SAVIVALDYBĖS ĮMONĖ „VILNIAUS MIESTO BŪSTAS“ DIREKTORIUS

ĮSAKYMAS DĖL SĮ „VILNIAUS MIESTO BŪSTAS“ ASMENS DUOMENŲ TVARKYMO TAISYKLIŲ PATVIRTINIMO

2020 m. liepos 2 d. Nr. 1.23-20/65
Vilnius

Vadovaudamasis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 30 straipsnio 1 dalimi:

1. T v i r t i n u SĮ „Vilniaus miesto būstas“ asmens duomenų tvarkymo taisykles (pridedama).

2. L a i k a u netekusiu galios 2018 m. kovo 23 d. įsakymą Nr. 1.23-18/23 „Dėl asmens duomenų tvarkymo Savivaldybės įmonėje „Vilniaus miesto būstas“ taisyklių patvirtinimo“.

3. Į p a r e i g o j u referentę Viktoriją Karpavičienę su šiuo įsakymu bei taisyklėmis pasirašytinai supažindinti visus Savivaldybės įmonės „Vilniaus miesto būstas“ darbuotojus.

Direktorius Tadas Balsevičius

PATVIRTINTA
SĮ „Vilniaus miesto būstas“
Direktoriaus
2020-07-02
įsakymu Nr. 1.23-20/65

SĮ „VILNIAUS MIESTO BŪSTAS“ ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Šių asmens duomenų tvarkymo taisyklių (toliau – **Taisyklės**) tikslas – reglamentuoti asmens duomenų tvarkymą SĮ „Vilniaus miesto būstas“ (toliau – **Įmonė**) užtikrinant 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**), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ir kitų teisės aktų, nustatančių asmens duomenų tvarkymą ir apsaugą, laikymąsi ir įgyvendinimą.

2. Vartojamos sąvokos:
2.1. **Duomenų valdytojas** – SĮ „Vilniaus miesto būstas“, įmonės kodas 124568293, registruotos buveinės adresas Švitrigailos g. 7, LT-03110, Vilnius.
2.2. **Duomenų subjektas** – fizinis asmuo (darbuotojas/klientas), kurio asmens duomenis tvarko Duomenų valdytojas.
2.3. **Duomenų teikimas** – asmens duomenų atskleidimas perduodant ar kitu būdu padarant juos prieinamus (išskyrus paskelbimą visuomenės informavimo priemonėse).
2.4. **Vidaus administravimas** – veikla, kuria užtikrinamas duomenų valdytojo savarankiškas funkcionavimas (struktūros tvarkymas, personalo valdymas, finansinių išteklių valdymas ir naudojimas, raštvedybos tvarkymas).
2.5. **Darbuotojai** – darbuotojai, dirbantys pagal darbo sutartis.
2.6. Kitos šiose Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente bei Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme.

3. Už tinkamą šių Taisyklių ir asmens duomenų apsaugos priemonių įgyvendinimą atsakingas Įmonės vadovas, kuris turi teisę įsakymu paskirti asmenį, atsakingą už asmens duomenų apsaugą.

4. Asmenys, neteisėtai tvarkę asmens duomenis, sukliudę asmeniui susipažinti su savo duomenimis ar informacija apie tokius duomenis, atsako teisės aktų nustatyta tvarka.

II SKYRIUS BENDRIEJI ASMENS DUOMENŲ TVARKYMO PRINCIPAI

5. Įmonėje asmens duomenys tvarkomi laikantis reikalavimų, numatytų Reglamente ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir šiose Taisyklėse numatytos tvarkos, tiek, kiek ji neprieštarauja paminėtiems ir kitiems teisės aktams.

6. Įmonės tvarkomų asmens duomenų tvarkymo tikslai, teisėto tvarkymo pagrindai, duomenų subjektų kategorijos, asmens duomenų kategorijos, asmens duomenų šaltiniai ir gavėjai,

asmens duomenų tvarkymo ir saugojimo trukmė bei kita su asmens duomenų tvarkymu susijusi detalesnė informacija nurodoma Įmonės asmens duomenų tvarkymo veiklos įrašų registre (toliau – Registras).

7. Įmonės įgalioti darbuotojai, kurie tvarko asmens duomenis, privalo saugoti asmens duomenų paslaptį, jei šie asmens duomenys neskirti skelbti viešai. Ši pareiga galioja taip pat ir pasibaigus darbo santykiams.

8. Įmonė užtikrina, kad asmens duomenys būtų tvarkomi laikantis šių principų:
8.1. asmens duomenys yra renkami apibrėžtais ir teisėtais tikslais, kurie nustatomi prieš pradedant rinkti asmens duomenis, o vėliau tvarkomi su šiais tikslais suderintais būdais;
8.2. asmens duomenys tvarkomi tiksliai, sąžiningai ir nepažeidžiant teisės aktuose įtvirtintų reikalavimų;
8.3. asmens duomenys yra tikslūs ir, jei reikia dėl asmens duomenų tvarkymo, yra nuolat atnaujinami. Netikslūs ar neišsamūs duomenys yra ištaisomi, papildomi, sunaikinami arba sustabdomas jų tvarkymas;
8.4. asmens duomenys yra tapatūs, tinkami ir tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti;
8.5. asmens duomenys yra saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir toliau tvarkomi;
8.6. asmens duomenys tvarkomi atsižvelgiant į Reglamente, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir kituose atitinkamą veiklą reglamentuojančiuose teisės aktuose nustatytus asmens duomenų tvarkymo reikalavimus.

9. Asmens duomenys yra saugomi ne ilgiau, nei to reikalauja duomenų tvarkymo tikslai, duomenų subjektai ir (ar) teisės aktai.

III SKYRIUS
ASMENS DUOMENŲ TVARKYMO VEIKLOS ĮRAŠŲ PILDYMAS IR ATNAUJINIMAS

10. Registras yra skirtas nustatyti visus Įmonėje tvarkomus asmens duomenis, suskirstant juos į asmens duomenų kategorijas bei įvardinant kiekvienai kategorijai taikomą teisinį pagrindą, kuriuo remiantis nustatomas asmens duomenų tvarkymo teisėtumas, techninės ir organizacinės priemonės, asmens duomenų saugojimo terminai, asmens duomenų saugojimo vietos bei kita informacija, kuri leidžia visapusiškai užtikrinti tiek atskiru tikslu tvarkomų asmens duomenų, tiek visos Įmonės tvarkomų asmens duomenų teisėtą tvarkymą bei tvarkomų asmens duomenų saugumą.

11. Visi asmens duomenų tvarkymo tikslai, asmens duomenų tvarkymo kategorijos, asmens duomenų saugojimo terminai, asmens duomenų saugojimo vieta ir kita su asmens duomenų tvarkymu susijusi informacija nurodoma Registro formoje, pateiktoje Taisyklių 2 priede ir pateikiama Registre.

12. Registro pildymui Įmonėje paskiriamas atsakingas darbuotojas, kuris atsako už Registre esančios informacijos teisingumą, aktualumą, jos savalaikį atnaujinimą bei reikalingų saugos priemonių diegimo koordinavimą. Registrą pildo paskirtas atsakingas Įmonės darbuotojas, atliekamus veiksmus derindamas su duomenų apsaugos pareigūnu.

13. Registre pateikta informacija turi būti atnaujinama ne vėliau kaip per 10 (dešimt) darbo dienų, kai pasikeičia Registre nurodytų tvarkomų asmens duomenų kategorijos, jų tvarkymo tikslai,

duomenų gavėjai, duomenų tvarkytojai, asmens duomenų saugojimo terminai. Kitos Registre nurodytos informacijos atnaujinimas vykdomas, atliekant metinę Registro peržiūrą.

14. Duomenų apsaugos pareigūnas koordinuoja Registro atnaujinimą, įskaitant ir metinę jo peržiūrą, atliekant:
14.1. reikalingus pakeitimus, atsiradusius dėl bet kokio pakeitimų valdymo proceso metu (pvz., projektas, pakeitimas);
14.2. reikalingus pakeitimus, atsiradusius Registro peržiūros metu.

15. Duomenų apsaugos pareigūnas ne rečiau kaip vieną kartą per metus arba įvykus saugumo pažeidimui, teisinio reglamentavimo pakeitimams ir (ar) kitoms esminę reikšmę duomenų atnaujinimui turinčioms aplinkybėms, inicijuoja Registro peržiūrą ir atnaujinimą:
15.1. išsiunčia atsakingiems darbuotojams pranešimus dėl peržiūros vykdymo;
15.2. iš Įmonės darbuotojų surenka ir apibendrina gautą informaciją, susijusią su asmens duomenų tvarkymu;
15.3. koordinuoja reikalingus Registro pakeitimus.

IV SKYRIUS
DARBUOTOJŲ ASMENS DUOMENŲ TVARKYMAS

16. Įmonė, tvarkydama darbuotojų asmens duomenis, atlieka darbuotojų asmens duomenų tvarkymą tik ta apimtimi, kuri yra reikalinga šiose Taisyklėse ir Registre apibrėžtiems tikslams pasiekti.

17. Darbuotojų asmens duomenis turi teisę tvarkyti tik tie asmenys, kuriems jie yra būtini funkcijų vykdymui, ir tik tuomet, kai yra būtina atitinkamiems tikslams pasiekti. Įmonės vadovas įsakymu gali paskirti atsakingą asmenį, kuris atsakingas už darbuotojų asmens duomenų tvarkymą.

18. Potencialūs Įmonės darbuotojai (kandidatai, asmenys ieškantys darbo) Įmonei pateikia šiuos duomenis: CV, motyvacinis laiškas, vardas, pavardė, kontaktai. Potencialūs darbuotojai apie jų asmens duomenų tvarkymą, duomenų saugojimo terminus informuojami pirmo kontakto metu žodžiu ar elektroniniu paštu (jei potencialus darbuotojas į Įmonę kreipiasi elektroniniu paštu). Kai potencialūs darbuotojai kandidatuoja į konkrečią poziciją, jų asmens duomenys tvarkomi sutarties sudarymo su duomenų subjektu pagrindu kol vyksta atranka. Pasibaigus atrankai, jei duomenų subjektas neatrenkamas ir nepateikia sutikimo dėl tolesnio duomenų saugojimo, tokie duomenys ištrinami. Jei potencialūs darbuotojai savo duomenis pateikia ne konkrečiai skelbiamai pozicijai ar pasibaigus atrankai sutinka, kad jų duomenys būtų toliau tvarkomi Įmonėje, tokių duomenų subjektų asmens duomenys tvarkomi duomenų subjekto sutikimo pagrindu.

19. Potencialių Įmonės darbuotojų asmens duomenys, pasibaigus Įmonėje vykdytai atrankai į konkrečią poziciją, sunaikinami, jei darbo sutartis nesudaroma.

20. Įmonė gali teikti darbuotojų asmens duomenis (pvz., vardas, pavardė, telefono numeris, el. pašto adresas) savo pasitelktiems paslaugų teikėjams, partneriams ar kitiems asmenims, kiek tai susiję su Įmonės įsipareigojimų ar įprastinės veiklos vykdymu, taip pat auditą atliekančioms bendrovėms bei teisės konsultantams pagrįsta apimtimi, kiek to pagrįstai reikia šiame punkte nustatytiems tikslams pasiekti.

21. Įmonės darbuotojų asmens duomenys gali būti teikiami tretiesiems asmenims Įmonei įsigyjant paslaugas iš tokių asmenų ir kai paslaugų teikimui būtina atskleisti darbuotojų asmens

duomenis (pvz., kelionių agentūroms, organizuojant darbuotojų keliones ir kelionės dokumentus; ryšio paslaugų teikėjams užsakant SIM korteles darbuotojams; darbuotojų medicinines patikras vykdančioms įmonėms (klinikoms), kitiems paslaugų teikėjams ir partneriams, kurie teikia paslaugas Įmonei).

22. Įmonė duomenis tretiesiems asmenims taip pat teikia įstatymuose nustatytais atvejais ir tvarka (pvz., duomenų perdavimas Valstybinei mokesčių inspekcijai, Valstybinio socialinio draudimo fondo valdybai prie Socialinės apsaugos ir darbo ministerijos (SODRA), kitoms kompetetingoms įstaigoms, institucijoms, organizacijoms). Asmens duomenys be atskiro duomenų subjekto sutikimo taip pat gali būti pateikti ikiteisminio tyrimo įstaigoms, kaip įrodymai, taip pat kitais įstatymų nustatytais atvejais.

V SKYRIUS
TELEFONINIŲ POKALBIŲ ĮRAŠŲ DUOMENŲ TVARKYMAS

23. Paslaugų kokybės kontrolės tikslu, t. y. siekiant užtikrinti aptarnavimo kokybę ir kontroliuoti paslaugų teikimą, Įmonėje vykdomas telefoninių pokalbių įrašymas. Duomenų subjektų asmens duomenys tvarkomi teisėto Įmonės intereso pagrindu.

24. Pokalbių įrašų duomenys negali būti tvarkomi nesuderinamais su Taisyklėse ir (ar) Registre nustatytais duomenų tvarkymo tikslais.

25. Įrašomi tik Įmonei priskirtų telefonų įeinantys ir išeinantys pokalbiai, vykstantys Įmonės darbo laiku. Telefono ryšio numeriai ir Įmonės darbo laikas viešai skelbiami Įmonės interneto svetainėje.

26. Pokalbių įrašai, be tikslų, nustatytų šiose Taisyklėse, gali būti naudojami ir įtariamoms nusikalstamoms veikoms, administraciniams teisės pažeidimams atskleisti, Įmonei ar tretiesiems asmenims padarytai žalai įrodyti, atskleisti ir gali būti perduoti tik įstatymų nustatyta tvarka turintiems teisę gauti šiuos duomenis asmenims.

27. Pokalbio įrašus gali būti leidžiama perklausyti ir, esant būtinybei, perduoti teisėsaugos institucijoms gavus rašytinį teisėsaugos institucijų prašymą. Jei pokalbio įrašai perklausomi ne teisėsaugos institucijų, teismo patalpose, pokalbio įrašų perklausa turi vykti uždaroje Įmonės patalpoje. Tokioje perklausoje turi teisę dalyvauti duomenų subjektas; atsakingas Įmonės darbuotojas; teisėsaugos institucijų atstovai.

28. Įmonė turi teisę pasitelkti pokalbių įrašų (asmens duomenų) tvarkytojus, atitinkančius Taisyklėse numatytus reikalavimus. Teisė susipažinti su telefono pokalbio įrašu įgyvendinama duomenų subjektui atvykus išklausyti garso įrašo Įmonės buveinės adresu arba atsiimant garso įrašo kopiją išorinėje Įmonės pateiktoje laikmenoje.

29. Duomenų subjektas, kurio pokalbis įrašomas, turi Taisyklių VII skyriuje numatytas duomenų subjekto teises.

30. Duomenų subjektas, Įmonės darbuotojas, apie Įmonės vykdomą pokalbių įrašymą informuojamas jį supažindinant su šiomis Taisyklėmis.

31. Duomenų subjektui, paskambinus į Įmonę ar konsultuojančiam Įmonės darbuotojui telefonu susisiekus su duomenų subjektu apie vykdomą telefoninių pokalbių įrašymą duomenų subjektas informuojamas pateikiant informaciją apie:

31.1. pokalbio įrašymo faktą;

31.2. pokalbio įrašymo tikslą, Įmonės (duomenų valdytojo) pavadinimą.

32. Duomenų subjektai, Įmonės klientai, taip pat informuojami apie Įmonėje vykdomą pokalbių įrašymą ir su tuo susijusį asmens duomenų tvarkymą, tvarkymo tikslus ir apimtį Įmonės interneto svetainėje viešai skelbiamoje privatumo politikoje.

VI SKYRIUS
DUOMENŲ VALDYTOJO PAREIGOS

33. Įmonė privalo sudaryti sąlygas duomenų subjektui įgyvendinti šių Taisyklių VII skyriaus 43 punkte numatytas teises.

34. Asmens duomenys Įmonės gaunami tik teisės aktų nustatyta tvarka, juos gaunant tiek tiesiogiai iš duomenų subjektų, tiek iš trečiųjų šalių duomenų valdytojų.

35. Informacija apie duomenų subjekto duomenų tvarkymą turi būti jam suteikta duomenis renkant arba, kai asmens duomenys gaunami ne iš duomenų subjekto, o iš kito šaltinio, per pagrįsta laikotarpį, priklausomai nuo konkretaus atvejo aplinkybių. Kai asmens duomenis galima teisėtai atskleisti kitam duomenų gavėjui, duomenų subjektas apie tai turėtų būti informuojamas pirmo asmens duomenų atskleidimo jų gavėjui metu. Jeigu Įmonė ketina tvarkyti duomenis kitu tikslu nei tikslas, kuriuo jie buvo renkami, prieš taip toliau tvarkydama duomenis, Įmonė turi pateikti duomenų subjektui informaciją apie tą kitą tikslą ir kitą būtiną informaciją. Tais atvejais, kai asmens duomenų kilmė duomenų subjektui negali būti nurodyta dėl to, kad buvo naudoti įvairūs šaltiniai, turėtų būti pateikta bendro pobūdžio informacija.

36. Tais atvejais, kai asmens duomenys gaunami ne iš duomenų subjekto, informacija apie duomenų subjekto asmens duomenų tvarkymą gali būti neteikiama jeigu ir tokia apimtimi, kiek:
36.1. duomenų subjektas jau turi informacijos;
36.2. informacijos pateikimas yra neįmanomas arba pareikalautų neproporcingų pastangų. Tokiais atvejais turi būti konsultuojamasi su duomenų apsaugos pareigūnu dėl duomenų subjekto teisių ir laisvių apsaugos būdų, įskaitant viešą informacijos paskelbimą.

37. Įmonė užtikrina, kad visa reikalinga informacija duomenų subjektui būtų pateikiama aiškiai ir suprantamai, laikantis teisės aktų reikalavimų. Pagal sąžiningo ir skaidraus duomenų tvarkymo principus duomenų subjektui pranešama apie vykdomą duomenų tvarkymo operaciją ir jos tikslus. Įmonė turi pateikti duomenų subjektui visą papildomą informaciją, kuri būtina tam, kad būtų užtikrintas sąžiningas ir skaidrus duomenų tvarkymas, atsižvelgiant į konkrečias asmens duomenų tvarkymo aplinkybes ir kontekstą. Be to, duomenų subjektas turėtų būti informuotas apie tai, ar vykdomas profiliavimas, ir apie tokio profiliavimo pasekmes. Kai asmens duomenys renkami iš duomenų subjekto, duomenų subjektas taip pat turėtų būti informuojamas, ar jis privalo pateikti asmens duomenis, taip pat apie tokių duomenų nepateikimo pasekmes.

38. Įmonė turi užtikrinti duomenų subjektui teisę susipažinti su apie jį Įmonėje surinktais asmens duomenimis ir galimybę ta teise lengvai ir pagrįstais laiko tarpais pasinaudoti, kad žinotų apie duomenų tvarkymą ir galėtų patikrinti jo teisėtumą. Duomenų subjektas turi teisę žinoti ir būti informuotas visų pirma apie tai, kokiais tikslais asmens duomenys tvarkomi, jei įmanoma – kokiu laikotarpiu jie tvarkomi, kas yra duomenų gavėjai, pagal kokią logiką asmens duomenys yra tvarkomi automatiškai ir kokios galėtų būti tokio asmens duomenų tvarkymo pasekmės bent jau tais atvejais, kai duomenų tvarkymas grindžiamas profiliavimu.

39. Duomenų subjektas turi teisę reikalauti ištaisyti jo asmens duomenis ir teisę būti pamirštam, kai tokių duomenų saugojimas pažeidžia teisės aktus, taikomus Įmonei. Duomenų subjektas turi teisę reikalauti, kad jo asmens duomenys būtų ištrinti ir toliau nebetvarkomi, (i) kai asmens duomenų Įmonei nebereikia tiems tikslams, kuriais jie buvo renkami ar kitaip tvarkomi, kai duomenų subjektas atšaukė savo sutikimą ir nesutinka, kad jo asmens duomenys būtų tvarkomi, (ii) arba kai jo asmens duomenų tvarkymas dėl kitų priežasčių neatitinka teisės aktų reikalavimų. Tačiau Įmonė turi teisę toliau saugoti asmens duomenis, jei tai būtina siekiant įvykdyti teisinę prievolę, atlikti užduotį, vykdomą dėl viešojo intereso arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas, dėl viešojo intereso priežasčių visuomenės sveikatos srityje, archyvavimo tikslais arba siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus, susijusius su Įmone. Sutikimo atšaukimas, kai duomenų subjekto asmens duomenys buvo tvarkomi sutikimo pagrindu, galioja tik į ateitį ir tai neturi įtakos asmens duomenų tvarkymui iki sutikimo atšaukimo.

40. Jei Įmonė asmens duomenis gauna ne iš duomenų subjekto, ji privalo apie tai informuoti duomenų subjektą prieš pradedant tvarkyti asmens duomenis. Jei Įmonė ketina teikti duomenis tretiesiems asmenims, ji privalo apie tai informuoti duomenų subjektą ne vėliau kaip iki to momento, kai duomenys teikiami pirmą kartą, išskyrus atvejus, kai įstatymai ar kiti teisės aktai apibrėžia tokių duomenų rinkimo ir teikimo tvarką bei duomenų gavėjus. Įmonė neprivalo informuoti duomenų subjektų apie tai, kuriems Įmonės išoriniams paslaugų teikėjams (duomenų tvarkytojams) Įmonė leidžia tvarkyti asmens duomenis, tačiau jei Įmonė gauna duomenų subjekto paklausimą, Įmonė privalo informuoti duomenų subjektą apie savo duomenų tvarkytojus.

41. Kai Įmonė renka ar ketina rinkti asmens duomenis iš duomenų subjekto ir juos tvarko ar ketina tvarkyti tiesioginės rinkodaros tikslais, prieš teikdama duomenų subjekto asmens duomenis, ji privalo informuoti duomenų subjektą, kam ir kokiais tikslais jo asmens duomenys bus teikiami.

42. Teisės aktų nustatytais atvejais ir tvarka Įmonė gali teikti jos tvarkomus asmens duomenis tretiesiems asmenims, kuriems asmens duomenis teikti Įmonę įpareigoja įstatymai ar kiti teisės aktai, pagal Įmonės ir duomenų gavėjo sudarytą asmens duomenų teikimo sutartį.

VII SKYRIUS
DUOMENŲ SUBJEKTO TEISĖS

43. Duomenų subjektas turi teisę:
43.1. žinoti (būti informuotas) apie savo asmens duomenų tvarkymą;
43.2. susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi;
43.3. reikalauti ištaisyti, sunaikinti savo asmens duomenis arba sustabdyti asmens duomenų tvarkymo veiksmus, išskyrus saugojimą, kai duomenys tvarkomi nesilaikant teisės aktuose įtvirtintų reikalavimų ir šių Taisyklių;
43.4. nesutikti, kad būtų tvarkomi jo asmens duomenys.

44. Naudoti elektroninių ryšių paslaugas, įskaitant elektroninio pašto pranešimų siuntimą, tiesioginės rinkodaros tikslu paprastai galima tik gavus išankstinį duomenų subjekto sutikimą. Įmonė turi siekti turėti tokius duomenų subjektų sutikimus dėl tiesioginės rinkodaros.

45. Duomenų subjektas, Įmonei pateikęs asmens tapatybę patvirtinantį dokumentą arba teisės aktų nustatyta tvarka ar elektroninių ryšių priemonėmis, kurios leidžia tinkamai identifikuoti asmenį, patvirtinęs savo asmens tapatybę, turi teisę susipažinti su Įmonės tvarkomais jo

duomenimis ir gauti informaciją, iš kokių šaltinių ir kokie jo asmens duomenys surinkti, kokiu tikslu jie tvarkomi, kokiems duomenų gavėjams teikiami ir buvo teikti per paskutinius vienerius metus.

46. Įgyvendindamas šių Taisyklių VII skyriuje 43 punkte numatytas teises, duomenų subjektas gali kreiptis į Įmonę, o pastaroji kaip duomenų valdytojas, gavusi duomenų subjektų prašymą, nedelsdama, tačiau bet kuriuo atveju ne vėliau kaip per vieną mėnesį nuo prašymo gavimo, pateikia duomenų subjektui informaciją apie veiksmus, kurių imtasi gavus prašymą pagal Reglamento 15-22 straipsnius. Tas laikotarpis prireikus gali būti pratęstas dar dviem mėnesiams, atsižvelgiant į prašymų sudėtingumą ir skaičių. Įmonė per vieną mėnesį nuo prašymo gavimo dienos informuoja duomenų subjektą apie tokį pratęsimą, kartu pateikdama vėlavimo priežastis. Kai duomenų subjektas prašymą pateikia elektroninės formos priemonėmis, informacija jam taip pat pateikiama, jei įmanoma, elektroninėmis priemonėmis, išskyrus atvejus, kai duomenų subjektas paprašo ją pateikti kitaip. Duomenų subjektui teikiama informacija ir visi parnešimai bei visi veiksmai pagal Reglamento 15-22 ir 34 straipsnius yra nemokami. Kai duomenų subjekto prašymai yra akivaizdžiai nepagrįsti arba neproporcingi, visų pirma dėl jų pasikartojančio turinio, Įmonė gali arba: (i) imti pagrįstą mokestį, atsižvelgdama į informacijos teikimo arba pranešimų ar veiksmų, kurių prašoma, administracines išlaidas; arba (ii) gali atsisakyti imtis veiksmų pagal prašymą. Informacija teikiama lietuvių kalba.

47. Jei duomenų subjektas nesutinka, kad Įmonė tvarkytų jo asmens duomenis tiesioginės rinkodaros tikslais, duomenų subjektas turi teisę nesutikti nenurodydamas jokių motyvų, kad Įmonė tvarkytų jo asmens duomenis tiesioginės rinkodaros tikslais.

48. Jeigu duomenų subjektas, susipažinęs su savo duomenimis, nustato, kad jo duomenys yra neteisingi, neišsamūs ar netikslūs, jis gali kreiptis į Įmonę, o ši nedelsdama duomenis patikrina ir duomenų subjekto prašymu ištaiso neteisingus, neišsamius, netikslius duomenis ir (arba) sustabdo tokių duomenų tvarkymo veiksmus, išskyrus jų saugojimą.

49. Jeigu duomenų subjektas, susipažinęs su savo asmens duomenimis, nustato, kad jie yra tvarkomi neteisėtai, nesąžiningai, ir kreipiasi į Įmonę, ši nedelsdama neatlygintinai patikrina duomenų tvarkymo teisėtumą, sąžiningumą ir duomenų subjekto prašymu sunaikina neteisėtai ir nesąžiningai sukauptus duomenis ar sustabdo tokių duomenų tvarkymo veiksmus, išskyrus saugojimą.

50. Įmonė nedelsdama praneša duomenų subjektui apie jo prašymu atliktą ar neatliktą duomenų ištaisymą, sunaikinimą ar duomenų tvarkymo veiksmų sustabdymą.

51. Duomenų subjektas, norėdamas įgyvendinti šiame Taisyklių skyriuje numatytas teises, pateikia rašytinį prašymą, kuriame turi nurodyti savo pageidavimą, vardą, pavardę, gyvenamąją vietą ir duomenis ryšiui palaikyti, jeigu dėl duomenų subjekto teisių įgyvendinimo kreipiasi duomenų subjekto atstovas, jis savo prašyme turi nurodyti savo vardą, pavardę, gyvenamąją vietą, taip pat atstovaujamo asmens vardą, pavardę, gyvenamąją vietą ir pridėti atstovavimą patvirtinantį dokumentą. Visi raštu, įskaitant elektronine forma, Įmonei pateikti prašymai turi būti pasirašyti duomenų subjekto arba jo atstovo. Duomenų subjekto rašytinis prašymas gali būti pateikiamas asmeniškai, paštu ar elektroninių ryšių priemonėmis.

52. Informacija duomenų subjektui, atsižvelgiant į jo prašymą, gali būt pateikiama žodžiu, leidžiant susipažinti su dokumentu, pateikiant pažymą, dokumento išrašą ar popierinę dokumento kopiją, elektroninę laikmeną. Jei prašyme nenurodyta informacijos pateikimo forma, Įmonė ją pateikia tokia pat forma, kokia gautas prašymas.

53. Sustabdžius duomenų tvarkymo veiksmus, atitinkami duomenys saugomi tol, kol bus ištaisyti ar sunaikinti (duomenų subjekto prašymu arba pasibaigus duomenų saugojimo terminui). Kiti tvarkymo veiksmai su tokiais duomenimis gali būti atliekami tik:
53.1. turint tikslą įrodyti aplinkybes, dėl kurių duomenų tvarkymo veiksmai buvo sustabdyti;
53.2. jei duomenų subjektas duoda sutikimą toliau tvarkyti savo duomenis;
53.3. jei reikia apsaugoti trečiųjų asmenų teises ar teisėtus interesus.

54. Jeigu Įmonės darbuotojai abejoja duomenų subjekto pateiktų duomenų teisingumu, jie privalo sustabdyti tokių duomenų tvarkymo veiksmus, duomenis patikrinti ir patikslinti. Tokie duomenys gali būti naudojami tik jų teisingumui patikrinti.

55. Įmonės veiksmai ar neveikimas, susiję su duomenų subjekto teisių įgyvendinimu, gali būti skundžiami Valstybinei duomenų apsaugos inspekcijai.

VIII SKYRIUS
DUOMENŲ APSAUGOS PAREIGŪNO FUNKCIJOS

56. Duomenų apsaugos pareigūnas turi šias teises:
56.1. gauti visą reikiamą informaciją bei dokumentus iš bet kurio Įmonės darbuotojo ir (ar) Įmonės partnerio, kuris atlieka asmens duomenų tvarkymą;
56.2. suderinęs su Įmonės vadovu, pasitelkti bet kurį Įmonės darbuotoją duomenų apsaugos pareigūno funkcijoms įgyvendinti;
56.3. būti tinkamai ir laiku įtraukiamas į visų su asmens duomenų apsauga susijusių klausimų (pvz., naujų projektų įgyvendinimo procesą) sprendimą. Duomenų apsaugos pareigūnui suteikiama pakankamai laiko nuomonei pareikšti. Jei į duomenų apsaugos pareigūno nuomonę neatsižvelgiama, duomenų apsaugos pareigūnas yra atsakingas už su tuo susijusių priežasčių dokumentavimą ir šios informacijos saugojimą;
56.4. informuoti Įmonės vadovą apie kylančius organizacinius ar kitus trukdžius tinkamai vykdyti šiose Taisyklėse nurodytas pareigas (pvz., darbuotojai nevykdo duomenų apsaugos pareigūno nurodymų asmens duomenų tvarkymo srityje);
56.5. duomenų apsaugos pareigūnas funkcijų vykdymo metu negali gauti privalomų nurodymų dėl duomenų apsaugos pareigūno kompetencijai priskirtų klausimų sprendimo, pvz., iš anksto numatyto atsakymo pateikimo (duomenų apsaugos pareigūno nepriklausomumo garantija);
56.6. reikalauti skirti būtinus ir protingus išteklius (finansinius, organizacinius, žmogiškuosius, informacinius) duomenų apsaugos pareigūno funkcijoms vykdyti (duomenų apsaugos pareigūno veiklos išteklių garantija);
56.7. nebūti baudžiamas ar patirti bet kokių neigiamų pasekmių dėl tinkamo duomenų apsaugos pareigūno pareigų vykdymo;
56.8. kreiptis į Įmonės vadovą, kai darbuotojai atsisako paklusti duomenų apsaugos pareigūno nurodymams, tiesiogiai susijusiems su asmens duomenų tvarkymo veiksmais.

57. Duomenų apsaugos pareigūnas atlieka šias užduotis:
57.1. informuoja Įmonę ir duomenis tvarkančius darbuotojus apie jų prievoles pagal Reglamentą ir kitus Europos Sąjungos bei Lietuvos Respublikos asmens duomenų apsaugą reglamentuojančių teisės aktų nuostatas ir konsultuoja juos šiais klausimais;
57.2. prižiūri, kaip laikomasi asmens duomenų apsaugą reglamentuojančių teisės aktų, kitų teisės aktų reikalavimų, šių Taisyklių bei kitų Įmonės lokalinių teisės aktų, susijusių su asmens duomenų tvarkymu;
57.3. organizuoja, o prireikus ir pats nustatytu periodiškumo vykdo asmens duomenų tvarkymo veiklos auditą, poveikio duomenų apsaugai vertinimo procesą, asmens duomenų tvarkymo veiklos keliamos rizikos įvertinimą;

57.4. informuoja Įmonės vadovą apie neįgyvendintas asmens duomenų apsaugą reglamentuojančių teisės aktų, Taisyklių pareigas;
57.5. siūlo konkrečias priemones bei būdus, užtikrinančius Įmonės veiklos atitikimą Reglamentui, šioms Taisyklėms bei kitų teisės aktų nuostatoms;
57.6. konsultuoja darbuotojus, duomenų subjektus ir Įmonę visais su asmens duomenų apsauga susijusiais klausimais;
57.7. esant poreikiui bendradarbiauja su Valstybine duomenų apsaugos inspekcija (toliau – Inspekcija) ir atlieka kontaktinio asmens funkcijas, Inspekcijai kreipiantis į Įmonę su asmens duomenų tvarkymu susijusiais klausimais;
57.8. organizuoja, o prireikus ir pats vykdo, pranešimų apie asmens duomenų saugumo pažeidimus teikimą Inspekcijai ir duomenų subjektams;
57.9. organizuoja, o prireikus ir pats vykdo, duomenų subjektų teisių įgyvendinimo ir duomenų subjektų skundų nagrinėjimo procesą;
57.10. ne rečiau kaip kas 2 (du) metus peržiūri ir, jei reikia, organizuoja Taisyklių ir kitos dokumentacijos atnaujinimą;
57.11. atsako į Įmonės darbuotojų klausimus dėl asmens duomenų tvarkymo;
57.12. užtikrina visos jam žinomos ir (ar) patikėtos konfidencialios informacijos slaptumą.

58. Jei darbuotojas ar kitas atsakingas asmuo abejoja įdiegtų asmens duomenų apsaugos saugumo priemonių patikimumu, jis turi kreiptis į Įmonės vadovą arba į duomenų apsaugos pareigūną, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir įdiegimas.

59. Tais atvejais, kai į Įmonę kreipiasi duomenų subjektas dėl VI skyriuje nurodytų savo teisių įgyvendinimo, Įmonės atsakingi darbuotojai dėl asmens duomenų duomenų subjektui pateikimo sprendžia tik gavus raštišką prašymą bei pagrindimą tokius duomenis atskleisti. Kiekvienu tokiu atveju Įmonės atsakingi darbuotojai konsultuojasi su duomenų apsaugos pareigūnu.

60. Darbuotojai, įgalioti tvarkyti asmens duomenis ir (arba) dalyvaujantys priimant sprendimus dėl asmens duomenų tvarkymo ar naujų asmens duomenų tvarkymo technologijų diegimo, privalo užtikrinti, kad būtų laikomasi su asmens duomenų tvarkymu susijusių principų ir dėl jų įgyvendinimo konsultuojasi su duomenų apsaugos pareigūnu.

61. Visi Įmonėje rengiami vidaus dokumentai negali prieštarauti Taisyklėse išdėstytoms nuostatoms. Visi Įmonėje rengiami dokumentų ir daugkartinio taikymo dokumentų, susijusių su asmens duomenų apsauga, projektai, pateikiamai derinti duomenų apsaugos pareigūnui ir tvirtinami tinkamai atsižvelgus į duomenų apsaugos pareigūno rekomendacijas.

62. Bet kuri Įmonėje naudojama duomenų subjektų sutikimo ar pranešimo dėl asmens duomenų tvarkymo forma suderinama su duomenų apsaugos pareigūnu.

63. Visais su asmens duomenų tvarkymu susijusiais klausimais, Įmonės darbuotojai gali kreiptis tiesiogiai į duomenų apsaugos pareigūną el. paštu.

IX SKYRIUS
ASMENS DUOMENŲ SAUGUMĄ UŽTIKRINANČIOS PRIEMONĖS

64. Duomenų valdytojas, saugodamas asmens duomenis, įgyvendina ir užtikrina tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

65. Pasikeitus duomenų subjektų asmens duomenis ir duomenų subjektams apie tai raštu informavus Įmonę, duomenys turi būti atnaujinami, ištrinant neaktualius asmens duomenis ir įrašant aktualius duomenis.

66. Naikinant dokumentus, kurių saugojimo terminas yra pasibaigęs, Įmonės dokumentai, kuriuose naudojami asmens duomenys, ir jų kategorijos turi būti sunaikinti taip, kad šių dokumentų nebūtų galima atkurti ar atpažinti jų turinio.

67. Duomenų subjektų pateikti dokumentai ir jų kopijos, kuriose yra asmens duomenų, saugomos rakinamose spintose arba patalpose. Dokumentai, kuriuose yra asmens duomenų, neturi būti laikomi visiems prieinamoje matomoje vietoje, kur neturintys teisės asmenys nekliudomai galėtų su jais susipažinti.

68. Asmens duomenų rinkmenos, saugomos darbuotojų kompiuteriuose, turi būti apsaugotos slaptažodžiu arba naudojant šifravimo būdą. Darbuotojai yra asmeniškai atsakingi už duomenų apsaugą jų naudojamuose asmeniniuose įrenginiuose.

69. Prieigos prie Įmonės kompiuterių slaptažodžiai suteikiami, keičiami ir saugomi užtikrinant jų konfidencialumą, yra unikalūs, sudaryti iš ne mažiau kaip 7 simbolių (slaptažodyje turi būti didžioji raidė), nenaudojant asmeninio pobūdžio informacijos, keičiami susidarius tam tikroms aplinkybėms (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims, ir pan.) ir naudotojo pirmojo prisijungimo metu. Įmonės darbuotojas prieigos prie asmens duomenų slaptažodžiais turi naudotis asmeniškai ir neatskleisti jų tretiesiems asmenims.

70. Įmonės kompiuterinė įranga turi būti apsaugota nuo kenksmingos programinės įrangos (antivirusinių programų įdiegimas, atnaujinimas ir pan.). Už kompiuterių priežiūrą atsakingas darbuotojas ar išorinis paslaugų teikėjas privalo užtikrinti, kad būtų daromos kompiuterinėse darbo vietose tvarkomų asmens duomenų rinkmenų atsarginės kopijos. Praradus ar sugadinus asmens duomenis, atsakingas darbuotojas turi jas atstatyti ne vėliau kaip per 24 val.

71. Atsitikus duomenų saugumo pažeidimui, darbuotojas ar išorinis paslaugų teikėjas turi nedelsiant informuoti Įmonės vadovą ir jos duomenų apsaugos pareigūną. Vadovas arba jo paskirtas atsakingas asmuo imasi visų reikiamų priemonių, kad būtų pašalintos pažeidimo pasekmės bei atstatyti asmens duomenys. Apie įvykusį duomenų saugumo pažeidimą per 72 val. informuojama Valstybinė duomenų apsaugos inspekcija bei duomenų subjektai, kurių teisės ir laisvės buvo pažeistos, teisės aktų nustatyta tvarka.

72. Įmonės darbuotojai ar išoriniai paslaugų teikėjai (duomenų tvarkytojai), paskirti tvarkyti asmens duomenis, turi laikytis konfidencialumo principo ir laikyti paslaptyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino vykdydami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas. Pareiga saugoti asmens duomenų paslaptį galioja taip pat ir perėjus dirbti į kitas pareigas, pasibaigus darbo ar sutartiniams santykiams.

73. Naujai priimtas darbuotojus pasirašytinai supažindinamas su Taisyklėmis ir privalo užtikrinti šių Taisyklių įgyvendinimą.

74. Įmonės darbuotojai ir išoriniai paslaugų teikėjai turi imtis priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, saugodami dokumentus bei duomenų rinkmenas tinkamai, saugiai bei vengiant nereikalingų kopijų darymo. Jei darbuotojas ar išorinis

paslaugų teikėjas abejoja įdiegtų saugumo priemonių patikimumu, jis turi kreiptis į tiesioginį savo vadovą, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir įdiegimas.

75. Įmonėje nustatomos tokios asmens duomenų saugumą užtikrinančios priemonės:

75.1. patalpos yra apsaugotos nuo neteisėto įsibrovimo į jas, asmens duomenys apsaugoti nuo netyčinio sunaikinimo ar praradimo;

75.2. neleidžiama įgaliojimų neturintiems asmenims patekti į patalpas, kuriose tvarkomi arba naudojami asmens duomenys. Jeigu į patalpas gali patekti kiti asmenys, yra užtikrinama, kad šie asmenys neturėtų galimybės susipažinti su saugomais asmens duomenimis ar kita susijusia informacija bei šią informaciją ar duomenis kopijuoti;

75.3. susipažinti su asmens duomenimis leidžiama tik ribotam asmenų skaičiui. Įgaliojimų neturintiems asmenims naudotis asmens duomenų tvarkymo sistemomis yra draudžiama. Prieigos teises ir įgaliojimus tvarkyti duomenis Įmonės darbuotojams suteikia, naikina ir keičia Įmonės vadovas arba kitas jo įgaliotas asmuo. Įmonės darbuotojus, kuriems suteikta teisė tvarkyti duomenis, informuoja ir jų apmokymus organizuoja už šių Taisyklių įgyvendinimą atsakingas asmuo, atsižvelgiant į teisės aktuose įtvirtintus reikalavimus, Įmonės realius poreikius ir finansines galimybes;

75.4. tarp organizacinių padalinių (jei tokie yra) ir darbuotojų aiškiai paskirstytos funkcijos dėl duomenų naudojimo;

75.5. užtikrinama, kad duomenų tvarkymo sistemą naudojantys įgalioti asmenys galėtų susipažinti tik su tais duomenimis, su kuriais dirbti jie yra įgalioti, taip pat, kad asmens duomenų nebūtų galima be leidimo skaityti, kopijuoti, keisti ar pašalinti tvarkymo, naudojimo ar įrašymo metu;

75.6. paliekant darbo vietą, kompiuteriai yra išjungiami, informacija su asmens duomenimis laikoma tretiesiems asmenims neprieinamoje vietoje;

75.7. užtikrinama, kad atskleidžiant asmens duomenis elektroniniu būdu ar juos transportuojant ar laikant duomenų laikmenoje, jų nebūtų galima skaityti, kopijuoti, keisti ar pašalinti be leidimo, kad būtų galima patikrinti ir nustatyti, kurioms įstaigoms planuojama atskleisti asmens duomenis naudojant duomenų atskleidimo įrangą;

75.8. jokia informacija nėra atskleidžiama telefonu kitam asmeniui, prieš tai nepatikrinus jo tapatybės (pvz., perskambinant į iš anksto nurodytą telefono numerį ir pan.);

75.9. tvarkant asmens duomenis dirbama tik su sertifikuota technine ir programine įranga;

75.10. įdiegtos antivirusinės programos, periodiškai tikrinančios virusų atsiradimą ir jos periodiškai atnaujinamos;

75.11. vartotojui registruojantis sistemoje nurodomas vartotojo vardas ir slaptažodis;

75.12. sukurtas vartotojų teisių ir privilegijų mechanizmas, t. y. kiekvienas duomenų bazių vartotojas turi teises, priskiriamas sistemos administratoriaus;

75.13. visos laikmenos laikomos saugiai užrakintos, kai jos yra nenaudojamos. Kiekviena laikmena (atspausdinta medžiaga, kompaktiniai diskai, atminties laikmenos ir pan.), kuri nėra naudojama, turi būti visiškai ištrinta ir (ar) fiziškai sunaikinta ar perduota į archyvą;

75.14. be Įmonės vadovo raštiško leidimo arba IT paslaugas teikiančio paslaugų tiekėjo leidimo negalima diegti jokios programinės įrangos;

75.15. visi duomenų apdorojimo sistemų ir kompiuterių tinklų įrengimo ir pakeitimo darbai atliekami kompetentingų specialistų;

75.16. siekiant apsaugoti asmens duomenis nuo praradimo neteisėto pakeitimo, jie yra kopijuojami. Nustačius duomenų pažeidimus, duomenys atkuriami iš kopijų. Kopijų saugojimui yra taikoma tokia pati tvarka kaip tai numatyta šiose Taisyklėse;

75.17. Įmonėje reguliariai atliekamas rizikos, susisijusios su duomenų tvarkymu vertinimas. Atsižvelgiant į rizikos vertinimo rezultatus, įdiegiamos reikiamos duomenų saugumo priemonės. Vertinimo ar audito rezultatai įforminami, jei Įmonėje nustatoma duomenų apsaugos trūkumų. Duomenų saugumo pažeidimų valdymą Įmonėje nuolatos atlieka už šių Taisyklių įgyvendinimą atsakingas asmuo bei duomenų apsaugos pareigūnas. Nustatęs

konkrečias duomenų apsaugos Įmonėje rizikas ir (ar) faktinius duomenų saugumo pažeidimus, jie nedelsiant informuoja atsakingus asmenis ir imasi visų galimų techninių ir organizacinių priemonių joms pašalinti.

76. Įgyvendinant pritaikytosios duomenų apsaugos (angl. *privacy by design*) ir standartizuotosios duomenų apsaugos (angl. *privacy by default*) principus, turi būti užtikrinamas pastovus asmens duomenų tvarkymo ir su tuo susijusių rizikų vertinimas. Šiame punkte nurodytų principų įgyvendinimas Įmonėje realizuojamas:

76.1. numatant privalomą asmens duomenų tvarkymo vertinimą pradiniame kiekvieno pokyčio etape – kuriant naują produktą ar jį keičiant, vykdant sudėtingą ar supaprastintą projektą, atliekant informacinių technologijų sistemų pakeitimą ir kt. Vertinimą atlieka duomenų apsaugos pareigūnas, kuris atsako už vertinimo rezultatų teisingumą;

76.2. įtraukiant duomenų apsaugos pareigūną į Įmonės sprendimų priėmimą, tuo užtikrinant, kad veiklos atstovų teikiami pasiūlymai būtų vertinami dėl su asmens duomenų tvarkymu susijusių klausimų;

76.3. prieš pradedant naudoti naujas asmens duomenų rinkimo ir tvarkymo priemones, pavyzdžiui, diegiant informacinę sistemą ar jos pakeitimus, įsigyjant programinę įrangą ar pradedant naudoti kitas asmens duomenų tvarkymo priemones, turi būti konsultuojamasi su duomenų apsaugos pareigūnu dėl numatomų naudoti priemonių atitikties, atsižvelgiant į nustatytą asmens duomenų tvarkymo tikslą ir būtiną duomenų apimtį bei į konkrečiu atveju būtinas užtikrinti organizacines ir technines duomenų saugumo priemones. Duomenų apsaugos pareigūno siūlymu gali būti pasitelkiami išorės paslaugų teikėjai (konsultantai). Visais atvejais privalo būti atsižvelgta į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į duomenų tvarkymo keliamus pavojus duomenų subjektų teisėms ir laisvėms.

77. Jei Įmonė įgalioja duomenų tvarkytoją tvarkyti asmens duomenis, ji privalo parinkti tokį duomenų tvarkytoją, įvertinant ar šis turi pakankamas galimybes ir išteklius garantuoti reikiamas technines ir organizacines duomenų apsaugos priemones ir užtikrinti, kad tokių priemonių būtų laikomasi. Įmonė, įgaliodama duomenų tvarkytoją tvarkyti asmens duomenis, nustato, kad duomenys turi būti tvarkomi tik pagal Įmonės nurodymus. Įmonės ir duomenų tvarkytojo santykiai turi būti reglamentuojami rašytine sutartimi, išskyrus atvejus, kai tokius santykius nustato įstatymai ar kiti teisės aktai.

X SKYRIUS
REIKALAVIMAI ASMENIMS, TVARKANTIEMS ASMENS DUOMENIS IR ASMENS DUOMENŲ TEIKIMAS

78. Išorinis paslaugų teikėjas (duomenų tvarkytojas) pradeda tvarkyti Įmonės asmens duomenis nuo sutarties, kurioje, be kita ko, turi būti nustatytos duomenų tvarkymo sąlygos, pasirašymo dienos arba sutartyje nurodytos datos. Paslaugų teikėjas netenka teisės tvarkyti asmens duomenis, kai pasibaigia sutarties galiojimo terminas arba sutartis nutraukiama. Bet koks išorinis paslaugų teikėjo (duomenų tvarkytojo) atliekamas Įmonės duomenų tvarkymas privalo būti reglamentuojamas sutartimi, kurioje nustatomi duomenų tvarkymo dalykas ir trukmė, duomenų tvarkymo pobūdis ir tikslas, asmens duomenų rūšis ir duomenų subjektų kategorijos bei duomenų valdytojo prievolės ir teisės. Tokioje sutartyje turi būti nustatyta, kad duomenų tvarkytojas (i) tvarko asmens duomenis tik pagal Įmonės (duomenų valdytojo) dokumentais įformintus nurodymus, (ii) užtikrina, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję neterminuotai užtikrinti konfidencialumą; (iii) imasi visų priemonių, kurių reikalaujama pagal Reglamento 32 straipsnį; (iv) privalo gauti Įmonės rašytinį leidimą prieš pasitelkdamas pagalbinį duomenų tvarkytoją; (v) atsižvelgdamas į duomenų tvarkymo pobūdį, padeda Įmonei taikydamas tinkamas technines ir organizacines

priemones, kiek tai įmanoma, kad būtų įvykdyta Įmonės prievolė atsakyti į duomenų subjektų prašymus pasinaudoti duomenų subjekto teisėmis; (vi) padeda duomenų valdytojui užtikrinti Reglamento 32–36 straipsniuose nustatytų prievolių laikymąsi, atsižvelgdamas į duomenų tvarkymo pobūdį ir duomenų tvarkytojo turimą informaciją; (vii) pagal Įmonės pasirinkimą, užbaigus teikti su duomenų tvarkymu susijusias paslaugas, ištrina arba grąžina Įmonei visus asmens duomenis ir ištrina esamas jų kopijas, išskyrus atvejus, kai teisės aktai reikalauja asmens duomenis saugoti; (viii) pateikia Įmonei visą informaciją, būtiną siekiant įrodyti, kad vykdomos Reglamento 28 straipsnyje nustatytos prievolės, ir sudaro sąlygas bei padeda Įmonei arba kitam Įmonės įgaliotam auditoriui atlikti auditą, įskaitant patikrinimus. Įmonė yra atsakinga prieš duomenų subjektus ir priežiūros institucijas už savo pasitelktus duomenų tvarkytojus ir jų padarytus duomenų apsaugos teisės aktų pažeidimus.

79. Įmonės darbuotojas ar išorinis paslaugų teikėjas (duomenų tvarkytojas), tvarkantis duomenų subjektų asmens duomenis, kuriuos tvarko Įmonė, privalo: (i) laikytis pagrindinių asmens duomenų tvarkymo reikalavimų ir saugumo reikalavimų, įtvirtintų Reglamente, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, šiose Taisyklėse, kituose teisės aktuose; (ii) laikytis konfidencialumo ir laikyti paslaptyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jis susipažino vykdydamas savo funkcijas, nebent tokia informacija būtų vieša pagal teisės aktų nuostatas. Pareiga saugoti asmens duomenų paslaptį galioja ir perėjus dirbti į kitas pareigas ar pasibaigus darbo ar paslaugų teikimo santykiams su Įmone; (iii) laikytis šiose Taisyklėse nustatytų organizacinių ir techninių asmens duomenų saugumo priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, saugoti dokumentus, duomenų rinkmenas bei duomenų bazėse saugomus duomenis ir vengti nereikalingų kopijų darymo; (iv) neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su asmens duomenimis nė vienam asmeniui, kuris nėra įgaliotas tvarkyti asmens duomenis; (v) nedelsiant pranešti Įmonei apie bet kokią įtartiną situaciją, kuri gali kelti grėsmę Įmonės tvarkomų asmens duomenų saugumui.

80. Asmens duomenų tvarkymo funkcijas vykdantys ir su Įmonės tvarkomais asmens duomenimis galintys susipažinti darbuotojai turi pasirašyti nustatytos formos konfidencialumo pasižadėjimą (forma pateikiama Taisyklių priede), kuris saugomas darbuotojo asmens byloje.

81. Įmonės darbuotojas ar išorinis paslaugų teikėjas netenka teisės tvarkyti duomenų subjektų asmens duomenis, kai pasibaigia darbo arba paslaugų teikimo santykiai su Įmone arba kai jam pavedama vykdyti su duomenų tvarkymu nesusijusias funkcijas. Darbuotojui arba paslaugų teikėjui iš karto panaikinama prieiga prie asmens duomenų informacinėse sistemose. Darbuotojas ar išorinis paslaugų teikėjas privalo nedelsiant perduoti klientų asmens duomenis Įmonei bei ištrinti visas kopijas jo asmeniniuose įrenginiuose.

82. Asmens duomenys gali būti teikiami:

82.1. daugkartinio teikimo atveju – pagal Įmonės ir duomenų gavėjo sudarytą asmens duomenų teikimo sutartį.

82.2. vienkartinio teikimo atveju – pagal duomenų gavėjo prašymą ir tik įstatymų nustatytais atvejais. Prašyme turi būti nurodytas duomenų naudojimo tikslas.

83. Kiekvienas vienkartinis ir daugkartinis asmens duomenų teikimo poreikis turi būti suderintas su duomenų apsaugos pareigūnu. Daugkartinio teikimo atveju Įmonė ir duomenų gavėjas sudaro duomenų teikimo sutartį, kurioje nurodoma asmens duomenų naudojimo tikslas, sąlygos ir tvarka. Jei duomenų gavėjas nesutinka su Įmonės pateikiama duomenų teikimo sutartimi, į derybas dėl sutarties sąlygų įtraukiamas duomenų apsaugos pareigūnas arba, jo

siūlymu pasitelkiamas reikiamos srities specialistas (teisininkas, informacinių technologijų ekspertas ar kt.).

XI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

84. Įmonės darbuotojai su šiomis Taisyklėmis supažindinami pasirašytinai. Priėmus naują darbuotoją, jis su Taisyklėmis privalo būti supažindintas pirmąją jo darbo dieną.

85. Šios Taisyklės įsigalioja nuo jų patvirtinimo datos.

86. Už Taisyklių laikymosi priežiūrą ir kontrolę, periodinį, ne rečiau kaip kartą per 2 metus, atnaujinimą atsakingas Įmonės vadovas. Įmonės darbuotojams periodiškai, bet ne rečiau kaip kartą per 2 metus, organizuojami mokymai asmens duomenų apsaugos tema. Už mokymų organizavimą atsakingas Įmonės vadovas.

87. Įmonė, Įmonės darbuotojai ir išoriniai paslaugų teikėjai (duomenų tvarkytojai), pažeidę šių Taisyklių reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.
88. Pasikeitus teisės aktų reikalavimams dėl asmens duomenų apsaugos, Įmonės vadovas yra atsakingas už vidinės Įmonės dokumentacijos, Taisyklių bei sutarčių su paslaugų teikėjais nuostatų peržiūrėjimą ir pakeitimą, jeigu to reikia.

89. Dėl šių Taisyklių įvykdytos informavimo ir konsultavimo procedūros su profesine sąjunga.

90. Šių Taisyklių neatsiejama dalimi yra jų priedai:
90.1. 1 priedas – Įmonės darbuotojo įsipareigojimo saugoti asmens duomenų paslaptį forma;
90.2. 2 priedas – Asmens duomenų tvarkymo veiklos įrašų forma;
90.3. 3 priedas – Pranešimo potencialiems darbuotojams dėl asmens duomenų tvarkymo forma;
90.4. 4 priedas – Prašymo įgyvendinti duomenų subjekto teisę forma;
90.5. 5 priedas – Asmens duomenų saugumo pažeidimų registras;
90.6. 6 priedas – Duomenų subjektų prašymų registras;
90.7. 8 priedas – Asmens duomenų saugumo pažeidimų reagavimo tvarka.

(SĮ „Vilniaus miesto būstas“ (toliau – Įmonė) darbuotojo įsipareigojimo saugoti asmens duomenų paslaptį forma)

(Įsipareigojimą pateikiančio asmens vardas, pavardė didžiosiomis raidėmis)

SĮ „VILNIAUS MIESTO BŪSTAS“
DARBUOTOJO
ĮSIPAREIGOJIMAS SAUGOTI ASMENS DUOMENŲ PASLAPTĮ

(data)

Vilnius

Aš suprantu:
- kad dirbdamas (-a) Įmonėje naudosiu ir tvarkysiu asmens duomenis, kurie negali būti atskleisti ar perduoti neįgaliotiems asmenims ar institucijoms;
- kad netinkamas asmens duomenų tvarkymas gali užtraukti atsakomybę man ir Įmonei pagal Europos Sąjungos ir Lietuvos Respublikos teisės aktus;
- kad draudžiama perduoti ar dalintis su kitais asmenimis Įmonės viduje ar už jos ribų slaptažodžiais ir kitais duomenimis, leidžiančiais programinėmis ir techninėmis priemonėmis tvarkyti asmens duomenimis.

Aš pasižadu:
- saugoti Įmonės tvarkomų asmens duomenų paslaptį;
- tvarkyti asmens duomenis vadovaudamasis (-i) teisės aktais, taip pat Įmonės asmens duomenų tvarkymo taisyklėmis ir nurodymais;
- neatskleisti, neperduoti ir nesudaryti sąlygų įvairiomis priemonėmis susipažinti su tiek Įmonės viduje, tiek už jos ribų tvarkoma informacija nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija;
- pranešti Įmonės duomenų apsaugos pareigūnui arba vadovui apie bet kokį įtartiną elgesį ar situaciją, kurie gali kelti grėsmę Įmonės tvarkomų asmens duomenų saugumui.

Aš žinau:
- kad už bet kokį šio įsipareigojimo nesilaikymą ir asmens duomenų teisės aktų pažeidimą turėsiu atsakyti pagal galiojančius Lietuvos Respublikos įstatymus ir kad man gali būti taikoma drausminė nuobauda pagal Lietuvos Respublikos darbo kodeksą;
- kad šis įsipareigojimas galios visą mano darbo Įmonėje laiką ir perėjus dirbti į kitas pareigas arba pasibaigus darbo santykiams;
- kad Įmonės klientas ar kitas duomenų subjektas turi teisę reikalauti atlyginti turtinę ar neturtinę žalą, patirtą dėl neteisėto asmens duomenų tvarkymo;
- kad Įmonė kaip duomenų valdytojas, Įmonės duomenų tvarkytojas arba kitas asmuo atlygina asmeniui padarytą žalą, o nuostolį išreikalauja įstatymų nustatyta tvarka iš asmens duomenis tvarkančio darbuotojo, dėl kurio kaltės atsirado ši žala.

Aš esu susipažinęs su: vidinėmis Įmonės tvarkomis, Bendruoju duomenų apsaugos reglamentu, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais, reglamentuojančiais atsakomybę bei duomenų apsaugą.

(Pareigos, vardas, pavardė) (Parašas)

Duomenų valdytojas	
Pavadinimas ir kontaktai	
Pavadinimas	SĮ "Vilniaus miesto būstas"
Adresas	Švitrigailos g. 7, Vilnius
El. paštas	vilniaus.bustas@vmb.lt
Telefonas	852 779 090

Duomenų apsaugos pareigūnas (kai taikoma)	
Pavadinimas	MB Asmens duomenų apsauga
Kontaktinis asmuo	Rusnė Juozapaitienė
Adresas	Mokslininkų g. 6A, Vilnius
El. paštas	rusne@duomenuapsauga.eu
Telefonas	37069834316

Asmens duomenų tvarkymo taisyklių 3 priedas

PRANEŠIMAS DĖL ASMENS DUOMENŲ TVARKYMO

2020- - , Vilnius

Duomenų valdytojas SĮ „Vilniaus miesto būstas“, juridinio asmens kodas 124568293, adresas Švitrigailos g. 7, Vilnius (toliau – Įmonė arba Mes), informuoja Jus – potencialų Įmonės darbuotoją – apie Jūsų asmens duomenų tvarkymą Įmonėje.

Jūsų asmens duomenys, kuriuos pateikiate Įmonei kandidatuodami į konkrečią Įmonėje skelbiamą poziciją, tvarkomi darbo sutarties su Jumis sudarymo tikslu. Jūsų anketoje ir pridedamuose dokumentuose mums pateikti asmens duomenys bus įrašyti į Įmonės kandidatų duomenų bazę ir bus tvarkomi, kol vykdoma atranka į konkrečią poziciją, į kurią Jūs kandidatavote.

Kaip tvarkomi, kiek laiko tvarkomi Jūsų asmens duomenys, duomenų tvarkymo tikslai, pagrindai, taip pat kokias teises Jūs kaip duomenų subjektas turite, kam perduodami Jūsų asmens duomenys ir kita informacija yra pateikiama Įmonės interneto svetainėje www.vmb.lt skelbiamoje Privatumo politikoje.

Pateikdamas kandidato anketą ir (ar) susijusius dokumentus Jūs patvirtinate:

- ✓ pateikiamų duomenų teisingumą;
- ✓ esate susipažinę su Įmonės interneto svetainėje www.vmb.lt skelbiama Privatumo politika;
- ✓ esate informuoti apie tai, kad klausimais, susijusiais su asmens duomenų tvarkymu, taip pat norėdami įgyvendinti savo kaip duomenų subjekto teises, galite kreiptis į Įmonę elektroniniu paštu vilniaus.bustas@vmb.lt

(Pažymėkite, jei sutinkate)

☐ Sutinku, kad mano asmens duomenys būtų saugomi ir tvarkomi Įmonės kandidatų duomenų bazėje būsimoms atrankoms 3 (trijų) mėnesių terminą mano kandidatūros vertinimo ir pasiūlymų į darbo vietas Įmonėje gavimo tikslu.

_____

(kandidato vardas, pavardė, parašas, data)

Asmens duomenų tvarkymo taisyklių 4 priedas

(Prašymo įgyvendinti duomenų subjekto teisę (-es) rekomenduojama forma)

(Duomenų subjekto vardas, pavardė[1])

(Adresas ir (ar) kiti kontaktiniai duomenys (telefono ryšio numeris ar el. pašto adresas (nurodoma pareiškėjui pageidaujant)

(Atstovas ir atstovavimo pagrindas, jeigu prašymą pateikia duomenų subjekto atstovas)[2]

SĮ „Vilniaus miesto būstas“

PRAŠYMAS
ĮGYVENDINTI DUOMENŲ SUBJEKTO TEISĘ (-ES)

_____
(Data)

_____
(Vieta)

1. Prašau įgyvendinti šią (šias) duomenų subjekto teisę (-es):
(Tinkamą langelį pažymėkite kryželiu):

☐ Teisę gauti informaciją apie duomenų tvarkymą
☐ Teisę susipažinti su duomenimis
☐ Teisę reikalauti ištaisyti duomenis
☐ Teisę reikalauti ištrinti duomenis („teisė būti pamirštam“)
☐ Teisę apriboti duomenų tvarkymą
☐ Teisę į duomenų perkeliamumą
☐ Teisę nesutikti su duomenų tvarkymu
☐ Teisę reikalauti, kad nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas

2. Nurodykite, ko konkrečiai prašote ir pateikite kiek įmanoma daugiau informacijos, kuri leistų tinkamai įgyvendinti Jūsų teisę (-es) *(pavyzdžiui, jeigu norite gauti asmens duomenų kopiją, nurodykite, kokių konkrečiai duomenų (pavyzdžiui, 2018 m. x mėn. x d. elektroninio pašto laiško kopiją, 2018 m. x mėn. x d. vaizdo įrašą (x val. x min. – x val. x min.) kopiją pageidaujate gauti; jeigu norite ištaisyti duomenis, nurodykite, kokie konkrečiai Jūsų asmens duomenys yra netikslūs; jeigu nesutinkate, kad būtų tvarkomi Jūsų asmens duomenys, tuomet nurodykite argumentus, kuriais grindžiate savo nesutikimą, nurodykite dėl kokio konkrečiai duomenų tvarkymo nesutinkate; jeigu kreipiatės dėl teisės į duomenų perkeliamumą įgyvendinimo, prašome nurodyti, kokių duomenų*

[1] Gali būti prašoma nurodyti daugiau duomenų, siekiant nustatyti, ar duomenų subjekto duomenys yra tvarkomi, pavyzdžiui, nurodyti duomenų valdytojo duomenų subjektui priskirtą kodą ir pan.

[2] Jeigu prašymą pateikia duomenų subjekto atstovas, kartu turi būti pridedamas atstovo įgaliojimus patvirtinantis dokumentas.

atžvilgiu šią teisę pageidaujate įgyvendinti, ar pageidaujate juos perkelti į savo įrenginį ar kitam duomenų valdytojui, jeigu pastarajam, tuomet nurodykite kokiam):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____.

PRIDEDAMA[3]:

1. _____.
2. _____.
3. _____.
4. _____.

_____ _____
(Vardas, pavardė) (Parašas)

[3] Jeigu prašymas yra siunčiamas paštu, prie prašymo pridedama asmens tapatybę patvirtinančio dokumento kopija, patvirtinta notaro ar kita teisės aktų nustatyta tvarka.

Jeigu kreipiamasi dėl netikslių duomenų ištaisymo, pateikiamos tikslius duomenis patvirtinančių dokumentų kopijas; jeigu jos siunčiamos paštu, tuomet turi būti patvirtintos notaro ar kita teisės aktų nustatyta tvarka.

Jeigu duomenų subjekto asmens duomenys, tokie kaip vardas, pavardė, yra pasikeitę, kartu pateikiamos dokumentų, patvirtinančių šių duomenų pasikeitimą, kopijos; jeigu jos siunčiamos paštu, tuomet turi būti patvirtintos notaro ar kita teisės aktų nustatyta tvarka.

Incidentų pavyzdžiai

1) Konfidencialios informacijos praradimas (duomenų vagystė).
2) Informacijos vientisumo netekimas (duomenų sugadinimas ar neleistinas pakeitimas).
3) Fizinio IT turto, įskaitant kompiuterius, saugojimo įrenginius, spausdintuvus, ir kt., vagystė.
4) Žala fiziniam IT turtui, įskaitant kompiuterius, saugojimo įrenginius, spausdintuvus ir kt.
5) Paslaugų teikimo sutrikimai.
6) Netinkamas sistemų naudojimas pasitelkiant neleistiną programinę įrangą.

7) Sistemų užkrėtimas naudojant neleistiną programinę įrangą.
8) Bandymas naudoti neleistiną prieigą.
9) Neleistini programinės įrangos arba konfigūracijos pakeitimai.
10) Neįprastos sistemos veikimo atskaitos.
11) Įsibrovimo į sistemas pavojaus signalai („alarmai“).

Asmens duomenų tvarkymo taisyklių 6 priedas

SĮ "Vilniaus miesto būstas" duomenų subjektų prašymų registras

Eilės numeris	Prašymo gavimo data	Prašymą pateikęs asmuo (duomenų subjektas)	Prašymo turinys	Prašymo gavimo šaltinis (paštu, el. paštu, atvykus į buveinę)	Tapatybės nustatymas	Prašymo vertinimas	Prašymo įgyvendinimo veiksmai, įrodymai	Perdavimas duomenų valdytojui (jei tinkama)	Atsakingas darbuotojas

PATVIRTINTA
SĮ „Vilniaus miesto būstas“
Direktoriaus
2020-07-02
įsakymu Nr. 1.23-20/65

SĮ VILNIAUS MIESTO BŪSTAS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REAGAVIMO TVARKA

2020-_____

1. BENDROSIOS NUOSTATOS

1.1.1. Šios asmens duomenų saugumo pažeidimų reagavimo tvarkos (toliau – **Tvarka**) tikslas nustatyti SĮ „Vilniaus miesto būstas“, juridinio asmens kodas 124568293, (toliau – **Įmonė**), Asmens duomenų pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie juos procedūras.

1.1.2. Tvarka yra privaloma visiems Įmonės darbuotojams.

1.1.3. Įmonės vadovui šioje Tvarkoje pavestas funkcijas gali įgyvendinti Įmonės vadovo įsakymu paskirtas asmuo.

1.1.4. Ši Tvarka yra SĮ „Vilniaus miesto būstas“ Asmens duomenų tvarkymo taisyklių (toliau – **Taisyklės)** priedas. Tvarkoje naudojamos sąvokos, jei nenurodyta kitaip, atitinka Taisyklėse nurodytas sąvokas.

2. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

2.1. Asmens duomenų saugumo pažeidimas yra tuomet, kai:

2.1.1. be leidimo ar neteisėtai atskleidžiama ar suteikiama prieiga prie Įmonės tvarkomų asmens duomenų (konfidencialumo pažeidimas);

2.1.2. kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba jie sunaikinami (prieinamumo pažeidimas);

2.1.3. kai be leidimo ar netyčia pakeičiami Asmens duomenys (vientisumo pažeidimas).

(toliau bet kuris iš 2.1 p. nurodytų veiksmų ar visi kartu ar keli iš jų – **ADSP**).

2.2. ADSP be kita ko apima šiuos atvejus:

2.2.1. konfidencialios informacijos atskleidimas asmenims, neturintiems teisės juos gauti;

2.2.2. duomenų arba įrangos, kuriuose saugomi duomenys, praradimas ar vagystė;

2.2.3. popierinių įrašų praradimas ar vagystė;

2.2.4. netinkamos prieigos kontrolės priemonės, leidžiančios neteisėtai naudoti informaciją;

2.2.5. įtariamas Įmonės Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos aprašo pažeidimas;

2.2.6. mėginimas gauti neteisėtą prieigą prie kompiuterių sistemų, pvz., įsilaužimas;

2.2.7. įrašai pakeičiami arba ištrinami be leidimo;

2.2.8. virusai ar kita saugumo ataka prieš IT sistemas ar tinklus;

2.2.9. fizinio saugumo pažeidimai, pvz., fizinis ar elektroninis durų ar langų pažeidimas patalpose, kuriose laikoma konfidenciali informacija;

2.2.10. konfidencialios informacijos palikimas laisvai prieinamose vietose;

2.2.11. IT įrangos palikimas be priežiūros, kai prisijungiama prie vartotojo abonemento, neužblokuojamas ekranas;

2.2.12. sustabdoma neįgaliotų asmenų prieiga prie informacijos;

2.2.13. el. laiškai, kuriuose yra asmens duomenys, klaidingai išsiunčiami neteisingam gavėjui ir kt.

3. ADSP PRIELAIDOS

3.1. Pagrindiniai šaltiniai, kuriais naudojantis gali būti sukeltas ADSP ir sutrikdyta Įmonės infrastruktūra, yra:

3.1.1. išorinės kompiuterinės laikmenos;

3.1.2. internetas;

3.1.3. interneto svetainių pagrindu veikianti programinė įranga;

3.1.4. paprasta įranga;

3.1.5. kiti ADSP šaltiniai.

3.2. Informacija apie galimą ADSP gali būti gaunama iš įvairių informacijos šaltinių:

3.2.1. IT paslaugų teikėjo, kuris atlieka asmens duomenų saugumo pažeidimų stebėseną;

3.2.2. asmens duomenų tvarkytojų;

3.2.3. kompetentingų valstybės institucijų;

3.2.4. tarptautinių organizacijų arba institucijų, atliekančių asmens duomenų saugumo užtikrinimo funkcijas;

3.2.5. Įmonės darbuotojų, paslaugų teikėjų, duomenų tvarkytojų;

3.2.6. žiniasklaidos priemonių;

3.2.7. kitų juridinių ar fizinių asmenų.

3.3. Bet kuris darbuotojas, paslaugų teikėjas ar duomenų tvarkytojas, gavęs informacijos apie galimą ADSP, nedelsiant, ne vėliau kaip per 4 valandas, praneša Duomenų apsaugos pareigūnui raštu (elektroniniu paštu) arba kitam Įmonės vadovo paskirtam atsakingam asmeniui (toliau – Atsakingas asmuo), o nesant galimybės pranešti raštu, nedelsiant informuoti Duomenų apsaugos pareigūną arba Atsakingą Asmenį telefonu apie pastebėtą asmens duomenų saugos pažeidimą. Duomenų tvarkytojui ar paslaugų teikėjui šiame punkte nustatyta pareiga nurodoma ir su duomenų tvarkytoju ar paslaugų teikėju sudarytoje sutartyje.

3.4. Reaguojant į galimą ADSP, atliekami tokie veiksmai (žr. lentelę apačioje):

3.4.1. ADSP nustatymas;

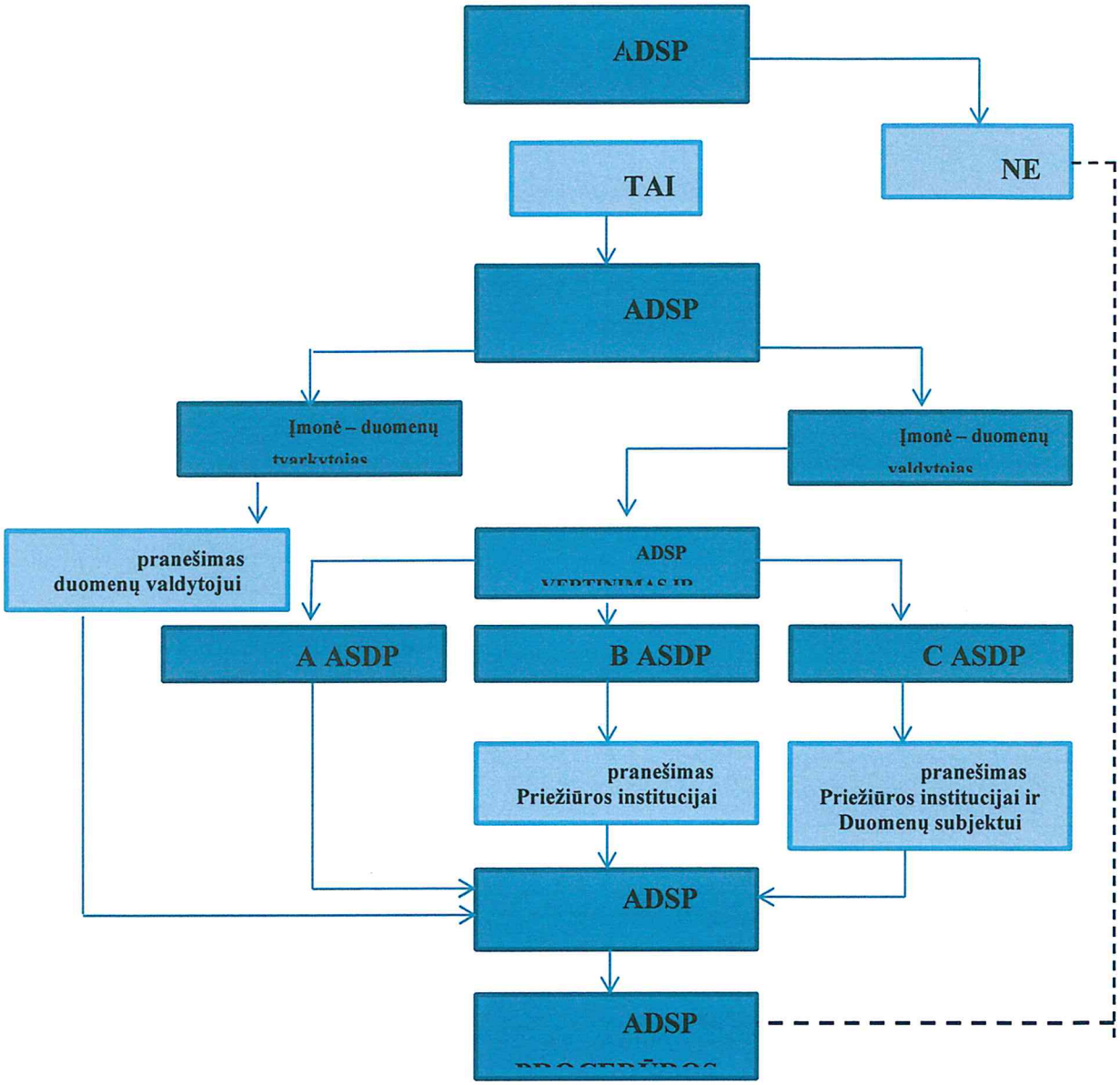
3.4.2. ADSP nutraukimas ir asmens duomenų atkūrimas;

3.4.3. ADSP laipsnio vertinimas ir nustatymas;

3.4.4. pranešimas apie ADSP;

3.4.5. ADSP registro pildymas;

3.4.6. ADSP procedūros užbaigimas.



4. ADSP NUSTATYMAS

4.1. Duomenų apsaugos pareigūnas arba Atsakingas asmuo įvertina gautą informaciją apie galimą ADSP pagal Tvarkos 2.1, 2.2 p. nurodytus kriterijus ir patvirtina arba paneigia ADSP nustatymo faktą.

4.2. Duomenų apsaugos pareigūnas arba Atsakingas asmuo, patvirtinęs ADSP nustatymo faktą, per kuo trumpesnį laiką praneša Įmonės vadovui apie ADSP. Jei reikia, sudaroma ADSP valdymo komisija (toliau – **Valdymo komanda**), į kurios sudėtį įeina Duomenų apsaugos pareigūnas, Įmonės vadovas, IT specialistas.

4.3. Valdymo komanda (jei sudaroma) ar Duomenų apsaugos pareigūnas arba Atsakingas asmuo nustato ar pažeidimas susijęs su asmens duomenimis kuriuos tvarkydama Įmonė veikia kaip duomenų valdytojas, ar kaip tvarkytojas.

4.4. Atliekant pirminį tyrimą ir siekiant nustatyti, ar ADSP iš tikrųjų įvyko, išsaugomi esamos situacijos įrodymai, o vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės, pvz., duomenų srauto ir prisijungimų analizės įrankiai bei kt.

5. PAŽEIDIMO NUTRAUKIMAS IR PADĖTIES ATKŪRIMAS

5.1. Įmonės vadovas, gavęs informacijos iš Duomenų apsaugos pareigūno arba Atsakingo asmens apie ADSP, nedelsiant imasi visų įmanomų priemonių ADSP nutraukti ir padėčiai atstatyti. Jei būtina, pasitelkiami kiti Įmonės darbuotojai, IT paslaugų teikėjai, Valdymo komanda.

5.2. Duomenų apsaugos pareigūnas arba Atsakingas asmuo, veikdamas kartu su Valdymo komanda, priklausomai nuo situacijos įvertina Įmonės informacinės infrastruktūros būklę, nustato pažeistas jos dalis ir per kuo trumpesnį laiką imasi veiksmų pažeistoms dalims atkurti arba pakeisti ir (arba) teikia Įmonės IT infrastruktūros paslaugos teikėjams siūlymus dėl pažeistų dalių atkūrimo arba pakeitimo, jeigu to negalima padaryti savo jėgomis.

5.3. Prieš atkurdamas Įmonės informacinės infrastruktūros veiklą, Įmonės vadovas, veikdamas kartu su IT specialistu, privalo įsitikinti, ar pašalintas pažeidžiamumas, dėl kurio įvyko ADSP.

5.4. Pagrindiniai kriterijai, kuriais vadovaujantis priimamas sprendimas dėl ADSP valdymo priemonių:

5.4.1. numatytas galimas poveikis ir žala;

5.4.2. ADSP įrašų išsaugojimo, jų patikimumo, vientisumo ir pasiekiamumo užtikrinimas;

5.4.3. informacinės infrastruktūros neveikimo terminas;

5.4.4. ADSP valdymo sprendimui įgyvendinti reikalingas laikas ir ištekliai;

5.4.5. numatoma kita žala, kurią gali padaryti ADSP, priėmus jo valdymo sprendimą.

5.5. Konkretūs veiksmai, siekiant nutraukti ADSP ir atstatyti padėtį galėtų būti tokie:

5.5.1. duomenų ištrynimas nuotoliniu būdu iš pamesto ar pavogto įrenginio;

5.5.2. kuo skubesnis kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti asmens duomenys, su prašymu neatidarinėti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;

5.5.3. tretiesiems asmenims atskleisto ar kitaip sužinoto prisijungimo prie duomenų bazės slaptažodžio pakeitimas;

5.5.4. prarastų asmens duomenų atkūrimas iš turimos atsarginės kopijos.

5.6. Vykdant šią procedūrą reikia imtis atsargumo priemonių tam, kad būtų užtikrinta, jog būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį ADSP (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 asmens duomenimis).

6. PAŽEIDIMO RIZIKOS IR LAIPSNIO VERTINIMAS

6.1. Duomenų apsaugos pareigūnas arba Atsakingas asmuo nedelsiant, bet ne vėliau, kaip per 8 valandas nuo ADSP, kuris susijęs su asmens duomenimis, kuriuos Įmonė tvarko kaip duomenų valdytojas, nustatymo, išsiaiškina ADSP aplinkybes ir įvertina riziką, kurią gali sukelti ADSP, atsižvelgiant į ADSP sunkumą, suteikiant ADSP vieną iš šių laipsnių: A – tikėtina, kad rizikos asmenims dėl ADSP nėra (toliau – **A ADSP**); B – dėl ADSP kyla rizika asmenims (toliau – **B ADSP**); C – dėl ADSP yra didelė rizika asmenims (toliau – **C ADSP**). Konkretus ADSP sunkumo laipsnis nustatomas pagal žemiau nurodytus kriterijus. Konkretų ADSP laipsnį patvirtina ir imasi tolesnių veiksmų Įmonės vadovas pagal Duomenų apsaugos pareigūno arba Atsakingo asmens rekomendaciją.

6.2. Vertinant ADSP rizikos laipsnį, atsižvelgiama į konkrečias ADSP aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika turėtų būti vertinama remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus:

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

6.2.2. kaip lengvai identifikuojamas fizinis asmuo;
6.2.3. pasekmių rimtumą fiziniams asmenims;
6.2.4. specialias fizinio asmens savybes (pvz., duomenys susiję su vaikais ar kitais pažeidžiamais asmenimis);
6.2.5. nukentėjusiųjų fizinių asmenų skaičių;
6.2.6. specialias duomenų valdytojo savybes (pvz., Įmonės veiklos pobūdį).

6.3. A ADSP laipsnis (žemas rizikos laipsnis) nustatomas tada, kai patiriamas ADSP, dėl kurio neturėtų kilti pavojaus duomenų subjekto teisėms ir laisvėms. A ADSP gali būti, pavyzdžiui, kai nustatoma, kad paliktas kompiuteris neužrakintu ekranu, tačiau jokie asmenys, neturintys prieigos prie duomenų, nepateko į patalpą.

6.4. B ADSP laipsnis (vidutinis rizikos laipsnis) nustatomas tada, kai patiriamas ADSP, kuris kelia pavojų duomenų subjektams (pavojų keliančiu laikytinas toks pažeidimas, dėl kurio asmuo galėtų patirti materialinę ar nematerialinę žalą, teisių apribojimą, diskriminaciją, galėtų būti pavogta ar suklastota asmens tapatybė, asmeniui padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta asmens reputacijai, prarasti asmens duomenys, kurie laikomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala). Tokie atvejai galėtų būti pavyzdžiui, laikmenos praradimas su kelių klientų fizinių asmenų kontaktais.

6.5. C ADSP laipsnis (aukštas rizikos laipsnis) nustatomas tada, kai dėl ADSP gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms (didelį pavojų keliančiu ADSP laikytinas bet kuris 6.3. punkte nurodytų pasekmių riziką keliantis ADSP tada, jei tokios pažeidimo pasekmės yra labai tikėtinos, tvarkomi jautrūs Asmens duomenys (pavyzdžiui, duomenys apie sveikatą), pažeidimas turi neigiamą poveikį dideliam duomenų subjektų skaičiui ir pan.). Pavyzdžiui, pametamas nešiojamasis kompiuteris, kuriame yra sutartys su klientais fiziniais asmenimis.

7. PRANEŠIMAS APIE ADSP

7.1. Patvirtinus A ADSP, pranešimas nei Valstybinei duomenų apsaugos inspekcijai (toliau – **Priežiūros institucija**), nei duomenų subjektams nėra teikiamas, nebent kyla abejonių, ar apie ADSP reikia pranešti Priežiūros institucijai. Jei kyla abejonių, ar apie ADSP reikia pranešti Priežiūros institucijai, Duomenų apsaugos pareigūnas arba Atsakingas asmuo informuoja apie tai Įmonės vadovą, kuris gali nuspręsti, kad konkrečiu A ADSP atveju turi būti teikiamas pranešimas Priežiūros institucijai. ADSP dokumentuojama, kaip nurodyta Asmens duomenų tvarkymo taisyklių Priede Nr. 5 ir užbaigiama ADSP procedūra.

7.2. Nustačius B ADSP, Duomenų apsaugos pareigūnas arba Atsakingas asmuo ne vėliau kaip per 72 valandas nuo ADSP patvirtinimo momento Priežiūros institucijai pateikia reikiamą informaciją, užpildydamas Pranešimo formą, pateiktą Priede Nr. 2.

7.3. Pranešimas Priežiūros institucijai teikiamas per interneto svetainę www.ada.lt naudojantis elektronine paslaugų sistema; nesant tokios galimybės, pranešimas teikiamas elektroninio pašto adresu ada@.lt; nesant tokių galimybių, Valstybinė duomenų apsaugos inspekcija informuojama telefono ryšio numeriu (8 5) 271 2804 arba faksu (8 5) 261 9494 ir nedelsiant informacija išsiunčiama registruotu laišku.

7.4. Jei Priežiūros institucijai apie ADSP nepranešama per 72 valandas, prie pranešimo Įmonė privalo pateikti vėlavimo priežastis ir tokiu atveju informacija apie ADSP teikiama etapais, apie informacijos teikimą etapais pažymint pirmame pranešime Priežiūros institucijai. Kai informacija teikiama etapais, pirmasis pranešimas turi būti pateiktas per 72 valandas.

7.4.1. jei Priežiūros institucija paprašo patikslinti arba papildyti informaciją apie ADSP, Duomenų apsaugos pareigūnas arba Atsakingas asmuo organizuoja papildomos informacijos surinkimą ir pateikimą Priežiūros institucijai jos nustatytu laiku.

7.5. Patvirtinus C ADSP, Įmonė nepagrįstai nedelsdama praneša apie ADSP duomenų subjektams bei Priežiūros institucijai *(pranešimas Priežiūros institucijai teikiamas tokia pačia tvarka, kaip ir nustačius B ADSP)*. Duomenų pareigūnas arba kitas atsakingas asmuo duomenų subjektams turi pateikti aiškią ir suprantamą informaciją, kurioje turi būti bent ši informacija:

7.5.1. ADSP apibūdinimas;

7.5.2. tikėtinų padarinių, kurie jau atsirado arba gali atsirasti ateityje, sąrašas;

7.5.3. priemonių, kurių buvo imtasi ir/ar bus imtasi norint sustabdyti ADSP bei pašalinti atsiradusius arba atsirasiančius padarinius, priemonių galimoms neigiamoms pasekmėms sumažinti sąrašas (pvz., siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);

7.5.4. duomenų apsaugos pareigūno kontaktai;

7.5.5. kita reikšminga informacija, susijusi su ADSP, kuri, duomenų valdytojo manymu, turėtų būti pateikta duomenų subjektui.

7.6. 7.5 punkte nurodyta informacija duomenų subjektui turi būti pateikiama 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. Jei tiesioginis komunikavimas pareikalautų neproporcingai daug pastangų, tokiu atveju apie įvykusį ADSP Įmonės vadovui patvirtinus, paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

7.7. 7.5 punkte nurodytas pranešimas duomenų subjektui gali būti neteikiamas, jei egzistuoja bet kuri iš šių aplinkybių:

7.7.1. Įmonė įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems ADSP turėjo poveikį;

7.7.2. Įmonė vėliau ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

7.8. Įmonė išsaugo įrodymus, patvirtinančius tiesioginę ar viešą komunikaciją duomenų subjektui apie įvykusį ADSP, bei Priežiūros institucijai pareikalavus privalo jai pateikti šiuos įrodymus.

7.9. Duomenų apsaugos pareigūnas arba Atsakingas asmuo, įvertinęs gautą informaciją apie ADSP, esant Įmonės vadovo sutikimui, nedelsdamas informuoja apie ADSP nustatymo faktą ne tik Priežiūros instituciją ar duomenų subjektą (kai reikia), bet ir policiją – nustačius, kad ADSP gali turėti nusikalstamos veikos požymių.

7.10. Jei nustatoma, kad ADSP susijęs su Asmens duomenimis, kuriuos Įmonė tvarko kaip duomenų tvarkytojas, informuojamas minėtų asmens duomenų valdytojas.

8. ADSP REGISTRO PILDYMAS

8.1. Visi veiksmai, kurių imamasi ADSP valdymo procedūros metu, turi būti aprašomi ir visi susiję įrašai apie ADSP peržiūrimi tam, kad būtų užtikrintas jų išbaigtumas, tikslumas ir atitiktis atitinkamam teisiniam reguliavimui. Šiam tikslui pasiekti turi būti vedamas ADSP žurnalas, kuriame tiksliai aprašomi veiksmai, kurių buvo imtasi įgyvendinant ADSP valdymo procedūrą.

8.2. ADSP žurnalas yra elektroninės formos ir pateiktas Asmens duomenų tvarkymo taisyklių Priede Nr. 5. Elektroninį ADSP registrą pildo Duomenų apsaugos pareigūnas. Elektroninis žurnalas yra saugomas, prieigos prie elektroninio žurnalo suteikiamos Duomenų apsaugos

pareigūnui arba Atsakingam asmui ir Įmonės vadovui. Įmonė saugo įrašus apie tai, kas, kada turėjo prieigas prie ADSP žurnalo, ar buvo atliktos modifikacijos. Įrašas ADSP žurnale saugomas 10 metų nuo ADSP procedūros ar Priežiūros institucijos tyrimo užbaigimo, atsižvelgiant į tai, kas įvyko vėliau.

8.3. Įrašai į ADSP žurnalą įvedami, per 5 darbo dienas po to, kai nustatomas galimas ADSP ir įvertinama rizika. ADSP žurnale nurodoma:

8.3.1. visi su ADSP susiję faktai – ADSP priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

8.3.2. ADSP poveikis ir pasekmės;

8.3.3. ADSP taisomieji veiksmai (techninės priemonės), kurių buvo imtasi;

8.3.4. priežastys dėl su ADSP susijusių sprendimų priėmimo (pvz., kodėl Įmonė nusprendė nepranešti apie ADSP Priežiūros institucijai ir (ar) duomenų subjektui, t. y. kodėl nusprendė, kad tikėtina, jog ADSP negali sukelti pavojaus fizinių asmenų teisėms ir laisvėms, arba kokią sąlygą įvykdė, kuomet pranešti apie ADSP duomenų subjektui nereikia);

8.3.5. pranešimo Priežiūros institucijai pateikimo vėlavimo priežastys (jeigu pranešimą vėluojama pateikti ar pranešimas teikiamas etapais);

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

8.3.7. kita reikšminga informacija susijusi su ADSP (pvz., kad tyrimo metu nustatyta, jog faktiškai ADSP nebuvo, o buvo tik saugumo incidentas).

9. ADSP PROCEDŪROS UŽBAIGIMAS

9.1. Suvaldžius ADSP, Duomenų apsaugos pareigūnas arba Atsakingas asmuo apie ADSP suvaldymo rezultatus informuoja Įmonės vadovą.

9.2. Duomenų apsaugos pareigūnas arba Atsakingas asmuo, gavęs supažindinto su ADSP ir jo pašalinimo aplinkybėmis Įmonės vadovo pritarimą, priima sprendimą užbaigti ADSP valdymo procedūrą tada, kai ADSP laikytinas likviduotu, o visoms reikalingoms šalims apie ADSP yra pranešta.

10. PAŽEIDIMŲ ANALIZĖ IR PREVENCIJOS PRIEMONIŲ ĮGYVENDINIMO KONTROLĖ

10.1. Duomenų apsaugos pareigūnas arba Atsakingas asmuo vieną kartą per metus peržiūri įrašus ADSP žurnale, atlieka žurnale esančių ADSP analizę. Atsižvelgdamas į ADSP analizės rezultatus, Duomenų apsaugos pareigūnas arba Atsakingas asmuo Įmonės vadovui pateikia rekomendacijas dėl ADSP prevencijos priemonių, tam kad ADSP ateityje nepasikartotų, įgyvendinimo.

10.2. Įmonės vadovas atsakingas už Duomenų apsaugos pareigūno arba Atsakingo asmens rekomenduotų ADSP prevencijos priemonių įgyvendinimą.

11. SUPAŽINDINIMAS SU TVARKA

11.1. Darbuotojai, supažindinami su šia Tvarka pasirašytinai.

SĮ „Vilniaus miesto būstas“
Asmens duomenų
saugumo pažeidimų reagavimo tvarkos
2 priedas

SĮ „Vilniaus miesto būstas“

(duomenų valdytojo (juridinio asmens) pavadinimas, duomenų valdytojo atstovo pavadinimas, duomenų valdytojo (fizinio asmens) vardas, pavardė)

Kodas 124568293, adresas Švitrigailos g. 7, Vilnius, LT-03110 Lietuvos Respublika

(juridinio asmens kodas ir buveinės adresas arba fizinio asmens kodas, gimimo data (jeigu asmuo neturi asmens kodo) ir asmens duomenų tvarkymo vieta

el. p. vilniaus.bustas@vmb.lt, tel. 8 5 277 9090

(telefono ryšio ir (ar) elektroninio pašto adresas, ir (ar) elektroninės siuntos pristatymo dėžutės adresas)

Valstybinei duomenų apsaugos inspekcijai

PRANEŠIMAS

APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____Nr. _____

(data) (rašto numeris)

1.Asmens duomenų saugumo pažeidimo apibūdinimas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:

Asmens duomenų saugumo pažeidimo:

Data _____ Laikas _____

Asmens duomenų saugumo pažeidimo nustatymo:

Data _____ Laikas _____

1.2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us):

- ☐ Informacinė sistema
- ☐ Duomenų bazė
- ☐ Tarnybinė stotis
- ☐ Internetinė svetainė
- ☐ Debesų kompiuterijos paslaugos
- ☐ Nešiojami / mobilus įrenginiai
- ☐ Neautomatiniu būdu susistemintos bylos (archyvas)
- ☐ Kita _____

1.3.Asmens duomenų saugumo pažeidimo aplinkybės (pažymėti tinkamą (-us):

☐ Asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas)
☐ Asmens duomenų vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas)
☐ Asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas)

1.4. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:
_____

1.5. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (atskiriamos pagal jai būdingą požymį):
_____
_____

1.6. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-as):

☐ Asmens tapatybę patvirtinantys asmens duomenys (vardas, pavardė, amžius, gimimo data, lytis ir kt.):

_____

_____

☐ Specialių kategorijų asmens duomenys (duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, sveikatos duomenys, duomenys apie lytinį gyvenimą ir lytinę orientaciją):

_____

_____

_____

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

_____

_____

☐ Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai (pavyzdžiui, asmens kodas, mokėtojo kodas, slaptažodžiai):

_____

_____

☐ Kiti:

_____

_____

☐ Nežinomi (pranešimo teikimo metu)

1.7. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

_____

1.8. Kita duomenų valdytojo nuomone reikšminga informacija apie asmens duomenų saugumo pažeidimą:

_____

_____

_____

_____

_____

2.	Galimos asmens duomenų saugumo pažeidimo pasekmės

2.1. Konfidencialumo praradimo atveju:

☐ Asmens duomenų išplitimas labiau nei yra būtina ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pavyzdžiui, asmens duomenys išplito internete)

☐ Skirtingos informacijos susiejimas (pavyzdžiui, gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)

☐ Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pavyzdžiui, komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)

☐ Kita

_____

_____

_____

_____

_____

_____

2.2. Vientisumo praradimo atveju:

☐ Pakeitimas į neteisingus duomenis dėl ko asmuo gali netekti galimybės naudotis paslaugomis

☐ Pakeitimas į galiojančius duomenis, kad asmens duomenų tvarkymas būtų nukreiptas (pavyzdžiui, pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)

☐ Kita

_____

_____

_____

_____

_____

_____

2.3. Duomenų prieinamumo praradimo atveju:

☐ Dėl asmens duomenų trūkumo negalima teikti paslaugų (pavyzdžiui, administracinių procesų sutrikdymas, dėl ko negalima prieiti, pavyzdžiui, prie asmens sveikatos istorijų ir teikti pacientams sveikatos paslaugų, arba įgyvendinti duomenų subjekto teises)

☐ Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pavyzdžiui, asmens sveikatos istorijoje neliko informacijos apie asmens alergijas, tam tikra informacija iš mokesčių deklaracijos išnyko, dėl ko negalima tinkamai apskaičiuoti mokesčių ir pan.)

☐ Kita

_____

_____

_____

_____

2.4. Kita:

3. Priemonės, kurių imtasi siekiant pašalinti pažeidimą ar sumažinti jo pasekmes

3.1. Taikytos priemonės siekiant sumažinti poveikį duomenų subjektams:

3.2. Taikytos priemonės siekiant pašalinti asmens duomenų saugumo pažeidimą:

3.3. Taikytos priemonės siekiant, kad pažeidimas nepasikartotų:

3.4. Kita:

4. Siūlomos priemonės sumažinti asmens duomenų saugumo pažeidimo pasekmėms

5. Duomenų subjektų informavimas apie asmens duomenų saugumo pažeidimą

5.1. Duomenys apie informavimo faktą:

☐ Taip, duomenų subjektai informuoti (nurodoma data) _____

☐ Ne, bet jie bus informuoti (nurodoma data) _____

☐ Ne

5.2. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, neinformavimo priežastys:

☐ Ne, nes nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodoma kodėl)

☐ Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami (nurodomos kokios)

_____

_____

☐ Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos kokios)

_____

_____

_____

_____

_____

☐ Ne, nes tai pareikalautų neproporcingai daug pastangų ir apie tai viešai paskelbta (arba taikyta panaši priemonė) (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta)

_____

_____

☐ Ne, nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas

5.3. Informacija, kuri buvo pateikta duomenų subjektams (gali būti pridėtas pranešimo duomenų subjektui kopija):

_____

_____

_____

_____

_____

_____

_____

5.4. Būdas, kokiu duomenų subjektai buvo informuoti:

☐ Paštu
☐ Elektroniniu paštu
☐ Kitu būdu

_____

5.5. Informuotų duomenų subjektų skaičius _____

6. Asmuo galintis suteikti daugiau informacijos apie asmens duomenų saugumo pažeidimą (duomenų apsaugos pareigūnas ar kitas kontaktinis asmuo)

6.1. Vardas ir pavardė_____

6.2. Telefono ryšio numeris _____

6.3. Elektroninio pašto adresas _____

6.4. Pareigos _____

6.5. Darbovietės pavadinimas ir adresas_____

_____

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

_____
_____
_____
_____
_____
_____
_____

8. Kita reikšminga informacija

_____
_____
_____
_____
_____
_____
_____
_____
_____

_____ _____ _____

(pareigos) (parašas) (vardas, pavardė)