Kinnitas:	Priit Perens	Juhatuse esimees	17.10.2023
Koostas:	Priit Piir	Andmekaitsespetsialist	02.10.2023
	Ees- ja perekonnanimi	Ametikoht	kuupäev

ANDMEKAITSE KORD

1. Sissejuhatus

1.1. Andmekaitse korraga (edaspidi **Kord**) sätestab sihtasutus Tartu Ülikooli Kliinikum (edaspidi **Kliinikum**) isikuandmete kaitse korralduse ja põhimõtted. Korraga on kohustatud tutvuma kõik Kliinikumi personali liikmed, sh töötajad, töövõtu- või muu võlaõigusliku lepingu alusel tegutsevad, õppetööl osalevad ja teised füüsilised isikud, kes kasutavad oma ülesannete täitmisel Kliinikumi infosüsteeme või töötlevad muul viisil Kliinikumi nimel isikuandmeid (edaspidi koos **Personal** või eraldi **Personali liige**).

1.2. Isikuandmete kaitse eesmärgid on Kliinikumis toimuva ravi-, õppe- ja teadustöö ning neid teenindavate tugiprotsesside läbiviimiseks vajalike isikuandmete töötlemisel tagada:

1.2.1. andmesubjektide põhivabadusete ja -õiguste kaitse;

1.2.2. isikuandmete käideldavus, terviklus ja konfidentsiaalsus;

1.2.3. vastavus kohalduvale õigusele, eriti Euroopa Parlamendi ja Nõukogu määrusele (EL) 2016/679 (isikuandmete kaitse üldmäärus) (edaspidi **IKÜM**), isikuandmete kaitse seadusele, muudele kohalduvatele eriseadustele ja Euroopa Andmekaitsenõukogu ning Andmekaitse Inspektsiooni juhendmaterjalidele (edaspidi koos **Andmekaitseõigus**).

1.3. Korra lähtekohtadeks on Andmekaitseõigus, Kliinikumi põhikirjalised eesmärgid ja poliitikad, eriti infoturvapoliitika PKL-224 isikuandmete kaitset puudutavas osas.

1.4. Korraga seotud mõistete tähendus on toodud IKÜM artiklis 4.

1.5. Kord on Kliinikumis isikuandmete kaitset reguleeriv peamine dokument, mille asjakohasust hindab perioodiliselt andmekaitsespetsialist, kes teeb ettepanekud vajalike muudatuste osas. Andmekaitseõiguses ja Korras toodud nõuete täpsustamiseks ja selgitamiseks on andekaitsespetsialistil õigus kehtestada juhendeid, vorme, teatmestuid ja muud lisadokumentatsiooni vastavalt Kliinikumi dokumendiohje reeglitele.

1.6. Kliinikum rakendab isikuandmete töötlemisel isikuandmete kaitse põhimõtteid vastavalt Korras täpsustatud nõuetele:

1.6.1. vastutus;

1.6.2. läbipaistvus;

1.6.3. seaduslikkus;

1.6.4. eesmärgi piirang;

1.6.5. minimaalsus ja õigsus;

1.6.6. usaldusväärsus ja konfidentsiaalsus;

1.6.7. säilitamise piirang;

1.6.8. lõimitud ja vaikimisi andmekaitse.

2. Vastutus

2.1. Isikuandmete kaitse on Kliinikumi kollektiivne vastutus ja iga Personali liikme üldine kohustus. Iga isikuandmete töötlemises osalev Personali liige on individuaalselt vastutav Korraga tutvumise, sellest arusaamise ja Korras toodud nõuete järgimise eest.

2.2. Korra täitmise eest vastutab Kliinikumi juhatus, kes:

2.2.1. määratleb isikuandmete kaitse strateegia, peamised eesmärgid ja riskid ning eraldab vahendid riskide juhtimiseks ja/või aktsepteerib jääkriskid;

2.2.2. kinnitab andmekaitsespetsialisti ametijuhendi vastavalt IKÜM artiklites 37-39 toodud tingimustele ja ülesannetele ning määrab ametisse andmekaitsespetsialisti vastavalt IKÜM artiklis 37(5) toodud pädevusnõutele. Juhatus teavitab andmekaitsespetsialisti määramisest:

2.2.2.1. Andmekaitse Inspektsiooni ja avalikkust äriregistri ettevõtjaportaalis andmekaitsespetsialisti nime ja kontaktandmete avaldamise teel; ja

2.2.2.2. Personali Kliinikumi siseveebis andmekaitsespetsialisti nime ja kontaktandmete avaldamise teel.

2.2.3. kinnitab Kliinikumi isikuandmete töötlemise toimingud (edaspidi **töötlustoiming**) ja isikuandmeid töötlevad struktuuriüksused Kliinikumi isikuandmete töötlemisülevaates;

2.2.4. kinnitab täiendavad isikuandmete töötlemisega seotud korrad ja nõuded ning tagab, et Personali liikmed oleksid kordadest tulenevate nõuetega kursis ja neid rakendaksid;

2.2.5. tellib isikuandmete kaitsele Kliinikumis sõltumatuid hinnanguid ja haldab tuvastatud riske.

2.3. Töötlustoimingu õiguspärasuse ja vastavuse eest Korras toodud isikuandmete kaitse põhimõtetele ja nõuetele vastutab isikuandmeid töötleva struktuuriüksuse juht.

2.4. Andmekaitsespetsialist vastutab isikuandmete kaitse valdkonna koordineerimise, Andmekaitseõigusest ja Korrast tulenevate nõuete kontrollimise ja Personali teadlikkuse tõstmise eest läbi oma ametijuhendis toodud tegevuste. Oma ülesannete täitmiseks on andmekaitsespetsialistil õigus:

2.4.1. saada juurdepääs töödeldavatele isikuandmetele ja kontrollida isikuandmete kaitse nõuete täitmist;

2.4.2. nõuda Personali liikmetelt isikuandmete kaitse nõuete täitmist;

2.4.3. nõuda asjakohastelt Personali liikmetelt teavet ja saada neilt selgitusi isikuandmete töötlemise ja isikuandmetega seotud rikkumise asjaolude kohta.

3. Läbipaistvus ja õiglus

3.1. Isikuandmete töötlemise läbipaistvuse tagamiseks registreerib Kliinikum kõik töötlustoimingud isikuandmete töötlemisülevaates (edaspidi **töötlemisülevaade**), järgnevalt:

3.1.1. Töötlustoimingute registreerimise eest vastutab andmekaitsespetsialist, kellel on töötlustoimingu registreerimisse õigus kaasata Kliinikumi struktuuriüksusi, volitatud töötlejaid ja muid koostööpartnereid ning saada neilt vajalikku teavet;

3.1.2. Töötlemisülevaate andmekoosseisu määrab kindlaks andmekaitsespetsialist, kuid see peab sisaldama vähemalt IKÜM § 30 ja Korras nõutud teavet. Andmekaitsespetsialistil on õigus põhjendatud ja dokumenteeritud juhtudel muuta töötlemisülevaate andmekoosseisu;

3.1.3. Isikuandmete töötlemine, mida teostatakse samadel tingimustel, loetakse samaks isikuandmete töötlemiseks ning registreeritakse ühe kirjena;

3.1.4. Töötlemisülevaade vaadatakse üle ja vajadusel uuendatakse vähemalt kord aastas ja töötlustoimingu oluliste muudatuste puhul.

3.2. Kliinikum teavitab andmesubjekte isikuandmete töötlemise tingimustest läbi andmekaitsetingimuste avaldamise, mis peavad sisaldama vähemalt IKÜM artiklites 13-14 nõutud teavet kokkuvõtlikus, selges ja lihtsasti kättesaadavas vormis ning arusaadavas sõnastuses:

3.2.1. Kliinikumi töötajatele esitatakse tööle asumisel elektroonilisel kujul kord isikuandmete töötlemine töösuhtes PKL-212, mille kehtiv versioon on igal hetkel kättesaadav Kliinikumi siseveebis;

3.2.2. Kliinikumi patsiendid ja teised andmesubjektid saavad neid puudutavate töötlustoimingute osas igal hetkel tutvuda Kliinikumi isikuandmete töötlemise üldtingimustega PKL-194, mille kehtiv elektrooniline versioon on kättesaadav Kliinikumi kodulehel;

3.2.3. Patsiendi teavitamisel ja patsiendi või patsiendi lähedaste küsimustele vastamisel patsiendi terviseandmete osas lähtuvad Kliinikumi Personali liikmed kutse-eetikast ja Kliinikumi juhendist Kliinikumi töötaja käitumine suhtlemisel töökaaslase, patsiendiga ja tema lähedastega JKL-100.

3.3. Andmesubjektidel on igal hetkel õigus pöörduda Kliinikumi poole täiendava teabe saamiseks ja oma õiguste teostamiseks isikuandmete töötlemisel. Kliinikum aitab kaasa ja tagab kõigi andmesubjektide IKÜM artiklitest 15-22 tulenevate õiguste rakendamise kohalduvas ulatuses, järgnevalt:

3.3.1. andmesubjekti pöördumise registreerib dokumendihaldussüsteemis ja pöördumisele vastab Kliinikumi kantselei või struktuuriüksus, kellele pöördumine esitati. Keerulisemate pöördumiste lahendamiseks ja vastuse koostamiseks kaasatakse vajadusel andmekaitsespetsialist;

3.3.2. enne pöördumisele vastamist tuleb alati tuvastada andmesubjekti isikusamasus Kliinikumis kehtivate nõuete alusel, eelkõige läbi digitaalselt allkirjastatud või Kliinikumis kohapeal omakäeliselt allkirjastatud pöördumise esitamise. Kui Kliinikum ei suuda andmesubjekti tuvastada, võib andmesubjektilt nõuda täiendavat teavet;

3.3.3. andmesubjekti pöördumisele vastatakse andmesubjekti pöördumises toodud viisil välja arvatud juhul kui toodud viis ei võimalda isikuandmeid turvaliselt edastada;

3.3.4. andmesubjekti pöördumisele vastatakse ilma põhjendamatu viivituseta, kuid mitte hiljem kui ühe kalendrikuu jooksul alates andmesubjekti pöördumise saamisest. Pöördumise keerulisuse või pöördumiste suure hulga korral võib Kliinikum vastamise tähtaega pikendada kahe täiendava kalendrikuu võrra, teavitades andmesubjekti tähtaja pikendamisest ja viivituse põhjusest;

3.3.5. kui andmesubjekti isikusamasust ei ole võimalik tuvastada, pöördumine on põhjendamatu või ülemäärane, keeldub Kliinikum pöördumise täitmisest. Kliinikum teavitab andmesubjekti keeldumise põhjustest ja selgitab võimalust pöörduda Andmekaitse Inspektsiooni poole ja kasutada õiguskaitsevahendeid;

3.3.6. Kliinikum vastab andmesubjektide pöördumistele tasuta.

4. Seaduslikkus

4.1. Isikuandmeid töötlev struktuuriüksus tagab, et töötlustoimingul on õiguslik alus vastavalt IKÜM artiklile 6. Eriliiki isikuandmete töötlemisel peab töötlustoimingul olema täiendav, IKÜM artiklist 9(2) tulenev õiguslik alus. Töötlustoimingute õiguslikud alused dokumenteeritakse töötlemisülevaates.

4.2. Kui töötlustoimingu õiguslik alus on andmesubjekti nõusolek, peab nõusolek kehtivuseks täitma kõik järgnevad tingimused:

4.2.1. **vajalik** - nõusolekule ei või tugineda, kui isikuandmete töötlemiseks esineb muu õiguslik alus (sh seaduslik kohustus või tervishoiuteenuse osutamise leping);

4.2.2. **vabatahtlik** - andmesubjektil on nõusoleku andmiseks valikuvõimalus ja talle ei järgne keeldumise korral kahjulikke tagajärgi (sh keeldumine tervishoiuteenuse osutamisest);

4.2.3. **konkreetne** - nõusolek on muudest tahteavaldusest selgesti eristatud. Mitme isikuandmete töötlemise nõusoleku puhul peab andmesubjektil olema otsustusõigus iga erineva eesmärgi kohta;

4.2.4. **teadev, lihtsas ja arusaadavas sõnastuses** - teadva nõusoleku minimaalne andmekoosseis on Kliinikumi kui vastutava töötleja üld- ja kontaktandmed,

isikuandmete töötlemise eesmärk, töödeldavate isikuandmete kategooriad, isikuandmete edastamise korral isikuandmete vastuvõtjad, isikuandmete töötlemise tähtaeg ja andmesubjekti õigus nõusolek tagasi võtta;

4.2.5. **selgesõnaline** - andmesubjekt annab isikuandmete töötlemise nõusoleku tahteavalduse vormis või muu selget nõusolekut väljendava tegevusega;

4.2.6. **tõendatav** - nõusolek antakse vähemalt kirjalikku taasesitamist võimaldavas vormis, sh tuleb dokumenteerida suuliselt või tegevusega antud nõusolek. Õigusaktist, Kliinikumi sisekorrast, lepingust või muust alusest tuleneva vorminõude puhul tuleb järgida kohalduvat nõusoleku vorminõuet. Nõusoleku dokumendid tuleb nõuetekohaselt säilitada;

4.2.7. **tagasivõetav** - nõusoleku tagasivõtmine peab olema vähemalt sama lihtne kui nõusoleku andmine ja peab toimuma üldjuhul nõusoleku kogumisega samas vormis ja viisil;

4.2.8. kliinilistes uuringutes osalemise nõusoleku küsimisel tuleb lisaks kohaldada Euroopa Parlamendi ja Nõukogu määruse (EL) number 536/2014 5. peatüki „Kliinilises uuringus osaleja kaitse ja teadev nõusolek“ sätteid.

4.3. Kui töötlustoimingu õiguslik alus on Kliinikumi või kolmanda isiku õigustatud huvi IKÜM artikli 6(1)(f) kohaselt, peab isikuandmeid töötlev struktuuriüksus enne töötlustoiminguga alustamist läbi viima õigustatud huvi hinnangu järgnevatel tingimustel:

4.3.1. õigustatud huvi hinnang viiakse läbi vähemalt kirjalikku taasesitamist võimaldavas vormis vastavalt Andmekaitseõiguses toodud sisulistele nõuetele. Andmekaitsespetsialist võib kehtestada õigustatud huvi hindamisele kohustusliku vormi;

4.3.2. isikuandmeid töötleva struktuuriüksuse juht teavitab õigustatud huvi hinnangu koostamisest andmekaitsespetsialisti, kes registreerib töötlustoimingu ja/või õigustatud huvi hinnangu isikuandmete töötlemisülevaates ning esitab oma põhjendatud arvamuse õigustatud huvi õiguspärasuse osas. Asjakohasel juhul tuleb dokumenteerida andmekaitsespetsialisti arvamuse mittejärgimine- Struktuuriüksuse juht esitab õigustatud huvi hinnangu kinnitamiseks Kliinikumi juhatusele;

4.3.3. õigustatud huvi alusel ei ole lubatud töödelda eriliiki isikuandmeid, sh terviseandmeid.

5. Eesmärgi piirang

5.1. Struktuuriüksused töötlevad isikuandmeid ainult selgelt kindlaksmääratud ja õiguspärastel eesmärkidel. Töötlustoimingute eesmärgid dokumenteeritakse isikuandmete töötlemisülevaates.

5.2. Isikuandmeid ei ole lubatud hiljem töödelda viisil, mis ei ole isikuandmete kogumise eesmärgiga kooskõlas, välja arvatud täiendava õigusliku aluse olemasolul.

5.3. Kliinikumis on patsientide isikuandmete töötlemise esmaseks eesmärgiks tervishoiuteenuste osutamine ja seda tagavate tugiprotsesside haldamine (sh broneeringute ja ravijärjekorra haldamine, raviarveldus ja ravikvaliteedi tagamine - edaspidi koos **ravitöö**). Isikuandmete töötlemine ravitöö eesmärkidel on lubatud:

5.3.1. patsiendile tervishoiuteenuse osutamiseks;

5.3.2. tervishoiuteenuste osutamisele kohalduvate seaduslike kohustuste täitmiseks tuginedes Eesti Vabariigi õigusaktidele, eelkõige tervishoiuteenuste korraldamise seadusele (edaspidi **TTKS**) ja selle rakendusaktidele ning teistele tervishoiu valdkonna eriseadustele; või

5.3.3. patsiendi või muu isiku eluliste huvide kaitsmiseks.

5.4. Ülikoolihaiglana viib Kliinikum teisese eesmärgina läbi õppetööd. Õppetöö on igasugune õpiväljundite saavutamise eesmärgil läbiviidav tegevus, sh praktika ehk tegevus

juhendaja juhendamisel Kliinikumi töökeskkonnas ja kutse omandamine ehk osalemine tervishoiuteenuse osutamisel. Õppetöö eesmärgil on isikuandmete töötlemine lubatud järgnevatel tingimustel:

5.4.1. õppetöösse kaasatav või kaasatud patsient, tema põhiõigused, talle osutatav tervishoiuteenus, talle tervishoiuteenust osutav Kliinikumi Personali liige ja patsiendi lähedased on tingimusteta ja alati esikohal ning neid ei kahjustata ei otseselt ega kaudselt;

5.4.2. patsiendi isikuandmete töötlemine on õppetöö eesmärgi saavutamiseks vältimatult vajalik;

5.4.3. õppetöö eesmärgil isikuandmete töötlemine, sh haiguslooga tutvumine ja raviprotsessi jäädvustamine mis tahes vahendiga või viisil on lubatud ainult Korra punkti 4.2 vastavale nõusolekule. Patsientide isikuandmetel põhinevad õppematerjalid peavad olema koostatud mitteisikustatud ehk anonüümitud kujul.

5.4.4. praktika eesmärgil tervishoiuteenuse osutamise juures viibimine on lubatud on lubatud ainult Korra punkti 4.2 vastavale nõusolekule või seaduses toodud alusele. Praktika läbiviimisel tuleb järgida Kliinikumi praktika läbiviimise korras PKL-63 ja struktuuriüksuses kehtestatud reegleid isikuandmete kaitse osas;

5.4.5. kutse omandamise eesmärgil on lubatud TTKS § 4[3] toodud isikute osalemine tervishoiuteenuse osutamisel ja juurdepääs patsiendi isikuandmetele haigla ja tervise infosüsteemis tervise- ja tööministri määruses toodud tingimustel ja ulatuses.

5.5. Ülikoolihaiglana töötleb Kliinikum patsientide isikuandmeid teadustöö läbiviimise, sh teadusuuringu, kliinilise uuringu ja ravimiuuringute läbiviimise eesmärkidel vastavalt isikuandmete kaitse seaduse § 6 ja Kliinikumi kliiniliste teadusuuringute läbiviimise korras PKL-127 toodud tingimustele.

5.6. Eesmärgi piirangu tagamiseks, pääsuõiguste väärkasutamise ärahoidmiseks ja rikkumiste uurimiseks logib Kliinikum haigla infosüsteemis vähemalt isikuandmete sisestamise, muutmise, vaatamise ja kustutamise toimingud vastavalt õigusaktides ja Kliinikumi sisekordades toodud nõuetele. Logiandmeid säilitatakse vähemalt 5 aastat logitavast toimingust. Andmekaitsespetsialistil on juurdepääsuõigus kõikide Kliinikumi infosüsteemide logidele eesmärgi piirangu kontrollimise eesmärgil.

6. Minimaalsus ja õigsus

6.1. Isikuandmeid töötlev struktuuriüksus tagab, et töötlustoimingu eesmärgi saavutamiseks töödeldakse minimaalses vajalikus ulatuses isikuandmeid. Töödeldavate isikuandmete kategooriad dokumenteeritakse isikuandmete töötlemisülevaates.

6.2. Isikuandmeid koguvad vormid (nii elektroonilisel kui ka paberkujul) peavad sisaldama üksnes isikuandmeid, mis on töötlustoimingu eesmärgist lähtuvalt vältimatult vajalikud. Vabatahtlikud andmeväljad peavad olema selgelt tähistatud.

6.3. Ravitöö tuleb dokumenteerida vastavalt TTKSis, selle rakendusaktides ning teistes eriseadustes ja Kliinikumi kordades toodud nõuetele ja andmekoosseisudele.

6.4. Kui isikuandmete töötlemise eesmärgist tulenevalt (eelkõige õppe- ja/või teadustöö puhul) ei ole vajalik isikuandmete töötlemine isikustatud kujul, siis isikuandmeid töötlev struktuuriüksus anonüümib või pseudonüümib isikuandmed või kasutab isikuandmete kaitseks muud samaväärset meedet.

6.5. Isikuandmeid töötlev struktuuriüksus rakendab Kliinikumis ja/või struktuuriüksuses kehtivaid kvaliteediprotseduure, et tagada töödeldavate isikuandmete terviklus, ajakohasus ja asjakohasus. Andmesubjekti või muu õigustatud isiku taotlusel parandatakse ebaõiged isikuandmed ja asjakohastel juhtudel teavitatakse parandatud isikuandmete edastajaid ja/või vastuvõtjaid.

7. Konfidentsiaalsus

7.1. Kõik Personali liikmed peavad isikuandmete töötlemisel järgima lepingulist tähtajatut saladuse hoidmise kohustust.

7.2. Kliinikumile tervikuna ja kõigile Kliinikumi Personali liikmetest tervishoiutöötajatele ning teistele tervishoiuteenuse osutamisel osalevatele isikutele isiklikult kehtib tervishoiuteenuse osutamisel patsienti ja teda puudutava teabe osas seadusest tulenev tähtajatu saladuse hoidmise kohustus. Patsiendi saladuse hoidmise kohustusest võib kõrvale kalduda Korra käesoleva peatüki tingimustel ning lähtudes esmajoones patsiendi tahteavaldustest ja kutse-eetika normidest

7.3. Isikuandmeid edastav Personali liige tuvastab igakordselt vastuvõtja isikusamasuse ning vastuvõtja õiguse isikuandmeid töödelda vastavalt Korra punktidele 7.5-7.9.

7.4. Patsientide terviseandmete edastamisel järgib isikuandmeid edastav Personali liige Kliinikumis kehtivaid nõudeid, eriti isiku tervislikku seisundit kajastavate andmete andmekandjatel väljastamise, kasutamise ja transportimise juhendit JKL-62.

7.5. Andmesubjektil või tema seaduslikul esindajal on õigus tutvuda enda isikuandmetega, sh saada neist elektrooniline koopia riikliku tervise infosüsteemi patsiendiportaali digilugu.ee või Kliinikumi patsiendiportaali ePatsient vahendusel või esitades pöördumise vastavalt Korra punktile 3.3.

7.6. Isikuandmeid töötlev struktuuriüksus võib isikuandmeid edastada või muul viisil kättesaadavaks teha Personali liikmetele nende ülesannete täitmiseks vajalikus ulatuses. Kõik isikuandmeid töötlevad Personali liikmed peavad olema seotud lepingulise konfidentsiaalsuskohustusega ja olema teavitatud Kliinikumis kehtivate isikuandmete kaitse ja infoturbe nõuete osas.

7.7. Isikuandmeid töötlev struktuuriüksus võib edastada isikuandmeid Kliinikumi välistele vastuvõtjatele Eesti Vabariigis:

- 7.7.1. **seadusest tuleneva kohustuse olemasolul**:
  - 7.7.1.1. riigiasutustele, sealhulgas Tervisekassale, Sotsiaalministeeriumile ja tema allasutustele tervishoiu õigusaktides ettenähtud andmekoosseisus ja tingimustel;
  - 7.7.1.2. pädevatele riigi- või kohaliku omavalitsuse asutusele või eraõiguslikele isikutele muudes eriseadustes toodud teavitamiskohustuste täitmiseks minimaalselt vajalikus ulatuses;
- 7.7.2. **seadusest tuleneva õiguse olemasolul minimaalselt vajalikus ulatuses**:
  - 7.7.2.1. haiglaravil viibiva andmesubjekti lähedastele, kui andmesubjekt või muu pädev isik pole andmete edastamist keelanud;
  - 7.7.2.2. pädevale riigiasutusele, sh uurimisasutusele või kohtule, või kohaliku omavalitsuse asutusele patsiendi või teise isiku olulise kahjustamise ärahoidmiseks. Isikuandmeid edastada plaaniv Personali liige konsulteerib enne isikuandmete edastamist vajadusel andmekaitsespetsialistiga;
- 7.7.3. **koostöölepingus ettenähtud ulatuses koostööpartneritele**. Isikuandmeid töötleva struktuuriüksuse juht teavitab enne koostöölepingu sõlmimist ja isikuandmete edastamist andmekaitsespetsialisti, kes nõustab struktuuriüksust isikuandmete töötlemise rollide ja lepingusätete osas. Andmekaitsespetsialist võib kehtestada Kliinikumi andmetöötluslepingute kohustuslikud vormid;
- 7.7.4. **patsiendi nõusolekul** vastavas nõusolekus toodud ulatuses ja vastuvõtjatele;
- 7.7.5. muudel erandjuhtudel **patsiendi eluliste huvide** kaitseks.

7.8. Isikuandmeid võib edastada väljaspool Eesti Vabariiki asuvatele vastuvõtjatele, kui vastuvõtja töötleb isikuandmeid Euroopa Majanduspiirkonnas või muus piisava

andmekaitse tasemega riigis vastavalt Euroopa Komisjoni veebilehel edastamise hetkel kehtivale loetelule.

7.9. Kui vastuvõtja töötleb isikuandmeid ebapiisava andmekaitse tasemega riigis, tuleb enne isikuandmete edastamist kaasata andmekaitsespetsialist, et tagada IKÜM artiklitele 46-49 vastava kaitsemeetme rakendamine ja hinnata andmekaitsealase mõjuhinnangu läbiviimise vajadust.

7.10. Töötlustoimingu väliste vastuvõtjate kategooriad ja isikuandmete edastamine ebapiisava andmekaitse tasemega riiki registreeritakse isikuandmete töötlemisülevaates.

8. Usaldusväärsus

8.1. Kliinikum rakendab isikuandmete konfidentsiaalsuse, käideldavuse, ja tervikluse tagamiseks isikuandmete töötlemisele ohule vastavaid turvameetmeid. Töötlustoimingu kaitsetase ja sellest lähtuvad füüsilised, tehnilised ja korralduslikud turvameetmed määratakse kindlaks vastavalt Kliinikumi infoturvapoliitikas PKL-224 toodud reeglitele.

8.2. Isikuandmeid võib töödelda ainult Kliinikumi poolt ettenähtud või heaks kiidetud infosüsteemide ja muude tehniliste vahenditega (edaspidi koos **infosüsteemid**). Kliinikum dokumenteerib töötlustoimingus kasutatavad infosüsteemid isikuandmete töötlemisülevaates.

8.3. Isikuandmeid töötlev struktuuriüksus kinnitab Personali liikmete juurdepääsud infosüsteemidele nende ülesannete täitmiseks vajalikus ulatuses vastavalt infosüsteemi õiguste korrale PKL-109, infosüsteemi haldamise korrale PKL-197 ja õiguste registri pidamise korrale PKL-198.

8.4. Kõik Personali liikmed peavad isikuandmete töötlemisel rakendama Kliinikumi sisekordades kehtestatud turvameetmeid, eriti Kliinikumi infosüsteemi kasutamise korras PKL-126 ja isikliku seadme kasutamisel Kliinikumi töökorras PKL-65 toodud nõudeid.

8.5. Isikuandmeid töötlev struktuuriüksus tagab kasutatavate hoonete ja ruumide turvalisuse vastavalt Kliinikumi ruumide turvameetmete ning läbipääsusüsteemide haldamise ja nende rakendamise korrale PKL-120.

8.6. Kliinikum rakendab eraõigusliku teabevaldajana avalikus teabes sisalduvate isikuandmete kaitseks avaliku teabe seaduses toodud nõudeid vastavalt Kliinikumi asjaajamise ja teabehalduse korrale PKL-28.

8.7. Iga Personali liige on kohustatud isikuandmetega seotud rikkumisest (edaspidi **rikkumine**) või selle kahtlusest teadasaamisest viivitamata teavitama andmekaitsespetsialisti. Kliinikumi infosüsteemiga seotud intsidendi puhul tuleb täiendavalt teavitada Kliinikumi informaatikateenistuse kasutajatuge.

8.8. Rikkumist menetleb andmekaitsespetsialist, kes:

8.8.1. kogub vajadusel täiendavat teavet rikkumise asjaolude väljaselgitamiseks;

8.8.2. võimalusel korraldab meetmeid rikkumise ärahoidmiseks või kahjude vähendamiseks. Asjakohased Personali liikmed on kohustatud tegema andmekaitsespetsialistiga koostööd parandusmeetmete rakendamisel, rikkumise mõjude vähendamisel ja rikkumise lõpetamisel;

8.8.3. hindab rikkumise poolt põhjustatud ohtu või kahju andmesubjektidele ning esitab oma hinnangu infoturbe nõukogule:

8.8.3.1. kui rikkumine põhjustas või tõenäoliselt põhjustab **ohu** andmesubjektide õigustele ja vabadustele, otsustab infoturbe nõukogu rikkumise teavitamise osas ja korraldab meetmed rikkumise ärahoidmiseks, lahendamiseks või kahjude vähendamiseks. Andmekaitsespetsialist teavitab vastavalt infoturbe nõukogu otsusele viivitamata, kuid mitte hiljem kui 72 tunni jooksul pärast rikkumisest teadasaamist Andmekaitse Inspektsiooni;

8.8.3.2. Kui rikkumine põhjustas või tõenäoliselt põhjustab **suure ohu** andmesubjektide õigustele ja vabadustele, teavitab infoturbe nõukogu Kliinikumi juhatust, kes otsustab rikkumise teavitamise ja korraldab meetmed isikuandmetega seotud rikkumise ärahoidmiseks, lahendamiseks või kahjude vähendamiseks. Lisaks Andmekaitse Inspektsioonile teavitab Kliinikum juhatuse otsusel rikkumisest põhjendamatu viivituseta kõiki mõjutatud andmesubjekte. Andmesubjektidele edastatav teade peab selgitama selges ja lihtsas keeles rikkumise olemust, võimalike tagajärgede kirjeldust, parandusmeetmete kirjeldust ja Kliinikumi kontaktisiku nime ja kontaktandmeid. Andmesubjektide teavitamine ei ole vajalik IKÜM artiklis 34 lõikes 3 toodud asjaolude esinemisel.

8.8.4. registreerib rikkumise, analüüsib rikkumist ja teeb isikuandmeid töötlevale struktuuriüksusele ettepanekuid parandusmeetmete rakendamiseks. Andmekaitsespetsialist teeb registreeritud rikkumistest juhatusele ülevaate vähemalt üks kord aastas.

8.9. Kui rikkumisel on Kliinikumi infosüsteemide turvalisusele või teenuste toimepidevusele oluline mõju või olulist mõju võib mõistlikult eeldada küberturvalisuse seaduse § 8 tähenduses, teavitab Kliinikum

8.9.1. Riigi Infosüsteemi Ametit hiljemalt 24 tundi pärast rikkumisest teada saamist; ja

8.9.2. isikuid, keda olulise mõjuga küberintsident võib mõjutada, mõistliku aja jooksul pärast rikkumisest teada saamist.

8.10. Kliinikumi juhatuse otsusel teavitatakse ka muid pädevaid riigi- või kohaliku omavalitsuse asutusi, sealhulgas kuriteost Politsei- ja Piirivalveametit või elutähtsa teenuse katkestusest Sotsiaalministeeriumi.

9. Säilitamise piirang

9.1. Kliinikum säilitab isikuandmeid õigusaktidega sätestatud korras ja tähtajal, nende puudumisel määrab Kliinikum isikuandmete säilitamise tähtaja lähtuvalt Kliinikumi sisemisest vajadusest, koostöölepingust või muust kohalduvast alusest. Isikuandmete säilitamise tähtaeg või selle määramise alused dokumenteeritakse töötlemisülevaates.

9.2. Kliinikumi dokumentide säilitamise tähtajad määratakse kindlaks Kliinikumi dokumentide loetelus TKL-90.

9.3. Isikuandmete ja/või dokumentide säilitamise tähtaja ületamisel tagab isikuandmeid töötlev struktuuriüksus isikuandmete hävitamise:

9.3.1. Füüsilisel kujul andmekandjad kogutakse eraldi ja

9.3.1.1. arhiveeritakse vastavalt arhiivitöö eeskirjale PKL-121; või

9.3.1.2. hävitatakse vastavalt Kliinikumi jäätmekäitluseeskirjale PKL-89.

9.3.2. Elektroonilisel kujul isikuandmed arhiveeritakse, anonüümitakse või kustutatakse vastavalt infosüsteemi tehnilistele võimalustele.

10. Lõimitud ja vaikimisi andmekaitse

10.1. Isikuandmeid töötlev struktuuriüksus arvestab iga uue töötlustoimingu juurutamisel või olemasoleva töötlustoimingu muudatuste kavandamisel võimalikku ohtu andmesubjektidele. Ohu maandamiseks rakendab töötlustoimingu eest vastutav struktuuriüksus Korras toodud andmekaitse põhimõtteid ja ohule vastavaid turvameetmed kogu isikuandmete töötlemise elutsükli jooksul. Vajadusel konsulteerib isikuandmeid töötlev struktuuriüksus enne muudatuste rakendamist andmekaitsespetsialistiga.

10.2. Kui olemasoleva töötlustoimingu muudatused või uus töötlustoiming võivad kujutada andmesubjektidele suurt ohtu, kaasab isikuandmeid töötlev struktuuriüksus

andmekaitsespetsialisti, kes nõustab struktuuriüksust andmekaitsealase mõjuhinnangu (edaspidi **Mõjuhinnang**) läbiviimise vajaduse osas.

10.3. Suur oht andmesubjektidele võib esinda iga käesolevas punktis toodud tingimuse esinemise korral. Mida rohkem tingimusi esineb, seda suurem on oht andmesubjektidele. Mõjuhinnangu võib alati läbi viia ka vabatahtlikult, kuid mõjuhinnangu läbiviimine on üldjuhul kohustuslik kahe või enama järgneva tingimuse esinemise korral:

10.3.1. isikuandmete ulatuslik töötlemine (tavaliiki isikuandmete puhul rohkem kui 10 000 ja eriliiki isikuandmete puhul rohkem enam kui 5000 andmesubjekti isikuandmed);

10.3.2. eriliiki isikuandmete, sh terviseandmete või geneetiliste andmete, töötlemine;

10.3.3. haavatavate andmesubjektide kategooriate (sh alaealised patsiendid, piiratud teovõimega patsiendid, sotsiaalabi vajavad patsiendid) isikuandmete töötlemine;

10.3.4. isikuandmete edastamine ebapiisava andmekaitse tasemega riiki või vastuvõtjale;

10.3.5. andmesubjektide süstemaatiline hindamine või jälgimine;

10.3.6. osaliselt või täielikult automatiseeritud otsuste tegemine, mis toob andmesubjektile kaasa õigusliku tagajärje või muu olulise mõju, sealhulgas tervishoiuteenuse osutamisest keeldumise;

10.3.7. olemasoleva tehnoloogia uuenduslik kasutamine või uue tehnoloogia juurutamine;

10.3.8. andmekogumite sobitamine või kombineerimine;

10.3.9. muu Andmekaitse Inspektsiooni poolt kehtestatud töötlustoiming vastavalt IKÜM artiklile 35(4) või muu töötlustoiming, mis toob kaasa eeltoodud tingimustega võrreldava suure ohu.

10.4. Mõjuhinnangu mitte läbiviimine vähemalt kahele suurele ohule viitava tingimuse esinemisel tuleb dokumenteerida koos andmekaitsespetsialisti arvamusega ja soovitustega vähemalt kirjalikult taasesitamist võimaldavas vormis.

10.5. Pärast suure ohu tuvastamist viib isikuandmeid töötlev struktuuriüksus läbi Mõjuhinnangu. Eesmärk on hinnata, kas isikuandmete kaitseks rakendatavad meetmed on piisavad, et tõenäolisi ohte maandada või leevendada vastuvõetavale tasemele.

10.5.1. Isikuandmeid töötlevad struktuuriüksused kaasavad Mõjuhinnangu läbiviimisesse andmekaitsespetsialisti, kes registreerib Mõjuhinnangu ja nõustab struktuuriüksuseid Mõjuhinnangu läbiviivise metodoloogia, ohtude tuvastamise, hindamise ja maandamise osas;

10.5.2. Kui Mõjuhinnangu raames on vajalik ka infosüsteemi(de) riskianalüüsi koostamine küberturvalisuse seaduse alusel, kaasatakse Mõjuhinnangu läbiviimisesse infoturbejuht ja riskianalüüs viiakse läbi koos Mõjuhinnanguga;

10.5.3. Mõjuhinnang tuleb koostada vähemalt kirjalikku taasesitamist võimaldavas vormis ja peab sisaldama vähemalt IKÜM artiklis 33 nõutud teavet. Andmekaitsespetsialist võib kehtestada mõjuhinnangule kohustusliku vormi;

10.5.4. Sarnast suurt ohtu kujutavaid töötlustoiminguid võib hinnata koos, sh juba läbi viidud Mõjuhinnanguid täiendades;

10.5.5. Kui Kliinikum ei suuda Mõjuhinnangus tuvastada meetmeid, mis maandaksid ohu vastuvõetavale tasemele ja suure ohu realiseerumine andmesubjektidele on tõenäoline, edastab andmekaitsespetsialist mõjuhinnangu projekti eelkonsulteerimiseks Andmekaitse Inspektsioonile. Kliinikum järgib Mõjuhinnangu edasise läbiviimise osas Andmekaitse Inspektsiooni juhiseid;

10.5.6. Isikuandmeid töötlev struktuuriüksus esitab Mõjuhinnangu kinnitamiseks Kliinikumi juhatusele, kes kinnitab tuvastatud ohtude maandamiseks rakendatavad meetmed;

10.5.7. Andmekaitsespetsialist registreerib juhatuse poolt kinnitatud mõjuhinnangud ja jälgib tuvastatud ohtude maandamist isikuandmeid töötlevate struktuuriüksuste poolt;

10.5.8. Mõjuhinnangut uuendatakse töötlustoimingu oluliste muudatuste puhul, uue sarnase töötlustoimingu lisandumisel või hiljemalt 3 aasta jooksul mõjuhinnangu kinnitamisest.

VIITED

PKL-224	Infoturvapoliitika
PKL-212	Isikuandmete töötlemine töösuhtes
PKL-194	Isikuandmete töötlemise üldtingimused
TKL-268	Kliinikumi töötlemisülevaade
JKL-100	Kliinikumi töötaja käitumine suhtlemisel töökaaslase, patsiendi ja tema lähedastega
PKL-63	Praktika läbiviimise kord
PKL-127	Kliiniliste teadusuuringute läbiviimise kord
JKL-62	Isiku tervislikku seisundit kajastavate andmete andmekandjatel väljastamise, kasutamise ja transportimise juhend
PKL-109	Infosüsteemi õiguste kord
PKL-197	Infosüsteemi haldamise kord
PKL-198	Infosüsteemi õiguste registri pidamise kord
PKL-65	Töökord
PKL-120	Ruumide turvameetmete ning läbipääsusüsteemide haldamise ja nende rakendamise kord
TKL-90	Kliinikumi dokumentide loetelu
PKL-121	Arhiivitöö eeskiri
PKL-89	Jäätmekäitluseeskiri