

ANDMEKAITSE KORD

SISUKORD

1. SISSEJUHATUS	1
2. ASJAKOHASED ÕIGUSAKTID	1
3. MÕISTED	2
4. ANDMETE TÖÖTLEMISE PÕHIMÕTTED	3
5. ANDMETE TÖÖTLEMINE PILVETEENUSTES JA TEHISINTELLEKTI ABIL	3
6. VASTUTUS.....	4
7. ANDMESUBJEKTI ÕIGUSED.....	5
8. ANDMETE AVALDAMINE KOLMANDATELE OSAPOOLTELE.....	6

1. SISSEJUHATUS

- 1.1 Käesoleva juhendi eesmärk on tagada andmete väärtust loov, turvaline ja seaduslik töötlemine, mis toetab Ravimiameti ülesannete täitmise tõhusust, usaldusväärsust ja andmesubjektide õiguste kaitset.
- 1.2 Käesolev juhend kirjeldab andmetele juurdepääsu andmise ning andmete kogumise, töötlemise, jagamise, säilitamise ja kustutamise põhimõtted, Ravimiameti ja teenistujate vastutust ja käitumisjuhiseid, Ravimiameti teenistujatele suunatud tegevusjuhiseid andmete turvalisust mõjutavate intsidentidele ja andmesubjektide pöördumistele reageerimiseks; samuti andmesubjekti õiguste tagamise, sealhulgas isikuandmetele juurdepääsu, nende parandamise ja ajakohastamise korda.

2. ASJAKOHASED ÕIGUSAKTID

- 1) Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).
- 2) Isikuandmete kaitse seadus (IKS).
- 3) Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus (EKTÄKS).
- 4) Avaliku teabe seadus (AvTS).
- 5) Ravimiseadus (RavS).
- 6) Andmekaitse Inspektsiooni juhised.

3. MÕISTED

- 3.1 **Andmed** - andmeteks, mille töötlemisele käesolev juhend kohaldub, on 1) isikuandmed, sh eriliigilised isikuandmed ja 2) andmed, mida tuleb käsitleda ärisaladusena. Muu juurdepääsupiiranguga teabe töötlemisel lähtub Ravimiameti teenistuja ülalviidatud õigusaktidest.
- 3.2 **Isikuandmed** - igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.
- 3.3 **Eriliiki isikuandmed** - eriliiki isikuandmeteks loetakse selliseid isikuandmeid, mis annavad teavet isiku rassilise või etnilise kuuluvuse kohta, näitavad tema poliitilisi, religioosseid või maailmavaatelisi veendumusi, seksuaalset sättumust, ametiühingusse kuulumist või on seotud isiku tervisega. Biomeetrilised andmed ja geenandmed on samuti eriliiki isikuandmed. Eriliiki isikuandmed puudutavad eriti isiklikke ja intiimseid eluvaldkondi, seetõttu võib nende seadusevastane või hooletu töötlemine viia eelarvamuste tekke või diskrimineerimiseni. Nendel asjaoludel on eriliiki isikuandmete töötlemine lubatud üksnes erandjuhtudel.
- 3.4 **Isikuandmete töötlemine** - isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamine, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine.
- 3.5 **Ärisaladus** - ärisaladus on ettevõtja konkurentsieelis. Ärisaladuseks on eelkõige kaubanduslikku või tehnilist laadi teave, mis ei ole avalikult kättesaadav ja mida ettevõtja hoiab salajas, sest selle teabe teistele isikutele õigustamata teatavaks saamine kahjustab ettevõtja ärihuve. Ärisaladus on teave, mis vastab EKTÄKS § 5 lõikes 2 sätestatud tingimustele.
- 3.6 **Andmesubjekt** – isikuandmete puhul on andmesubjektiks füüsiline isik ehk inimene, kelle andmeid töödeldakse. Ärisaladuse puhul on andmesubjektiks juriidiline isik, kelle ärihuve see puudutab.
- 3.7 **Krüpteerimine** - loetaval kujul oleva informatsiooni muutmine loetamatuks. Failide krüpteerimine aitab kaitsta failide sisu.
- 3.8 **Pseudonümiseerimine** – isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga, tingimusel et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava füüsilise isikuga seostamise vältimise tagamiseks võetakse tehnilisi ja korralduslikke meetmeid.
- 3.9 **Anonüümimine** - teabest kõikide jälgede kaotamist, mis võiksid viia tuvastatavate isikuteni. Kui pseudonümimine ja krüpteerimine on tagasipööratav umbisikustamine, siis anonüümimine tähendab tagasipööramatut ehk lõplikku umbisikustamist.
- 3.10 **Pilveteenus** - internetipõhine lahendus, mida kasutatakse andmete töötlemiseks, varundamiseks, failide jagamiseks ning erinevate veebirakenduste kasutamiseks ilma, et kasutajal oleks vaja neid ressursse oma seadmesse paigaldada või hallata.
- 3.11 **Tehisintellekt/tehisintellektirakendus** – lahendus, mis kasutab andmetest õppivaid mudeleid või reeglipõhiseid algoritme, et teha järeldusi, prognoose või soovitusi; selliste lahenduste kasutamisel tuleb tagada andmekaitse põhimõtete järgimine ja teabe turvaline käsitlemine.

4. ANDMETE TÖÖTLEMISE PÕHIMÕTTED

- 4.1 Raviamet on haldusasutus, mis töötleb isikuandmeid seaduse ja nende alusel antud õigusaktidega temale pandud ülesannete täitmisel ja täitmiseks ning seadusega lubatud ulatuses.
- 4.2 Andmete töötlemine Raviametis on seaduslik, õiglane ja andmesubjektile läbipaistev (seaduslikkus, õiglus, läbipaistvus).
- 4.3 Isikuandmete töötlemise põhimõtted on kooskõlas isikuandmete kaitse üldmääruse artiklis 5 sätestatud nõuetega.
- 4.4 Andmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus.
- 4.5 Isikuandmete töötlemine on igasugune isikuandmetega tehtav toiming nagu kogumine, dokumenteerimine, kohandamine, muutmine, lugemine, säilitamine, hävitamine jmt.
- 4.6 Raviametis töödeldakse nii isikuandmeid, sh eriliigilisi isikuandmeid, kui ettevõtja ärisaladusena käsitletavaid andmeid.
- 4.7 Üldiseid isikuandmeid töödeldakse isikutega suhtlemisel, kui teada on isiku nimi ja kontaktandmed (nimi, elukohta aadress, telefoninumber või e-maili aadress).
- 4.8 Eriliigilisi isikuandmeid töödeldakse järelevalve tegemisel (näiteks retseptiravimite müüki kontrollides, kliiniliste uuringute inspekteerimisel), müügiloata ravimite turustamiseks ja ravimitega reisimiseks lubade andmisel, ravimite kvaliteedidefekti teadete hindamisel, meditsiiniseadmetega seotud kaebuste käsitlemisel, patsiendi kõrvaltoime teatiste kogumisel ja vaktsiinikahju taotluse menetluses põhjusliku seose hindamisel.
- 4.9 Töödeldavate andmete liigid, nende töötlemise alused ja säilitustähtajad on dokumenteeritud Raviameti töötlemistoimingute registrist (SISE_RA Üldine\Andmekaitse).
- 4.10 Raviametis säilitatakse teenistujate ja klientide isikuandmeid töötlemistoimingute registris kirjeldatud eesmärkidel.
- 4.11 Isikuandmeid töödeldakse senikaua, kuni neid on vaja eesmärgi täitmiseks ning vastavalt kehtestatud säilitusaegadele (seadustest või tehingu iseloomust tulenevad säilitusajad). Kui isikuandmete säilitusaeg on möödunud, isikuandmed kustutakse vastavalt andmekaitsealasele seadusandlusele.
- 4.12 Andmesubjektile on Raviameti veebilehel avaldatud teave isikuandmete töötlemisest.

5. ANDMETE TÖÖTLEMINE PILVETEENUSTES JA TEHISINTELLEKTI ABIL

- 5.1 Teenistujal on lubatud tööülesannete täitmisel andmete töötlemiseks kasutada arvutitöökoha või raviametite võrgustiku raames pakutavaid või juhtkonna poolt heakskiidetud pilveteenuseid ja tehisintellekti rakendusi, vastav info on leitav siseveebis (IT-abi). Andmete töötlemisel pilveteenustes ja tehisintellekti rakendustes tuleb järgida avaliku teabe seaduses (AvTS) ning kehtivates andmekaitse regulatsioonides, eelkõige isikuandmete kaitse üldmääruses (IKÜM) ja isikuandmete kaitse seaduses (IKS) sätestatud nõudeid.
- 5.2 Avalikke andmeid on üldjuhul lubatud töödelda piiranguteta. Avalikeks andmeteks on mh üldised kodulehe tekstid, tehnilised juhendid, mis pole konfidentsiaalsed, turundusmaterjalid, anonüümsed näited, sisekasutuseks mõeldud, kuid mittetundlikud tekstid, mis ei sisalda isikuandmeid ega ärisaladusi.
- 5.3 Dokumentide liigitusskeemis asutusesiseseks kasutamiseks liigitatud andmeid (v.a p 5.4) on lubatud pilveteenustes töödelda minimaalsuse põhimõttel (nii vähe kui võimalik) ja tehisintellekti rakendustesse sisestada redigeeritult, st pärast füüsiliste ja juriidiliste isikute andmete eemaldamist (näiteks asutuse ja isikute nimedeta protsessikirjeldused, juhendid, aruanded, projektid, mittetundlik statistika ning tuvastamist võimaldavatest isikuandmetest puhastatud tööfailid).
- 5.4 Konfidentsiaalset ja tundlikku teavet on lubatud pilveteenustes töödelda minimaalsuse põhimõttel (nii vähe kui võimalik), kustutades selle esimesel võimalusel. Kehtivad järgmised põhimõtted:
 - Eriliigiliste isikuandmete *Sharepointis* töötlemine on lubatud menetluse ajal ainult SISE_RA või osakonna(teenuse)põhisel saidil, juurdepääsupiiranguga kaustas volitatud isikutele. Menetlusjärgsel säilitamisel tuleb andmed krüpteerida ka Raviameti nimele.

Igal võimalusel tuleks andmeid säilitada menetlusejärgselt ainult dokumendihaldussüsteemis.

- E-kirja sisutekstina kirjeldatud krüpteerimata eriliigiliste isikuandmete töötlemisel tuleb need asutusesiseses infovahetuses anonüümida. Menetlusejärgselt tuleb krüpteerimata kujul eriliigilisi isikuandmeid sisaldavad e-kirjad nii individuaalsetest kui ühiselt kasutatavatest e-posti kaustadest kustutada. Säilitamine on lubatud ainult krüpteeritud kujul või dokumendihaldussüsteemis.
- Ärisaladuse töötlemine ja säilitamine on lubatud ainult *Sharepointi* SISE_RA või osakonna(teenusepõhisel) saidil. Üldjuhul on vaikimisi lugemisõigus kõigile, muutmisõigus on lubatud ainult volitatud isikutele.

Tehisintellekti rakendustesse ei ole lubatud konfidentsiaalset ja tundlikku teavet sisestada. Konfidentsiaalsete ja tundlike andmete hulka kuuluvad mh isikuandmed; eriliigilised isikuandmed; järelevalveinfo; klientide nimed, kontaktid, isikukoodid, aadressid; lepingud, mis sisaldavad identifitseeritavaid detaile; ärisaladust sisaldav teave, dokumendid detailsete kliendiandmetega; siseauditid, turvaraportid, turvanõrkused; kogu info, mille avalikuks tulek põhjustaks kahju isikule või asutusele.

5.5 Teenistuja veendub enne andmete sisestamist, kas andmed vastavad lubatud kategooriale, kas pilveteenused ja tehisintellekti rakendused on tööalaseks kasutamiseks lubatud, kas andmete sisestamine on tööülesannete täitmiseks vajalik. Isikuandmed ja muud tundlikud andmed tuleb enne sisestamist eemaldada või anonüümida.

5.6 Teenistuja kontrollib alati tehisintellekti rakendusest saadud informatsiooni, mh selle faktitäpsust ja allikate usaldusväärsust. Saadud informatsiooni kasutamine ilma täiendava kontrollita ei ole lubatud.

6. VASTUTUS

6.1 Ravimiamet tagab, et isikuandmeid töötlevad teenistujad on teadlikud andmekaitse regulatsioonist ja isikuandmete vastutustundliku töötlemise põhimõtetest. Teadlikkust andmete töötlemise olulisusest ja järgimise vajadusest hoitakse ja tõstetakse järjepidevalt. Teenistujaid koolitatakse vähemalt kord aastas.

6.2 Kogutud isikuandmetele määratakse säilitamistähtaeg sõltuvalt andmete töötlemise eesmärgist. Säilitamistähtaja saabumisel isikuandmeid sisaldav andmestik kustutatakse või isikuandmed anonüümitakse.

6.3 Iga teenistuja vastutab selle eest, et tema valduses olevad isikuandmed oleksid hoolikalt hoitud ning nõuetekohaselt töödeldud. Isikuandmeid, millele juurdepääsuõigus on teenistujal oma tööülesannete täitmiseks, ei tohi edastada kõrvalistele isikutele.

6.4 Kui teenistujal on oma ülesannete täitmiseks antud juurdepääs mõnele andmekogule või infosüsteemile, tohib sealt teha üksnes tööülesannetega seonduvaid päringuid. Lubatud ei ole teha päringuid kellegi palvel või mõnel muul eesmärgil (lisaks, vt p 5.10).

6.5 Kui teenistuja saadab e-kirja ekslikult valele adressaadile, tuleb e-kirja saajat kohe teavitada toimunud eksimusest ning vajadusest saadud kiri kustutada. Teenistuja kustutab e-kirja saadetud andmete hulga (lisaks, vt p 5.10). Ravimiameti teenistujatel on juurdepääs tema ülesannete täitmiseks vajalikele isikuandmetele. Juurdepääs piiratud juurdepääsuga andmete võrguketastel ja dokumendihaldussüsteemis on määratud isikupõhiselt teenistuja tööülesannetest lähtuvalt.

6.6 Isikuandmetega kokku puutuvad teenistujad:

- 1) töötlevad isikuandmeid üksnes isikuandmete kaitse üldmääruses ja isikuandmete kaitse seaduses ettenähtud tingimustel ja korras ning lubatud eesmärkidel;
- 2) hoiduvad turvanõuete rikkumisest, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu;
- 3) täidavad Ravimiameti rakendatud asjakohaseid tehnilisi ja korralduslikke meetmeid, mis tagavad isikuandmete töötlemise kooskõlas isikuandmete kaitse üldmääruse ja isikuandmete kaitse seadusega,
- 4) täidavad teisi isikuandmete kaitse üldmäärusest ja isikuandmete kaitse seadusest tulenevaid kohustusi.

- 6.7 Andmete volitatud töötlejad on RIT (Riigi IT Keskus) ja TEHIK (Tervise ja Heaolu Infosüsteemide Keskus). Sõlmitud teenuslepingu kohaselt tagab volitatud töötleja logimise, logide regulaarse kontrolli, varundamise ja varukoopiate säilitamise. Andmete varundamise aeg on kokku lepitud teenuslepingu lisades, ligipääsu taotletakse põhjendatud vajadusel vastavalt Infovara juurdepääsuõiguste haldamise korrale.
- 6.8 Ravimiamet teeb logide pistelist ja juhtumipõhist kontrolli, kontrollib ja testib regulaarselt andmete töötlemisel tehniliste meetmete rakendamist, et veenduda nende tõhususes, turvalisuses ning vastavuses asjakohaste õigusaktidega.
- 6.9 Andmete volitamata töötlemisest teavitab teenistuja viivitamatult Ravimiameti andmekaitse spetsialisti (andmekaitse@ravimiamet.ee). Koheselt tuleb kasutusele võtta meetmed rikkumise lõpetamiseks.
- 6.10 Andmekaitse spetsialist hindab, kas toimunud rikkumine kujutab endast tõenäolist ohtu andmesubjekti õigustele ja vabadustele. Sellisel juhul vormistatakse selle kohta nõutud dokumendid ning esitatakse need Andmekaitse Inspeksioonile. Kui rikkumise tulemusena tekib andmesubjekti õigustele ja vabadustele tõenäoliselt suur oht, teavitatakse sellest andmesubjekti, et andmesubjektil oleks võimalik endal võtta vajalikke ettevaatusabinõusid olukorra leevendamiseks.

7. ANDMESUBJEKTI ÕIGUSED

- 7.1 Saada kinnitust, kas tema isikuandmeid töödeldakse (õigus saada ülevaadet).
- 7.2 Saada tasuta teavet, milliseid andmeid tema kohta töödeldakse (õigus olla informeeritud).
- 7.3 Nõuda isikuandmete kustutamist, kui seda võimaldavad ka teistest seadustest tulenevad nõuded (õigus unustamisele).
- 7.4 Nõuda isikuandmete korrigeerimist ja täiendamist, kui need on ebakorrektset (õigus parandada enda andmeid).
- 7.5 Nõuda oma isikuandmete töötlemise piiramist (õigus töötlemise piiramisele).
- 7.6 Õigus saada enda isikuandmed struktureeritud ja masinloetavas formaadis (õigus andmete edastamisele).
- 7.7 Õigus vaidlustada enda isikuandmete töötlemist (õigus esitada vastuväiteid).
- 7.8 Õigus igal ajal tagasi võtta vabalt antud nõusolek enda andmete töötlemiseks.
- 7.9 Andmesubjektile eriliigiliste isikuandmete saatmisel andmed krüpteeritakse, ärisaladuse saatmisel andmed võimalusel krüpteeritakse või küsitakse kirjalik nõusolek krüpteerimata kujul saatmiseks.
- 7.10 Teenistuja hoiab oma isikuandmeid ja isiklikke dokumente ainult selleks ettenähtud markeeritud kaustas OneDrive's. Personaalse OneDrive'i kasutamise kohta on sätestatud Infovara kasutamise kord. Teenistusest lahkumise korral saab teenistuja isiklikud dokumendid kaasa võtta.
- 7.11 Ravimiametist lahkunud teenistuja faile ja e-kirju säilitatakse 30 päeva, pikemaks säilitamiseks peab kasutaja vahetu juht saatma IT-kasutajatoele põhjendatud taotluse enne teenistuja teenistus- või töösuhte lõppemist märkides failide ja e-posti säilitamise soovitud tähtaja. Pärast seatud tähtaega kustutatakse teenistuja personaalseks kasutuseks antavatelt seadmetelt ja andmekandjatelt (sh irdandmekandjad) kõik andmed.

8. ANDMETE AVALDAMINE KOLMANDATELE OSAPPOOLTELE

- 8.1 Andmeid kolmandatele osapooltele ei jagata, välja arvatud juhul kui selleks on andmesubjekti nõusolek või kui see on seadusega nõutud (sh kohtuvaidluste korral). Isikuandmete kolmandate osapooltega jagamine võib osutuda vajalikuks näiteks kriminaalmenetluse käigus tehtud päringutele vastamiseks, ohtlike olukordade vältimiseks või intellektuaalomandi kaitseks.
- 8.2 Andmete jagamisel kolmandatele osapooltele õigustatud huvi olemasolul andmed vajadusel anonümiseeritakse, asendades piiratud juurdepääsuga andmed kas varjutuse või xxx-ga.