PATVIRTINTA
Valstybės įmonės Registrų centro
generalinio direktoriaus 2019-06-10
įsakymu Nr. VE-116 (1.3 E)

PRANEŠIMO APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Pranešimo apie asmens duomenų saugumo pažeidimą tvarkos aprašas (toliau – Aprašas) nustato informacijos apie asmens duomenų saugumo pažeidimus parengimo ir pateikimo Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams eigą.

2. Aprašas taikomas valstybės įmonei Registrų centrui (toliau – Registrų centras), kaip asmens duomenų valdytojui, ir juridiniams asmenims, pagal Registrų centro suteiktus įgaliojimus tvarkantiems asmens duomenis pagal su Registrų centru sudarytą paslaugų teikimo ar darbų atlikimo sutartį arba asmens duomenų tvarkymo sutartį (toliau – duomenų tvarkytojai). Pranešimo apie asmens duomenų saugumo pažeidimą eigos schema pateikta Aprašo priede „Pranešimo apie asmens duomenų saugumo pažeidimą eigos schema“.

3. Apraše vartojamos šios sąvokos:

3.1. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių, arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

3.2. **Asmens duomenų saugumo pažeidimas** – kibernetinis, elektroninės informacijos saugos ar kitokio pobūdžio incidentas fizinėje arba kibernetinėje erdvėje, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami, persiunčiami, saugomi arba kitaip tvarkomi Registrų centro tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.

3.3. **Duomenų apsaugos pareigūnas** – Registrų centro darbuotojas, atsakingas už duomenų apsaugai taikomų reikalavimų įgyvendinimą ir laikymąsi, atliekantis 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 – Reglamentas (ES) 2016/679) ir kituose teisės aktuose nustatytas funkcijas.

3.4. **Elektroninė informacija** – duomenys, dokumentai ir informacija, tvarkomi Registrų centro tvarkomuose registruose ir informacinėse sistemose.

3.5. **Elektroninės informacijos saugos incidentas** – įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie Registrų centro tvarkomų ryšių ir informacinių sistemų, ypatingos svarbos informacinės infrastruktūros (toliau – RIS) galimybę, sutrikdyti ar pakeisti RIS veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

3.6. **Kibernetinis incidentas** – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį RIS perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys RIS veikimą, valdymą ir paslaugų jomis teikimą.

3.7. **Ryšių ir informacinė sistema** – Registrų centro tvarkomas elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema ir jų valdymo, naudojimo, apsaugos ir priežiūros tikslais laikoma, tvarkoma, atkuriama arba perduodama elektroninė informacija.

3.8. **SD portalas** – Registrų centro specializuota taikomoji programinė įranga, kurioje registruojami kibernetiniai incidentai, elektroninės informacijos saugos incidentai, asmens duomenų saugumo pažeidimai ir pranešimai apie saugumo spragas.

Kitos Apraše vartojamos sąvokos atitinka sąvokas, apibrėžtas ir vartojamas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir Lietuvos Respublikos elektroninių ryšių įstatyme.

4. Registrų centras pranešimus apie asmens duomenų saugumo pažeidimus Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams teikia, jeigu asmens duomenis tvarko kaip asmens duomenų valdytojas. Kitais atvejais Registrų centras informaciją apie asmens duomenų saugumo pažeidimus teikia Registrų centro tvarkomų registrų ir informacinių sistemų, ypatingos svarbos valstybės informacinės infrastruktūros valdytojams ir (arba) asmens duomenų valdytojams (toliau – duomenų valdytojai) šių valdytojų nustatyta tvarka, kurie toliau yra atsakingi už kitų asmenų – Valstybinės duomenų inspekcijos ir duomenų subjektų – informavimą apie asmens duomenų saugumo pažeidimus.

5. Galimi asmens duomenų saugumo pažeidimų tipai:

5.1. asmens duomenų konfidencialumo pažeidimas – kibernetinis, elektroninės informacijos saugos ar kitokio pobūdžio incidentas, dėl kurio atsitiktinai arba neteisėtai atskleidžiami duomenys arba gaunama prieiga prie asmens duomenų;

5.2. asmens duomenų prieinamumo pažeidimas – kibernetinis, elektroninės informacijos saugos ar kitokio pobūdžio incidentas, dėl kurio atsitiktinai arba neteisėtai prarandama galimybė naudotis asmens duomenimis ar sunaikinami asmens duomenys;

5.3. asmens duomenų vientisumo pažeidimas – kibernetinis, elektroninės informacijos saugos ar kitokio pobūdžio incidentas, dėl kurio atsitiktinai arba neteisėtai pakeičiami asmens duomenys;

5.4. mišrus asmens duomenų saugumo pažeidimas – kibernetinis ar elektroninės informacijos saugos ar kitokio pobūdžio incidentas, susijęs su asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimu tuo pačiu metu, taip pat su bet kokiu asmens duomenų saugumo pažeidimų, nurodytų Aprašo 5.1–5.3 papunkčiuose, deriniu.

6. Duomenų apsaugos pareigūnas pranešimą apie asmens duomenų saugumo pažeidimą Aprašo 4 punkte nurodytiems subjektams rengia remdamasis kibernetinių incidentų ir elektroninės informacijos saugos incidentų (toliau kartu – kibernetinis incidentas) valdymo etapų metu gauta informacija ir asmens duomenų saugumo pažeidimo poveikio duomenų subjektų teisėms ir laisvėms vertinimo rezultatais. Kai / jei pranešimo neįmanoma pateikti tuo pačiu metu, informacija toliau nepagrįstai nedelsiant gali būti teikiama etapais.

II SKYRIUS
INFORMAVIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

7. Duomenų tvarkytojai, nustatę ar sužinoję apie galimą asmens duomenų saugumo pažeidimą, nepagrįstai nedelsdami, tačiau ne vėliau kaip per 24 (dvidešimt keturias) valandas nuo tada, kai nustato ar sužino apie galimą asmens duomenų saugumo pažeidimą, apie tai praneša Registrų centro Aptarnavimo departamento Monitoringo skyriui Kibernetinių ir elektroninės informacijos saugos incidentų valdymo tvarkos aprašo 18 punkte nurodytais būdais. El. pašto adresu duomenusauga@registrucentras.lt ar kitais būdais duomenų apsaugos pareigūnui pateikta informacija apie galimus asmens duomenų saugumo pažeidimus turi būti registruojama SD portale. Už gautos informacijos apie galimus asmens duomenų saugumo pažeidimus šiame punkte nustatyta tvarka pateikimą Aptarnavimo departamento Monitoringo skyriui atsakingas duomenų apsaugos pareigūnas.

8. Pranešime apie galimą asmens duomenų saugumo pažeidimą turi būti pateikta 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 – Reglamentas (ES) 2016/679) 33 straipsnio 3 dalyje nurodyta informacija.

9. Duomenų tvarkytojai kartu su pranešimu apie galimą asmens duomenų saugumo pažeidimą Registrų centrui turi pateikti užpildytą Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamą formą, patvirtintą Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“, (toliau – Pranešimo apie asmens duomenų saugumo pažeidimą VDAI forma) ir duomenų tvarkytojo išvadas dėl asmens duomenų saugumo pažeidimo sukelto pavojaus duomenų subjekto teisėms ir laisvėms.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO PATVIRTINIMAS IR POVEIKIO VERTINIMAS

10. Duomenų apsaugos pareigūnas, gavęs iš Aptarnavimo departamento Monitoringo skyriaus pranešimą apie galimą asmens duomenų saugumo pažeidimą, įsitikina, ar informacija atitinka asmens duomenų saugumo pažeidimo požymius. Laikoma, kad Registrų centras apie asmens duomenų saugumo pažeidimą sužino tada, kai duomenų apsaugos pareigūnas SD portale patvirtina asmens duomenų saugumo pažeidimo faktą. Jeigu pranešimas yra susijęs su RIS, duomenų apsaugos pareigūnas apie nustatytą asmens duomenų saugumo pažeidimą nepagrįstai nedelsdamas praneša duomenų valdytojams šių valdytojų nustatyta tvarka.

11. Patvirtinęs asmens duomenų saugumo pažeidimą, duomenų apsaugos pareigūnas atlieka asmens duomenų saugumo pažeidimo poveikio asmenų teisėms ir laisvėms vertinimą (toliau – poveikio vertinimas). Prireikus, į poveikio vertinimą gali būti įtraukti ir kiti Registrų centro, asmens duomenų tvarkytojų darbuotojai.

12. Poveikio vertinimas atliekamas atsižvelgiant į faktines pasekmes arba galimų pasekmių tikimybę ir žalą, kuri kilo ar galėtų kilti, jei šios pasekmės atsirastų. Įvairios tikimybės ir rimtumo pavojus duomenų subjektų teisėms ir laisvėms gali kilti dėl asmens duomenų saugumo pažeidimo, jei dėl jo laiku nesiimama tinkamų priemonių. Fiziniai asmenys dėl asmens duomenų saugumo pažeidimo gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą, pavyzdžiui, 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.

13. Pavojaus duomenų subjekto teisėms ir laisvėms tikimybė ir rimtumas vertinami remiantis objektyviu įvertinimu, kurio metu nustatoma, ar asmens duomenų saugumo pažeidimas kelia pavojų arba didelį pavojų duomenų subjekto teisėms ir laisvėms. Siekiant įvertinti pavojaus laipsnį, vertinimo metu atsižvelgiama į šiuos kriterijus, susijusius su asmens duomenų saugumo pažeidimo tipais ir sunkumu, jo pasekmėmis ir neigiamais padariniais duomenų subjektui:

13.1. *Asmens duomenų saugumo pažeidimo tipas.* Asmens duomenų saugumo pažeidimo tipai nurodyti Aprašo 5 punkte. Asmens duomenų konfidencialumo pažeidimas tam tikrais atvejais gali sukelti didesnį pavojų duomenų subjekto teisėms ir laisvėms nei asmens duomenų prieinamumo pažeidimas.

13.2. *Asmens duomenų pobūdis ir apimtis* (pvz., specialių kategorijų asmens duomenys).

13.3. *Asmenų atpažįstamumas*. Fizinio asmens tapatybę galima tiesiogiai arba netiesiogiai nustatyti iš atsitiktinai arba neteisėtai atskleistų duomenų. Didesnis pavojus duomenų subjekto teisėms ir laisvėms gali kilti, jeigu fizinio asmens ir (arba) jo asmens duomenų identifikavimas nereikalauja didesnių pastangų ir laiko (pvz., specialių tyrimų, reikalingų nustatyti fizinio asmens tapatybę, poreikio gauti šifravimo raktą ir iššifruoti duomenis ir pan.).

13.4. *Pasekmių rimtumas asmenims*. Specialių kategorijų asmens duomenų (pvz., asmens duomenų, atskleidžiančių rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat genetinių duomenų, biometrinių duomenų, sveikatos duomenų arba duomenų apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją) saugumo pažeidimo padariniai gali būti ypač sunkūs, todėl toks asmens duomenų saugumo pažeidimas gali sukelti didesnį pavojų duomenų subjekto teisėms ir laisvėms nei kitų kategorijų asmens duomenų saugumo pažeidimas.

13.5. *Asmens ypatybės.* Asmens duomenų saugumo pažeidimas gali sukelti didesnį pavojų duomenų subjektų teisėms ir laisvėms, jeigu pažeidimas susijęs su vaikų ir kitų pažeidžiamų fizinių asmenų asmens duomenimis.

13.6. *Paveiktų asmenų skaičius.* Asmens duomenų saugumo pažeidimas gali turėti įtakos tik vienam asmeniui ar grupei asmenų. Įprastai, asmens duomenų saugumo pažeidimo poveikis yra didesnis tuo atveju, jeigu pažeidimas daro įtaką daugiau duomenų subjektų. Tačiau asmens duomenų saugumo pažeidimas gali turėti rimtą poveikį net ir vienam asmeniui atsižvelgiant į tvarkomų asmens duomenų pobūdį ir kontekstą.

13.7. *Duomenų valdytojo ypatybės*. Duomenų tvarkymas gali sukelti didesnį pavojų duomenų subjektų teisėms ir laisvėms, kai duomenų valdytojas tvarko specialių kategorijų asmens duomenis.

14. Poveikio vertinimo išvados gali būti šios:

14.1. Asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus duomenų subjektų teisėms ir laisvėms. Valstybinė duomenų apsaugos inspekcija ir duomenų subjektai apie asmens duomenų saugumo pažeidimą neinformuojami.

14.2. Dėl asmens duomenų saugumo pažeidimo gali kilti pavojus duomenų subjektų teisėms ir laisvėms. Apie asmens duomenų saugumo pažeidimą informuojama Valstybinė duomenų apsaugos inspekcija Aprašo IV skyriuje nustatyta tvarka.

14.3. Dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų subjektų asmenų teisėms ir laisvėms. Apie asmens duomenų saugumo pažeidimą informuojama Valstybinė duomenų apsaugos inspekcija ir duomenų subjektai.

IV SKYRIUS
PRANEŠIMAS VALSTYBINEI DUOMENŲ APSAUGOS INSPEKCIJAI

15. Asmens duomenų saugumo pažeidimo, kuris gali sukelti pavojų duomenų subjektų teisėms ir laisvėms, atveju, kai Registrų centras asmens duomenis tvarko kaip asmens duomenų valdytojas, duomenų apsaugos pareigūnas nepagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai patvirtinamas asmens duomenų saugumo pažeidimo faktas, apie tai praneša Valstybinei duomenų apsaugos inspekcijai. Jeigu Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų saugumo pažeidimą nepranešama per 72 valandas, prie pranešimo pridedamos vėlavimo priežastys.

16. Pranešime apie asmens duomenų saugumo pažeidimą turi būti nurodyta:

16.1. aprašytas asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;

16.2. nurodyta duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;

16.3. aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

16.4. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti;

16.5. kita informacija, nurodyta Pranešimo apie asmens duomenų saugumo pažeidimą VDAI formoje.

V SKYRIUS
PRANEŠIMAS DUOMENŲ SUBJEKTUI

17. Duomenų apsaugos pareigūnas pranešimą apie asmens duomenų saugumo pažeidimą, kuris gali sukelti didelį pavojų duomenų subjekto teisėms ir laisvėms, duomenų subjektui pateikia nepagrįstai nedelsdamas.

18. Pranešime apie asmens duomenų saugumo pažeidimą duomenų subjektui aiškia ir paprasta kalba aprašomas asmens duomenų saugumo pažeidimo pobūdis ir pateikiama ši informacija ir priemonės:

18.1. nurodyta duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;

18.2. aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

18.3. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

19. Pranešimas apie asmens duomenų saugumo pažeidimą duomenų subjektui neteikiamas, jeigu yra bent viena iš šių sąlygų:

19.1. įgyvendintos tinkamos techninės ir organizacinės apsaugos priemonės ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio, visų pirma tos priemonės, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės;

19.2. buvo imtasi priemonių, kuriomis užtikrinama, kad nebegalėtų grėsti didelis pavojus duomenų subjektų teisėms ir laisvėms;

19.3. pranešimo apie asmens duomenų saugumo pažeidimą pateikimas pareikalautų neproporcingai daug pastangų. Tokiu atveju apie asmens duomenų saugumo pažeidimą viešai paskelbiama arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

20. Jeigu duomenų subjektui apie asmens duomenų saugumo pažeidimą dar nėra pranešta, Valstybinė duomenų apsaugos inspekcija, apsvarsčiusi, kokia yra tikimybė, kad dėl asmens duomenų saugumo pažeidimo kils didelis pavojus, gali pareikalauti, kad Registrų centras apie tai informuotų duomenų subjektą, arba gali nuspręsti, kad įvykdyta bet kuri iš Aprašo 19 punkte nurodytų sąlygų.

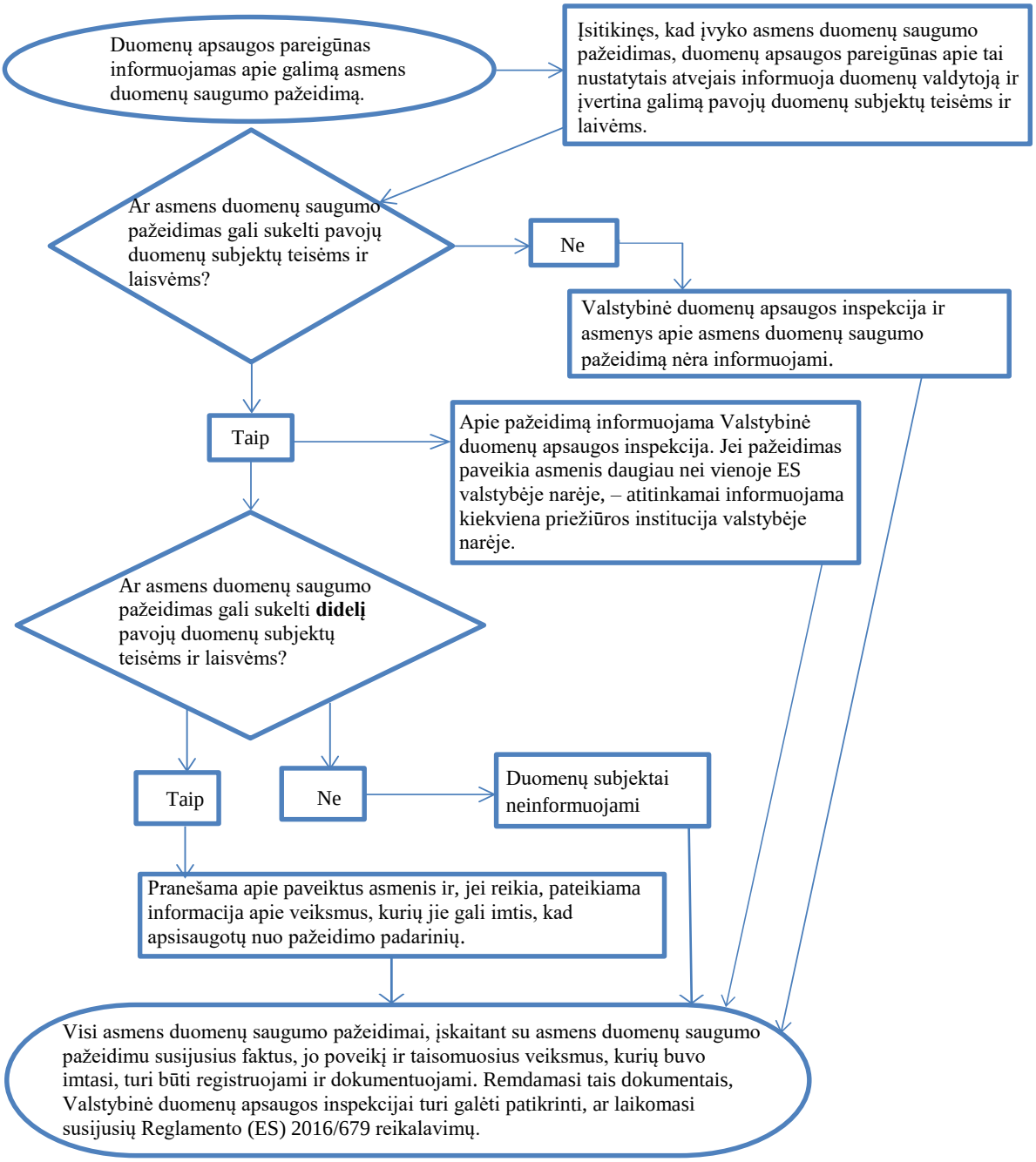
VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

21. Visi asmens duomenų saugumo pažeidimai, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jų poveikį ir taisomuosius veiksmus, kurių buvo imtasi, turi būti dokumentuojami ir registruojame SD portale.

_____

Pranešimo apie asmens duomenų saugumo pažeidimą tvarkos aprašo priedas

PRANEŠIMO APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ EIGOS SCHEMA



_____