

Incidentas V Registr centre: aktualios nuostatos dėl incidento tyrimo kiekvienam duomen valdytojui



2020-ųjų metų gegužės 24 d. Valstybinės duomenų apsaugos inspekcijos (VDAI) tinklalapyje buvo pranešta apie gautą pranešimą dėl Valstybės mokyklos Registrų centro vykusio incidento, kurio metu buvo sutrikdytos mokyklos informacinės sistemos. Dėl šio incidento kilo grėsmė šiose sistemose saugomiems asmens duomenims. Visuomenė informuota, kad šiuo metu atliekamas vidinis incidento ir galimo asmens duomenų saugumo pažeidimo tyrimas, kurio metu atlikti kiekvienas duomenų valdytojas, nustats arba sužinoys, kad buvo galimai neteisingai arba neteisingai sunaikinti, prarasti, pakeisti, be leidimo atskleisti persiųsti, saugomi ar kitaip tvarkomi asmens duomenys arba prie jų be leidimo gauta prieiga. Kuo vadovautis ir kaip atlikti galimo duomenų saugumo pažeidimo tyrimą, kad būtų užtikrinta Bendrojo duomenų apsaugos reglamento (BDAR) nuostatų atitikties?

Teisės aktai, kuriais reikalinga vadovautis atliekant galimo duomenų saugumo pažeidimo tyrimą

Duomenų valdytojas, tirdamas duomenų saugumo incidentą (galimą duomenų saugumo pažeidimą), turėtų vadovautis pagal BDAR 33-34 straipsnių nuostatas, 29 straipsnio duomenų apsaugos darbo grupės gairėmis dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679, Patvirtinta 2017 m. spalio 3 d. Paskutinį kartą peržiūrta ir patvirtinta 2018 m. vasario 6 d., Valstybinės duomenų apsaugos inspekcijos (VDAI) 2018 m. gegužės 02 d. rekomendacija „Dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos“ parengta ir patvirtinta Duomenų valdytojo asmens duomenų saugumo pažeidimų fiksavimo, tyrimo, dokumentavimo ir pranešimo apie juos VDAI bei duomenų [subjektams](#) tvarka. Šioje tvarkoje rekomenduojama numatyti procesus, kuriuos reikia laikytis vykus pažeidimui:

Procesai, kuriuos reikia laikytis vykus pažeidimui:

- 1) **Pranešimas** apie galimą pažeidimą (rekomenduojama nurodyti, kas (darbuotojai), kada (vos pastebėjus galimą pažeidimą), kam (galiojantiems imtis priemoni) asmenims) ir kokia forma (rekomenduojama informaciją teikti visais manomais būdais) turi pranešti apie galimą pažeidimą ir pan.);
- 2) **Pranešimo tyrimo eiga** (rekomenduojama nurodyti, koks saugumo incidentas tiriamas, kokių būdu vertinama rizika, kada pranešama VDAI ir (ar) duomenų subjektui ir pan.);
- 3) **Pažeidimų dokumentavimas** (rekomenduojama nurodyti, kas [registruoja](#) asmens duomenų saugumo pažeidimus, kokia informacija turėtų būti rašyta Asmens duomenų saugumo pažeidimų žurnale, kur ir kokia forma šis žurnalas pildomas, kiek laiko saugomas ir pan.);
- 4) **Tyrimo rezultatų formavimas**, pažeidimų analizė ir prevencijos priemonių įgyvendinimo kontrolė (numatant, kada peržiūrėti žurnale esantys rašai, kada atliekama pažeidimų analizė ir prevencijos priemonių įgyvendinimas).

Galimo duomenų saugumo pažeidimo tyrimo eiga

Vadovaujantis Valstybins duomen apsaugos inspekcijos (VDAI) 2018 m. liepos 02 d. rekomendacija „Dl asmens duomen saugumo pažeidim nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos“, sužinojs apie galim asmens duomen saugumo pažeidim, už j tyrim organizacijos paskirtas atsakingas asmuo turi atlikti pirmin tyrim, kurio metu turi vertinti galimas pasekmes asmenims, t.y., vertinti rizik.

Pirmiausia reikalinga nustatyti, koks pažeidimo pobdis (tipas). Vadovaujantis minta rekomendacija, galimi pažeidimo tipai:

- 1) konfidencialumo pažeidimas** – kai yra be leidimo ar neteistai atskleidžiami asmens duomenys arba gaunama prieiga prie j;
- 2) prieinamumo pažeidimas** – kai netyia arba neteistai prarandama prieiga prie arba sunaikinami asmens duomenys;
- 3) vientisumo pažeidimas** – kai asmens duomenys pakeičiami be leidimo ar netyia.

Priklausomai nuo aplinkybi, Pažeidimas tuo pat metu gali sietis su asmens duomen konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors j deriniu.

Priklausomai nuo pažeidimo pobdžio (tipo), atliekant pirmin tyrim ir siekiant nustatyti, ar pažeidimas iš tikrj vyko, turt bti išsaugomi esamos situacijos rodymai bei vliau naudojamos visos tinkamos technins ir organizacins priemonis, pvz., duomen srauto ir prisijungim analizs rankiai bei kt.

Vertinant rizik, kuri gali atsirasti dl pažeidimo, turt bti atsižvelgiama konkreias pažeidimo aplinkybes, pavojaus duomen subjekto teisms ir laisvms atsiradimo tikimyb ir rimtum.

Rizika turt bti vertinama remiantis objektyviu vertinimu ir atsižvelgiant šiuos kriterijus:

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

Vertinant rizik, turt bti laikoma, kad pažeidimas, galintis kelti pavoj asmen teisms ir laisvms yra toks, dl kurio, laiku nesimus tinkam priemoni, fiziniai asmenys gali patirti kno sužalojim, materialin ar nematerialin žal, pvz., prarasti savo asmens duomen kontrol, patirti teisi apribojim, diskriminacij, gali bti pavogta ar suklastota jo asmens tapatyb, jam padaryta finansini nuostoli, neleistina panaikinti pseudonimai, gali bti pakenkta jo reputacijai, prarastas asmens duomen, kurie saugomi profesine paslaptimi.

vertinus rizik rekomenduojama nustatyti rizikos tikimybės dyd:

- 1) žema rizikos tikimyb;
- 2) vidutin rizikos tikimyb;
- 3) didel (aukšta) rizikos tikimyb.

vertins ir nustats mintus aspektus organizacijos atsakingas asmuo turi pateikti duomen valdytojo vadovui (ar jo galiotam asmeniui) išvad dl pažeidimo buvimo ir rizikos fizini asmen teisms bei laisvms vertinimo. Duomen valdytojo vadovas (ar jo galiotas asmuo) turi priimti sprendim dl tolimesni veiksm, susijusi su asmens duomen saugumo pažeidimu. Rizikoms vertinti gali bti naudojamas naudoti Allaw [Rizik fizini asmen teisms ir laisvms pagal BDAR vertinimo rankis](#).

Pranešimai VDAI ir duomen subjektams

Vadovaujantis BDAR 33 str. 3 d. ir Valstybins duomen apsaugos inspekcijos (VDAI) [2018 m. liepos 02 d. rekomendacija „Dl asmens duomen saugumo pažeidim nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos“](#), 29 straipsnio duomen apsaugos darbo grups gairimis dl pranešimo apie asmens duomen saugumo pažeidim pagal Reglament (ES) 2016/679, Patvirtinta 2017 m. spalio 3 d. Paskutin kart peržiurta ir patvirtinta 2018 m. vasario 6 d. tais atvejais, kai nustatoma, kad asmens duomen saugumo pažeidimas kelia pavoj asmen teisms ir laisvms duomen valdytojas turi pranešti Valstybinei duomen apsaugos inspekcijai (VDAI), užpildydamas VDAI direktoriaus patvirtint form ir nepraleisdamas 72 val. termino. Jeigu nustatoma, kad dl asmens duomen saugumo pažeidimo gali kilti didelis pavojus fizini asmen teisms ir laisvms duomen valdytojas turi pranešti ir duomen subjektams.

DAP vaidmuo duomen saugumo incident tyrime

Remiantis BDAR 39 str. 1 d. a) ir b) punktais [duomen apsaugos pareignas](#) informuoja duomen valdytoj (tvarkytoj) ir jo darbuotojus apie j prievoles ir stebi, kaip laikomasi BDAR bei konsultuoja ir atlieka kontaktinio asmens [funkcijas](#) kreipiantis ar teikiant pranešimus VDAI ar duomen subjektams. Remiantis 29 straipsnio duomen apsaugos darbo grups nuomone, vykus duomen saugumo pažeidimui ar kitam incidentui **visada privaloma nedelsiant pasikonsultuoti su duomen apsaugos pareignu**. Taigi, visuose aukšiau pamintuose procesuose duomen valdytojas gali tiktis DAP pagalbos, t.y., duomen apsaugos pareignas ne tik teikia konsultacijas, padeda numatyti pažeidimo valdymo ir prevencijos priemones, teikia išvadas dl pažeidimo buvimo ir rizikos fizini asmen teisms bei laisvms vertinimo, bet ir teikia pranešimus VDAI ir duomen subjektams dl vykusio duomen saugumo pažeidimo ir padeda dokumentuoti organizacijoje vykusius duomen saugumo incidentus.

vykusi duomen saugumo incident dokumentavimas

Vadovaujantis BDAR 33 str. 5 d. ir Valstybės duomen apsaugos inspekcijos (VDAI) [2018 m. liepos 02 d. rekomendacija „Dl asmens duomen saugumo pažeidim nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos“](#), 29 straipsnio duomen apsaugos darbo grups gairėmis dl pranešimo apie asmens duomen saugumo pažeidim pagal Reglament (ES) 2016/679, Patvirtinta 2017 m. spalio 3 d. Paskutin kart peržiūrta ir patvirtinta 2018 m. vasario 6 d. visi asmens duomen saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, turt bti registruojami duomen valdytojo Asmens duomen saugumo pažeidim registravimo žurnale.

Informacija apie asmens duomen saugumo pažeidim Asmens duomen saugumo pažeidim registravimo žurnal turt bti vedama nedelsiant, kai tik nustatomas asmens duomen saugumo pažeidimo faktas ir vertinama rizika (rekomenduotina ne ilgiau kaip per 5 darbo dienas). Esant btinybei, mintame žurnale esanti informacija turt bti papildoma ir (ar) koreguojama. Asmens duomen saugumo pažeidim registravimo žurnalas turt bti tvarkomas raštu, skaitant elektronine form, ir saugomas pagal duomen valdytojo patvirtint dokument saugojimo tvark.

Asmens duomen saugumo pažeidim registravimo žurnale turt bti nurodoma:

- 1) visi su asmens duomen saugumo pažeidimu susij faktai – pažeidimo priežastis, kas vyko ir kokie asmens duomenys pažeisti;
- 2) asmens duomen saugumo pažeidimo poveikis ir pasekms;
- 3) taisomieji veiksmai (technins priemonės), kuri buvo imtasi;
- 4) priežastys dl su asmens duomen saugumo pažeidimu susijusi sprendim primimo (pvz., kodl duomen valdytojas nusprend nepranešti apie pažeidim VDAI ir (ar) duomen subjektui, t. y. kodl nusprend, kad tikina, jog pažeidimas negali sukelti pavojaus fizini asmen teisms ir laisvms, arba koki slyg vykd, kuomet pranešti apie Pažeidim duomen subjektui nereikia);
- 5) pranešimo VDAI pateikimo vlavimo priežastys (jeigu pranešim vluojama pateikti ar pranešimas teikiamas etapais);
- 6) informacija, susijusi su pranešimu duomen subjektui (pvz., ar buvo pranešta, kodl nepranešta ir pan.);
- 7) kita reikšminga informacija susijusi su asmens duomen saugumo pažeidimu (pvz., kad tyrimo metu nustatyta, jog faktiškai pažeidimo nebuvo, o buvo tik saugumo incidentas).

Duomen valdytojas turt paskirti asmen (darbuotoj), atsaking už Asmens duomen saugumo pažeidim registravimo žurnalo pildym. Remdamasi mintame žurnale pateikta informacija, VDAI turi galti patikrinti, kaip gyvendinama duomen valdytojo prievol pranešti apie asmens duomen saugumo pažeidimus.

VDAI rekomenduoja periodiškai peržiūrėti Asmens duomen saugumo pažeidim registravimo žurnale esančius rašus ir numatyti, kokios prevencijos priemonės turt bti gyvendintos bei kaip bus kontroliuojamas ši prevencijos priemoni diegimas, kad ateityje analogiški pažeidimai nesikartot.

Duomen saugumo incident prevencija

Siekiant išvengti duomen saugumo pažeidim, itin svarbu taikyti tinkamas ir duomen tvarkymo proces keliamas rizikas atitinkanias bei nuolat atnaujinamas technines ir organizacines duomen saugumo priemones. Labai svarbu skirti dmes atitiktis teis akt reikalavimams bkls stebjimui bei kad parengti dokumentai: veiklos tstinimo planas, atsargini kopij atlikimo tvarkos aprašas bei kitos organizacins ir technins priemonės bt tinkamai taikomos, periodiškai peržiūrimos, tikrinamas j efektyvumas ir nustaus poreik gyvendinamas j atnaujinimas. Duomen apsaugos teis akt stebsen atlikti ir incident prevencij organizacijoms vykdyti padeda Allaw komanda ir jos naudojamas rankis [Duomen apsaugos teisinio reguliavimo stebjimo rankis](#).

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

Nuorodos

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

Blog: [Incidentas V Registr centre: aktualios nuostatos dl incident tyrimo kiekvienam duomen valdytojui](#)