugas duomenų subjektui reikia mokėti; arba*
>
> (b) *elgesio, kai jie veikia Sąjungoje, stebėsena.“*

71. Šiuo atžvilgiu taip pat svarbi BDAR 3 straipsnio 3 dalis, kurioje nustatyta[35]:

> *„Šis reglamentas taikomas asmens duomenų tvarkymui, kai asmens duomenis tvarko duomenų valdytojas, įsisteigęs ne Sąjungoje, o vietoje, kurioje pagal viešąją tarptautinę teisę taikoma valstybės narės teisė.“*

---

[32] Žr. 29 straipsnio darbo grupės išleistas duomenų valdytojo ar duomenų tvarkytojo vadovaujančios priežiūros institucijos nustatymo gaires, skelbiamas šiuo interneto adresu: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[33] Visų Europos nacionalinių duomenų apsaugos institucijų kontaktinių duomenų sąrašas skelbiamas čia: https://www.edpb.europa.eu/about-edpb/about-edpb/members_lt

[34] Taip pat žr. 23 ir 24 konstatuojamąsias dalis.

[35] Taip pat žr. BDAR 25 konstatuojamąją dalį.

72. Jei ES neįsisteigusiam duomenų valdytojui taikoma BDAR 3 straipsnio 2 arba 3 dalis, pažeidimo atveju jam vis tiek taikomos BDAR 33 ir 34 straipsniuose nustatytos prievolės pranešti. BDAR 27 straipsnyje reikalaujama, kad tuo atveju, kai taikoma BDAR 3 straipsnio 2 dalis, duomenų valdytojas (ir duomenų tvarkytojas) paskirtų atstovą ES.

73. Tačiau vien dėl to, kad valstybėje narėje yra atstovas, vieno langelio sistema nepradedama taikyti[36]. Dėl šios priežasties apie pažeidimą turės būti pranešta visoms priežiūros institucijoms, kurių valstybėje narėje gyvena nukentėję duomenų subjektai. Už šį pranešimą (-us) atsako duomenų valdytojas[37].

74. Atitinkamai, jei BDAR 3 straipsnio 2 dalis taikoma duomenų tvarkytojui, jis privalo vykdyti duomenų tvarkytojams nustatytas prievoles, pirmiausia, šiuo atveju, – prievolę pagal BDAR 33 straipsnio 2 dalį apie pažeidimą pranešti duomenų valdytojui.

D. Sąlygos, kuriomis nebūtina pranešti apie pažeidimą

75. BDAR 33 straipsnio 1 dalyje aiškiai nurodyta, kad priežiūros institucijai nebūtina pranešti apie pažeidimus, kurie „neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms“. Tokio pažeidimo pavyzdys galėtų būti atvejis, kai asmens duomenys jau yra viešai prieinami ir jų atskleidimas neturėtų kelti pavojaus fizinių asmeniui. Tačiau pagal Direktyvą 2009/136/EB viešųjų elektroninių ryšių paslaugų teikėjams šiuo metu keliami kitokie reikalavimai pranešti apie pažeidimus – šioje direktyvoje reikalaujama, kad apie visus svarbius pažeidimus būtų pranešta kompetentingai institucijai.

76. Nuomonėje 03/2014 dėl pranešimo apie pažeidimą[38] 29 straipsnio darbo grupė paaiškino, kad asmens duomenų, kurie buvo užšifruoti pagal pažangų algoritmą, konfidencialumo pažeidimas vis vien yra asmens duomenų saugumo pažeidimas ir apie jį turi būti pranešta. Tačiau, jei rakto konfidencialumas nebuvo pažeistas, t. y. rakto atžvilgiu nebuvo padaryta jokio saugumo pažeidimo, ir jei raktas buvo sukurtas taip, kad prieigos teisės neturintis asmuo jo negalėtų nustatyti jokiomis prieinamomis techninėmis priemonėmis, tuomet galima teigti, kad duomenys iš esmės yra nesuprantami. Taigi pažeidimas neturėtų neigiamai paveikti asmenų, todėl apie pažeidimą tiems asmenims pranešti nereikės[39]. Tačiau, net jei duomenys yra užšifruoti, bet duomenų valdytojas neturi tinkamų atsarginių kopijų, tokių duomenų praradimas arba pakeitimas gali turėti neigiamų pasekmių duomenų subjektams. Tokiu atveju, net jei patys duomenys ir buvo tinkamai užšifruoti, reikėtų informuoti duomenų subjektus.

77. 29 straipsnio darbo grupė taip pat paaiškino, kad panašus atvejis būtų toks, kai asmens duomenys, pvz., slaptažodžiai, buvo patikimai užšifruoti maišos ir druskos įterpimo metodais, maišos būdu užšifruotoji vertė buvo apskaičiuota taikant pažangų šifravimo rakto naudojimu pagrįstą maišos funkciją, duomenims užšifruoti maišos metodu naudoto rakto atžvilgiu nebuvo padaryta jokių pažeidimų ir tas raktas buvo sukurtas taip, kad joks asmuo, kuriam nėra suteikta prieiga prie to rakto, jo negalėtų nustatyti pasinaudodamas prieinamomis technologinėmis priemonėmis.

78. Taigi, jei asmens duomenys buvo padaryti iš esmės nesuprantami neįgaliotoms šalims ir jei yra kita arba atsarginė duomenų kopija, priežiūros institucijos gali nereikėti informuoti apie tinkamai užšifruotų

---

[36] Žr. 29 straipsnio darbo grupės išleistas duomenų valdytojo ar duomenų tvarkytojo vadovaujančios priežiūros institucijos nustatymo gaires, skelbiamas šiuo interneto adresu: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[37] Vadovaudamasi gairėmis Nr. 3/2018 dėl BDAR teritorinės taikymo srities (3 straipsnis), kurias galima rasti adresu https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en, EDAV mano, kad atstovo Sąjungoje funkcija nesuderinama su išorės duomenų apsaugos pareigūno (DAP) vaidmeniu, todėl pareiga pranešti priežiūros institucijai apie asmens duomenų saugumo pažeidimą išlieka duomenų valdytojo pareiga pagal BDAR 27 straipsnio 5 dalį. Tačiau atstovas gali dalyvauti pranešimo procese, jei tai aiškiai nurodyta rašytiniame įgaliojime.

[38] Žr. 29 straipsnio darbo grupės nuomonę 03/2014 dėl pranešimo pažeidimą http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf .

[39] Taip pat žr. Reglamento 611/2013 4 straipsnio 1 ir 2 dalis.

asmens duomenų konfidencialumo pažeidimą. Tai grindžiama tuo, kad toks pažeidimas neturėtų kelti pavojaus asmenų teisėms ir laisvėms. Žinoma, tai reiškia, kad asmens informuoti taip pat nereikės, nes tikėtina, kad didelio pavojaus nėra. Tačiau reikėtų atminti, kad nors tuo atveju, kai neturėtų kilti pavojaus asmenų teisėms ir laisvėms, iš pradžių gali ir nereikėti pranešti apie pažeidimą, po kurio laiko situacija gali pasikeisti ir pavojų reikėtų įvertinti iš naujo. Pavyzdžiui, jei vėliau nustatoma, kad kilo pavojus rakto saugumui arba kad šifravimo programinė įranga turi saugumo spragų, pranešimą vis vien gali reikėti pateikti.

79. Be to, reikėtų pažymėti, kad tuo atveju, jei pažeidimas padaromas tokiomis aplinkybėmis, kai nėra užšifruotų asmens duomenų atsarginių kopijų, laikoma, kad buvo padarytas prieinamumo pažeidimas, o dėl to gali kilti pavojų asmenis, taigi gali reikėti pranešti apie pažeidimą. Atitinkamai, jei padarius pažeidimą prarandami užšifruoti duomenys, net ir tuo atveju, kai yra asmens duomenų atsarginė kopija, atsižvelgiant į laiką, kurio reikės duomenims atkurti iš tos atsarginės kopijos, ir neprieinamumo poveikį asmenims, gali vis vien reikėti pranešti apie pažeidimą. BDAR 32 straipsnio 1 dalies c punkte nustatyta, kad *„svarbus saugumo veiksnys yra „gebėjimas laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“.*

Pavyzdys

Pažeidimo, apie kurį nereikėtų pranešti priežiūros institucijai, pavyzdys – duomenų valdytojo ir jo darbuotojų naudoto patikimai užšifruoto mobiliojo įrenginio praradimas. Jei duomenų valdytojas ir toliau saugiai kontroliuoja užšifravimo raktą ir nebuvo prarasta vienintelė asmens duomenų kopija, įsilaužėlis negalės pasinaudoti asmens duomenimis. Tai reiškia, kad dėl pažeidimo neturėtų kilti pavojaus aptariamų duomenų subjektų teisėms ir laisvėms. Vėliau paaiškėjus, kad kilo pavojus užšifravimo rakto saugumui arba kad šifravimo programinė įranga arba algoritmas turi saugumo spragų, pavojus fizinių asmenų teisėms ir laisvėms pasikeis ir tada jau reikės pranešti apie pažeidimą.

80. Tačiau, jei duomenų valdytojas nepraneš apie pažeidimą tokiu atveju, kai duomenys iš tikrųjų nebuvo patikimai užšifruoti, bus laikoma, kad BDAR 33 straipsnyje nustatyti reikalavimai nebuvo įvykdyti. Todėl, pasirinkdami šifravimo programinę įrangą, duomenų valdytojai turėtų atidžiai įvertinti jos kokybę ir tai, ar tinkamai įgyvendintas siūlomas šifravimas, taip pat suvokti, kokio lygio apsauga iš tiesų užtikrinama ir ar ji yra tinkama atsižvelgiant į kylančius pavojus. Be to, duomenų valdytojai turėtų susipažinti su jų naudojamo šifravimo produkto veikimo ypatumais. Pavyzdžiui, gali būti, kad įrenginys yra užšifruojamas, kai išjungiamas, o budėjimo būsenoje jis nėra užšifruotas. Kai kuriuose produktuose, kuriuos naudojamas šifravimas, yra numatytieji klavišai, kuriuos kiekvienas pirkėjas turi pakeisti, kad jie būtų veiksmingi. Be to, gali būti, kad šiuo metu, saugumo ekspertų nuomone, šifravimas yra tinkamas, tačiau po kelerių metų jis gali pasenti, taigi kyla klausimas, ar, naudojant tą produktą, duomenys bus pakankamai patikimai užšifruojami ir ar bus užtikrinama tinkamo lygio pasauga.

III. 34 STRAIPSNIS. PRANEŠIMAS DUOMENŲ SUBJEKTUI

A. Asmenų informavimas

81. Tam tikrais atvejais, be pranešimo priežiūros institucijai, duomenų valdytojas apie pažeidimą taip pat privalo informuoti asmenis, kuriems pažeidimas turi poveikio.

BDAR 34 straipsnio 1 dalyje nustatyta:

„Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, duomenų valdytojas nepagrįstai nedelsdamas praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui.“

82. Duomenų valdytojai turėtų atminti, kad apie pažeidimą privaloma pranešti priežiūros institucijai, nebent tas pažeidimas neturėtų kelti pavojaus asmenų teisėms ir laisvėms. Be to, jei dėl pažeidimo kyla

didelis pavojus asmenų teisėms ir laisvėms, apie jį taip pat turi būti informuojami asmenys. Todėl aplinkybių, kuriomis apie pažeidimą turi būti informuojami asmenys, yra nustatyta mažiau nei aplinkybių, kuriomis turi būti pranešama priežiūros institucijoms, taigi asmenis reikės informuoti ne apie visus pažeidimus, taip juos apsaugant nuo nereikalingo pranešimų pertekliaus.

83. Bendrajame duomenų apsaugos reglamente nustatyta, kad asmenims apie pažeidimą turėtų būti pranešama „nepagrįstai nedelsiant“, t. y. kuo skubiau. Pagrindinis pranešimo asmenims tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jie turėtų imtis, kad apsisaugotų[40]. Kaip jau minėta, atsižvelgiant į pažeidimo pobūdį ir keliamą pavojų, laiku pateikus pranešimą, asmenims bus lengviau imtis veiksmų norint apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

84. Šių gairių B priede pateiktas nebaigtinis pavyzdžių, kai dėl pažeidimo gali kilti didelis pavojus asmenims, ir atitinkamai atvejų, kai duomenų valdytojas turės pranešti apie pažeidimą asmenims, kuriems jis turi poveikio, sąrašas.

B. Teiktina informacija

85. BDAR 34 straipsnio 2 dalyje dėl pranešimo asmenims nustatyta:

> *„Šio straipsnio 1 dalyje nurodytame pranešime duomenų subjektui aiškia ir paprasta kalba aprašomas asmens duomenų saugumo pažeidimo pobūdis ir pateikiama bent 33 straipsnio 3 dalies b, c ir d punktuose nurodyta informacija ir priemonės.“*

86. Pagal šią nuostatą duomenų valdytojas turėtų pateikti bent šią informaciją:

- pažeidimo pobūdžio aprašymą;
- duomenų apsaugos pareigūno arba kito kontaktinio asmens vardą ir pavardę (pavadinimą) ir kontaktinius duomenis;
- tikėtinų pažeidimo pasekmių aprašymą taip pat
- priemonių, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas tas pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti, aprašymą.

87. Pavyzdžiui, dėl priemonių, taikytų siekiant pašalinti pažeidimą ir sumažinti galimą neigiamą jo poveikį, duomenų valdytojas galėtų nurodyti, kad, pranešęs apie pažeidimą atitinkamai priežiūros institucijai, jis gavo patarimų, kaip suvaldyti pažeidimą ir sumažinti jo poveikį. Prireikus duomenų valdytojas asmenims taip pat turėtų konkrečiai patarti, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių, pvz., jei kilo pavojus asmens prieigos duomenų saugumui, jie galėtų pakeisti savo slaptažodžius. Duomenų valdytojas taip pat gali nuspręsti pateikti daugiau informacijos nei šiuo atveju reikalaujama.

C. Susisiekimas su asmenimis

88. Apie atitinkamą pažeidimą duomenų subjektai, kuriems pažeidimas turi poveikio, iš principo turėtų būti informuojami tiesiogiai, nebent tam reikėtų neproporcingų pastangų. Tokiu atveju vietoj to turi būti paskelbiamas viešas pranešimas arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai (BDAR 34 straipsnio 3 dalies c punktas).

89. Duomenų subjektai apie pažeidimą turėtų būti informuojami specialiais pranešimais, kurie neturėtų būti siunčiami kartu su kita informacija, pvz., su reguliariai siunčiama naujausia aktualia informacija, informaciniais biuleteniais ar įprastais pranešimais. Tai padės užtikrinti, kad pranešimas apie pažeidimą būtų aiškus ir skaidrus.

[40] Taip pat žr. BDAR 86 konstatuojamąją dalį.

90. Skaidrių informavimo būdų pavyzdžiai yra tiesioginiai pranešimai (pvz., el. pašto pranešimai, SMS, tiesioginės žinutės), gerai matomos reklamjuostės, pašto pranešimai ir gerai matomi skelbimai spausdintinėje žiniasklaidoje. Vien tik pranešimo spaudai paskelbimas arba pranešimo pateikimas įmonės tinklaraštyje nėra veiksminga asmens informavimo apie pažeidimą priemonė. EDAV valdytojams rekomenduoja rinktis tokias priemones, kuriomis būtų užtikrinta didžiausia tikimybė, kad informacija pasieks visus asmenis, kuriems pažeidimas turi poveikio. Tai reiškia, kad, atsižvelgdamas į aplinkybes, duomenų valdytojas gali pasitelkti kelis informavimo būdus, o ne vieną ryšio kanalą.

91. Kad asmenys suprastų jiems pateiktą informaciją, duomenų valdytojams taip pat gali reikėti užtikrinti, kad su pranešimu būtų galima susipažinti tinkamais alternatyviais formatais ir atitinkamomis kalbomis. Pavyzdžiui, asmuo apie pažeidimą paprastai turėtų būti informuojamas ta kalba, kuria su duomenų gavėju anksčiau buvo palaikomas ryšys įprastais dalykiniais klausimais. Tačiau, jei pažeidimas turi poveikio duomenų subjektams, į kuriuos duomenų valdytojas anksčiau nebuvo kreipęsis, arba visų pirma duomenų subjektams, gyvenantiems ne toje pačioje valstybėje narėje arba ES nepriklausančioje šalyje, kurioje yra įsisteigęs duomenų valdytojas, atsižvelgiant į reikiamas lėšas, pranešimas gali būti teikiamas nacionaline kalba. Svarbiausia padėti duomenų subjektams suprasti pažeidimo pobūdį ir veiksmus, kurių jie gali imtis, norėdami apsisaugoti.

92. Duomenų valdytojai geriausiai žino, koks ryšio kanalas yra tinkamiausias asmenims informuoti apie pažeidimą, ypač jei jie dažnai palaiko ryšį su savo klientais. Be abejo, duomenų valdytojas turėtų atsargiai naudoti kanalą, kurio saugumas buvo pažeistas, nes juo taip pat gali pasinaudoti duomenų valdytoju apsimetę įsilaužėliai.

93. Be to, BDAR 86 konstatuojamojoje dalyje paaiškinta:

> *„Tokie pranešimai duomenų subjektams turėtų būti pateikti kuo greičiau ir glaudžiai bendradarbiaujant su priežiūros institucija, laikantis jos ar kitų atitinkamų valdžios institucijų, tokių kaip teisėsaugos institucijos, pateiktų nurodymų. Pavyzdžiui, siekiant sumažinti tiesioginį žalos pavojų, reikėtų nedelsiant apie tai pranešti duomenų subjektams, o ilgesnį pranešimo terminą būtų galima pateisinti būtinybe įgyvendinti tinkamas priemones, kuriomis siekiama užkirsti kelią besikartojantiems ar panašiems asmens duomenų saugumo pažeidimams.“*

94. Todėl duomenų valdytojams gali reikėti susisiekti ir pasitarti su priežiūros institucija ne tik tam, kad gautų patarimą dėl duomenų subjektų informavimo apie pažeidimą pagal 34 straipsnį, bet ir dėl to, kokius pranešimus derėtų nusiųsti asmenims ir kaip būtų tinkamiausia su jais susisiekti.

95. Šiuo atžvilgiu BDAR 88 konstatuojamojoje dalyje patariama, kad pranešant apie pažeidimą „reikėtų atsižvelgti į teisėtus teisėsaugos institucijų interesus, kai ankstyvas informacijos atskleidimas galėtų bereikalingai pakenkti asmens duomenų pažeidimo aplinkybių tyrimui“. Tai gali reikšti, kad tam tikromis aplinkybėmis, kai tai yra pagrįsta, duomenų valdytojas, pasitaręs su teisėsaugos institucijomis, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą apie pažeidimą iki to laiko, kai tai netrukdys tokiems tyrimams. Tačiau po to vis vien gali reikėti skubiai informuoti duomenų subjektus.

96. Jei duomenų valdytojas negali informuoti asmens apie pažeidimą, nes neturi pakankamai duomenų, kuriais remdamasi galėtų susisiekti su tuo asmeniu, tokiomis aplinkybėmis duomenų valdytojas tą asmenį turėtų informuoti iš karto, kai tik tai taps įmanoma (pvz., kai asmuo pasinaudos 15 straipsnyje jam suteikta teise susipažinti su asmens duomenimis ir pateiks duomenų valdytojui reikiamą papildomą informaciją, kuria remiantis su juos bus galima susisiekti).

D. Sąlygos, kuriomis nebūtina informuoti apie pažeidimą

97. BDAR 34 straipsnio 3 dalyje nustatytos trys sąlygos, kurias įvykdžius, asmenims nebūtina pranešti apie pažeidimą. Tai:

    - duomenų valdytojas taikė tinkamas technines ir organizacines priemones, kad apsaugotų asmens duomenis, kol dar nebuvo padarytas pažeidimas, visų pirma tas priemones, kuriomis

užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami. Pavyzdžiui, asmens duomenų apsauga gali būti užtikrinama taikant pažangų šifravimą arba naudojant prieigos raktus;

- iškart po pažeidimo duomenų valdytojas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms. Pavyzdžiui, atsižvelgiant į konkretaus atvejo aplinkybes, duomenų valdytojas galėjo skubiai nustatyti ir imtis veiksmų prieš asmenį, kuris gavo asmens duomenis, kol šis su jais dar nieko nespėjo nuveikti. Atsižvelgiant į susijusių duomenų pobūdį, taip pat būtina skirti pakankamai dėmesio konfidencialumo pažeidimų pasekmėms;
- susisiekimas su asmenimis pareikalautų neproporcingai daug pastangų [41], pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nėra žinomi. Pavyzdžiui, statistikos biuro sandėlis buvo užlietas, o dokumentai su asmens duomenimis buvo saugomi tik popierine forma. Vietoj tiesioginio asmenų informavimo duomenų valdytojas turi paskelbti viešą pranešimą arba taikyti panašią priemonę, kuria duomenų subjektai informuojami taip pat veiksmingai. Jei susisiekimas su asmenimis pareikalautų neproporcingai daug pastangų, taip pat galėtų būti numatytos techninės priemonės, kuriomis prireikus būtų informuojama apie pažeidimus; tai galėtų būti naudinga, kai pažeidimas galėjo turėti poveikio asmenims, su kuriais duomenų valdytojas negali kitaip susisiekti.

98. Pagal atskaitomybės principą duomenų valdytojai turėtų sugebėti įrodyti priežiūros institucijai, kad įvykdė vieną ar daugiau iš šių sąlygų[42]. Reikėtų atminti, kad nors tuo atveju, kai nekyla pavojaus fizinių asmenų teisėms ir laisvėms, iš pradžių gali ir nereikėti pranešti apie pažeidimą, po kurio laiko situacija gali pasikeisti ir tuomet pavojų reikėtų įvertinti iš naujo.

99. BDAR 34 straipsnio 4 dalyje paaiškinta, kad tuo atveju, kai duomenų valdytojas nusprendžia neinformuoti asmens apie pažeidimą, priežiūros institucija gali pareikalauti, kad jis tą padarytų, jei, jos nuomone, dėl pažeidimo gali kilti didelis pavojus asmenims. Kita vertus, ji gali nuspręsti, kad buvo įvykdytos BDAR 34 straipsnio 3 dalyje nustatytos sąlygos, o tokiu atveju pranešti asmenims nereikalaujama. Jei priežiūros institucija nustato, kad sprendimas nepranešti duomenų subjektams nėra tinkamai pagrįstas, ji gali nuspręsti pasinaudoti savo įgaliojimais ir taikyti numatytas sankcijas.

IV. PAVOJAUS VERTINIMAS IR DIDELIO PAVOJAUS NUSTATYMAS

A. Pavojus, kuriam esant reikia pranešti apie pažeidimą

100. Nors BDAR nustatyta prievolė pranešti apie pažeidimą, šis reikalavimas taikomas ne visomis aplinkybėmis:

- pranešti kompetentingai institucijai nebūtina, jei dėl pažeidimo neturėtų kilti pavojaus asmenų teisėms ir laisvėms;
- asmenį apie pažeidimą būtina informuoti tik tada, kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus to asmens teisėms ir laisvėms.

101. Tai reiškia, kad labai svarbu, jog duomenų valdytojas, tik sužinojęs apie pažeidimą, ne tik imtųsi priemonių incidentui suvaldyti, bet ir įvertintų pavojų, kuris gali kilti dėl to incidento. To reikia dėl dviejų priežasčių: pirma, žinant poveikio asmeniui tikimybę ir galimą rimtumą, duomenų valdytojui bus lengviau imtis veiksmingų priemonių pažeidimui sustabdyti ir pašalinti; antra, tai jam padės nustatyti, ar apie pažeidimą būtina pranešti priežiūros institucijai ir, jei reikia, susijusiems asmenims.

---

[41] Neproporcingų pastangų klausimu žr. 29 straipsnio darbo grupės išleistas skaidrumo užtikrinimo gaires, skelbiamas šiuo interneto adresu: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[42] Žr. BDAR 5 straipsnio 2 punktą.

102. Kaip paaiškinta pirmiau, pranešti apie pažeidimą yra būtina, išskyrus atvejus, kai dėl jo neturėtų kilti pavojaus asmenų teisėms bei laisvėms, o pagrindinis kriterijus, kuriuo remiantis nustatoma, ar apie pažeidimą reikia informuoti duomenų subjektus, yra tai, ar dėl pažeidimo gali kilti didelis pavojus asmenų teisėms ir laisvėms. Toks pavojus kyla tuomet, kai dėl pažeidimo asmenys, kurių duomenų saugumas buvo pažeistas, gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą. Tokios žalos pavyzdžiai yra diskriminacija, tapatybės vagystė arba klastojimas, finansiniai nuostoliai ir pakenkimas reputacijai. Jei pažeidimas yra susijęs su asmens duomenimis, iš kurių galima sužinoti rasinę arba etninę kilmę, politines pažiūras, religinius arba filosofinius įsitikinimus arba priklausymą profesinei sąjungai, arba kuriuose yra genetinių duomenų, duomenų apie asmens sveikatą arba lytinį gyvenimą, apkaltinamuosius nuosprendžius ir nusikalstamas veikas arba susijusias apsaugos priemones, tikėtina, kad tokia žala bus padaryta[43].

B. Veiksniai, į kuriuos reikia atsižvelgti vertinant pavojų

103. Remiantis BDAR 75 ir 76 konstatuojamosiomis dalimis, vertinant pavojų paprastai reikėtų atsižvelgti į pavojaus duomenų subjektų teisėms ir laisvėms tikimybę ir rimtumą. Be to, jose teigiama, kad pavojus turėtų būti vertinamas remiantis objektyviu įvertinimu.

104. Reikėtų pažymėti, kad vertinant pavojų, kuris dėl pažeidimo kyla žmonių teisėms ir laisvėms, atsižvelgiama į kitus pavojus nei atliekant poveikio duomenų apsaugai vertinimą[44]. Atliekant poveikio duomenų apsaugai vertinimą, atsižvelgiama į pavojus, kylančius, kai duomenys tvarkomi taip, kaip buvo numatyta, ir į pavojus, kylančius pažeidimo atveju. Nagrinėjant galimą pažeidimą, bendrai įvertinama pažeidimo tikimybė ir žala, kurią dėl to pažeidimo gali patirti duomenų subjektas; kitaip tariant, vertinamas hipotetinis įvykis. Faktinio pažeidimo atveju tas įvykis jau yra įvykęs, todėl nagrinėjamas tik pavojus, kuris asmenims gali kilti dėl pažeidimo.

Pavyzdys

Iš poveikio duomenų apsaugai vertinimo matyti, kad tam tikras apsaugos programinės įrangos produktas, kurį siūloma naudoti asmens duomenims apsaugoti, yra tinkama priemonė siekiant užtikrinti saugumo lygį, atitinkantį duomenų tvarkymo pavojų, kuris kiltų asmenims, jei tokia priemonė nebūtų taikoma. Tačiau, vėliau sužinojus apie kokią nors saugumo spragą, programinės įrangos tinkamumas suvaldyti saugomiems asmens duomenimis gresiantį pavojų gali pasikeisti, todėl, atliekant tęstinį poveikio duomenų apsaugai vertinimą, tą programinę įrangą reikės įvertinti iš naujo. Vėliau pasinaudojama produkto saugumo spraga ir padaromas pažeidimas. Duomenų valdytojas turėtų įvertinti konkrečias pažeidimo aplinkybes, duomenis, kuriems tas pažeidimas turi poveikio, galimą poveikio asmenims lygį ir tikimybę, kad pavojus taps realiu pažeidimu.

105. Taigi, vertindamas pavojų, kuris dėl pažeidimo kyla asmenims, duomenų valdytojas turėtų išnagrinėti konkrečias pažeidimo aplinkybes, įskaitant galimo poveikio rimtumą ir to poveikio padarymo tikimybę. Todėl EDAV rekomenduoja vertinant atsižvelgti į toliau nurodytus kriterijus[45].

- **Pažeidimo pobūdis**

106. Nuo padaryto pažeidimo pobūdžio gali priklausyti pavojaus, kuris kyla asmenims, dydis. Pavyzdžiui, konfidencialumo pažeidimas, padarytas medicininę informaciją atskleidus šalims, kurios

[43] Žr. BDAR 75 ir 85 konstatuojamąsias dalis.

[44] Žr. darbo grupės išleistas poveikio duomenų apsaugai vertinimo gaires, skelbiamas šiuo interneto adresu: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[45] Reglamento (ES) Nr. 611/2013 3 straipsnio 2 dalyje nurodyti veiksniai, į kuriuos reikėtų atsižvelgti pranešant apie pažeidimus elektroninių ryšių paslaugų sektoriuje; į šiuos veiksnius gali būti naudinga atsižvelgti ir teikiant pranešimus pagal BDAR. Žr. http://eur-http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:lt:PDF

neturi teisės gauti tokios informacijos, gali turėti skirtingų pasekmių asmeniui, kurio atžvilgiu buvo padarytas pažeidimas, kai asmens medicininiai duomenys prarandami ir jų nebelieka.

- **Asmens duomenų pobūdis, jautrumas ir kiekis**

107. Žinoma, vertinant pavojų, vienas iš pagrindinių veiksnių yra asmens duomenų, kurių saugumas buvo pažeistas, pobūdis ir jautrumas. Paprastai galioja taisyklė, kad kuo jautresni duomenys, tuo didesnės žalos pavojus kyla asmenims, kuriems pažeidimas turi poveikio, tačiau reikėtų atsižvelgti ir į kitus duomenų subjekto asmens duomenis, kurie jau gali būti prieinami. Pavyzdžiui, įprastomis aplinkybėmis atskleidus asmens vardą ir pavardę bei adresą, didelės žalos neturėtų būti padaryta. Tačiau, įtėvio arba įmotės vardo ir pavardės bei adreso atskleidimas biologiniam tėvui arba motinai gali turėti labai rimtų pasekmių tiek įtėviui arba įmotei, tiek vaikui.

108. Sveikatos duomenų, asmens tapatybės dokumentų arba finansinių duomenų, pvz., kredito kortelės duomenų, saugumo pažeidimai gali padaryti ne tik tiesioginės žalos, bet, naudojami kartu, taip pat gali padėti pavogti tapatybę. Įvairių asmens duomenų derinys paprastai yra jautresnio pobūdžio nei pavieniai asmens duomenys.

109. Kai kurių rūšių asmens duomenys iš pirmo žvilgsnio gali atrodyti negalintys padaryti žalos, tačiau reikėtų atidžiai apsvarstyti, ką iš tų duomenų galima sužinoti apie asmenį, kuriam pažeidimas turi poveikio. Reguliariai siuntas gaunančių klientų sąrašas gali neatrodyti labai jautraus pobūdžio, tačiau tie patys duomenys apie klientus, kurie paprašė, kad siuntos jiems laikinai nebūtų siunčiamos, nes jie atostogaus, gali būti naudinga informacija nusikaltėliams.

110. Nedidelis labai jautraus pobūdžio asmens duomenų kiekis taip pat gali turėti didelio poveikio asmeniui, o iš didelio įvairių duomenų rinkinio galima dar daugiau sužinoti apie tą asmenį. Be to, jei pažeidžiamas didelio kiekio asmens duomenų, susijusio su daugybe duomenų subjektų, saugumas, poveikis gali būti padarytas tokiam pat dideliam asmenų kiekiui.

- **Asmenų tapatybės nustatymo lengvumas**

111. Svarbus veiksnys, į kurį reikia atsižvelgti, yra tai, kaip kokiai nors šaliai, kuriai yra prieinami asmens duomenys, kurių saugumui kilo pavojus, bus lengva nustatyti konkrečių asmenų tapatybę arba tuo pačiu tikslu susieti tuos duomenis su kita informacija. Atsižvelgiant į aplinkybes, gali būti, kad asmens tapatybę bus galima nustatyti tiesiogiai remiantis asmens duomenimis, kurių saugumas buvo pažeistas, neatliekant jokio specialaus tyrimo asmens tapatybei atskleisti, arba gali būti, kad asmens duomenis susieti su konkrečiu asmeniu bus labai sunku, bet tam tikromis sąlygomis vis vien įmanoma. Nors, remiantis duomenimis, kurių saugumas buvo pažeistas, ir gali būti įmanoma tiesiogiai arba netiesiogiai nustatyti asmens tapatybę, tai taip pat gali priklausyti nuo konkrečių pažeidimo aplinkybių ir to, ar susiję asmens duomenys yra skelbiami viešai. Tai daugiau taikytina konfidencialumo ir prieinamumo pažeidimams.

112. Kaip jau minėta, tinkamu lygiu užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, neturintiems iššifravimo rakto. Be to, tinkamai įgyvendinus pseudonimų suteikimą (BDAR 4 straipsnio 5 dalyje jis apibrėžtas kaip *„asmens duomenų tvarkymas taip, kad asmens duomenys nebegalėtų būti priskirti konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jos atžvilgiu taikomos techninės bei organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti“*), taip pat galima sumažinti tikimybę, kad pažeidimo atveju bus nustatyta asmenų tapatybė. Tačiau vien pseudonimų suteikimo nepakanka, kad duomenys būtų nesuprantami.

- **Pasekmių rimtumas asmenims**

113. Atsižvelgiant į asmens duomenų, kurių saugumas buvo pažeistas, pobūdį, pvz., jei tai yra specialių kategorijų duomenys, galima žala asmenims gali būti labai didelė, pirmiausia, jei padarius

pažeidimą pavagiama arba suklastojama tapatybė, padaromas kūno sužalojimas, sukeliama psichologinė kančia, patiriamas pažeminimas arba pakenkiama reputacijai. Jei pažeidimas susijęs su pažeidžiamų asmenų asmens duomenimis, jiems gali kilti dar didesnis žalos pavojus.

114. Galimo pavojaus dydis priklauso nuo to, ar duomenų valdytojas žino, kad asmens duomenys yra žmonių, kurių ketinimai yra nežinomi arba galbūt piktavališki, rankose. Asmens duomenis per klaidą atskleidus trečiajai šaliai, kaip apibrėžta 4 straipsnio 10 dalyje, arba kitam duomenų gavėjui, gali būti padarytas konfidencialumo pažeidimas. Pavyzdžiui, taip gali atsitikti, kai asmens duomenys atsitiktinai nusiunčiami ne tam organizacijos padaliniui arba tiekėjo organizacijai, kurios paslaugomis dažnai naudojamasi. Duomenų valdytojas gali pareikalauti, kad duomenų gavėjas grąžintų arba patikimai sunaikintų gautus duomenis. Abiem atvejais, jei duomenų valdytojas nuolat palaiko ryšį su minėtu subjektu ir yra susipažinęs su jo procedūromis, istorija ir kita svarbia informacija, duomenų gavėjas gali būti laikomas patikimu. Kitaip tariant, duomenų gavėjas gali būti įgijęs tam tikrą duomenų valdytojo pasitikėjimą leidžiantį pagrįstai tikėtis, kad toji šalis nežiūrės per klaidą nusiųstų duomenų ar nepasinaudos prieiga prie jų ir laikysis duomenų valdytojo nurodymų dėl tų duomenų grąžinimo. Net jei bus pasinaudota prieiga prie duomenų, duomenų valdytojas vis vien galės tikėtis, kad duomenų gavėjas nesiims jokių papildomų veiksmų ir skubiai grąžins duomenis duomenų valdytojui, taip pat bendradarbiaus juos susigrąžinant. Tokiais atvejais į tai gali būti atsižvelgta per pavojų vertinimą, kurį duomenų valdytojas atlieka po pažeidimo: dėl to, kad duomenų gavėju galima pasitikėti, gali sumažėti pažeidimo pasekmių rimtumas, tačiau tai nereiškia, kad pažeidimas nebuvo padarytas. Tačiau dėl to savo ruožtu gali išnykti pavojaus asmenims tikimybė, todėl gali nebereikėti teikti pranešimo priežiūros institucijai arba asmenims, kuriems pažeidimas turi poveikio. Tai vėlgi priklausys nuo konkretaus atvejo. Nepaisant to, duomenų valdytojas, vykdydamas prievolę tvarkyti įrašus apie pažeidimus, vis tiek turi saugoti informaciją apie pažeidimą (žr. V skyrių).

115. Taip pat reikėtų atsižvelgti į pasekmių asmenims ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai ir jo poveikis veikiausiai bus didesnis.

- **Asmens specifiniai ypatumai**

116. Pažeidimas gali turėti poveikio asmens duomenims, susijusiems su vaikais arba kitais pažeidžiamais asmenimis, kuriems dėl pažeidimo gali kilti didesnė pavojaus rizika. Taip pat gali būti kitų su asmeniu susijusių veiksnių, galinčių turėti įtakos tam, koks poveikis asmeniui bus padarytas.

- **Duomenų valdytojo specifiniai ypatumai**

117. Duomenų valdytojo ir jo veiklos pobūdis bei reikšmė gali turėti įtakos pavojui, kuris dėl pažeidimo kyla asmenims. Pavyzdžiui, medicininės paslaugas teikianti organizacija numato tvarkyti specialių kategorijų asmens duomenis, taigi, pažeidus susijusių asmenų asmens duomenų saugumą, tiems asmenims kils didesnė grėsmė nei tuo atveju, kai pažeidimas bus susijęs su laikraščio gavėjų el. pašto adresų sąrašu.

- **Asmenų, kuriems pažeidimas turi poveikio, skaičius**

118. Pažeidimas gali turėti poveikio tik vienam ar keliems asmenims arba net keliems tūkstančiams ar dar daugiau asmenų. Paprastai galioja taisyklė, kad kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnį poveikį tas pažeidimas gali padaryti. Tačiau, atsižvelgiant į asmens duomenų pobūdį ir aplinkybes, kuriomis kilo pavojus tų duomenų saugumui, pažeidimas gali padaryti didelį poveikį net ir vienam asmeniui. Šiuo atveju taip pat svarbu įvertinti poveikio asmenims, kuriems pažeidimas turi poveikio, tikimybę ir rimtumą.

- **Bendrosios nuostatos**

119. Taigi, vertindamas pavojų, kuris dėl pažeidimo gali kilti asmenims, duomenų valdytojas turėtų bendrai atsižvelgti į galimo poveikio asmenų teisėms ir laisvėms rimtumą ir tikimybę, kad toks poveikis bus padarytas. Akivaizdu, kad kuo rimtesnės pažeidimo pasekmės, tuo didesnis kyla pavojus; be to,

pavojus didėja ir didėjant pažeidimo tikimybei. Kilus abejonių, duomenų valdytojas turėtų vadovautis atsargumo principu ir pranešti apie pažeidimą. B priede pateikta naudingų įvairaus pobūdžio pažeidimų, dėl kurių kyla pavojus (arba didelis pavojus) asmenims, pavyzdžių.

120. Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA) yra paskelbusi rekomendacijas dėl pažeidimo rimtumo vertinimo metodikos, kurios duomenų valdytojams ir duomenų tvarkytojams gali būti naudingos rengiant savo reagavimo į pažeidimus planus[46].

V. ATSKAITOMYBĖ IR ĮRAŠŲ SAUGOJIMAS

A. Pažeidimų dokumentavimas

121. Nepaisant to, ar apie pažeidimą reikia pranešti priežiūros institucijai, duomenų valdytojas privalo dokumentuoti visus pažeidimus, kaip paaiškinta BDAR 33 straipsnio 5 dalyje:

> *„Duomenų valdytojas dokumentuoja visus asmens duomenų saugumo pažeidimus, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kurių buvo imtasi. Remdamasi tais dokumentais, priežiūros institucija turi galėti patikrinti, ar laikomasi šio straipsnio.“*

122. Šis reikalavimas susijęs su BDAR 5 straipsnio 2 dalyje nustatytu atskaitomybės principu. Pažeidimų, apie kuriuos nereikia pranešti ir apie kuriuos reikia pranešti, registravimo tikslas taip pat yra susijęs su BDAR 24 straipsnyje nustatytomis duomenų valdytojo prievolėmis; priežiūros institucija gali pareikalauti leisti susipažinti su tais įrašais. Todėl duomenų valdytojai raginami turėti pažeidimų vidaus registrą, nepaisant to, ar jie privalo pranešti apie pažeidimą, ar ne[47].

123. Nors duomenų valdytojas pats pasirenka pažeidimų dokumentavimo būdą ir sistemą, yra keletas visais atvejais privalomų registruojamos informacijos elementų. Kaip reikalaujama BDAR 33 straipsnio 5 dalyje, duomenų valdytojas turi užregistruoti išsamią informaciją apie pažeidimą, nurodydamas jo priežastis, vietą ir asmens duomenis, kuriems tas pažeidimas turi poveikio. Be to, jis turėtų nurodyti pažeidimo poveikį, pasekmes ir taisomuosius veiksmus, kurių jis ėmėsi.

124. Bendrajame duomenų apsaugos reglamente šių dokumentų saugojimo laikotarpio nėra nustatyta. Jei tokiame registre yra asmens duomenų, duomenų valdytojas pagal asmens duomenų tvarkymo principus privalės nustatyti tinkamą jų saugojimo laikotarpį[48] ir užtikrinti teisėtą duomenų tvarkymo pagrindą[49]. Jis turės saugoti dokumentus pagal BDAR 33 straipsnio 5 dalį, nes jo gali būti paprašyta priežiūros institucijai pateikti to straipsnio reikalavimų arba, apskritai kalbant, atskaitomybės principo laikymosi įrodymus. Žinoma, jei registre asmens duomenų nėra, BDAR nustatytas saugojimo trukmės apribojimo principas[50] netaikomas.

125. EDAV rekomenduoja, kad, be šios informacijos, duomenų valdytojas taip pat dokumentuotų sprendimų, priimtų reaguojant į pažeidimą, pagrindą. Visų pirma, jei apie pažeidimą nepranešama, turėtų būti dokumentuotas tokio sprendimo pagrindimas. Pagrindžiant sprendimą, turėtų būti nurodytos priežastys, kodėl duomenų valdytojas mano, kad dėl pažeidimo neturėtų kilti pavojaus asmenų teisėms ir laisvėms[51]. Kita vertus, jei duomenų valdytojas mano, kad yra įvykdyta kuri nors iš

---

[46] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches (liet. „Rekomendacijos dėl pažeidimo rimtumo vertinimo metodikos“), https://www.enisa.europa.eu/publications/dbn-severity.

[47] Duomenų valdytojas gali nuspręsti dokumentuoti pažeidimus pagal BDAR 30 straipsnį tvarkomame duomenų tvarkymo veiklos registre. Jei tokiame registre galima aiškiai atskirti su pažeidimu susijusią informaciją ir prireikus ją išrinkti iš to registro, atskiro registro tvarkyti nebūtina.

[48] Žr. BDAR 5 straipsnį.

[49] Žr. BDAR 6 straipsnį, taip pat jo 9 straipsnį.

[50] Žr. BDAR 5 straipsnio 1 dalies e punktą.

[51] Žr. BDAR 85 konstatuojamąją dalį.

BDAR 34 straipsnio 3 dalyje nustatytų sąlygų, jis turėtų sugebėti pateikti tinkamus tų sąlygų įvykdymo įrodymus.

126. Jei duomenų valdytojas priežiūros institucijai praneša apie pažeidimą, tačiau pranešimas pateikiamas pavėluotai, duomenų valdytojas turi sugebėti pagrįsti to vėlavimo priežastis; su tuo susiję dokumentai gali padėti įrodyti, kad vėlavimas pranešti yra pagrįstas ir kad vėlavimas nebuvo pernelyg didelis.

127. Duomenų valdytojas, apie pažeidimą informuodamas asmenis, kuriems pažeidimas turi poveikio, pranešime turėtų aiškiai nurodyti pažeidimą ir pranešimą pateikti veiksmingai bei tinkamu laiku. Išsaugojus tokio pranešimo įrodymus, duomenų valdytojui bus lengviau įrodyti atskaitomybę ir reikalavimų laikymąsi.

128. Kad būtų lengviau laikytis BDAR 33 ir 34 straipsnių reikalavimų, duomenų valdytojams ir duomenų tvarkytojams būtų naudinga įgyvendinti dokumentais patvirtintą pranešimų teikimo tvarką, pagal kurią būtų nustatyta procedūra, taikytina nustačius pažeidimą, įskaitant tai, kaip sustabdyti ir suvaldyti pažeidimą, pašalinti jo padarinius, įvertinti pavojų ir pranešti apie pažeidimą. Šiuo atžvilgiu pažymėtina, kad norint įrodyti BDAR reikalavimų laikymąsi, taip pat gali būti naudinga įrodyti, kad darbuotojai yra informuoti apie tokių procedūrų ir mechanizmų buvimą ir žino, kaip reaguoti į pažeidimus.

129. Reikėtų pažymėti, kad tinkamai nedokumentavus pažeidimo, priežiūros institucija gali pasinaudoti BDAR 58 straipsnyje jai suteiktais įgaliojimais ir (arba) skirti administracinę baudą pagal BDAR 83 straipsnį.

B. Duomenų apsaugos pareigūno vaidmuo

130. Duomenų valdytojas arba duomenų tvarkytojas gali turėti duomenų apsaugos pareigūną[52], kaip reikalaujama BDAR 37 straipsnyje, arba paskirti tokį pareigūną savanoriškai, atsižvelgdami į gerąją praktiką. BDAR 39 straipsnyje nustatyta keletas privalomų užduočių, kurias turi vykdyti duomenų apsaugos pareigūnas, tačiau jame nėra draudžiama prireikus šiam pareigūnui pavesti papildomų užduočių.

131. Be kitų užduočių, itin svarbios yra šios su pranešimu apie pažeidimą susijusios duomenų apsaugos pareigūno užduotys: duomenų valdytojo arba duomenų tvarkytojo konsultavimas duomenų apsaugos klausimais, stebėjimas, kaip laikomasi BDAR, ir patarimų dėl poveikio duomenų apsaugai vertinimo teikimas. Be to, duomenų apsaugos pareigūnas privalo bendradarbiauti su priežiūros institucija ir būti kontaktiniu asmeniu, į kurį galėtų kreiptis priežiūros institucija ir duomenų subjektai. Taip pat reikėtų pažymėti, kad BDAR 33 straipsnio 3 dalies b punkte reikalaujama, jog pranešdamas apie pažeidimą priežiūros institucijai, duomenų valdytojas nurodytų savo duomenų apsaugos pareigūno arba kito kontaktinio asmens vardą bei pavardę (pavadinimą) ir kontaktinius duomenis.

132. Dėl pažeidimų dokumentavimo pažymėtina, kad duomenų valdytojui arba duomenų tvarkytojui gali būti naudinga sužinoti duomenų apsaugos pareigūno nuomonę dėl šios dokumentacijos struktūros, rengimo sistemos ir administravimo. Be to, duomenų apsaugos pareigūnui gali būti pavesta tvarkyti šiuos dokumentus.

133. Tai reiškia, kad duomenų apsaugos pareigūnas, teikdamas konsultacijas ir stebėdamas atitiktį, turėtų būti svarbus pagalbininkas vykdant pažeidimų prevenciją arba rengiantis reaguoti į pažeidimą, taip pat tuo metu, kai padaromas pažeidimas (t. y. kai teikiamas pranešimas priežiūros institucijai) ir kai priežiūros institucija atlieka tolesnį tyrimą. Atsižvelgdama į tai, EDAV rekomenduoja, kad duomenų

[52] Žr. darbo grupės gaires išleistas duomenų apsaugos pareigūnų gaires, skelbiamas šiuo interneto adresu: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

apsaugos pareigūnas būtų skubiai informuojamas apie tai, kad buvo padarytas pažeidimas, ir dalyvautų visame pažeidimo valdymo ir pranešimo apie jį procese.

VI. KITUOSE TEISĖS AKTUOSE NUSTATYTOS PRIEVOLĖS PRANEŠTI

134. Be BDAR reikalavimų pranešti ir informuoti apie pažeidimus, duomenų valdytojai taip pat turėtų žinoti kitų susijusių teisės aktų, kurie gali būti jiems taikomi, reikalavimus pranešti apie saugumo incidentus ir tai, ar pagal juos jiems taip pat gali reikėti tuo pat metu pranešti priežiūros institucijai apie asmens duomenų pažeidimą. Nors šie reikalavimai įvairiose valstybėse gali skirtis, galima pateikti tokius kituose teisės aktuose nustatytų reikalavimų pranešti ir jų sąsajų su BDAR pavyzdžius:

- *Reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje (eIDAS reglamentas)*[53].

135. eIDAS reglamento 19 straipsnio 2 dalyje reikalaujama, kad patikimumo užtikrinimo paslaugų teikėjai praneštų priežiūros įstaigai apie kiekvieną saugumo arba vientisumo pažeidimą, turėjusį didelį poveikį teikiamai patikimumo užtikrinimo paslaugai arba ją teikiant naudojamiems asmens duomenims. Jei taikytina, t. y. jei toks pažeidimas arba praradimas taip pat yra Bendrajame duomenų apsaugos reglamente nustatytas asmens duomenų saugumo pažeidimas, patikimumo užtikrinimo paslaugų teikėjas apie jį taip pat turėtų pranešti priežiūros institucijai.

- *Direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyva)*[54].

136. TIS direktyvos 14 ir 16 straipsniuose reikalaujama, kad esminių paslaugų operatoriai ir skaitmeninių paslaugų teikėjai apie saugumo incidentus praneštų savo kompetentingai institucijai. Kaip pripažįstama TIS direktyvos [55] 63 konstatuojamojoje dalyje, dėl incidentų dažnai gali kilti pavojus asmens duomenų saugumui. Nors TIS direktyvoje reikalaujama, kad kompetentingos institucijos ir priežiūros institucijos bendradarbiautų susijusiais klausimais ir keistųsi informacija, jei tokie incidentai yra BDAR nustatyti asmens duomenų saugumo pažeidimai arba jei jie tampa tokiais, tie operatoriai ir (arba) paslaugų teikėjai priežiūros institucijai apie juos vis vien turėtų pranešti atskirai, o ne vykdydami TIS direktyvos reikalavimus pranešti apie incidentus.

Pavyzdys

Debesijos paslaugų teikėjui, pranešančiam apie pažeidimą pagal TIS direktyvą, apie tą pažeidimą, jei tai yra asmens duomenų saugumo pažeidimas, taip pat gali reikėti pranešti duomenų valdytojui. Patikimumo užtikrinimo paslaugų teikėjui, teikiančiam pranešimą pagal eIDAS reglamentą, apie pažeidimą taip pat gali reikėti pranešti atitinkamai duomenų apsaugos institucijai.

- *Direktyva 2009/136/EB (Direktyva dėl piliečių teisių) ir Reglamentas (ES) Nr. 611/2013 (Reglamentas dėl pranešimo apie pažeidimus).*

137. Viešųjų elektroninių ryšių paslaugų teikėjai, kuriems taikoma Direktyva 2002/58/EB[56], apie pažeidimus privalo pranešti kompetentingoms nacionalinėms institucijoms.

---

[53] Žr. http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[54] Žr. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[55] 63 konstatuojamoji dalis: *„daugeliu atvejų dėl incidentų kyla pavojus asmens duomenų saugumui. Šiomis aplinkybėmis kompetentingos institucijos ir duomenų apsaugos institucijos turėtų bendradarbiauti ir keistis informacija visais su tuo susijusiais klausimais, kad galėtų imtis bet kokių dėl incidentų įvykusių asmens duomenų saugumo pažeidimų nagrinėjimo“.*

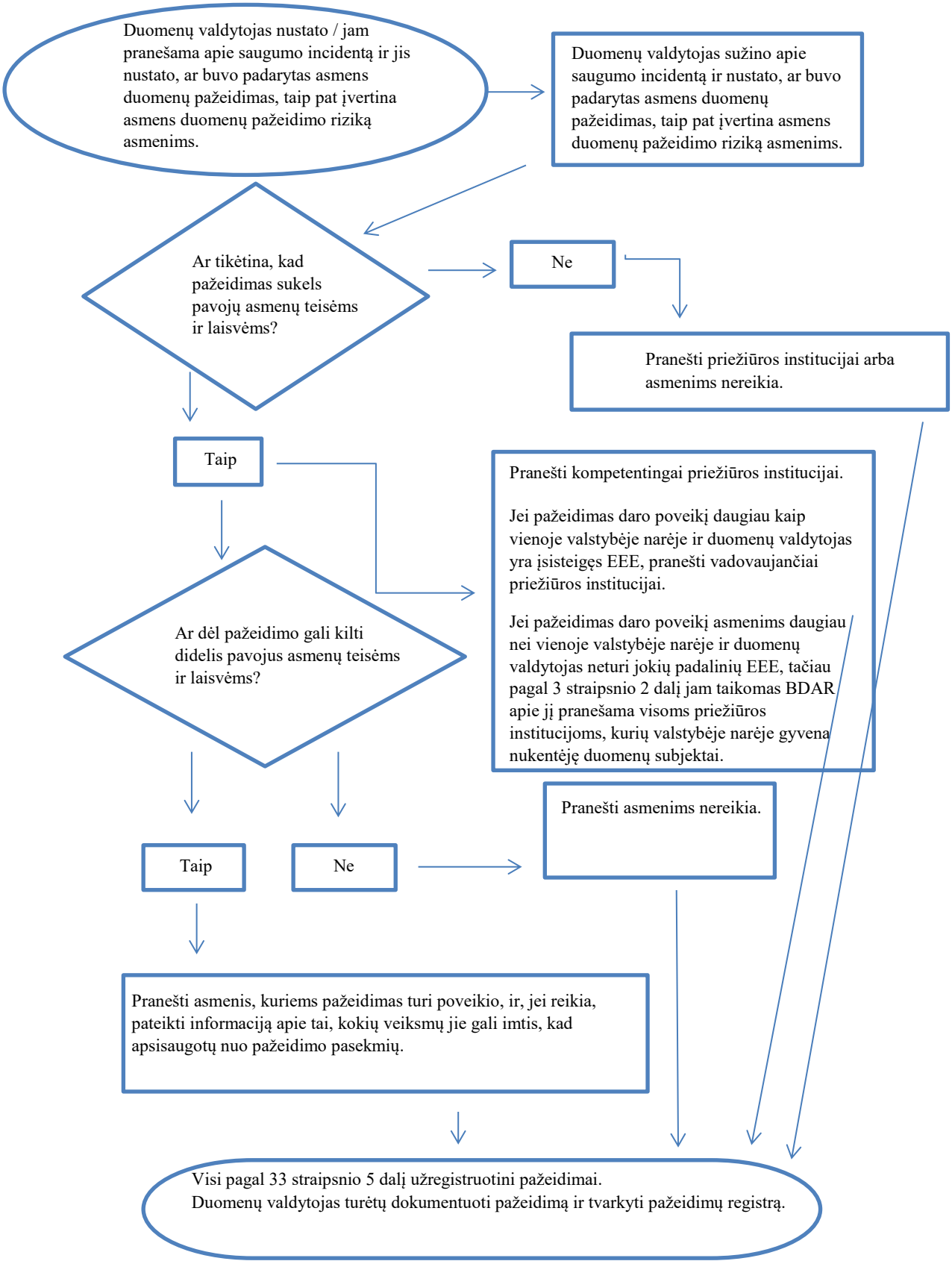
[56] 2017 m. sausio 10 d. Europos Komisija pasiūlė priimti Reglamentą dėl privatumo ir elektroninių ryšių, kuriuo būtų pakeista Direktyva 2009/136/EB ir panaikinti reikalavimai pranešti. Tačiau, kol šį pasiūlymą

138. Be to, duomenų valdytojai turėtų būti susipažinę su visomis kitomis teisinėmis, medicininėmis arba profesinėmis prievolėmis pranešti, nustatytomis pagal kitas taikomas tvarkas.

patvirtins Europos Parlamentas, galioja dabartiniai reikalavimai pranešti, žr. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications

VII. PRIEDAS

A. Reikalavimų pranešti vykdymo schema



B. Asmens duomenų saugumo pažeidimų ir informuotinų subjektų pavyzdžiai

Toliau pateiktas nebaigtinis pavyzdžių sąrašas padės duomenų valdytojams nustatyti, ar jie turi pranešti apie pažeidimą esant įvairiems asmens duomenų saugumo pažeidimo scenarijams. Šie pavyzdžiai taip pat gali padėti atskirti pavojų asmenų teisėms ir laisvėms nuo didelio pavojaus asmenų teisėms ir laisvėms.

	Pavyzdys	Pranešti priežiūros institucijai	Pranešti duomenų subjektui	Pastabos / rekomendacijos
i	Duomenų valdytojas užšifruotų asmens duomenų archyvo atsarginę kopiją įrašė į USB raktą. Įsilaužimo metu raktas buvo pavogtas.	Ne.	Ne.	Jei duomenys buvo užšifruoti taikant pažangų algoritmą, jei yra atsarginės duomenų kopijos, jei nekilo pavojaus unikalaus rakto saugumui ir jei tinkamu laiku galima atkurti duomenis, gali būti, kad apie pažeidimą pranešti nereikės. Tačiau, jei vėliau kils pavojus unikalaus rakto saugumui, apie pažeidimą reikės pranešti.
ii	Duomenų valdytojas teikia internetinę paslaugą. Tos paslaugos atžvilgiu įvykdžius kibernetinį išpuolį, išrenkami tam tikrų asmenų asmens duomenys. Duomenų valdytojo klientai yra vienoje valstybėje narėje.	Taip, jei gali kilti pasekmių asmenims, pranešti priežiūros institucijai.	Taip, atsižvelgiant į asmens duomenų, kuriems pažeidimas turi poveikio, pobūdį ir jei asmenims gali kilti labai rimtų pasekmių, pranešti asmenims.	
iii	Trumpas, kelias minutes trunkantis energijos tiekimo nutrūkimas duomenų valdytojo informacijos centre, dėl kurio klientai negali susisiekti su duomenų valdytoju ir prieiti prie savo duomenų.	Ne.	Ne.	Apie tokį pažeidimą pranešti nereikia, tačiau incidentas vis vien turi būti užregistruotas pagal 33 straipsnio 5 dalį. Duomenų valdytojas turėtų tvarkyti atitinkamą registrą.

iv	Duomenų valdytojo atžvilgiu įvykdomas išpuolis naudojant išpirkos reikalaujančią programą ir visi duomenys užšifruojami. Atsarginių kopijų nėra, duomenų atkurti negalima. Atliekant tyrimą, paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti duomenis ir kad jokios kitos kenkimo programinės įrangos sistemoje nėra.	Taip, pranešti priežiūros institucijai, jei gali kilti pasekmių asmenims (nes tai yra prieinamumo praradimas), pranešti priežiūros institucijai.	Taip, atsižvelgiant į asmens duomenų, kuriems pažeidimas turi poveikio, pobūdį, galimą duomenų neprieinamumo poveikį ir kitas tikėtinas pasekmes, pranešti asmenims.	Jei buvo padaryta atsarginė kopija ir tinkamu laiku galima atkurti duomenis, pranešti priežiūros institucijai arba asmenims nereikės, nes nebuvo negrąžinamai prarastas prieinamumas arba konfidencialumas. Tačiau, jei priežiūros institucija apie incidentą sužinotų kitais būdais, ji gali apsvarstyti galimybę atlikti tyrimą, kad įvertintų atitiktį platesniems saugumo reikalavimams, nustatytiems 32 straipsnyje.
v	Asmuo paskambina į banko informacijos centrą, norėdamas pranešti apie duomenų saugumo pažeidimą. Jis iš kažkokio kito subjekto gavo mėnesio ataskaitą. Duomenų valdytojas atlieka trumpą tyrimą (pvz., per 24 valandas) ir gana patikimai nustato, kad buvo padarytas asmens duomenų saugumo pažeidimas, ir išsiaiškina, ar jis buvo padarytas dėl sistemos spragos, t. y. ar buvo arba galėjo būti padarytas poveikis kitiems asmenims.	Taip.	Jei kyla didelis pavojus ir tikrai žinoma, kad kitiems asmenims poveikio nebuvo padaryta, pranešama tik asmenims, kuriems buvo padarytas poveikis.	Jei, atlikus tyrimą, nustatoma, kad pažeidimas turėjo poveikio daugiau asmenų, priežiūros institucijai turi būti pateiktas atnaujintas pranešimas ir, jei kyla didelis pavojus asmenims, duomenų valdytojas taip pat informuoja tuos asmenis.

vi	Duomenų valdytojas valdo elektroninę prekyvietę, jo klientai yra įvairiose valstybėse narėse. Prekyvietės atžvilgiu įvykdomas kibernetinis išpuolis, įsilaužėlis internete paskelbia naudotojų vardus, slaptažodžius ir pirkimo istoriją.	Taip, jei atliekamas tarpvalstybinis duomenų tvarkymas, pranešti vadovaujančiai priežiūros institucijai.	Taip, nes gali kilti didelis pavojus.	Duomenų valdytojas turėtų imtis veiksmų, pvz., paraginti atnaujinti paskyrų, kurioms buvo padarytas poveikis, slaptažodžius, taip pat imtis kitų veiksmų, kad būtų sumažintas pavojus. Be to, duomenų valdytojas turėtų atsižvelgti į kitas prievoles pranešti, pvz., jam, kaip skaitmeninių paslaugų teikėjui, nustatytas TIS direktyvoje.
vii	Saityno svetainių prieglobos įmonė, kaip duomenų tvarkytoja, aptinka programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas naudotojams, klaidą. Dėl šios spragos bet koks naudotojas gali gauti kito naudotojo paskyros duomenis.	Saityno svetainių prieglobos įmonė, kaip duomenų tvarkytoja, privalo nedelsdama informuoti visus savo klientus (duomenų valdytojus), kuriems pažeidimas turi poveikio. Numanydami, kad saityno svetainių prieglobos įmonė atliko tyrimą, duomenų valdytojai, kuriems pažeidimas turi poveikio, turėtų būti pagrįstai įsitikinę, kad kiekvieno iš jų atžvilgiu buvo padarytas pažeidimas, taigi turėtų būti laikoma, kad jie „sužinojo“ apie pažeidimą, kai gavo pranešimą iš saityno svetainių prieglobos įmonės (duomenų tvarkytojos). Tuomet duomenų valdytojas privalo informuoti priežiūros instituciją.	Jei neturėtų kilti didelio pavojaus asmenims, jų informuoti nebūtina.	Saityno svetainių prieglobos įmonė (duomenų tvarkytoja) privalo atsižvelgti į kitas prievoles pranešti (pvz., jai, kaip skaitmeninių paslaugų teikėjai, nustatytas TIS direktyvoje). Jei nėra įrodymų, kad kuris nors iš susijusių duomenų valdytojų pasinaudojo šiuo pažeidimu, apie pažeidimą gali nereikėti pranešti, tačiau jį veikiausiai reikės užregistruoti arba laikyti 32 straipsnyje nustatytų reikalavimų nesilaikymo atveju.
viii	Dėl kibernetinio išpuolio 30 valandų nebėra galimybės naudotis ligoninės turėtais medicinos dokumentais.	Taip, ligoninė privalo pranešti apie šį pažeidimą, nes gali kilti didelis pavojus pacientų gerovei ir privatumui.	Taip, pranešti asmenims, kuriems pažeidimas turi poveikio.	
ix	Daugybės studentų asmens duomenys per klaidą nusiunčiami netinkamais adresais, pasinaudojant	Taip, pranešti priežiūros institucijai.	Taip, atsižvelgiant į susijusių duomenų aprėptį ir pobūdį bei galimų pasekmių rimtumą, pranešti asmenims.	

	daugiau kaip tūkstančio el. pašto adresatų sąrašu.			
x	Tiesioginės rinkodaros tikslais išsiunčiamas e. laiškas adresatams laukuose „gavėjas“ arba „kopija“, kad kiekvienas gavėjas galėtų matyti kitų gavėjų e. pašto adresą.	Taip, jei poveikis padaromas daugybei asmenų, jei atskleidžiami jautraus pobūdžio duomenys (pvz., jei tai psichoterapeuto el. pašto adresų sąrašas) arba jei dėl kitų veiksnių kyla dideli pavojai (pvz., el. laiške yra nurodyti pradiniai slaptažodžiai), gali būti privalu pranešti priežiūros institucijai.	Taip, atsižvelgiant į susijusių duomenų aprėptį ir pobūdį bei galimų pasekmių rimtumą, pranešti asmenims.	Jei neatskleidžiami jautraus pobūdžio duomenys ir jei atskleidžiama labai nedaug el. pašto adresų, pranešimo gali nereikėti.