VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

# ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI LIETUVOJE 2026 M. I PUSM.

Asmens duomenų saugumo pažeidimas (toliau – ADSP) – 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 (Bendrojo duomenų apsaugos reglamento (toliau – BDAR) 4 straipsnio 12 punktas).

Pranešimai apie ADSP teikiami Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) ir duomenų subjektams, vadovaujantis BDAR 33 ir 34 straipsniais.

VDAI apie ADSP privalo pranešti visi duomenų valdytojai pateikdami pranešimą apie ADSP, išskyrus, kai tikėtina, kad toks ADSP nekels pavojaus asmenų teisėms ir laisvėms. Kai dėl ADSP pobūdžio ir rizikos rimtumo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas apie ADSP privalo pranešti ir duomenų subjektams.

2026 m. I pusm. VDAI buvo gauta 140 pranešimų apie ADSP, Lietuvoje paveiktų duomenų subjektų skaičius – 1 647 399. 2026 m. I pusm. dėl kibernetinių incidentų buvo paveikti net 75 proc., t. y. 1 235 050 (iš visų 2026 m. I pusm. paveiktų duomenų subjektų), duomenų subjektų duomenys, dėl kitų priežasčių buvo paveikti 25 proc. (412 349) duomenų subjektų duomenys (Diagrama Nr. 1).

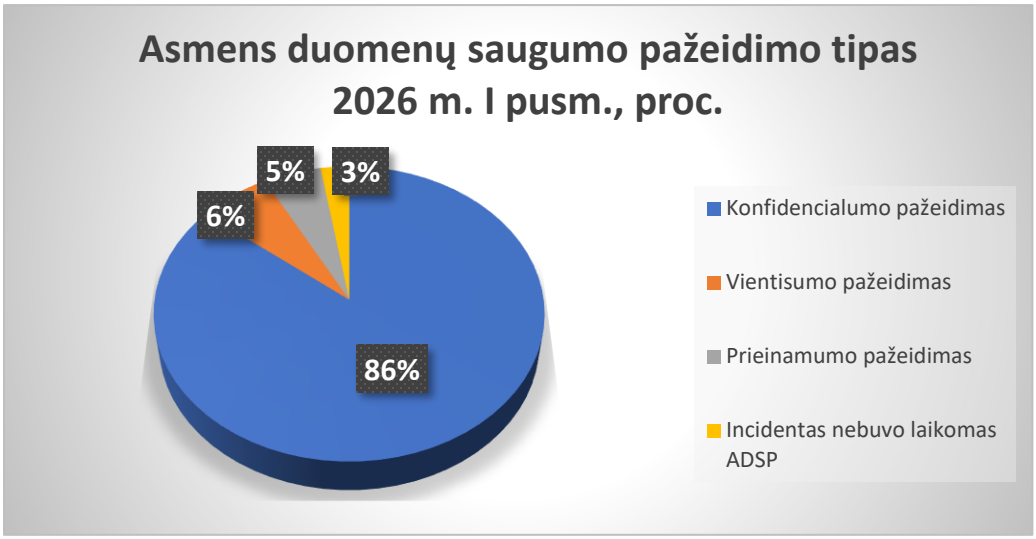
***Diagrama Nr. 1***


Pagal ADSP pobūdį Lietuvoje statistiškai vyrauja konfidencialumo pažeidimai, kurių skaičius per 2026 m. I pusm. sudarė net 87 proc. (visų atvejų), 7 proc. atvejų sudarė vientisumo pažeidimai, 5 proc. atvejų –

prieinamumo pažeidimai ir 1 proc. atvejų incidentas nebuvo laikomas ADSP (neatitiko sąvokos) (Diagrama Nr. 2).

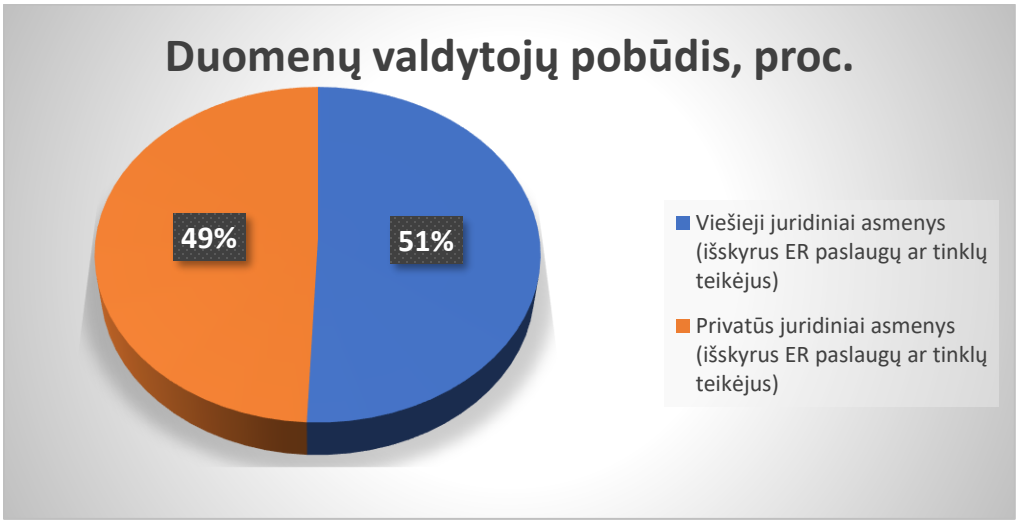
VDAI, įvertinusi gautus pranešimus apie incidentus, kurie nėra laikomi ADSP, nustatė, kad tokie pranešimai buvo susiję su naujienlaiškių siuntimu be asmens sutikimo. Pažymėtina, kad VDAI 2025-09-10 paskelbtame atnaujintame atvejų, kurie nelaikomi ADSP, apibendrinime yra nurodyta, kad toks atvejis nelaikytinas ADSP, atitinkamai, duomenų valdytojui nekyla pareiga informuoti VDAI.

***Diagrama Nr. 2***




2026 m. I pusm. daugiausia ADSP pranešimų gauta iš viešųjų juridinių asmenų – 51 proc., iš privačių juridinių asmenų – 49 proc., 2026 m. I pusm. nebuvo gauta pranešimų apie ADSP iš elektroninių ryšių paslaugų ar tinklų teikėjų (Diagrama Nr. 3).

***Diagrama Nr. 3***



## ADSP TENDENCIJOS 2026 M. I PUSM.

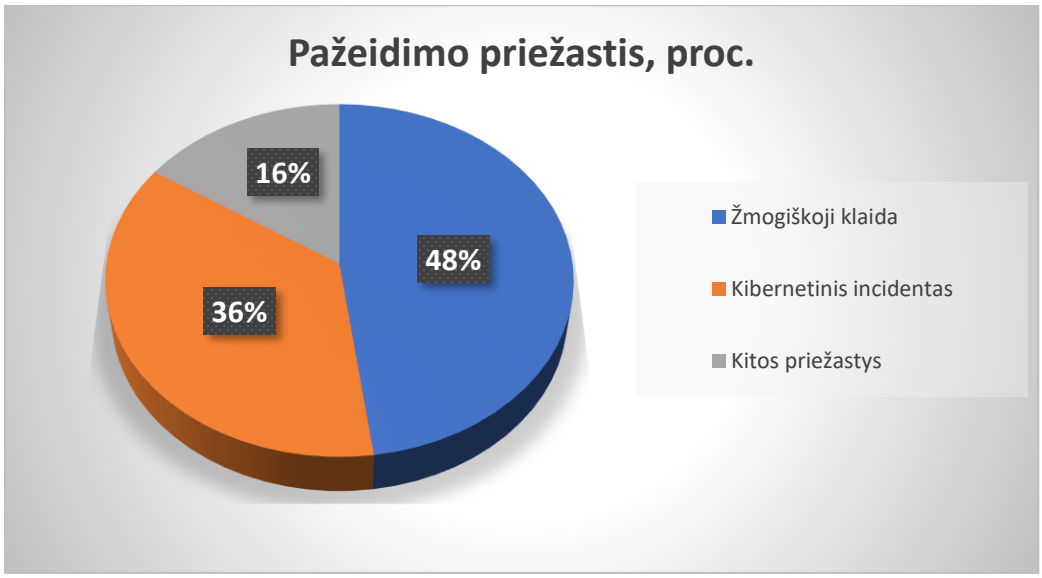
VDAI, išanalizavusi per 2026 m. I pusm. gautus pranešimus apie ADSP, nustatė, kad 51 (36 proc.) ADSP įvyko dėl kibernetinių incidentų (duomenų užšifravimo ir išpirkos reikalavimo, socialinės inžinerijos metodais paremtų atakų, taip pat SQL injekcijų atakos ir kt.) (Diagrama Nr. 4).

2026 m. I pusm. 67 (48 proc.) ADSP įvyko dėl žmogiškosios klaidos (Diagrama Nr. 4). Aptariami ADSP įvyksta dėl žmogaus padaromų veiksmų, kurie pasireiškia neapdairumu, nežinojimu, kad veiksmai gali sukelti ADSP, taip pat dėl veiksmų, nuo kurių įprastai apsaugoti negali taikomos techninės ir organizacinės priemonės, pavyzdžiui, el. pašto adresų įrašymas į „Kopija“ (angl. *CC*), o ne „Nematoma kopija“ (angl. *BCC*), dokumentų su asmens duomenimis siuntimas netinkamiems adresatams, netinkamai nuasmeninto dokumento paviešinimas ir kt.

Nors ADSP įvykę dėl žmogiškosios klaidos dažniausiai nėra tyčiniai, jie gali sukelti reikšmingą riziką duomenų subjektų teisėms ir laisvėms, įskaitant konfidencialios informacijos atskleidimą, tapatybės vagystės ar finansinių nuostolių grėsmę. Todėl siekiant mažinti tokių incidentų tikimybę, būtina nuolat ugdyti darbuotojų sąmoningumą duomenų apsaugos srityje, taikyti aiškias procedūras bei reguliariai vykdyti mokymus.

2026 m. I pusm. 22 (16 proc.) ADSP įvyko dėl kitų priežasčių (Diagrama Nr. 4): t. y. įvairūs IT sistemų trikdžiai, kilę dėl IT sistemų klaidų, dėl kurių atnaujinti duomenys nebuvo laiku perduoti, todėl duomenų valdytojai negalėjo laiku suteikti paslaugų. Taip pat nustatyta, kad netinkamai atlikti programavimo darbai arba neatliktas sistemų testavimas, prieš pradedant jas eksploatuoti, tai sudarė sąlygas situacijoms, kai asmens duomenys buvo prieinami neturintiems teisės su jais susipažinti asmenims.

***Diagrama Nr. 4***



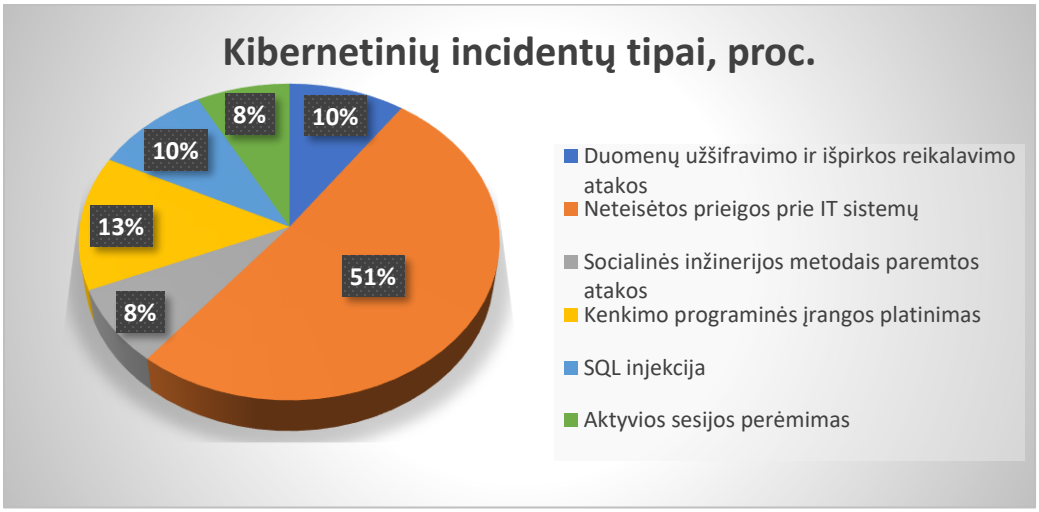

2026 m. I pusm. ADSP įvyko dėl šių kibernetinių incidentų (Diagrama Nr. 5):

- dėl duomenų užšifravimo ir išpirkos reikalavimo atakų (angl. *Ransomware*), t. y. buvo ne tik užšifruoti serveriai, buhalterinės programos ir kitos sistemos, bet prieš duomenų užšifravimą

įsilaužėliai juos nukopijavo ir reikalavo išpirkos už duomenų dešifravimą, grasindami nukopijuotus asmens duomenis paskelbti tamsiojo interneto forumuose (angl. *Dark Web Forums)*;

- piktavaliams neteisėtai prisijungus prie IT sistemų, t. y. pasinaudojus viešai prieinamais prisijungimo duomenimis, išnaudojus pažeidžiamumus ir kita, buvo gautos prieigos prie asmens duomenų, taip pažeidžiant jų konfidencialumą;
- dėl socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) metodais paremtų atakų, siekiant išvilioti įvairiausius prisijungimų duomenis ar kitus asmens duomenis, pasitelkiant gerai apgalvotus scenarijus;
- dėl perimtų aktyvių sesijų (angl. *Session Hijacking*), kurių metu neteisėtai perimama teisėto naudotojo aktyvi autentifikavimo sesija, siekiant įgyti prieigą prie informacinės sistemos, elektroninės paslaugos ar joje tvarkomų duomenų. Tokios atakos metu piktavalis pasinaudoja galiojančiu sesijos identifikatoriumi, autentifikavimo žetonu ar kitomis sesijos valdymo priemonėmis ir vykdo veiksmus teisėto naudotojo vardu;
- dėl kenkimo programinės įrangos platinimo kibernetinių atakų, kurių metu į informacines sistemas, įrenginius ar tinklus įdiegiama arba platinama kenkėjiška programinė įranga, siekiant neteisėtai gauti prieigą prie duomenų, sutrikdyti sistemų veiklą, sunaikinti ar pakeisti informaciją, užšifruoti duomenis arba sudaryti sąlygas tolesniems kibernetiniams incidentams;
- Dėl SQL injekcijos (angl. *XSS, Cross-Site Scripting*)atakų.

***Diagrama Nr. 5***




Dėl aktyvios sesijos perėmimo rizikos sumažinimo atskirai paminėtina, kad sesijų identifikatoriai turi būti generuojami naudojant saugias ir sunkiai nuspėjamas reikšmes, po naudotojo autentifikavimo turi būti sukuriamas naujas sesijos identifikatorius, o naudotojui atsijungus arba pasibaigus sesijos galiojimo laikui visi su sesija susiję identifikatoriai turi būti nedelsiant panaikinami. Taip pat turi būti nustatytas automatinis sesijos užbaigimas po nustatyto neaktyvumo laikotarpio, užtikrinama aktyvių sesijų registracija ir stebėsena bei sudaryta galimybė nedelsiant nutraukti aktyvias sesijas įtarus

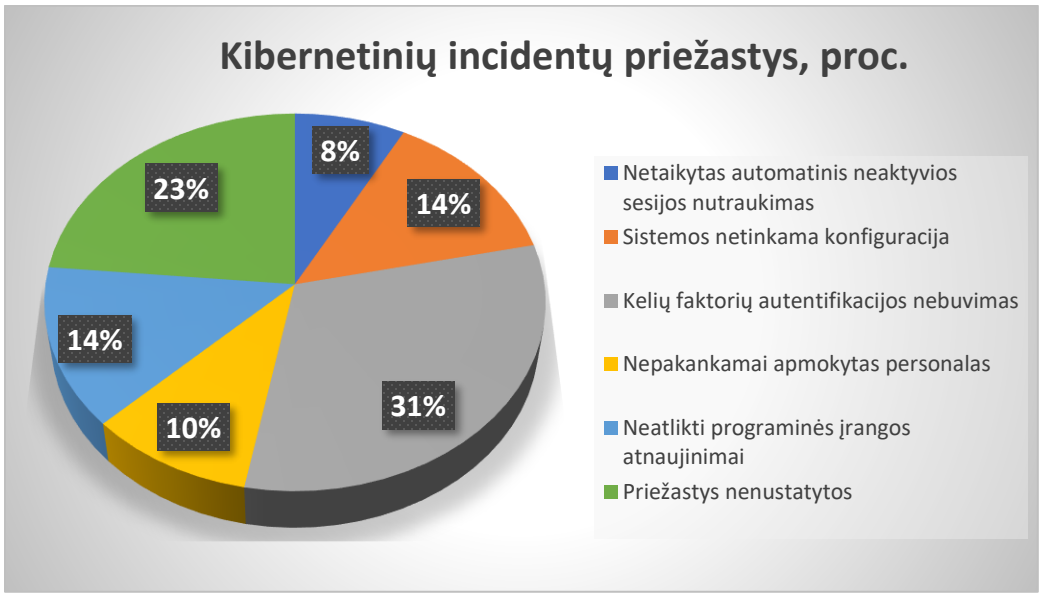
saugumo incidentą. Taigi šiomis priemonėmis informacinėje sistemoje turi būti užtikrinamas saugus sesijų valdymas.

## KIBERNETINIŲ INCIDENTŲ, DĖL KURIŲ ĮVYKO ADSP, PRIEŽASTYS

2026 m. I pusm. ADSP metu viena pagrindinių ADSP priežasčių išlieka nepakankamai efektyvus prieigų valdymas. Dažniausiai nustatomos spragos yra susijusios su kelių veiksnių autentifikavimo (angl. *MFA*) nenaudojimu, nepakankamu prisijungimų ribojimu pagal IP adresus, reguliarios naudotojų ir administratorių paskyrų peržiūros nevykdymu bei laiku nešalinamomis nebenaudojamomis paskyromis. Šių ADSP priežasčių pašalinimas yra esminės priemonės siekiant sumažinti neteisėtos prieigos riziką (atsižvelgiant į gautų pranešimų apie ADSP turinį).

Statistika rodo, kad pagrindinės kibernetinių incidentų priežastys, dėl kurių įvyko ADSP yra kelių faktorių autentifikacijos nebuvimas bei reguliariai ir nedelsiant neatliekami programinės įrangos atnaujinimai (Diagrama Nr. 6).

***Diagrama Nr. 6***




Papildomi faktoriai, dėl kurių įvyko ADSP:

- nevykdoma kompiuterių tinklų duomenų srautų stebėsena, nevykdomas įsilaužimų aptikimas ir prevencija;
- netinkami serverio nustatymai ir taisyklės;
- nevykdoma prieigos kontrolė;
- perteklinis privilegijuotų teisių naudojimas;
- nėra taikomas IP filtravimas;
- neatliekama reguliari naudotojų ir administratorių paskyrų peržiūra;
- nenaudojamos administratorių paskyros nėra nedelsiant panaikinamos arba deaktyvuojamos;

- naršyklėse saugomi prisijungimo duomenys;
- naudojami slaptažodžiai nėra stiprūs ir kompleksiški;
- naudojami slaptažodžiai nėra reguliariai keičiami.

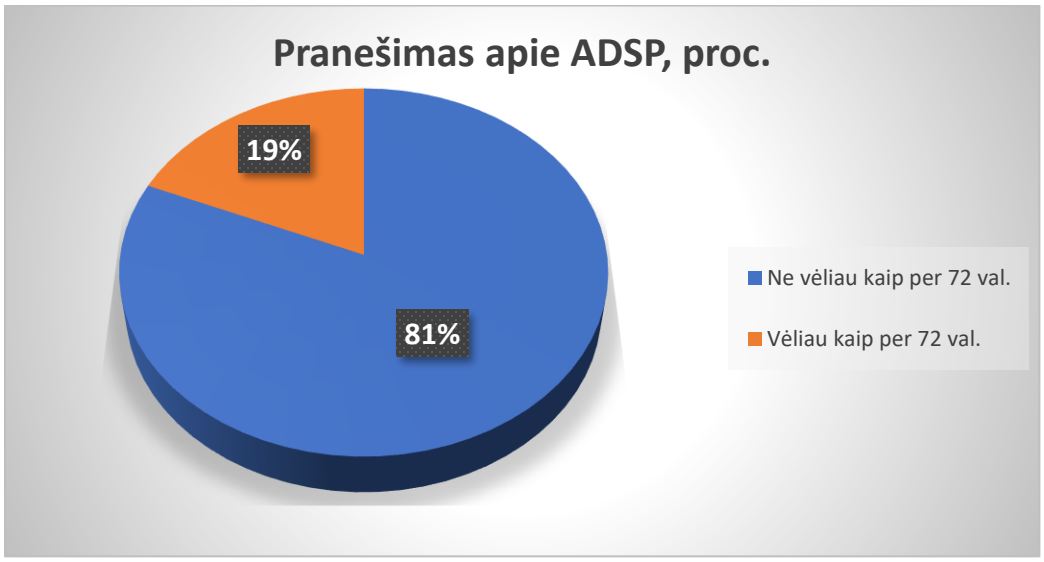
Papildomai atkreiptinas dėmesys, kad net 23 proc. atvejų iš visų 2026 m. I pusm. gautų pranešimų apie ADSP (įvykusių dėl kibernetinių incidentų) nebuvo nustatytos incidento priežastys (Diagrama Nr. 6). Šis rodiklis rodo, kad dažnai pasitaiko atvejų, kai įvykus kibernetiniam incidentui duomenų valdytojai ar duomenų tvarkytojai negalėjo tinkamai atlikti kibernetinio incidento tyrimo ir nustatyti priežastis, kurių išaiškinimas galėtų ateityje padėti išvengti tokio pobūdžio atakų. Taip atsitinka dėl to, kad žurnaliniai įrašai yra saugomi per trumpą laiką, saugomi tame pačiame serveryje arba nėra taikomos priemonės, apribojančios galimybę žurnalinius įrašus ištrinti, sugadinti ar pakeisti.

## PRANEŠIMŲ APIE ADSP TEIKIMAS PRIEŽIŪROS INSTITUCIJAI

VDAI atkreipia dėmesį, kad nustatęs, jog įvyko ADSP ir yra pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas nedelsdamas, ne vėliau kaip per 72 val. nuo sužinojimo apie ADSP, privalo pranešti apie tai VDAI, kaip tai numato BDAR.

2026 m. I pusm. 81 proc. duomenų valdytojų apie įvykusį ADSP pranešė laiku, t. y. ne vėliau kaip per 72 val., 19 proc. – vėliau kaip per 72 val. (Diagrama Nr. 7).

***Diagrama Nr. 7***




Išanalizavus ADSP pranešimus, kurie pateikti vėliau nei per 72 val. nuo sužinojimo apie ADSP momento, nustatyta, kad duomenų valdytojai kartais nenurodo vėlavimo priežasčių (BDAR 33 straipsnio 1 dalis). Taip pat paminėtina, kad dažniausia pranešimo VDAI vėlavimo priežastis – duomenų valdytojas ilgai aiškinasi ADSP aplinkybes ir duomenų subjektams keliamą pavojų. VDAI atkreipia dėmesį, kad duomenų valdytojai, nustatę, kad ADSP yra sudėtingas ir jo tyrimas užtruks (jei duomenų valdytojas nustato, kad per 72 val. visos informacijos pateikti negalės), **pranešimus gali teikti dalimis**, t. y. pirminis pranešimas

turi būti teikiamas iškart sužinojus apie įvykusį ADSP, jame nurodant, kad tai yra pirminis pranešimas ir papildoma informacija bus pateikta vėliau.

Taip pat dažnai pasitaiko, kad duomenų valdytojai, teikdami pranešimus VDAI, nenurodo visos būtinos pateikti informacijos, kaip tai numato BDAR 33 straipsnio 3 dalis.

Pranešimuose apie įvykusį ADSP, turi būti nurodoma:

- asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;
- duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;
- tikėtinos asmens duomenų saugumo pažeidimo pasekmės;
- priemonės, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas ADSP, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

Atsižvelgdama į tai, VDAI rekomenduoja naudoti VDAI patvirtintą pranešimo apie ADSP formą ir pildant pranešimą pateikti išsamią informaciją apie įvykusį ADSP.

Taip pat pasitaiko atvejų, kad duomenų valdytojai, negalėdami nurodyti privalomos informacijos, nurodo, kad buvo pradėtas tyrimas dėl ADSP ar kibernetinio incidento ir iki pranešimo teikimo dienos jis nėra baigtas. Atsižvelgiant į tai, teikiant pirminius pranešimus VDAI, siūloma nurodyti, kada planuojama pradėtą tyrimą baigti.

## PRANEŠIMŲ APIE ADSP TEIKIMAS DUOMENŲ SUBJKETAMS

VDAI atkreipia dėmesį, kad remiantis BDAR 34 straipsnio 1 dalimi, nustatęs, jog įvykęs ADSP gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms, duomenų valdytojas nepagrįstai nedelsdamas turi pranešti apie ADSP duomenų subjektui.

Pranešimuose duomenų subjektui turi būti aiškia ir paprasta kalba aprašomas asmens duomenų saugumo pažeidimo pobūdis ir pateikiama bent BDAR 33 straipsnio 3 dalies b, c ir d punktuose nurodyta informacija ir priemonės:

- duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;
- tikėtinos asmens duomenų saugumo pažeidimo pasekmės;
- priemonės, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas ADSP, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

Taip pat pasitaiko, kad duomenų valdytojai, teikdami pranešimus duomenų subjektams, nenurodo visos būtinos pateikti informacijos:

- nėra nurodoma, kokių veiksmų pats duomenų subjektas gali imtis, kad sumažintų ADSP pasekmes (pavyzdžiui, blokuotų kredito kortelę ir pan.);
- nenurodomi duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, duomenys (pavyzdžiui, privalo būti pateiktas ir kontaktinio asmens vardas bei pavardė);
- informacija apie įvykusį ADSP duomenų subjektui pateikiama sudėtinga kalba, naudojant sudėtingus terminus ir pan.;
- nėra aprašomos tikėtinos ADSP pasekmės;
- nėra aprašomos priemonės, kurių ėmėsi duomenų valdytojas, kad būtų pašalintas ADSP.

## 2026 M. I PUSM. DUOMENŲ VALDYTOJAMS TAIKYTOS POVEIKIO PRIEMONĖS

2026 m. kovo mėn. VDAI, atlikusi ADSP tikrinimą, priėmė sprendimą privačiam juridiniam asmeniui, kaip duomenų tvarkytojui, skirti 4 500 eurų baudą už nustatytus BDAR 32 straipsnio 1 dalies b punkto pažeidimus. VDAI nustatė, kad ADSP metu buvo paveikta viešosios debesijos platforma, kai piktavalis užšifravo dalį saugomų atsarginių kopijų ir virtualiuose serveriuose esančių klientų sistemų, tai paveikė 180 fizinių asmenų duomenis. Šiuo atveju duomenų tvarkytojas neužtikrino, kad jungimuisi iš vidinio tinklo būtų įdiegtas prieigos ribojimas tik įgaliotiems asmenims, jungimuisi prie vidinio tinklo nebuvo įdiegtas virtualus privatus tinklas (angl. VPN), išoriniams prisijungimams nebuvo taikomas kelių faktorių autentifikavimas (angl. MFA), taip pat nebuvo užtikrinta griežta virtualiųjų mašinų izoliacija tiek tinklo, tiek prieigos aspektais.

2026 m. birželio mėn. VDAI, atlikusi dviejų ADSP tikrinimus, priėmė sprendimą sveikatos priežiūros paslaugas teikiančiai įmonei skirti 450 tūkst. eurų baudą už nustatytus BDAR 5 straipsnio 1 dalies f punkto ir 32 straipsnio 1 dalies b ir d punktų pažeidimus. VDAI nustatė, kad pirmojo ADSP metu piktavalis, pasinaudodamas darbuotojo prisijungimo duomenimis, prisijungė prie informacinės sistemos ir peržiūrėjo 63 pacientų duomenis. Antrojo ADSP metu pasinaudojus privilegijuotas prieigos teises turinčia paskyra, buvo įsilaužta į bendrovės sistemas ir jose esančius duomenis užšifravus, paveikiant beveik 400 tūkst. duomenų subjektų asmens duomenis. Abiejų ADSP atvejais duomenų valdytojas neužtikrino, kad jungimuisi iš išorės būtų įdiegtas prieigos ribojimas tik įgaliotiems asmenims, išoriniams prisijungimams nebuvo taikomas kelių faktorių autentifikavimas (angl. MFA).

2026 m. I pusm. VDAI, įvertinusi gautus pranešimus apie ADSP ir nustačiusi, kad yra netinkamai užtikrinamas duomenų subjektų asmens duomenų saugumas, vadovaudamasi teisės aktų nuostatomis teikė 11 nurodymų duomenų valdytojams arba duomenų tvarkytojams suderinti duomenų tvarkymo operacijas su BDAR nuostatomis. Taip pat teikė 3 rekomendacijas duomenų valdytojams, kurios padės užtikrinti, kad asmens duomenų tvarkymas atitiktų BDAR reikalavimus.

---