

REAGAVIMO Į ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS APRAŠAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Reagavimo į asmens duomenų saugumo pažeidimus procedūros aprašas (toliau – Aprašas) nustato Biudžetinės įstaigos VDU „Atžalyno“ progimnazijos, įstaigos kodas 290136920, registracijos adresas Partizanų g. 46, LT-49460 Kaunas (toliau – Įstaiga) darbuotojų, dirbančių pagal darbo sutartis, veiksmus, įvykus duomenų saugumo pažeidimui, jų išaiškinimo, pranešimo priežiūros institucijai, duomenų subjektams tvarką, pažeidimo prevencinio plano sudarymo bei kitus atvejus, įgyvendinant 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 straipsnių reikalavimus.

2. Aprašu privalo vadovautis:

2.1. Įstaigos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo ar kitas sutartis (toliau – darbuotojai);

2.2. Įstaigos duomenų tvarkytojai, kuriems pavesta laikytis Aprašo duomenų tvarkymo sutartyje nustatyta tvarka ir apimtimi.

3. Darbuotojai privalo užtikrinti, kad Įstaigos pasitelkiami duomenų tvarkytojai, be kitų reikalavimų, numatytų BDAR 28 straipsnyje, būtų įpareigoti laikytis atitinkamų Apraše numatytų reikalavimų, užtikrinančių pareigą duomenų tvarkytojui tinkamai informuoti Įstaigą apie jos pavedimu tvarkomų duomenų pažeidimą, bendradarbiauti aiškinantis duomenų saugumo pažeidimo priežastis, teikti visą reikiamą informaciją, kad Įstaiga galėtų tinkamai įgyvendinti visas duomenų valdytojui tenkančias pareigas, numatytas BDAR.

4. Apraše vartojamos sąvokos:

4.1. **duomenų saugumo pažeidimas** – bet koks įvykis, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga;

4.2. **priežiūros institucija** – valstybės narės pagal BDAR 51 straipsnį įsteigta nepriklausoma valdžios institucija. Įstaigos atžvilgiu tai Valstybinė duomenų apsaugos inspekcija (įmonės kodas 188607912, A. Juozapavičiaus g. 6, 09310 Vilnius, el. paštas ada@ada.lt);

4.3. kitos Apraše vartojamos sąvokos atitinka BDAR įtvirtintas sąvokas.

II SKYRIUS

DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMAS IR ANALIZĖ

5. Duomenų saugumo pažeidimu (toliau – Pažeidimas) laikomas bet koks saugumo incidentas, dėl kurio įvyksta vienas arba keli toliau numatyti pažeidimai:

5.1. konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama (gaunama) prieiga tam teisės neturintiems asmenims, pavyzdžiui, duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio paviešinimas, praradimas, atskleidimas kitam darbuotojui, nešiojamojo kompiuterio, kuriame sukaupti duomenys, praradimas, popierinių dokumentų praradimas, vagystė ir pan.;

5.2. pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami. Tokio pobūdžio pažeidimu galėtų būti laikomas duomenų bazės ištrynimasis, praradimas (vagystė), sunaikinimas, pavyzdžiui, gaisro, liūties atveju ir nesant atsarginės kopijos, iš kurios būtų galima atkurti prarastus duomenis. Pasiekiamumo pažeidimu laikytinas ir įprastinę Įstaigos veiklą sutrikdęs prieigos prie duomenų praradimas;

5.3. vientisumo pažeidimas – netyčia ar neteisėtai atlikti asmens duomenų pakeitimai. Tai galėtų būti trečiojo asmens, įgijusio neteisėtą prisijungimą prie duomenų bazės, įvykdyti joje esančių įrašų pakeitimai, taip pat programinės įrangos ar kitokie procedūrų sutrikimai, dėl kurių atsiranda duomenų netikslumų arba pasikeitimų.

6. Kai yra nustatomas arba įtariamas pažeidimas, atitinkantis Aprašo 5 reikalavimus, jį nustatęs darbuotojas asmeniškai el. paštu, telefonu ir (arba) kitomis komunikacijos priemonėmis turi kuo skubiau informuoti savo tiesioginį vadovą ir įstaigos duomenų apsaugos pareigūną (toliau – pareigūnas).

7. Darbuotojas arba jo tiesioginis vadovas įstaigos direktoriui ir pareigūnui pateikia jam žinomą pažeidimo nustatymui būtiną informaciją:

7.1. poveikio informacinių technologijų (toliau – IT) infrastruktūrai mastą;

7.2. informacinius išteklius, kuriems gali kilti arba yra kilęs pavojus (kokios duomenų bazės yra arba gali būti paveiktos);

7.3. žinomą arba tikėtiną pažeidimo trukmę (kada įvyko ir kada buvo sustabdytas arba kada, tikėtina, galima būtų tai padaryti);

7.4. paveiktus arba galimai paveiktus duomenų subjektus ir poveikio jiems mastą (ar paveikti tik konkrečios duomenų subjektų grupės duomenys, kokia konkrečios grupės dalis yra paveikta ir pan.);

7.5. pradinius pažeidimo pasekmių požymius (pavyzdžiui, prieigos prie duomenų praradimas, nustatyti neteisėti duomenų pakeitimai, rasti paviešinti duomenys ir pan.).

8. Nustatant pažeidimą ir vykdant jo analizę darbuotojai pažeidimo tyrimo komisijai arba pareigūnui privalo teikti visapusišką, išsamią, tikslią ir operatyvią informaciją dėl galimo pažeidimo.

9. Nustačius pažeidimą, atliekamas pirminis įvykusio galimo pažeidimo vertinimas ir nustatoma, ar egzistuoja šios aplinkybės:

9.1. prarastas arba gali būti prarastas reikšmingas kiekis asmens duomenų, ypač kai pažeidimas susijęs su specialių kategorijų duomenimis arba jautresniais duomenimis, pavyzdžiui, sveikatos duomenimis, religiniais, filosofiniais įsitikinimais, naryste profesinėse sąjungose, lytine orientacija, asmenų teistumu, finansine informacija ir pan. Nereikšmingu kiekiu gali būti laikomas vienkartinis, atsitiktinis duomenų praradimas, pavyzdžiui, elektroninio laiško išsiuntimas ne tam adresatui, popieriaus lapo, bylos praradimas (pametimas);

9.2. Pažeidimas tikėtina gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms;

9.3. daromas poveikis dideliam duomenų subjektų skaičiui, ypač kai poveikis daromas labiau pažeidžiamiems duomenų subjektams, pavyzdžiui, vaikams;

9.4. susiklostė bet kokia kita situacija, kuri gali sukelti reikšmingą poveikį duomenų subjektams ir (arba) įstaigai.

10. Jeigu nustatoma, kad turimais duomenimis Pažeidimas atitinka Aprašo 5 ir 9 punktų kriterijus, pradedama reagavimo į asmens duomenų saugumo pažeidimus procedūra ir įstaigos direktoriaus įsakymu sudaroma Pažeidimo tyrimo komisija (toliau – Komisija).

11. Komisiją sudaro pareigūnas ir kiti darbuotojai, atsakingi už pažeidimą arba turintys informacijos apie įvykusį pažeidimą ir (ar) galintys padėti jį sustabdyti, taip pat kiti pažeidimui svarbūs asmenys. Paprastai Komisija sudaroma iš Įstaigos direktoriaus arba jo įgalioto asmens, pareigūno, IT specialistų.

12. Jeigu Pažeidimas neatitinka Aprašo 5 ir (ar) 9 punkto reikalavimų, Komisija nesudaroma ir vykdoma supaprastinta reagavimo į asmens duomenų saugumo pažeidimus procedūra (toliau – Supaprastinta procedūra). Vykdamas Supaprastintą procedūrą visus pažeidimo išaiškinimo, apribojimo ir kitus būtinus atlikti veiksmus koordinuoja pareigūnas. Atlikus visus būtinus veiksmus Supaprastinta procedūra užbaigiama užpildžius Supaprastintos procedūros atlikimo protokolą.

13. Vykdamt Supaprastintą procedūrą ir nustatčius, kad įvykęs pažeidimas atitinka Aprašo 5 ir 9 punktų kriterijus, pareigūnas teikia siūlymą įstaigos direktoriui pažeidimo tyrimui sudaryti Komisiją.

14. Visa gauta, renkama informacija fiksuojama tokiu būdu, kad atliekant vėlesnę peržiūrą būtų galima nustatyti aiškią chronologinę veiksmų seką ir situacijos eigą bei priemones, kurių buvo imtasi.

III SKYRIUS

DUOMENŲ SAUGUMO PAŽEIDIMO APRIBOJIMAS, LIKVIDAVIMAS IR ATKŪRIMAS

15. Nustatčius, kad įvyko pažeidimas pirmiausia būtina imtis priemonių, kad pažeidimas būtų kuo skubiau apribotas (sustabdytas, nutrauktas, pašalintas). Konkretūs veiksmai pažeidimui apriboti atliekami įvertinus konkretaus pažeidimo aplinkybes, mastą, specifiką ir pan. Siekiant pažeidimą apriboti, gali būti imamasi šių priemonių:

15.1. duomenų ištrynimasis nuotoliniu būdu iš pamesto, pavogto ar kitaip prarasto įrenginio;

15.2. skubus kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti ar kitaip atskleisti duomenys, su prašymu neatidaryti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;

15.3. atskleisto tretiesiems asmenims prisijungimo prie duomenų bazės slaptažodžio pakeitimas;

15.4. prarastų duomenų atkūrimas iš turimos atsarginės kopijos.

16. Šiame etape būtina imtis atsargumo priemonių siekiant užtikrinti, kad būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį pažeidimą (pavyzdžiui, užfiksuojama, kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės, kam konkrečiai buvo per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su duomenimis).

17. Veiksmai, skirti ištaisyti arba sumažinti žalą duomenų subjektui, sukeltą pažeidimo, turėtų būti nukreipti ne vien į esamo pažeidimo priežasties pašalinimą, bet ir siekiant neleisti pažeidimui pasikartoti. Turėtų būti nustatytos bent vykdomų procesų, naudojamų sistemų pažeidimo priežastys, dėl kurių ir toliau gali įvykti pažeidimų arba kurios savaime sudaro prielaidas įvykti pažeidimui.

18. Atkūrimo stadijoje sistemos turėtų būti pagal galimybes atkurtos į ankstesnę būklę, siekiant užtikrinti įstaigos veiklos tęstinumą.

IV SKYRIUS

DUOMENŲ VALDYTOJO PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

19. Kai nustatoma, kad įvyko pažeidimas, atitinkantis Aprašo 5 ir 9 punktų reikalavimus, ir dėl jo gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, įstaiga nepagrįstai nedelsdama, bet ne vėliau kaip per 72 valandas nuo pažeidimo paaikšėjimo momento informuoja duomenų subjektus, kurių teisėms ir laisvėms gali kilti didelis pavojus.

20. Įstaiga, informuodama duomenų subjektus, aiškia, paprasta kalba aprašo pažeidimo pobūdį bei pateikia toliau nurodytą informaciją:

20.1. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis arba pareigūno kontaktus;

20.2. Pažeidimo aprašymą;

20.3. tikėtinų pažeidimo pasekmių duomenų subjektui aprašymą;

20.4. priemones, kurių ėmėsi arba planuoja imtis Įstaiga tam, kad būtų pašalintas pažeidimas.

20.5. kitą reikšmingą informaciją, susijusią su pažeidimu, kuri gali būti reikšminga duomenų subjektui.

V SKYRIUS

DUOMENŲ SAUGUMO PAŽEIDIMO DOKUMENTAVIMAS IR PROCEDŪROS UŽBAIGIMAS

21. Kai pažeidimas laikytinas pašalintu, o visiems reikiams asmenims apie pažeidimą yra pranešta Komisijos įgaliotas asmuo arba pareigūnas sudaro prevencinių veiksmų planą, kuriuo būtų siekiama ateityje užkirsti kelią analogiškam ar panašiam pažeidimui įvykti, ir jis pateikiamas įstaigos direktoriui spręsti dėl jo įgyvendinimo.

22. Sudarius ir įstaigos direktoriui patvirtinus prevencinių veiksmų planą procedūra laikoma baigta.

23. Procedūros dokumentai turi būti saugomi teisės aktų nustatyta tvarka.
