Sisukord

„Isikuandmete töötlemise korra" (edaspidi: kord) eesmärk on fikseerida Tervise ja Heaolu Infosüsteemide Keskuses (edaspidi: *TEHIK*) kokku lepitud praktika isikuandmete töötlemiseks.

1. Olulised mõisted isikuandmete töötlemisel

1.1. Isikuandmete kaitse üldmäärus (edaspidi: *üldmäärus*) – Euroopa parlamendi ja nõukogu määrus (EL) 2016/679, vastu võetud 27.04.2016 ning mis reguleerib füüsiliste isikute kaitset isikuandmete töötlemisel ja selliste andmete vaba liikumist. Üldtuntud nimedega ka IKÜM või GDPR. Määrus on liikmesriikidele täitmiseks kohustuslik ja seab riikide ülesed reeglid isikuandmete töötlemisele.

1.2. Isikuandmete kaitse seadus (IKS) – siseriiklik õigusakt, mis loob isikuandmete töötlemisega seotud reeglid nendeks juhtudeks, mille üldmäärus on jätnud iga liikmesriigi otsustuspädevusse (näiteks surnud isiku andmete töötlemise tingimused).

1.3. Isikuandmed – mistahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, kas andmed võimaldavad isiku tuvastamist kaudsel või otsesel teel. Isikuandmeteks on muuhulgas isiku nimi, foto, aadress ja muud kontaktandmeid, ekraaninimi (nn avatar), IP-aadress, jne. isikuandmetena ei ole käsitletavad juriidilise isiku (organisatsioon, ettevõte) andmed.

1.4. Eriliiki isikuandmed - andmeid, millest ilmneb isiku rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilised andmed, terviseandmed või andmed seksuaalelu ja seksuaalse sättumuse kohta ning füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed. Eriliiki isikuandmete töötlemine on keelatud, kui selleks ei esine konkreetset õiguslikku alust - nt tervishoiuteenuse osutamine, andmesubjekti enda nõusolek või andmete avaldamine, ülekaalukas avalik huvi jms (täpsemalt üldmääruse art 9 lg 2).

1.5. Anonümiseeritud isikuandmed – ka anonüümitud isikuandmed. Isikuandmed on muudetud või rikutud viisil, mis välistab nende konkreetse füüsilise isikuga seostamise. Isiku tunnused on viidud lõplikult tuvastamatule kujule ning isikut ei saa otse ega kaudselt tuvastada andmete omanik ja teised andmesaajad enda poolt andmete täiendamisega. Anonüümitud isikuandmetele ei kohaldu isikuandmete kaitse üldmäärusest tulenevad reeglid ning neid ei käsitleta isikuandmetena.

1.6. Pseudonümiseeritud/pseudonüümitud isikuandmed – Isikuandmed on muudetud või rikutud viisil, mis välistab nende konkreetse füüsilise isikuga seostamise pseudonüümitud kujul, kuid eksisteerib võimalus pseudonüümitud andmed taas isikustada (nt teades isikuandmete muutmise loogikat, saab pseudonüümimise tagasi pöörata).

1.7. Isikuandmete töötlemine – mistahes tegevus või toiming seoses isikuandmetega. Töötlemine hõlmab isikuandmete säilitamist, lugemist, saatmist, muutmist jne.

1.8. Andmetöötluse põhimõtted – üldmäärusest tulenevad ja tuletatud põhimõtted, mida tuleb mistahes isikuandmete töötlemisel järgida.

1.9. Andmekaitseametnik– direktori määratud töötaja, kellel on teadmised ja pädevus nõustada isikuandmete töötlemisel, õigus seada sisse asutuses kehtiv isikuandmete töötlemise kord ning kohustus tagada TEHIKus isikuandmete töötlemise seaduslikkus ja olla kontaktisikuks teistele asutustele.

1.10. Vastutav töötleja – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes määrab isikuandmete töötlemise eesmärgid ja vahendid – st töötlemise põhjuse ja viisi.

1.11. Kaasvastutav töötleja - füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes koos ühe või mitme isikuga määrab isikuandmete töötlemise eesmärgid ja vahendid, kuna nende poolne isikuandmete töötlemine on lahutamatult seotud. Ühine osalemine hõlmab eesmärkide ja vahendite kindlaksmääramist.

1.12. Volitatud töötleja - füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel. Volitatud töötleja töötleb andmeid vastutavat töötlejat ja volitatud töötlejat omavahel siduva lepingu või liidu või liikmesriigi õiguse kohase siduva õigusakti alusel. Volitatud töötleja ei tohi töödelda andmeid muul viisil kui vastutava töötleja juhiste kohaselt. Riiklikes andmekogudes ja TEHIKu poolt hallatavates

muudes infosüsteemides ja andmekogudes on TEHIK reeglina volitatud töötleja ega oma pädevust määrata isikuandmete töötlemise eesmärke ega vahendeid.

2. Üldnõuded isikuandmetega töötamisel

2.1. Isikuandmetele tohib töötaja ligipääsu saada üksnes talle määratud tööülesannete täitmiseks ja ettenähtud ajaks. Kui vajadus ligipääsu järele on lõppenud (nt tööülesanded teostatud või muutunud), tuleb ligipääs andmetele lõpetada vastavalt TEHIKus kehtestatud korrale.

2.2. Isikuandmete edastamine või muul viisil neile ligipääsu võimaldamine selleks õigust mitteomavale isikule on keelatud. Igaüks, kellele on tööülesannete täitmiseks isikuandmete töötlemise õigus tagatud, vastutab oma tegevuse õiguspärasuse eest.

2.3. Isikuandmeid peab töötlema turvalisel viisil, rakendades otstarbekaid infoturbemeetmeid.

2.4. Isikuandmete töötlusel tuleb tagada andmetöötluse minimaalsuse põhimõte. Isikuandmeid tuleb töödelda nii vähe kui võimalik, et seatud eesmärk saavutada. Keelatud on isikuandmeid töödelda suuremas mahus, kui see on tööks ja eesmärgi saavutamiseks vajalik.

2.5. Isikuandmete töötlemisel peab olema konkreetne eesmärk, mis ei saa andmetöötluse kestel muutuda. TEHIKu puhul tulenevad andmete töötlemise eesmärgid õigusaktist või asutusele pandud ülesannetest ja kohustustest (nt töölepingu seadusest tulenevad kohustused). Andmetöötluse eesmärgi muutumiseks on vajalik muudatus õigusaktist või kohustavas dokumendis/kokkuleppes. Uuel eesmärgil andmete töötlemiseks tuleb eelnevalt veenduda eesmärgi seaduslikkuses ja konsulteerida andmekaitseametnikuga.

2.6. Isikuandmeid on lubatav säilitada vaid nii kaua, kui see on eesmärgi täitmiseks vajalik või õigusaktis sätestatud tähtajani. Peale säilitamistähtaja möödumist tuleb andmed kustutada jäädavalt.

2.7. Isikuandmete töötlemisel tuleb läbi mõelda ja tagada isikuandmete turvalisus, sealhulgas kaitse loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustumise eest, rakendades asjakohaseid tehnilisi või korralduslikke meetmeid.

2.8. Kõik isikuandmete töötlemistoimingud infosüsteemis või andmekogus peavad olema logitud ja hiljem üheselt tuvastatavad. Logimisega tuleb tagada, et hilisemalt oleks ajaliselt tuvastatav nii andmete sisestamine, muutmine, vaatamine, edastamine kui ka kustutamine.

2.9. Isikuandmetele ligipääsu andmine kolmandale isikule, kes ei ole TEHIKu töötaja, peab võimalusel toimuma TEHIKu kontoriruumides ja seadmetega ning TEHIKu töötaja järelevalve all. Isikuandmete töötlemisel väljaspool kontoriruume peab andmeväljastaja veenduma, et on tagatud andmete töötlemise turvalisus ning välistatud kõrvaliste isikute kokkupuude isikuandmetega.

2.10. Isikuandmete töötlemine võib toimuda ainult õigusliku aluse olemasolul. TEHIK töötleb isikuandmeid reeglina üksnes õigusaktist tuleneval konkreetsel alusel avalikes huvides oleva ülesande täitmiseks või avaliku võimu teostamiseks.

2.11. Töödeldavad isikuandmed peavad olema õiged ja ajakohastatud, ebaõigeks muutunud või aegunud isikuandmed tuleb kustutada.

3. Isikuandmete töötlemistoimingute registreerimine

3.1. Kõik isikuandmete töötlemisega seotud tegevused peavad olema registreeritud andmetöötlusregistris. Andmetöötlusregistrisse lisatud andmete õigsuse ja tervikluse eest vastutab vastava osakonna juht, kus andmetöötlus põhiliselt (suuremas mahus) aset leiab.

3.2. Uute andmetöötlustoimingute või -viiside lisandumisel tuleb teha sellekohane kanne andmetöötlusregistrisse soovitatavalt enne andmetöötlusega alustamist, kuid mitte hiljem kui 30 päeva jooksul alates isikuandmete töötlemisega alustamisest.

3.3. Andmetöötlusregistrit peetakse TEHIKu ühiskettal tugiteenuste osakonna kaustas ja sellele on ligipääs kõigil töötajatel.

3.4. Andmetöötlusregistri olemasolu ja uuendamise eest vastutab andmekaitseametnik, võttes aluseks osakonna juhtidelt saadud info isikuandmete töötlemise kohta.

4. Isikuandmete töötlemine lepingute täitmisel

4.1. Isikuandmete töötlemist lepingulise partneri või muu selleks õigusakti kohaselt õigust mitteomava kolmanda asutuse (edaspidi: *kolmas asutus*) poolt tuleb vältida, kui töö on võimalik teostada ilma isikuandmeid töötlemata.

4.2. Võimalusel tuleb enne isikuandmete töötlemist andmed anonümiseerida (anonüümida) või pseudonümiseerida (pseudonüümida), jättes pseudonüümimisvõtme TEHIKu valdusesse.

4.3. Kui isikuandmete töötlemist ei ole võimalik mõistlikult vältida ilma, et tööd jääksid nõuetekohaselt teostamata, peab vastutav töötleja või volituse olemasolul TEHIKu esindusõiguslik isik sõlmima isikuandmeid töötleva asutusega kirjalikus vormis andmetöötluskokkuleppe.

4.4. Töötaja, kes taotleb andmetöötluskokkuleppe sõlmimist, peab esitama ja säilitama sisulised põhjendused, miks on tööde nõuetekohaseks teostamiseks isikuandmete töötlemine vältimatult vajalik.

4.5. Andmetöötluskokkuleppe vorm on avaldatud TEHIKu siseveebis või edastab selle andmekaitseametnik küsimisel. Vormi järgimine ja kasutamine kokkuleppe sõlmimisel on kohustuslik. Kõrvalekalded peab heaks kiitma andmekaitseametnik.

4.6. Vastutavat töötlejat tuleb andmetöötluskokkuleppe sõlmimisest teavitada ka kokkuleppe sõlmimiseks kirjaliku volituse olemasolul.

4.7. Kui isikuandmete töötlemine on vajalik hankelepingu täitmiseks, avaldatakse andmetöötluskokkuleppe tingimused riigihanke läbiviimisel.

4.8. Isikuandmetele ligipääsu võimaldamine kolmandale asutusele enne kirjaliku andmetöötluskokkuleppe sõlmimist on keelatud.

5. Isikuandmete töötlemine arendus- ja haldustöödes

5.1. Isikuandmete töötlemine arendus- ja haldustöödes (edaspidi töö). sh testimisel on keelatud.

5.2. Eeltoodud punktist saab põhjendatud erandi otsustada üksnes isikuandmete vastutav töötleja. Tööde teostamiseks isikuandmetega, peab TEHIK saama vastutava töötleja nõusoleku. Nõusolek võib olla antud TEHIKu ja vastutava töötleja vahel sõlmitud lepinguga.

5.3. Enne planeeritud tööde algust taotletakse erandit vastavalt Lisale 1.1 Taotlus isikuandmete kasutamiseks arendus- ja haldustöödes. Taotlus esitatakse kooskõlastamiseks Infoturbeosakonna juhile, äriteenuse osakonna juhile ja arhitektile. Taotlus säilitatakse dokumendihaldussüsteemis projekti materjalide juures.

5.4. Muuhulgas peab vastutav töötleja andma nõusoleku isikuandmete töötlemiseks, kui:

5.4.1. töödes esinevaid vigu on võimalik tuvastada üksnes isikuandmete abil ja vea tuvastamist ei ole võimalik teostada ühelgi muul mõistlikul viisil;

5.4.2. anonüümitud või pseudonüümitud isikuandmete kasutamine on võimatu, muudaks testimise töömahu ebamõistlikuks ja/või vea tuvastus ei ole muul viisil simuleeritav;

5.4.3. vajadus isikuandmete töötlemiseks on infosüsteemi või andmekogu arhitekti kinnitusel sisuliselt põhjendatud, tööde teostamine ei ole muul viisil võimalik.

5.5. Erandi taotlemisele lisatakse vajadusel mõjuhinnang. Mõjuhinnangu läbiviimise otsustab vastutav töötleja.

5.6. Tööde teostamiseks vajalikele isikuandmetele võimaldatakse ligipääs üksnes töötajatele, kellel on volitus tööde läbiviimiseks ja töödes esinevate vigade parandamiseks.

5.7. Kui isikuandmete töödeldakse testkeskkonnas, peab see vastama järgmistele nõuetele:

5.7.1. testkeskkonnale kohalduvad toodangukeskkonnaga sarnased turvanõuded, et tagada isikuandmete kaitse sarnaselt toodangukeskkonnas rakendatule. Mistahes erandid toodangukeskkonnast peavad olema fikseeritud ja põhjendatud;

5.7.2. testkeskkonnas teostatavad andmetöötlustoimingud teostatakse, sh logitakse toodangukeskkonna nõuete kohaselt, sh peab olema tagatud logide kättesaadavus järelevalve teostamiseks. Logid peavad olema kasutatavad TEHIKu keskse logihaldussüsteemi kaudu;

5.7.3. kasutatud andmekandjad tühjendatakse testimisel kasutatud andmetest säilitustähtaja lõppedes;

5.7.4. enne logide kustutamist tehakse logide analüüs. Logide analüüsi viib läbi infosüsteemi või andmekogu administraator ning esitab selle kooskõlastamiseks infoturbeosakonnale.

5.8. Testkeskkonnale esitatud nõuete täitmise eest vastutab testimise eest vastutav isik.

5.9. Testandmete kustutamisel peab osalema vähemalt kaks TEHIKu töötajat,

5.10. Testandmete kustutamine akteeritakse, akt säilitatakse dokumendihaldussüsteemis. Testandmete kustutamise akti peab allkirjastama 2 isikut, kellest vähemalt üks, kes osales logide analüüsis.

6. Mõjuhinnangu läbiviimine

6.1. Mõjuhinnang on isikuandmete töötlemisega alustamisele eelnev kirjalik analüüs, mis on kohustuslik läbi viia, kui isikuandmete töötlemise, eelkõige uut tehnoloogiat kasutava töötlemise tulemusena ning isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht. Sarnast suurt ohtu kujutavaid sarnaseid isikuandmete töötlemise toiminguid võib hinnata ühe mõjuhinnangu koostamise käigus.

6.2. Kohustus mõjuhinnangu tegemiseks on, kui toimub:

6.2.1. isiklike aspektide (nt isiku vaated, seisukohad, isikuomadused, harjumused, huvid, eelistused, sotsiaalne staatus, käitumine, asukoht, liikumine) süstemaatiline ja ulatuslik hindamine, mis põhineb automaatsel isikuandmete töötlemisel, sealhulgas profiilianalüüsil, ja millel põhinevad otsused, millel on füüsilise isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt füüsilist isikut;

6.2.2. isikuandmete eriliikide (nt terviseandmed) ulatuslik töötlemine.

6.3. Mõjuhinnangut uuendatakse, kui andmetöötluse viis või eesmärgid muutuvad.

6.4. Mõjuhinnangu läbiviimise ja koostamise eest vastutab isikuandmete vastutav töötleja. TEHIK kohustub enne arendustööde toodangu-keskkonnas kasutusele võtmist juhtima vastutava töötleja tähelepanu mõjuhinnangu läbiviimise kohustusele, kui on selge, et mõjuhinnang on või võib olla vajalik.

6.5. Kui mõjuhinnangu läbiviimine osutub vastutava töötleja hinnangul mittevajalikuks, tuleb säilitada sellekohane vastutava töötleja kirjalik hinnang.

6.6. Mõjuhinnangu läbiviimisel on kohustuslik kaasata andmekaitseametnik.

6.7. Kui isikuandmete vastutavaks töötlejaks on TEHIK, Mõjuhinnang peab sisaldama vähemalt järgnevat:

6.7.1. isikuandmete töötlemise toimingute ja töötlemise eesmärkide, sealhulgas vastutava töötleja õigustatud huvi kirjeldus;

6.7.2. isikuandmete töötlemise toimingute vajalikkuse ja proportsionaalsuse hindamine töötlemise eesmärkide suhtes;

6.7.3. andmesubjektide õigusi ja vabadusi puudutavate ohtude hinnang;

6.7.4. ohtude käsitlemiseks kavandatud meetmed, sealhulgas tagatised, turvameetmed ja mehhanismid isikuandmete kaitse tagamiseks ja määruse järgimise tõendamiseks, võttes arvesse andmesubjektide ja teiste asjaomaste isikute õigusi ja õigustatud huve.

6.8. TEHIK andmetöötluse kohta koostatava mõjuhinnangu vorm on avaldatud TEHIKu siseveebis või edastab selle andmekaitseametnik küsimisel. Vormi järgimine ja kasutamine kokkuleppe sõlmimisel on kohustuslik, kõrvalekalded peab heaks kiitma andmekaitseametnik. Kui TEHIK on andmekogu volitatud töötleja tagab mõjuhinnangu läbiviimise vastutav töötleja.

7. Isikuandmete kaitse nõuete rikkumine

7.1. Mistahes isikuandmetega seotud rikkumise kohta peab olema registreeritud Jira intsidendi raport, millele on lisatud juurde silt (*label*) „Andmekaitse". Raport peab olema koostatud niipea kui võimalik.

7.2. Mistahes isikuandmetega seotud rikkumisest tuleb teavitada viivitamatult TEHIKu andmekaitseametnikule aadressil andmekaitse@tehik.ee.
   7.2.1. Teavitus ei tohi olla esitatud hiljem, kui 24 tunni jooksul rikkumisest teada saamisest.
   7.2.2. Teavitus peab sisaldama kõiki rikkumisega seotud andmeid, mis sel hetkel teada on. Andmekaitseametnik vastutab õigeaegse ja täieliku info edastamise eest vastutavale töötlejale ja järelevalveasutusele, mistõttu on tema eest andmete varjamine keelatud.
   7.2.3. Andmekaitseametnikul on õigus nõuda rikkumise kohta täpsemate andmete välja selgitamist, kaasata asja lahendamisse täiendavaid TEHIKu töötajaid ning paluda esitada rikkumise kohta täpsemad andmed konkreetsel vormil. Viimasel juhul edastab andmekaitseametnik vastava vormi täitmiseks e-kirjaga.

7.3. Rikkumisega seotud teabevahetust teiste asutustega (vastutava töötlejaga), sh järelevalveasutusega korraldab andmekaitseametnik . Rikkumisega seotud info edastamine teistele asutustele ilma andmekaitseametnikuga konsulteerimata on keelatud, v.a esmase teavituse viivitamatu saatmine erakorralist reageerimist nõudval juhul, kui rikkumisest tulenevalt on vaja piirata või lõpetada teise asutuse tegevust või sellest on mõjutatud avalike teenuste pakkumine vmt. Andmekaitseametnikku tuleb teisele asutusele saadetud täielikust infost informeerida.

7.4. Rikkumisega seotud teabevahetust registreeritakse Deltas. Rikkumisteadete register asub Jiras.

Lisa 1.1

„Taotlus isikuandmete kasutamiseks arendus- ja haldustöödes"

1. Andmekogu nimi ja vastutav töötleja.
2. Kasutatavate andmete koosseis ja maht (arvesta p 2.4).
3. Töötlemise eesmärk ja läbiviimise aeg.
4. Põhjendus, miks ei ole võimalik töid läbi viia isikuandmeteta.
5. Vastutava töötleja kinnitus mõjuhinnangu läbiviimise või selle läbiviimise vajaduse puudumise kohta. Mõjuhinnangu olemasolul lisatakse see taotlusele.
6. Testkeskkonna loomise ja haldamise ning alternatiivsete lahenduste hinnanguline maksumus.
7. Töötlemisel rakendatavad kaitsemeetmed.
8. Töötlemisega seotud andmed säilitamise tähtaeg ja põhjendus ning kuidas tagatakse nõuetekohane kustutamine.
9. Töötlemise eest vastutava isiku kontaktandmed (nimi, e-posti aadress, osakond ja ametikoht).