2018 m. liepos 2 d.

Apie asmens duomenų saugumo pažeidimus

1. Pranešimai apie asmens duomenų saugumo pažeidimus teikiami Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) ir duomenų subjektams, vadovaujantis:

1.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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) (toliau – BDAR) 33 ir 34 straipsniais;

1.2. Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo (toliau – Įstatymas) 29 ir 30 straipsniais.

2. Šioje rekomendacijoje vartojamos sąvokos atitinka BDAR ir Įstatyme vartojamas sąvokas. Asmens duomenų saugumo pažeidimas šiuose teisės aktuose apibrėžiamas kaip:

2.1. **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 punktas);

2.2. **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio neatsargiai arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (Įstatymo 2 straipsnio 2 dalis).

3. VDAI apie asmens duomenų saugumo pažeidimą (toliau – Pažeidimas) privalo pranešti visi duomenų valdytojai pateikdami pranešimą apie asmens duomenų saugumo pažeidimą (toliau – Pranešimas), išskyrus, kai tikėtina, kad toks Pažeidimas nekels pavojaus asmenų teisėms ir laisvėms. Kai dėl Pažeidimo pobūdžio ir rizikos rimtumo kyla didelė grėsmė fizinių asmenų teisėms ir laisvėms, duomenų valdytojas apie Pažeidimą privalo pranešti ir duomenų subjektui.

4. Siekiant tinkamai įgyvendinti BDAR reikalavimus, susijusius su Pažeidimais, rekomenduotina atsižvelgti į Europos Parlamento ir Tarybos direktyvos 95/46/EB 29 straipsnio darbo grupės 2017 m. spalio 3 d. parengtas Pranešimo apie asmens duomenų saugumo pažeidimą gaires pagal Reglamentą 2016/679.

Pranešimas apie galimą asmens duomenų saugumo pažeidimą

5. Rekomenduotina, kad duomenų valdytojas ir duomenų tvarkytojas patvirtintų rašytinį dokumentą, reglamentuojantį Pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie juos tvarką. Šiame dokumente, atsižvelgiant į atliekamus asmens duomenų tvarkymo veiksmus, turėtų būti aprašyti procesai, kurių reikia laikytis įvykus Pažeidimui:

5.1. Pranešimas apie galimą Pažeidimą (rekomenduojama nurodyti, kas (darbuotojai), kada (vos pastebėjus galimą Pažeidimą), kam (įgaliotiems imtis priemonių asmenims) ir kokia forma (rekomenduotina informaciją teikti visais įmanomais būdais) turi pranešti apie galimą Pažeidimą ir pan.);

5.2. Pranešimų tyrimo eiga (rekomenduojama nurodyti, koks saugumo incidentas tiriamas, kokiu būdu vertinama rizika, kada pranešama VDAI ir (ar) duomenų subjektui ir pan.);

5.3. Pažeidimų dokumentavimas (rekomenduojama nurodyti, kas registruoja Pažeidimus, kokia informacija turėtų būti įrašyta Asmens duomenų saugumo pažeidimų žurnale (toliau – Žurnalas), kur ir kokia forma šis Žurnalas pildomas, kiek laiko saugomas ir pan.);

5.4. Tyrimo rezultatų įforminimas, Pažeidimų analizė ir prevencijos priemonių įgyvendinimo kontrolė (numatant, kada peržiūrimi Žurnale esantys įrašai, kada atliekama Pažeidimų analizė ir prevencijos priemonių įgyvendinimas).

6. Duomenų valdytojas ir duomenų tvarkytojas privalo informuoti darbuotojus apie jų pareigą pranešti apie galimus Pažeidimus ir supažindinti juos su nustatyta pranešimų apie Pažeidimus pateikimo tvarka.

7. Duomenų valdytojas ir duomenų tvarkytojas turėtų paskirti asmenį ar skyrių, atsakingą už Pažeidimų valdymą (toliau – Atsakingas asmuo), pvz., už Pažeidimų tyrimą, pranešimų VDAI ir duomenų subjektui teikimą, prevencinių priemonių įdiegimo kontrolę ir pan.

8. Duomenų valdytojo ir duomenų tvarkytojo darbuotojas, sužinojęs ar pats nustatęs galimą Pažeidimą arba kai informacija apie galimą Pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio, privalo nedelsdamas apie tai informuoti Atsakingą asmenį (priklausomai nuo organizacijos dydžio, pobūdžio ar pan.). Pranešimas galėtų būti pateikiamas žodžiu, raštu ar elektroninėmis priemonėmis.

9. Duomenų tvarkytojas, sužinojęs apie Pažeidimą, turėtų nedelsdamas (rekomenduotina ne ilgiau kaip per 24 val.) apie tai pranešti duomenų valdytojui. Apie tokią pareigą duomenų valdytojas turėtų iš anksto informuoti duomenų tvarkytoją (pvz., sudaromoje duomenų tvarkymo sutartyje).

10. Duomenų tvarkytojas apie Pažeidimą gali pranešti tiesiogiai VDAI, jeigu tai yra aiškiai numatyta duomenų tvarkymo sutartyje su duomenų valdytoju. Tačiau bet kuriuo atveju teisinę prievolę pranešti VDAI turi duomenų valdytojas.

11. Atsakingas asmuo apie Pažeidimą taip pat turėtų informuoti duomenų apsaugos pareigūną (jeigu toks yra paskirtas) bei laiku ir tinkamai suteikti jam visą informaciją, susijusią su galimu Pažeidimu.

Asmens duomenų saugumo pažeidimo tyrimas

12. Atsakingas asmuo, sužinojęs apie galimą Pažeidimą, turėtų kaip įmanoma greičiau atlikti pirminį tyrimą, išsiaiškinti ir nustatyti, ar Pažeidimas iš tikrųjų įvyko, bei kokios galimos pasekmės asmenims (t. y. įvertinti riziką).

13. Galimi Pažeidimo tipai:

13.1. „Konfidencialumo Pažeidimas“ – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

13.2. „Prieinamumo Pažeidimas“ – kai netyčia arba neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;

13.3. „Vientisumo Pažeidimas“ – kai asmens duomenys pakeičiami be leidimo ar netyčia.

Priklausomai nuo aplinkybių, Pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

14. Priklausomai nuo Pažeidimo pobūdžio (tipo), atliekant pirminį tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, turėtų būti išsaugomi esamos situacijos įrodymai bei vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės, pvz., duomenų srauto ir prisijungimų analizės įrankiai bei kt.

15. Vertinant riziką, kuri gali atsirasti dėl Pažeidimo, turėtų būti atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika turėtų būti vertinama remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus:

15.1. Pažeidimo tipą;

15.2. Asmens duomenų pobūdį, apimtis (pvz., specialių kategorijų asmens duomenys);

15.3. Kaip lengvai identifikuojamas fizinis asmuo;

15.4. Pasekmių rimtumą fiziniams asmenims;

15.5. Specialias fizinio asmens savybes (pvz., duomenys susiję su vaikais ar kitais pažeidžiamais asmenimis);

15.6. Nukentėjusiųjų fizinių asmenų skaičių;

15.7. Specialias duomenų valdytojo savybes (pvz., veiklos pobūdį).

16. Vertinant riziką, turėtų būti laikoma, kad Pažeidimas, galintis kelti pavojų asmenų teisėms ir laisvėms yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą, pvz., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

17. Įvertinus riziką rekomenduotina nustatyti, kad yra:

17.1. Žema rizikos tikimybė;

17.2. Vidutinė rizikos tikimybė;

17.3. Didelė (aukšta) rizikos tikimybė.

18. Išvadą dėl Pažeidimo buvimo ir rizikos fizinių asmenų teisėms bei laisvėms įvertinimo Atsakingas asmuo turėtų pateikti duomenų valdytojo vadovui (ar jo įgaliotam asmeniui). Duomenų valdytojo vadovas (ar jo įgaliotas asmuo) turi priimti sprendimą dėl tolimesnių veiksmų, susijusių su Pažeidimu.

19. Atsakingas asmuo visų pirma turėtų imtis visų tinkamų techninių ir organizacinių priemonių, kad Pažeidimas būtų išsamiai ištirtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų ir tuomet pateikti Pranešimą VDAI.

Pranešimas priežiūros institucijai

20. Nustačius, kad Pažeidimas buvo ir, kad yra rizika fizinių asmenų teisėms ir laisvėms, Atsakingas asmuo nedelsdamas, ne vėliau kaip per 72 val. nuo sužinojimo apie Pažeidimą, turėtų pranešti apie tai VDAI [1].

21. Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie Pažeidimą VDAI, rekomenduotina pranešti.

22. Jeigu, priklausomai nuo Pažeidimo pobūdžio, duomenų valdytojui yra būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su Pažeidimu (pvz., dar nėra išsiaiškinta Pažeidimo apimtis), ir per 72 val. nuo sužinojimo apie Pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, Pranešimui reikalinga informacija galėtų būti teikiama etapais. Esant galimybei, apie informacijos teikimą etapais, VDAI turėtų būti informuota teikiant pirminį Pranešimą.

23. Jeigu po Pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo jokio Pažeidimo, apie tai nedelsiant turėtų būti informuojama VDAI ir pažymėta Žurnale.

[1] Žr. VDAI direktoriaus įsakymus, kuriais patvirtinta Pranešimo rekomenduojama forma, pateikimo tvarka ir sąlygos.

24. Jeigu Pažeidimas paveikia fizinių asmenų duomenis daugiau negu vienoje valstybėje narėje ir yra reikalinga pranešti priežiūros institucijai, duomenų valdytojas turėtų pranešti vadovaujančiai priežiūros institucijai (BDAR preambulės 55 punktas). Jeigu duomenų valdytojas abejoja kuri priežiūros institucija yra vadovaujanti, bet Pažeidimas įvyko Lietuvos Respublikoje, tuomet jis turėtų pranešti VDAI. Šiuo atveju, teikiant Pranešimą, rekomenduotina nurodyti, ar toks Pažeidimas apima ir kitose valstybėse narėse esančias duomenų valdytojo buveines, ir kuriose valstybėse narėse esančius duomenų subjektus Pažeidimas galėjo paveikti.

Pranešimas duomenų subjektui

25. Nustačius, kad Pažeidimas buvo ir, kad yra didelė rizika fizinių asmenų teisėms ir laisvėms, Atsakingas asmuo nedelsdamas (rekomenduojama per 72 val.) apie tai turėtų pranešti duomenų subjektui, kurio teisėms ir laisvėms dėl šio Pažeidimo gali kilti didelis pavojus.

26. VDAI informavimas apie Pažeidimą neatleidžia duomenų valdytojo nuo pareigos informuoti duomenų subjektą.

27. Pranešime duomenų subjektui aiškia ir paprasta kalba turėtų būti pateikiama:

27.1. Pažeidimo pobūdžio aprašymas;

27.2. Duomenų apsaugos pareigūno arba kito kontaktinio asmens vardas, pavardė (pavadinimas) ir kontaktiniai duomenys;

27.3. Tikėtinų Pažeidimo pasekmių aprašymas;

27.4. Priemonių, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas Pažeidimas, įskaitant (kai tinkama) priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas (pvz., kad apie Pažeidimą yra informuota VDAI ir, kad yra gautas patarimas dėl Pažeidimo tvarkymo ir jo poveikio sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);

27.5. Kita reikšminga informacija, susijusi su Pažeidimu, kuri, duomenų valdytojo manymu, turėtų būti pateikta duomenų subjektui.

28. Duomenų subjektai apie Pažeidimą turėtų būti informuoti tiesiogiai, pvz., siunčiant jiems pranešimą el. paštu, SMS, paštu ar pan. Šis pranešimas turėtų būti atskirtas nuo kitos siunčiamos informacijos, tokios kaip nuolatiniai atnaujinimai, naujienlaiškiai ar standartiniai pranešimai.

29. Kai tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai daug pastangų, vietoj to apie įvykusį Pažeidimą gali būti paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai, pvz., pranešimas žinomos interneto svetainės antraštėje ar pranešimuose, žinomos reklamos spausdintoje žiniasklaidoje ar pan.

30. Duomenų valdytojas turėtų pasirinkti tokius pranešimo duomenų subjektui būdus, kurie maksimaliai didintų galimybę tinkamai pranešti informaciją visiems nukentėjusiems asmenims.

31. Duomenų valdytojas gali pasirinkti kelis pranešimo duomenų subjektui apie Pažeidimą būdus.

32. Esant Pažeidimui, pranešimo duomenų subjektui teikti nereikia, jeigu:

32.1. Duomenų valdytojas įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikio;

32.2. Iš karto po Pažeidimo duomenų valdytojas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus asmenų teisėms ir laisvėms;

32.3. Tai pareikalautų neproporcingai daug pastangų susisiekti su asmenimis (pvz., kai jų kontaktiniai duomenys buvo prarasti dėl Pažeidimo arba pirma nežinomi). Tokiu atveju vietoj to apie Pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

33. Duomenų valdytojas turėtų gebėti įrodyti VDAI, kad jis įvykdė vieną ar daugiau šių rekomendacijų 31 punkte nurodytų sąlygų.

34. Jeigu tiriant Pažeidimą pradžioje nustatoma, kad nėra pavojaus fizinių asmenų teisėms ir laisvėms, tačiau detalesnio Pažeidimo tyrimo metu nustatoma, kad toks pavojus gali kilti, duomenų valdytojas turėtų riziką vertinti iš naujo.

Asmens duomenų saugumo pažeidimų dokumentavimas

35. Visi Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, turėtų būti registruojami duomenų valdytojo Žurnale.

36. Informacija apie Pažeidimą į Žurnalą turėtų būti įvedama nedelsiant, kai tik nustatomas Pažeidimo faktas ir įvertinama rizika (rekomenduotina ne ilgiau kaip per 5 darbo dienas). Esant būtinybei, Žurnale esanti informacija turėtų būti papildoma ir (ar) koreguojama.

37. Žurnale turėtų būti nurodoma:

37.1. Visi su Pažeidimu susiję faktai – Pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

37.2. Pažeidimo poveikis ir pasekmės;

37.3. Taisomieji veiksmai (techninės priemonės), kurių buvo imtasi;

37.4. Priežastys dėl su Pažeidimu susijusių sprendimų priėmimo (pvz., kodėl duomenų valdytojas nusprendė nepranešti apie Pažeidimą VDAI ir (ar) duomenų subjektui, t. y. kodėl nusprendė, kad tikėtina, jog Pažeidimas negali sukelti pavojaus fizinių asmenų teisėms ir laisvėms, arba kokią sąlygą įvykdė, kuomet pranešti apie Pažeidimą duomenų subjektui nereikia);

37.5. Pranešimo VDAI pateikimo vėlavimo priežastys (jeigu Pranešimą vėluojama pateikti ar Pranešimas teikiamas etapais);

37.6. Informacija, susijusi su pranešimu duomenų subjektui (pvz., ar buvo pranešta, kodėl nepranešta ir pan.);

37.7. Kita reikšminga informacija susijusi su Pažeidimu (pvz., kad tyrimo metu nustatyta, jog faktiškai Pažeidimo nebuvo, o buvo tik saugumo incidentas).

38. Žurnalas turėtų būti tvarkomas raštu, įskaitant elektronine formą, ir saugomas pagal duomenų valdytojo patvirtintą dokumentų saugojimo tvarką.

39. Duomenų valdytojas turėtų paskirti asmenį (darbuotoją), atsakingą už Žurnalo pildymą.

40. Remdamasi Žurnale pateikta informacija, VDAI turi galėti patikrinti, kaip įgyvendinama duomenų valdytojo prievolė pranešti apie Pažeidimus.

41. Rekomenduotina periodiškai peržiūrėti Žurnale esančius įrašus ir numatyti, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip bus kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje analogiški Pažeidimai nesikartotų.