

REKOMENDACIJA
KAIP VERTINTI ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO KELIAMĄ PAVOJŲ?

1 versija
2026 m. spalio 23 d.

Turinys

1. Įžanga	2
2. Rizika ir pavojus BDAR kontekste	2
3. Pranešimas duomenų subjektui	2
4. Didelio pavojaus nustatymas	3
5. Veiksniai, į kuriuos reikia atsižvelgti vertinant pavojų	3
5.1. ADSP pobūdis.....	3
5.2. Asmens duomenų pobūdis, jautrumas ir kiekis	4
5.3. Asmenų tapatybės nustatymo lengvumas	6
5.4. Pasekmių sunkumas asmenims	7
5.5. Kai ADSP metu paveikiamos pažeidžiamų asmenų grupės	8
5.6. Apibendrinimas: kada reikia pranešti apie ADSP	8
6. ADSP keliamo pavojaus lygio nustatymas.....	9
6.1. ADSP keliamo pavojaus nustatymo pavyzdžiai	11
6.2. DI technologijų poveikis ADSP keliamo pavojaus lygio nustatymui	13
7. Aktualūs EDAV metodiniai dokumentai	13

1. Įžanga

Bendrasis duomenų apsaugos reglamentas (toliau – BDAR) reikalauja, kad duomenų valdytojai ir duomenų tvarkytojai įgyvendintų tinkamas technines ir organizacines saugumo priemones, kad **būtų užtikrintas** tvarkomiems asmens duomenims **kylančius pavojus atitinkantis saugumo lygis**. Turėtų būti atsižvelgiama 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 (BDAR 32 straipsnis).

Asmens duomenų saugumo pažeidimo (toliau – ADSP) 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 (šiuo atveju Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI)), **nebent ADSP neturėtų kelti pavojaus** fizinių asmenų teisėms ir laisvėms (BDAR 33 straipsnio 1 dalis). Tuo tarpu BDAR 34 straipsnio 1 dalyje nustatyta, kad kai dėl ADSP gali kilti **didelis pavojus** fizinių asmenų teisėms ir laisvėms, duomenų valdytojas nepagrįstai **nedelsdamas praneša** apie ADSP duomenų subjektui. Akivaizdu, kad šios dvi pareigos yra glaudžiai susijusios ir abi priklauso nuo to paties vertinimo, todėl tinkamas pavojaus lygio nustatymas yra abiejų pareigų taikymo pagrindas.

Taigi itin svarbu, kad duomenų valdytojas, kai tik sužino apie ADSP, ne tik **imtųsi priemonių incidentui suvaldyti**, bet ir **įvertintų pavojų**, kuris gali kilti dėl to incidento:

žinant poveikio asmeniui tikimybę ir galimą poveikio sunkumą, bus lengviau imtis veiksmingų priemonių ADSP suvaldyti ir pašalinti jo pasekmes.	tai padės nustatyti, ar apie ADSP būtina pranešti VDAI ir, jei reikia, susijusiems fiziniams asmenims, kuriems gali kilti pavojus
--	---

Pavojaus lygio nustatymas – ne formalumas, o BDAR atskaitomybės principo įgyvendinimo dalis. Tinkamai dokumentuotas pavojaus vertinimas padeda duomenų valdytojui priimti sprendimus bei padeda užtikrinti ir įrodyti atitiktį BDAR reikalavimams.

2. Rizika ir pavojus BDAR kontekste

Verta atkreipti dėmesį, kad originaliame anglų kalba BDAR tekste vartojamas terminas „risk“ (liet. rizika) lietuvių kalba BDAR tekste išverčiamas kaip „pavojus“, o tai labiau atitiktų terminą „grėsmė“ (angl. *threat*). Praktikoje dėl to kyla nedidelė painiava, nes remiantis nusistovėjusia informacijos saugumo standartuose terminologija, šie terminai reiškia nors ir susijusius, bet skirtingus dalykus.

Rizikos ir pavojaus terminų santykį galima apibūdinti taip, kad „pavojaus (ar grėsmės) vertinimas yra rizikos vertinimo dalis“, taigi **rizikos vertinimas yra platesnė sąvoka**. Pavyzdžiui, atliekant rizikos vertinimą pirmiau yra identifikuojamos grėsmės ir pavojai, o kitame etape vertinama rizikos tikimybė ir poveikis.

3. Pranešimas duomenų subjektui

Pagrindinis kriterijus, kuriuo remiantis nustatoma, ar apie ADSP reikia informuoti duomenų subjektus, yra tai, ar dėl ADSP gali kilti didelis pavojus asmenų teisėms ir laisvėms.

Pranešimo fiziniams asmenims tikslas – pateikti konkrečią informaciją apie tai, kas įvyko, kokių atsargumo priemonių ar veiksmų jie turėtų imtis, kad apsisaugotų nuo galimų neigiamų ADSP pasekmių.

Nors BDAR yra nustatyta prievolė pranešti apie ADSP, šis reikalavimas taikomas ne visada. Jei yra įvykdytos BDAR 34 straipsnio 3 dalyje nustatytos sąlygos, tokiu atveju pranešti asmenims nereikalaujama. BDAR 34 straipsnio 4 dalyje paaiškinta, kad tuo atveju, kai duomenų valdytojas nusprendžia neinformuoti asmens apie ADSP, priežiūros institucija (šiuo atveju VDAI) gali pareikalauti, kad jis tą padarytų, jei, jos nuomone, dėl ADSP visgi gali kilti didelis pavojus asmenims.

Pastabėtina, Europos duomenų apsaugos valdyba (EDAV) yra parengusi gaires Nr. [9/2022](#) dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal BDAR, kuriose detalčiau aptariamas pranešimas duomenų subjektui.

4. Didelio pavojaus nustatymas

Didelis pavojus gali kilti tuomet, kai dėl ADSP asmenys, kurių duomenų saugumas buvo pažeistas, gali patirti **kūno sužalojimą, materialinę ar nematerialinę žalą**. Tokios žalos pavyzdžiai yra diskriminacija, tapatybės vagystė arba jos klastojimas, finansiniai nuostoliai ir pakenkimas reputacijai. Tikėtina, kad žala bus padaryta, jei ADSP 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 nusprendžius ir nusikalstamas veikas arba susijusias apsaugos priemones (BDAR preambulės 75 ir 85 konstatuojamosios dalys).

5. Veiksniai, į kuriuos reikia atsižvelgti vertinant pavojų

ADSP atveju **incidentas jau yra įvykęs**, todėl vertinamas tik tas pavojus, kuris asmenims gali kilti dėl šio ADSP. Duomenų valdytojas turėtų išnagrinėti visas reikšmingas ADSP aplinkybes, įskaitant **galimo poveikio rimtumą ir to poveikio padarymo tikimybę**. Vertinant ADSP, rekomenduojama atsižvelgti į toliau nurodytus **veiksnius (kriterijus)**.

5.1. ADSP pobūdis

ADSP yra tokia **saugumo incidento rūšis**, kai pažeidimas yra susijęs su asmens duomenimis. Nuo padaryto ADSP pobūdžio gali priklausyti pavojaus, kuris kyla asmenims, dydis. Pavyzdžiui, konfidencialumo pažeidimas, padarytas medicininę informaciją atskleidus šalims, kurios neturi teisės gauti tokios informacijos, gali turėti skirtingų pasekmių asmeniui, kurio atžvilgiu buvo padarytas pažeidimas, kai asmens medicininiai duomenys prarandami ir jų nebelieka.

1 lentelė. ADSP pažeidimų rūšys

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 prie asmens duomenų praradimas arba asmens duomenų sunaikinimas

Reikėtų pažymėti, kad, atsižvelgiant į aplinkybes, ADSP vienu metu gali būti susijęs su asmens duomenų konfidencialumu, vientisumu ir prieinamumu prie asmens duomenų, taip pat su bet koku šių savybių deriniu. Vertinant ADSP keliamą pavojų svarbu kontekstas, nes tos pačios rūšies ADSP skirtingomis aplinkybėmis gali kelti skirtingo lygio pavojų.

Pavojaus lygiui įtaką daro ir tai, kad dėl dirbtinio intelekto įrankių prieinamumo ir spartaus tobulėjimo bet koks duomenų nutekėjimas ženkiai didina efektyvaus socialinės inžinerijos metodų išnaudojimo grėsmę.

Nustatyti, ar buvo padarytas konfidencialumo arba vientisumo ADSP, yra palyginti nesunku, tačiau prieinamumo ADSP nėra tokie akivaizdūs. Prieinamumo ADSP visada laikomi tokie pažeidimai, kai asmens duomenys negrąžinamai prarandami arba sunaikinami. Kibernetinis incidentas, dėl kurio asmens duomenys tam tikrą laiką tampa neprieinami, taip pat yra prieinamumo ADSP. Visgi pažymėtina, kad tuo atveju, kai asmens duomenys yra neprieinami dėl atliekamų numatytų (iš anksto) sistemos techninės priežiūros darbų, tai nėra laikoma prieinamumo ADSP, kaip apibrėžta BDAR 4 straipsnio 12 dalyje.

5.2. Asmens duomenų pobūdis, jautrumas ir kiekis

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. Net ir nedidelis labai jautraus pobūdžio asmens duomenų kiekis gali turėti didelį poveikį asmeniui.

Sveikatos duomenų, asmens tapatybės dokumentų arba finansinių duomenų, pavyzdžiui, kredito kortelės duomenų, saugumo pažeidimai gali padaryti **ne tik tiesioginės žalos**, bet, naudojami kartu su kitais duomenimis, gali padėti pavogti tapatybę. Įvairių asmens duomenų **derinys** dažnai yra jautresnio pobūdžio nei pavieniai asmens duomenys.

Pavojaus vertinimui gali turėti įtakos konkretaus atvejo aplinkybės. 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 sukelti reikšmingų neigiamų pasekmių tiek įtėviams, tiek vaikui.

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.

2 lentelė. Asmens duomenų pobūdžio ir jautrumo vertinimo pavyzdžiai

Duomenų tipas	Tikėtinas pavojaus lygis	Pavyzdžiai
Specialių kategorijų duomenys (sveikatos, lytinė orientacija)	Didelis pavojus	- Atskleidžiama informacija apie tai, kad konkretus asmuo yra žmogaus imunodeficitu viruso (ŽIV) nešiotojas; - atskleidžiama informacija apie nepilnamečio lytinę orientaciją.
Specialių kategorijų duomenys (biometriniai duomenys)	Didelis pavojus	Kibernetinio incidento metu neįgalioti asmenys neteisėtai prisijungė prie duomenų

		bazės ir gavo prieigą prie joje nešifruotu pavidalu saugomų biometrinių duomenų – pirštų atspaudų.
Kreditinių kortelių duomenys	Didelis pavojus	Neteisėtam gavėjui atskleidžiami galiojančios kreditinės kortelės duomenys (numeris, galiojimo data ir saugos kodas).
Nekilnojamojo turto duomenys (savininko vardas, pavardė, turto adresas, asmens kodas)	Didelis pavojus	Neteisėtos prieigos prie registro duomenų atveju nukopijuojami 1500 asmenų NTR duomenys.
Prisijungimo duomenys, slaptažodžiai, šifravimo raktai	Didelis pavojus	Pažeistas informacinės sistemos, paskyrų naudotojų vardų ir slaptažodžių konfidencialumas.
Vardas, pavardė, gyv. vietos adresas	Didelis pavojus	- Teisėjų, teisėsaugos pareigūnų duomenų atskleidimas; - įvaikinto vaiko duomenų atskleidimas biologiniams tėvams.
Specialių kategorijų duomenys (sveikatos)	Kyla pavojus	Poliklinikos darbuotojas, kurio darbo funkcijos nebuvo tiesiogiai susijusios su konkreto paciento gydymu, šešis kartus peržiūrėjo paciento el. medicininės kortelės duomenis, įskaitant diagnozes.
Specialių kategorijų duomenys (genetiniai duomenys)	Kyla pavojus	Pacientui per klinikos savitarnos portalą trumpam tampa prieinamas kito paciento genetinio tyrimo rezultatas. Klaida ištaisyta tą pačią darbo dieną, nėra požymių, kad duomenys būtų buvę nukopijuoti.
Asmens kontaktiniai duomenys, adresai, užsakymų informacija	Kyla pavojus	Dėl programinės įrangos klaidingos konfigūracijos sutrinka savitarnos portalo veikimas. Dalis klientų pateiktų užsakymų išsaugomi neteisingai, todėl daliai klientų prekės pristatytos neteisingu adresu.
Finansiniai duomenys, darbo laiko apskaitos duomenys	Kyla pavojus	Dėl serverio gedimo kavinė dvi darbo dienas negali pasiekti darbuotojų darbo laiko apskaitos, grafikų ir atlyginimams apskaičiuoti reikalingų duomenų. Atsarginė kopija yra, tačiau jos atkūrimas užtrunka.
Specialių kategorijų duomenys (politinės pažiūros)	Pavojaus nėra	- Atskleidžiamos paties asmens viešai deklaruojamos politinės pažiūros; - atskleidžiamas faktas, kad vaikas lankėsi sveikatos įstaigoje dėl pažymos mokyklai.
Finansiniai, mokėjimų	Pavojaus nėra	Sąskaita už komunalines paslaugas su asmens vardu, pavarde, kliento kodu, suteiktomis paslaugomis ir mokėjimo paskirtimi el. paštu išsiunčiama neteisingam gavėjui, kuris patvirtina laiško ištrynimą.
Nekilnojamojo turto duomenys (savininko vardas, pavardė, turto adresas, asmens kodas)	Pavojaus nėra	Nekilnojamojo turto vertintojas per klaidą išsiunčia klientui el. paštu kitam asmeniui priklausančio turto registro išrašą. Klientas

		patvirtina gauto laiško sunaikinimą, duomenų nenaudojimą.
Vardas, pavardė, adresas	Pavojaus nėra	Atskleidžiama informacija apie savininką ir numatomą remontą jam priklausančiose patalpose neteisėtam duomenų gavėjui.
Tik pseudonimizuoti / šifruoti duomenys (be šifravimo raktų)	Pavojaus nėra	Prarandama stipriu algoritmu užšifruota atsarginė duomenų kopija, tačiau šifravimo raktai saugomi atskirai ir nėra požymių, kad jie buvo pažeisti.

5.3. Asmenų tapatybės nustatymo lengvumas

Svarbus veiksnys, į kurį reikia atsižvelgti, yra tai, kaip piktavaliui ar neįgaliotam asmeniui, gavus prieigą prie duomenų, 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 susieti su konkrečiu asmeniu bus labai sunku, bet tam tikromis sąlygomis vis vien įmanoma. Tai priklauso nuo konkrečių ADSP aplinkybių ir to, ar susiję asmens duomenys yra skelbiami **viešai**.

Vertindamas šį veiksnių, duomenų valdytojas turėtų atsakyti į du klausimus:

Ar naudojant pažeistus duomenis įmanoma tiesiogiai ar netiesiogiai susieti ir identifikuoti asmenį?	Ar asmens duomenims apsaugoti buvo naudojamas tinkamo lygio šifravimas ar duomenų pseudonimizacija ?
---	--

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 ADSP atveju bus nustatyta asmenų tapatybė. Tačiau vien pseudonimų suteikimo nepakanka, kad duomenys būtų neįskaitomi ar nesusiejami su konkrečiu asmeniu.

Skiriamos kelios pagrindinės asmens duomenų apsaugos nuo tiesioginio identifikavimo priemonės, kurios skiriasi tiek jų atšaukiamumu (galimybė atkurti pradinis duomenis), tiek pasiekiamu duomenų apsaugos lygiu (3 lentelė).

3 lentelė. Duomenų apsaugos nuo tiesioginio identifikavimo priemonės

Pilna anonimizacija (angl. <i>full anonymization</i>)	Pseudonimizacija (angl. <i>pseudonymization</i>)	Duomenų maskavimas (angl. <i>data masking</i>)
Duomenys pakeičiami taip, kad fizinis asmuo nebūtų identifikuojamas nei	Asmens duomenys (vardas, pavardė, asmens kodas) pakeičiami pseudonimais (kodais, inicialais, slapyvardžiais).	Techninė priemonė, kai dalies ar visų duomenų reikšmės uždengiamos, pakeičiamos arba užšifruojamos.

tiesiogiai, nei netiesiogiai. • Negalima atkurti ryšio su konkrečiu asmeniu. • Tai neatšaukiamas procesas.	• Duomenys išlieka susieti su konkrečiu asmeniu, bet reikia papildomos informacijos (rakto) identifikavimui atkurti. • Tai atšaukiamas procesas.	• Gali būti atšaukiamas arba neatšaukiamas procesas (priklauso nuo pasirinkto metodo).
Pavyzdys: Iš statistinių duomenų pašalinami visi unikalūs ar retai pasitaikantys bruožai (pavyzdžiui, reta profesija, išskirtinis išsilavinimas, specifiniai įgūdžiai).	Pavyzdys: Asmeniui priskiriamas identifikatorius (pavyzdžiui, naudotojas_123), kuris laikomas atskiroje duomenų bazėje nuo vardo, pavardės ir adreso.	Pavyzdys: Asmens gimimo data vietoje tikslios datos pakeista į „1980-ieji“, jautrūs duomenys pakeisti unikaliais žetonais (angl. Data Tokenization).

Tinkamu lygiu užšifruoti, pakeisti asmens duomenys nebus suprantami neįgaliesiems asmenims, neturintiems iššifravimo rakto.

4 lentelė. Asmenų tapatybės nustatymo lengvumo vertinimo pavyzdžiai

Situacija	Nustatymo lengvumas
Vairuotojo pažymėjimo ar IBAN sąskaitos duomenys	Aiškiai identifikuojami asmenys
IP adreso ar geolokaciniai duomenys	Asmenys gali būti identifikuojami netiesiogiai
Duomenys yra pseudonimizuoti ar užšifruoti stipriu algoritmu (pavyzdžiui, atsarginė duomenų kopija užšifruota, šifravimo raktų konfidencialumas nebuvo pažeistas)	Identifikuoti sudėtinga , bet nėra neįmanoma

Pastebėtina, kad šifravimas mažina pavojų tik tada, kai naudojamas stiprus algoritmas, užtikrinamas tinkamas jo įgyvendinimas, šifravimo raktai nėra pažeisti, nėra nutekėjusių atsarginių kopijų ir nėra kitų realių būdų identifikuoti fizinius asmenis.

5.4. Pasekmių sunkumas asmenims

Atsižvelgiant į asmens duomenų, kurių saugumas buvo pažeistas, pobūdį, pavyzdžiui, jei tai yra specialių kategorijų duomenys, galima žala asmenims gali būti labai didelė: sveikatos sutrikdymas, sukeliama psichologinė kančia, patiriamas pažeminimas arba pakenkiama reputacijai. Tapatybės vagystė taip pat gali sukelti reikšmingas pasekmes.

Galimos ADSP pasekmės:

Fizinės (žala sveikatai, pavojus saugumui)	Psichologinės (baimė, stresas, persekiojimas)
Finansinės (sukčiavimas, tapatybės vagystė)	Socialinės (pažeminimas, reputacijos pablogėjimas)

Taip pat vertinant pavojų reikėtų atsižvelgti į tikimybę, kad žala įvyks, žalos intensyvumą bei pasekmių asmenims **ilgalaikiškumą**: jei pažeidimo pasekmės yra ilgalaikės, tai ir jo poveikis veikiausiai yra didesnis. Svarbus aspektas – ADSP poveikis ir pasekmės kartais pasireiškia ne iškart, o tolimesnėje ateityje (pavyzdžiui, piktavaliai asmenys kaupia nutekintų duomenų bazę, sukaupę didelį jų kiekį, po keleto mėnesių ar net metų ima juos naudoti neteisėtais tikslais).

Todėl, jei vėliau paaiškėja naujų aplinkybių ar gaunama papildomų faktinių duomenų, dėl kurių ADSP keliamas pavojaus lygis padidėja, duomenų valdytojas privalo **iš naujo įvertinti pavojų** ir, jei reikia, įvykdyti su padidėjusiu pavojaus lygiu susijusias BDAR pareigas – be kita ko, informuoti apie ADSP duomenų subjektus, net jeigu pirminio vertinimo metu tokios pareigos nebuvo nustatyta.

Rekomenduotina sudėtingesnių ADSP atvejais atlikti potencialių **scenarijų analizę**, siekiant išvengti neišsames, fragmentiško ADSP keliamo pavojaus vertinimo. Praktiškai tai reikštų, kad tokio ADSP atveju turėtų būti **išanalizuoti** bent trys galimi scenarijai: tiesioginis (kas gali nutikti per pirmąsias savaites), vidutinės trukmės (per kelis mėnesius) ir ilgalaikis (per metus ir ilgiau). Pavyzdžiui, gal atrodo, kad nutekėję duomenys trumpuoju laikotarpiu nekelia didelio pavojaus, tačiau ilgalaikėje perspektyvoje tokie duomenys gali būti sujungiami su kitais nutekėjusiais duomenų rinkiniais juodojoje rinkoje, sukuriant išsamų asmens profilį, kuris vėliau gali būti panaudotas tikslinei tapatybės vagystei.

5.5. Kai ADSP metu paveikiamos pažeidžiamų asmenų grupės

Pažeidimas gali turėti poveikį vaikams ar kitiems **pažeidžiamiems asmenims**, kuriems dėl ADSP gali kilti didesnė pavojaus rizika. Vertinant šį veiksni, svarbu atsižvelgti į asmenų gebėjimą savarankiškai apsaugoti nuo galimų neigiamų pasekmių, priklausomybę nuo duomenų valdytojo teikiamų paslaugų ir galimą socialinį, fizinį ar ekonominį pažeidžiamumą. Taip pat gali būti kitų veiksnių, galinčių turėti įtakos tam, koks poveikis asmeniui bus padarytas. Įvertinkite, ar tarp paveiktų asmenų yra:

vaikai ir paaugliai?	socialiai jautrios grupės?
sunkiai sergantys asmenys?	asmenys su intelekto ar kognityviniais sutrikimais?

Laikoma, kad pavojus yra **didelis** vien dėl to, kad buvo paveiktos pažeidžiamų asmenų grupės.

5.6. Apibendrinimas: kada reikia pranešti apie ADSP

Skirtingai nei ankstesni šio skyriaus poskyriai, šis poskyris nėra atskiras pavojaus vertinimo veiksnys – jame tik apibendrinama, kokias pareigas lemia jau nustatytas pavojaus lygis. Ar reikia apie ADSP pranešti VDAI ir informuoti duomenų subjektus, galima nustatyti, įvertinus, kokį pavojų kelia įvykęs ADSP asmenų teisėms ir laisvėms.

5 lentelė. Dokumentavimo ir pranešimo pareigos pagal pavojaus lygį

Pavojaus lygis	Ar dokumentuoti?	Pranešti VDAI?	Pranešti duomenų subjektams?
Pavojaus nėra	Taip	Ne	Ne
Kyla pavojus	Taip	Taip	Ne
Kyla/gali kilti didelis pavojus	Taip	Taip	Taip*

*Nebent įvykdyta bent viena BDAR 34 straipsnio 3 d. numatyta sąlyga (pavyzdžiui, taikytos pažangios šifravimo priemonės, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami).

6. ADSP keliamo pavojaus lygio nustatymas

EDAV yra parengusi gaires Nr. [01/2021](#) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą pavyzdžių“. Jose yra pateikiama 18 ADSP atvejų pavyzdžių su prevencinių priemonių ir pavojų vertinimu bei poveikio mažinimo priemonėmis.

Pavojaus nustatymui yra **svarbi duomenų konteksto analizė**, kuri apima ADSP pobūdį, paveiktų asmenų specifiką, galimas pasekmes ir priimtas poveikio mažinimo priemonės. **Tie patys duomenys gali turėti skirtingą pavojaus lygį priklausomai nuo konteksto.** Pavyzdžiui, vien vardo ir pavardės atskleidimas profesiniame kontekste paprastai kelia nedidelį (ar mažai tikėtiną) pavojų, tačiau tie patys duomenys kartu su informacija apie asmens dalyvavimą priklausomybių gydymo programoje gali kelti didelį pavojų ir lemti diskriminaciją.

6 lentelė. ADSP keliamo pavojaus vertinimo kriterijai

SUNKUMAS (angl. Severity) Įvertinkite galimą neigiamą poveikį fiziniams asmenims atsižvelgdami į šiuos kriterijus:	TIKIMYBĖ (angl. Likelihood) Įvertinkite tikimybę, kad neigiami įvykiai iš tikrųjų įvyks, atsižvelgdami į šiuos kriterijus:
Duomenų jautrumas Ar pažeisti specialių kategorijų duomenys (sveikatos, biometriniai, genetiniai duomenys, rasinė/etninė kilmė, lytinė orientacija)?	Duomenų prieinamumas Kas turi prieigą prie pažeistų asmens duomenų? Ar jie viešai paskelbti internete, ar jais disponuoja piktavaliai asmenys, ar su jais susipažino tik ribotas skaičius (ne)patikimų asmenų?
Galimas žalos pobūdis Fizinės, (ne)materialinės žalos galimybė (žala sveikatai, tapatybės vagystė, sukčiavimas, finansiniai nuostoliai, reputacijos praradimas, pažeminimas).	Techninės apsaugos priemonės Ar asmens duomenys buvo užšifruoti? Ar šifravimo raktai saugūs? Ar naudoti stiprūs slaptažodžiai? Ar buvo įdiegti papildomi prieigos kontrolės sluoksniai ir taikyti apribojimai?
Pažeidžiamos grupės Ar paveikti vaikai, asmenys su negalia, medicinos pacientų paramos ir pagalbos grupių nariai ar kitos pažeidžiamos asmenų grupės?	Poveikio mažinimo priemonės Ar galima efektyviai sušvelninti poveikį (pavyzdžiui, pakeisti slaptažodžius, blokuoti prieigą, informuoti asmenis)?
Duomenų kiekis ir jų detalumas Ar pažeistas didelis asmens duomenų kiekis, ar nutekėjo detali naudotojų profilių informacija ar tik informacijos fragmentai?	Identifikavimo lengvumas Kaip lengvai būtų galima iš turimų duomenų identifikuoti konkrečius asmenis? Ar reikia papildomo atskiro tyrimo asmens tapatybei atskleisti?

Įvertinus galimą **ADSP poveikio ar žalos sunkumą ir poveikio atsiradimo tikimybę** (pagal šių dviejų įverčių susikirtimo tašką), pasinaudojant ADSP keliamo pavojaus matrica (7 lentelė) yra nustatomas **ADSP keliamo pavojaus įvertinimas**.

Tikimybė turi būti vertinama tiek faktiniais, tiek techniniais įrodymais, pavyzdžiui, ar duomenys realiai paimti, nukopijuoti ar paskelbti; ar prieigą gavęs asmuo yra patikimas; ar yra piktavališkumo požymių; ar įvertinti žurnalinių įrašų ar kitų techninių šaltinių duomenys; ar yra pagrįstų įrodymų,

kad duomenys nebuvo peržiūrėti, atsisiųsti ar pan. Pastebėtina, kad ateityje paaiškėjus naujoms ADSP aplinkybėms ar poveikiui, gavus naujų faktinių įrodymų, rizikos vertinimas gali kisti.

Operatyviai pritaikytos rizikos švelninimo priemonės (priverstinis visų paskyrų slaptažodžių keitimas, prarastų fizinių prieigos kortelių atšaukimas, pažeistų sistemų apribojimas ir atskyrimas nuo kompiuterių tinklo) po ADSP gali sumažinti pavojaus lygį, tačiau jos turi būti realiai veiksmingos ir pagrįstos įrodymais.

7 lentelė. ADSP keliamo pavojaus matrica

Didelė tikimybė	Pavojaus nėra	Didelis pavojus	Didelis pavojus
Vidutinė tikimybė	Pavojaus nėra	Kyla pavojus	Didelis pavojus
Maža tikimybė	Pavojaus nėra	Pavojaus nėra	Kyla pavojus
	Žemas sunkumas	Vidutinis sunkumas	Didelis sunkumas

Sunkumas (galimo poveikio duomenų subjektui mastas ir reikšmingumas, jei žala pasireikštų):

- **Žemas:** nereikšminga arba nežymi žala, neturinti arba turinti tik minimalų poveikį duomenų subjekto teisėms ir laisvėms;
- **Vidutinis:** reikšminga, tačiau laikina arba bent iš dalies ištaisoma žala (pvz., laikini finansiniai nuostoliai, nepatogumai, ribotas reputacijos pablogėjimas);
- **Didelis:** rimta, ilgalaikė arba nepataisoma žala, galinti sukelti reikšmingų fizinių, materialinių ar nematerialinių pasekmių (pvz., tapatybės vagystę, diskriminaciją, reikšmingą finansinę žalą ar reputacijos pablogėjimą).

Tikimybė (kad žala iš tikrųjų atsiras):

- **Maža:** mažai tikėtina, kad žala pasireikš, ir tai pagrįsta objektyviais faktais (pvz., duomenys buvo tinkamai užšifruoti, o šifravimo raktai nebuvo pažeisti);
- **Vidutinė:** yra reali galimybė, kad žala pasireikš, tačiau turima informacija neleidžia daryti išvados, kad ji tikėtina arba jau vyksta;
- **Didelė:** yra pakankamas pagrindas manyti, kad žala pasireikš arba jau pasireiškia (pvz., duomenys viešai paskelbti, nustatytas jų panaudojimas piktavališkais tikslais).

ADSP pavojaus matrica yra pagalbinė priemonė pirminiam ADSP pavojaus vertinimui atlikti, o galutinį ADSP pavojaus lygį vis dėlto nustato pats duomenų valdytojas, nes tik jis geriausiai žino savo veiklos procesus ir ADSP kontekstą, todėl, atsižvelgiant į neįprastas, netipines ADSP aplinkybes, keliamo ADSP pavojaus lygis gali būti tiek padidinamas, tiek sumažinamas.

6.1. ADSP keliamo pavojaus nustatymo pavyzdžiai

Pateikiami keli ADSP keliamo pavojaus nustatymo pavyzdžiai.

ADSP pavyzdys Nr. 1

Prieigos prie duomenų bazės sutrikimas	
Situacija: Dėl programinės įrangos klaidos draudimo įmonės duomenų bazės veikla tapo nestabili, asmenys ribotą laiką (iki 1 val.) negalėjo naudotis savitarnos portalu ir mobiliąja aplikacija. Kai kuriems įmonės klientams sutrikimo metu pavyko sudaryti draudimo sutartis, tačiau buvo pažeistas 53 sutarčių duomenų vientisumas – joms buvo suteikti vienodi numeriai. Problema identifikuota ir pašalinta. Sutrikimas neturėjo įtakos draudimo apsaugos galiojimui ar galimybei pasinaudoti sutartyse nustatytomis teisėmis.	
Sunkumas: žemas (asmens duomenys sutartyse nebuvo sumaišyti, sugadinti ar atskleisti tretiesiems asmenims; paveiktas tik automatinis sutarčių numeravimas).	
Tikimybė: maža (žala mažai tikėtina, vientisumo pažeidimas neturėjo įtakos sutarčių turiniui, jų teisei galiai ar pagal jas vykdomiems mokėjimams).	
Identifikavimas: Neaktualu. Duomenų konfidencialumas nebuvo pažeistas.	
Pavojaus mažinimas: paveiktos sutartys sugeneruotos iš naujo, joms suteikti nauji numeriai.	
Papildomai: Peržiūrėti sistemos konfigūraciją, patikrinti atsarginių kopijų prieinamumą.	
PAVOJAUS NĖRA	Reikia dokumentuoti ADSP, pranešti VDAI nereikia. Duomenų subjektų informuoti nereikia.

ADSP pavyzdys Nr. 2

Dokumento pasirašymo nuoroda pateikta nesusijusiems asmenims	
Situacija: Įmonės Dokumentų valdymo sistemoje, įvykus sistemos programinei klaidai, pranešimas su dokumento (NT pirkimo-pardavimo sutarties) pasirašymo nuoroda buvo išsiųstas ne 2, o 133 asmenims (klientams). Kol prieiga prie nuorodos buvo panaikinta, dokumentą atsidarė 15 asmenų, 1 asmuo dokumentą pasirašė.	
Sunkumas: didelis (asmenį identifikuojantys duomenys, adreso ir nuosavybės duomenys, asmens kodas, kontaktiniai duomenys).	
Tikimybė: maža (duomenis sužinoję asmenys yra įmonės klientai arba darbuotojai, yra žinomi tikslūs jų kontaktiniai ir tapatybės duomenys). Prieiga prie dokumento operatyviai panaikinta.	
Identifikavimas: tiesioginis, pilnas (vardas, pavardė, asmens kodas, gyv. vietos adresas).	
Pavojaus mažinimas: dokumento nuoroda ir prieiga prie dokumento skubiai pašalinta, aktyvi buvo tik 53 min. Nustatyta sistemos programavimo klaida ir funkcija, kurios veikimas sutriko.	
Papildomai: Parengti sistemos programinio kodo pataisymus ir po testavimo įdiegti į sistemą.	
KYLA PAVOJUS	Reikia dokumentuoti ADSP, pranešti VDAI per 72 val. Duomenų subjektų informuoti nereikia.

ADSP pavyzdys Nr. 3

Darbuotojo el. pašto paskyros kompromitavimas (sukčiavimo ataka)	
Situacija: Darbuotojas paspaudė sukčiavimo laiške pateiktą nuorodą, suvedė prisijungimo duomenis, dėl to buvo kompromituota darbuotojo el. pašto paskyra. Kompromituotoje el. pašto paskyroje buvo klientų, tiekėjų ir kitų asmenų vardai, pavardės, el. pašto adresai bei darbinės korespondencijos turinys.	
Sunkumas: vidutinis (pašto dėžutėje buvo klientų, partnerių ir darbuotojų kontaktiniai duomenys bei susirašinėjimas, tačiau nebuvo nustatyta specialių kategorijų, finansinių ar autentifikavimo duomenų atskleidimo).	

Tikimybė: vidutinė (nustatyta neautorizuota prieiga prie pašto dėžutės, tačiau techninio tyrimo metu nerasta įrodymų, kad prie paskyros būtų buvę neteisėtai prisijungta).

Identifikavimas: tiesioginis (vardas, pavardė, el. pašto adresas ir kita korespondencijoje esanti informacija leidžia identifikuoti konkretų asmenį).

Pavojaus mažinimas: ribotas (kompromituota el. pašto paskyra buvo nedelsiant užblokuota, pakeistas slaptažodis, nutrauktos aktyvios sesijos, užblokuotas kenkėjiškas URL bei darbuotojo kompiuteryje perinstaliuota operacinė sistema).

Papildomai: darbuotojai buvo operatyviai įspėti nespausti nuorodų, neatidaryti prisegtų įtartinų failų ir prevenciškai inicijuotas slaptažodžių keitimas. Įdiegtas 2FA naudojimas. Taip pat numatyti papildomi darbuotojų mokymai bei pašto serverio konfigūracijos stiprinimas.

**KYLA
PAVOJUS**

Reikia dokumentuoti ADSP, pranešti VDAI per 72 val.
Duomenų subjektų informuoti nereikia.

ADSP pavyzdys Nr. 4

Neteisėtas masinis Nekilnojamojo turto registro (NTR) duomenų nuskaitymas

Situacija: Naudojantis kompromituotomis teisėtų naudotojų paskyromis, per kelis mėnesius iš NTR buvo neteisėtai nuskaityta daugiau kaip 500 tūkst. registro įrašų. Incidento metu tretiesiems asmenims tapo prieinami asmens duomenys, įskaitant vardus, pavardes, asmens kodus, nekilnojamojo turto adresus ir kitą su nuosavybe susijusią informaciją.

Sunkumas: didelis (atskleistas didelis kiekis tiesiogiai identifikuojančių duomenų, įskaitant asmens kodus, taip pat informacija apie asmenų valdomą nekilnojamąjį turtą ir jo vietą).

Tikimybė: didelė (duomenys buvo sistemingai kopijuojami ilgą laiką, nėra galimybės užtikrinti, kad jie nebus panaudoti neteisėtiems tikslams).

Identifikavimas: tiesioginis, pilnas (vardas, pavardė, asmens kodas, nekilnojamojo turto adresas ir kiti registrų duomenys leidžia aiškiai identifikuoti konkretų asmenį).

Pavojaus mažinimas: ribotas (nejmanoma susigrąžinti ar „atšaukti“ jau nuskaitytų duomenų; galima tik blokuoti neteisėtą prieigą, stiprinti prieigos kontrolę ir informuoti paveiktus asmenis).

Papildomai: didesnė tikslinio sukčiavimo, socialinės inžinerijos, tapatybės pasisavinimo ir kitų pažeidimų rizika.

**DIDELIS
PAVOJUS**

Reikia dokumentuoti ADSP, pranešti VDAI per 72 val.
Duomenų subjektus informuoti reikia.

ADSP pavyzdys Nr. 5

Neteisėta prieiga prie informacinės sistemos ir masinis neteisėtas duomenų kopijavimas

Situacija: Piktavaliu asmuo, pasinaudojęs administratoriaus prieiga prie informacinės sistemos, kelias dienas vykdė neteisėtą duomenų kopijavimą ir išsiuntė apie 22 000 sukčiavimo laiškų, apsimesdamas įmonės darbuotoju. Dėl incidento gauta neteisėta prieiga prie klientų ir darbuotojų asmens duomenų (įskaitant vardus, pavardes, el. pašto adresus, telefono numerius, pareigas) bei nukopijuota apie 58 000 duomenų bazės įrašų.

Sunkumas: didelis (pažeistas didelio kiekio asmenų duomenų konfidencialumas; duomenys gali būti panaudoti sukčiavimui, apsietimui kitu asmeniu ir duomenų išviliojimo atakoms).

Tikimybė: didelė (nustatyta, kad duomenys faktiškai buvo nukopijuoti, o nutekinta informacija jau panaudota organizuojant masinę duomenų išviliojimo kampaniją).

Identifikavimas: tiesioginis (vardas, pavardė, el. pašto adresas, telefono numeris, pareigos ir kita kontaktinė informacija leidžia tiesiogiai identifikuoti duomenų subjektą).

Pavojaus mažinimas: ribotas (duomenų išviliojimo kampanijos sustabdytos, pakeisti slaptažodžiai, apribota prieiga prie sistemos, tačiau neįmanoma atšaukti jau nukopijuotų duomenų ir išsiųstų laiškų).

Papildomai: sustiprinta prieigos kontrolė, apribota prieiga prie informacinės sistemos pagal IP adresus, mažinamas privilegijuotų naudotojų skaičius, įdiegtas dviejų veiksmų autentifikavimas (2FA).

DIDELIS PAVOJUS	Reikia dokumentuoti ADSP, pranešti VDAI per 72 val. Duomenų subjektus (darbuotojus ir klientus) informuoti reikia.
----------------------------	---

6.2. DI technologijų poveikis ADSP keliamo pavojaus lygio nustatymui

Dirbtinio intelekto (DI) technologijų plėtra keičia ne pačią ADSP pavojaus vertinimo tvarką, bet aplinkybes, kuriomis jis atliekamas. Vertinant ADSP keliamą pavojų svarbiausia atsakyti, ar iš pažeistų duomenų gali kilti žala asmenims. DI mažina kliūtis, skiriančias duomenų atskleidimą nuo žalos: automatizuoti ir dažnai patikimai atrodantys sukčiavimo laiškai, potencialių taikinių atranka pagal nutekėjusią informaciją ir kalbos barjerų nebuvimas leidžia mažesnėmis sąnaudomis ir didesniu mastu vykdyti įtikinamas socialinės inžinerijos atakas. Todėl kai kuriais atvejais ta pati duomenų grupė šiandien gali kelti didesnę žalą tikimybę nei prieš keletą metų.

Antra, DI keičia identifikavimo lengvumą ir duomenų jautrumo vertinimą. DI įrankiai geba susieti skirtingų šaltinių duomenų grupes, išgauti informaciją iš nestruktūruotų dokumentų, nuotraukų, garso įrašų ar komunikacijos ir sudaryti asmens profilį, kurio nebūtų galima sudaryti rankiniu būdu. Dėl to duomenys, kurie pavieniui vertinami kaip mažo ar vidutinio jautrumo (pavyzdžiui, vardas, pavardė, kontaktiniai duomenys, elgsenos duomenys), kartu su kitais nutekėjusiais ar viešais duomenimis gali padaryti didesnę žalą. Ypač tai aktualu, kai ADSP metu atskleidžiami dideli neanonimizuoti tekstiniai, garso ar vaizdo archyvai, nes iš jų DI gali išgauti jautrią informaciją, kurios duomenų valdytojas duomenų tvarkymo metu nefiksavo.

Trečia, DI pabrėžia poreikį įvertinti ilgalaikį scenarijų. Nutekėję duomenys gali būti saugomi ir naudojami vėliau, kai atsiranda pigesnių ar galingesnių analizės įrankių, todėl trumpuoju laikotarpiu žemos tikimybės vertinimas gali nebeatitikti realybės po keleto mėnesių ar metų. Tokiu atveju svarbu ne tik įvertinti pirminę ADSP situaciją, bet ir dokumentuoti prielaidas apie piktavalių asmens galimybes bei periodiškai peržiūrėti vertinimą, jei atsiranda naujų faktų. Tai ypač aktualu šifruotiems duomenims: šiandien stiprus šifravimas laikomas patikima apsauga, bet algoritmų patikimumas laikui bėgant gali keistis (pavyzdžiui, dėl kvantinių kompiuterių pažangos), todėl reikėtų atsižvelgti į šifravimo algoritmo brandą ir raktų valdymo praktiką.

7. Aktualūs EDAV metodiniai dokumentai

- EDAV Gairės Nr. [9/2022](#) „Dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal BDAR“ (2.0 versija);
- EDAV Gairės Nr. [01/2021](#) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą pavyzdžių“.