VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI LIETUVOJE 2024 M.

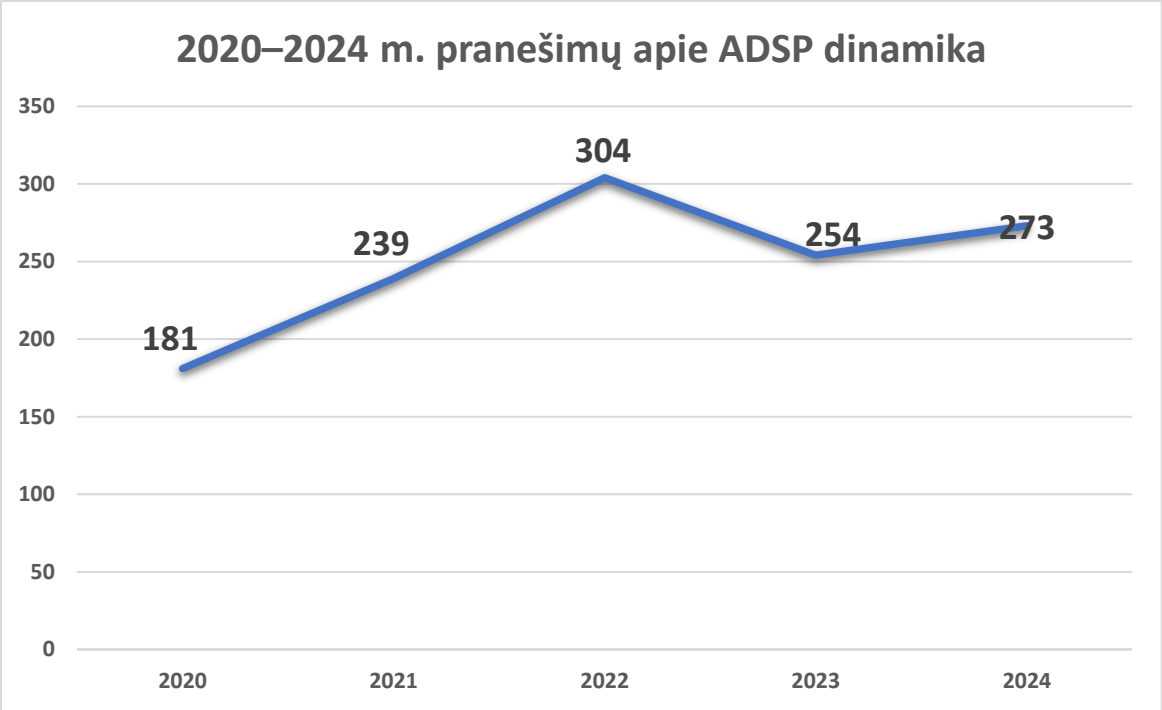
Asmens duomenų saugumo pažeidimas (toliau – ADSP) – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (Bendrojo duomenų apsaugos reglamento (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.

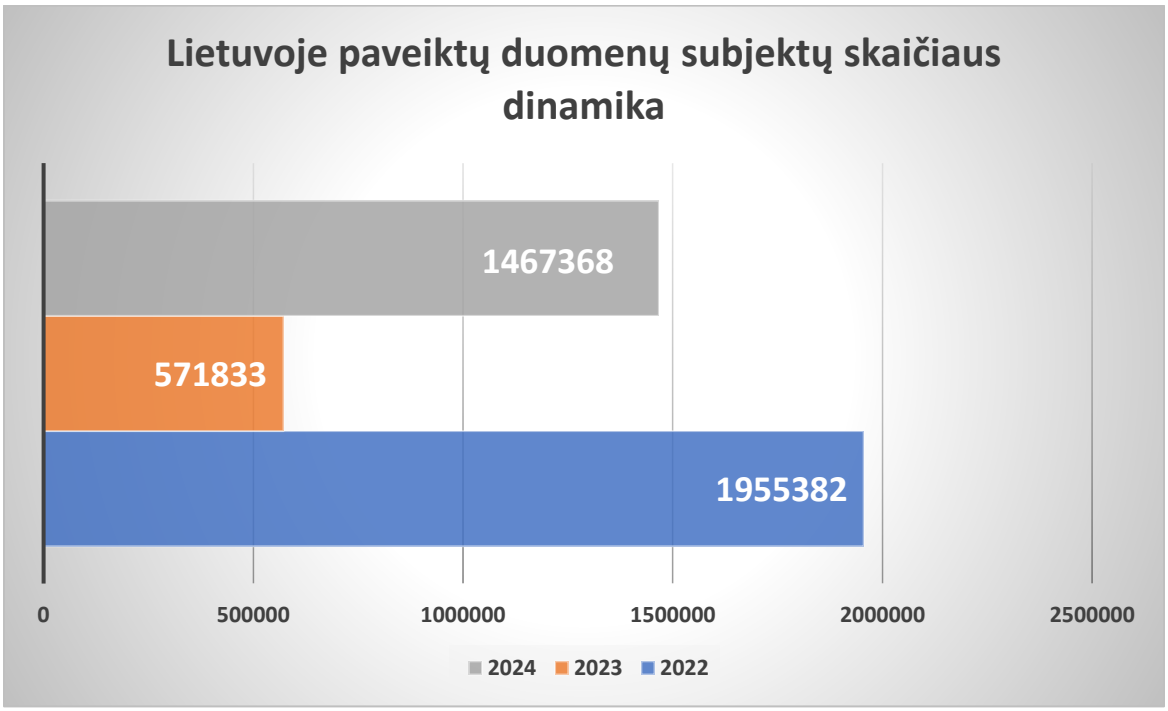
VDAI apie ADSP privalo pranešti visi duomenų valdytojai pateikdami pranešimą apie ADSP, išskyrus, kai tikėtina, kad toks ADSP nekels pavojaus asmenų teisėms ir laisvėms. Kai dėl ADSP pobūdžio ir rizikos rimtumo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas apie ADSP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

2024 m. VDAI buvo gauti 273 pranešimai apie ADSP (žr. 1 diagrama). Šių pranešimų duomenimis, Lietuvoje paveiktų duomenų subjektų skaičius – 1 467 368 (žr. 2 diagrama). Palyginti su ankstesnių metų duomenimis, 2024 m. VDAI gavo daugiau pranešimų apie ADSP negu 2023 m. (2023 m. VDAI gautų pranešimų apie ADSP – 254), pokytis nėra ženklus, todėl negalima daryti prielaidos, kad keliančių pavojų asmenims ADSP skaičius Lietuvoje išaugo. Pastebėtina, kad beveik 3 kartus padidėjo Lietuvoje paveiktų duomenų subjektų skaičius (2023 m. Lietuvoje paveiktų duomenų subjektų skaičius – 571 833), tai lėmė didesnis skaičius ADSP, kurie įvyko dėl kibernetinio incidento ir kurių metu buvo paveiktas didelis skaičius duomenų subjektų, pavyzdžiui, 2024 m. įvyko 1 kibernetinis incidentas, kurio metu buvo paveikti 250 768 duomenų subjektai.

1 diagrama.



2 diagrama.



Svarbu paminėti, kad dėl kibernetinių incidentų buvo paveikti 49 proc., t. y. 712 881 (iš visų 2024 m. paveiktų duomenų subjektų), duomenų subjektų duomenys, dėl kitų priežasčių buvo paveikti 51 proc. (754 487) duomenų subjektų duomenys (žr. 3 diagrama).

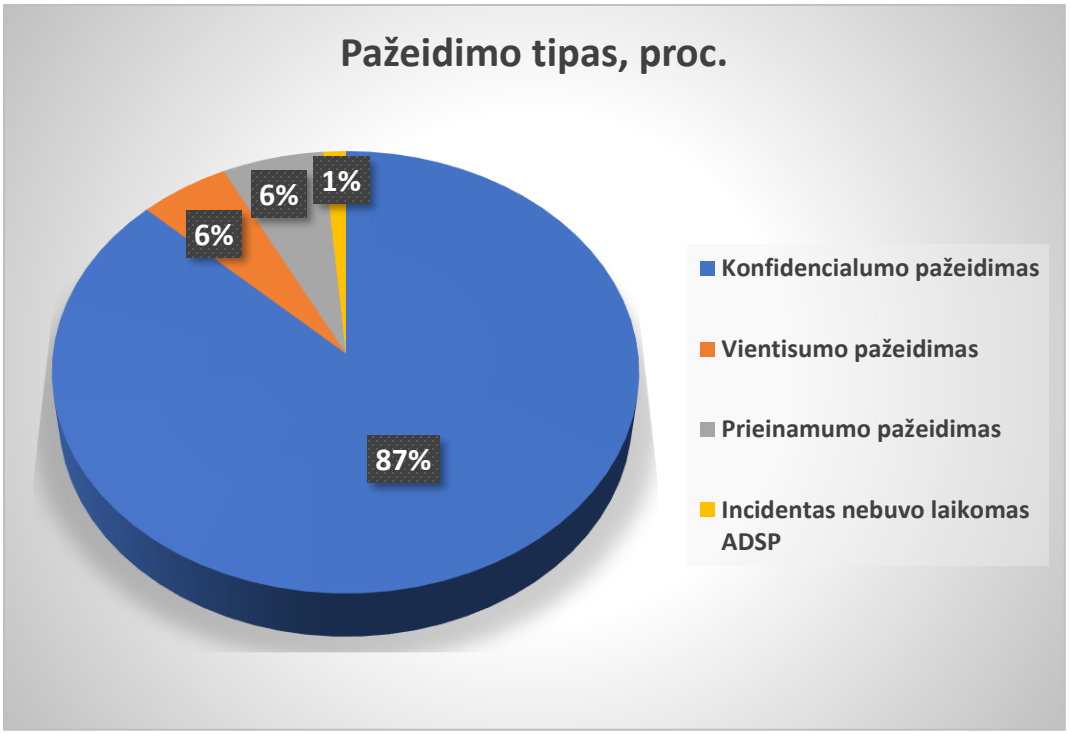
3 diagrama.

Pagal ADSP pobūdį Lietuvoje statistiškai vyrauja konfidencialumo pažeidimai, kurių skaičius 2024 m. sudarė net 87 proc. visų atvejų (2023 m. sudarė 76 proc.), 6 proc. atvejų sudarė vientisumo pažeidimai (2023 m. sudarė 10 proc.), dar 6 proc. atvejų – prieinamumo pažeidimai (2023 m. sudarė 10 proc.) ir 1 proc. atvejų incidentas nebuvo laikomas ADSP (neatitiko sąvokos) (2023 m. sudarė 4 proc.) (žr. 4 diagrama).

Papildomai atkreiptinas dėmesys, kad VDAI 2024-01-11 paskelbė atvejų, kurie nelaikomi ADSP[1], apibendrinimą. Pastebėtina, kad duomenų valdytojai 2024 m. nepateikė pranešimų apie atvejus, kurie yra aprašyti apibendrinime.

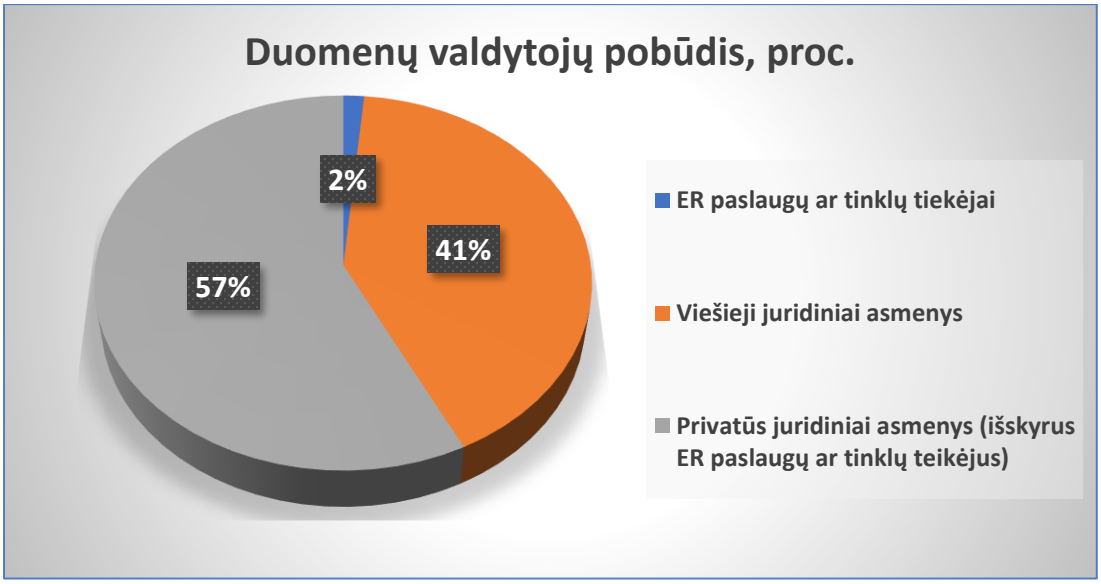
[1] https://vdai.lrv.lt/lt/naujienos/vdai-pataria-del-pasitaikanciu-atveju-kai-pranesama-apie-ivykusius-incidentus-kurie-nera-laikomi-asmens-duomenu-saugumo-pazeidimais/

4 diagrama.



2024 m. daugiausia pranešimų apie ADSP buvo gauta iš privačių juridinių asmenų – 57 proc., iš viešųjų juridinių asmenų – 41 proc. ir 2 proc. – iš elektroninių ryšių paslaugų ar tinklų teikėjų (žr. 5 diagrama). Papildomai pažymėtina, kad 2023 m. ADSP pranešimų, gautų iš privačių juridinių asmenų, buvo tik 38 proc., todėl pastebima tendencija, kad privatūs juridiniai asmenys tampa atsakingesni ir įvykus ADSP informuoja VDAI, kaip to reikalauja BDAR nuostatos.

5 diagrama.



ADSP TENDENCIJOS 2024 M.

VDAI, išanalizavusi 2024 m. gautus pranešimus apie ADSP, nustatė, kad 90 (33 proc.) ADSP įvyko dėl kibernetinių incidentų (duomenų užšifravimo, išpirkos reikalavimo, socialinės inžinerijos metodais paremtų ir kredencialų brukimo kibernetinių atakų ir kt.) (žr. 6 diagrama). Svarbu paminėti, kad 2023 m. VDAI pranešimus apie ADSP dėl kibernetinių incidentų gavo tik 37, t. y. 15 proc. iš visų 2023 m. gautų pranešimų apie ADSP. Atsižvelgiant į tai, pastebima, kad kibernetinių incidentų skaičius turi tendenciją augti.

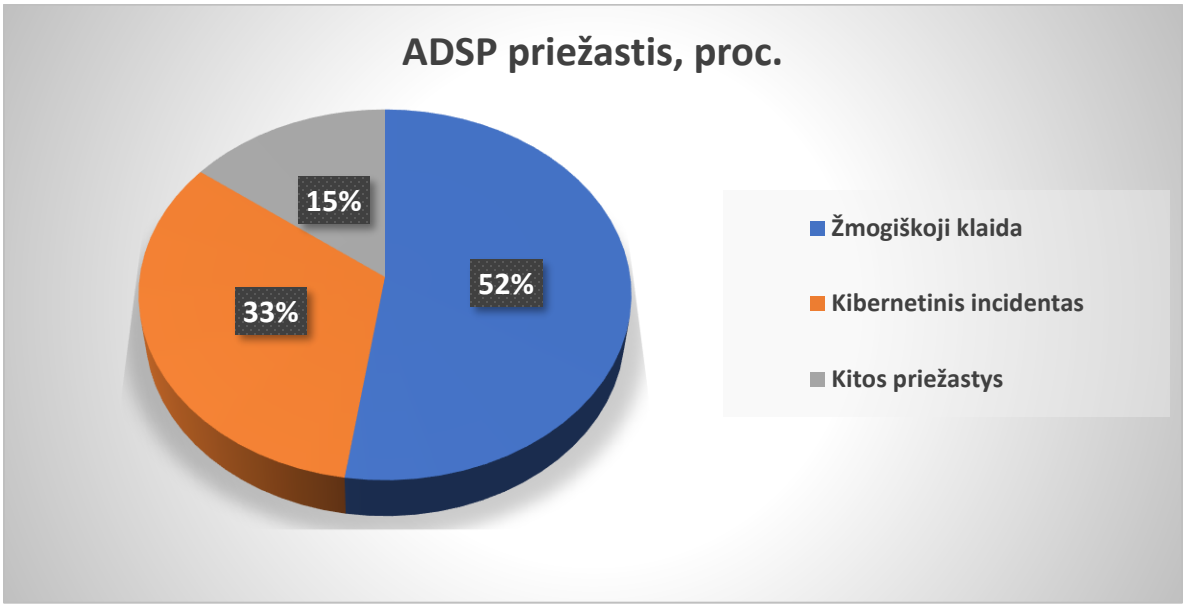
2024 m. 52 proc. ADSP įvyko dėl žmogiškosios klaidos (žr. 6 diagrama) (2023 m. dėl žmogiškosios klaidos – 72 proc.). Aptariami ADSP įvyksta dėl žmogaus padaromų veiksmų, kurie pasireiškia neapdairumu, nežinojimu, kad veiksmai gali sukelti ADSP, taip pat dėl veiksmų, nuo kurių įprastai apsaugoti negali taikomos techninės ir organizacinės priemonės, pavyzdžiui, el. pašto adresų įrašymas į „Kopija“, o ne į „Nematoma kopija“ (ar angl. *Blind Carbon Copy ar BCC*), dokumentų su asmens duomenimis siuntimas netinkamiems adresatams, netinkamai nuasmeninto dokumento paviešinimas ir kt.

VDAI, atsižvelgdama į tai, kad ADSP skaičius dėl žmogiškosios klaidos sumažėjo, tačiau vis tiek ši priežastis, dėl kurios 2024 m. įvyko ADSP, išlieka dažniausia, atkreipia dėmesį, kad darbuotojų mokymai ir darbuotojų supažindinimas su kylančiomis grėsmėmis ir atsakomybėmis yra svarbios priemonės minimizuojant žmogiškąsias klaidas. Mokymai apie duomenų apsaugą svarbūs vykdant prevenciją dėl netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų (BDAR 32 straipsnio 2 dalis). Taip pat efektyvi priemonė užkardant netyčinius asmens duomenų atskleidimo atvejus dėl žmogaus klaidos yra „Keturių akių“ principo įgyvendinimas. Be kita ko, siekdami išvengti ADSP dėl žmogiškosios klaidos, kai asmens duomenys per klaidą yra išsiunčiami netinkamiems adresatams, duomenų valdytojai gali, pavyzdžiui, organizacinėmis ir techninėmis priemonėmis užtikrinti, kad siunčiami failai su asmens duomenimis būtų užšifruoti ir apsaugoti slaptažodžiu (slaptažodis turi būti siunčiamas kitu komunikacijos kanalu arba iš anksto sutartas), el. pašto programinėje įrangoje naudoti gavėjų grupių klasifikatorius (padės užtikrinti siunčiamos informacijos saugumą pagal pritaikytas saugumo politikas, pavyzdžiui, siunčiant dokumentus išorės gavėjams, dokumentai siunčiami šifruoti ir apsaugoti slaptažodžiais bei nustatoma, kiek laiko siunčiami dokumentai gali būti pasiekiami). Taip pat galima naudoti siunčiamų el. laiškų ir jų priedų filtravimą, kurie prieš siunčiant el. laiškus įvertina, ar siunčiamuose el. laiškuose ir jų prieduose nėra tam tikrų duomenų elementų ir kt.

2024 m. ADSP, įvykę dėl kitų priežasčių, sudaro 15 proc. (žr. 6 diagrama): įvairūs IT sistemų trikdžiai, įvykę dėl IT sistemų klaidų, dėl kurių atnaujinti duomenys nebuvo laiku perduoti ir duomenų valdytojai negalėjo laiku suteikti paslaugų, taip pat netinkamai atlikus programavimo

darbus, asmens duomenys buvo pasiekiami asmenims, kurie neturėjo teisės su jais susipažinti ir kt.

6 diagrama.



2024 m. gauta 10 (11 proc.) pranešimų apie ADSP, kurių metu vyko duomenų užšifravimo ir išpirkos reikalavimo atakos (angl. *Ransomware*). Tuo tarpu 66 proc. (59) pranešimų apie ADSP buvo dėl neteisėtai gautos prieigos prie IT sistemų (pastebėta, kad tokie incidentai dažnai įvykdavo darbuotojams išsaugojus IT sistemų prisijungimo duomenis naršyklėse) (žr. 7 diagrama).

Pastebima, kad 2024 m. 18 proc. (16) iš visų įvykusių kibernetinių incidentų buvo dėl socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) metodais paremtų atakų, siekiant išvilioti įvairiausius prisijungimų duomenis ar kitus asmens duomenis, pasitelkiant gerai apgalvotus scenarijus. Palyginus su 2023 m. gautais pranešimais apie ADSP, pastebima, kad 2024 m. buvo vykdomos kredencialų brukimo (angl. *Credential stuffing*) kibernetinės atakos (5 proc. iš visų 2024 m. gautų pranešimų apie ADSP dėl kibernetinių incidentų), kurių metu piktavaliai, pasinaudoję nutekėjusiais duomenimis (pvz., prisijungimo duomenimis), bandė prisijungti prie svetainėse esančių vartotojų paskyrų (žr. 7 diagrama).

7 diagrama.

2024 m. išryškėjo prieigos kontrolės valdymo organizacijų kompiuterių tinkluose spragos, kai suteikiant prieigą nėra taikomi apribojimai, nesilaikoma „mažiausių teisių privilegijos“ ir „būtina žinoti“ principų, netaikomas dviejų ir daugiau veiksnių autentifikavimas aukštesnes teises turintiems, nuotoliniu būdu besijungiantiems ar virtualų privatų tinklą naudojantiems vartotojams.

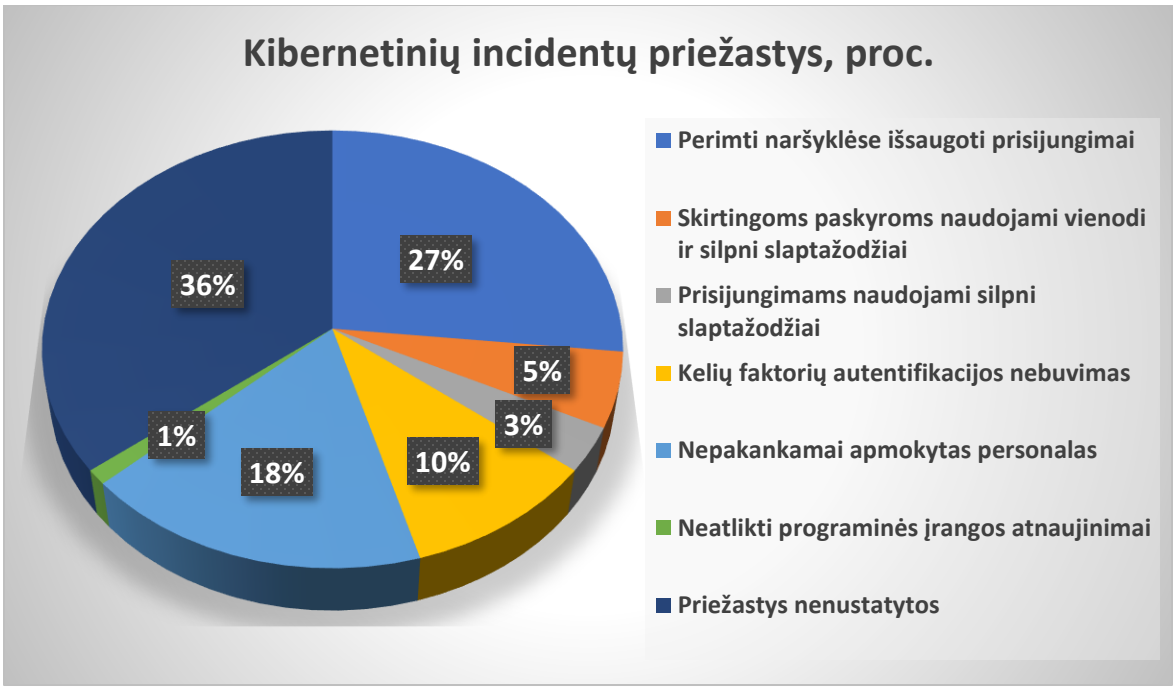
Taip pat pastebima, kad vis dažniau duomenų valdytojams užtikrinant, kad jungiantis prie sistemų, naudotojams būtų taikomas kelių veiksnių autentifikavimas, piktavaliai, atsižvelgdami į tai, ieško sprendimų, kaip apeiti kelių veiksnių autentifikavimą. VDAI gauna vis daugiau pranešimų apie ADSP dėl įvykusių kibernetinių incidentų, kurių metu piktavaliams išnaudojus socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) metodus, nesudėtingai pavyksta apeiti kelių veiksnių autentifikavimą. Taip atsitinka, kai darbuotojai nėra tinkamai apmokyti atpažinti kenkėjiškus laiškus ir paspaudę gautas kenkėjiškas nuorodas suveda ne tik savo prisijungimo duomenis, bet ir papildomą autentifikatorių (pavyzdžiui, telefone suveda slaptažodį, kuriuo bus atliktas papildomas autentifikavimas). Atsižvelgdamas į tai, duomenų valdytojas turi užtikrinti, kad būtų taikomos ne tik tinkamos techninės priemonės, kurios padėtų apsaugoti duomenų subjektų asmens duomenis, bet ir organizacinės, tokios kaip nuolatinis darbuotojų švietimas, kad darbuotojai, gavę kenkėjiškus laiškus, juos atpažintų ir neatidarinėtų kenkėjiškų nuorodų ar priedų.

Įvykus duomenų užšifravimo ir išpirkos reikalavimo atakoms, piktavaliai dažnai pašalina duomenų atsarginės kopijas ir įvykių žurnalinius įrašus, kurie buvo saugomi toje pačioje vietoje, kaip ir užšifruoti duomenys, dėl to duomenų valdytojai nebegali lengvai atkurti duomenų prieinamumo bei tinkamai atlikti kibernetinio incidento ir ADSP tyrimo.

Atsižvelgdamas į tai, duomenų valdytojas turi periodiškai daryti pilnas ir dalines atsargines duomenų kopijas (angl. *Backup*) ir saugoti jas geografiškai skirtingose vietose.

KIBERNETINIŲ INCIDENTŲ, DĖL KURIŲ ĮVYKO ADSP, PRIEŽASTYS

8 diagrama.



VDAI pastebi, kad **pagrindinės kibernetinių incidentų priežastys (žr. 8 diagrama):**

- 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;
- naršyklėse saugomi prisijungimo duomenys;
- skirtingoms paskyroms naudojami vienodi slaptažodžiai;
- naudojami slaptažodžiai nėra stiprūs ir kompleksiški;
- naudojami slaptažodžiai nėra reguliariai keičiami;
- kelių faktorių autentifikavimo nebuvimas;
- nepakankamai apmokytas personalas;
- pasenusios programinės įrangos naudojimas.

Papildomai atkreiptinas dėmesys, kad net 36 proc. atvejų visų 2024 m. gautų pranešimų apie ADSP (įvykusių dėl kibernetinių incidentų) nebuvo nustatytos incidento priežastys (žr. 8 diagrama). Šis rodiklis rodo, kad daugiau nei trečdalis duomenų valdytojų, įvykus kibernetiniam incidentui, negebėjo tinkamai atlikti kibernetinio incidento tyrimo ir nustatyti priežastis, kurių išaiškinimas galėtų ateityje padėti išvengti tokio pobūdžio atakų.

Organizacinės ir techninės saugumo priemonės, padedančios išvengti ADSP dėl kibernetinio incidento:

- Užtikrinti įsilaužimų stebėjimą, aptikimą ir užkardymą;
- Užtikrinti periodinį kritinių operacinių sistemos saugos atnaujinimų diegimą;
- Tinkamai sukonfigūruoti išorinėje komunikacijoje dalyvaujančius serverius ir kitą įrangą pagal gerąsias praktikas;
- Apriboti išorinio prisijungimo galimybes tokiais protokolais kaip *Windows Remote Desktop Protocol*, daiktų interneto SSH prievadais ir pan.;
- Prie IT sistemų leisti jungtis tik iš žinomų IP adresų (angl. *Allow List*) arba prisijungimui naudoti virtualaus privataus tinklo technologijas (angl. *Virtual Private Network*, *VPN*);
- Turimuose įrenginiuose įdiegti pažangią antivirusinę programinę įrangą;
- Nenaudoti tų pačių slaptažodžių skirtingoms paskyroms, užtikrinti, kad prisijungimų prie IT sistemų slaptažodžiai būtų saugūs, kompleksiški[2] ir periodiškai keičiami, naudoti kelių lygių autentifikavimą (el. pašto internetinei prieigai, VPN prieigai, paskyroms, kurios turi prieigą prie kritiškai svarbių sistemų);
- Apriboti asmeninių įrenginių darbo funkcijoms naudojimą;
- Įdiegti el. pašto filtravimo mechanizmus, gebančius filtruoti laiškus pagal žinomus grėsmių indikatorius ir specifinius raktažodžius;
- Įdiegti prieigos kontrolę pagal organizacijos saugumo politiką, taikant „mažiausių teisių privilegijos“ ir „būtina žinoti“ principus;
- Periodiškai mokyti darbuotojus apie IT sistemų saugumo reikalavimus;
- Periodiškai organizuoti duomenų viliojimo metodais paremtų atakų simuliacijas.

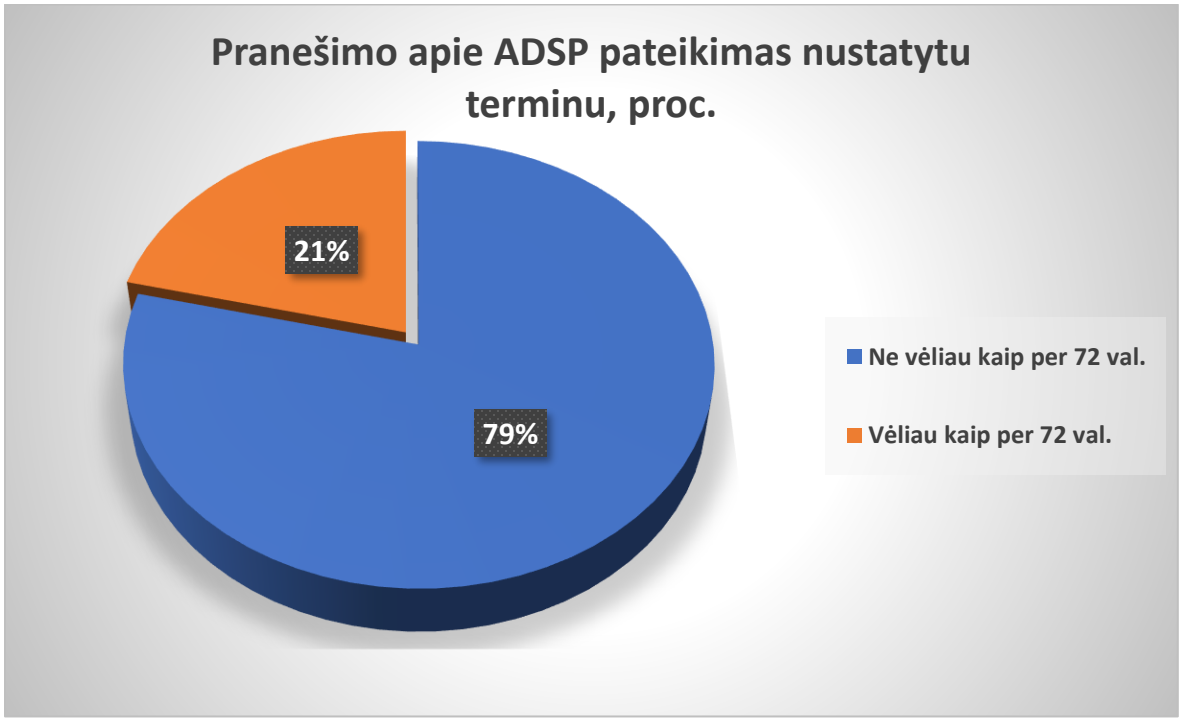
PRANEŠIMŲ APIE ADSP TEIKIMAS PRIEŽIŪROS INSTITUCIJAI

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

[2] Rekomendacija dėl saugių ir stiprių slaptažodžių naudojimo svarbos
https://vdai.lrv.lt/public/canonical/1734937137/678/Rekomendacija_del_slaptazodziu_2024.pdf

2024 m. 79 proc. duomenų valdytojų apie įvykusį ADSP pranešė ne vėliau kaip per 72 val., 21 proc. – vėliau kaip per 72 val. (žr. 9 diagrama). Palyginti su ankstesnių metų duomenimis, duomenų valdytojai teikia tik nežymiai mažiau pranešimų apie ADSP pavėluotai (2023 m. 77 proc. duomenų valdytojų apie įvykusį ADSP pranešė ne vėliau kaip per 72 val., 23 proc. – vėliau kaip per 72 val.).

9 diagrama.



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 pateikimo 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 etapais**, 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 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 asmens duomenų saugumo pažeidimas, 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[3]. Paminėtina, kad nagrinėjant pranešimus apie ADSP vis dažniau aktualu vertinti informaciją apie duomenų valdytojo taikytas technines ir organizacines priemones prieš įvykstant asmens duomenų saugumo pažeidimui, kurios galėjo turėti įtakos, kad asmens duomenų saugumo pažeidimas neįvyktų.

Taip pat pasitaiko atvejų, kad duomenų valdytojai, negalėdami nurodyti privalomos informacijos, nurodo, kad buvo pradėtas tyrimas dėl ADSP ir iki pranešimo teikimo dienos jis nėra baigtas. Tokiu atveju, teikiant pirminius pranešimus apie ADSP, VDAI rekomenduoja nurodyti datą, kada planuojama pradėtą tyrimą baigti.

2024 M. DUOMENŲ VALDYTOJAMS TAIKYTOS POVEIKIO PRIEMONĖS

2024 m. spalio mėn. VDAI, atlikusi ADSP tyrimą, priėmė sprendimą viešojo sektoriaus organizacijai skirti 9 tūkst. eurų baudą už nustatytus BDAR nuostatų pažeidimus. VDAI nustatė, kad dėl netinkamai vykdomos prieigų kontrolės ir autentifikavimo buvo prisijungta prie įstaigos serverių, serveriuose buvę duomenys užšifruoti. Įstaigos veiklos tęstinumas tapo apsunkintas, kadangi nebuvo daromos serverių atsarginės kopijos.

2024 m. VDAI, įvertinusi gautus pranešimus apie ADSP ir nustačiusi, kad yra netinkamai užtikrinamas duomenų subjektų asmens duomenų saugumas, vadovaudamasi teisės aktų nuostatomis,[4] pateikė 18 nurodymų duomenų valdytojams arba duomenų tvarkytojams suderinti duomenų tvarkymo operacijas su BDAR nuostatomis. Taip pat buvo pateiktos 38 rekomendacijos, kurios konkrečiais atvejais padės užtikrinti atitiktį BDAR reikalavimams.

[3] https://vdai.lrv.lt/lt/adsp-ir-dap/pranesimas-apie-asmens-duomenu-saugumo-pazeidima/

[4] BDAR 5 straipsnio 2 dalimi, 58 straipsnio 2 dalies d punktu, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 12 straipsnio 2 dalies 5 punktu.

NETINKAMAS PAVOJAUS FIZINIŲ ASMENŲ TEISĖMS IR LAISVĖMS NUSTATYMAS ĮVYKUS ADSP

Įvertinus 2024 m. gautus pranešimus apie ADSP, konstatuotina, kad pasitaiko atvejų, kai pavojus fizinio asmens teisėms ir laisvėms dėl įvykusio ADSP yra vertintas formaliai, t. y. nurodoma, kad pavojus kilo arba nekilo, tačiau nepateikiama argumentacija, dėl kokių priežasčių daromos tokios išvados. Taip pat pastebima, kad duomenų valdytojai, netinkamai atlikę pavojaus fizinių asmenų teisėms ir laisvėms vertinimą, nustato, kad duomenų subjektams didelis pavojus dėl įvykusio ADSP nekyla (atitinkamai duomenų subjektai neinformuojami), nors atsižvelgiant į ADSP pobūdį, specifiką ir rimtumą, toks pavojus fiziniams asmenims gali kilti. Netinkamo pavojaus fizinių asmenų teisėms ir laisvėms vertinimo atlikimas kelia riziką, kad duomenų valdytojas nesiims tinkamų taisomųjų priemonių, o duomenų subjekto neinformavimas užkirs kelią pačiam duomenų subjektui imtis reikiamų priemonių pavojaus dėl įvykusio ADSP rizikoms sumažinti.

VDAI atkreipia dėmesį, kad įvykus ADSP ir atlikdamas pavojaus fizinių asmenų teisėms ir laisvėms vertinimą, duomenų valdytojas turėtų vadovautis BDAR preambulės 75 konstatuojamąja dalimi, rekomendacija[5] bei gairėmis[6].

DIDELĮ PAVOJŲ DUOMENŲ SUBJEKTŲ TEISĖMS IR LAISVĖMS KELIANTYS ADSP

Pastebėtina, kad atsižvelgiant į BDAR ir Europos duomenų apsaugos valdybos metodinius dokumentus (žr. 6 išnaša), **didelį pavojų duomenų subjektų teisėms ir laisvėms keliantys ADSP yra atvejai, kai[7]**:

- dėl įvykusio ADSP gali kilti diskriminacija (atskleidžiami duomenys apie rasinę arba etninę kilmę, politines pažiūras, religiją ar filosofinius įsitikinimus, priklausymą profesinėms sąjungoms);
- gali būti pavogta ar suklastota tapatybė;
- gali būti padaryta finansinių nuostolių;
- pakenkta reputacijai;
- prarastas asmens duomenų, kurie laikomi profesine paslaptimi, konfidencialumas;
- neleistinai panaikinti pseudonimai;

[5] VDAI 2018 m. liepos 2 d. rekomendacija dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos.

[6] 2017 m. spalio 3 d. 29 straipsnio duomenų apsaugos darbo grupės gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679 (nauja redakcija nuo 2023 m. kovo 28 d.) bei 2021 m. gruodžio 14 d. Europos duomenų apsaugos valdybos gairės 01/2014 dėl pranešimo apie asmens duomenų saugumo pažeidimą pavyzdžių.

[7] Pastebėtina, kad paprastai priežasčių kilti dideliam pavojui asmeniui gali būti ne viena. Šios priežastys neretai yra persipynusios, tačiau užtenka bent vienos, kad būtų galima konstatuoti, kad asmeniui kyla didelis pavojus.

- padaryta didelė ekonominė ar socialinė žala;
- duomenų subjektai gali netekti galimybės naudotis savo teisėmis ir laisvėmis ar jiems užkertamas kelias kontroliuoti savo asmens duomenis;
- atskleidžiami kitokio pobūdžio asmeniui jautrūs duomenys, pavyzdžiui, genetiniai duomenys, sveikatos duomenys ar duomenys apie lytinį gyvenimą, duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas ir kt.

Pavyzdžiui, 2024 m. pas duomenų valdytoją „X“ įvyko ADSP, kai informacija apie duomenų subjektų apsilankymus pas gydytojus ir atliktų tyrimų rezultatai buvo paskelbta viešai. Dėl tokio pobūdžio ADSP gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, nes sveikatos duomenų tvarkymui pagal BDAR yra taikomi griežtesni reikalavimai ir tokios informacijos viešas paskelbimas gali turėti tiesioginės neigiamos įtakos asmeniui (darbinei veiklai, socialiniam gyvenimui).

Duomenų subjektams taip pat kyla didelis pavojus, kai piktavaliai iš duomenų valdytojo naudojamų serverių eksfiltruoja (angl. *Data Exfiltration*) nešifruotus asmens duomenis, įskaitant specialiųjų kategorijų duomenis, o vėliau juos užšifruoja.

Jeigu nėra atsarginių kopijų ir negalima atkurti saugotų asmens duomenų, šis ADSP gali turėti tiesioginę įtaką duomenų subjekto materialinei padėčiai (pavyzdžiui, dėl laiku neišmokamų išmokų).

Tokiam ADSP įvykus sveikatos priežiūros įstaigoje, išlieka pavojus dėl rimtų padarinių, susijusių su pacientų duomenų prieinamumu, kilimo. Tokiu atveju, nors būtų padaryta atsarginė duomenų kopija ir duomenis būtų galima atkurti per kelias dienas, pavojus duomenų subjektų teisėms ir laisvėms išliktų didelis dėl vėluojamų suteikti sveikatos priežiūros paslaugų.

BDAR 34 straipsnyje reglamentuota pareiga duomenų valdytojui informuoti duomenų subjektus, jeigu jiems dėl įvykusio ADSP gali kilti didelis pavojus. Primintina, kad pranešimuose duomenų subjektams turi būti nurodoma:

- 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 asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

Pasitaiko atvejų, kad duomenų valdytojas, nors ir nustatęs, kad duomenų subjektui gali kilti didelis pavojus, vertina, kad informuoti duomenų subjektą apie įvykusį ADSP nereikia, kadangi jis apie situaciją žino arba teikiant pranešimą yra abstrakčiai nurodoma, kas įvyko. Tačiau papildomai pažymėtina, kad duomenų valdytojui informuojant duomenų subjektus apie įvykusį ADSP kyla pareiga informuoti taip, kad duomenų subjektas iš gauto pranešimo aiškiai suprastų, kad įvyko ADSP ir jo asmens duomenys buvo paveikti (ar galėjo būti paveikti).

Pastaba. Atkreiptinas dėmesys, kad laikoma, jog ADSP nekelia pavojaus duomenų subjektų teisėms ir laisvėms, jei asmens duomenys netyčia išsiunčiami netinkamam adresatui, tačiau susisiekus su adresatu, gaunamas patvirtinimas, kad duomenys buvo sunaikinti, nebuvo atskleisti tretiesiems asmenims ir ateityje nebus panaudoti. Tokiu atveju laikytina, kad ADSP neturės neigiamų pasekmių duomenų subjekto teisėms ir laisvėms, dėl ADSP kilusi rizika yra suvaldyta. Pastebėtina, kad šiuo atveju išlieka pareiga duomenų valdytojui dokumentuoti įvykusį ADSP.

VDAI, įvertinusi 2024 m. gautus pranešimus, atkreipia dėmesį, kad dažniausiai pasitaikančios klaidos išlieka tos pačios:

Nėra nurodoma, kokių veiksmų pats duomenų subjektas gali imtis, kad sumažintų ADSP pasekmes (pavyzdžiui, blokuotų kredito kortelę ir pan.).

Informacija apie įvykusį ADSP duomenų subjektui pateikiama sudėtinga kalba, naudojant sudėtingus terminus ir pan. VDAI pažymi, kad teikiant pranešimą duomenų subjektui, informacija turi būti pateikiama aiškia ir paprasta kalba, kad duomenų subjektas suprastų esminę informaciją, susijusią su įvykusiu ADSP.

Nenurodomi duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, duomenys. Atkreiptinas dėmesys į tai, kad BDAR nustatyta, kad pranešime duomenų subjektui be kontaktinių duomenų privalo būti pateiktas ir kontaktinio asmens vardas bei pavardė.

Atsižvelgiant į tai, VDAI ragina duomenų valdytojus ir toliau skirti dėmesį tinkamam duomenų subjektų informavimui.