PATVIRTINTA
VšĮ „Actio Catholica Patria“ direktorės
2026 m. spalio 28 d. įsakymu Nr. T-26/10/28-1

VŠĮ „ACTIO CATHOLICA PATRIA“ ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šios VšĮ „Actio Catholica Patria“ asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) nustato asmens duomenų tvarkymo, apsaugos ir atskaitomybės reikalavimus, duomenų subjektų teisių įgyvendinimo, asmens duomenų saugumo pažeidimų valdymo, darbo informacinėmis ir ryšių technologijomis bei kitas organizacines procedūras.

2. Taisyklės parengtos vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 (Bendruoju duomenų apsaugos reglamentu, toliau – BDAR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, Lietuvos Respublikos darbo kodeksu ir kitais taikytinais teisės aktais.

3. Duomenų valdytoja yra VšĮ „Actio Catholica Patria“, juridinio asmens kodas 190777829, buveinės adresas Smalininkų g. 9, LT-44295 Kaunas (toliau – Organizacija). Su asmens duomenų apsauga susijusiais klausimais kreipiamasi Organizacijos viešai skelbiamu elektroninio pašto adresu arba kitais nurodytais kontaktais.

4. Taisyklės taikomos visiems Organizacijos darbuotojams, savanoriams, praktikantams, mentoriams, tutoriams, stažuotojams, lektoriams ir kitiems asmenims, kurie vykdydami funkcijas gauna prieigą prie Organizacijos tvarkomų asmens duomenų.

5. Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos BDAR ir kituose taikytinuose teisės aktuose. Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas nėra laikomi specialių kategorijų duomenimis, tačiau tvarkomi tik BDAR 10 straipsnyje ir nacionalinėje teisėje nustatytomis sąlygomis.

6. Organizacijos direktorė užtikrina Taisyklių įgyvendinimą, atsakomybių paskirstymą, reikalingų išteklių skyrimą ir sprendimų dėl didesnės rizikos duomenų tvarkymo priėmimą. Kiekvienas asmuo atsako už Taisyklių laikymąsi savo funkcijų ribose.

6.1. Direktorė įsakymu ar kitu dokumentu paskiria asmenį arba asmenis, koordinuojančius duomenų subjektų prašymų nagrinėjimą, saugumo pažeidimų registravimą, veiklos įrašų, saugojimo terminų rodyklės ir duomenų tvarkytojų bei gavėjų registro atnaujinimą.

6.2. Paskyrimas nepanaikina direktorės atsakomybės už Organizacijos atitiktį, o paskirti asmenys veikia pagal aiškiai apibrėžtas funkcijas ir turi teisę gauti joms vykdyti būtiną informaciją.

6.3. Darbuotojai, savanoriai, praktikantai ir kiti prieigą turintys asmenys bendradarbiauja su atsakingais asmenimis, laiku pateikia informaciją apie pasikeitusius procesus, sistemas, gavėjus ir pastebėtus neatitikimus.

II SKYRIUS
ASMENS DUOMENŲ TVARKYMO PRINCIPAI IR TEISĖTUMAS

7. Asmens duomenys tvarkomi teisėtai, sąžiningai ir skaidriai, tik nustatytais tikslais, tik būtina apimtimi, užtikrinant jų tikslumą, saugojimo trukmės apribojimą, vientisumą, konfidencialumą ir Organizacijos gebėjimą įrodyti šių principų laikymąsi.

8. Prieš pradedant naują tvarkymo veiklą, naudojant naują sistemą, renkant naujos kategorijos duomenis arba perduodant duomenis naujam gavėjui, atsakingas darbuotojas įvertina tikslą, būtinumą, proporcingumą, teisinį pagrindą, saugojimo terminą, gavėjus ir rizikas duomenų subjektų teisėms.

9. Paprastieji asmens duomenys tvarkomi tik esant bent vienai BDAR 6 straipsnio 1 dalyje nustatytai sąlygai. Specialių kategorijų duomenims papildomai turi būti taikoma bent viena BDAR 9 straipsnio 2 dalies sąlyga.

10. Duomenys apie apkaltinamuosius nuosprendžius, nusikalstamas veikas, neteistumą ar teisę dirbti su vaikais tvarkomi tik tiek, kiek tai leidžia arba įpareigoja taikytini teisės aktai. Kai tikslui pasiekti pakanka patikrinti dokumentą ar kodą, kopija nesaugoma, o fiksuojamas patikrinimo faktas, data ir rezultatas.

11. Organizacija ypatingą dėmesį skiria nepilnamečių, socialinę riziką patiriančių jaunuolių, globos įstaigų auklėtinių, neįgalių asmenų ir kitų pažeidžiamų duomenų subjektų duomenims. Prieiga prie individualių konsultacijų užrašų, socialinių vertinimų, pagalbos planų, sveikatos ir apgyvendinimo informacijos suteikiama tik tiesiogiai tokias funkcijas vykdantiems asmenims.

12. Asmens kodas, tapatybės dokumentų kopijos, sveikatos duomenys, šeiminės ar socialinės padėties informacija ir kiti jautrūs duomenys renkami tik tada, kai jie objektyviai būtini konkrečiam tikslui ir jų tvarkymas pagrįstas. Draudžiama rinkti duomenis „atsargai“.

13. Tvarkymo tikslai, duomenų subjektų ir duomenų kategorijos, teisiniai pagrindai, gavėjai, saugojimo terminai, perdavimai į trečiąsias valstybes ir bendras saugumo priemonių aprašymas nustatomi Organizacijos duomenų tvarkymo veiklos įrašuose.

14. Jeigu planuojamas duomenų tvarkymas gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms, prieš pradedant tvarkymą atliekamas poveikio duomenų apsaugai vertinimo poreikio įvertinimas, o esant BDAR 35 straipsnio sąlygoms – poveikio duomenų apsaugai vertinimas.

III SKYRIUS
PAREIGOS IR KONFIDENCIALUMAS

15. Asmens duomenis galima tvarkyti tik pagal Organizacijos suteiktus įgaliojimus, teisėtus nurodymus ir tiek, kiek būtina pavestoms funkcijoms vykdyti.

16. Asmenys, turintys prieigą prie duomenų, privalo saugoti jų konfidencialumą darbo, savanorystės, praktikos ar paslaugų teikimo metu ir pasibaigus atitinkamiems santykiams. Konfidencialumo pareiga neterminuota, išskyrus atvejus, kai informacija teisėtai tapo vieša.

17. Draudžiama asmens duomenis perduoti neįgaliotiems asmenims, aptarinėti viešose vietose, palikti be priežiūros, naudoti asmeniniais tikslais, kopijuoti į nepatvirtintas laikmenas ar siųsti nepatvirtintais kanalais.

18. Darbuotojas nedelsdamas informuoja direktorę arba kitą paskirtą atsakingą asmenį apie netikslius ar perteklinius duomenis, nepagrįstą prieigą, netinkamą gavėją, prarastą įrenginį, įtartiną laišką, kenkėjišką programą ar kitą aplinkybę, galinčią kelti pavojų asmens duomenims.

19. Organizacija periodiškai organizuoja darbuotojų, savanorių ir kitų prieigą turinčių asmenų mokymus bei supažindinimą su saugaus duomenų tvarkymo reikalavimais.

IV SKYRIUS
ASMENS DUOMENŲ TVARKYMAS SUTIKIMO PAGRINDU IR ATVAIZDO NAUDOJIMAS

20. Sutikimas naudojamas tik tada, kai duomenų subjektas turi realų pasirinkimą ir duomenų tvarkymas nėra būtinas sutarčiai vykdyti, teisinei prievolei, viešojo intereso užduočiai ar teisėtam interesui įgyvendinti.

21. Sutikimas turi būti laisvas, konkretus, informuotas, nedviprasmiškas ir įrodomas. Atskiriems tarpusavyje nesusijusiems tikslams sudaroma galimybė sutikti atskirai. Tylėjimas, neveikimas ar iš anksto pažymėti pasirinkimai nelaikomi sutikimu.

21.1. Sutikimas nelaikomas duotu laisva valia, jeigu paslaugos, darbo, praktikos, savanorystės ar kito santykio vykdymas nepagrįstai siejamas su sutikimu tvarkyti tam santykiui nebūtinus duomenis arba atsisakymas gali sukelti neigiamų pasekmių.

21.2. Kai tvarkymas apima kelis savarankiškus tikslus ar viešinimo kanalus, asmeniui sudaroma galimybė pasirinkti kiekvieną tikslą ar kanalą atskirai.

21.3. Sutikimo tekstas turi būti aiškiai atskirtas nuo kitų sąlygų, pateiktas paprasta ir suprantama kalba, jame negali būti klaidinančių ar pernelyg abstrakčių formuluočių.

21.4. Organizacija privalo gebėti įrodyti sutikimo davimo faktą, jo turinį, pateiktą informaciją, davimo datą ir, kai taikoma, sutikimo atšaukimą.

22. Prieš gaunant sutikimą pateikiama informacija apie duomenų valdytoją, tikslus, duomenis, gavėjus ar viešinimo kanalus, saugojimo laikotarpį, teisę bet kada atšaukti sutikimą ir tai, kad atšaukimas neturi įtakos iki jo atlikto tvarkymo teisėtumui.

23. Sutikimas registruojamas ir saugomas visą sutikimu pagrįsto tvarkymo laikotarpį bei tiek, kiek būtina sutikimo faktui ir tvarkymo teisėtumui pagrįsti. Atšaukus sutikimą, tvarkymas atitinkamu tikslu nutraukiamas, išskyrus atvejus, kai taikomas kitas teisinis pagrindas.

24. Renginių ir veiklų fotografavimas ar filmavimas nėra laikomas nuolatiniu vaizdo stebėjimu. Prieš renginį dalyviai aiškiai informuojami apie fotografavimą ar filmavimą, tikslus, numatomus viešinimo kanalus ir galimybę pranešti, kad asmuo nenori būti fotografuojamas ar filmuojamas, kai tokia galimybė taikoma.

25. Atpažįstamo asmens portretinio atvaizdo naudojimas viešinimo tikslais paprastai grindžiamas atskiru sutikimu. Bendro pobūdžio renginio vaizdai gali būti tvarkomi kitu tinkamu teisiniu pagrindu tik atlikus konkrečių aplinkybių, pagrįstų lūkesčių, viešinimo apimties ir galimo poveikio asmeniui vertinimą.

26. Nepilnamečių ir socialiai pažeidžiamų asmenų atvaizdai viešinami ypač atsargiai. Negali būti skelbiama informacija, iš kurios be būtinybės būtų galima nustatyti sveikatos būklę, negalią, socialinę situaciją, gyvenamąją vietą ar kitas jautrias aplinkybes.

27. Mokymų, nuotolinių susitikimų ar individualių konsultacijų įrašymas leidžiamas tik iš anksto nustačius būtinumą, teisinį pagrindą, informavimo tvarką, prieigos ratą ir saugojimo

terminą. Individualios konsultacijos neįrašomos, jeigu nėra atskiro dokumentuoto sprendimo ir tinkamo teisinio pagrindo.

V SKYRIUS
DUOMENŲ SUBJEKTŲ INFORMAVIMAS

28. Duomenų subjektams BDAR 13 arba 14 straipsnyje nustatyta informacija pateikiama glaustai, skaidriai, suprantamai ir lengvai prieinama forma, aiškia bei paprasta kalba. Nepilnamečiams skirta informacija pritaikoma jų amžiui ir gebėjimui suprasti.

29. Organizacija, atsižvelgdama į duomenų subjektų grupę ir veiklą, naudoja atskirus arba kombinuotus privatumo pranešimus darbuotojams, kandidatams, savanoriams, praktikantams, paslaugų teikėjams, jaunuoliams ir jų atstovams, konsultacijų ir apgyvendinimo paslaugų gavėjams, mokymų bei renginių dalyviams.

30. Kai duomenys gaunami ne iš paties asmens, privatumo pranešime nurodomos duomenų kategorijos ir jų šaltinis. Informacija pateikiama BDAR nustatytu laiku, atsižvelgiant į pirmą komunikaciją ar duomenų atskleidimą gavėjui.

VI SKYRIUS
DUOMENŲ SUBJEKTŲ TEISĖS IR JŲ ĮGYVENDINIMAS

31. Duomenų subjektas turi teisę gauti informaciją apie duomenų tvarkymą, susipažinti su duomenimis, prašyti juos ištaisyti ar ištrinti, apriboti tvarkymą, nesutikti su tvarkymu, gauti duomenis perkeliamu formatu, kai taikoma, atšaukti sutikimą ir nebūti vien automatizuotu tvarkymu grindžiamo sprendimo subjektu.

32. Prašymas gali būti pateiktas Organizacijos viešai skelbiamu elektroninio pašto adresu, paštu, asmeniškai arba kitu Organizacijos nurodytu būdu. Prašyme turi būti aiškiai nurodyta prašoma įgyvendinti teisė ir informacija, leidžianti nustatyti su prašymu susijusius duomenis.

33. Jeigu kyla pagrįstų abejonių dėl prašymą pateikusio asmens tapatybės, Organizacija gali paprašyti pateikti papildomą informaciją, būtiną tapatybei patvirtinti. Negali būti reikalaujama daugiau duomenų, negu būtina tapatybei patikrinti.

34. Gautas prašymas nedelsiant užregistruojamas Duomenų subjektų prašymų registre. Direktorė arba jos paskirtas asmuo koordinuoja prašymo nagrinėjimą, surenka informaciją iš atsakingų padalinių ir užtikrina atsakymo pateikimą.

35. Informacija apie veiksmus, kurių imtasi gavus prašymą, pateikiama nepagrįstai nedelsiant ir ne vėliau kaip per vieną mėnesį nuo prašymo gavimo. Atsižvelgiant į prašymų sudėtingumą ir skaičių, terminas gali būti pratęstas dar dviem mėnesiams, apie pratęsimą ir jo priežastis informuojant per pirmąjį mėnesį.

36. Jeigu veiksmų pagal prašymą nesiimama, duomenų subjektui ne vėliau kaip per vieną mėnesį nurodomos priežastys ir teisė pateikti skundą Valstybinei duomenų apsaugos inspekcijai bei kreiptis į teismą.

37. Prašymai vykdomi neatlygintinai. Kai prašymai yra akivaizdžiai nepagrįsti arba neproporcingi, ypač dėl pasikartojimo, Organizacija gali imti pagrįstą mokestį arba atsisakyti imtis veiksmų, tačiau privalo įrodyti prašymo nepagrįstumą ar neproporcingumą.

38. Prieš pateikiant kopijas ar atskleidžiant informaciją, pašalinami kitų asmenų duomenys ir saugoma komercinė, profesinė, socialinio darbo ar kita teisės saugoma paslaptis, kiek tai būtina kitų asmenų teisėms ir laisvėms apsaugoti.

39. Kai prašymas susijęs su nepilnamečiu, vertinama jo amžius, brandumas, atstovavimo pagrindas ir geriausi interesai. Informacija atstovui neteikiama automatiškai, jeigu jos atskleidimas galėtų pažeisti nepilnamečio teises, saugumą ar teisėtus interesus.

VII SKYRIUS
DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI IR SAUGOJIMO TERMINAI

40. Organizacija tvarko ir reguliariai atnaujina duomenų tvarkymo veiklos įrašus. Nauja ar pakeista veikla negali būti vykdoma, kol neįvertinti ir veiklos įrašuose neužfiksuoti esminiai jos elementai.

40.1. Veiklos įrašai tvarkomi raštu, įskaitant elektroninę formą, turi būti tikslūs, aktualūs ir atspindėti faktinę Organizacijos veiklą.

40.2. Darbuotojai prieš pradėdami naują veiklą ar pakeisdami esamą duomenų tvarkymą informuoja už veiklos įrašus atsakingą asmenį ir pateikia informaciją apie tikslą, duomenis, subjektus, gavėjus, sistemas, saugojimo terminą ir saugumo priemones.

40.3. Veiklos įrašai peržiūrimi periodiškai ir kiekvieną kartą pasikeitus tvarkymo tikslui, duomenų apimčiai, teisiniam pagrindui, sistemai, gavėjui, saugojimo terminui ar perdavimui į trečiąją valstybę.

40.4. Valstybinei duomenų apsaugos inspekcijai paprašius, veiklos įrašai pateikiami jos nustatytu terminu.

41. Asmens duomenys saugomi Organizacijos patvirtintoje saugojimo terminų rodyklėje, veiklos įrašuose, teisės aktuose, projektų ar finansavimo dokumentuose nustatytą laiką. Kai taikomi keli terminai, dokumentuojama, kuris terminas ir dėl kokios priežasties taikomas.

42. Pasibaigus terminui, duomenys saugiai sunaikinami, ištrinami arba negrįžtamai nuasmeninami. Popieriniai dokumentai sunaikinami taip, kad informacijos nebūtų galima atkurti, o elektroniniai duomenys ištrinami iš aktyvių sistemų ir pagal nustatytą ciklą – iš atsarginių kopijų.

43. Duomenų saugojimas gali būti laikinai sustabdytas, kai jie būtini pareikšti, vykdyti ar apginti teisinius reikalavimus, atlikti tyrimą arba vykdyti kompetentingos institucijos nurodymą. Sustabdymo priežastis, apimtis ir peržiūros data dokumentuojamos.

VIII SKYRIUS
DUOMENŲ GAVĖJAI TVARKYTOJAI IR TARPTAUTINIAI PERDAVIMAI

44. Duomenys gavėjams teikiami tik esant teisėtam pagrindui, tik nustatytu tikslu ir tik būtina apimtimi. Prieš teikiant jautrius duomenis patikrinamas gavėjas, perdavimo pagrindas ir naudojamas saugus perdavimo būdas.

45. Organizacija gali teikti duomenis finansuotojams, projektus administruojančioms institucijoms, savivaldybėms, ministerijoms, Jaunimo reikalų agentūrai, socialinėms ir vaiko teisių apsaugos institucijoms, mokymo įstaigoms, teisėsaugos ir kitoms institucijoms, jeigu toks teikimas pagrįstas teisės aktu, sutartimi, viešojo intereso užduotimi ar kitu teisėtu pagrindu.

46. Duomenų tvarkytojas pasitelkiamas tik sudarius BDAR 28 straipsnio reikalavimus atitinkančią sutartį ar kitą teisės aktą. Prieš pasitelkiant tvarkytoją įvertinamos jo saugumo priemonės, subtvarkytojai, duomenų saugojimo vieta, incidentų valdymas ir duomenų grąžinimo ar ištrynimo sąlygos.

47. Duomenų tvarkytojai, savarankiški gavėjai ir, kai taikoma, bendri duomenų valdytojai registruojami Organizacijos tvarkytojų ir gavėjų registre.

48. Duomenys į trečiąją valstybę ar tarptautinei organizacijai perduodami tik laikantis BDAR V skyriaus. Prieš naudojant debesijos, vaizdo konferencijų, socialinių tinklų ar kitas paslaugas įvertinamos faktinės duomenų saugojimo vietos, perdavimo mechanizmas ir papildomos apsaugos priemonės.

IX SKYRIUS
TECHNINĖS IR ORGANIZACINĖS SAUGUMO PRIEMONĖS

49. Organizacija, atsižvelgdama į duomenų pobūdį, apimtį, kontekstą, tikslus, technologijų išsivystymą, įgyvendinimo sąnaudas ir riziką asmenų teisėms, taiko tinkamas technines ir organizacines priemones.

50. Prieigos suteikiamos pagal funkcijų būtinybę ir mažiausių teisių principą. Naudojamos individualios paskyros; bendros paskyros leidžiamos tik išimtiniais dokumentuotais atvejais. Prieigos periodiškai peržiūrimos ir nedelsiant panaikinamos pasikeitus funkcijoms ar pasibaigus santykiams.

51. Paskyros turi būti apsaugomos stipriais unikaliais slaptažodžiais. Kelių veiksnių autentifikavimas turi būti naudojamas el. pašto, debesijos, nuotolinės prieigos ir kitose sistemose, kuriose tai techniškai įmanoma ir proporcinga rizikai.

52. Darbo įrenginiai turi būti apsaugoti ekrano užraktu, atnaujinama operacine sistema, antivirusinėmis ar kitomis apsaugos priemonėmis. Naudotojai negali savavališkai išjungti apsaugos, diegti nepatvirtintos programinės įrangos ar perduoti įrenginio kitam asmeniui.

53. Jautrūs duomenys perduodami šifruotu ar kitu saugiu kanalu. Asmens kodai, sveikatos, negalios, socialinių atvejų ir apgyvendinimo duomenys nesiunčiami atviru el. paštu, jeigu nėra papildomos apsaugos arba kito dokumentuoto saugaus sprendimo.

54. Popieriniai dokumentai saugomi rakinamose spintose ar patalpose. Laikomasi švaraus stalo ir švaraus ekrano principų; dokumentai nepaliekami spausdintuvuose, automobiliuose ar viešai prieinamose vietose.

55. Svarbių duomenų atsarginės kopijos turi būti daromos atsižvelgiant į veiklos tęstinumo poreikį, o jų atkūrimo galimybė periodiškai tikrinama. Atsarginėms kopijoms taikoma prieigos kontrolė ir apsauga nuo neteisėto pakeitimo ar sunaikinimo.

56. Organizacija turi užtikrinti darbuotojų mokymą, techninės įrangos priežiūrą, programinės įrangos atnaujinimus, prieigų valdymą ir periodinę saugumo priemonių tinkamumo peržiūrą. Priemonių faktinis įgyvendinimas ir už jas atsakingi asmenys fiksuojami Taisyklių 4 priede arba kituose Organizacijos dokumentuose.

X SKYRIUS
MOBILIEJI ĮRENGINIAI, EL. PAŠTAS, DEBESIJA IR SUSIRAŠINĖJIMO PROGRAMĖLĖS

57. Darbo duomenys tvarkomi Organizacijos suteiktomis arba aiškiai patvirtintomis paskyromis, sistemomis ir įrenginiais. Asmeninės el. pašto paskyros, asmeninės debesų saugyklos ir nepatvirtintos programėlės darbo dokumentams nenaudojamos.

58. Jeigu leidžiama naudoti asmeninį įrenginį, jis turi būti apsaugotas PIN kodu ar slaptažodžiu, automatiniu ekrano užraktu, atnaujinimais ir, kai įmanoma, šifravimu. Organizacija turi teisę reikalauti pašalinti darbo duomenis pasibaigus funkcijoms, praradus įrenginį ar kilus saugumo rizikai.

59. El. paštu siunčiant asmens duomenis patikrinami gavėjai, priedai ir adresų laukai. Siunčiant keliems tarpusavyje nesusijusiems išoriniams gavėjams naudojamas BCC laukas arba individualūs laiškai, išskyrus atvejus, kai gavėjų atskleidimas būtinas ir teisėtas.

60. Nuorodos į debesijos dokumentus suteikiamos konkretiems naudotojams, o ne neribotam ratui, kai dokumentuose yra asmens duomenų. Viešos nuorodos naudojamos tik įvertinus, kad jose nėra neviešų duomenų.

61. Bendraujant su jaunuoliais per „Messenger“, „WhatsApp“, „Signal“, SMS ar kitus kanalus teikiama tik tiek informacijos, kiek būtina operatyviai komunikacijai. Sveikatos, negalios, socialinių atvejų, konsultacijų ir pagalbos planų išsami informacija tokiuose kanaluose netvarkoma, išskyrus dokumentuotą skubų atvejį ir naudojant saugiausią prieinamą kanalą.

62. Darbuotojas ir mentorius darbo susirašinėjimų be būtinybės nekopijuoja į asmenines paskyras, nedaro ekrano nuotraukų ir nepalieka duomenų programėlėse ilgiau, negu reikia komunikacijos tikslui. Esminė informacija perkeliama į patvirtintą sistemą, o iš programėlės pašalinama pagal nustatytą terminą.

63. Praradus telefoną, kompiuterį ar laikmeną, pastebėjus neteisėtą prisijungimą arba išsiuntus duomenis netinkamam gavėjui, apie tai pranešama nedelsiant, nelaukiant darbo dienos pabaigos.

64. Organizacijos įrenginių asmeninis naudojimas galimas tik tiek, kiek tai netrukdo darbui, nekelia saugumo rizikos ir neprieštarauja vidaus taisyklėms. Darbuotojai informuojami apie galimą proporcingą ir teisėtą darbo priemonių patikrinimą; nuolatinė darbuotojų komunikacijos kontrolė nevykdoma.

64.1. Naudotojams draudžiama skelbti ar perduoti Organizacijos neviešus dokumentus ir asmens duomenis, jeigu tai nesusiję su pavestomis funkcijomis arba nėra tinkamo teisinio pagrindo.

64.2. Draudžiama savavališkai keisti įrenginių ar programinės įrangos saugumo nustatymus, išjungti apsaugos priemones, diegti nepatvirtintą programinę įrangą ar prijungti nepatikrintas laikmenas.

64.3. Draudžiama perduoti darbo įrenginius, paskyras, prisijungimo duomenis ar autentifikavimo priemones kitiems asmenims. Slaptažodžiai negali būti siunčiami kartu su jais apsaugotu dokumentu tuo pačiu kanalu.

64.4. Draudžiama naudoti Organizacijos sistemas neteisėtai prieigai, saugumo patikroms, tinklo srautui stebėti ar kitiems veiksmams, jeigu tai nėra tiesiogiai pavesta įgaliotam specialistui.

64.5. Pastebėjus įtartiną laišką, nuorodą, failą ar neįprastą sistemos veikimą, naudotojas neatlieka papildomų veiksmų, išsaugo reikšmingą informaciją ir nedelsdamas kreipiasi į atsakingą asmenį.

XI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

65. Asmens duomenų saugumo pažeidimu laikomas saugumo pažeidimas, dėl kurio netyčia ar neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami perduodami, saugomi ar kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.

66. Apie galimą pažeidimą darbuotojas ar kitas prieigą turintis asmuo nedelsdamas praneša direktorei ar jos paskirtam atsakingam asmeniui ir, jei saugu, imasi veiksmų žalai sustabdyti: atšaukia laišką, kreipiasi į netinkamą gavėją, pakeičia slaptažodį, atjungia įrenginį arba išsaugo tyrimui reikalingą informaciją.

67. Gavus pranešimą, nedelsiant registruojamas įvykis, nustatomas jo laikas, pobūdis, paveikti duomenys ir asmenys, gavėjai, sistemos, galimos pasekmės, taikytos suvaldymo priemonės ir atsakingi asmenys.

68. Direktorė arba jos paskirta grupė įvertina tikimybę ir poveikio sunkumą, atsižvelgdama į duomenų jautrumą, mastą, asmenų pažeidžiamumą, identifikavimo galimybę, konfidencialumo, vientisumo ar prieinamumo praradimą ir realias neigiamas pasekmes.

68.1. Rizikos vertinimas, sprendimas pranešti arba nepranešti Inspekcijai ir duomenų subjektams, sprendimo motyvai bei sužinojimo apie pažeidimą laikas dokumentuojami.

68.2. Duomenų tvarkytojas, sužinojęs apie Organizacijos vardu tvarkomų duomenų pažeidimą, privalo pranešti Organizacijai be nepagrįsto delsimo ir pateikti visą tyrimui bei pranešimui būtiną informaciją.

69. Jeigu pažeidimas gali kelti pavojų fizinių asmenų teisėms ir laisvėms, apie jį nepagrįstai nedelsiant ir, jei įmanoma, ne vėliau kaip per 72 valandas nuo sužinojimo pranešama Valstybinei duomenų apsaugos inspekcijai. Vėluojant nurodomos vėlavimo priežastys. Informacija gali būti teikiama etapais.

70. Jeigu pažeidimas gali kelti didelį pavojų asmenų teisėms ir laisvėms, duomenų subjektai informuojami nepagrįstai nedelsiant, aiškia ir paprasta kalba, išskyrus BDAR 34 straipsnio 3 dalyje nustatytas išimtis.

71. Visi pažeidimai, įskaitant tuos, apie kuriuos nepranešta Inspekcijai ar duomenų subjektams, dokumentuojami Asmens duomenų saugumo pažeidimų registre, nurodant sprendimo nepranešti motyvus.

72. Po pažeidimo nustatomos korekcinės priemonės, atsakingi asmenys ir terminai; įvertinama, ar reikia pakeisti prieigas, procedūras, sistemas, sutartis, mokymus ar atlikti rizikos vertinimą.

XII SKYRIUS
DARBUOTOJŲ IR KANDIDATŲ DUOMENŲ TVARKYMO YPATUMAI

73. Darbuotojų duomenys tvarkomi darbo sutarties sudarymo ir vykdymo, teisinių prievolių, Organizacijos ar trečiųjų asmenų teisėtų interesų ir kitais taikytinais pagrindais. Sutikimas nenaudojamas duomenims, kuriuos būtina tvarkyti darbo santykiams administruoti.

74. Kandidatų duomenys renkami tik tiek, kiek būtina atrankai. Informacija iš buvusio darbdavio renkama prieš tai informavus kandidatą, o iš esamo darbdavio – tik gavus kandidato sutikimą, kaip nustato teisės aktai.

75. Viešai prieinama informacija apie kandidatą ar darbuotoją renkama tik tada, kai ji tiesiogiai susijusi su profesinėmis funkcijomis ir būtina teisėtam tikslui. Draudžiama sistemingai tikrinti asmenines socialinių tinklų paskyras ar rinkti su pareigomis nesusijusią informaciją.

76. Neatrinktų kandidatų duomenys saugomi saugojimo terminų rodyklėje nustatytą laiką. Ilgesniam saugojimui būsimoms atrankoms gaunamas atskiras sutikimas.

77. Organizacijos suteiktos darbo priemonės, paskyros ar jose esanti su darbu susijusi informacija gali būti tikrinama tik esant konkrečiam teisėtam tikslui ir kai šio tikslo negalima pasiekti mažiau darbuotojo privatumą ribojančiomis priemonėmis. Nuolatinė ar slapta darbuotojų komunikacijos kontrolė nevykdoma.

77.1. Darbuotojas iš anksto informuojamas apie galimą darbo priemonių tikrinimą, jo tikslus, apimtį ir taikomas garantijas, išskyrus išimtinius teisės aktuose nustatytus atvejus.

77.2. Patikrinimas galimas, kai yra objektyvių duomenų apie galimą teisės aktų, darbo pareigų, konfidencialumo ar informacijos saugumo reikalavimų pažeidimą, būtina užtikrinti veiklos tęstinumą arba apsaugoti Organizacijos ar kitų asmenų teises.

77.3. Prieš patikrinimą nustatomas konkretus tikrinamas laikotarpis, paskyra, įrenginys, projektas, dokumentas ar aplinkybė. Tikrinama tik tokia apimtimi, kiek būtina nustatytam tikslui pasiekti.

77.4. Patikrinimą atlieka direktorės įgalioti asmenys. Sprendimas, pagrindas, apimtis, atlikti veiksmai ir rezultatai dokumentuojami, o nesusijusi asmeninė informacija nevertinama ir nekopijuojama.

77.5. Nustačius, kad darbo priemonėje yra asmeninės informacijos, ji tvarkoma tik tiek, kiek neišvengiamai būtina patikrinimo tikslui, ir apsaugoma nuo nepagrįsto atskleidimo.

78. Organizacija nevykdo nuolatinio vaizdo stebėjimo darbo vietose. Nusprendus ateityje pradėti vaizdo stebėjimą, prieš tai atliekamas būtinybės ir proporcingumo vertinimas, nustatomas teisinis pagrindas, patvirtinamos atskiros sąlygos ir tinkamai informuojami duomenų subjektai.

XIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

79. Su Taisyklėmis supažindinami visi asmenys, kuriems jos taikomos. Supažindinimas gali būti patvirtinamas parašu arba elektroninėmis priemonėmis. Visiems darbuotojams, savanoriams, praktikantams ir kitiems prieigą turintiems asmenims išduodama ir supažindinimui pateikiama Asmens duomenų saugos atmintinė (Taisyklių 5 priedas).

80. Taisyklių laikymasis peržiūrimas periodiškai ir pasikeitus teisės aktams, veikloms, naudojamoms sistemoms, duomenų kategorijoms, gavėjams arba įvykus reikšmingam saugumo pažeidimui.

81. Taisyklių pažeidimai nagrinėjami teisės aktų ir Organizacijos vidaus dokumentų nustatyta tvarka. Taisyklių pažeidimas gali lemti drausminę, civilinę, administracinę ar baudžiamąją atsakomybę.

82. Taisyklės įsigalioja jų patvirtinimo dieną, jeigu įsakyme nenustatyta kitaip.