Priedas Nr. 1

PATVIRTINTA
VšĮ Klaipėdos greitosios medicininės
pagalbos stoties vyriausiojo gydytojo
2020 m. vasario 18 d. įsakymu Nr. 6 V/1.1

VIEŠOSIOS ĮSTAIGOS KLAIPĖDOS GREITOSIOS MEDICININĖS PAGALBOS STOTIES ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Viešosios įstaigos Klaipėdos greitosios medicininės pagalbos stoties (toliau – Įstaiga) asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) reguliuoja fizinių asmenų (toliau – Duomenų subjektas) asmens duomenų tvarkymo tikslus; duomenų apsaugos pareigūno teises ir pareigas; asmens duomenų saugumo pažeidimų valdymo ir reagavimo į šiuos pažeidimus tvarka; įtvirtina organizacines ir technines duomenų apsaugos priemones; reguliuoja asmens duomenų tvarkytojo pasitelkimo atvejus.

2. Šios Taisyklės parengtos remiantis:

2.1. ES Bendruoju duomenų apsaugos reglamentu (toliau - Reglamentas);

2.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – ADTAĮ);

2.3. Lietuvos Respublikos sveikatos sistemos įstatymu;

2.4. Lietuvos Respublikos sveikatos priežiūros įstaigų įstatymu;

2.5. kitais teisės aktais, susijusiais su asmens duomenų tvarkymu ir apsauga.

3. Taisyklėse vartojamos sąvokos atitinka ADTAĮ ir Reglamento vartojamas sąvokas. Taisyklių nuostatos negali plėsti ar siaurinti ADTAĮ taikymo srities bei prieštarauti ADTAĮ ir Reglamento nustatytiems asmens duomenų tvarkymo reikalavimams ir kitiems asmens duomenų tvarkymą reglamentuojantiems teisės aktams.

4. Šios Taisyklės taikomos tvarkant Duomenų subjekto duomenis automatiniu būdu, taip pat ir neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: pacientų medicininių dokumentų formas, sąrašus, kartotekas, bylas, sąvadus ir kita.

5. Šių Taisyklių reikalavimai privalomi visiems Įstaigos darbuotojams (toliau – Darbuotojai), kurie tvarko Įstaigoje esančius asmens duomenis arba eidami savo pareigas juos sužino. Šių Taisyklių taip pat privalo laikytis duomenų tvarkytojai, kurie teikdami Įstaigai duomenų tvarkymo paslaugas, sužino ir tvarko asmens duomenis.

6. Duomenų valdytojas – VšĮ Klaipėdos greitosios medicininės pagalbos stotis, 190470591, Jurginų g. 33, LT-91206 Klaipėda.

7. Duomenų valdytojas gali pasitelkti duomenų tvarkytoją tvarkyti asmens duomenims.

II SKYRIUS ASMENS DUOMENŲ TVARKYMO PRINCIPAI IR TIKSLAI

8. Tvarkant asmens duomenis laikomasi asmens duomenų tvarkymo principų:

8.1. duomenys renkami ir tvarkomi apibrėžtais ir teisėtais tikslais, nustatytais prieš renkant duomenis ir toliau netvarkomi su tais tikslais nesuderinamu būdu (laikomasi tikslo apribojimo principo);

8.2. duomenys tvarkomi turint duomenų subjekto sutikimą, arba vykdant su duomenų subjektu sudarytą sutartį, esant teisėtam interesui, vykdant Duomenų valdytojui taikomą teisinę

prievolę arba remiantis bent vienu kitu teisėtu duomenų tvarkymo pagrindu (laikomasi teisėtumo principo);

8.3. duomenų subjekto atžvilgiu duomenys tvarkomi teisėtu, sąžiningu ir skaidriu būdu (laikomasi teisėtumo, sąžiningumo ir skaidrumo principo);

8.4. duomenys tvarkomi tikslūs ir, jei reikia dėl duomenų tvarkymo, nuolat atnaujinami; netikslūs ar neišsamūs duomenys ištaisomi, papildomi, sunaikinami arba sustabdomas jų tvarkymas, imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi (laikomasi tikslumo principo);

8.5. tvarkomi adekvatūs, tinkami ir tik tokie duomenys, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (laikomasi duomenų kiekio mažinimo principo);

8.6. duomenys saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia pasiekti tiems tikslams, dėl kurių šie duomenys buvo surinkti ir yra tvarkomi (laikomasi saugojimo trukmės apribojimo principo);

8.7. duomenys tvarkomi tokiu būdu, kad taikant atitinkamas technines ar 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 (laikomasi vientisumo ir konfidencialumo principo).

9. Duomenų valdytojas ir tvarkytojas taip pat laikosi pritaikytosios ir standartizuotos duomenų apsaugos principų.

10. Siekiant laikytis pritaikytosios asmens duomenų apsaugos reikalavimo, tiek nustatant duomenų tvarkymo priemones, tiek paties duomenų tvarkymo metu, duomenų valdytojas ir tvarkytojas privalo taikyti tinkamas technines ir organizacines priemones, kuriomis įgyvendinami duomenų apsaugos principai ir į duomenų tvarkymą yra integruojamos apsaugos priemonės, kurių tikslas yra atitikti Reglamento reikalavimus ir apsaugoti duomenų subjektų teises.

11. Siekiant laikytis standartizuotosios duomenų apsaugos reikalavimo, duomenų valdytojas ir tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kuriomis užtikrina, kad standartizuotai būtų tvarkomi tik tie asmens duomenys, kurie yra būtini kiekvienam konkrečiam duomenų tvarkymo tikslui atlikti, ir tokiomis priemonėmis visų pirma būtų užtikrinama, kad standartizuotai, be fizinio asmens įsikišimo, su asmens duomenimis negalėtų susipažinti neribotas fizinių asmenų skaičius.

12. Už kiekvienos naujos ar esamos 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.

13. Jeigu pokyčiai apima naujų technologijų naudojimą arba yra pagrindo manyti, kad pokyčiai gali kelti fizinių asmenų teisėms ir laisvėms didelį pavojų, atliekamas poveikio duomenų apsaugai vertinimas.

14. Nauja veikla ar esamos veiklos pokyčiai, kurie susiję su asmens duomenimis, nėra pradedami teikti tol, kol nėra įvertinta jų atitiktis Reglamento reikalavimams arba, kai to reikia, nėra atliktas poveikio duomenų apsaugai vertinimas.

15. Duomenų valdytojo ir tvarkytojo darbuotojai savo kompetencijos ribose tvarkydami asmens duomenis privalo užtikrinti, kad principų, išvardintų šiame skyriuje, būtų laikomasi.

16. Įstaigos Duomenų subjektų asmens duomenys tvarkomi būtinosios medicinos pagalbos paslaugų teikimo tikslu; vidaus administravimo tikslu; įstaigos turto saugumo užtikrinimo tikslais.

17. Už Duomenų subjektų duomenų atnaujinimą atsako Įstaigos darbuotojai, Įstaigos vadovo įgalioti tvarkyti Duomenų subjektų duomenis.

III SKYRIUS
DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

18. Duomenų valdytojas ir tvarkytojas veda asmens duomenų tvarkymo veiklos, už kurią jis atsako, įrašus, kuriuose turi būti pateikiama bei nuolatos atnaujinama toliau išvardinta faktinė informacija apie asmens duomenų tvarkymą:

18.1.duomenų valdytojo ir duomenų apsaugos pareigūno vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;

18.2. duomenų tvarkymo tikslai;

18.3. duomenų subjektų kategorijų ir asmens duomenų kategorijų aprašymas;

18.4. duomenų gavėjų, kuriems atskleisti asmens duomenys, įskaitant duomenų gavėjus trečiosiose valstybėse, kategorijos;

18.5. kai taikoma, asmens duomenų perdavimai į trečiąją valstybę, įskaitant tos trečiosios valstybės pavadinimą, ir privalomi tinkamų apsaugos priemonių dokumentai;

18.6. duomenų saugojimo terminai;

18.7. kai įmanoma, bendras techninių ir organizacinių saugumo priemonių aprašymas.

19. Duomenų tvarkymo veiklos įrašai yra tvarkomi raštu. Rašytinei formai yra prilyginama ir elektroninė forma, saugoma kompiuteryje.

20. Duomenų tvarkymo veiklos įrašų sąrašas yra nuolat, bet ne rečiau kaip kartą per kalendorinius metus, tikrinamas ir atnaujinamas, kad atitiktų realią asmens duomenų tvarkymo situaciją Įstaigoje.

IV SKYRIUS
DUOMENŲ TVARKYTOJAI IR GAVĖJAI

21. Duomenų tvarkytojai pasitelkiami ir teisė tvarkyti asmens duomenis jiems suteikiama laikantis šių taisyklių:

21.1. Duomenų valdytojas gali įgalioti asmens duomenis tvarkyti duomenų tvarkytojus, t. y. informacinių technologijų, ryšių ir kitokių paslaugų teikėjus, patarėjus, konsultantus, ir kitus, kurie asmens duomenų netvarko savarankiškais tikslais, o teikdami paslaugas turi prieigą prie asmens duomenų ir juos tvarko Duomenų valdytojo nustatytais tikslais bei pagal jo nurodymus, tiek, kiek tai būtina paslaugai suteikti.

21.1. Duomenų valdytojas pasitelkia tokius duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, jog duomenų tvarkymas atitiktų Reglamento reikalavimus ir būtų užtikrinta tinkama duomenų subjekto teisių apsauga.

21.1. Prieš duomenų tvarkytojams suteikiant prieigą prie asmens duomenų, su duomenų tvarkytojais Duomenų valdytojas sudaro rašytines sutartis, kuriose turi būti numatoma, kad duomenų tvarkytojai duomenis tvarko tik pagal Duomenų valdytojo nurodymus. Į duomenų tvarkymo sutartis taip pat įtraukiamos kitos pagal Reglamentą privalomos nuostatos.

22. Duomenų gavėjams asmens duomenys teikiami laikantis šių taisyklių:

22.1. Duomenų valdytojo tvarkomi duomenys duomenų gavėjams, kurie po duomenų perdavimo asmens duomenis tvarko savarankiškais tikslais, o ne pagal Duomenų valdytojo nurodymus, teikiami tokią pareigą teikti duomenis numatant teisės aktui, esant duomenų subjekto sutikimui arba kitam teisėto duomenų teikimo (tvarkymo) pagrindui.

22.2. Duomenų teikimas duomenų gavėjui turi būti būtinas siekiant pasiekti duomenų tvarkymo tikslui, nustatytam prieš renkant duomenis, arba turi egzistuoti tinkamas teisinis pagrindas duomenis tvarkyti ir teikti nauju tikslu.

22.3. Prieš tiekiant asmens duomenis duomenų gavėjui, Įstaiga apsvarstys reikalingumą su juo pasirašyti duomenų teikimo sutartį, kurioje būtų įvardinamas duomenų teikimo tikslas ir teisinis pagrindas, aprašomi teikiami duomenys, šalių atsakomybė. Jeigu duomenų teikimas yra vienkartinis, minėta informacija gali būti įtraukta į duomenų gavėjo prašymą, skirtą Įstaigai.

22.4. Nesant teisinio pagrindo teikti Įstaigos tvarkomus duomenis, apie tai informuojamas duomenų prašantis asmuo ar institucija.

23. Duomenų valdytojo tvarkomi duomenys duomenų gavėjams už Europos ekonominės erdvės ribų teikiami, taip pat duomenų tvarkytojai pasitelkiami tik užtikrinus tinkamą duomenų teisinės apsaugos lygį ir, jeigu nėra kito pagrindo, gavus Valstybinės duomenų apsaugos inspekcijos leidimą.

V SKYRIUS
DUOMENŲ SUBJEKTO TEISĖS IR JŲ ĮGYVENDINIMAS

24. Duomenų subjekto teisės įgyvendinamos kaip tai numato Įstaigos asmens duomenų subjekto teisių įgyvendinimo tvarkos aprašas.

VI SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS IR IŠANKSTINĖS KONSULTACIJOS

25. Tais atvejais, kai fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus bei esant kitiems teisiniams pagrindams, prieš pradėdamas tvarkyti asmens duomenis Duomenų valdytojas ir tvarkytojas atlieka numatytų duomenų tvarkymo operacijų poveikio asmens duomenų apsaugai vertinimą. Panašių didelį pavojų keliančių duomenų tvarkymo operacijų sekai išnagrinėti gali būti atliekamas vienas vertinimas.

26. Pagal teisės aktus privaloma informacija ir poveikio vertinimo išvados pateikiamos ataskaitoje, kurią pasirašo Įstaigos vadovas arba kitas už duomenų apsaugą atsakingas asmuo.

27. Prireikus duomenų valdytojas ir tvarkytojas atlieka peržiūrą, kad įvertintų, ar asmens duomenys tvarkomi laikantis poveikio duomenų apsaugai vertinimo, bent tais atvejais, kai pakinta tvarkymo operacijų keliamas pavojus.

28. Duomenų valdytojas ir tvarkytojas, prieš pradėdamas tvarkyti duomenis, konsultuojasi su Valstybine duomenų apsaugos inspekcija, jeigu poveikio duomenų apsaugai vertinime nurodyta, kad tvarkant asmens duomenis kiltų didelis pavojus ir duomenų valdytojas ar tvarkytojas nesiimtų priemonių pavojui sumažinti.

VII SKYRIUS
DUOMENŲ APSAUGOS PAREIGŪNAS

29. Duomenų valdytojas ir tvarkytojas paskiria duomenų apsaugos pareigūną, kai:

29.1. duomenis tvarko valdžios institucija ar įstaiga;

29.2. duomenų valdytojo arba tvarkytojo pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus;

29.3. duomenų valdytojo arba tvarkytojo pagrindinė veikla yra specialių kategorijų duomenų tvarkymas dideliu mastu.

30. Asmens duomenų pareigūnas atsakingas už vykdomą duomenų tvarkymo veiklą savo kompetencijos ribose.

31. Duomenų apsaugos pareigūno teisės ir pareigos:

31.1. privalo turėti asmens duomenų apsaugos teisės ir praktikos žinių;

31.2. turi teisę įsitraukti į visus su asmens duomenų apsauga ir privatumu susijusių klausimų nagrinėjimą Įstaigoje;

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

31.4. turi teisę gauti reikiamus išteklius bei galimybę tobulinti duomenų apsaugos ir praktikos žinias;

31.5. atsako už duomenų tvarkymo veiklos įrašų parengimą;

31.6. sprendžia dėl poreikio atlikti poveikio duomenų apsaugai vertinimą ir prireikus jį atlieka;

31.7. prireikus, kreiptis į Valstybinę duomenų apsaugos inspekciją dėl išankstinių konsultacijų;

31.8. vykdo kitas teisės aktuose priskirtas pareigas.

32. Duomenų apsaugos pareigūnas privalo vykdyti šias užduotis:

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

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

32.3. įvykus asmens duomenų incidentui imasi įmanomų priemonių siekiant atstatyti prarastus asmens duomenis ir (ar) sumažinti incidentu asmens duomenims padarytą žalą;

32.4. nustatytais atvejais apie įvykusį asmens duomenų incidentą praneša Duomenų subjektui ir Valstybinei duomenų apsaugos inspekcijai;

32.5. informuoti vadovą apie bet kokius pažeidimus asmens duomenų apsaugos srityje, kuriuos duomenų apsaugos pareigūnas nustato vykdydamas savo funkcijas;

32.6. konsultuoti darbuotojus, dirbančius su asmens duomenimis, asmens duomenų apsaugos klausimais;

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

32.8. duomenų apsaugos pareigūno kontaktiniai duomenys skelbiami Įstaigos interneto svetainėje;

32.9. vykdo kitas teisės aktuose priskirtas užduotis.

VIII SKYRIUS
ORGANIZACINĖS IR TECHNINĖS ASMENS DUOMENŲ APSAUGOS PRIEMONĖS

33. Organizacinės ir techninės duomenų saugumo priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką.

34. Duomenų valdytojams ir tvarkytojams taikomos minimalios organizacinės duomenų saugumo priemonės:

34.1. užtikrinti, kad prie asmens duomenų prieigą turėtų tik įgalioti asmenys, įgaliotiems veiksmams atlikti, tokia apimtimi, kokia yra būtina darbo funkcijoms vykdyti;

34.2. turėti IT išteklių, naudojamų asmens duomenims tvarkyti, registrą (techninės, programinės ir tinklo įrangos). Registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz. tarnybinę stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę);

34.3. programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų naudojamų tvarkant asmens duomenis. Testuojant sistemas turi būti naudojami tęstiniai duomenys;

34.4. duomenų valdytojas pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina tinkamų techninių ir organizacinių priemonių įgyvendinimą tokiu būdu, kad duomenų tvarkymas atitiktų Reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga. Duomenų tvarkytojas turi veikti pagal sutartį ar kitą teisės aktą;

34.5. nustatyti reagavimo į incidentus tvarka. Apie asmens duomenų pažeidimus turi būti nedelsiant pranešama duomenų apsaugos pareigūnui ir Įstaigos vadovui. Turi būti nustatyta pranešimo apie pažeidimus kompetentingoms institucijoms, tarp jų ir Valstybinei duomenų apsaugos inspekcijai, bei duomenų subjektams tvarka;

34.6. nustatyti pagrindines procedūras, kurių reikia laikytis incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas;

34.7. užtikrinti, kad visi darbuotojai suprastų savo atsakomybes ir įsipareigojimus, susijusius su asmens duomenų tvarkymu;

34.8. rengti reguliarius duomenų apsaugos mokymus darbuotojams.

35. Duomenų valdytojams ir tvarkytojams taikomos minimalios techninės duomenų saugumo priemonės:

35.1. turi būti įdiegta ir įgyvendinta bei visiems IT sistemos naudotojams taikoma prieigų kontrolės sistema. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras. Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas. Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio;

35.2. techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, taikomajai programai, naudojamai asmens duomenų apdorojimui. Techniniuose žurnaluose turi būti matomi visi įmanomi prieigų prie asmens duomenų įrašų tipai (pvz., data, laikas, peržiūrėjimas, keitimas, panaikinimas). Saugojimo terminas: ne mažiau kaip 6 mėnesiai. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį;

35.3. duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų korektiškai ir naudotų atskirą paskyrą su priskirtomis žemiausiomis operacinės sistemos privilegijomis. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi apdoroti tik tuos asmens duomenis, kurie yra reikalingi darbui, atitinkančiam duomenų apdorojimo tikslus;

35.4. naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti saugos nustatymų. Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti atnaujinamos ne rečiau kaip kas savaitę. Naudotojams negalima turėti privilegijų diegti, šalinti, administruoti neautorizuotos programinės įrangos. IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam, neveiksniam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Neaktyvios sesijos laikas: ne daugiau kaip 15 min. Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant;

35.5. kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS, SSL);

35.6. atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų. Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą, išsamumą. Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Rekomenduojamas atsarginių kopijų darymo dažnumas*:* kasdien – pridedamoji kopija kas savaitę – pilna kopija;

35.7. mobilieji, nešiojami įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti. Mobilieji įrenginiai turi būti adekvataus prieigos kontrolės lygio, kaip ir kita naudojama įranga asmens duomenims apdoroti. Mobiliuosiuose įrenginiuose informacija šifruojama ar apsaugoma tokiomis priemonėmis, kurios atitiktų Asmens duomenų atskleidimo keliamą riziką;

35.8. informacinėse sistemose naudojama programinė įranga (asmens duomenims apdoroti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus;

35.9. prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Tais atvejais, kai to padaryti neįmanoma (pvz., CD, DVD laikmenos ir pan.), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti. Popierius ir nešiojamos duomenų laikmenos, kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinami tam skirtais smulkintuvais;

35.10. turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.

IX SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO IR REAGAVIMO Į ŠIUOS PAŽEIDIMUS TVARKA

36. Duomenų valdytojas ir tvarkytojas užtikrina tinkamą asmens duomenų saugumo pažeidimų nustatymą, pašalinimą bei prevenciją.

37. Asmens duomenų saugumo pažeidimu laikomas saugumo pažeidimas, dėl kurio:

37.1. sunaikinami, prarandami, pakeičiami asmens duomenys;

37.2. be leidimo atskleidžiami asmens duomenys;

37.3. be leidimo darbuotojai ar trečiosios šalys, neturintys tam teisės, gauna prieigą prie asmens duomenų.

38. Darbuotojas, pastebėjęs asmens duomenų saugumo pažeidimą, privalo nedelsiant pranešti apie jį už duomenų apsaugą atsakingam asmeniui.

39. Atlikęs pirminį asmens duomenų saugumo pažeidimo įvertinimą už asmens duomenų apsaugą atsakingas asmuo, atsižvelgdamas į pažeidimo rimtumą ir galimą poveikį asmens duomenų subjekto teisėms:

39.1. jeigu būtina - suformuoja pažeidimo tyrimo bei padarinių šalinimo komandą;

39.2. imasi visų reikiamų priemonių siekiant pašalinti asmens duomenų saugumo pažeidimo padarinius ir sumažinti padarytą žalą;

39.3. jeigu tam egzistuoja teisinis pagrindas, kreipiasi į atsakingas valstybės institucijas;

39.4. imasi prevencinių priemonių tokiems patiems ar panašiems asmens duomenų saugumo pažeidimams ateityje išvengti.

40. Asmens duomenų saugumo pažeidimai turi būti dokumentuojami.

41. Apie asmens duomenų saugumo pažeidimą, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai apie jį buvo sužinota, turi būti pranešta Valstybinei duomenų apsaugos inspekcijai, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms.

42. Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, apie pažeidimą pranešama duomenų subjektams.

X SKYRIUS
BAIGIAMOSIOS NUOSTATOS

43. Darbuotojai, kurie yra įgalioti tvarkyti asmens duomenis arba eidami savo pareigas juos sužino, privalo laikytis šių Taisyklių, pagrindinių asmens duomenų tvarkymo reikalavimų bei konfidencialumo ir saugumo reikalavimų, įtvirtintų Reglamente ir šiose Taisyklėse.

44. Patvirtinus Taisykles, darbuotojai su jomis supažindinami pasirašytinai. Priėmus naują darbuotoją, jis su Taisyklėmis privalo būti supažindintas pirmąją jo darbo dieną.

45. Įstaiga užtikrina savo darbuotojų, kuriems suteikta teisė tvarkyti asmens duomenis, mokymus.

46. Šios Taisyklės atnaujinamos (peržiūrimos, keičiamos, papildomos, rengiamos naujos)
ne rečiau kaip kartą per metu arba pasikeitus teisės aktams, kurie reglamentuoja asmens duomenų tvarkymą.

47. Šias Taisykles pažeidę asmenys atsako Lietuvos Respublikos teisės aktu nustatyta tvarka.