Incidentas V Registr centre: aktualios nuostatos dl incident tyrimo kiekvienam duomen valdytojui

2020-j met iepos 24 d. Valstybins duomen apsaugos inspekcijos (VDAI) tinklalapyje buvo pranešta apie gaut pranešim dl Valstybs monje Registr centras vykusio incidento, kurio metu buvo sutrikdytos mintos mons informacins sistemos. Dl šio incidento kilo grsm šiose sistemose saugomiems asmens duomenims. Visuomen informuota, kad šiuo metu atliekamas vidinis incidento ir galimo asmens duomen saugumo pažeidimo tyrimas, kur turi atlikti kiekvienas duomen valdytojas, nustats arba sužinojs, kad buvo galimai netyia arba neteistai sunaikinti, prarasti, pakeisti, be leidimo atskleisti persisti, saugomi ar kitaip tvarkomi asmens duomenys arba prie j be leidimo gauta prieiga. Kuo vadovautis ir kaip atlikti galimo duomen saugumo pažeidimo tyrim, kad bt užtikrinta Bendrojo duomen apsaugos reglamento (BDAR) nuostat atitiktis?

Teiss aktai, kuriais reikalinga vadovautis atliekant galimo duomen saugumo pažeidimo tyrim

Duomen valdytojas, tirdamas duomen saugumo incident (galim duomen saugumo pažeidim), turt vadovautis pagal BDAR 33-34 str. nuostatas, 29 straipsnio duomen apsaugos darbo grups gairmis dl pranešimo apie asmens duomen saugumo pažeidim pagal Reglament (ES) 2016/679, Patvirtinta 2017 m. spalio 3 d. Paskutin kart peržirta ir patvirtinta 2018 m. vasario 6 d., Valstybins duomen apsaugos inspekcijos (VDAI) 2018 m. liepos 02 d. rekomendacija „Dl asmens duomen saugumo pažeidim nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos“ parengta ir patvirtinta Duomen valdytojo asmens duomen saugumo pažeidim fiksavimo, tyrimo, dokumentavimo ir pranešimo apie juos VDAI bei duomen subjektams tvarka. Šioje tvarkoje rekomenduojama numatyti procesus, kuri reikia laikytis vykus pažeidimui:

Procesai, kuri reikia laikytis vykus pažeidimui:

1) Pranešimas apie galim pažeidim (rekomenduojama nurodyti, kas (darbuotojai), kada (vos pastebjus galim pažeidim), kam (galiotiems imtis priemoni asmenims) ir kokia forma (rekomenduotina informacij teikti visais manomais bdais) turi pranešti apie galim pažeidim ir pan.);

2) Pranešim tyrimo eiga (rekomenduojama nurodyti, koks saugumo incidentas tiriamas, kokiu bdu vertinama rizika, kada pranešama VDAI ir (ar) duomen subjektui ir pan.);

3) Pažeidim dokumentavimas (rekomenduojama nurodyti, kas registruoja asmens duomen saugumo pažeidimus, kokia informacija turt bti rašyta Asmens duomen saugumo pažeidim žurnale, kur ir kokia forma šis žurnalas pildomas, kiek laiko saugomas ir pan.);

4) Tyrimo rezultat forminimas, pažeidim analiz ir prevencijos priemoni gyvendinimo kontrol (numatant, kada peržirimi žurnale esantys rašai, kada atliekama pažeidim analiz ir prevencijos priemoni gyvendinimas).

Galimo duomen 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 pakeiiami 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 priemons, 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, neleistinai panaikinti pseudonimai, gali bti pakenkta jo reputacijai, prarastas asmens duomen, kurie saugomi profesine paslaptimi.

vertinus rizik rekomenduojama nustatyti rizikos tikimybs 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 gairmis dl pranešimo apie asmens duomen saugumo pažeidim pagal Reglament (ES) 2016/679, Patvirtinta 2017 m. spalio 3 d. Paskutin kart peržirta 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 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 gairmis dl pranešimo apie asmens duomen saugumo pažeidim pagal Reglament (ES) 2016/679, Patvirtinta 2017 m. spalio 3 d. Paskutin kart peržirta 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 priemons), 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 tiktina, 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 peržirti Asmens duomen saugumo pažeidim registravimo žurnale esanius rašus ir numatyti, kokios prevencijos priemons 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 atitikties teiss akt reikalavimams bkls stebjimui bei kad parengti dokumentai: veiklos tstinumo planas, atsargini kopij atlikimo tvarkos aprašas bei kitos organizacins ir technins priemons bt tinkamai taikomos, periodiškai peržirimos, tikrinamas j efektyvumas ir nustaius poreik gyvendinamas j atnaujinimas. Duomen apsaugos teiss 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