PATVIRTINTA
Greitosios medicinos pagalbos
tarnybos generalinio direktoriaus
2024 m. vasario 20 d.
įsakymu Nr. V-79
(Greitosios medicinos pagalbos
tarnybos generalinio direktoriaus
2025 m. gegužės 27 d.
įsakymo Nr. V-206 redakcija)

ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. **Greitosios medicinos pagalbos tarnyboje** (toliau – GMP tarnyba) Asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) reguliuoja fizinių asmenų, kurių duomenis tvarko GMP tarnyba, Asmens duomenų tvarkymo tikslus, nustato jų teisių įgyvendinimo tvarką, numato pagrindines asmens duomenų tvarkymo ir asmens duomenų saugos organizacines priemones.

2. Taisyklių privalo laikytis visi GMP tarnybos darbuotojai, savanoriai, praktikantai, stažuotojai (toliau – darbuotojas, darbuotojai), taip pat kiti asmenys, kurie, tvarkydami asmens duomenis GMP tarnyboje ir (arba) eidami savo pareigas, sužino asmens duomenis arba turi bet kokio pobūdžio prieigą prie asmens duomenų ir yra atsakingas už šių Taisyklių laikymąsi ir įgyvendinimą, o asmeninė atsakomybė taikoma teisės aktų nustatyta tvarka.

3. Taikomos sąvokos:

3.1. **ADTAĮ** – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

3.2. **Asmens duomenys** – GMP tarnybos tvarkoma informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (asmens duomenų subjektas), gauta iš jo paties ar kitų duomenų valdytojų. Tai gali būti duomenų subjekto vardas, pavardė, asmens kodas, kontaktinė informacija, adresas, gyvenimo aprašymas, GMP tarnybos administracijos darbuotojų organizuotų posėdžių, kuriuose dalyvauja duomenų subjektas, garso įrašai, paciento sveikatos duomenys teikiant būtinąją medicininę pagalbą, teisėto darbo su vaikais GMP tarnybos darbuotojų QR kodų rinkimas, pacientų ir (arba) GMP tarnybos darbuotojų vaizdo ir (arba) garso stebėjimas ir (arba) įrašymas mobiliais vaizdo stebėjimo įrenginiais, specializuotame transporte įdiegta automatizuota duomenų rinkimo ir stebėjimo sistema ar eismo stebėjimas vaizdo registratoriais, GMP tarnybos patalpų ir teritorijos vaizdo stebėjimo metu užfiksuota informacija, ir bet kuri kita duomenų subjektą identifikuoti leidžianti asmeninė informacija, kurią GMP tarnyba tvarko vykdydama savo veiklas (sąrašas nėra baigtinis).

3.3. **Asmens duomenis tvarkantis darbuotojas** – tai bet kuris GMP tarnybos darbuotojas, tvarkantis asmens duomenis, šiame procese atsakingas už duomenų subjektų informavimą apie duomenų subjekto tvarkomus duomenis, už duomenų subjekto sutikimo dėl asmens duomenų tvarkymo gavimą (kai taikoma), už informacijos, susijusios su asmens duomenimis, pateikimą duomenų apsaugos pareigūnui, už asmens duomenų subjektų prašymų įgyvendinimą.

3.4. **Asmens duomenų tvarkytojas** – GMP tarnybai nepavaldi trečioji šalis, kuri tvarko asmens duomenis tik duomenų valdytojo vardu (duomenų tvarkytojo pareigos duomenų valdytojo atžvilgiu nustatomos sutartimi, įgaliojimu, įstatymu ar kitu teisės aktu).

3.5. **Asmens duomenų tvarkymas** – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais GMP tarnyboje atliekama operacija ar operacijų seka (rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.

3.6. **Asmens duomenų tvarkymas automatizuotu būdu** – duomenų tvarkymo veiksmai, visiškai ar iš dalies atliekami automatinėmis priemonėmis t. y. informacinėmis sistemomis ar elektroninėmis priemonėmis, pavyzdžiui, kompiuteriais, planšetėmis, mobiliaisias telefonais, vaizdo kameromis, fotoaparatais, pokalbio įrašymo funkciją turinčia programine įranga ir kita įranga leidžianti automatizuotai rinkti, saugoti, analizuoti ir perduoti duomenis be tiesioginio žmogaus įsikišimo arba su minimalia priežiūra.

3.7. **Asmens duomenų gavėjas** – fizinis arba juridinis asmuo, valstybės institucija ar įstaiga, kuriai pagal pagrįstą prašymą pateikiami asmens duomenys, įskaitant ir trečiuosius asmenis. Valstybės ir savivaldybių institucijos ir įstaigos nėra laikomi duomenų gavėjais ar trečiaisiais asmenimis, kai šios institucijos ir įstaigos teisės aktų nustatyta tvarka gauna asmens duomenis įstatymų nustatytoms kontrolės funkcijoms atlikti.

3.8. **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų prieigą gauna asmuo, neturintis leidimo. Asmens duomenų saugumo pažeidimai gali būti:

3.8.1. **konfidencialumo pažeidimas** – netyčinis arba neteisėtas asmens duomenų laikinas ar nuolatinis atskleidimas ar prieigos suteikimas asmenims, kurie neturi teisės susipažinti su asmens duomenimis;

3.8.2. **prieinamumo pažeidimas** – netyčinis arba neteisėtas, laikinas ar nuolatinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas;

3.8.3. **vientisumo pažeidimas** – netyčinis arba neteisėtas asmens duomenų laikinas ar nuolatinis pakeitimas.

3.9. **Duomenų subjektas** – bet kuris fizinis asmuo, kurio asmens duomenys tvarkomi.

3.10. **Duomenų valdytojas** – GMP tarnyba, tvarkanti asmens duomenis (pvz. pacientų) automatiniu būdu (informacinių technologijų priemonėmis) ar neautomatiniu būdu susistemintose rinkmenose (pvz. popierinėse darbuotojų asmens bylose ir pan.).

3.11. **Duomenų tvarkytojas** – GMP tarnyba arba bet kuris juridinis ar fizinis asmuo, duomenų valdytojo įgaliota tvarkyti asmens duomenis.

3.12. **GMP** – greitosios medicinos pagalba.

3.13. **GMP brigada** – greitosios medicinos pagalbos paslaugas teikianti brigada.

3.14. **PDAV** – poveikio duomenų apsaugai vertinimas.

3.15. **Pavojus fizinių asmenų teisėms bei laisvėms** – situacija, kai dėl duomenų tvarkymo arba dėl galimo duomenų saugumo pažeidimo duomenų subjektams gali būti sunkiau naudotis savo teisėmis ir laisvėmis, duomenų subjektas gali patirti atskirtį arba diskriminaciją, finansinius nuostolius, gali būti pakenkta jo reputacijai arba atsirasti kitokie rimti padariniai kasdieniam fizinio asmens gyvenimui.

3.16. **Reglamentas** – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmens duomenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas, BDAR).

3.17. **Specialiųjų kategorijų asmens duomenys** – asmens duomenys, susiję su duomenų subjekto sveikata, teistumu, rasine ar etnine kilme, politinėmis pažiūromis, religiniais ar filosofiniais įsitikinimais ar naryste profesinėse sąjungose, lytiniu gyvenimu ir lytine orientacija, taip pat genetiniais duomenimis ir biometriniais duomenis.

3.18. **Trečiasis asmuo** – juridinis ar fizinis asmuo tam tikroms sąlygoms gali turėti prieigą prie asmens duomenų, išskyrus duomenų subjektą, duomenų valdytoją, duomenų tvarkytoją ir asmenis, kurie yra tiesiogiai duomenų valdytojo ar duomenų tvarkytojo įgalioti tvarkyti asmens duomenis.

3.19. Kitos Taisyklėse vartojamos sąvokos suprantamos taip, kaip jas apibrėžia Reglamente ir ADTAĮ.

4. Taisyklės parengtos vadovaujantis Reglamentu, ADTAĮ, 29 straipsnio duomenų apsaugos darbo grupės metodiniais nurodymais, Lietuvos Respublikos sveikatos sistemos įstatymu, Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymu (toliau – Pacientų teisių ir žalos sveikatai atlyginimo įstatymas), Lietuvos Respublikos bendrojo pagalbos centro įstatymu (toliau - Bendrasis pagalbos centro įstatymas), Lietuvos Respublikos kibernetinio saugumo įstatymu (toliau – Kibernetinio saugumo įstatymas), Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu, Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ nuostatomis ir šiuo nutarimu patvirtintais įgyvendinamaisiais teisės aktais, siekiant užtikrinti asmens duomenų saugumą, Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių įstaigų įstatymu, 2024 m. rugpjūčio 13 d. Inspekcijos parengtoms gairėmis „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“, taip pat atsižvelgiant į Lietuvos standartus LST ISO/IEC 27001:2022, LST ISO/IEC 27002:20222 ir kitus teisės aktus reglamentuojančius duomenų saugumą.

II SKYRIUS
ASMENS DUOMENŲ TVARKYMO BENDROSIOS NUOSTATOS

5. GMP tarnyboje asmens duomenys yra tvarkomi vadovaujantis Reglamento (ES) 2016/679 5 straipsnio 1 dalyje nustatytų teisėtumo, sąžiningumo ir skaidrumo, tikslo apribojimo, duomenų kiekio mažinimo, tikslumo, saugojimo trukmės apribojimo, vientisumo ir konfidencialumo principais.

6. Asmens duomenys gali būti tvarkomi tik tuo tikslu, kuriuo yra renkami. Jeigu asmens duomenys nėra būtini tam, kad būtų pasiektas konkretus tikslas, jie negali būti tvarkomi. Konkrečiam tikslui pasiekti yra tvarkomas kiek įmanoma mažesnis kiekis asmens duomenų. Asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, turi būti nedelsiant ištrinami arba ištaisomi – GMP tarnyba imamasi visų pagrįstų priemonių užtikrinti, kad būtų laikomasi Reglamento 5 straipsnio 1 dalyje nustatytų principų, išimtys taikomos siekiant apsaugoti gyvybinius duomenų subjekto (fizinio asmens) interesus, tai yra būtinosios medicinos pagalbos teikimo tikslu, taip pat GMP tarnybos darbuotojų saugumo tikslu. Asmens duomenys tvarkomi ir saugomi ne ilgiau, negu nustatytas jų saugojimo terminas, kuris turi būti ne ilgesnis, negu yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi.

7. GMP tarnyboje asmens duomenys gali būti tvarkomi jeigu yra bent viena iš Reglamento 6 straipsnio 1 dalyje įtvirtintų teisėto tvarkymo sąlygų ir, jei taikoma, 9 straipsnio 2 dalies sąlygos. Asmens duomenys gali būti teisėtai tvarkomi GMP tarnyboje esant bent vienai iš sąlygų:

7.1. sudaryta sutartis, siekiant sudaryti ar vykdyti darbo, civilinę ar kitokią sutartį su fiziniu asmeniu, įskaitant sutarties sąlygų vykdymą, teisės aktų atitinkamai sutarčiai numatytų

šalių teisių ir pareigų vykdymą ir iš sutarties kylančių šalių įsipareigojimų vykdymą, ir kitas čia nepaminėtas sąlygas;

7.2. teisinė prievolė, GMP tarnyba nacionaliniais teisės aktais įpareigota tvarkyti asmens duomenis teikti greitosios medicinos pagalbos paslaugas, sveikatos priežiūros paslaugos, mokesčių, Sodros, darbo ir kitose srityse;

7.3. tvarkyti asmens duomenis būtina siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus (išsaugoti žmogaus gyvybę);

7.4. tvarkyti asmens duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas (pvz. darbo saugos, pacientų pervežimą tarp gydymo įstaigų, kai tai būtina jų sveikatos būklei);

7.5. teisėto intereso pagrindu, tvarkyti asmens duomenis, kai tai būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai duomenų subjekto teisės ir laisvės yra viršesnės (vaizdo stebėjimas turto ar asmenų saugumui užtikrinti, incidentų tyrimui atlikti, ginčo nagrinėjimo atveju ir pan.). Duomenys galėtų būtų tvarkomi šia teisine sąlyga atlikus GMP tarnybos generalinio direktoriaus įsakymu „Teisėto intereso pusiausvyros (balanso) atlikimo testo, tvarkant asmens duomenis“, patvirtintomis taisyklėmis;

7.6. asmens duomenų tvarkymą GMP tarnybos valdomose informacinėse sistemose reglamentuoja šių informacinių sistemų nuostatai;

7.7. kai asmens duomenys tvarkomi sutikimo pagrindu, kaip nurodyta šių Taisyklių III skyriuje.

8. Asmens duomenys gaunami tiesiogiai iš duomenų subjekto arba oficialiai kreipiantis į reikalingą informaciją tvarkančius ir turinčius teisę ją teikti subjektus, registrus bei informacines sistemas apie tai tinkamai informavus duomenų subjektą.

9. GMP tarnyboje duomenų subjektų asmens duomenys gali būti tvarkomi tik tuo tikslu, kuriuo jie buvo renkami, ir negali būti naudojami su tais tikslais nesuderinamu būdu. Bet koks duomenų tvarkymo nukrypimas nuo pirminio tikslo turi būti pagrįstas teisėtu pagrindu ir atitikti Reglamento (ES) 2016/679 nuostatas. Jei duomenys nėra būtini, jie negali būti renkami, saugomi ar kitaip tvarkomi. GMP tarnybos darbuotojai privalo užtikrinti, kad duomenų kiekis būtų minimalus ir proporcingas siekiamam tikslui.

10. Konkretūs tvarkomi duomenys, jų tvarkymo tikslai, saugojimo terminai ir teisiniai pagrindai yra nurodyti GMP tarnybos veiklos įrašuose, kurie turi atitikti Reglamento (ES) 2016/679 30 straipsnio reikalavimus. GMP tarnybos darbuotojai privalo vadovautis šiais įrašais tvarkydami duomenis, išskyrus atvejus, kai konkrečius asmens duomenų tvarkymo procesus tiesiogiai reglamentuoja galiojantys teisės aktai. Veiklos įrašai tvarkomi vadovaujantis Taisyklių V skyriuje nustatyta tvarka.

11. Asmens duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas GMP tarnyboje tvarkomi pagal generalinio direktoriaus patvirtintą pareigybių sąrašą, sveikatos priežiūros paslaugas vaikams teikiančių darbuotojų teisėto darbo su vaikais (QR) kodo užsakymo ir administravimo tikslu.

12. Darbuotojai prieš kiekvieną asmens duomenų tvarkymo operaciją (veiksmą) privalo įvertinti, ar toks asmens duomenų tvarkymas atitinka Taisyklių 5 ir 6 punktuose įtvirtintus reikalavimus, bei užtikrinti, kad kiekviena duomenų tvarkymo operacija (veiksmas) atitiktų minėtus reikalavimus, taip pat įvertinti, ar toks asmens duomenų tvarkymas turi asmens duomenų tvarkymo pagrindą, bei užtikrinti, kad asmens duomenys nebūtų tvarkomi, jei nėra bent vieno iš minėtų teisinių pagrindų.

13. GMP tarnybos vidaus dokumentuose pildomi duomenų subjektų identifikavimo duomenys, tokie kaip asmens kodas, naudojami tik tuo atveju, jei tai būtina duomenų subjekto tapatybei nustatyti, siekiant teisėto tikslo arba jei to reikalauja galiojantys teisės aktai. Jei tokio pagrindo nėra, šie duomenys nėra naudojami.

14. Pasibaigus asmens duomenų saugojimo terminui, jo pratęsimas galimas, jei GMP tarnyba nustato, kad tolesnis duomenų saugojimas yra būtinas. Toks atvejis galėtų būti, kai asmens duomenys gali būti panaudoti kaip įrodymas ikiteisminiame ar kitokiame tyrime, pacientų teisių ir žalos sveikatai atlyginimo ginčo nagrinėjime, priežiūros institucijos (pvz. Valstybinės duomenų apsaugos inspekcijos (toliau – Inspekcija)) vykdomame tyrime, civilinėje, administracinėje ar baudžiamojoje byloje, arba kitais teisės aktų nustatytais atvejais. Prieš priimant sprendimą pratęsti asmens duomenų saugojimo terminą, GMP tarnyba konsultuojasi su duomenų apsaugos pareigūnu.

15. GMP tarnyboje įgyvendinamos duomenų apsaugos priemonės, kurios užtikrina:

15.1. organizacines kontrolės priemones:

15.1.1. nustato vaidmenys ir atsakomybes;

15.1.2. prieigos valdymą ir teises;

15.1.3. turi IT išteklių registrą;

15.1.4. sudarytos sutartys su duomenų tvarkytojais užtikrina, kad paslaugų teikėjai, kaip duomenų tvarkytojai laikysis visų reikalavimų, taikomų sveikatos priežiūros įstaigoms;

15.1.5. turi saugumo incidentų likvidavimo planą, kuris užtikriną greitą ir veiksmingą incidentų valdymą;

15.1.6. turi veiklos tęstinumo planą, kuriame nurodytos pagrindinės procedūros, kurių reikia laikytis asmens duomenų saugumo pažeidimo atveju.

15.2. darbuotojų kontrolės priemones:

15.2.1. sutartyse su sveikatos priežiūros darbuotojais ar kituose dokumentuose (pvz. pareigybėse) turi būti aiškiai numatyti darbuotojų vaidmenys, atsakomybės, įsipareigojimai susiję su asmens duomenų sauga;

15.2.2. darbuotojai yra susipažinę su GMP tarnyboje taikomomis asmens duomenų saugos taisyklėmis, žinoti kur ir kaip pranešti apie duomenų saugumo pažeidimus, bazines saugos valdymo priemones (pvz. slaptažodžio keitimas, švaraus stalo politiką);

15.2.3. reguliariai mokintis ir išmanyti IT sistemų saugumą, įskaitant ir kibernetinio saugumo reikalavimus;

15.2.4. darbuotojai prieš pradėdami tvarkyti asmens duomenis, turi pasirašyti konfidencialumo ir duomenų neatskleidimo įsipareigojimus.

15.3. fizines kontrolės priemones:

15.3.1. duomenų saugyklos, serverinės ir pan. apsaugoti nuo neautorizuotos prieigos;

15.3.2. taikomos įėjimo valdymo priemonės į pastatus, kurios užtikrintų tik įgalioto personalo įleidimą;

15.3.3. įgyvendinta švaraus stalo ar švaraus ekrano politika.

15.4. technines kontrolės priemones:

15.4.1. personalas, pacientai, įstaigos IS ir duomenų bazių administratoriai, paslaugas teikiančių tiekėjų administratoriai ir programinę įrangą prižiūrintys paslaugų teikėjai turi prieigas tik prie tų duomenų, kurie jiems būtini funkcijoms atlikti, ir būtų identifikuojami rizikos lygį atitinkančiomis priemonėmis, pvz. kelių faktorių autentifikacija, stiprūs ir saugūs slaptažodžiai;

15.4.2. darbuotojams ribojamos teisės IT sistemų nustatymų kompiuterinėse darbo vietose;

15.4.3. kiekviena GMP tarnybos IT sistema, kurioje tvarkomi asmens duomenys būtų įgyvendinta techninių žurnalų įrašai ir stebėsena;

15.4.4. IT sistemų pokyčiai registruojami GMP tarnybos paskirto IT specialisto arba saugos įgaliotinio.

16. Vaidmenys ir atsakomybės:

16.1. Asmens duomenų tvarkymo principų ir duomenų valdytojo pareigų įgyvendinimą užtikrina:

16.1.1 generalinis direktorius priima sprendimus dėl GMP tarnybos departamentų, filialų direktorių, teritorinių skyrių ir struktūrinių padalinių vadovų ir padaliniams nepriskirtų darbuotojų inicijuotų asmens duomenų tvarkymo ir saugumo klausimų, skiria duomenų apsaugos pareigūną, tvirtina su asmens duomenų apsauga susijusias taisykles, tvarkas, aprašus ir kitus susijusius su asmens duomenų apsauga GMP tarnybos dokumentus;

16.1.2. Asmens duomenis tvarkantys darbuotojai asmens duomenis tvarko duomenų valdytojo vardu. Asmens duomenis tvarkantys darbuotojai turi teisę susipažinti, rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip tvarkyti asmens duomenis tik siekdami atlikti savo tiesiogines funkcijas, apibrėžtas pareigybės aprašyme ir struktūrinio padalinio nuostatuose ar vykdydami tiesioginio vadovo arba generalinio direktoriaus pavedimą;

16.1.3. GMP tarnybos darbuotojus atšaukus iš pareigų, darbuotojai tiesioginiam vadovui turi perduoti savo turėtas teises, atsakomybes, prieigas ir informaciją apie jų tvarkomus asmens duomenys arba kaip yra nurodyta struktūrinio padalinio vidaus dokumentuose, tokiu būdu užtikrinant veiklos tęstinumą;

16.1.4. duomenų apsaugos pareigūno vaidmuo nustatytas šių Taisyklių VI skyriuje ir 29 straipsnio duomenų apsaugos darbo grupės Duomenų apsaugos pareigūno gairėse;

16.1.5. saugos įgaliotinio vaidmuo ir atsakomybė nustatyta Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose ir atliekant kitas kibernetinio saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas bei turi atitikti Kibernetinio saugumo įstatymo 15 straipsnio reikalavimus;

16.1.6. GMP tarnyboje IT administratorius atsakingas už techninių ir organizacinių priemonių įgyvendinimą, kad būtų apsaugoti asmens duomenys nuo neteisėtos prieigos, praradimo ar nutekėjimo, užtikrina, kad prie asmens duomenų galėtų prieiti tik įgalioti asmenys, taikydamas autentifikavimo ir autorizacijos mechanizmus, stebi, kaip įstaigoje tvarkomi asmens duomenys, ir užtikrina, kad tai būtų daroma pagal BDAR reikalavimus, reaguoja į duomenų saugumo pažeidimus, vykdo tyrimus ir praneša atsakingoms institucijoms, jei pažeidimas kelia riziką duomenų subjektams, bendradarbiauja su duomenų apsaugos pareigūnu ir padeda įgyvendinti BDAR reikalavimus įstaigoje.

16.1.7. GMP tarnybos Informacinių technologijų skyriaus specialistai yra atsakingi už informacinių technologijų (informacinių sistemų, tarnybinių stočių, kompiuterinių darbo vietų, mobilių/nešiojamų įrenginių, programinės įrangos) išteklių, naudojamų asmens duomenis tvarkyti, priežiūrą.

16.1.8. GMP tarnybos filialų direktoriai, teritorinių skyrių ir struktūrinių padalinių vadovai, bei kiti padaliniams nepriskirti darbuotojai pagal kuruojamas sritis turi šias pareigas:

16.1.8.1 inicijuoja savo vadovaujamo padalinio veiklai reikalingų naujų asmens duomenų tvarkymą ir esamų asmens duomenų inventorizaciją;

16.1.8.2. priima sprendimus dėl duomenų gavimo ir teikimo;

16.1.8.3. įgyvendina nustatytas asmens duomenų saugumo priemones;

16.1.8.4. pagal poreikį inicijuoja duomenų tvarkymo veiklos įrašų atnaujinimą;

16.1.8.5. užtikrina, kai jų pavaldume esantys darbuotojai planuoja vykdyti asmens duomenų tvarkymo operacijas, dėl kurių teisės aktai numato poveikio duomenų apsaugai vertinimą (PDAV), kreiptasi į duomenų apsaugos pareigūną ir gautos jo išvados;

16.1.8.6. organizuoja sutarčių pasirašymą tarp duomenų valdytojo ir duomenų tvarkytojo, kai tai numatyta Reglamente;

16.1.8.7. atsako už tinkamą asmens duomenų tvarkymą ir saugą.

16.1.9. tais atvejais, kai asmens duomenų tvarkymo teisinis pagrindas yra duomenų valdytojo teisėtas interesas, GMP tarnyba privalo atlikti tinkamą vertinimą. Prieš pradėdama

tvarkymo veiklą arba nustatydama, kad ji jau vykdoma pagal Reglamento 6 straipsnio 1 dalies (f) punktą, GMP tarnyba turi įvertinti, ar jos arba trečiosios šalies interesai nėra viršesni už duomenų subjekto teises, laisves ir interesus.

16.1.10. jeigu GMP tarnyba atlikusi Taisyklių 16.1.9. punkte numatytą teisėto intereso įvertinimą, nustato, kad duomenų tvarkymo teisėtumas negali remtis Reglamento 6 straipsnio 1 dalies (f) punktu, neatidėliodama nutraukia tokį duomenų tvarkymą;

16.1.11. darbuotojai, atsakingi už asmens duomenų tvarkymą, atlieka svarbias funkcijas, užtikrinančias duomenų apsaugą ir reglamentavimą, jie:

16.1.11.1 teikia siūlymus kai identifikuojamos problemos, susijusios su duomenų saugumo pažeidimais;

16.1.11.2 užtikrina, kad vidaus dokumentuose ir šiose Taisyklėse nustatytos duomenų tvarkymo priemonės būtų tinkamai taikomos.

III SKYRIUS
REIKALAVIMAI SUTIKIMUI

17. Asmens duomenys sutikimo pagrindu (Reglamento 6 straipsnio 1 dalies a punktas, kai tvarkomi specialių kategorijų duomenys – Reglamento 9 straipsnio 2 dalies a punktas) tvarkomi tik tuo atveju, kai jie yra pagrįstai reikalingi GMP tarnybos vykdomai veiklai ir GMP tarnyba neturi kito teisinio pagrindo tvarkyti asmens duomenis.

18. Pirmenybė teikiama duomenų subjekto sutikimui gautam raštu (įskaitant gautus elektroninėmis priemonėmis), kiti sutikimo būdai gali būti naudojami tik įsitikinus, kad yra įmanoma įrodyti duomenų subjekto sutikimo davimo faktą. Duomenų subjekto tylėjimas, iš anksto pažymėti laukai arba neveikimas, nelaikomi duomenų subjekto sutikimu. Rekomenduojama sutikimo forma yra šių Taisyklių 1 priede.

19. Visais atvejais, kai asmens duomenys tvarkomi duomenų subjekto sutikimo pagrindu, GMP tarnyba privalo saugoti ir turėti įrodymus, kad duomenų subjektas davė sutikimą.

20. Sutikimo pagrindu tvarkomi tik tie asmens duomenys, kurie nurodyti sutikime ir tik nurodytais sutikime tikslais, su jais atliekami tik sutikime nurodyti tvarkymo veiksmai. Jeigu keičiasi tvarkomų duomenų kiekis, tvarkymo tikslas ar tvarkymo veiksmai, privaloma gauti papildomą sutikimą tvarkyti duomenis arba turi būti kitas GMP tarnybos duomenų tvarkymo veiklos įrašuose nustatytas asmens duomenų tvarkymo teisinis pagrindas.

21. Visais atvejais sutikimas turi būti gaunamas prieš atliekant duomenų tvarkymo veiksmus, dėl kurių prašomas sutikimas.

22. Duomenų subjektas turi teisę, bet kuriuo metu atšaukti savo sutikimą. Duomenų subjektui atšaukus sutikimą, draudžiama tvarkyti asmens duomenis tais tikslais ir atlikti duomenų tvarkymo veiksmus, kurie buvo atliekami tokio sutikimo pagrindu, išskyrus atvejus, kai tokiam duomenų tvarkymui yra kitas GMP tarnybos duomenų tvarkymo veiklos įrašuose nustatytas asmens duomenų tvarkymo teisinis pagrindas. Sutikimui atšaukti sudaromos analogiškos sąlygos kaip ir sutikimui duoti, draudžiama apsunkinti ar sudaryti papildomas sąlygas sutikimui atšaukti. Sutikimo atšaukimas negali sukelti duomenų subjektui neigiamų padarinių. Sutikimo atšaukimas nedaro poveikio sutikimu pagrįsto duomenų tvarkymo, atlikto iki sutikimo atšaukimo, teisėtumui. Duomenų subjektas apie šiame punkte nurodytas nuostatas privalo būti informuojamas prieš jam duodant sutikimą.

23. Sutikimas galioja iki jo atšaukimo arba iki jame nurodyto jo galiojimo termino pabaigos.

24. Už duomenų subjektų informavimą atsako GMP tarnybos darbuotojas, kuris renka ir tvarko konkretaus duomenų subjekto duomenis. Dėl sutikimų atitikties Taisyklėse ir

Reglamente nustatytiems reikalavimams tinkamo vykdymo konsultuojamasi su duomenų apsaugos pareigūnu.

IV SKYRIUS
TVARKOMŲ ASMENS DUOMENŲ INVENTORIZACIJA

25. GMP tarnybos struktūriniai padaliniai ir padaliniams nepriskirti darbuotojai, kurie savo veikloje tvarko asmens duomenis, privalo vykdyti tvarkomų asmens duomenų, jų tvarkymo tikslų, teisinio pagrindo ir kitų su struktūrinio padalinio ar padaliniui nepriskirto darbuotojo atliekamu asmens duomenų tvarkymu susijusių veikų nustatymą ir vertinimą – tvarkomų asmens duomenų inventorizaciją (toliau – inventorizacija).

26. Inventorizacijos metu turėtų būti įvertintos visos aplinkybės: kokius asmens duomenis tvarko ar ketina tvarkyti, kokiu būdu (automatizuotu ar neautomatizuotu susistemintose rinkmenose) tvarkomi asmens duomenys, kurie darbuotojai atsakingi ir kokios jų funkcijos tvarkant asmens duomenis, kokios darbuotojų funkcijos ir atsakomybės kibernetinių incidentų ir duomenų saugumo pažeidimų atveju, kur saugomi asmens duomenys ir kokiose laikmenose (debesija, duomenų centrai, aplankai su failais, spintose, kabinetuose ir pan.), koks yra asmens duomenų judėjimas (duomenų srautai įstaigos viduje ir išorėje), ar atliktas techninės ir programinės įrangos inventorizavimas.

27. Inventorizacija atliekama periodiškai, kartą per metus arba pasikeitus GMP tarnybos duomenų tvarkymo procesams ir (ar) asmens duomenų tvarkymą reglamentuojantiems teisės aktams.

28. Labiausiai saugotini asmens duomenys ir jiems reikia taikyti aukščiausias saugumo priemones yra pacientų (specialių kategorijų) sveikatos duomenys.

29. Dėl inventorizacijos atlikimo būdo ir formos konsultuojamasi su duomenų apsaugos pareigūnu.

30. GMP tarnybos struktūrinių padalinių vadovai ir padaliniams nepriskirti darbuotojai, kurie savo veikloje tvarko asmens duomenis, inventorizacijos rezultatus Dokumentų valdymo sistemos (toliau – DVS) priemonėmis teikia susipažinti duomenų apsaugos pareigūnui, o šis juos apibendrina ir išsaugo DVS vidiniuose dokumentuose.

V SKYRIUS
DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

31. GMP tarnyboje duomenų tvarkymo veiklos įrašai pildomi pagal šiose Taisyklėse patvirtintą formą (2 priedas). Visa vykdoma asmens duomenų tvarkymo veikla privalo atitikti duomenų tvarkymo veiklos įrašuose aprašytą veiklą.

32. GMP tarnyboje yra tvarkomi tie asmens duomenys ir tuo tikslu bei tuo teisiniu pagrindu, kurie nurodyti duomenų tvarkymo veiklos įrašuose.

33. Kiekvienas GMP tarnybos struktūrinis padalinys ar padaliniui nepriskirtas darbuotojas, kuris savo veikloje tvarko asmens duomenis, privalo pasirengti duomenų tvarkymo veiklos, už kurią jis atsakingas, įrašus.

34. Duomenų tvarkymo veiklos įrašai pildomi raštu, įskaitant elektronine forma.

35. Duomenų tvarkymo veiklos įraše pateikiama Reglamento 30 straipsnio 1 dalyje nurodyta informacija, kurioje aprašoma GMP tarnybos, kaip duomenų valdytojo, ir Reglamento 30 straipsnio 2 dalyje nurodyta informacija, kurioje aprašoma GMP tarnybos, kaip duomenų tvarkytojos, veikla.

36. Už duomenų tvarkymo veiklos įrašų registravimą atsakingas duomenų apsaugos pareigūnas. Duomenų tvarkymo veiklos įrašai registruojami DVS priemonėmis.

37. Darbuotojai nedelsiant informuoja duomenų apsaugos pareigūną, jeigu GMP tarnybos duomenų tvarkymo veiklos įrašai neatitinka GMP tarnybos realaus poreikio dėl asmens duomenų tvarkymo, pateikdami naują duomenų tvarkymo veiklos įrašu užpildytą formą (2 priedas).

38. Duomenų tvarkymo veiklos įrašų išrašai, gavus prašymą, pateikiami Inspekcijai jos prašyme nurodytais terminais.

39. GMP tarnyboje periodiškai, ne rečiau kaip kartą per metus, tikrinama, ar GMP tarnyboje vykdoma asmens duomenų tvarkymo veikla atitinka duomenų tvarkymo veiklos įrašus. Už šias patikras yra atsakingas duomenų apsaugos pareigūnas, jis gali siūlyti į metinį Vidaus audito skyriaus veiklos planą įtraukti duomenų tvarkymo veiklos įrašų vidaus auditą arba pasitelkti kitus darbuotojus patikrai atlikti. Patikros rezultatai yra įforminami išvada, kurioje nurodoma, ar GMP tarnyboje vykdoma asmens duomenų tvarkymo veikla atitinka duomenų tvarkymo veiklos įrašus, nurodomi trūkumai, jeigu tokie nustatyti, bei rekomendacijos, kaip nustatytus trūkumus ištaisyti.

VI SKYRIUS
DUOMENŲ SUBJEKTŲ INFORMAVIMAS

40. GMP tarnyba privalo informuoti duomenų subjektą apie jo asmens duomenų tvarkymo veiklą. Kai asmens duomenys gaunami iš paties duomenų subjekto, duomenų subjektui pateikiama informacija apie asmens duomenų tvarkymą, nurodyta Reglamento 13 straipsnyje.

41. Taisyklių 40 punkte nurodyta informacija duomenų subjektui pateikiama prieš gaunant asmens duomenis arba asmens duomenų gavimo metu.

42. Taisyklių 40 ir 41 punktai netaikomi, jeigu duomenų subjektas jau turi informaciją apie jo asmens duomenų tvarkymą, ir tokia apimtimi, kiek tos informacijos jis turi.

43. Kai asmens duomenys gaunami ne iš paties duomenų subjekto, GMP tarnyba privalo duomenų subjektui pateikti informaciją apie asmens duomenų tvarkymą, nurodytą Reglamento 14 straipsnyje.

44. Kai asmens duomenys gaunami ne iš paties duomenų subjekto, šių Taisyklių 43 punkte nurodyta informacija duomenų subjektui pateikiama:

44.1. ne vėliau kaip per vieną mėnesį nuo asmens duomenų gavimo;

44.2. jeigu asmens duomenys bus naudojami ryšiams su duomenų subjektu palaikyti, – ne vėliau kaip pirmą kartą susisiekiant su tuo duomenų subjektu;

44.3. jeigu numatoma asmens duomenis atskleisti kitam duomenų gavėjui, – ne vėliau kaip atskleidžiant duomenis pirmą kartą.

45. Taisyklių 43 ir 44 punktai netaikomi, jeigu ir tiek, kiek:

45.1. duomenų subjektas jau turi informaciją;

45.2. tokios informacijos pateikimas yra neįmanomas arba tam reikėtų neproporcingų pastangų, arba jeigu dėl informavimo pareigos gali tapti neįmanoma pasiekti to tvarkymo tikslus arba ji gali labai sukliudyti pasiekti to tvarkymo tikslus. Tokiais atvejais GMP tarnyba imasi tinkamų priemonių duomenų subjekto teisėms ir laisvėms ir teisėtiems interesams apsaugoti, įskaitant viešą informacijos apie asmens duomenų tvarkymą paskelbimą GMP tarnybos interneto svetainės www.greitojipagalba.lt skiltyje „Asmens duomenų apsauga“;

45.3. duomenų gavimas ar atskleidimas aiškiai nustatytas teisės aktuose, kurie taikomi GMP tarnybai;

45.4. kai asmens duomenys privalo išlikti konfidencialūs laikantis teisės aktų reglamentuojamos profesinės paslapties prievolės.

46. Jei GMP tarnyba ketina toliau tvarkyti asmens duomenis kitu tikslu, nei tas, kuriuo asmens duomenys buvo renkami, prieš toliau tvarkydama asmens duomenis GMP tarnyba pateikia duomenų subjektui informaciją apie kitą tikslą ir informaciją.

47. GMP tarnybos struktūriniai padaliniai ir padaliniams nepriskirti darbuotojai, kurie savo veikloje tvarko asmens duomenis, rengia pranešimus dėl privatumo duomenų subjektams, kurių duomenis tvarko atlikdami struktūrinio padalinio nuostatuose ar pareigybės aprašyme nustatytas funkcijas, parengtus pranešimus dėl privatumo teikia susipažinti duomenų apsaugos pareigūnui, o šis juos registruoja vidinių dokumentų registre kartu su duomenų tvarkymo veiklos įrašais arba atskiru registru ir jei reikia, per pateikimus supažindina visus darbuotojus, kuriems privalu gauti informavimą apie jų tvarkomus duomenis.

48. Pranešimai dėl privatumo duomenų subjektams pateikiami juos skelbiant GMP tarnybos interneto svetainės www.greitojipagalba.lt skiltyje „Asmens duomenų apsauga“, polapyje „Informavimas apie tvarkomus asmens duomenis“ taip pat gali būti teikiama elektroniniu paštu, struktūriniuose padaliniuose arba bendruoju kontaktiniu telefonu. Privatumo pranešimai apie GMP tarnybos darbuotojų asmens duomenų tvarkymą darbuotojai supažindinami DVS priemonėmis.

49. Už duomenų subjektų informavimą atsakingas darbuotojas, kuris renka ir tvarko konkretaus duomenų subjekto duomenis. Dėl informavimo pareigos tinkamo vykdymo konsultuojamasi su duomenų apsaugos pareigūnu.

VII SKYRIUS
DUOMENŲ APSAUGOS PAREIGŪNAS

50. GMP tarnybos generalinis direktorius įsakymu paskiria GMP tarnybos duomenų apsaugos pareigūną bei, jam negalint vykdyti funkcijų ir atlikti užduočių, jį pavaduojantį asmenį.

51. GMP tarnybos duomenų apsaugos pareigūno kontaktiniai duomenys (vardas, pavardė, el. pašto adresas ir (ar) telefono ryšio numeris) yra skelbiami GMP tarnyboje taip, kad darbuotojams būtų aišku, jog konkretus asmuo eina duomenų apsaugos pareigūno pareigas. Taip pat pateikiama informacija apie jo funkcijas ir uždavinius. Šie kontaktiniai duomenys pranešami Inspekcijai, nurodomi GMP tarnybos internetinės svetainės www.greitojipagalba.lt skiltyje „Asmens duomenų apsauga“, taip pat Sutikimo dėl asmens duomenų tvarkymo formoje, Informavimo apie asmens duomenų tvarkymą formoje bei kitose vietose, kad suinteresuoti asmenys galėtų be kliūčių susisiekti su duomenų apsaugos pareigūnu.

52. Visi GMP tarnybos darbuotojai privalo bendradarbiauti su duomenų apsaugos pareigūnu, skubiai teikti jo paprašytus dokumentus ir informaciją. Darbuotojai turi palaikyti nuolatinį ryšį su duomenų apsaugos pareigūnu, užtikrindami, kad su jais būtų lengva susisiekti, operatyviai reaguoti į duomenų apsaugos pareigūno užklausas ir sudaryti sąlygas efektyviam funkcijų vykdymui.

VIII SKYRIUS
DUOMENŲ SUBJEKTŲ TEISĖS IR JŲ ĮGYVENDINIMO TVARKA

53. Duomenų subjektas (įskaitant darbuotoją, praktiką atliekantį asmenį, savanorį, stažuotoją, pacientą, klientą ir pan.), kurio asmens duomenys yra tvarkomi GMP tarnyboje, esant nustatytam pagrindui turi teises numatytas Reglamento 12-22 straipsniuose.

54. Duomenų subjektų teisės GMP tarnyboje įgyvendinamos generalinio direktoriaus įsakymu patvirtintose Duomenų subjektų teisių įgyvendinimo taisyklėse nustatyta tvarka.

55. Įgyvendinant duomenų subjekto prašymus informacija teikiama nemokamai, išskyrus atvejus, kai neproporcingai didėlės informacijos apimtys ir administracines išlaidas, gali būti imamas Finansų tarnybos nustatytas mokestis.

56. Duomenų subjektas, jo atstovas arba įgaliota ne pelno įstaiga, organizacija ar asociacija, atitinkanti Reglamento 80 straipsnio reikalavimus, turi teisę skųsti duomenų valdytojo ar (ir) duomenų tvarkytojo veiksmus arba neveikimą, pažeidžiančius Reglamento ir (ar) ADTAĮ nuostatas Inspekcijai, Žurnalistų etikos inspektoriui arba teismui.

IX SKYRIUS
DARBUOTOJŲ ASMENS DUOMENŲ TVARKYMO YPATUMAI

57. GMP tarnyboje gali būti tvarkomi tik tie darbuotojų asmens duomenys, kurie yra būtini darbo teisiniams santykiams įgyvendinti, GMP tarnybos teisės aktuose nustatytoms teisinėms prievolėms vykdyti ar konkrečiam teisėtam GMP tarnybos interesui apsaugoti. Darbuotojų asmens duomenų tvarkymo tikslai nustatyti asmens duomenų tvarkymo veiklos įrašuose. Sutikimas kaip teisėtas duomenų tvarkymo pagrindas gali būti taikomas tik tuo atveju, jei yra užtikrinta, kad įgyvendinti šių Taisyklių nustatyti reikalavimai.

58. Kandidato dirbti pagal darbo sutartį GMP tarnyboje (toliau – kandidatas) asmens duomenis, susijusius su kvalifikacija, profesiniais gebėjimais ir dalykinėmis savybėmis, galima rinkti iš buvusio darbdavio/valstybės ir savivaldybių įstaigų, kurioje kandidatas dirbo pagal darbo sutartį, prieš tai informavus kandidatą, o iš esamo darbdavio/valstybės ir savivaldybės įstaigos, kurioje kandidatas eina pareigas ar dirba pagal darbo sutartį, – tik kandidato sutikimu.

59. Viešai prieinami asmens duomenys apie kandidatus ar darbuotojus gali būti renkami tik tiek ir tik tokia apimtimi, kiek tie asmens duomenys yra tiesiogiai reikalingi ir aktualūs darbo pareigoms užimti ir funkcijoms vykdyti. Apie šią galimybę kandidatai yra informuojami darbo skelbimo pranešime.

60. Neatrinkto kandidato asmens duomenys saugomi ne ilgiau nei 12 mėnesių nuo momento, kai kandidatui buvo pranešta, kad su juo nebus sudaryta darbo sutartis. Ilgesnį terminą tokie asmens duomenys gali būti saugomi tik tada, jeigu yra gaunamas kandidato sutikimas, atitinkantis Taisyklėse įtvirtintus reikalavimus, arba atsiranda kitas teisinis pagrindas ilgiau saugoti duomenis.

61. Darbuotojai ir kiti asmenys turi būti supažindinti su GMP tarnybos informacinių technologijų naudojimo tvarkos aprašais prieš pradedant dirbti su suteikiamomis informacinėmis technologijomis.

62. Pasibaigus darbo santykiams, nauji duomenys apie darbuotoją gali būti renkami tik esant teisiniam pagrindui ir tik tiek, kiek jie yra susiję ir būtini remiantis konkrečiu teisiniu pagrindu pagrįstam tikslui pasiekti. Apie tokį duomenų rinkimą darbuotojai yra informuojami pateikiant Informavimą apie asmens duomenų tvarkymą.

63. Atsižvelgiant į darbuotojų pareigas, GMP tarnyba suteikia darbuotojams šias darbo priemones: medicininę įrangą ir medicinines priemones, GMP specializuotą transportą su įranga, radijo ryšio ir navigacijos įrangą, kompiuterių techninę įrangą, planšetes, judriojo ryšio telefono aparatus su SIM kortele, fiksuoto ryšio telefono aparatus (jei reikia), prieigas prie interneto, prie darbinio elektroninio pašto, prie DVS, pagal vykdomas funkcijas – prieigas prie Greitosios medicinos pagalbos informacinės sistemos bei prie kitų informacinių sistemų, kurių duomenų valdytoją ir (ar) duomenų tvarkytoją – GMP tarnyba.

64. Darbuotojai darbo funkcijoms vykdyti suteiktą kompiuterį, planšetę, elektroninį paštą ir kitus GMP tarnybos įrenginius, prietaisus, įtaisus, informacijos ir ryšių technologijas, programinę įrangą naudoja darbo funkcijoms atlikti.

65. Darbuotojams rekomenduojama atsakingai įvertinti ir nenaudoti GMP tarnybos suteiktų kompiuterių, telefonų ar kitos įrangos asmeniniais tikslais, taip pat nekaupti jose asmeninio pobūdžio informacijos ar asmens duomenų, išskyrus Taisyklių 66 punkte numatytą išimtį. Jei darbuotojas naudojasi GMP tarnybos suteikta įranga asmeniniais tikslais ar joje saugo asmeninio pobūdžio informaciją, jis prisiima riziką, kad tokia informacija patikrinimo metu gali būti pastebėta Tarnybos. Tarnyba neužtikrina asmeninės informacijos konfidencialumo, kai darbuotojai asmeniniais tikslais naudoja elektroninį paštą, internetą, socialinius tinklus ar programinę įrangą.

66. Interneto paslaugos gali būti naudojamos asmeniniais tikslais (socialinių tinklų naudojimas, asmeniniai mokestiniai ir bankiniai pervedimai, elektroninio pašto paslauga, momentiniai susirašinėjimai asmeniniais tikslais ir pan.), kiek tai netrukdo optimaliai ir kokybiškai atlikti darbo pareigas, nepažeidžiant Taisyklių 67 punkte nurodytų reikalavimų.

67. Darbuotojai savo darbo funkcijas vykdo naudodami GMP tarnybos suteiktus kompiuterius, elektroninius paštus ir kitus GMP tarnybos įrenginius, prietaisus, įtaisus, informacijos ir ryšių technologijas, programinę įrangą, išskyrus tuos atvejus, kai GMP tarnybos generalinis direktorius ar jo įgaliotas asmuo priima sprendimą dėl leidimo GMP tarnybos darbuotojui darbo funkcijas atlikti naudojantis asmeninėmis priemonėmis. Darbuotojai, turintys nuotolinę prieigą prie GMP tarnybos infrastruktūros, privalo imtis visų priemonių, kad būtų užtikrintas informacijos ir duomenų saugumas bei konfidencialumas, o GMP tarnyba privalo padėti darbuotojui įgyvendinti šią pareigą.

68. Nuolatinį darbuotojui suteikto kompiuterio, elektroninio pašto ir kitų GMP tarnybos įrenginių, prietaisų, įtaisų, informacijos ir ryšių technologijų, programinės įrangos stebėjimą ar tikrinimą vykdyti draudžiama. GMP tarnybos darbuotojams suteiktos darbo priemonės, įranga, įskaitant elektroninius paštus, kompiuterius, mobiliuosius telefonus, juose esantys asmens duomenys, kiti duomenys bei informacija gali būti tikrinami tik esant šioms sąlygoms:

68.1. darbuotojas yra informuotas apie patikrinimo galimybę;

68.2. yra pagrindas manyti, kad darbuotojas padarė darbo pareigų pažeidimą arba vykdė veiklą, nesuderinamą su GMP tarnybos interesais, arba vykdė teisės aktams prieštaraujančią veiklą, arba GMP tarnyba siekia patikrinti, ar darbuotojas laikosi įsipareigojimų GMP tarnybai, tinkamai vykdo teisės aktų, įskaitant GMP tarnybos vidinių dokumentų, reikalavimus, arba egzistuoja kitos svarbios tokį patikrinimą pagrindžiančios priežastys;

68.3. nėra galimybės pasiekti tikrinimo tikslo kitomis priemonėmis, kurios mažiau ribotų darbuotojo privatumą.

69. Šiose Taisyklėse įtvirtintas tikrinimas vykdomas limituota apimtimi, t. y. apibrėžtas konkretus laikotarpis, už kurį tikrinama, tikrinamas konkretaus projekto vykdymas, tikrinamas konkrečių funkcijų vykdymas ir tikrinamas tik tiek, kiek yra būtina išsiaiškinti šiose Taisyklėse išdėstytas aplinkybes ir apginti GMP tarnybos interesus. Duomenų apsaugos pareigūnas teikia konsultacijas, kad tikrinimas nepažeistų Reglamento, Taisyklių nuostatų bei duomenų subjektų teisės į privatumą.

70. Darbuotojai (taip pat ir praktikantai/savanoriai/stažuotojai) turi būti supažindinti su informacinių technologijų ir ryšių naudojimo darbo vietoje tvarka. Darbuotojai privalo laikytis konfidencialumo principo ir saugoti asmens duomenų paslaptį, tai patvirtindami rašytinai (3 priedas).

71. Vaizdo stebėjimas ir (ar) garso įrašymas darbuotojų darbo vietose gali būti vykdomas tik tada, kai dėl darbo specifikos būtina užtikrinti asmenų, turto ar visuomenės saugumą, ir kitais atvejais, kai kiti būdai ar priemonės yra nepakankami ir (arba) netinkami siekiant išvardytų tikslų. Apie vaizdo stebėjimą ir garso įrašymą konkrečioje vietoje informuojama vaizdiniu žymeniu matomoje vietoje.

X SKYRIUS
PACIENTŲ ASMENS DUOMENŲ TVARKYMO YPATUMAI

72. GMP paslaugos – GMP tarnybos teikiamos asmens sveikatos priežiūros paslaugos, siekiant laiku suteikti pacientui reikalingą medicinos pagalbą jo buvimo vietoje ir prireikus transportuoti sergantį ar sužeistą pacientą į asmens sveikatos priežiūros įstaigą. GMP paslaugos laikomos paslaugomis, skirtomis gyvybei gelbėti ir išsaugoti.

73. Pacientų asmens duomenys tvarkomi 72 punkte nurodytu tikslu. GMP tarnybos sveikatos priežiūros specialistai teikdami būtinosios medicinos pagalbos paslaugas tvarko pacientų asmens duomenis tokia apimtimi kiek to reikalauja būtinosios ar skubiosios medicinos pagalbos paslaugų teikimą reglamentuojantys teisės aktai.

74. GMP iškvietimas visoje Lietuvoje vykdomas nepriklausomai nuo operatoriaus, skambinant skubiosios pagalbos numeriu 112 arba konsultuojantis numeriu 113. Visi pokalbiai įrašomi be išankstinio paciento ar pagalbos kvietėjo įspėjimo vadovaujantis Bendrojo pagalbos centro įstatymu, sveikatos apsaugos ministro 2012 m. lapkričio 7 d. įsakymu Nr.V-996 „Dėl greitosios medicinos pagalbos dispečerinių veiklos aprašo patvirtinimo“. Pokalbių duomenys fiksuojami tarp paciento ar pagalbos kvietėjo ir dispečerio, ar tarp paciento/pagalbos kvietėjo ir GMP brigados nario.

75. GMP sveikatos priežiūros specialistai pacientų sveikatos duomenis tvarko vadovaudamiesi, bet neapsiribojant: Lietuvos Respublikos Konstitucija, Lietuvos Respublikos sveikatos sistemos įstatymu, Pacientų teisių ir žalos sveikatai atlyginimo įstatymu, sveikatos apsaugos ministro 2007 m. lapkričio 6 d. įsakymu Nr. V-895 „Dėl Greitosios medicinos pagalbos paslaugų teikimo organizavimo tvarkos aprašo patvirtinimo“ patvirtintu tvarkos aprašu, sveikatos apsaugos ministro 2015 m. rugpjūčio 27 d. įsakymu Nr. V-1004 „Dėl Greitosios medicinos pagalbos paslaugų iškvietimų įvertinimo ir GMP brigados siuntimo į iškvietimo vietą tvarkos aprašo patvirtinimo“ patvirtintu aprašu, sveikatos apsaugos ministro 2013 m. gruodžio 20 d. įsakymu Nr. V-1234 „Dėl kortelės Nr. 110/a „Greitosios medicinos pagalbos kvietimo kortelė“ duomenų sąrašo ir jos pildymo, pateikimo ir tikslinimo taisyklių patvirtinimo“, patvirtintomis taisyklėmis. Šios taisyklės nustato formos Nr. 110/a „Greitosios medicinos pagalbos kvietimo kortelė“ duomenų sąrašą, pildymo, pateikimo ir tikslinimo tvarką, taikomą asmens sveikatos priežiūros įstaigoms, teikiančioms GMP paslaugas. Kvietimo kortelės pildymas vykdomas informacinių technologijų priemonėmis, tačiau esant IT sutrikimams gali būti naudojamos ir popierinės formos.

76. Popierinės pacientų kvietimo kortelės GMP tarnybos gydytojų ar pajėgų valdytojų kabinetuose, budėjimų pastotėse ir pan. turi būti sudėtos taip, kad su jose esančiais asmens duomenimis (pvz., viršutiniame kvietimo kortelės lape nurodytu vardu, pavarde, adresu, kvietimo pagalbos aprašymu ir t. t.) negalėtų susipažinti tokios teisės neturintys kiti GMP tarnybos darbuotojai ar kiti asmenys.

77. Vadovaujantis sveikatos apsaugos ministro 1999 m. lapkričio 29 d. įsakymu Nr. 515 „Dėl sveikatos priežiūros įstaigų veiklos apskaitos ir atskaitomybės tvarkos“ patvirtintu aprašu pacientų asmens duomenys, surinkti teikiant greitosios medicinos pagalbos paslaugas, kvietimo kortelėse saugomi 3 (trejus) metus, kaip nustatyta dokumentų saugojimo terminų nuostatuose.

78. Duomenų gavėjai yra:

78.1. asmens sveikatos priežiūros įstaigos, į kurias pristatomas pacientas;

78.2. pirminės sveiktos priežiūros įstaigos, kurios teikia pirmines sveikatos priežiūros paslaugas pacientams (šeimos gydytojai);

78.3. Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos vykdanti PSDF lėšų skyrimo kontrolės funkcijas;

78.4. Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba nagrinėjanti pacientų prašymus ir skundus;

78.5. draudimo bendrovės dėl patirtos pacientų sveikatai žalos, pateikus teisinį pagrindą;

78.6. teisėsaugos institucijos nurodžiusios teisinį pagrindą (pvz. policija);

78.7. Lietuvos Respublikos sveikatos apsaugos ministerijai, kaip dalininkės nagrinėjančios gautus skundus ar prašymus.

79. Kompiuterių monitoriai, pagalbos kvietimo planšetės, GMP vairuotojo planšetės, kuriuose sveikatos priežiūros specialistai, paramedikai, dispečeriai, GMP vairuotojai peržiūri su paciento sveikata susijusią informaciją, turėtų būti nukreipti taip, kad su monitoriuje matomais asmens duomenimis negalėtų susipažinti tokios teisės neturintys kiti darbuotojai, pacientai ar kiti asmenys, užėję į kabinetą, esantys kvietimo pagalbos vietoje ar vykdami GMP specializuotu transportu.

80. Kalbant su pacientais telefonu turi būti užtikrintas pokalbių su pacientais konfidencialumas (t. y., pokalbis turi vykti taip, kad pokalbio metu pateiktų asmens duomenų negalėtų girdėti neįgalioti asmenys); Telefonu asmens duomenys neturi būti teikiami, jeigu GMP tarnyba neturi galimybės identifikuoti skambinančio asmens.

81. Siunčiant pacientams informaciją arba apie pacientams suteiktas paslaugas, kontrolę vykdančioms institucijoms kuomet yra teisinis pagrindas tokius duomenis teikti, sveikatos duomenis teikiami vadovaujantis sveikatos apsaugos ministro 2001 m. vasario 1 d. įsakymu Nr. 65 „Dėl informacijos apie pacientą valstybės institucijoms ir kitoms įstaigoms teikimo tvarkos aprašo patvirtinimo ir asmens sveikatos paslapties kriterijų nustatymo“ (aktuali redakcija) nustatyta tvarka.

82. Vaizdo stebėjimas ir garso įrašymas neturi būti vykdomas ten kur pacientams teikiamos sveikatos priežiūros paslaugos, arba ten kur atskleidžiami pacientų ypatingi asmens duomenys, išskyrus atvejus, kai teikiant asmens sveikatos priežiūros paslaugas pacientų ir (arba) sveikatos priežiūros specialisto saugumo užtikrinimo tikslais, sveikatos apsaugos ministro nustatyta tvarka gali būti atliekamas vaizdo ir (arba) garso stebėjimas ir (arba) įrašymas.

83. Tvarkant archyvą, kur yra saugomi pacientų sveikatos duomenys, pasibaigus nustatytam asmens duomenų saugojimo terminui, šie duomenys turi būti sunaikinami.

84. Tiek rašytiniai dokumentai, tiek pačios įgyvendinamos asmens duomenų saugumo priemonės turi būti periodiškai peržiūrimos.

XI SKYRIUS
VAIZDUO DUOMENŲ TVARKYMO YPATUMAI

85. Tvarkant vaizdo ir (ar) garso duomenis darbo vietose ir GMP tarnybos patalpose ar teritorijose, kuriose dirba darbuotojai, tvarkant asmens duomenis, susijusius su darbuotojų elgesio, vietos ar judėjimo stebėsena, šie darbuotojai apie tokį jų asmens duomenų tvarkymą turi būti informuojami būdu, įrodančiu informavimo faktą.

86. Vaizdo stebėjimas vaizdo registratoriais vykdomas GMP tarnybai priklausančiame specializuotame transporte atsižvelgiant į atliekamų darbo funkcijų bei teikiamų paslaugų specifiką. Toks stebėjimas būtinas siekiant užtikrinti GMP tarnybos turto ir visuomenės saugumą, GMP tarnybos specializuoto transporto dalyvavimą eisme, įvykio aplinkybių fiksavimą, taip pat kitais atvejais, kai kiti būdai ar priemonės yra nepakankami.

87. Automatizuotos duomenų rinkimo ir stebėjimo sistemos duomenys (buvimo vietos koordinatės, laikas, kuro sąnaudos, greitis ir kiti parametrai) renkami GMP specializuoto transporto dirbančių brigadų pamainos budėjimo metu arba darbo valandomis jei automatizuotos duomenų rinkimo ir stebėjimo sistemos įdiegtos administracijos tarnybiniuose automobiliuose. Po darbo valandų stebėjimas turi būti sustabdytas.

88. Teikiant greitosios medicinos pagalbos paslaugas, duomenų subjektas, vadovaudamasis sveikatos apsaugos ministro 2025 m. kovo 21 d. įsakymu Nr. V-252 „Dėl vaizdo ir garso stebėjimo ir įrašymo teikiant asmens sveikatos priežiūros paslaugas ir vaizdo ir garso duomenų tvarkymo tvarkos aprašo patvirtinimo“, gali vykdyti vaizdo ir garso stebėjimą bei įrašymą mobiliomis vaizdo stebėjimo priemonėmis, jei kyla pavojus sveikatos priežiūros specialisto ar paciento sveikatai ar gyvybei. Prieš pradedant vaizdo ar garso stebėjimą ir įrašymą (taip pat ir tais atvejais, kai tai daroma paciento prašymu), asmenys aiškiai įspėjami žodžiu apie stebėjimo ir įrašymo vykdymą bei jo tikslą – užtikrinti sveikatos priežiūros specialistų ir pacientų saugumą.

89. Vaizdo stebėjimą GMP tarnyboje reglamentuoja Vaizdo duomenų tvarkymo taisyklės.

90. Viešosios informacijos rengėjų, skleidėjų, žurnalistų ir trečiųjų asmenų filmavimo, fotografavimo, garso ar vaizdo įrašų darymo bei kitų techninio pobūdžio priemonių naudojimo (toliau – vaizdo ir garso fiksavimo techninės priemonės) principai ir tvarka GMP tarnybos patalpose, teritorijoje ar GMP tarnybai priskirtų funkcijų vykdymo metu ne tarnybos patalpose:

91.1. GMP tarnybos darbuotojai privalo užtikrinti, kad vaizdo ir garso fiksavimo techninių priemonių naudojimo metu asmens duomenys būtų apsaugoti nuo neteisėto jų užfiksavimo. Darbo vietose, tarnybos patalpose, teritorijoje ir (ar) darbuotojų funkcijų vykdymo metu ne GMP tarnybos patalpose negali būti dokumentų, užrašų ar kitos informacijos, kurioje yra asmens duomenų, išskyrus tuos, kuriuos būtina ir teisėta atskleisti (pvz., viešuose renginiuose ar oficialių vizitų metu).

91.2. Jei reikalingą informaciją galima pateikti kitomis (lygiavertėmis) priemonėmis nei vaizdo ir garso fiksavimo techninės priemonės arba kitose (lygiavertėse) patalpose ar erdvėse (pvz., viešose vietose arba ne darbuotojų darbo vietose), rekomenduojama pasirinkti šias alternatyvas, siekiant išvengti perteklinio asmens duomenų fiksavimo.

XII SKYRIUS
GARSO ĮRAŠŲ DARYMAS

92. Garso įrašas gali būti daromas GMP tarnybos rengiamuose nuotoliniuose susitikimuose su kitomis institucijomis, organizacijomis arba vidinio susitikimo protokolui parengti. Prieš pradedant įrašymą, duomenų subjektai informuojami žodžiu ar raštu apie įrašymo faktą ir jo tikslą. Parengus posėdžio protokolą, garso įrašas sunaikinamas ir toliau nebesaugomas, nebent teisės aktai nustato kitą saugojimo terminą.

93. Kai vyksta telefoninis pokalbis Duomenų subjektas turi būti informuotas apie telefoninių pokalbių garso įrašo darymą ir įrašuose fiksuojamų asmens duomenų tvarkymą prieš pradedant įrašymą. Už informavimą atsakingi darbuotojai, kurie skambina duomenų subjektui arba kuriems skambina duomenų subjektas, išskyrus atvejus, kai informavimas atliekamas automatinėmis priemonėmis.

XIII SKYRIUS
TELEFONIJOS IR RADIJO RYŠIO PRIEMONĖS

94. Telefoninio pokalbio ar radijo ryšio metu įrašai daromi, kai pacientai ar pagalbos kvietėjai skambina bendruoju pagalbos centro numeriu 112, o skambutis peradresuojamas GMP tarnybos dispečeriui arba kai skambinama numeriu 113 medicininėms konsultacijoms teikti ir GMP kvietimams priimti pagal sveikatos apsaugos ministro 2012 m. lapkričio 7 d. įsakymu Nr. V-996 „Dėl greitosios medicinos pagalbos dispečerinių veiklos aprašo patvirtinimo“ ir sveikatos apsaugos ministro 2015 m. rugpjūčio 27 d. įsakymu Nr. V-1004 „Dėl greitosios medicinos pagalbos iškvietimų įvertinimo ir greitosios medicinos pagalbos brigados siuntimo į iškvietimo vietą tvarkos aprašas“ patvirtintais aprašais.

95. Telefoninio pokalbio įrašai daromi, kai fiziniai asmenys skambina Karštosios linijos 1808 telefono numeriu dėl pacientų pavėžėjimo paslaugos užsakymo ar su ja susijusios informacijos pagal Lietuvos Respublikos Vyriausybės 2022 m. lapkričio 30 d. nutarimu Nr. 1196 „Dėl Pacientų pavėžėjimo paslaugų organizavimo ir teikimo tvarkos aprašo patvirtinimo“ nustatyta tvarka ir minėtu nutarimu pavirtintomis paslaugos teikimo taisyklėmis.

96. Duomenų subjektų teisės, susijusios su kvietimo pagalbos (telefoninio ar radijo ryšio) įrašais duomenų tvarkymu, įgyvendinamos Taisyklių VIII skyriuje nustatyta tvarka. Įgyvendinant duomenų subjekto teisę susipažinti su tvarkomais savo asmens duomenimis, t. y. GMP tarnyboje užregistruotu ir saugomu kvietimo pagalbos (telefoninio ar radijo ryšio) įrašu, turi būti užtikrinama trečiųjų asmenų teisė į privatų gyvenimą, t. y. duomenų subjektui susipažinti gali būti pateikiama tik tą garso įrašo dalis, kuri susijusi su duomenų subjektu.

97. Karštosios linijos 1808 paslaugų teikimo metu duomenų subjektas informuojamas apie pokalbio įrašymą ir garso įrašuose fiksuojamų asmens duomenų tvarkymą prieš pradedant pokalbį gavus iš anksto sutikimą. Už duomenų subjekto informavimą, sutikimo gavimą ir garso įrašų tvarkymą atsakingi Karštosios linijos 1808 operatoriai.

98. Telefoninių pokalbių įrašymas vykdomas siekiant užtikrinti teikiamų paslaugų kokybę, informavimą ir susijusių aplinkybių patvirtinimą:

98.1. skambučiai numeriais 112 ir 113 priimami be išankstinio duomenų subjekto sutikimo, vadovaujantis Reglamento (ES) 2016/679 (BDAR) 6 straipsnio 1 dalies c) punktu, kuris numato teisinę prievolę GMP tarnybai vykdant Lietuvos Respublikos sveikatos priežiūrą ir teikiant greitosios medicinos pagalbos paslaugas. Taip pat vadovaujamasi 6 straipsnio 1 dalies d) punktu, kai duomenų tvarkymas būtinas siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus, ir 9 straipsnio 2 dalies c) punktu, kai duomenų subjektas dėl fizinių ar teisinių priežasčių negali duoti sutikimo;

98.2. skambinant Karštosios linijos 1808 numeriu, duomenų subjektas informuojamas apie pokalbio įrašymą. Jei po informacijos pateikimo pokalbis tęsiamas, laikoma, kad yra duotas sutikimas įrašymui. GMP tarnyba tvarko šių įeinančių skambučių įrašus vadovaudamasi Reglamento 6 straipsnio 1 dalies a) punktu ir 9 straipsnio 2 dalies a) punktu (asmens sutikimas) ir 6 straipsnio 2 dalies c) punktu bei 9 straipsnio 2 dalies b) punktu nes numatyta teisinė prievolė teikti pacientų pavėžėjimo paslaugas.

99. Pokalbio duomenys sudaro (įskaitant techninius duomenis): garso įrašas (balso duomenys), pokalbio turinys, pokalbio data, laikas, trukmė, telefono numeris ir kiti duomenys kai skambinančiojo prašoma nurodyti asmeninę informaciją, pvz., vardą, pavardę, adresą ar kitus duomenis.

XIV SKYRIUS
ASMENS DUOMENŲ SAUGUMO POLITIKA

100. Asmens duomenų saugumas (toliau – ir duomenų sauga) apima pagrindinius principus:

100.1. asmens duomenų konfidencialumą – apsaugą nuo nesankcionuoto atskleidimo;

100.2. asmens duomenų vientisumą – apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;

100.3. asmens duomenų prieinamumą – užtikrinimą, kad GMP tarnyboje asmens duomenys prieinami tada, kai jie yra reikalingi.

101. Bendrieji duomenų saugos tikslai:

101.1. įgyvendinti technines ir organizacines priemones, užtikrinančias veiklos tęstinumą;

101.2. atitiktis teisės aktams: kasmetinis atitikties vertinimas, trūkumų šalinimas ir politikos atnaujinimas;

101.3. rizikos valdymas: identifikavimas, vertinimas ir sumažinimas iki priimtino lygio.

102. Duomenų saugos reikalavimai:

102.1. GMP tarnyba vadovaujasi Kibernetinio saugumo įstatymu, TIS 2 direktyvos nuostatomis;

102.2. GMP tarnyboje atliekama informacinių sistemų kibernetinio saugumo rizikos analizė ir jų valdymas;

102.3. yra privalomas incidentų registravimas ir Nacionaliniam kibernetinio saugumo centrui ataskaitų teikimas.

102.4. Tiekimo grandinės saugumas. Tiekėjai ir partneriai užtikrina duomenų apsauga.

103. Veiklos tęstinumas:

103.1. GMP tarnyba nustato pagrindines procedūras, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas;

103.2. sudaromas periodinis veiklos tęstinumo planas, atliekamas peržiūrėjimas ir testavimas;

103.3. paskirti darbuotojai, turintys reikiamą atsakomybę, įgaliojimus ir kompetenciją valdyti veiklos tęstinumą saugumo incidento, asmens duomenų saugumo pažeidimo atveju;

103.4. numatyta alternatyvos, atsižvelgiant į GMP tarnybos veiklą ir jai priimtiną IT sistemų prastovą.

104. GMP tarnyboje asmens duomenys skirstomi pagal jautrumą ir teisinius reikalavimus:

104.1.1. vieši duomenys – informacija, kuri gali būti prieinama visiems be apribojimų;

104.1.2. nuasmeninti duomenys – kai teikiami nuasmeninti, užšifruoti pacientų sveikatos asmens duomenys moksliniais ar kitais teisės aktuose nustatytais tyrimų tikslais;

104.1.3. konfidencialūs duomenys – duomenys, kuriuos gali pasiekti tik tam tikri įgalioti asmenys, pvz., darbuotojų asmeninė informacija;

104.1.4. specialus duomenys – jautri informacija, kurios praradimas ar atskleidimas gali turėti rimtų pasekmių (pvz., pacientų sveikatos duomenys).

105. Duomenų klasifikavimo kriterijai, nustatomi remiantis šiais veiksniais:

105.1. teisiniais ir reguliavimo reikalavimais (BDAR, nacionaliniai teisės aktai);

105.2. potencialios žalos dydžiu GMP tarnybai ir asmenims pažeidus duomenų saugumą;

105.3. duomenų dalinimosi (viduje, išorėje) ir saugojimo reikalavimais.

106. Prieigos valdymas:

106.1. prieigos kontrolė užtikrina, kad prie asmens duomenų gali prieiti tik autorizuoti asmenys pagal nustatytus principus:

106.1.1. mažiausios teisės – vartotojai gauna tik būtiniausias prieigos teises pagal savo pareigas;

106.1.2. visi duomenų tvarkytojai privalo naudoti dviejų faktorių autentifikaciją (2FA) ir unikalius prisijungimus;

106.1.3. periodinis prieigos peržiūrėjimas – kasmetinis peržiūrėjimas, siekiant pašalinti perteklines ar pasenusias prieigos teises;

106.1.4. sesijų valdymas – nustatomas automatinis sesijų uždarymas po tam tikro neveiklumo laiko.

106.2. Prieigos valdymo procesas:

106.2.1. naujo vartotojo prieigos suteikimas, patvirtinta atsakingo asmens;

106.2.2. duomenų naudojimo stebėjimas ir neįprastos veiklos aptikimas;

106.2.3. prieigos panaikinimas, kai darbuotojas išeina iš darbo arba jo pareigos keičiasi;

106.2.4. sistemų administratoriams prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas dviejų veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamas dviejų veiksnių autentifikavimas;

107. Techninių žurnalų įrašai ir stebėsena. IT sistemų ir taikomųjų programų, naudojamų asmens duomenų tvarkymui, veikla turi būti nuolat stebima, siekiant užtikrinti duomenų saugumą, atsekamumą ir atitiktį reglamentavimo reikalavimams:

107.1. GMP tarnyboje naudojamos IT sistemos privalo turėti techninių žurnalų įrašų mechanizmus, kurie fiksuoja prieigos prie asmens duomenų operacijas, įskaitant:

107.1.1. prieigos registravimą (vartotojo ID, duomenų peržiūrėjimas, keitimas, panaikinimas);

107.1.2. veiksmų laiką ir datą, kad būtų galima tiksliai identifikuoti vykdytus pakeitimus;

107.1.3. sisteminius įvykius, susijusius su saugos konfigūracijomis ir neįprastomis prieigos operacijomis.

107.2. Techninių žurnalų įrašai turi būti saugomi ne trumpiau kaip 6 mėnesius, užtikrinant galimybę peržiūrėti ankstesnius(istorinius) auditus ir tyrimus. Prireikus, saugojimo laikotarpis gali būti pratęstas pagal reglamentuojančius teisės aktus.

107.3. Techninių žurnalų įrašai turi būti apsaugoti nuo:

107.3.1. suklastojimo ar modifikavimo – naudojamos vientisumo patvirtinimo priemonės;

107.3.2. neautorizuotos prieigos – taikoma prieigos kontrolė ir šifravimas;

107.3.3. sugadinimo ar praradimo – duomenys saugomi rezervinėse kopijose ir patikimose saugojimo vietose;

107.4. IT sistemos turi naudoti sinchronizuotus laiko apskaitos mechanizmus, suderintus su patvirtintu laiko atskaitos šaltiniu, kad būtų išvengta laiko neatitikimų atliekant saugumo tyrimus.

108. Atsarginės kopijos ir duomenų atstatymas. Atsarginės kopijos yra esminė duomenų apsaugos dalis, užtikrinanti veiklos tęstinumą ir duomenų atkūrimą po incidentų.

108.1. GMP tarnyboje įgyvendinama atsarginių kopijų politiką, kuri apima:

108.1.1. reguliarų atsarginių kopijų kūrimą – duomenys turi būti kopijuojami pagal nustatytą grafiką;

108.1.2. duomenų atstatymo procedūras – aiškiai dokumentuotas procesas, kaip atkurti duomenis po incidento;

108.1.3. prieigos kontrolę – atsarginės kopijos turi būti prieinamos tik įgaliotiems asmenims.

108.2. Atsarginių kopijų laikmenų saugumas turi atitikti reikalavimus:

108.2.1. taikoma fizinė apsauga, kopijos saugomos saugiose patalpose su ribota prieiga;

108.2.2 . duomenys turi būti šifruoti, kad būtų apsaugoti nuo neteisėtos prieigos;

108.2.3. kopijos laikomos skirtingose vietose, kad būtų išvengta duomenų praradimo.

108.3. Atsarginių kopijų darymo rekomenduojamas grafikas:

108.3.1. kasdien – pridedamoji kopija (tik naujai pakeisti duomenys);

108.3.2. kas savaitę – pilna kopija (visi duomenys);

108.3.3. kas mėnesį – ilgalaikė kopija, saugoma atskiroje vietoje.

108.4. Atsarginių kopijų darymas turi būti nuolat stebimas, siekiant užtikrinti:

108.4.1. užbaigtumą ir išsamumą – kopijos turi būti pilnos ir tinkamai suformuotos.

108.4.2. reguliarų testavimą – duomenų atkūrimo bandymai atliekami periodiškai;

108.4.3. automatizuotą stebėseną – naudojamos IT sistemos, fiksuojančios kopijų kūrimo būseną.

109. Išteklių ir turto valdymas. IT išteklių ir turto valdymas yra būtinas siekiant užtikrinti skaidrumą, efektyvumą ir saugumą tvarkant asmens duomenis.

110. IT išteklių registras apima:

110.1. GMP tarnyba privalo turėti IT išteklių registrą, kuriame būtų fiksuojami visi naudojami ištekliai, įskaitant:

110.1.1. serverius;

110.1.2. duomenų saugojimo sistemas;

110.1.3. programinę įrangą, naudojamą asmens duomenų tvarkymui,

110.1.4. tinklo infrastruktūrą;

110.1.5. prieigos kontrolės mechanizmus,

110.1.6. nešiojamas laikmenas ir mobiliuosius įrenginius.

110.2. Atsakomybės paskirstymas. IT išteklių registras turi būti priskirtas konkrečiam atsakingam asmeniui, kuris:

110.2.1. užtikrina registro atnaujinimą ir tikslumą;

110.2.2. stebi išteklių naudojimą ir prieigos kontrolę;

110.2.3. atlieka periodinius auditus, siekiant užtikrinti atitiktį saugumo reikalavimams.

111. Turto apsauga ir stebėsena. GMP tarnyba užtikrina, kad IT ištekliai būtų apsaugoti nuo netinkamo naudojimo, fizinės žalos, duomenų praradimo.

112. Pokyčių valdymas. IT sistemų pokyčių valdymas yra būtinas siekiant užtikrinti stabilumą, saugumą ir atitiktį reglamentavimo reikalavimams, kurie apima:

112.1. Pokyčių registravimas. IT sistemų pokyčiai turi būti registruojami ir stebimi, įskaitant: 112.1.1. programinės įrangos atnaujinimus;

112.1.2. konfigūracijos pakeitimus;

112.1.3. prieigos teisių keitimus;

112.1.4. saugumo pataisas ir spragų šalinimą.

112.2. Pokyčių valdymo procesas. GMP tarnyba turi užtikrinti, kad pokyčių valdymo procesas apimtų šiuos etapus:

112.2.1. dokumentuojamas pokyčio poreikis ir tikslai;

112.2.2. rizikos vertinimas – įvertinamas poveikis sistemoms ir duomenų saugumui;

112.2.3. pokytis turi būti patvirtintas atsakingų asmenų ir (ar) saugos įgaliotinio;

112.2.4. pokytis atliekamas pagal nustatytą planą;

112.2.5. testuojama ir užtikrinama, kad pokytis nekelia grėsmių sistemų veiklai, asmens duomenims;

112.2.6. visi pakeitimai registruojami ir saugomi audito tikslais.

112.3. Įgyvendinant pokyčių stebėseną ir ataskaitų teikimą GMP tarnyba turi:

112.3.1. nuolat stebėti IT sistemų pokyčius ir jų poveikį;

112.3.2. teikti ataskaitas apie reikšmingus pakeitimus atsakingoms institucijoms;

112.3.3. atlikti periodinius pokyčių valdymo auditus, siekiant užtikrinti atitiktį saugumo reikalavimams.

113. Duomenų naikinimo ir šalinimo būtinas procesas, užtikrinantis, kad asmens duomenys nebūtų neteisėtai atkurti ar panaudoti po jų pašalinimo.

114. Duomenų naikinimo būdai:

114.1. elektroninių duomenų naikinimas. Prieš pašalinant bet kokią duomenų laikmeną, visi joje esantys duomenys, naudojant tam skirtą programinę įranga, kuri palaiko patikimus duomenų naikinimo algoritmus, arba užtikrinantis duomenų perrašymą keliais sluoksniais, arba užtikrinantys visišką duomenų pašalinimą;

114.2. fizinis duomenų laikmenų sunaikinimas. Kai elektroninių duomenų naikinimas neįmanomas (pvz., CD, DVD, magnetinės juostos), turi būti įvykdytas fizinis sunaikinimas, užtikrinantis, kad duomenys negalėtų būti atkurti, kaip pvz., mechaninis laikmenų susmulkinimas į mažas daleles, saugus laikmenų sudeginimas kontroliuojamoje aplinkoje, specialių cheminių medžiagų naudojimas duomenų laikmenų struktūrai sunaikinti;

114.3. popieriniai dokumentai ir nešiojamos duomenų laikmenos (pvz., CD, DVD), kuriose buvo saugomi asmens duomenys, turi būti naikinami naudojant: smulkintuvą – dokumentų naikinimas pagal DIN 66399 standartą, užtikrinantį tinkamą dalelių dydį; ar kitomis mechaninėmis priemonėmis, magnetinį ištrynimą – naudojamas kietųjų diskų ir magnetinių juostų duomenų pašalinimui;

114.4. duomenų naikinimo procesai turi būti registruojami ir dokumentuojami, įskaitant: naikinimo datą ir laiką, atsakingus asmenis, naudotus metodus, patvirtinimą, kad duomenys nebegali būti atkurti;

114.5. jei saugiems įrašų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečio asmens paslaugos, turi būti užtikrinta, kad šis procesas vyktų duomenų valdytojo ir (ar) tvarkytojo patalpose, siekiant išvengti duomenų perdavimo tretiesiems asmenims. Atskirais atvejais, kai to neįmanoma atlikti duomenų valdytojo ir (ar) tvarkytojo patalpose, sunaikinimas gali būti atliekamas kitoje fizinėje vietoje, tačiau tik stebint įgaliotam duomenų valdytojo atstovui.

115. Personalo konfidencialumas. GMP tarnyba turi užtikrinti, kad visi darbuotojai suprastų savo atsakomybes ir įsipareigojimus, susijusius su asmens duomenų tvarkymu. Tiesioginiai vadovai turi aiškiai išdėstyti darbuotojui prieš jam pradedant vykdyti paskirtas funkcijas ir darbus dėl saugaus asmens duomenų tvarkymo.

116. Visi nauji darbuotojai, savanoriai, praktikantai ir pan. prieš pradėdami savo veikla pasirašo konfidencialumo pasižadėjimą dėl asmens duomenų konfidencialumo užtikrinimo (3 priedas). GMP tarnybos sveikatos priežiūros specialistai yra atsakingi už aukštos rizikos asmens duomenų tvarkymo operacijas, todėl turi laikytis konkrečių jiems taikomų konfidencialumo sąlygų (pagal jų darbo sutartį ir priskirtas funkcijas: GMP brigadų nariai, gydytojai, dispečeriai, padalinių vadovai.

117. GMP tarnyba turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo kontrolę, susijusią su jų kasdieniu darbu.

118. Darbuotojai, susiję su asmens duomenų tvarkymu mokomi dėl atitinkamų duomenų apsaugos reikalavimų. Mokymų dažnumas ne rečiau kaip kartą per metus.

119. Reikalavimai duomenų tvarkytojams:

119.1. prieš pradedant asmens duomenų tvarkymo veiklą, duomenų valdytojai ir duomenų tvarkytojai turėtų apibrėžti, dokumentuoti ir suderinti tarpusavio formalumus ir procedūras taikomas duomenų tvarkytojams;

119.2. duomenų tvarkytojas privalo nedelsdamas pranešti duomenų valdytojui apie nustatytus asmens duomenų saugumo pažeidimus;

119.3. paskirtas duomenų tvarkytojas turi užtikrinti, kad techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų Reglamente reikalavimus ir būtų užtikrinta fizinių asmenų teisių apsauga.

119.4. duomenų tvarkytojo darbuotojams, dirbantiems su asmens duomenimis, turi būti taikomi konkretūs dokumentais įtvirtinti informacijos konfidencialumo, neatskleidimo susitarimai.

XV SKYRIUS
PROGRAMINĖS ĮRANGOS SAUGA

120. GMP tarnyboje naudojama informacinėse sistemose programinė įranga (asmens duomenims tvarkyti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras (angl. frameworks), standartus (pvz., Agile, OWASP ir kt.). Po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją, turi būti laikomasi pagrindinių saugos reikalavimų;

121. Projektuojant ir kuriant naujas programinės įrangos sistemas, kuriose numatoma tvarkyti asmens duomenis, būtina laikytis BDAR 25 straipsnyje numatytų principų.

122. Pritaikytoji duomenų apsauga (angl. privacy by design) duomenų valdytojui nurodo pareigas įgyvendinti tinkamas technines ir organizacines priemones, pvz., pseudonimų suteikimą, duomenų kiekio mažinimo principą, į duomenų tvarkymą integruoti būtinas apsaugos priemones, kad jis atitiktų šio reglamento reikalavimus ir apsaugotų duomenų subjektų teises.

123. Standartizuotoji duomenų apsauga (angl. privacy by default) nustato duomenų valdytojui įgyvendinti tinkamas technines ir organizacines priemones, kuriomis užtikrintų, kad standartizuotai būtų tvarkomi tik tie asmens duomenys, kurie yra būtini kiekvienam konkrečiam duomenų tvarkymo tikslui.

124. Standartizavimo prievolė taikoma surinktų asmens duomenų kiekiui, jų tvarkymo apimčiai, jų saugojimo laikotarpiui ir jų prieinamumui. Tokiomis priemonėmis užtikrinama, kad standartizuotai be fizinio asmens įsikišimo su asmens duomenimis negalėtų susipažinti neribotas fizinių asmenų skaičius.

XVI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

125. Asmens duomenų saugumo pažeidimai fiksuojami kartu su visa susijusia informacija apie įvykį ir atliktus incidento poveikio mažinimo veiksmus.

126. Asmens duomenų saugumo pažeidimų ir jų priežasčių klasifikavimą, pranešimo apie pažeidimus GMP tarnyboje, Inspekcijai ir duomenų subjektams, pažeidimų tyrimo, jų ir jų pasekmių pašalinimo ir mažinimo, pažeidimų prevencijos ir dokumentavimo tvarką nustato GMP tarnybos Asmens duomenų saugumo pažeidimų valdymo taisyklės.

XVII SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS IR KONSULTACIJOS SU PRIEŽIŪROS INSTITUCIJA

127. Prieš pradedant tvarkyti asmens duomenis, poveikio duomenų apsaugai vertinimas atliekamas tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus.

128. PDAV vertinimo tikslai:

128.1. nustatyti, ar dėl duomenų tvarkymo kyla pavojus arba didelis pavojus fizinių asmenų teisėms ir laisvėms;

128.2. įvertinti grėsmių pagrįstumą ir (ar) jos yra pateisinamos GMP tarnybos numatytiems tikslams pasiekti;

128.3. nustatyti ir (ar) imtis tinkamų priemonių šių grėsmių sumažinimui ir (ar) išvengimui.

129. Duomenų apsaugos pareigūnas privalo nuolat, esant poreikiui, bet ne rečiau kaip kartą per kalendorinius metus, vertinti PDAV atlikimo būtinybę ir tokiu atveju priima sprendimą dėl PDAV vertinimo atlikimo reikalingumo.

130. Nustatant, ar reikia atlikti PDAV vertinimą, vadovaujamasi Priežiūros institucijos sudarytu ir viešai skelbiamu tų rūšių duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašu, kuris patvirtintas Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. kovo 14 d. įsakymu Nr. 1T-35 (1.12.E) „Dėl Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“.

131. GMP tarnybos darbuotojai, kurie yra atsakingi už konkrečių GMP tarnybos funkcijų įgyvendinimo organizavimą, privalo informuoti duomenų apsaugos pareigūną, jei ketinama atlikti naujas operacijas su asmens duomenimis ar ketinama tvarkyti naujus asmens duomenis, kurių GMP tarnyba iki šiol netvarkė. Duomenų apsaugos pareigūnas įvertina naujas asmens duomenų tvarkymo operacijas ar ketinamus naujai tvarkyti asmens duomenis ir priima sprendimą dėl PDAV atlikimo reikalingumo.

132. PDAV atlieka GMP tarnybos struktūrinio padalinio vadovas arba darbuotojas nepriskirtas padaliniui, bet kuriam pavesta organizuoti GMP tarnybos funkcijų, kurių metu numatoma tvarkyti asmens duomenis, įgyvendinimą. PDAV atliekantis darbuotojas konsultuojasi su duomenų apsaugos pareigūnu.

133. PDAV dėl asmens duomenų tvarkymo operacijų, nenumatytų taisyklių 130 punkte, atliekamas šiais atvejais:

133.1. sistemingas ir išsamus su fiziniais asmenimis susijusių asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, ir kuriuo remiantis priimami sprendimai, kuriais padaromas su fiziniu asmeniu susijęs teisinis poveikis arba kurie daro panašų didelį poveikį fiziniam asmeniui;

133.2. specialiųjų kategorijų asmens duomenų arba asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu (išskyrus kai jų tvarkymą numato teisės aktai);

133.3. sistemingas viešosios vietos stebėjimas dideliu mastu.

134. Tais atvejais, kai kyla abejonių dėl poreikio atlikti PDAV, rekomenduojama jį atlikti.

135. Atliekant PDAV privaloma vertinti ne tik asmens duomenų tvarkymo atitiktį Reglamento nustatytiems reikalavimams, bet ir įvairaus pobūdžio pavojus fizinių asmenų teisėms ir laisvėms, įskaitant bet kokios žymios sveikatos, socialinės ar ekonominės žalos tikimybę. Būtina vertinti fizinės, turtinės ar neturtinės žalos tikimybę tiek atskiriems duomenų subjektams, tiek bendruomenėms ar socialinėms grupėms.

136. Duomenų tvarkymo operacijų, keliančių panašaus pobūdžio didelius pavojus duomenų subjektų teisėms ir laisvėms, sekai išnagrinėti galima atlikti vieną PDAV arba jeigu buvo jau atliktas dėl panašaus pobūdžio operacijų.

137. PDAV atliekamas užpildant Poveikio duomenų apsaugai vertinimo formos pavyzdį (Taisyklių 4 priedas).

138. Tais atvejais, kai PDAV atliekamas dėl duomenų tvarkymo operacijų, susijusių su GMP tarnybos darbuotojų, specialiųjų kategorijų asmens duomenimis, poveikio duomenų apsaugai vertinimą atliekantis asmuo turi išsiaiškinti duomenų subjektų ar jų atstovų nuomonę

apie asmens duomenų tvarkymą, nepažeisdamas komercinių ar viešųjų interesų apsaugos arba duomenų tvarkymo operacijų saugumo reikalavimų.

139. Užpildytą PDAV formą darbuotojas pateikia duomenų apsaugos pareigūnui.

140. Duomenų apsaugos pareigūnas pateikia savo nuomonę bei grąžina vertinimą atlikusiam darbuotojui.

141. PDAV atliekantis darbuotojas, gavęs duomenų apsaugos pareigūno nuomonę, atsižvelgia į ją ir pakoreguoja poveikio duomenų apsaugai vertinimą.

142. Jeigu poveikio duomenų apsaugai vertinimą atliekantis darbuotojas, gavęs duomenų apsaugos pareigūno nuomonę, į ją neatsižvelgia, poveikio duomenų apsaugai vertinimo formoje pagrindžia kodėl ir pateikia GMP tarnybos generaliniam direktoriui patvirtinti.

143. GMP tarnybos generalinis direktorius įsakymu patvirtina arba atsisako patvirtinti užpildytą poveikio duomenų apsaugai vertinimo formą.

144. Poveikio duomenų apsaugai vertinimas turi būti atliktas prieš pradedant įgyvendinti duomenų tvarkymo operacijas (veiksmus) arba iš karto paaiškėjus, kad turi būti atliktas PDAV.

145. Poveikio duomenų vertinimui atlikti gali būti pasitelkti išorės konsultantai, specialistai, ekspertai (teisininkai, informacinių sistemų ar technologijų specialistai, saugos ekspertai, etikos specialistai ir pan.), jeigu GMP tarnybos žmogiškųjų išteklių, laiko, kompetencijų nepakanka tinkamam poveikio duomenų apsaugai vertinimui atlikti.

146. Jeigu GMP tarnybos generalinio direktoriaus patvirtintoje poveikio duomenų apsaugai vertinimo formoje nurodyta, kad tvarkant duomenis kiltų didelis pavojus, jei GMP tarnyba ar kitas duomenų valdytojas arba tvarkytojas nesiimtų priemonių pavojui sumažinti, GMP tarnyba prieš pradėdama tvarkyti asmens duomenis, privalo konsultuotis su Inspekcija.

147. Duomenų apsaugos pareigūnas konsultuodamasis su Inspekcija jai privalo pateikti:

147.1. kai taikoma, atitinkamas duomenų tvarkymo procese dalyvaujančio duomenų valdytojo, bendrų duomenų valdytojų ir duomenų tvarkytojų atsakomybės sritis;

147.2. numatyto duomenų tvarkymo tikslus ir priemones;

147.3. nustatytas priemones bei apsaugos priemones duomenų subjektų teisėms ir laisvėms apsaugoti pagal Reglamentą;

147.4. Duomenų apsaugos pareigūno kontaktinius duomenis;

147.5. patvirtintą poveikio duomenų apsaugai vertinimo formą;

147.6. bet kokią kitą Inspekcijos prašomą informaciją.

128. Jeigu Inspekciją po konsultacijų pateikia rekomendacijas ar imasi kitų veiksmų pagal savo kompetenciją, pvz., atlieka tyrimą ar kt., duomenų apsaugos pareigūnas ir (arba) GMP tarnybos darbuotojai suteikia visą reikiamą informaciją ir pagalbą Inspekcijai bei bendradarbiauja su ja.

129. Duomenų apsaugos pareigūnas turi prižiūrėti asmens duomenų tvarkymo atitiktį PDAV formoje nurodytoms išvadoms ir sprendimams.

XVII SKYRIUS
ASMENS DUOMENŲ TVARKYMAS DUOMENŲ TVARKYTOJO STATUSU

130. Šio skyriaus nuostatos yra taikomos tais atvejais, kai GMP tarnyba tvarko duomenis kaip duomenų tvarkytoja. GMP tarnyba, kaip duomenų tvarkytojos, duomenų tvarkymo veikla fiksuoja duomenų tvarkymo veiklos įrašuose, informacinių sistemų nuostatuose, bendradarbiavimo sutartyse su duomenų valdytoju ar pagal įgaliojimą ir pan.

131. GMP tarnyba turi teisę tvarkyti kitų duomenų valdytojų duomenis tik tada, jeigu duomenų valdytojas yra aiškiai nustatęs ir nurodęs duomenų tvarkymo dalyką ir trukmę,

duomenų tvarkymo pobūdį ir tikslą, asmens duomenų kategorijas ir duomenų subjektų kategorijas bei duomenų valdytojo prievoles ir teises.

132. Tais atvejais, kai GMP tarnyba tvarko duomenis kaip duomenų tvarkytoja, GMP tarnyba privalo laikytis duomenų valdytojo nustatyto duomenų tvarkymo tikslo, priemonių ir kitų duomenų tvarkymo sąlygų, taip pat privalo tvarkyti tik tokį kiekį duomenų ir tik tokią trukmę, kurią nurodė duomenų valdytojas.

133. GMP tarnyba turi teisę tvarkyti asmens duomenis kaip duomenų tvarkytoja esant vienam iš šių teisinių pagrindų:

133.1. sudaryta sutartis su duomenų valdytoju. Gali būti sudaryta atskira duomenų tvarkymo sutartis arba atskiros duomenų tvarkymo veiklos nuostatos įtrauktos į kitą sutartį;

133.2. pareiga tvarkyti duomenis nustatyta teisės aktuose, Valstybės valdomų informacinių sistemų nuostatuose.

134. GMP tarnyba nepasitelkia kito duomenų tvarkytojo be išankstinio konkretaus arba bendro rašytinio duomenų valdytojo leidimo. Bendro rašytinio leidimo atveju GMP tarnyba informuoja duomenų valdytoją apie visus planuojamus pakeitimus, susijusius su kitų duomenų tvarkytojų pasitelkimu ar pakeitimu, ir taip suteikia duomenų valdytojui galimybę nesutikti su tokiais pakeitimais.

135. Kai GMP tarnyba konkrečiai duomenų tvarkymo veiklai duomenų valdytojo vardu atlikti pasitelkia kitą duomenų tvarkytoją, sutartimi ar kitu teisės aktu tam kitam duomenų tvarkytojui nustatomos tos pačios duomenų apsaugos prievolės, kaip ir prievolės, nustatytos GMP tarnyba teisės aktų bei duomenų valdytojo, visų pirma užtikrinti, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos taip, kad duomenų tvarkymas atitiktų Reglamento reikalavimus.

136. Visais atvejais, be duomenų valdytojo nustatytų papildomų pareigų, GMP tarnyba, tvarkydama duomenis kaip duomenų tvarkytoja, turi šias pareigas:

136.1. tvarkyti asmens duomenis tik pagal duomenų valdytojo dokumentais įformintus nurodymus, išskyrus atvejus, kai tai daryti reikalaujama pagal teisės aktų reikalavimus, kurie yra taikomi GMP tarnybai;

136.2. užtikrinti, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję užtikrinti konfidencialumą;

136.3. imtis visų techninių ir organizacinių priemonių, kad būtų užtikrintas tvarkomų duomenų saugumas;

136.4. laikytis Taisyklėse nustatytų kito duomenų tvarkytojo pasitelkimo sąlygų;

136.5. atsižvelgdama į duomenų tvarkymo pobūdį, padėti duomenų valdytojui taikydama tinkamas technines ir organizacines priemones, kad būtų įvykdyta duomenų valdytojo prievolė atsakyti į prašymus, susijusius su duomenų subjektų teisių įgyvendinimu;

136.6. padėti duomenų valdytojui įgyvendinti jo prievoles pranešti apie Asmens duomenų saugumo pažeidimus bei atlikti poveikio duomenų apsaugai vertinimą, atsižvelgiant į duomenų tvarkymo pobūdį ir GMP tarnybos turimą informaciją;

136.7. užbaigus teikti su duomenų tvarkymu susijusias paslaugas, ištrinti arba grąžinti duomenų valdytojui visus asmens duomenis ir ištrinti esamas jų kopijas, išskyrus atvejus, kai teisės aktai nustato reikalavimą asmens duomenis saugoti;

136.8. duomenų valdytojo prašymu pateikti informaciją, būtiną siekiant įrodyti, kad vykdomos šiame straipsnyje nustatytos prievolės, ir sudaryti sąlygas bei padėti duomenų valdytojui arba kitam duomenų valdytojo įgaliotam auditoriui atlikti auditą, įskaitant patikrinimus.

137. GMP tarnyba informuoja duomenų valdytoją, jei, GMP tarnybos nuomone, duomenų valdytojo nurodymas pažeidžia Reglamentą ar kitas duomenų apsaugos teisės nuostatas.

XVIII SKYRIUS
DUOMENŲ TVARKYTOJŲ PASITELKIMAS

138. GMP tarnyba turi teisę sutarties pagrindu duomenų tvarkymo veiksmams atlikti pasitelkti duomenų tvarkytoją. GMP tarnyba pasitelkia tik tuos duomenų tvarkytojus, kurie užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos taip, kad duomenų tvarkymas atitiktų Reglamento ir šių Taisyklių reikalavimus ir būtų užtikrintas duomenų subjekto teisių įgyvendinimas bei apsauga.

139. GMP tarnybos valdomų informacinių sistemų tvarkytojas (tvarkytojai) paskiriamas (paskiriami) teisės aktu, kuriuo tvirtinami informacinės sistemos nuostatai arba atskiru teisės aktu, sutartimi, įgaliojimu.

140. Sutartims su duomenų tvarkytojais taikomi reikalavimai nustatyti GMP tarnybos vidaus dokumentuose.

141. Kitiems asmenims (ne duomenų tvarkytojams) GMP tarnybos tvarkomi asmens duomenys gali būti perduoti tik duomenų subjekto prašymo ar sutikimo pagrindu, taip pat, kai tokia teisė yra numatyta teisės aktuose.

XIX SKYRIUS
ASMENS DUOMENŲ PERDAVIMAS Į TREČIĄSIAS VALSTYBES IR TARPTAUTINES ORGANIZACIJAS

142. Perduoti asmens duomenis į trečiąją valstybę arba tarptautinę organizaciją galima tik esant bent vienai iš šių sąlygų:

142.1. yra priimtas Europos Komisijos sprendimas, kad atitinkama trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečioje valstybėje, arba atitinkama tarptautinė organizacija užtikrina tinkamo lygio apsaugą;

142.2. jeigu nėra priimtas sprendimas dėl tinkamo apsaugos lygio užtikrinimo arba nenustatytos tinkamos apsaugos priemonės, asmens duomenys gali būti perduoti į trečiąją valstybę arba tarptautinei organizacijai tik tuo atveju, jeigu GMP tarnyba yra nustačiusi tinkamas apsaugos priemones, įskaitant tai, kad duomenų subjektams bus užtikrinta galimybė naudotis vykdytinomis duomenų subjektų teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis.

143. Jeigu nėra priimtas Europos Komisijos sprendimas dėl tinkamo apsaugos lygio užtikrinimo arba nenustatytos tinkamos apsaugos priemonės, kaip nurodyta Reglamento 46 straipsnio 2 ir 3 dalyse, asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai gali būti atliekamas tik tada, jeigu egzistuoja bent viena iš Reglamento 49 straipsnio 1 dalyje nurodytų sąlygų.

XX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

144. Taisyklės ne rečiau kaip kartą per metus, peržiūrimos ir, prireikus, atnaujinamos. Už šį procesą yra atsakingas duomenų apsaugos pareigūnas.

145. Dėl konkrečių duomenų tvarkymo operacijų (veiksmų), kuriems būtinas poveikio duomenų apsaugai vertinimas, GMP tarnyboje konsultuoja duomenų apsaugos pareigūnas.

146. GMP tarnyboje periodiškai, bet ne rečiau kaip kartą per metus, vyksta darbuotojų mokymai Reglamento, Taisyklių taikymo ir įgyvendinimo bei kitais asmens duomenų apsaugos klausimais. Už mokymų organizavimą atsakingas duomenų apsaugos pareigūnas.

147. Su šiomis Taisyklėmis GMP tarnybos darbuotojai supažindinami pasirašytinai priėmimo į darbą metu o vėliau su Taisyklių pakeitimais – DVS priemonėmis.

148. GMP tarnybos darbuotojai, pažeidę Taisyklių reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.