

DAŽNIAUSIAI PASITAİKANTYS ATVEJAI, KAI PRANEŠAMA DĖL ĮVYKUSIŲ INCIDENTŲ, KURIE NĖRA LAIKOMI ASMENS DUOMENŲ SAUGUMO PAŽEIDIM AIS

2025-09-08

II versija

Vadovaudamiesi BDAR 33 straipsnio 1 dalimi, duomenų valdytojai turi pareigą informuoti Valstybinę duomenų apsaugos inspekciją (toliau – VDAI) apie įvykusį asmens duomenų saugumo pažeidimą (toliau – ADSP), kuris gali kelti pavojų fizinių asmenų teisėms ir laisvėms. Šio apibendrinimo tikslas – **atkreipti duomenų valdytojų dėmesį į incidentus, kurių VDAI nelaiko ADSP arba įvykęs ADSP neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms, todėl jiems įvykus duomenų valdytojai neturi pareigos pranešti VDAI** (žr. BDAR 33 ir 34 straipsnius, [EDAV gairės](#), [EDAV pavyzdžiai dėl ADSP](#), [VDAI rekomendacija dėl ADSP](#) ir [VDAI pranešimas apie ADSP](#)).

Šiame apibendrinime pateikiami pavyzdžiai yra skirti pareigos, numatytos BDAR 33 straipsnyje, tinkamam įgyvendinimui. Atkreiptinas dėmesys, kad vien tai, kad pavyzdžiuose aptariami atvejai nėra laikomi ADSP, nereiškia, kad jie negalėtų būti laikomi kitų BDAR nustatytų pareigų pažeidimu, pavyzdžiui, neteisėtu duomenų tvarkymu ar kt. Taip pat pažymėtina, kad nors kai kuriais atvejais incidentai įvyksta dėl pačių duomenų subjektų neatsargaus elgesio, tačiau tai neatleidžia duomenų valdytojų ir duomenų tvarkytojų nuo pareigos vertinti duomenų tvarkymo keliamą riziką ir įgyvendinti tinkamas saugumo priemones.

APIBENDRINIME VARTOJAMOS SANTRUMPOS

VDAI – Valstybinė duomenų apsaugos inspekcija

BDAR – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)

EDAV – Europos duomenų apsaugos valdyba

ADTAJ – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas

ADSP – Asmens duomenų saugumo pažeidimas (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) (BDAR 4 straipsnio 12 dalis).

ATVEJAI, KAI ASMENS DUOMENYS YRA PASKELBTI VIEŠAI

Pasitaiko atvejų, kai duomenų valdytojas informuoja VDAI apie jo veikloje įvykusį ADSP, kai atskleidžiami asmens duomenys, kurie jau yra teisėtai paskelbti viešai.

1 pavyzdys

Socialiniuose tinkluose paviestas pranešimas, skirtas tik įmonės darbuotojams, su vieno įmonės darbuotojo asmens duomenimis (t. y. vardas, pavardė, pareigos, darbinis el. paštas ir darbinis telefono numeris, pranešimo turinyje kitos informacijos, tiesiogiai ar netiesiogiai identifikuojančios darbuotojus nėra). Kadangi iki incidento darbuotojo asmens duomenys buvo skelbiami įmonės tinklapyje ir buvo prieinami bet kuriam šiame tinklalapyje besilankančiam asmeniui, juos paskelbus viešai, tai nebus laikoma ADSP.

2 pavyzdys

Sukūrus netikrą svetainę ir pasinaudojus internete prieinamais juridinio asmens duomenimis (t. y. įmonės pavadinimas, įmonės kodas ir buveinės adresas, taip pat ir juridinio asmens direktoriaus vardas ir pavardė), nežinomas asmuo naudojo šiuos duomenis savo veikloje. Kadangi naudojami duomenys yra skelbiami viešai, todėl, VDAI nuomone, juridinio asmens duomenų atskleidimas nėra laikomas ADSP.

ATVEJAI, KAI GAUTA PRIEIGA PRIE DUOMENŲ, KURIŲ TVARKYMU NĖRA TAIKOMAS BDAR

Pasitaiko atvejų, kai duomenų valdytojas praneša VDAI apie įvykusį ADSP, kurio metu yra neteisėtai gaunama prieiga prie duomenų, kurių tvarkymui nėra taikomas BDAR, pavyzdžiui, ADSP susijęs su statistiniais duomenimis, anonimine informacija (BDAR konstatuojamosios dalies 26 punktą), mirusių asmenų asmens duomenimis (BDAR konstatuojamosios dalies 27 punktą) ar duomenimis, kuriuos tvarko fizinis asmuo, užsiimdamas išimtinai asmenine ar namų ūkio veikla (BDAR konstatuojamosios dalies 18 punktą). Atsižvelgiant į tai, tokie incidentai nėra laikomi ADSP.

3 pavyzdys

Įsilaužus į duomenų saugyklą, kuriame saugomi tik statistiniai duomenys, buvo užšifruoti ne tik visi serveryje buvę statistiniai duomenys, bet ir jų atsarginės kopijos. Šiuo incidentu buvo apribotas prieinamumas prie duomenų ir pažeistas jų konfidencialumas. Atsižvelgiant į tai, kad serveryje nebuvo laikomi asmens duomenys, o tik statistiniai duomenys, šis incidentas nėra laikomas ADSP.

4 pavyzdys

Įmonės darbuotojas peržiūrėjo mirusio asmens duomenis. Atsižvelgiant į tai, kad darbuotojas peržiūrėjo duomenis, kurių tvarkymui nėra taikomas BDAR, toks incidentas nėra laikomas ADSP.

ATVEJAI, KAI SIUNČIAMY PRANEŠIMAI SUBJEKTAMS BE LEIDIMO

VDAI gauna pranešimus apie įvykusius incidentus, kai netinkamiems gavėjams buvo išsiųsti pranešimai be asmens duomenų. Jei šiuose pranešimuose nėra asmens duomenų, tokie incidentai nėra laikomi ADSP, todėl BDAR netaikomas. Papildomai atkreiptinas dėmesys, kad duomenų valdytojas, atlikdamas pavojaus fizinių asmenų teisėms ir laisvėms vertinimą, turi vertinti ne tik siųsto pranešimo turinį, bet ir tai, ar nėra matomi laiško gavėjų adresai kitiems gavėjams.

5 pavyzdys

Duomenų valdytojas be duomenų subjektų sutikimo dėl žmogiškosios klaidos išsiuntė daugiau kaip 20 000 el. laiškų, kuriuose siūlo sudaryti sutartis. Buvo nustatyta, kad išsiųstuose el. laiškuose nebuvo nurodyta asmens duomenų, gavėjų el. pašto adresai nebuvo matomi kitiems gavėjams, o siunčiami pranešimai buvo bendro pobūdžio. Toks atvejis nebus laikomas ADSP.

ATVEJAI, KAI PRANEŠAMA DĖL LAIKU NEATNAUJINAMOS INFORMACIJOS INFORMACINĖJE SISTEMOJE

Praktikoje taip pat pasitaiko situacijų, kai VDAI teikiami pranešimai apie tai, kad duomenų valdytojų informacinėse sistemose nebuvo laiku atnaujinti pasikeitę asmens duomenys, pavyzdžiui, neatnaujinta informacija apie asmenų skolos sumokėjimą ar pan., todėl asmenys patiria nepatogumų negalėdami tinkamai naudotis tam tikromis paslaugomis. Pastebėtina, kad aptariamasis atvejis nėra susijęs su asmens duomenų saugumo užtikrinimu, nes asmens duomenys nebuvo sunaikinti, nepagrįstai pakeisti, be leidimo atskleisti tretiesiems asmenims (pavyzdžiui, prie jų nebuvo suteikta prieiga neįgaliesiems asmenims). Taigi, atsižvelgiant į ADSP sąvoką, tokie atvejai nėra laikomi ADSP ir apie juos VDAI pranešti nereikia, tačiau duomenų valdytojas turėtų imtis veiksmų tinkamam asmens duomenų tvarkymui (asmens duomenų tikslumui) užtikrinti.

6 pavyzdys

Bendrovėje atliekant duomenų bazės programavimo darbus, buvo pakeistas informacijos automatinio atnaujinimo intervalas, dėl to duomenų bazėje duomenys atsinaujindavo kartą per mėnesį. Apie šią programavimo klaidą Bendrovė sužinojo tik gavusi pranešimą iš kliento ir atlikusi tyrimą. Dėl tokios klaidos klientai negalėjo tinkamai naudotis paslaugomis, kadangi duomenų bazės informacija nebuvo nedelsiant atnaujinama. Nors duomenų automatinio atnaujinimo intervalas buvo ilgesnis nei prieš tai buvęs, o klientams kilo nepatogumų naudojantis paslaugomis, tačiau tai nėra laikoma ADSP, kadangi

nejvesti duomenys nėra sunaikinti, prarasti, pakeisti, be leidimo atskleisti, taip pat nėra be leidimo gauta prieiga prie jų.

ATVEJAI, KAI DUOMENŲ VALDYTOJAS IŠSIUNČIA PRANEŠIMUS SU ASMENS DUOMENIMIS DUOMENŲ SUBJEKTO NETEISINGAI NURODYTAIS KONTAKTAIS

VDAI neretai sulaukia pranešimų apie atskleistus asmens duomenis asmenims, neturintiems teisės su jais susipažinti, tokiais atvejais, kai kontaktinius duomenis, kuriais buvo išsiųsta informacija su asmens duomenimis, nurodo pats duomenų subjektas, t. y. pats asmuo nurodė ne jam priklausantį elektroninio pašto adresą. Atsižvelgiant į tai, kad duomenų valdytojas siųsdamas pranešimus nesuklydo nurodydamas adresato kontaktus ir jam nebuvo žinoma, kad duomenų subjekto kontaktai yra pasikeitę ar jam nepriklauso (t. y. duomenų subjektas neatnaujino savo kontaktinių duomenų ar pats suklydo juos nurodydamas), toks incidentas nėra laikomas ADSP ir pranešti VDAI apie jį nereikia.

7 pavyzdys

Asmuo „A“ kreipėsi į įstaigą dėl į jo el. pašto dėžutę gautų procesinių dokumentų su kito asmens „B“ (kuriam skirti minėti dokumentai) asmens duomenimis. Įstaigai atlikus tyrimą, nustatyta, kad procesiniai dokumentai buvo siunčiami automatiškai būdu naudojant kontaktinius duomenis, kuriuos į duomenų bazę suveda patys duomenų subjektai. Šiuo atveju, asmuo „B“ suvedė ne savo el. pašto adresą, o asmuo „A“, kuris ir gavo asmeniui „B“ siųstus procesinius dokumentus.

8 pavyzdys

Duomenų valdytojas gavo el. laišką, kuriame nurodyta, kad laiško siuntėjas negavo šeimos kortelės ir mano, kad ją galimai atsiėmė kitas asmuo. Duomenų valdytojas atliko tyrimą ir nustatė, kad šeimos kortelė buvo siunčiama paštu ir atiduota asmeniui, kuris pašto darbuotojui pateikė gautą SMS pranešimą apie jam siunčiamą siuntą. Pristatymo adresą ir kontaktinį telefono numerį konkrečiu atveju nurodė asmuo, kuris užsakė šeimos kortelę. Duomenų valdytojas nesuklydo nurodydamas adresą ir kontaktinį telefono numerį siųsdamas korespondenciją. Incidentas įvyko dėl to, kad siuntą atsiėmė kitas asmuo. Šiuo atveju svarbu atkreipti dėmesį į pašto paslaugų teikimo taisykles, kuriose nustatyta, kad pašto darbuotojas atiduoda paprastą siuntą, jei jam pateikiamas siuntos gavimo pranešimas (popierinis variantas ar trumpoji SMS žinutė). Atsižvelgiant į tai, kad duomenų valdytojas nurodė tinkamą adresą bei kontaktinį numerį, o pašto darbuotojas atidavė siuntą laikydamasis pašto paslaugų teikimo taisyklių, incidentas nėra laikomas ADSP.

ATVEJAI, KAI NUSTATOMOS SAUGUMO SPRAGOS

Pasitaiko atvejų, kai duomenų valdytojas pats inicijuoja kibernetinio saugumo patikrinimą ar atlieka įsilaužimo testavimą (angl. *Penetration test*) siekdamas nustatyti, ar egzistuoja tinklo, informacinių technologijų infrastruktūros ar kitų įrenginių ar aplikacijų spragos, kurios leistų tikriems programišiams

įsibrauti į tinklą ar informacinę sistemą. Atlikus tokius patikrinimus yra nustatomi pažeidžiamumai, dėl kurių gali kilti ADSP, tačiau faktų, kad ADSP kilo, nebuvo nustatyta. Tokie atvejai nėra laikomi ADSP, nes poveikis asmens duomenims nebuvo padarytas (pavyzdžiui, jie nebuvo sunaikinti, pakeisti ar kt.), taip pat prie jų negavo prieigos tretieji asmenys. Taigi, vien tai, kad duomenų valdytojas aptiko saugumo spragas, nereiškia, kad įvyko ADSP, jei tokiomis spragomis nebuvo pasinaudota ir nebuvo pažeistas asmens duomenų konfidencialumas, prieinamumas ar vientisumas.

9 pavyzdys

Duomenų valdytojo iniciatyva atliktas bendrovės naudojamų el. laiškų siuntimo aplikacijos ir jos serverių kibernetinio saugumo patikrinimas, imituojant „Brute-force“ ataką. Atliekant kibernetinio saugumo serverių patikrinimą, buvo nustatyta, kad pasinaudojus „Brute-force“ ataka yra gaunami serverio, kuriame yra saugomi asmens duomenys, prisijungimai. Dėl šio pažeidžiamumo gali kilti rizika, kad piktaivaliui gavus prisijungimus prie šio serverio, gali būti pažeistas jame saugomų asmens duomenų konfidencialumas, vientisumas ar prieinamumas. Papildomai pažymėtina, kad tokiais atvejais duomenų valdytojas turi įvertinti, ar dėl nustatyto pažeidžiamumo nekilo ADSP (pavyzdžiui, įvertinus žurnalinius įrašus nebuvo nustatytos neautorizuotos prieigos). Kadangi toks atvejis neturi ADSP požymių, jis nelaikomas ADSP.

10 pavyzdys

Programišiui aptikus svetainės saugumo spragą, yra gaunama prieiga tik prie savo asmens duomenų (negaunant prieigos prie kitų duomenų subjektų asmens duomenų), apie rastą saugumo spragą jis informavo bendrovę, pateikdamas gautą prieigą prie savo asmens duomenų kaip įrodymus. Kadangi aptikus saugumo spragą kitų duomenų subjektų duomenys nebuvo sunaikinti, prarasti, pakeisti, be leidimo atskleisti, taip pat nebuvo be leidimo gauta prieiga prie jų, toks atvejis nėra laikomas ADSP.

ATVEJAI, KAI ASMENS DUOMENYS ATSKLEIDŽIAMAI DĖL DUOMENŲ SUBJEKTO KALTĖS

Vis dažniau pasitaiko atvejų, kai sukčiams pasinaudojus duomenų viliojimo metodu (angl. „Phishing“) ar kitais būdais yra išgaunami prisijungimo ar kiti duomenų subjektų duomenys, dėl kurių duomenų subjektai gali patirti neigiamų pasekmių, pavyzdžiui, finansinius nuostolių. VDAI sulaukia pranešimų dėl incidentų, kurių metu tretiesiems asmenims pasinaudojus socialinės inžinerijos metodais paremtomis atakomis ar pasinaudojus tinkamai nepasaugotais duomenų subjektų įrenginiais, duomenų subjektai patiria finansinių nuostolių ar yra atskleidžiami jų asmens duomenys, įskaitant ir prisijungimo duomenis. Tačiau tokie incidentai nebūtų laikomi ADSP, nes pats asmuo atskleidžia ar tinkamai neapsaugo savo duomenų, o duomenų valdytojo saugumo priemonės nebuvo pažeistos.

11 pavyzdys

Duomenų subjektui gavus el. laišką su kenkėjiška nuoroda, kuria naudojantis piktaivaliai siekia išvilioti duomenų subjekto prisijungimus prie finansų įstaigoje turimos paskyros. Duomenų subjektui

paspaudus kenkėjišką nuorodą ir pačiam suvedus reikalaujamus prisijungimo duomenis bei patvirtinus mokėjimą, pinigai buvo pervesti piktavaliams.

12 pavyzdys

Duomenų subjektui tinkamai neapsaugojus asmens duomenų, pavyzdžiui, asmuo prisijungimo duomenis yra išsaugojęs naršyklėse, asmens duomenys (įskaitant prisijungimo duomenys) perimami piktavaliui įsilaužus į asmens įrenginius. Duomenų valdytojas, gavęs informacijos, kad yra atskleisti prisijungimo duomenys prie asmens paskyros svetainėje, operatyviai blokavo paskyrą ar inicijavo privalomą prisijungimo duomenų keitimą. Duomenų valdytojo saugumo priemonės nebuvo pažeistos, todėl tokie atvejai nėra laikomi ADSP.

ATVEJAI, KAI DUOMENŲ SUBJEKTŲ PRIEIGOMIS FAKTIŠKAI NEBUVO PASINAUDOTA

Pasitaiko atvejų, kad duomenų subjektai tuos pačius paskyrų, kuriose yra saugomi asmens duomenys, prisijungimų duomenis (prisijungimo vardas ir slaptažodis) naudoja skirtingoms paskyroms. Kai vienos svetainės paskyros prisijungimai yra atskleidžiami, piktavaliai, turėdami atskleistus vienos svetainės naudotojų prisijungimo duomenis, bando patikrinti, ar įmanoma turimais prisijungimais prisijungti prie įvairių paskyrų (angl. „*Credential-stuffing attack*“). Šiuo atveju duomenų valdytojui nustatius, kad yra bandoma neautorizuotai prisijungti prie naudotojų paskyrų, kyla pareiga nustatyti, ar piktavaliui turimais prisijungimais pavyko faktiškai pasinaudoti.

13 pavyzdys

Duomenų valdytojas, nustatė, kad programišiai, pasinaudodami programine įranga, kurios pagalba buvo gauti patvirtinimai, kad turimi duomenų subjektų prisijungimai (prisijungimo vardas ir slaptažodis) yra naudojami svetainėje. Duomenų valdytojas, įvertinęs turimus sistemos žurnalinius įrašus, nustatė, kad prisijungta prie paskyros nebuvo. Šiuo atveju programišiams pavyko sužinoti tik tinkančius prisijungimus prie duomenų subjektų paskyrų, tačiau pačia prieiga nepasinaudojo ir prie jokių duomenų valdytojo tvarkomų asmens duomenų nepriėjo. Šiuo atveju nebuvo sunaikinti, prarasti, pakeisti, atskleisti, persiųsti ar kitaip tvarkomi asmens duomenys (įskaitant gautos prieigos prie asmens duomenų panaudojimą). Todėl toks incidentas nėra laikomas ADSP.

ATVEJAI, KAI YRA PAŽEISTOS SAUGUMO PRIEMONĖS

VDAI sulaukia pranešimų apie ADSP, kurių metu dėl žmogiškosios klaidos ar kibernetinio incidento buvo pažeistos saugumo priemonės, užtikrinančios asmens duomenų apsaugą nuo neteisėtos prieigos. Atvejai, kai duomenų valdytojas ar duomenų tvarkytojas nustato, kad nors ir buvo pažeista viena ar kelios saugumo priemonės, tačiau likusios saugumo priemonės apsaugojo asmens duomenis nuo neteisėtos prieigos, nėra laikomi ADSP ir VDAI apie juos pranešti nereikia.

14 pavyzdys

Duomenų tvarkytojas nustatė, kad duomenų valdytojo siunčiamas laiškas yra atplėštas, tačiau voko viduje buvusi siunta buvo įdėta į kitą užklijuotą voką, kuris liko nepažeistas. Šiuo atveju nebuvo atskleisti asmens duomenys, todėl toks incidentas nėra laikomas ADSP.
