

## PANEVĖŽIO MIESTO SAVIVALDYBĖS ADMINISTRACIJOS ASMENS DUOMENŲ TVARKYMO TAIŠYKLĖS

### I SKYRIUS BENDROSIOS NUOSTATOS

1. Asmens duomenų tvarkymo Panevėžio miesto savivaldybės administracijos taisyklių (toliau – Taisyklės) tikslas – reglamentuoti asmens duomenų tvarkymą Panevėžio miesto savivaldybės administracijoje (toliau – Administracija), nustatyti pagrindines asmens duomenų tvarkymo, duomenų subjekto teisių įgyvendinimo, duomenų apsaugos technines ir organizacines priemones ir kitas procedūras, siekiant užtikrinti Europos Parlamento ir Tarybos reglamento (ES) 2016 m. balandžio 27 d. 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (toliau – ADTAI) ir kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir apsaugą, laikymąsi ir įgyvendinimą.

2. Asmens duomenų valdytoja ir tvarkytoja – Panevėžio miesto savivaldybės administracija, juridinio asmens kodas 288724610, buveinės adresas: Laisvės a. 20, 35200 Panevėžys. Administracijos duomenų tvarkytojais gali būti ir kiti fiziniai ir juridiniai asmenys, kuriems šių duomenų tvarkymas pavedamas duomenų tvarkymo sutartimi ar kitu dokumentu ir kurių sąrašas gali būti skelbiamas Panevėžio miesto savivaldybės interneto svetainėje [www.panevezys.lt](http://www.panevezys.lt).

3. Šių Taisyklių privalo laikytis visi Administracijoje dirbantys darbuotojai ir kiti asmenys, kurie tvarko Administracijoje esančius asmens duomenis arba eidami savo pareigas juos sužino.

4. Pasikeitus Taisyklėse minimų teisės aktų nuostatoms, taikomos aktualios tų teisės aktų redakcijos nuostatos.

### II SKYRIUS PAGRINDINĖS SĄVOKOS

5. Šiose Taisyklėse vartojamos sąvokos:

5.1. **asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima tiesiogiai arba netiesiogiai nustatyti visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens kodą, buvimo vietos duomenis ir interneto identifikatorių, arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius;

5.2. **darbuotojai** – Administracijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo ar kitas sutartis;

5.3. **duomenų gavėjas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuriai atskleidžiami asmens duomenys, nesvarbu, ar tai trečioji šalis, ar ne;

5.4. **duomenų subjektas** – darbuotojai, interesantai ir kiti fiziniai asmenys, kurių duomenis tvarko Administracija;

5.5. **duomenų teikimas** – asmens duomenų atskleidimas perduodant ar kitu būdu padarant juos prieinamus (išskyrus paskelbimą visuomenės informavimo priemonėse);

5.6. **duomenų tvarkymas** – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų

seka, kaip antai: rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimasis arba sunaikinimas;

5.7. **duomenų tvarkytojas** – subjektai, kurie tvarko Panevėžio miesto savivaldybės administracijos valdomus asmens duomenis pagal Panevėžio miesto savivaldybės administracijos nurodymus ir vadovaujasi sudarytomis paslaugų sutartimis, ir kiti subjektai, turintys prieigą prie Administracijos duomenų;

5.8. **duomenų valdytojas** – Panevėžio miesto savivaldybės administracija, kuri tvarkydama interesantų, darbuotojų, kitų fizinių asmenų duomenis nustato tų duomenų naudojimo būdus, priemones ir tikslus;

5.9. **vidaus administravimas** – veikla, kuria užtikrinamas duomenų valdytojo savarankiškas funkcionavimas (struktūros tvarkymas, personalo valdymas, finansinių išteklių valdymas ir naudojimas, raštvedybos tvarkymas).

6. Kitos Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos BDAR.

### III SKYRIUS

#### ASMENS DUOMENŲ TVARKYMAS, SAUGOJIMAS IR DUOMENŲ TVARKYMO PRINCIPAI

7. Asmens duomenys Administracijoje tvarkomi automatinio ir neautomatinio būdu.

8. Prieiga prie asmens duomenų gali būti suteikiama tik tiems Administracijos darbuotojams ir asmenims, kuriems asmens duomenys yra reikalingi jų pareigybės aprašymuose nustatytoms funkcijoms vykdyti ir kurie yra pasirašę Įsipareigojimą saugoti asmens duomenų paslaptį (Taisyklių 1 priedas), kuris saugomas darbuotojų asmens bylose. Su asmens duomenimis galima atlikti tik tuos veiksmus, kuriuos atlikti Administracijos darbuotojams yra suteiktos teisės.

9. Dokumentai, kuriuose yra asmens duomenys, tvarkomi, įtraukiami į apskaitą, viešinami ir saugomi vadovaujantis Dokumentų tvarkymo ir apskaitos taisyklių, patvirtintų Lietuvos vyriausiojo archyvaro 2011 m. liepos 4 d. įsakymu Nr. V-118 „Dėl Dokumentų tvarkymo ir apskaitos taisyklių patvirtinimo“, Elektroninių dokumentų valdymo taisyklių, patvirtintų Lietuvos vyriausiojo archyvaro 2011 m. gruodžio 29 d. įsakymu Nr. V-158 „Dėl Elektroninių dokumentų valdymo taisyklių patvirtinimo“, reikalavimais ir Lietuvos vyriausiojo archyvaro tarnybos parengtomis Vaizdo ir garso dokumentų išsaugojimo rekomendacijomis.

10. Administracijoje tvarkomų asmens duomenų baigtinis sąrašas ir tikslai detalizuojami Administracijos asmens duomenų tvarkymo veiklos įrašuose, kurie gali būti skelbiami [www.panevezys.lt](http://www.panevezys.lt) ir (ar) kituose Administracijos dokumentuose.

11. Darbuotojai, atlikdami savo pareigas ir tvarkydami asmens duomenis, privalo:

11.1. asmens duomenis tvarkyti teisėtai, sąžiningai ir skaidriai;

11.2. asmens duomenis rinkti šių Taisyklių 2 priede apibrėžtais tikslais ir tvarkyti su šiais tikslais suderintais būdais;

11.3. rinkdami ir tvarkydami asmens duomenis laikytis tikslingumo, proporcingumo ir duomenų kiekio mažinimo principų, t. y. nereikalauti iš interesantų pateikti tų duomenų, kurie nėra būtini Administracijos funkcijoms vykdyti, nekaupiti ir netvarkyti perteklinių duomenų ir duomenų, kurie nėra būtini atitinkamiems tikslams pasiekti;

11.4. užtikrinti asmens duomenų tikslumą ir, jei reikia dėl asmens duomenų tvarkymo, juos atnaujinti; netikslus ar neišsamius duomenis ištaisyti, papildyti, sunaikinti arba jų tvarkymą sustabdyti;

11.5. asmens duomenis saugoti teisės aktų ir šių Taisyklių nustatyta tvarka;

11.6. asmens duomenis tvarkyti tokiu būdu, kad taikant atitinkamas fizines, technines ir organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas).

12. Asmens duomenų saugojimo terminus ir veiksmus, kurie atliekami pasibaigus šiam terminui, nustato teisės aktai, reglamentuojantys duomenų tvarkymą ir dokumentų saugojimą. Asmens duomenys saugomi ne ilgiau, negu to reikalauja teisės aktai ir duomenų tvarkymo tikslai. Konkretūs dokumentų (duomenų) saugojimo terminai gali būti nustatyti Administracijos direktoriaus patvirtintame dokumentacijos plane.

13. Kai asmens duomenys nebereikalingi jų tvarkymo tikslams įgyvendinti, jie yra perduodami į Administracijos archyvą arba valstybės archyvą arba sunaikinami:

13.1. Sunaikinimas apibrėžiamas kaip fizinis ar techninis veiksmas, kuriuo dokumente esantys duomenys padaromi neatkuriamais įprastinėmis komerciškai prieinamomis priemonėmis;

13.2. Elektronine forma saugomi asmens duomenys sunaikinami juos ištrinant be galimybės atkurti;

13.3. Naikinant dokumentus, kurių saugojimo terminas yra pasibaigęs, dokumentai, kuriuose nurodomi asmens duomenys, ir jų kopijos turi būti sunaikinti taip, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio.

14. Už kiekvienos naujos paslaugos, produkto ar kitokios veiklos vystymą atsakingas darbuotojas apie planuojamus pokyčius, kurie gali turėti įtakos asmens duomenų apsaugai, informuoja už asmens duomenų apsaugą atsakingą asmenį ir suteikia jam informaciją, reikalingą tinkamam įvertinimui atlikti ir duomenų apsaugos reikalavimams įgyvendinti:

14.1. Nauja paslauga ar produktas, kurie susiję su asmens duomenimis, nėra pradedami teikti tol, kol nėra įvertinta jų atitiktis BDAR reikalavimams arba, kai to reikia, nėra atliktas poveikio duomenų apsaugai vertinimas.

15. Darbuotojų asmens duomenis turi teisę tvarkyti tik tie asmenys, kuriems jie yra būtini funkcijoms vykdyti, ir tik tuomet, kai tai yra būtina atitinkamiems tikslams pasiekti:

15.1. darbuotojai apie jų asmens duomenų tvarkymą informuojami raštu jiems pateikiant nustatytą formą (Taisyklių 3, 4 priedai). Užpildytos formos yra saugomos darbuotojų asmens bylose.

16. Darbuotojų, kaip duomenų subjektų, teisės Administracijoje įgyvendinamos vadovaujantis BDAR ir Taisyklių IV skyriuje nustatyta tvarka.

#### **IV SKYRIUS DUOMENŲ SUBJEKTŲ TEISĖS IR JŲ ĮGYVENDINIMO TVARKA**

17. Duomenų subjektas, kurio duomenis tvarko Administracija, turi šias teises, įtvirtintas BDAR:

17.1. teisę žinoti (būti informuotam) apie savo asmens duomenų tvarkymą:

17.1.1. duomenų subjektų informavimas, kad Administracijos teikiamos žodinės konsultacijos telefonu bus įrašomos;

17.1.2. vartotojų, pirmą kartą besijungiančių prie Administracijos elektroninių paslaugų valdymo sistemos (EPVS), informavimas apie asmens duomenų tvarkymą;

17.1.3. apie asmens duomenų tvarkymą subjektai informuojami raštu (Taisyklių 9 priedas), elektronine forma (subjektai informuojami jiems pateikiant nuorodą į Taisyklių 9 priedą). Ši informacija viešai skelbiama Administracijos interneto svetainėje [www.panevezys.lt](http://www.panevezys.lt). Duomenų subjekto prašymu informacija gali būti suteikta žodžiu, tačiau visais atvejais apie konkretų asmenį renkama informacija pateikiama tik duomenų subjektui įrodžius savo tapatybę;

17.2. teisę susipažinti su tvarkomais savo asmens duomenimis ir gauti informaciją apie asmens duomenų tvarkymo tikslus, duomenų gavėjus arba jų kategorijas, numatomą asmens duomenų saugojimo laikotarpį, asmens duomenų šaltinius;

17.3. teisę reikalauti ištaisyti savo asmens duomenis, jei, jo nuomone, tvarkomi netikslūs ir neišsamūs jo asmens duomenys;

17.4. teisę reikalauti ištrinti savo asmens duomenis („teisė būti pamirštam“) šiais atvejais:

17.4.1. asmens duomenys nebėra reikalingi tikslams, kurie buvo nustatyti;

17.4.2. duomenų subjektas atšaukia sutikimą ir nėra jokio kito teisinio pagrindo tvarkyti duomenų subjekto asmens duomenis;

17.4.3. asmens duomenys buvo tvarkomi neteisėtai;

17.5. teisę apriboti savo asmens duomenų tvarkymą, jeigu yra vienas iš šių pagrindų:

17.5.1. duomenų subjektas užginčija Administracijoje tvarkomų jo asmens duomenų tikslumą. Tokiu atveju duomenų subjekto asmens duomenų tvarkymas gali būti apribotas tokiam laikotarpiui, per kurį duomenų valdytojas patikrina asmens duomenų tikslumą;

17.5.2. nustatoma, kad duomenų subjekto asmens duomenų tvarkymas buvo neteisėtas ir duomenų subjektas nesutinka, kad asmens duomenys būtų ištrinti, vietoje to duomenų subjektas prašo apriboti jų tvarkymą;

17.5.3. Administracijai nebereikia surinktų asmens duomenų nustatytiems tvarkymo tikslams, tačiau jų reikia duomenų subjektui, siekiančiam pareikšti, vykdyti ar apginti teisinius reikalavimus;

17.5.4. duomenų subjektas pateikė prašymą, kuriame išreiškė nesutikimą, kad Administracija tvarkytų jo asmens duomenis. Tokiu atveju duomenų subjekto asmens duomenų tvarkymas gali būti apribotas tokiam laikotarpiui, per kurį duomenų valdytojas patikrina, ar duomenų subjekto prašymas yra pagrįstas;

17.5.5. duomenų subjektas pateikia prašymą ištrinti jo tvarkomus asmens duomenis ir nustatoma, kad prašymas yra pagrįstas, tačiau nėra techninių galimybių nedelsiant ištrinti jo asmens duomenis. Tokiu atveju asmens duomenų tvarkymas gali būti apribotas iki tol, kol duomenų subjekto asmens duomenys bus ištrinti;

17.6. teisę į duomenų perkeliamumą, t. y. gauti su juo susijusius asmens duomenis ir prašyti persiųsti tvarkomus jo asmens duomenis kitam duomenų valdytojui;

17.7. teisę nesutikti su savo asmens duomenų tvarkymu;

17.8. teisę reikalauti, kad nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas.

18. Teisė reikalauti ištrinti asmens duomenis („teisė būti pamirštam“) Administracijoje neįgyvendinama, kai asmens duomenų tvarkymas yra grindžiamas įstatymuose ir kituose teisės aktuose nustatytų reikalavimų vykdymu ir archyvavimo tikslais viešojo intereso labui.

19. Duomenų subjekto prašymu apribojus asmens duomenų tvarkymo veiksmus, asmens duomenis galima tvarkyti, išskyrus saugojimą, tik gavus duomenų subjekto sutikimą arba siekiant pareikšti, vykdyti, apginti teisinius reikalavimus, siekiant apsaugoti kito fizinio ar juridinio asmens teises arba dėl svarbių viešojo intereso priežasčių.

20. Kai yra priimamas sprendimas panaikinti apribojimą tvarkyti duomenų subjekto asmens duomenis, Administracija, prieš panaikindama apribojimą, privalo raštu informuoti duomenų subjektą.

21. Asmens duomenys gali būti pateikti duomenų subjektui arba kitam duomenų valdytojui, jei duomenų subjektas prašyme nurodo, kad Administracija asmens duomenis turėtų persiųsti kitam duomenų valdytojui ir jeigu yra techninės galimybės pateikti asmens duomenis tiesiogiai kitam duomenų valdytojui.

22. Administracija nevertina, ar duomenų valdytojas, kuriam Taisyklių 21 punkte numatyta tvarka bus persiųsti duomenų subjekto asmens duomenys, turi teisinį pagrindą gauti duomenų subjekto asmens duomenis ir ar šis duomenų valdytojas užtikrins tinkamas asmens duomenų saugumo priemones. Administracija nepriima atsakomybės už persiųstų asmens duomenų tolimesnį tvarkymą, kurį atliks kitas duomenų valdytojas.

23. Jeigu yra nustatoma, kad duomenų subjekto prašymas dėl nesutikimo su savo asmens duomenų tvarkymu yra nepagrįstas, Administracija privalo atsakyme argumentuotai įrodyti, kad duomenų subjekto asmens duomenys yra tvarkomi dėl pagrįstų ir teisėtų priežasčių, kurios yra viršesnės už duomenų subjekto interesus.

24. Duomenų subjektai, siekdami įgyvendinti savo teises, numatytas Taisyklių 17.1–17.8 papunkčiuose, turi Administracijai asmeniškai, paštu ar elektroninių ryšių priemonėmis pateikti

rašytinį prašymą (toliau – prašymas). Prašymo įgyvendinti duomenų subjektų teisę (-es) forma pateikiama Taisyklių 5 priede.

25. Prašymas turi būti įskaitomas, duomenų subjekto pasirašytas, jame turi būti nurodytas duomenų subjekto vardas, pavardė, gyvenamosios vietos adresas ir (ar) kiti kontaktiniai duomenys ryšiams palaikyti (telefono numeris ar elektroninio pašto adresas (nurodoma pareiškėjo pageidavimu), informacija apie tai, kokią Taisyklių 17.1–17.8 papunkčiuose nurodytą teisę ir kokios apimties duomenų subjektas pageidauja įgyvendinti.

26. Pateikdamas prašymą, duomenų subjektas privalo patvirtinti savo tapatybę:

26.1. kai prašymas teikiamas tiesiogiai atvykus į Administraciją, pateikti galiojantį asmens tapatybę patvirtinantį dokumentą;

26.2. kai prašymas teikiamas paštu ar per pasiuntinį, kartu turi pateikti asmens tapatybę patvirtinančio dokumento kopiją, patvirtintą notaro, ar šio dokumento kopiją, patvirtintą kita teisės aktu nustatyta tvarka;

26.3. kai prašymas teikiamas elektroninių ryšių priemonėmis, prašymą pasirašyti elektroniniu parašu.

27. Jei atstovaujamo duomenų subjekto vardu į Administraciją kreipiasi duomenų subjekto atstovas, jis prašyme (Taisyklių 5 priedas) turi nurodyti savo vardą, pavardę, gyvenamosios vietos adresą, ir (ar) kitus kontaktinius duomenis ryšiams palaikyti (telefono numeris ar elektroninio pašto adresas (nurodoma pareiškėjo pageidavimu), taip pat atstovaujamo asmens vardą, pavardę, gyvenamąją vietą, informaciją, kurią iš Taisyklių 17.1–17.8 papunkčiuose nurodytų duomenų subjekto teisių ir kokia apimtimi pageidauja įgyvendinti, ir pateikti atstovavimą patvirtinantį dokumentą. Kai atstovo prašymas teikiamas elektroninėmis priemonėmis, prašymas turi būti pasirašytas elektroniniu parašu. Teikdamas prašymą paštu ar per pasiuntinį, atstovas turi pridėti asmens tapatybę patvirtinančio dokumento kopiją, patvirtintą notaro, taip pat atstovavimą patvirtinančio dokumento kopiją, patvirtintą notaro.

28. Administracija, gavusi duomenų subjekto prašymą dėl Taisyklių 17.1–17.8 papunkčiuose nustatytų teisių įgyvendinimo, privalo išnagrinėti prašymą, nustatyti, ar prašymas yra pagrįstas, priimti sprendimą, atlikti reikiamus veiksmus ir atsakymą duomenų subjektui pateikti ne vėliau kaip per 30 kalendorinių dienų nuo prašymo gavimo dienos.

29. Atsižvelgiant į prašymo sudėtingumą ir skaičių, prašymo nagrinėjimo terminas Administracijos direktoriaus sprendimu gali būti pratęstas dar iki 30 kalendorinių dienų, informuojant duomenų subjektą apie tokį pratęsimą, kartu pateikiant prašymo nagrinėjimo termino pratęsimo priežastis.

30. Administracija, atsisakydama tenkinti duomenų subjekto prašymą įgyvendinti Taisyklių 17.1–17.8 papunkčiuose nurodytas teises, ne vėliau kaip per 30 kalendorinių dienų nuo prašymo gavimo dienos duomenų subjektui pateikia tokio atsisakymo motyvus ir nurodo apskundimo tvarką.

31. Duomenų subjektas turi teisę skusti Administracijos veiksmus (neveikimą) Valstybinei duomenų apsaugos inspekcijai per 3 mėnesius nuo atsakymo iš Administracijos gavimo dienos arba per 3 mėnesius nuo tos dienos, kada baigiasi Taisyklių 28 ir 30 punktuose nurodytas terminas, pateikti atsakymą.

32. Visa informacija ir pranešimai duomenų subjektui pateikiami tuo pačiu būdu, kokiu buvo gautas prašymas, išskyrus atvejus, kai duomenų subjektas paprašo informaciją pateikti kitu būdu.

33. Duomenų subjektų teisės Administracijoje įgyvendinamos neatlygintinai.

34. Administracija, įgyvendindama duomenų subjekto teises, privalo užtikrinti, kad nebūtų pažeista kitų asmenų teisė į privataus gyvenimo neliečiamumą.

35. Duomenų subjekto teisės gali būti apribotos BDAR 23 straipsnio 1 dalyje nustatytais atvejais, Lietuvos Respublikos įstatymų ar kitų teisės aktų nustatyta tvarka.

## V SKYRIUS DUOMENŲ TEIKIMAS

36. Asmens duomenys trečiosioms šalims gali būti teikiami tik įstatymų ir kitų teisės aktų nustatytais atvejais ir tvarka:

36.1. asmenų, pateikusių Administracijai skundą ar prašymą, asmens duomenys skundo ar prašymo nagrinėjimo tikslu – juridiniams ir fiziniams asmenims, įgaliotiems pagal kompetenciją nagrinėti gautą prašymą ar skundą;

36.2. asmenų, pateikusių Administracijai skundą ar prašymą, ir duomenų valdytojų (fizinių asmenų) asmens duomenys ginčo dėl Administracijos priimto sprendimo teisėtumo nagrinėjimo tikslu – teismams, Lietuvos administracinių ginčų nagrinėjimo komisijai, teritorinėms administracinių ginčų nagrinėjimo komisijoms ir (ar) darbo ginčų komisijai ir kitoms ikiteisminėms institucijoms;

36.3. Administracijos darbuotojų asmens duomenys: socialinio draudimo mokesčio administravimo tikslu – Valstybinio socialinio draudimo fondo valdybai prie Socialinės apsaugos ir darbo ministerijos, mokesčių administravimo tikslu – Valstybinei mokesčių inspekcijai prie Lietuvos Respublikos finansų ministerijos, valstybės tarnybos valdymo tikslu – Valstybės tarnybos departamentui;

36.4. asmenų, patekusių į Administracijos atliekamo vaizdo stebėjimo lauką, vaizdo duomenys galimų teisės aktų pažeidimų nustatymo tikslu – ikiteisminio tyrimo institucijoms, teismams ar kitoms valstybės įgaliotoms institucijoms;

36.5. asmenų, skambinusių į Administraciją telefonu, pokalbių duomenys galimų teisės aktų pažeidimų nustatymo tikslu – ikiteisminio tyrimo institucijoms, teismams ar kitoms valstybės įgaliotoms institucijoms;

36.6. žiniasklaidos atstovų duomenys ginčo dėl Lietuvos Respublikos visuomenės informavimo įstatyme ir kituose visuomenės informavimą reglamentuojančiuose įstatymuose ir teisės aktuose nustatytų visuomenės informavimo principų nesilaikymo nagrinėjimo tikslu – Žurnalistų etikos inspektoriaus tarnybai, teismams ar kitoms valstybės įgaliotoms institucijoms.

37. Administracija duomenų subjektų duomenis duomenų gavėjams gali teikti ir pagal sudarytą sutartį arba vienkartinį duomenų gavėjo prašymą, nepažeisdama teisės aktuose įtvirtintų reikalavimų ir asmens duomenų konfidencialumo užtikrinimo ir laikydamasi duomenų valdytojo atskaitomybės principo.

38. Vienkartinio duomenų teikimo atveju Administracija, teikdama asmens duomenis pagal trečiosios šalies vienkartinį prašymą, pirmenybę teikia duomenų teikimui elektroninių ryšių priemonėmis, jeigu prašyme nenurodyta kitaip. Siekiant įgyvendinti BDAR 5 straipsnio 2 dalyje įtvirtintą duomenų valdytojo atskaitomybės principą, duomenys trečiosioms šalims gali būti teikiami tik, kai duomenų gavėjas teiktame prašyme nurodo aplinkybes, pagrindžiančias, kad duomenų tvarkymas (teikimas) atitinka BDAR 5 straipsnyje įtvirtintus principus ir yra pagrįstas bent viena BDAR 6 straipsnio 1 dalyje arba 9 straipsnio 2 dalyje įtvirtinta teisėto duomenų tvarkymo sąlyga. Prašyme privaloma nurodyti bent:

38.1. duomenų gavimo konkretų ir aiškiai apibrėžtą tikslą;

38.2. jeigu yra, duomenų tvarkymo (gavimo) teisinį pagrindą, įtvirtintą Lietuvos Respublikos arba Europos Sąjungos teisės aktuose, ir konkrečią jų nuostatą, suteikiančią teisę gauti asmens duomenis;

38.3. duomenų tvarkymo (gavimo) teisėtą sąlygą, įtvirtintą BDAR 6 straipsnio 1 dalyje arba 9 straipsnio 2 dalyje, kuria vadovaujantis suteikiama teisė gauti asmens duomenis;

38.4. duomenų teisėto tvarkymo (teikimo) sąlygą, įtvirtintą BDAR 6 straipsnio 1 dalyje arba 9 straipsnio 2 dalyje, kuria vadovaudamasi Administracija turi teisę pateikti šiuos duomenis trečiajam asmeniui;

38.5. konkrečią prašomų duomenų apimtį, t. y. kokių konkrečių duomenų prašoma: vardo, pavardės, paskirtos išmokos dydžio ir pan. Prašymai pateikti visą turimą informaciją apie asmenį nelaikytini konkrečiais;

38.6. kai įgyvendinant Taisyklių 38.4 papunkčio sąlygą nurodoma, kad duomenis pateikti prašoma vadovaujantis BDAR 6 straipsnio 1 dalies e arba f punktais, t. y. kai duomenis tvarkyti (teikti) reikia siekiant atlikti užduotį, vykdomą viešojo intereso labui, arba vykdant duomenų valdytojiui pavestas viešosios valdžios funkcijas, arba teikti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų apsaugos, prašyme turi būti išsamiai pagrįsta, kodėl šių asmenų interesai yra viršesni už duomenų subjekto teises ir laisves.

39. Administracijos darbuotojas, nagrinėjantis gautą prašymą pateikti asmens duomenis, privalo:

39.1. patikrinti, kad prašyme nurodytas asmens duomenų naudojimo tikslas yra konkretus ir teisėtas (nurodymas, kad duomenys reikalingi nagrinėjant bylą ar teikiant ieškinį, paprastai nelaikomas konkrečiu tikslu);

39.2. patikrinti, ar duomenų gavėjas pagrįstai remiasi prašyme nurodytu gavimo ir teikimo teisiniu pagrindu ir teisėta duomenų teikimo ir gavimo sąlyga, įtvirtinta BDAR 6 straipsnio 1 dalyje arba 9 straipsnio 2 dalyje;

39.3. kai duomenis pateikti prašoma remiantis BDAR 6 straipsnio 1 dalies e arba f punktais, įvertinti, ar gavėjo interesai tikrai yra svarbesni už duomenų subjekto teises ir laisves;

39.4. įvertinti, ar prašomų pateikti duomenų apimtis nėra per didelė nurodytam tikslui pasiekti;

39.5. kai duomenis teikti prašoma vadovaujantis BDAR 6 straipsnio 1 dalies e arba f punktais, prašymą nagrinėjantis Administracijos darbuotojas privalo supažindinti duomenų subjektą, kurio duomenis planuojama tvarkyti (teikti), su jo teise nesutikti, kad būtų teikiami jo duomenys.

40. Asmens duomenų teikimui valstybės ir savivaldybės institucijoms ir įstaigoms, kai šios institucijos ir įstaigos pagal konkretų paklausimą gauna asmens duomenis įstatymų nustatytoms kontrolės funkcijoms vykdyti, taikomos visos šiame skirsnyje aptartos duomenų teikimo (gavimo) sąlygos. Administracijos arba Administracijos duomenų tvarkytojo darbuotojai be papildomo teisinio reikalavimo gali būti asmens duomenų gavėjais, jeigu jie dalyvauja duomenų valdytojo arba duomenų tvarkytojo vykdomose tvarkymo operacijose arba šie duomenys yra būtini darbuotojo funkcijoms vykdyti. Teikdamas duomenis duomenų gavėjams, Administracijos darbuotojas, siekdamas užtikrinti duomenų konfidencialumą, turi teisę reikalauti duomenų gavėjo nurodyti duomenų gavimo tikslą ir konkrečią duomenų apimtį.

## **VI SKYRIUS**

### **ASMENS DUOMENŲ APSAUGOS PAREIGŪNAS**

41. Administracijos direktoriaus įsakymu asmens duomenų apsaugos pareigūnu (toliau – pareigūnas) skiriamas vienas iš esamų Administracijos darbuotojų, naujas darbuotojas arba asmuo, su kuriuo būtų sudaroma paslaugų teikimo sutartis.

42. Duomenų apsaugos pareigūnas yra nepriklausomas Administracijos patarėjas asmens duomenų apsaugos klausimais. Duomenų subjektai gali kreiptis į pareigūną visais klausimais, susijusiais su asmens duomenų tvarkymu ir naudojimu savo teisėmis pagal BDAR, tačiau konkrečias užduotis ar veiksmus, būtinus įgyvendinant asmens duomenų apsaugos reikalavimus, išskyrus šiose Taisyklėse tiesiogiai aptartus atvejus, atlieka už duomenų tvarkymą atsakingas duomenų tvarkytojas (Administracijos darbuotojas, padalinys ir pan.).

43. Pareigūno teisės ir pareigos:

43.1. pareigūnas privalo turėti tinkamų ekspertinių asmens duomenų apsaugos teisės ir praktikos žinių;

43.2. pareigūnas turi teisę būti informuotas ir įsitraukti į visų su asmens duomenų apsauga ir privatumu susijusių klausimų nagrinėjimą Administracijoje;

43.3. pareigūnas turi teisę susipažinti su asmens duomenimis, dalyvauti duomenų tvarkymo operacijose;

43.4. pareigūnas turi teisę atlikdamas savo funkcijas gauti visus reikiamus išteklius (laiko, tinkamų darbo sąlygų ir kt.) ir galimybę išlaikyti ekspertines duomenų apsaugos teisės ir praktikos žinias.

44. Pareigūnas Administracijoje privalo vykdyti šias užduotis:

44.1. padėti užtikrinti, kad Administracijoje vykdomas asmens duomenų tvarkymas atitiktų BDAR, kitų asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų reikalavimus, tinkamai įvertinant duomenų tvarkymo operacijas, duomenų tvarkymo pobūdį, aprėptį, kontekstą, tikslus, potencialų pavojų;

44.2. stebėti, kaip laikomasi BDAR ir kitų asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų reikalavimų, šių Taisyklių, kitų vidaus dokumentų, susijusių su asmens duomenų apsauga;

44.3. konsultuoti ir stebėti, kaip atliekamas poveikio duomenų apsaugai vertinimas, aptartas šių Taisyklių VII skyriuje;

44.4. informuoti Administracijos direktorių ir kitus darbuotojus apie jų pareigas pagal BDAR ir kitus asmens duomenų teisinę apsaugą reglamentuojančius teisės aktus ir juos konsultuoti dėl konkrečių pareigų vykdymo;

44.5. informuoti Administracijos direktorių apie bet kokias neatitiktis, pažeidimus asmens duomenų apsaugos srityje, kuriuos pareigūnas nustato vykdydamas savo funkcijas;

44.6. konsultuoti Administracijos darbuotojus, dirbančius su asmens duomenimis, asmens duomenų teisinės apsaugos klausimais;

44.7. bendradarbiauti, būti kontaktiniu asmeniu santykiuose su Valstybine duomenų apsaugos inspekcija;

44.8. vykdyti kitas pareigybės aprašyme nustatytas funkcijas;

44.9. privalo užtikrinti slaptumą ir (ar) konfidencialumą, susijusį su jo užduočių vykdymu, laikydamasis Europos Sąjungos ar valstybės narės teisės aktų reikalavimų;

44.10. privalo tvarkyti ir saugoti su asmens duomenų apsauga susijusios veiklos duomenis (toliau – veiklos įrašai), kurie nurodytų bent šią minimalią ir aktualią informaciją.

45. Už veiklos įrašų pateikimą Valstybinei duomenų apsaugos inspekcijai (esant jos prašymui (reikalavimui) atsako pareigūnas.

46. Pareigūnas nevykdo jokių kitų pareigų ar funkcijų, pavestų atlikti ne Administracijos direktoriaus, taip pat funkcijų, kurios galėtų sukelti interesų konfliktą su jo atliekamomis pareigūno funkcijomis.

47. Pareigūno vardas, pavardė ir kontaktiniai duomenys skelbiami Panevėžio miesto savivaldybės interneto svetainėje [www.panevezys.lt](http://www.panevezys.lt).

## **VII SKYRIUS**

### **POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS**

48. Administracija, prieš pradėdama vykdyti naują (-as) duomenų tvarkymo operaciją (-as) arba pasikeitus vykdomos operacijos pobūdžiui, mastui ir pan., privalo atlikti poveikio duomenų apsaugai vertinimą, jei duomenų tvarkymas:

48.1. keltų didelį pavojų duomenų subjektų teisėms ir laisvėms (pavyzdžiui, atvejai, kai duomenys būtų perduodami už Europos Sąjungos ribų ar būtų pradėti tvarkyti duomenys, kurie gauti juos sujungus su duomenimis iš kitų šaltinių, būtų pradėti naudoti nauji technologiniai sprendimai, pavyzdžiui, veido atpažinimo sistemos ir kt.);

48.2. automatizuotai būtų tvarkomi asmeniniai aspektai, vykdomas profiliavimas ir priimami teisiniai ar kiti didelio poveikio (pavyzdžiui, kai duomenų tvarkymas gali lemti asmenų atskirtį arba diskriminaciją) sprendimai;

48.3. būtų pradėtas vykdyti sistemingas vaizdo stebėjimas dideliu mastu;

48.4. būtų pradėti tvarkyti ypatingi asmens duomenys dideliu mastu.

49. Jei Administracija, atlikdama poveikio duomenų apsaugai vertinimą, nustatytų, kad duomenų subjektų teisėms ir laisvėms gali kilti didelis pavojus (žr. Taisyklių 48.1 papunktį), ji



privalo konsultuotis su Valstybine duomenų apsaugos inspekcija dėl tinkamų saugumo ir kitų priemonių įgyvendinimo.

50. Atliekant poveikio duomenų apsaugai vertinimą, Administracija privalo nustatyti:

50.1. kokia (-ios) bus atliekama (-os) duomenų tvarkymo operacija (-os);

50.2. kiek konkreči duomenų tvarkymo operacija yra reikalinga ir proporcinga;

50.3. koks gali būti poveikis duomenų subjektams;

50.4. kokios yra galimos potencialių pavojų šalinimo, saugumo užtikrinimo priemonės.

51. Administracija privalo užtikrinti, kad šiame skyriuje aprašytas ir Administracijos numatytais atvejais atliekamas poveikio duomenų apsaugai vertinimas būtų tinkamai dokumentuotas ir saugomas. Poveikio duomenų apsaugai vertinimo forma nustatyta šių Taisyklių 6 priede.

52. Poveikio duomenų apsaugai vertinimas gali būti atliekamas ir esamoms duomenų tvarkymo operacijoms (t. y. vykdomoms iki BDAR įsigaliojimo), jei tose operacijose atsirastų reikšmingų pokyčių, pavyzdžiui: būtų pradėtos naudoti naujos technologijos, duomenys būtų pradėti tvarkyti kitu tikslu nei iki tol, atsirastų naujos rizikos, susijusios su įvykdytomis kibernetinėmis atakomis, įsilaužimais į Administracijos sistemą, duomenys būtų pradėti teikti naujiems duomenų gavėjams, tvarkytojams už Europos Sąjungos ribų, kt.

53. Poveikio duomenų apsaugai vertinimas taip pat gali būti atliekamas ir šiame skyriuje neaptais atvejais, bet esant Administracijos direktoriaus, pareigūno ar Valstybinės duomenų apsaugos inspekcijos rekomendacijai tai atlikti.

54. Administracija, esant poreikiui, atlikdama poveikio duomenų apsaugai vertinimą konsultuojasi su duomenų tvarkytoju.

## **VIII SKYRIUS**

### **ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS**

55. Asmens duomenų saugumo pažeidimu yra laikomas bet kuris tyčinis ar neatsargus asmens duomenų apsaugos pažeidimas, kai:

55.1. sunaikinami, prarandami arba pakeičiami asmens duomenys;

55.2. be leidimo atskleidžiami asmens duomenys, trečiosioms šalims, darbuotojams, neturintiems teisės tvarkyti asmens duomenų;

55.3. be leidimo asmenys, įskaitant ir Administracijos darbuotojus, neturintys tam teisės, gautų prieigą prie asmens duomenų.

56. Jei dėl įvykdyto asmens duomenų saugumo pažeidimo kyla galimas pavojus duomenų subjektų teisėms ir laisvėms, kurio neįmanoma pašalinti imantis atitinkamų saugumo pažeidimo pašalinimo priemonių, pareigūnas ar kitas Administracijos direktoriaus paskirtas darbuotojas privalo nedelsdamas, bet ne vėliau kaip per 72 valandas nuo pažeidimo paaiškėjimo dienos pranešti Valstybinei duomenų apsaugos inspekcijai apie įvykusį duomenų saugumo pažeidimą. Jeigu Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų saugumo pažeidimą nepranešama per 72 valandas, pranešime turi būti nurodytos vėlavimo priežastys. Pranešimo Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų saugumo pažeidimą forma nustatyta Taisyklių 7 priede.

57. Kilus ypač dideliu duomenų subjektų teisėms ir laisvėms pavojui, pavyzdžiui: dėl įvykusio saugumo gali kilti realus arba labai tikėtinas duomenų subjekto kūno sužalojimas, turtinė ar neturtinė žala, diskriminacija, pavogta ir suklastota tapatybė, pakenkta reputacijai, panaikinti pseudonimai, prarasta galimybė naudotis savo teisėmis, užkirstas kelias kontroliuoti savo duomenis ir pan., informacija apie įvykusį saugumo pažeidimą nedelsiant taip pat turi būti pateikta ir duomenų subjektams.

58. Nesant galimybės informuoti visų duomenų subjektų dėl jų didelio skaičiaus ar kitų priežasčių, pareigūnas kartu su Administracijos direktoriumi apsvarsto ir priima sprendimą šią informaciją pateikti per visuomenės informavimo priemones (spauda, televizija, kt.).

59. Šių Taisyklių 56 ir 57 punktuose nurodytuose pranešimuose dėl įvykusio asmens duomenų saugumo pažeidimo Valstybinei duomenų apsaugos inspekcijai, duomenų subjektams privalo būti trumpai aprašytas asmens duomenų saugumo pažeidimo pobūdis, nurodant apytikslį duomenų subjektų skaičių, kurios asmens teisės ir laisvės galėjo būti pažeistos, pareigūno ar kito atsakingo darbuotojo kontaktai, trumpai aprašytos tikėtinos pažeidimo pasekmės ir priemonės, kurių Administracija imasi (imsis), kad būtų pašalintos neigiamos pasekmės, susijusios su įvykusiu duomenų saugumo pažeidimu.

60. Nustatydamas, ar būtina vykdyti informavimo pareigą, aptartą šių Taisyklių 56 ir 57 punktuose, pareigūnas ar kitas Administracijos direktoriaus paskirtas atsakingas darbuotojas privalo įvertinti, ar dėl įvykusio incidento:

60.1. įvyko konfidencialumo pažeidimas (pavyzdžiui, atskleisti duomenys ir jie tapo prieinami trečiosioms šalims ar Administracijos darbuotojams, neturintiems teisės tvarkyti asmens duomenų, suteikiant prieigą, tinkamai nešifruojant, kt.);

60.2. įvyko duomenų pasiekiamumo pažeidimas (pavyzdžiui, prarasti duomenys ir neturima atsarginių kopijų);

60.3. įvyko duomenų vientisumo pažeidimas (pavyzdžiui, kai yra neteisėtas ar netyčinis asmens duomenų praradimas).

61. Jei pareigūnas ar kitas Administracijos direktoriaus paskirtas atsakingas darbuotojas nustato, kad yra bent vienas iš šių Taisyklių 60.1–60.3 papunkčiuose numatytų pažeidimų, jis nedelsdamas vykdo informavimo pareigą, kaip tai aptarta Taisyklių 56 ir 57 punktuose.

62. Pareigūnas ar kitas Administracijos direktoriaus paskirtas atsakingas darbuotojas privalo užtikrinti, kad visi asmens duomenų apsaugos pažeidimai, įskaitant ir tuos, dėl kurių nevykdoma informavimo pareiga, kaip aptarta šiame Taisyklių skyriuje, būtų tinkamai dokumentuoti ir saugomi.

63. Įvykus asmens duomenų saugumo pažeidimui, aptartam šiame Taisyklių skyriuje, pareigūnas ar kitas Administracijos direktoriaus paskirtas atsakingas darbuotojas informuoja Administracijos darbuotojus ir duoda atitinkamas instrukcijas konkreitiems darbuotojams dėl jų pareigų, funkcijų vykdymo, susijusio su asmens duomenų saugumo pažeidimo valdymu.

64. Įvykus asmens duomenų saugumo pažeidimui, aptartam šiame Taisyklių skyriuje, pareigūnas, be kitų šiame skyriuje aptartų pareigų, taip pat sudaro prevencinių veiksmų planą, kuriuo būtų siekiama ateityje užkirsti kelią analogiškam ar panašiam duomenų saugumo pažeidimui, ir pateikia jį Administracijos direktoriui, kuris sprendžia dėl veiksmų plano įgyvendinimo.

65. Administracijoje vedamas asmens duomenų saugumo pažeidimų žurnalas (Taisyklių 8 priedas), kuriame nurodoma bent pažeidimo data, paveiktų duomenų subjektų skaičius, pažeidimo priežastys, pažeidimo aprašymas, priemonės, kurių buvo imtasi pažeidimo mastui sumažinti, pareiga informuoti duomenų subjektus ir Valstybinę duomenų apsaugos inspekciją ir kita informacija.

## **IX SKYRIUS**

### **VAIZDO STEBĖJIMAS IR TELEFONINIŲ POKALBIŲ ĮRAŠYMAS IR TVARKYMAS**

66. Vykdamas vaizdo stebėjimą vadovaujamasi BDAR, ADTAĮ ir kitais teisės aktais, reglamentuojančiais asmens duomenų apsaugą. Administracijoje vykdomo vaizdo stebėjimo tikslas – užtikrinti Administracijos darbuotojų ir kitų asmenų, kurie lankosi Administracijoje, patalpų ir jose esančio turto ir dokumentų saugumą, užtikrinti viešąją tvarką Panevėžio miesto teritorijoje, fiksuoti teisės pažeidimus, tyrimo veiksmus, vadovaujantis Lietuvos Respublikos administracinių nusižengimų kodeksu, tiriant administracinius nusižengimus. Vaizdo stebėjimo pagrindas – tvarkyti duomenis būtina Administracijai vykdamas pavestas viešosios valdžios funkcijas ir siekiant tiek teisėtų Administracijos, tiek ir Administracijoje besilankančių asmenų interesų užtikrinimo (BDAR 6 straipsnio 1 dalies e, f punktai):

66.1. Vaizdo stebėjimo duomenys negali būti naudojami kitiems tikslams, nesusijusiems su šių Taisyklių 66 punkte apibrėžtais tikslais, išskyrus atvejus, kai tokiam duomenų tvarkymui egzistuoja atskiras BDAR 6 straipsnio 1 dalyje įtvirtintas pagrindas.

67. Administracijos patalpose ir teritorijoje tvarkomas tik vaizdas (be garso) iš vaizdo stebėjimo kamerų, patenkantis į vaizdo stebėjimo lauką. Vaizdo stebėjimas vykdomas neįrašant vaizdo duomenų, o stebint realiu laiku (angl. „on-line“ režimu).

68. Vaizdo stebėjimas vykdomas ne didesnėje Administracijos patalpose ir teritorijos dalyje, negu tai yra būtina Administracijos darbuotojų ir kitų asmenų, kurie lankosi Administracijoje, patalpų ir jose esančio turto bei dokumentų saugumui užtikrinti. Vykdamas teisės pažeidimų ir tyrimų veiksmų fiksavimą filmuojant (fotografuojant), užtikrinti, kad būtų fiksuojami tik su minėtais veiksmais susiję asmens duomenys.

69. Vykdamas vaizdo stebėjimą draudžiama stebėti vaizdą:

69.1. Administracijos darbuotojų darbo vietose;

69.2. Administracijos patalpose, kuriose duomenų subjektas pagrįstai tikisi absoliučios privatumo apsaugos ir kur toks vaizdo stebėjimas žemintų žmogaus orumą (pvz. tualetuose, persirengimo kambariuose ir pan.);

69.3. Administracijos patalpose slaptomis vaizdo kameromis.

70. Prieiga prie vaizdo stebėjimo Administracijos patalpose ir teritorijoje duomenų, jų tvarkymo suteikta saugumą užtikrinantiems Vidaus administravimo skyriaus Ūkio ir eksploataavimo poskyrio darbuotojams ir vaizdo stebėjimo sistemą administruojantiems E. plėtros skyriaus darbuotojams.

71. Duomenis, gautus filmuojant (fotografuojant) teisės pažeidimus, tyrimo veiksmus tvarko Administracijos Teisės ir viešosios tvarkos skyriaus darbuotojai.

72. Administracija privalo užtikrinti, kad darbuotojai ir Administracijos lankytojai apie vykdomą vaizdo stebėjimą būtų aiškiai ir tinkamai informuojami matomoje vietoje iškabintais vaizdo stebėjimo informaciniais pranešimais (gali būti ženklai arba lipdukai su užrašu apie vykdomą vaizdo stebėjimą, atitinkantys BDAR 13 straipsnio reikalavimus). Duomenų subjektai turi visas duomenų subjektų teises, įtvirtintas šių Taisyklių IV skyriuje. Duomenų subjektų teisės įgyvendinamos šių Taisyklių nustatyta tvarka.

73. Asmenys apie vykdomą vaizdo stebėjimą privalo būti informuojami dar prieš patekdami į vaizdo stebėjimo kamerų fiksuojamą lauką, bet ne per toli nuo jo.

74. Darbuotojai, susipažindami su šiomis Taisyklėmis, taip pat patvirtina, jog jiems yra žinomas faktas apie Administracijoje vykdomą vaizdo stebėjimą, jo tikslą, duomenų saugojimo laiką ir kitą su tuo susijusią aktualią informaciją.

75. Patekti į patalpą, kurioje yra vaizdo stebėjimo valdymo įranga, turi teisę tik Administracijos direktoriaus įsakymu įgalioti už vaizdo stebėjimo sistemos priežiūrą atsakingi darbuotojai arba paslaugų teikėjai, kaip numatyta šiose Taisyklėse.

76. Viešųjų vietų stebėjimo, atliekamo siekiant užtikrinti viešąją tvarką, asmenų, jų turto saugumo ir nusižengimų prevencijos įgyvendinimą, sąlygos apibrėžiamos duomenų tvarkymo sutartyse.

77. Pokalbiai telefonu įrašomi ir pokalbių įrašų duomenys tvarkomi asmenų aptarnavimo ir teikiamų konsultacijų telefonu kokybės užtikrinimo ir asmenų prašymų bei skundų nagrinėjimo objektyvumo tikslais:

77.1. Pokalbių įrašų duomenys negali būti tvarkomi nesuderinamais su 77 punkte nustatytais tikslais;

77.2. Įrašomi tik sutartyje su fiksuoto ryšio paslaugas teikiančia įmone nurodytų telefonų įeinantys ir išeinantys pokalbiai ir tik Administracijos darbo metu;

77.3. Įrašomi ir tvarkomi šie telefoninio pokalbio įrašų metaduomenys: konsultuojančio asmens vardas ir pavardė (jeigu garsiai įvardijama prisistatant), darbuotojo ir skambinančiojo asmens telefono ryšio numeris, pokalbio turinys, data, pradžios ir pabaigos laikas;

77.4. Telefoninių pokalbių įrašymo tikslas ir apimtis gali būti keičiami tik pakeitus Taisykles;

77.5. Už telefoninių pokalbių įrašymą, duomenų saugumo užtikrinimą, duomenų pateikimą trečiosioms šalims, jų saugojimo terminą atsakinga įmonė, teikianti fiksuotojo ryšio paslaugas Administracijai.

## **X SKYRIUS ASMENS DUOMENŲ TVARKYTOJAI**

78. Tais atvejais, kai Administracija įgalioja duomenų tvarkytoją atlikti asmens duomenų tvarkymo veiksmus, tarp Administracijos ir duomenų tvarkytojo turi būti sudaroma rašytinė asmens duomenų tvarkymo sutartis.

79. Sprendimą perduoti duomenų subjekto duomenų tvarkymą asmens duomenų tvarkytojui priima Administracijos direktorius arba jo įgaliotas asmuo.

80. Administracija parenka duomenų tvarkytoją, kuris užtikrina, kad būtų įgyvendintos techninės ir organizacinės duomenų apsaugos priemonės ir užtikrintas tokių priemonių laikymasis, įskaitant ir šių Taisyklių XI skyriuje aptartas technines, organizacines duomenų saugumo užtikrinimo priemones.

81. Administracija, sutartimi įgaliodama duomenų tvarkytoją tvarkyti asmens duomenis, nurodo, kad asmens duomenys būtų tvarkomi atsižvelgiant į asmens duomenų tvarkymą reglamentuojančius teisės aktus, Administracijos nurodymus, taip pat nurodoma, kokius asmens duomenų tvarkymo veiksmus privalo atlikti duomenų tvarkytojas Administracijos vardu, duomenų tvarkytojo įsipareigojimai Administracijai, įskaitant įsipareigojimą laikytis BDAR įtvirtintų reikalavimų, duomenų tvarkymo trukmė, pobūdis, asmens duomenų rūšis, duomenų subjektų kategorijos, duomenų tvarkytojo pareiga ištrinti arba gražinti Administracijai asmens duomenis, jų kopijas, pabaigus Administracijai teikti paslaugas.

82. Administracija, sudarydama sutartį su duomenų tvarkytoju, be kita ko, nurodo, kad duomenų tvarkytojas privalo užtikrinti Administracijos perduodamų tvarkyti duomenų konfidencialumą, o ketindamas tvarkymui pasitelkti trečiuosius asmenis (kitus duomenų tvarkytojus), duomenų tvarkytojas privalo gauti išankstinį rašytinį Administracijos pritarimą ir užtikrinti, kad pasitelktas subtvarkytojas laikytųsi tų pačių reikalavimų, kurie nustatyti tvarkytojui.

83. Bendradarbiavimo su duomenų tvarkytojais sutarčių rengimo, pasirašymo, pakeitimo, atnaujinimo ar nutraukimo procedūras inicijuoja ir jas vykdo už asmens duomenų tvarkymą atsakingas Administracijos padalinys. Pasirašytas sutartis atsakingas padalinys privalo saugoti, peržiūrėti. Esant poreikiui inicijuoti bendradarbiavimo su duomenų tvarkytojais sutarčių atnaujinimą, pakeitimą ir (ar) nutraukimą gali ir pareigūnas.

## **XI SKYRIUS TECHNINĖS IR ORGANIZACINĖS ASMENS DUOMENŲ TVARKYMO PRIEMONĖS**

84. Administracijos darbuotojai privalo laikytis Taisyklių nuostatų ir prisidėti įgyvendinant Administracijos įdiegtas organizacines ir technines priemones, skirtas asmens duomenims apsaugoti nuo atsitiktinio ar neteisėto naikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

85. Administracijos darbuotojai turi laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino eidami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas.

86. Pareiga saugoti asmens duomenų paslaptį galioja visą darbuotojo darbo laiką, taip pat galioja darbuotoją paskyrus į kitas pareigas ir pasibaigus darbo santykiams.

87. Siekiant apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo turi būti taikomos šios infrastruktūrinės, administracinės ir telekomunikacinės (elektroninės) priemonės:

87.1. saugus ir tinkamas techninės įrangos išdėstymas ir jos priežiūra, informacinių sistemų (IS) priežiūra, tinklo (LAN, belaidžio) valdymas, naudojimosi internetu saugumo užtikrinimas ir kitos informacinių technologijų priemonės;

87.2. priešgaisrinės apsaugos tarnybos nustatytų normų laikymasis;

87.3. saugus ir tinkamas darbo organizavimas ir kitos administracinės priemonės;

87.4. būtina bent kartą per vienus metus vykdyti informacinių sistemų duomenų tvarkymo keliamos rizikos vertinimą;

87.5. Administracijos paruoštų organizacinių ir techninių duomenų saugumo priemonių įvertinimo auditas turi būti atliekamas bent vieną kartą per dvejus metus;

87.6. atsižvelgiant į rizikos vertinimo rezultatus, turi būti diegiamos būtinos duomenų saugumo priemonės;

87.7. atliekami praktiniai bandymai dėl avarinio asmens duomenų atkūrimo;

87.8. kiekvieną darbo dieną atliekamas duomenų atsarginių kopijų darymas;

87.9. atsarginių duomenų kopijos saugomos atsarginių kopijų saugykloje atskirai nuo pagrindinės buveinės;

87.10. užtikrinamas duomenų atkūrimas iš naujausių turimų atsarginių duomenų kopijų, praradus duomenis dėl aparatinės kompiuterių įrangos gedimo, programinės įrangos klaidos ar kitaip pažeidus duomenų vientisumą;

87.11. IS funkcionalumo ir duomenų vientisumo ir parengtumo testavimų atlikimas;

87.12. bent kartą per metus turi būti atliekamas bandomasis duomenų atkūrimas.

88. Darbuotojai, kurie tvarko fizinių asmenų duomenis, turi laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su fiziniais asmenimis susijusią informaciją, su kuria jie susipažino vykdydami savo pareigas. Ši pareiga išlieka galioti perėjus dirbti į kitas pareigas Administracijoje arba pasibaigus darbo ar sutartiniams santykiams su Administracija.

89. Darbuotojai automatiniu būdu tvarkyti asmens duomenis gali tik po to, kai jiems suteikiama prieigos teisė prie atitinkamos informacinės sistemos. Prieiga prie asmens duomenų gali būti suteikta tik tam asmeniui, kuriam asmens duomenys yra reikalingi jo funkcijoms vykdyti. Darbo santykiams pasibaigus, darbuotojui prieigos prie registrų ir informacinių sistemų teisės panaikinamos.

90. Darbuotojai gali perduoti dokumentus, kuriuose nurodyti asmens duomenys, tik tiems darbuotojams, kurie pagal pareigas ar atskirus pavedimus turi teisę dirbti su asmens duomenimis.

91. Darbuotojai, vykdančys duomenų subjekto duomenų tvarkymo funkcijas, turi užkirsti kelią atsitiktiniam ar neteisėtam tvarkymui, turi saugoti dokumentus tinkamai ir saugiai (vengdami nereikalingų kopijų su duomenų subjekto duomenimis kaupimo ir kt.). Dokumentų kopijos, kuriuose nurodomi duomenų subjekto duomenys, turi būti sunaikinamos tokiu būdu, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio, pavyzdžiui, susmulkinant, tačiau jokių būdų neišmetant į šiukšliadėžę ar nepaliekant duomenų šalia jos ar kitoje atviroje vietoje. Už duomenų sunaikinimą atsakingas duomenis naikinantis asmuo.

92. Darbuotojai, kurių darbo kompiuteriuose saugomi interesantų duomenys arba iš kurių kompiuterių galima patekti į Administracijos IS, kuriose yra saugomi interesantų duomenys, savo darbo kompiuteriuose turi naudoti slaptažodžius; „svečio“ (angl. *guest*) tipo, t. y. neapsaugoti slaptažodžiais, vartotojai yra draudžiami. Šiuose kompiuteriuose taip pat reikia naudoti ekrano užsklandą su slaptažodžiu.

93. Minimalūs reikalavimai slaptažodžiams:

93.1. juos turi sudaryti ne mažiau kaip 8 simboliai, iš kurių bent keli turi būti skaičius ir raidė;

93.2. jie negali sutapti su darbuotojų ar jų šeimos narių asmeniniais duomenimis;

93.3. juos saugo ir juos gali žinoti tik darbuotojai, dirbantys su konkrečiais kompiuteriais;

93.4. jie negali būti saugomi viešai ir negali būti prieinami kaip visuma.

94. Slaptažodžiai esant būtinybei (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei ir pan.) turi būti keičiami.

95. Darbuotojų darbo kompiuteriai, kuriuose saugomos rinkmenos su fizinių asmenų duomenimis, negali būti laisvai prieinami iš kitų tinklo kompiuterių. Šių kompiuterių antivirusinė programinė įranga turi būti nuolat atnaujinama.

96. Nesant būtinybės, rinkmenos su asmens duomenimis neturi būti dauginamos skaitmeniniu būdu, t. y. kuriamos rinkmenų kopijos vietiniuose kompiuterių diskuose, nešiojamuosiose laikmenose.

97. Administracijoje yra užtikrinamas saugių protokolų ir (arba) slaptažodžių naudojimas, kai asmens duomenys perduodami išoriniais duomenų perdavimo tinklais.

98. Administracijos informacinėse sistemose ir kompiuterių tinkluose įgyvendinamos šios saugumo priemonės:

98.1. mobiliuosiuose įrenginiuose (nešiojamuosiuose kompiuteriuose, planšetėse, išmaniuosiuose telefonuose ir pan.), jeigu jie naudojami ne Administracijos vidiniame kompiuterių tinkle, esantys asmens duomenys ir prisijungimo prie Administracijos tvarkomų asmens duomenų informacija šifruojami ar apsaugomi tokiomis priemonėmis, kurios atitiktų asmens duomenų atskleidimo keliamą riziką;

98.2. atsarginės asmens duomenų kopijos, jei jos daromos, saugomos kitoje patalpoje ar geografinėje vietoje negu aktyvi (veikianti) duomenų bazė;

98.3. šifruojami atsarginėse kopijose, archyvuose ir išorinėse duomenų laikmenose saugomi asmens duomenys;

98.4. šifruojami elektroniniu paštu perduodami asmens duomenys;

98.5. asmens duomenų paieškos užklausoje nurodomas asmens duomenų naudojimo tikslas (-ai).

99. Administracijos direktoriaus paskirtas atsakingas darbuotojas privalo užtikrinti:

99.1. pašalinių asmenų įėjimo į serverių patalpas kontrolę, naudojant koduotą durų rakinimo sistemą ir bendrą apsaugos signalizacijos sistemą;

99.2. vidinio Administracijos kompiuterių tinklo apsaugą.

100. Darbuotojai privalo taip organizuoti savo darbą, kad kiek įmanoma labiau apribotų galimybę kitiems asmenims (kitiems darbuotojams ar kitiems tretiesiems asmenims) sužinoti tvarkomus asmens duomenis. Ši nuostata įgyvendinama:

100.1. nepaliekant dokumentų su tvarkomais asmens duomenimis ar kompiuterio, kuriuo naudojantis galima atidaryti rinkmenas su asmens duomenimis, be priežiūros taip, kad juose esančią informaciją galėtų perskaityti darbuotojai, neturintys teisės dirbti su konkrečiais asmens duomenimis, kiti asmenys;

100.2. dokumentus laikant taip, kad jų (ar jų fragmentų) negalėtų perskaityti atsitiktiniai asmenys;

100.3. jei dokumentai, kuriuose yra asmens duomenų, kitiems darbuotojams, padaliniams, įstaigoms perduodami per asmenis, kurie neturi teisės tvarkyti asmens duomenų, arba per paštą ar kurjerį, jie privalo būti perduodami užklijuotame nepermatomame voke. Šis punktas netaikomas, jeigu minėti pranešimai įteikiami interesantams asmeniškai ir konfidencialiai.

101. Už asmens duomenų saugumo pažeidimų valdymą ir reagavimą į šiuos pažeidimus nuo informacijos gavimo atsakingas pareigūnas.

102. Šiame Taisyklių skyriuje aptartos organizacinės ir techninės asmens duomenų apsaugos priemonės taikomos kartu su Administracijos direktoriaus patvirtintomis darbo tvarkos taisyklėmis, informacinių sistemų techninėmis specifikacijomis ir aprašais ir jiems neprieštarauja.

## **XII SKYRIUS DUOMENŲ VEIKLOS ĮRAŠŲ VEDIMO TVARKA**

103. Duomenų veiklos įrašų vedimo tvarka Administracijoje yra naudojama vadovaujantis šiomis principinėmis nuostatomis:

103. 1. turi būti naudojama griežtai tik darbo reikmėms;

103.2. naudojantis turi būti laikomasi galiojančių Lietuvos Respublikos teisės aktų, Administracijos vidinių aktų, darbo sutarčių nuostatų ir naudojimo instrukcijų;

103.3. naudojantis turi būti laikomasi darbuotojų saugos, komercinės informacijos saugos, asmens duomenų apsaugos reikalavimų;

103.4. naudojimas turi užtikrinti konfidencialumo įsipareigojimų, intelektinės nuosavybės teisių, įskaitant trečiųjų asmenų teises ir teisėtus interesus, bendrųjų etikos ir moralės principų laikymąsi.

104. Duomenų veiklos įrašų vedimo dokumente (ir elektroninėje jo rinkmenoje) privalo būti nurodyta:

104.1. duomenų tvarkytojas – Administracijos padalinio pavadinimas, atsakingas asmuo;

104.2. duomenų tvarkymo tikslas – koku tikslu yra tvarkomi duomenys (aiškiai aprašyti pvz., socialinei pašalpai gauti);

104.3. duomenų subjektai ir asmens duomenys – kokie konkretūs duomenys yra renkami (pvz., vardas, pavardė, adresas, ID kortelės kodas);

104.4. duomenų tvarkymo pagrindas – dėl ko vyksta šis rinkimas (pavyzdžiui, sutartis, prašymas, sutikimas);

104.5. duomenų gavėjai – kas yra galutinis šių duomenų gavėjas (pavyzdžiui, privatus asmuo, įmonės, ne Europos Sąjungos šalys);

104.6. duomenų saugojimo terminai – laikotarpis metais, kuriais nurodoma, kiek saugomi šie duomenys, ir momentas, nuo kada šis laikotarpis skaičiuojamas (pavyzdžiui, vieni metai nuo intereso prašymo gavimo);

104.7. duomenų ištrynimo (panaikinimo) terminai – laikotarpis metais, kurias nurodoma, kuriam laikui praėjus šie saugomi duomenys bus ištinti, ir momentas, nuo kada šis laikotarpis skaičiuojamas (pavyzdžiui, dveji metai nuo darbo sutarties nutraukimo);

104.8. naudojamos techninės ir organizacinės saugumo priemonės – naudojami pseudonimai, šifravimas, veiklos tęstinumo užtikrinimas techninio incidento metu, nuolatinis vertinimo procesas ir pan.

105. Duomenų veiklos įrašų vedimo dokumente gali būti ir kitų nuostatų, pildomų pagal poreikį. Duomenų veiklos įrašai į dokumentą įvedami raštu (ir elektroniniu būdu) iš karto po kiekvieno veiksmo atlikimo. Tai turi būti daroma nuolat vykdant naujas duomenų tvarkymo operacijas.

106. Įvykus incidentui, įrašuose turi būti tai pažymėta remiantis Informacinių ir komunikacinių technologijų bendrosiomis naudojimo taisyklėmis ir ten nurodytomis tvarkomis.

107. Kartą per vienus metus turi būti atliekamas patikrinimas pasirinktinai iki 10 proc. įrašų auditavimui atlikti ir įvertinti.

108. Kartą per dvejus metus turi būti atliekamas išsamus patikrinimas ir auditavimas.

109. Duomenų veiklos įrašai vedami raštu, pildant duomenų veiklos įrašų žurnalą, kurio pavyzdinė forma pateikiama šių Taisyklių 10 priede arba kitokios formos dokumente.

110. Duomenų veiklos įrašų vedimo tvarka ne rečiau kaip kartą per vienus metus peržiūrima ir, prireikus ar pasikeitus asmens duomenų tvarkymą reglamentuojantiems teisės aktams, diegiant struktūrinius, technologinius ar kitokius pakeitimus, atnaujinama. Už šios tvarkos nuostatų laikymosi priežiūrą ir juose reglamentuotų nuostatų vykdymo kontrolę, atnaujinimo pagal poreikį inicijavimą yra atsakingas pareigūnas.

111. Visi šiame skyriuje nenumatyti veiksmai, susiję su duomenų veiklos įrašų vedimu Administracijoje, privalo būti derinami su pareigūnu.

### **XIII SKYRIUS**

#### **ASMENS DUOMENŲ GAVIMAS IR TEIKIMAS NAUDOJANTIS VALSTYBINĖMIS INFORMACINĖMIS SISTEMOMIS IR REGISTRAIS**

112. Administracijos darbuotojai, priklausomai nuo einamų pareigų ir atliekamų funkcijų, turi prieigą prie vieno ar keleto informacinių sistemų ir registru, iš kurių gaunami ir į kuriuos

teikiami asmens duomenys tiek, kiek tai būtina dėl viešojo intereso arba vykdamant Administracijai pavestas viešosios valdžios funkcijas:

- 112.1. Administracinių nusižengimų registro;
- 112.2. Adresų registro;
- 112.3. Švietimo valdymo informacinės sistemos (ŠVIS);
- 112.4. E-mokyklos sistemos;
- 112.5. Nacionalinio egzaminų centro IS (NECIS);
- 112.6. Informacinės sistemos „E. sąskaita“;
- 112.7. Įtariamųjų, nuteistųjų ir kaltinamųjų registro;
- 112.8. Licencijų informacinės sistemos;
- 112.9. Lietuvos Respublikos teritorijų planavimo stebėsenos informacinės sistemos;
- 112.10. Lietuvos Respublikos teritorijų planavimo dokumentų rengimo ir teritorijų planavimo proceso valstybinės priežiūros informacinės sistemos;
- 112.11. Metrikacijos paslaugų informacinės sistemos (MEPIS);
- 112.12. Mokinių, studentų registro;
- 112.13. Nacionalinės mokėjimo agentūros informacinio portalo informacinės sistemos;
- 112.14. Neįgalumo ir darbingumo nustatymo tarnybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos (NDNT IS);
- 112.15. Nekilnojamojo turto kadastro ir registro informacinės sistemos;
- 112.16. Pedagogų registro;
- 112.17. Elektroninio archyvo informacinės sistemos (EAIS);
- 112.18. Socialinės paramos šeimai informacinės sistemos (SPIS);
- 112.19. Socialinių išmokų apskaitos informacinės sistemos PARAMA;
- 112.20. Statybos leidimų ir statybos valstybinės priežiūros informacinės sistemos „Infostatyba“;
- 112.21. Švietimo ir mokslo institucijų registro;
- 112.22. Lietuvos teismų informacinės sistemos;
- 112.23. Švietimo informacinių technologijų centro informacinės sistemos NEMIS;
- 112.24. Ūkio subjektų, susijusių su kelių transportu, stebėsenos ir informavimo valstybės informacinės sistemos (VEKTRA);
- 112.25. Valstybinės mokesčių inspekcijos informacinės sistemos;
- 112.26. Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos;
- 112.27. Valstybės tarnautojų registro sistemos (VATARAS);
- 112.28. Valstybės tarnybos valdymo informacinės sistemos (VATIS);
- 112.29. Lietuvos erdvinės informacijos portalo informacinės sistemos (TOPD, SERD);
- 112.30. VĮ „Regitra“ informacinės sistemos;
- 112.31. VĮ Žemės ūkio informacijos ir kaimo verslo centras valdomų registru: Ūkininkų gyvūnų, Žemės ūkio ir kaimo verslo, Ūkininkų ūkių, Žemės ūkio valdų, Pasėlių deklaravimo duomenų ir Paraiškų priėmimo ir Traktorių, savaeigių ir žemės ūkio mašinų ir jų priekabų registro informacinių sistemų; Žemėtvarkos planavimo dokumentų rengimo informacinės sistemos;
- 112.32. Centrinės viešųjų pirkimų informacinės sistemos;
- 112.33. Gyvenamosios vietos deklaravimo informacinės sistemos (GVDIS);
- 112.34. Lietuvos Respublikos gyventojų registro;
- 112.35. Lietuvos Respublikos juridinių asmenų registro;
- 112.36. Neveiksnių ir ribotai veikusių asmenų registro;
- 112.37. Žemėtvarkos planavimo dokumentų rengimo informacinės sistemos (ŽPDRIS);
- 112.38. Lietuvos užimtumo tarnybos informacinės sistemos.



#### **XIV SKYRIUS BAIGIAMOSIOS NUOSTATOS**

113. Darbuotojai, kurie yra įgalioti tvarkyti asmens duomenis arba eidami savo pareigas juos sužino, privalo laikytis šių Taisyklių, pagrindinių asmens duomenų tvarkymo reikalavimų ir konfidencialumo ir saugumo reikalavimų, įtvirtintų teisės aktuose ir šiose Taisyklėse. Už Taisyklių nuostatų pažeidimą darbuotojai atsako teisės aktų nustatyta tvarka.

114. Darbuotojai, pasikeitus jų asmens duomenims, informuoja apie tai Vidaus administravimo skyrių, kuris patikslina ir atnaujina darbuotojų asmens duomenis bylose ir tam skirtose duomenų bazėse.

115. Taisyklės įsigalioja jas patvirtinus Administracijos direktoriui.

116. Patvirtinus ar pakeitus Taisyklės, darbuotojai su jomis supažindinami Panevėžio miesto savivaldybės administracijos darbo tvarkos taisyklėse numatyta tvarka.

117. Taisyklės skelbiamos Panevėžio miesto savivaldybės interneto svetainėje skiltyje „Asmens duomenų apsauga“.

118. Taisyklės peržiūrimos ir, reikalui esant, atnaujinamos pasikeitus asmens duomenų apsaugą reglamentuojantiems teisės aktams ar jų įgyvendinimo praktikai, taip pat pasikeitus Duomenų valdytojo atliekamam asmens duomenų tvarkymui, bet ne rečiau kaip kartą per dvejus metus.

119. Keičiantis teisės aktams, Administracija esant poreikiui gali sudaryti sutartis dėl duomenų teikimo ir (ar) gavimo iš kitų informacinių sistemų ir registru.

120. Administracijos veiksmai ar neveikimas, kuriais pažeidžiami teisės aktai, reglamentuojantys asmens duomenų tvarkymą ir apsaugą, gali būti skundžiami Valstybinei duomenų apsaugos inspekcijai (L. Sapiegos g. 17, Vilnius, el. paštas [ada@ada.lt](mailto:ada@ada.lt), interneto svetainė [www.vdai.lrv.lt](http://www.vdai.lrv.lt)), Vyriausiajai administracinių ginčų komisijai ir teismams Lietuvos Respublikos teisės aktų nustatyta tvarka.

---