VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

DAŽNIAUSIAI PASITAIKANTYS ATVEJAI, KAI PRANEŠAMA DĖL ĮVYKUSIŲ INCIDENTŲ, KURIE NĖRA LAIKOMI ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAIS

2024-01-11

Vadovaujantis BDAR 33 straipsnio 1 dalimi, duomenų valdytojai turi pareigą informuoti VDAI apie įvykusį ADSP, kuris gali kelti pavojų fizinių asmenų teisėms ir laisvėms. Šio apibendrinimo tikslas – **atkreipti duomenų valdytojų dėmesį į incidentus, kurių VDAI nelaiko ADSP** (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.

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
ADTAĮ – 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 paviešintas 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, tokių duomenų atskleidimas nėra laikomas ADSP.

Atvejai, kai tvarkomi tik statistiniai duomenys

Pasitaiko atvejų, kai duomenų valdytojas praneša VDAI apie įvykusį ADSP, kurio metu yra pažeidžiamas statistinių duomenų, iš kurių negalima nustatyti duomenų subjekto tapatybės, konfidencialumas ir (ar) prieinamumas. Remiantis BDAR konstatuojamosios dalies 26 punktu, BDAR netaikomas anonimiškos informacijos tvarkymui, įskaitant statistiniais ar tyrimų tikslais[1], todėl šis incidentas nėra laikomas ADSP.

3 pavyzdys

Įsilaužus į serverį, 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, todėl šis incidentas nėra laikomas ADSP.

Atvejai, kai pranešimai siunčiami ne tiems subjektams arba neturint sutikimo

VDAI gauna pranešimus apie įvykusius incidentus, kai ne tiems 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 ar nėra matomi laiško gavėjų adresai kitiems gavėjams.

4 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.

[1] Jeigu iš šių duomenų nei tiesiogiai, nei netiesiogiai negalima nustatyti duomenų subjekto tapatybės.

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 aptariamas 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 neįgaliotiems 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.

5 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 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 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.

6 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 automatiniu būdu naudojant kontaktinius duomenis, kuriuos į duomenų bazę suveda patys duomenų subjektai. Šiuo atveju asmuo „B“ suvedė ne savo el. pašto adresą, o asmens „A“, kuris ir gavo asmeniui „B“ siųstus procesinius dokumentus.

7 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, todėl 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*), siekiant 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.

8 pavyzdys

Duomenų valdytojo iniciatyva atliktas bendrovės naudojamų el. laiškų siuntimo aplikacijos ir jos serverių kibernetinio saugumo patikrinimas, imituojant *Brute-force* ataką. Atliekant serverių kibernetinio saugumo patikrinimą, buvo nustatyta, kad pasinaudojus *Brute-force* ataka yra gaunami serverio, kuriame yra saugomi asmens duomenys, prisijungimai. Dėl šio pažeidžiamumo gali kilti rizika, kad piktavaliui 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.

9 pavyzdys

Programišiui aptikus svetainės saugumo spragą, yra gaunama prieiga tik prie savo asmens duomenų (negaunant prieigos prie kitų duomenų subjektų asmens duomenų). Programišius apie rastą saugumo spragą 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, todėl toks atvejis nėra laikomas ADSP.

Atvejai, kai asmens duomenys atskleidžiami dėl duomenų subjekto kaltės

Vis dažniau pasitaiko atvejų, kai sukčiams pasinaudojus duomenų viliojimo metodu (angl. *Phishing*) išgaunami prisijungimo ar kiti duomenų subjektų duomenys, dėl kurių duomenų subjektai gali patirti neigiamas pasekmes, pavyzdžiui, finansinius nuostolius. VDAI sulaukia pranešimų dėl incidentų, kurių metu tretiesiems asmenims pasinaudojus socialinės inžinerijos metodais paremtomis atakomis duomenų subjektai patiria finansinius nuostolius. Tačiau tokie incidentai nebūtų laikomi ADSP, nes pats asmuo atskleidžia savo duomenis, o duomenų valdytojo saugumo priemonės nebuvo pažeistos.

10 pavyzdys

Duomenų subjektas gavo el. laišką su kenkėjiška nuoroda, kuria naudojantis piktavaliai 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.

Atvejai, kai duomenų subjektų prieigomis faktiškai nebuvo pasinaudota

Pasitaiko, 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 pastebėjus, kad yra bandoma neautorizuotai prisijungti prie naudotojų paskyrų, kyla pareiga nustatyti, ar piktavaliui turimais prisijungimais pavyko faktiškai pasinaudoti.

11 pavyzdys

Duomenų valdytojas „XXX“ nustatė, kad programišiai, pasinaudodami programine įranga gavo patvirtinimus, kad jų turimi duomenų subjektų prisijungimai (prisijungimo vardas ir slaptažodis) yra naudojami duomenų valdytojo „XXX“ svetainėje. Duomenų valdytojas, įvertinęs turimus sistemos žurnalinius įrašus, nustatė, kad prisijungta prie naudotojų paskyrų nebuvo. Šiuo atveju piktavaliai žinojo prisijungimus prie duomenų subjektų paskyrų, tačiau jais nepasinaudojo ir nepasiekė duomenų valdytojo tvarkomų asmens duomenų. Šiuo atveju nebuvo sunaikinti, prarasti, pakeisti, atskleisti, persiųsti ar kitaip duomenų valdytojo tvarkomi asmens duomenys (įskaitant gautos prieigos prie asmens duomenų panaudojimą), todėl toks incidentas nėra laikomas ADSP minėto duomenų valdytojo atžvilgiu.