

Per milijonas asmen galjo nukentti dingus j asmens duomenims iš Greitosios medicinos pagalbos stoties serverio



This page contains macros or features from a plugin which requires a valid license.

You will need to contact your administrator.

Pirmadien [žiniasklaidoje](#) buvo paviėšinta, kad Vilniaus greitosios medicinos pagalbos stoties serverio duomen bazje saugoti per milijono asmen asmens duomenys (tarp kuri ir speciali kategorij asmens duomenys - pacient ligos istorija) galimai prarasti bei nukopijuoti (perkeliant kit server), o prie j galjo gauti prieig tretieji asmenys. Kaip skelbiama, Valstybin duomen apsaugos inspekcija (VDAI) domisi šiuo atveju ir Greitosios medicinos pagalbos stoiai bus išsisitas raštas pateikti informacij, ar šis incidentas buvo vertintas kaip asmens duomen saugumo pažeidimas ir gyvendintos su tuo susijusios pareigos - imtasi priemoni incidentui suvaldyti, pranešta VDAI, duomen subjektams bei atitinkamai dokumentuota.

Koki priemoni buvo imtasi pacient duomen saugumo incidentui nustatyti ir suvaldyti?

Kaip teigiama [lrt.lt](#) straipsnyje, pacient duomen dingimus iš duomen bazs Vilniaus greitosios medicinos pagalbos stoties darbuotojai pastebjo dar vasar, kai dispečeriai negalėjo peržirti pagalb kviečiami pacient korteli, kuriose turi būti nurodyti net tik paciento kontaktiniai duomenys: adresas, telefonas, bet ir ligos istorija. Buvo tarta, kad prie ši duomen prieig galimai turi tretieji asmenys. Atlikus audit, buvo gautos išvados, kad asmens duomenys iš Greitosios medicinos pagalbos stoties serverio perkelti kit server ir prie j galimai prieig gavo ir tretieji asmenys. Gavs audito išvadas, Vilniaus greitosios medicinos pagalbos stoties vadovas kreipsi VDAI patarimo ir gavo konsultacij, kad pagal VDAI gaut informacij galimai buvo padarytas konfidencialumo ir prieinamumo pažeidimas. Tačiau, kiek galima sprsti iš viešai skelbiamos informacijos, pranešimo dėl galimo pažeidimo Vilniaus greitosios medicinos pagalbos stotis, kaip duomen valdytojas, VDAI neteik. Vienas motyv - paskelbtas karantinas, tačiau, kaip teigia advokatas Laimonas Marcinkevičius, **"karantinas neatleidžia duomen valdytojų nuo j pareig pagal BDAR vykdymo. Juolab, kad pranešim apie duomen saugumo pažeidim duomen valdytojai VDAI gali pateikti elektronini ryši priemonėmis, pvz., el. paštu. Vien konsultacija su VDAI, nesimusi technini ir organizacin duomen saugumo priemoni, negalt būti laikoma pakankama priemone pažeidimui valdyti."**

Pirmiausia, vadovaujantis [VDAI rekomendacijomis](#), duomen valdytojas sužinoys apie galim pažeidim, turt kaip manoma greičiau atlikti pirmin tyrim, išsiaiškinti ir nustatyti, ar pažeidimas iš tikrj vyko, bei kokios galimos pasekms asmenims (t. y. vertinti rizik). Vertinant rizik turt būti atsižvelgiant šiuos kriterijus:

- pažeidimo tip;
- asmens duomen pobd, apimtis (pvz., speciali kategorij asmens duomenys);
- kaip lengvai identifikuojamas fizinis asmuo;
- pasekmi rimtum fiziniam asmenims;
- specialias fizinio asmens savybes (pvz., duomenys susij su vaikais ar kitais pažeidžiamais asmenimis);
- nukentjusij fizini asmen skaii;
- specialias duomen valdytojo savybes (pvz., veiklos pobd).

Pareiga pranešti apie duomen saugumo pažeidimus - VDAI ir duomen subjektams

Dabar VDAI domsis, ar po gautos VDAI konsultacijos buvo imtasi veiksm ir sivertinta, ar šis atvejis yra asmens duomen saugumo pažeidimas. Vadovaujantis BDAR 4 str. 12 p. asmens duomen saugumo pažeidimu laikomas saugumo pažeidimas, dėl kurio netyčia arba neteistai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persisti, saugomi arba kitaip tvarkomi asmens duomenys arba prie j be leidimo gaunama prieiga. Duomen valdytojų vertinus, kad vyko asmens duomen saugumo pažeidimas, jis privalo ne vliau kaip per 72 val. nuo pažeidimo paaiškijimo momento pranešti VDAI. Kadangi pranešimo terminas yra itin trumpas, kaip teigia UAB "JURIDICON", teikianios duomen apsaugos pareigno paslaug Allaw, teisinink Migl Žvinyt, **"kiekvienas duomen valdytojas turi būti numats ir pasitvirtins duomen saugumo pažeidim nustatymo, tyrimo ir pranešimo apie juos procedr, kad galt efektyviai gyvendinti ši BDAR 33-34 str. nustatyt pareig."** Savo rekomendacijose VDAI akcentuoja, kad jelgu, vertinus rizik, abejojama, ar ji yra ir ar reikia pranešti apie duomen saugumo pažeidim VDAI, rekomenduotina pranešti. Tais atvejais, kai dėl pažeidimo pobdžio, duomen valdytojų yra būtina atlikti išsamesn tyrim ir nustatyti visus svarbius faktus, susijusius su asmens duomen saugumo pažeidimu (pvz., dar nra išsiaiškinta pažeidimo apimtis), ir per 72 val. nuo sužinojimo apie pažeidim dėl objektyvi aplinkybi to padaryti nemanoma, pranešimui reikalinga informacija galt būti teikiama etapais, apie tai nurodant pirminiame pranešime. Todl manytina, kad Vilniaus greitosios medicinos pagalbos stotis, nustatiusi mintas aplinkybes dėl galimo pacient duomen praradimo turjo ne konsultuotis, o teikti pirmin pranešim VDAI dėl galimo asmens duomen saugumo pažeidimo.

"Karantinas neatleidžia duomen valdytojų nuo j pareig pagal BDAR vykdymo. Juolab, kad pranešim apie duomen saugumo pažeidim duomen valdytojai VDAI gali pateikti elektronini ryši priemonėmis, pvz., el. paštu. Vien konsultacija su VDAI, nesimusi technini ir organizacin duomen saugumo priemoni, negalt būti laikoma pakankama priemone pažeidimui valdyti."

Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizini asmenų teisms ir laisvėms, duomenų valdytojas nepagrįstai nedelsdamas (rekomenduojama ne vėliau kaip per 72 val.) nuo pažeidimo paaiškinimo momento, privalo pranešti apie duomenų saugumo pažeidimą duomenų subjektams. Tais atvejais, kai toks pranešimas pareikalautų neproporcingai daug pastangų susiekti su asmenimis (pvz., kai jį kontaktiniai duomenys buvo prarasti dėl asmens duomenų saugumo pažeidimo arba yra nežinomi), tokiu atveju vietoj to apie asmens duomenų saugumo pažeidimą gali būti paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

Pareiga dokumentuoti asmens duomenų saugumo pažeidimus - kaip ir kaip reikia aprašyti?

Kaip teigiama, mintoje situacijoje VDAI sieks išsiaiškinti, ar Vilniaus greitosios pagalbos medicinos stotis dokumentavo šį atvejį kaip asmens duomenų saugumo pažeidimą. Vadovaujantis BDAR 33 str. 5 d., duomenų valdytojas turi dokumentuoti visus duomenų saugumo pažeidimus, nurodydamas su duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kuri buvo imtasi. Remdamasi šiais dokumentais, VDAI turi gauti patikrinti, ar laikomasi šio reikalavimo. Pati [VDAI savo rekomendacijose](#) yra akcentavusi, kad visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, turi būti registruojami duomenų valdytojo Asmens duomenų saugumo pažeidimų žurnale, kuris turi būti tvarkomas raštu, skaitant elektronine forma, jame nurodant:

- visus su asmens duomenų saugumo pažeidimu (toliau - pažeidimas) susijusius faktus – pažeidimo priežastį kas vyko ir kokie asmens duomenys pažeisti;
- pažeidimo poveikį ir pasekmes;
- taisomuosius veiksmus (technines priemones), kuri buvo imtasi;
- priežastis dėl su pažeidimu susijusi sprendimų primimo (pvz., kodėl duomenų valdytojas nusprendė nepranešti apie pažeidimą VDAI ir (ar) duomenų subjektui, t. y. kodėl nusprendė, kad tikėtina, jog pažeidimas negali sukelti pavojaus fizini asmeniui teisms ir laisvėms, arba kokią slygą vykdė, kuomet pranešti apie pažeidimą duomenų subjektui nereikia);
- pranešimo VDAI pateikimo įvykimo priežastis (jeigu pranešimas įvykdomas pateikti ar pranešimas teikiamas etapais);
- informaciją, susijusią su pranešimu duomenų subjektui (pvz., ar buvo pranešta, kodėl nepranešta ir pan.);
- kitą reikšmingą informaciją, susijusią su pažeidimu (pvz., kad tyrimo metu nustatyta, jog faktiškai pažeidimo nebuvo, o buvo tik saugumo incidentas).

Vis ši informaciją Vilniaus greitosios medicinos stotis, kaip ir bet kuris kitas VDAI paprašytas duomenų valdytojas, turi pateikti VDAI.

Kokios galimos nepranešimo apie asmens duomenų saugumo pažeidimą pasekmės?

Už BDAR 33-34 str. numatytą pareigą neįvykdinimą duomenų valdytojai gali būti taikoma atsakomybė ir skiriama bauda iki 10 000 000 EUR arba, mone atveju – iki 2 % jos ankstesni finansiniai meta bendros metinės pasaulinės apyvartos, atsižvelgiant tai, kuri suma yra didesnė. Už nepranešimą apie duomenų saugumo pažeidimą ir kitus susijusius pažeidimus vienai finansinei paslaugai monei VDAI jau yra skyrusi ženkli baudą, siekusi 61 500 eur. Anot advokato Laimono Marcinkevičiaus, nežinant vis faktinių aplinkybių, sudtinga spręsti, ar Greitosios medicinos pagalbos stotis bus pripažinta pažeidusi savo, kaip duomenų valdytojo, pareigas ir, ar bus taikoma atsakomybė. Bet kuriuo atveju, manytina, bus atsižvelgta į pažeidimo sunkumą ir galimai didelę nukentėjusių žmonių skaičių, ar pažeidimas buvo tyčinis, ar vykdytas dėl aplaidumo, ar duomenų valdytojas/duomenų tvarkytojas msi veiksmų žalai sumažinti, technines bei organizacines priemones, kurias gyvendino duomenų valdytojas/duomenų tvarkytojas ir pan.

Doctype	plain-confluence-page
---------	-----------------------

Nuorodos

<http://lrt.lt>

https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_ADSP_2018.pdf

<https://www.lrt.lt/naujienos/lietuvoje/2/1186311/greitosios-pagalbos-medikai-skambina-pavojaus-varpais-is-stoties-duomenu-bazes-issluoti-pacientu-duomenys>

Blog: Per milijoną asmenų galio nukentėti dingus į asmens duomenims iš Greitosios medicinos pagalbos stoties serverio

