VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Ko galime pasimokyti iš įvykusių asmens duomenų saugumo pažeidimų?

IRMA SANVAITYTĖ
VDAI Priežiūros skyriaus patarėja

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

ADSP DOKUMENTAVIMAS

- Nagrinėjant fizinių asmenų skundus, Inspekcija nustato atvejų dėl įvykusio arba galimai įvykusio ADSP ir kreipiasi į duomenų valdytoją, prašydama pateikti informaciją.

- Vadovaujantis BDAR 33 straipsnio 5 dalimi, bei duomenų valdytojui taikomu atskaitomybės principu, Inspekcija gali pareikalauti leisti susipažinti su ADSP dokumentacija.

- Pasitaiko atvejų, kai Inspekcijai kreipusis į duomenų valdytoją, prašant pateikti informaciją, apie įvykusį ADSP, duomenų valdytojas pateikia informaciją, kad situacijos, kaip ADSP nevertino, atsižvelgiant į tai ir veiksmų, kaip numato BDAR 33 ir 34 straipsniai, neatliko (pažeidimo nedokumentavo, poveikio fizinių asmenų teisėms ir laisvėms nevertino).

- Duomenų valdytojas turėtų dokumentuoti ne tik ADSP pažeidimus, bet ir pažeidimus, kurių ADSP nelaiko.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

ADSP (NE)DOKUMENTAVIMO PAVYZDŽIAI

I SITUACIJA:

- Pareiškėjas skunde nurodė, kad naudodamasis elektroninės sveikatos platforma pastebėjo, kad prie jo paskyros jungėsi Poliklinikos gydytoja.

- Poliklinika pateikė informaciją, kad gydytoja prie pareiškėjo paskyros prisijungė asmeniniais tikslais.

- Atvejis Poliklinikoje buvo užregistruotas ADSP registre, Poliklinika pateikė dokumentuotą informaciją.

II SITUACIJA:

- Pareiškėjas skunde nurodė, kad iš Bendrovės gavo SMS pranešimą apie paskirtą vizitą, nors vizitui registravęsis nebuvo.

- Bendrovė paaiškino, kad pareiškėjo vardu ir pavarde yra registruoti 3 pacientai. Vienam iš jų paskambinus užsiregistruoti vizitui, įvyko žmogiškoji klaida ir darbuotojas užregistravo pareiškėją.

- Bendrovė nurodė, kad ADSP nevertino: susidariusi situacija neatitinka ADSP apibrėžimo, pažeidimas nekelia pavojaus.

II SITUACIJA (Inspekcijos vertinimas):

- Bendrovė, nors ir dėl žmogiškosios klaidos, tačiau pareiškėjui atskleidė informaciją apie kito asmens Bendrovėje tvarkomus duomenis.

- Duomenų valdytojas privalo dokumentuoti visus pažeidimus, kaip paaiškinta BDAR 33 straipsnio 5 dalyje, ir šis reikalavimas yra susijęs su BDAR 5 straipsnio 2 dalyje nustatytu atskaitomybės principu.

- Viena ta aplinkybė, kad, duomenų valdytojo nuomone, nekilo pavojus, nereiškia, kad apskritai neįvyko ADSP.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

KOKIA INFORMACIJA TURĖTŲ BŪTI ADSP REGISTRE?

- Informacija apie pažeidimą, jo priežastys ir vieta; asmens duomenys, kuriems tas pažeidimas turi poveikio, pažeidimo poveikis; pasekmės ir taisomieji veiksmai, kurių buvo imtasi (BDAR 33 straipsnio 5 dalis).

- 29 straipsnio duomenų apsaugos darbo grupės Gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą.

- Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojama forma.

- **SVARBU**: duomenų valdytojas vidinėje tvarkoje turėtų reglamentuoti ADSP valdymo procedūrą.

- Taip pat Gairėse dėl ADSP yra nurodyta, kad **jei tokiame registre yra asmens duomenų, duomenų valdytojas pagal asmens duomenų tvarkymo principus, privalo nustatyti tinkamą jų saugojimo laikotarpį ir užtikrinti teisėtą duomenų tvarkymo pagrindą**.

Informacija apie pažeidimą (trumpas aprašymas)	Pažeidimo kilimo priežastis	Pažeidimo vieta

Pagal BDAR ir Gaires

Asmens duomenys, kuriems pažeidimas turi poveikio	Pažeidimo poveikis	Pažeidimo pasekmės

Pagal BDAR ir Gaires

Taisomieji veiksmai	Priimti sprendimai	Ar pranešta VDAI? Jei taip, kada?

Pagal BDAR ir Gaires

Jei pranešimas VDAI pateiktas praleidus terminą – vėlavimo priežastys	**Jei VDAI nepranešta - nepranešimo priežastys**	**Ar pranešta fiziniam asmeniui, jei taip, tai kada ir kokiu būdu?**	**Jei fiziniam asmeniui nepranešta – nepranešimo priežastys**

Pagal BDAR ir Gaires

Ar pažeidimas traktuojamas kaip ADSP?	Jei ne - pagrindimas	Šaltinis, iš kurio gauta informacija apie ADSP

Kita informacija, kuri galėtų būti registre

ADSP data ir laikas (kada įvyko ADSP?)	ADSP nustatymo data ir laikas	ADSP aplinkybės

Kita informacija, kuri galėtų būti registre

Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius	**Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos**	**Asmens duomenų, kurių saugumas pažeistas, kategorijos**

Kita informacija, kuri galėtų būti registre

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

ADSP POVEIKIO VERTINIMAS

Viena iš esminių pareigų, kylančių duomenų valdytojui – poveikio įvertinimas.

Svarbu: duomenų valdytojas, tik sužinojęs apie pažeidimą, turi imtis ne tik priemonių incidentui suvaldyti, bet ir įvertinti pavojų.

To reikia dėl dviejų priežasčių: pirma, žinant poveikio asmeniui tikimybę ir galimą rimtumą, duomenų valdytojui bus lengviau imtis veiksmingų priemonių pažeidimui sustabdyti ir pašalinti; antra, tai jam padės nustatyti, ar apie pažeidimą būtina pranešti priežiūros institucijai ir, jei reikia, susijusiems asmenims.

Gairėse dėl pranešimo apie ADSP nurodyta, kad duomenų valdytojas, vertindamas pavojų, turėtų atsižvelgti į šiuos kriterijus:

a) pažeidimo pobūdį; b) asmens duomenų jautrumą ir jų kiekį; c) asmens tapatybės nustatymo lengvumą; d) pasekmių rimtumą asmenims; e) asmens specifinius ypatumus; f) duomenų valdytojo specifinius ypatumus; g) asmenų, kuriems pažeidimas turi poveikio, skaičių.

Pavyzdys Nr. 1: Teisės skyriaus darbuotoja elektroniniu paštu per klaidą laišką su prisegtu dokumentu (informacija apie trečiąjį asmenį (vardas, pavardė, adresas)) išsiunčia Administravimo skyriaus darbuotojai.

Gairėse dėl pranešimo apie ADSP yra išaiškinta, kad *„Įprastomis aplinkybėmis atskleidus asmens vardą ir pavardę bei adresą, didelės žalos neturėtų būti padaryta“*.

Pavyzdys Nr. 2: Teisės skyriaus darbuotoja elektroniniu paštu per klaidą laišką su prisegtu dokumentu (informacija apie trečiąjį asmenį (vardas, pavardė, informacija apie gydymąsi sveikatos priežiūros įstaigose)) išsiunčia Administravimo skyriaus darbuotojai.

Tokiu atveju, duomenų valdytojas, vertindamas, ar kilo pavojus (didelis pavojus), turėtų atsižvelgti, kaip nurodoma Gairėse, į atitinkamus kriterijus (pvz., duomenų jautrumą ir jų kiekį) ir pan.