

ANDMETÖÖTLUSE LEPING

Käesolev isikuandmete töötlemist puudutav lepingulisa 3 (edaspidi: **lisa**) on lahutamatu osa riigihanke Majutamise teenuse osutamine Sotsiaalkindlustusametile ja Päästeametile“ (viitenumber 299920 tulemusena sõlmitud hankelepingust (edaspidi: **leping**), mis sõlmitakse Sotsiaalkindlustusameti (edaspidi: **vastutav töötleja**) ja AS Heal (edaspidi: **volitatud töötleja**) vahel.

Vastutavat töötlejat ja volitatud töötlejat nimetatakse edaspidi eraldi ka kui **pool** ning ühiselt kui **pooled**.

1. Lisa eesmärk

1.1. Käesoleva lisa eesmärk on kokku leppida vastastikustes õigustes ja kohustuses, mida pooled lepingu täitmise kaasaegselt isikuandmete töötlemisel järgivad. Käesolev lisa kujutab endast pooli omavahel siduvat andmetöötluslepingut Euroopa Liidu isikuandmete kaitse üldmääruse (2016/679) (edaspidi: **üldmäärus**) artikli 28 lõike 3 tähenduses.

1.2. Füüsiliste isikute (edaspidi: **andmesubjektide**) kategooriad ja nende kohta käivate isikuandmete liigid, mida lepingu täitmisel töödeldakse, isikuandmete töötlemise kestus, iseloom ja eesmärgid ning vastutava töötleja esmased dokumenteeritud juhised sisalduvad lepingus, sh selle juurde kuuluvates dokumentides. Vastutav töötleja võib anda isikuandmete töötlemiseks volitatud töötlejale täiendavaid dokumenteeritud juhiseid.

1.3. Pooled kohustuvad lepingu täitmisel järgima kõiki kohalduvaid andmekaitsealaseid õigusakte, kuid ka suuniseid, juhendeid ja tegevusjuhiseid, mis on koostatud isikuandmete kaitse valdkonnas järelevalve, teavitus- ja ennetustöö korraldamise eest vastutava kohaliku ja/või Euroopa Liidu asutuse poolt.

2. Mõisted

2.1. Käesolevas lisas olevate mõistete sisustamisel lähtutakse üldmääruses sätestatust, sealhulgas järgmistest terminitest ja nende definitsioonidest:

2.1.1. „**Isikuandmed**“ – igasugune teave tuvastatud või tuvastatava füüsilise isiku 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;

2.1.2. „**Isikuandmete töötlemine**“ – iga isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, näiteks 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;

2.1.3. „**Isikuandmetega seotud rikkumine**“ – turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu.

3. Isikuandmete töötlemine

3.1. Volitatud töötleja kohustub töötlemise isikuandmeid üksnes lepingu täitmise eesmärgil, vastutava töötleja dokumenteeritud juhiste alusel, lepingus kirjeldatud ulatuses ja viisil ning vastavalt käesolevas lisas sätestatud tingimustele. Kui see on lepingu täitmiseks vajalik, võib volitatud töötleja isikuandmeid töödelda ka järgmistel eesmärkidel:

3.1.1. asjakohaste info- ja sidesüsteemide hooldamine, tagades sellise töötlemise vastavuse käesolevas lisas nimetatud õigusaktidele ja juhenditele.

3.2. Volitatud töötleja teavitab andmesubjekte nende isikuandmete töötlemistingimustest ja tagab, et tal on isikuandmete töötlemiseks vajalikud õigused ja nõusolekud.

3.3. Volitatud töötleja vastutab vastutavale töötlejale edastatud isikuandmete õigsuse ja kättesaadavaks tegemise eest.

3.4. Kui volitatud töötleja ei ole vastutava töötleja juhistes kindel, kohustub ta mõistliku aja jooksul vastutava töötlejaga selgituste või täiendavate juhiste saamiseks ühendust võtma. Volitatud töötleja teavitab vastutavat töötlejat viivitamatult kõigist avastatud vastuoludest dokumenteeritud juhiste ja käesolevas lisas nimetatud õigusaktide või juhendite vahel.

3.5. Volitatud töötleja võib isikuandmete töötlemiseks kasutada teisi volitatud töötlejaid (edaspidi: **teine volitatud töötleja**) üksnes vastutava töötleja igakordsel eelneval loal, mis on antud vähemalt kirjalikku taasesitamist võimaldavas vormis.

3.6. Ilma vastutava töötaja kirjalikku taasesitamist võimaldava loata võib volitatud töötaja kasutada isikuandmete töötlemiseks teisi volitatud töötajaid üksnes juhul, kui see on vajalik volitatud töötaja info- ja sidesüsteemide hoolduseks, kui hoolduse läbiviimine ilma isikuandmeid töötlemata pole võimalik. Sellisel juhul teavitab volitatud töötaja vastutavat töötajat teise volitatud töötaja kaasamise, lisamise või asendamise kavatsusest, andes seeläbi vastutavale töötajale võimaluse esitada ettepaneku suhtes vastuväiteid. Kui vastutav töötaja ei ole esitanud volitatud töötajale 10 kalendripäeva jooksul vastuväiteid või kui vastutav töötaja selle heaks kiidab, võib volitatud töötaja teavituses märgitud viisil teise volitatud töötaja kaasata, lisada või asendada.

3.6.1. Volitatud töötaja vastutab kõigi teiste volitatud töötajate tegevuse eest nagu enda tegevuse eest ning sõlmib teise volitatud töötajaga isikuandmete töötlemiseks kirjalikud lepingud vastavalt üldmääruse artikli 28 lõikele 4, milles sisalduvad käesolevas lisas sätestatuga vähemalt samaväärsed andmekaitsekohustused.

3.6.2. Kui vastutav töötaja on andnud volitatud töötajale loa kasutada lepingust tulenevate kohustuste täitmiseks teisi volitatud töötajaid, on lepingust tulenevatele küsimustele vastamisel kontaktisikuks vastutavale töötajale üksnes volitatud töötaja ning volitatud töötaja tagab selle, et kõnealune teine volitatud töötaja täidab lepingu nõudeid. Vastutav töötaja võib igal ajahetkel võtta tagasi volitatud töötajale antud loa teise volitatud töötaja kasutamiseks.

3.7. Volitatud töötaja kohustub hoidma lepingu täitmise käigus teatavaks saanud isikuandmeid konfidentsiaalsena ning mitte töötlemata isikuandmeid muul kui lepingus sätestatud eesmärgil. Samuti kohustub volitatud töötaja tagama, et isikuandmeid töötlemata volitatud isikutel (sh volitatud töötaja töötajad, teised volitatud töötajad ja nende töötajad jt, kellel on ligipääs lepingu täitmise käigus töödeldavatele isikuandmetele) lasub samaväärne konfidentsiaalsuskohustus.

3.8. Volitatud töötaja kohustub rakendama asjakohaseid turvameetmeid, muu hulgas tehnilisi ja korralduslikke, viisil, et isikuandmete töötlemine vastaks üldmääruse artikli 32 nõuetele, sealhulgas:

3.8.1. vältima kõrvaliste isikute ligipääsu isikuandmete töötlemiseks kasutatavatele andmetöötlusseadmetele;

3.8.2. ära hoidma andmekandjate omavolilist teisaldamist;

3.8.3. tagama, et tagantjärele oleks võimalik kindlaks teha, millal, kelle poolt ja milliseid isikuandmeid töödeldi (sh kui andmeid töödeldi omavoliliselt);

3.8.4. tagama, et igal isikuandmete töötlemises osaleval isikul oleks juurdepääs ainult temale tööülesannete täitmiseks vajalikele isikuandmetele.

3.9. Volitatud töötaja aitab võimaluste piires vastutaval töötajal asjakohaste tehniliste ja korralduslike meetmete abil täita vastutava töötaja kohustusi vastata kõigile andmesubjekti taotlustele oma õiguste teostamisel, muu hulgas edastades kõik andmesubjektidelt saadud andmete kontrollimise, parandamise ja kustutamise, andmetöötluse keelamise ja muud taotlused vastutavale töötajale viivitamatult nende saamisest alates. Andmesubjekti taotluse lahendamise otsustab vastutav töötaja. Volitatud töötaja ei vasta andmesubjekti või mistahes muu kolmanda isiku päringule ilma vastutava töötaja eelneva kooskõlastuseta.

3.10. Volitatud töötaja aitab vastutaval töötajal täita üldmääruse artiklites 32–36 sätestatud kohustusi, võttes arvesse isikuandmete töötlemise laadi ja volitatud töötajale kättesaadavat teavet.

3.11. Vastutav töötaja võib viia läbi auditeid, eesmärgiga kontrollida volitatud töötaja käesolevast lisast tulenevate kohustuste täitmist. Volitatud töötaja teeb sel eesmärgil vastutava töötaja kirjalikku taasesitamist võimaldavas vormis taotluse alusel kättesaadavaks kogu teabe, mis on vajalik käesolevas lisas sätestatud kohustuste täitmise tõendamiseks. Pooled on kokku leppinud, et:

3.11.1. vastutava töötaja auditeid võib läbi viia vastutav töötaja ja/või kolmas isik, keda vastutav töötaja on selleks volitanud;

3.11.2. volitatud töötajal on kohustus anda vastutavale töötajale teavet, sh andmeid ja dokumente, mida on vaja selleks, et tõendada käesoleva lisa nõuetekohast järgimist;

3.11.3. vastutav töötaja käsitleb volitatud töötajalt auditi raames saadud teavet konfidentsiaalsena.

3.12. Volitatud töötaja suunab kõik järelevalveasutuste päringud viivitamatult, kuid hiljemalt päringu saamisele järgneva 3 kalendripäeva jooksul otse vastutavale töötajale, kuna suhtluses järelevalveasutustega pole volitatud töötajal õigust vastutavat töötajat esindada ega tema nimel tegutseda. Volitatud töötaja teeb järelevalveasutuse päringute lahendamisel ja neile vastamisel, iseäranis volitatud töötajat puudutavates küsimustes või toimingutes, vastutava töötajaga igakülgset koostööd.

4. Isikuandmete töötlemine väljaspool Euroopa Liitu ja Euroopa Majanduspiirkonda

4.1. Volitatud töötleja võib edastada isikuandmeid väljaspool Euroopa Liitu ja Euroopa Majanduspiirkonda asuvale vastuvõtjale (sh teisele volitatud töötlejale), ainult juhul, kui vastavaks andmeedastuseks ja edasiseks andmetöötluks esineb õiguslik alus, sh:

4.1.1. vastuvõtjale, kes asub riigis, kus on Euroopa Komisjoni kaitse piisavuse otsuse kohaselt tagatud Euroopa Liidu ja Euroopa Majanduspiirkonnaga samaväärne isikuandmete kaitse tase; või

4.1.2. asjakohaste kaitsemeetmete rakendamisel üldmääruse artikli 46 tähenduses.

4.2. Eelmises punktis sätestatust sõltumata töötleb volitatud töötleja isikuandmeid väljaspool Euroopa Liitu ja Euroopa Majanduspiirkonda (sh edastab kolmandas riigis asuvale vastuvõtjale) üksnes vastutava töötleja igakordsel kirjalikul loal.

5. Isikuandmete töötlemisega seotud rikkumistest teavitamine

5.1. Volitatud töötleja teavitab vastutavat töötlejat kõikidest isikuandmete töötlemisega seotud rikkumistest, või kui on alust kahtlustada, et selline rikkumine on aset leidnud, ilma põhjendamatu viivitusega alates hetkest, kui volitatud töötleja või tema poolt kasutatav teine volitatud töötleja saab isikuandmete töötlemisega seotud rikkumisest või selle kahtlusest teada.

5.2. Volitatud töötleja peab viivitamatult, aga mitte hiljem kui 24 tundi pärast rikkumisest teada saamist edastama vastutavale töötlejale kogu isikuandmetega seotud rikkumist puudutava asjakohase informatsiooni, täites käesolevas lisas toodud isikuandmete töötlemise rikkumisest teavitamise vormi (edaspidi: **vorm**) ja lisades juurde muu asjakohase dokumentatsiooni. Juhul, kui kõiki asjaolusid ei ole võimalik selleks ajaks välja selgitada, esitab volitatud töötleja vastutavale töötlejale vormi esialgsete andmetega. Täiendatud vorm lõpliku informatsiooniga rikkumise asjaolude kohta tuleb esitada vastutavale töötlejale esimesel võimalusel pärast esialgsete andmetega vormi esitamist.

5.3. Volitatud töötleja teeb isikuandmetega seotud rikkumise või selle kahtluse korral vastutava töötlejaga igakülgset koostööd selleks, et koostada tegevusplaan ja rakendada seda isikuandmetega seotud rikkumise või selle kahtluse kõrvaldamiseks. Volitatud töötleja peab tegema kõik temalt mõistlikult oodatava, et isikuandmetega seotud rikkumise jätkumist ja edasisi rikkumisi ära hoida ning kahju vähendada.

5.4. Järelevalveasutuse ja/või andmesubjekti teavitamise vajaduse üle isikuandmetega seotud rikkumise või selle kahtluse korral otsustab vastutav töötleja. Volitatud töötleja ei edasta järelevalveasutusele, andmesubjektile või mistahes muule kolmandale isikule teavitust ilma vastutava töötleja eelneva kooskõlastuseta.

6. Muud sätted

6.1. Volitatud töötleja kohustub lepingu lõppemisel kustutama, hävitama või tagastama vastutavale töötlejale kõik lepingu alusel töödeldavad isikuandmed ja nende koopiad vastavalt vastutava töötleja antud dokumenteeritud juhistele. Kui pole antud teistsuguseid juhiseid, siis tuleb isikuandmed kustutada, hävitada või tagastada hiljemalt 10 kalendripäeva jooksul alates lepingu lõppemisest, välja arvatud juhul, kui Euroopa Liidu või selle liikmesriigi õiguse kohaselt nõutakse andmete säilitamist. Isikuandmete kustutamise, hävitamise ja/või tagastamise kulud kannab volitatud töötleja.

6.2. Volitatud töötleja väljastab vastutavale töötlejale volitatud töötleja esindusõigusega isiku kirjaliku kinnituse, et tema ja kõik tema kasutatud teised volitatud töötlejad on teinud eelmises punktis nimetatud toimingud.

6.3. Volitatud töötleja teavitab vastutavat töötlejat kirjalikult kõigist muudatustest, mis võivad mõjutada volitatud töötleja võimet või väljavaateid pidada kinni käesolevast lisast ja vastutava töötleja dokumenteeritud juhistest. Pooled lepivad kõigis käesolevat lisa puudutavates täiendustes ja muudatustes kokku kirjalikult.

6.4. Kohustused, mis oma iseloomu tõttu peavad jääma jõusse hoolimata käesoleva lisa kehtivuse lõppemisest, nagu konfidentsiaalsuskohustus, jäävad jõusse ka pärast käesoleva lisa kehtivuse lõppemist ning nendele rakendatakse lepingus sätestatud, kui käesolevas lisas ei ole kokku lepitud teisiti.

Vastutav töötleja

Volitatud töötleja

/allkirjastatud digitaalselt/

/allkirjastatud digitaalselt/

Lisa

ISIKUANDMETE TÖÖTLEMISE RIKKUMISEST TEAVITAMISE VORM

1. Kontaktandmed

Isik, kellelt saab rikkumise asjaolude kohta täiendavat informatsiooni ja tema kontaktandmed:

2. Teavituse tüüp (märgi kast, üks või mitu valikut)

- Eelteavitus
- Lõplik teavitus
- Varasema teavituse täiendamine

3. Aeg (sisesta kuupäev ja märgi kast)

Millal sain rikkumisest teada (kuupäev/kuu/aasta): _____

Rikkumine toimus pikemal perioodil (algus- ja lõppkuupäev/kuu/aasta): _____

- Toimus ühekordne rikkumine
- Rikkumine jätkuvalt toimub

4. Rikkumise andmed

Kirjelda, mis juhtus ning kuidas rikkumise avastasite:

Rikkumise asjaolud (märgi kast, üks või mitu valikut)

- Seade isikuandmetega on kaotatud või varastatud
 - Paberdokument on varastatud, kaotatud või jäetud mitteturvalisse keskkonda
 - Isikuandmete loata avaldamine
 - Isikuandmeid nägi vale isik
 - Isikuandmed edastati valele isikule
 - Infosüsteemidesse loata või ebaseaduslik sisenemine (nt häkkimine, pahavara, lunavara või õngitsusrünne)
 - Isikuandmed olid kättesaadavad seoses andmekandjate ebapiisava hävitamisega
 - Muud (palun täpsusta): _____
-

Miks rikkumine toimus (märgi kast, üks või mitu valikut)

- Organisatsiooni töökorralduse reeglite, sisekorra rikkumine
- Töötajate vähene teadlikkus (nt puudulikud sisekorrad ja töökorralduse reeglid, töötajate mittepiisav koolitus)
- Inimlik viga
- Tehniline viga

Muu (nimetage siin ka koostööpartner(id) nt teine volitatud töötaja, kui rikkumine toimus tema juures): _____

- Asjaolud pole veel teada

5. Rikkumisest puudutatud isikuandmed

Rikkumisest puudutatud kaustade, dokumentide, failide, e-kirjade, andmebaaside arv, mis sisaldavad isikuandmeid. (nt mitu dokumenti edastati valele inimesele; märgi kast, valides vahemik või sisesta täpne arv või märgi „pole teada“)

- 1-9
- 10-49
- 50-99
- 100-499
- 500-999
- 1000-4999
- 5000 – 9999

10000 ja rohkem

Kui on teada, sisesta täpne arv: _____

Pole veel teada

Tee järgnevalt valik, millised isikuandmeid rikkumine puudutab (märgi kast, üks või mitu valikut)

Ees-, perenimi

Sünniaeg

Isikukood

E-post

Telefoni nr

Postiandmed või elukoha aadress

Kasutajanimed, salasõnad

Maksevahendite andmed (andmed, mis võimaldavad võtta üle isiku maksevahendi)

Majandus või finantsandmed (tehingu ajalugu, majanduslikku seisundit näitavad andmed, maksevõime hindamine)

AK teavet sisaldavad dokumendid (sh ameti- ja kutsesaladusega kaitstud teave)

Geolokatsiooni andmed

Suhtlusandmed (nt kes kellega ja millal rääkis, kirjutas)

Andmed süüteoasjades süüdimõistvate kohtuotsuste ja süütegude kohta

Lapsendamissaladuse andmed

Andmed sotsiaalkaitsevajaduse või eestkoste kohta

Rassiline või etniline päritolu

Poliitilised vaated

Usulised või filosoofilised (maailmavaatelised) veendumused

Ametiühingusse kuulumine

Geneetilised andmed

Biomeetrilised andmed

Terviseandmed

Seksuaalelu ja seksuaalne sättumus

Muu (palun täpsusta): _____

Kas isikuandmed olid asjakohaselt krüpteeritud? (sh krüptovõtmeid ei ole kompromiteeritud ja need on andmetöötaja kontrolli all. Märgi kast, üks valik)

Jah

Ei

6. Rikkumisest puudutatud isikud

Rikkumisest puudutatud isikute arv (märgi kast, valides vahemik või sisesta täpne arv või märgi „pole teada“)

1-9

10-49

50-99

100-499

500-999

1000-4999

5000-9999

10000 ja rohkem

Kui on teada, sisesta täpne arv: _____

Pole veel teada

Tee järgnevalt valik, milliseid isikute kategooriaid rikkumine puudutab (märgi kast, üks või mitu valikut)

Töötajad

Kliendid

- Alaealised (nt õpilased, lapsed).
- Patsiendid
- Sotsiaalset kaitset vajavad inimesed

Muu (palun selgita): _____

7. Võimalikud tagajärjed rikkumisest puudutatud isikutele
Konfidentsiaalsuskadu (andmetele said juurepääsu selleks mittevolitatud isikud. Märki kast, üks või mitu valikut)

- Oht isikuandmete ulatuslikumaks töötlemiseks kui näeb ette esialgne eesmärk või isiku nõusolek
- Oht isikuandmete kokku viimiseks muu isikuid puudutava infoga
- Oht, et isikuandmeid kasutatakse teistel eesmärkidel ja/või ebaõiglasel viisil

Muu (palun täpsusta): _____

Tervikluse kadu (andmeid on volitamata muudetud. Märki kast, üks või mitu valikut)

- Oht, et isikuandmeid on muudetud ja kasutatud, kuigi need ei pruugi olla enam kehtivad
- Oht, et isikuandmeid on muudetud muul moel kehtivateks andmeteks ja neid on hiljem kasutatud teistel eesmärkidel

Muu (palun täpsusta): _____

Käideldavuse kadu (puudub õigeaegne ja hõlbus juurdepääs andmetele. Märki kast)

- Puudub võime osutada rikkumisest puudutatud isikutele kriitilist (elutähtsat) teenust

Muu (palun täpsusta): _____

Füüsiline, varaline või mittevaraline kahju või muu samaväärne tagajärg (märki kast, üks või mitu valikut)

- Isik jääb ilma kontrollist oma isikuandmete üle
- Isiku õiguste piiramine (nt ei saa kasutada teenust või lepingust tulenevaid õigusi)
- Õiguslik tagajärg (nt isik ei saa hüvitist, toetust, luba mõneks tegevuseks)
- Diskrimineerimine
- Identiteedivargus
- Pettus
- Rahaline kahju
- Kahju tervisele
- Risk elule
- Pseudonümiseerimise loata tühistamine
- Mainekahju
- Usalduse kadu
- AK teabe või ameti- ja kutsesaladusega kaitstud teabe kadu

Muu (palun täpsusta): _____

8. Rikkumisega seotud järeltegevused

Isikute teavitamine

Juba teavitatud (kuupäev/kuu/aasta): _____

Kuidas teavitus toimus (märki kast, üks või mitu valikut):

- E-kirjaga
- Lühisõnumiga (SMS)
- Helistamisega
- Meedias sh sotsiaalmeedias
- Asutuse/ettevõtte vörgulehel

Muu (palun täpsusta): _____

Mis oli teavituse sisu: _____

Veel pole teavitanud, kuid teavitame: (kuupäev/kuu/aasta): _____

Pole selge kas on vaja teavitada

Ei ole vajalik teavitada

Kui pidasite vajalikuks isikuid mitte teavitada, siis selgitage, kuidas jõudsite järeldusele, et rikkumisega ei kaasne isikute õigustele ja vabadustele suurt riski:

Kirjeldage kavandatud ja rakendatud meetmeid rikkumise lahendamiseks, kahjulike mõjude leevendamiseks ja ennetamiseks tulevikus:

9. Rikkumise piiriülene mõju

Millises riigis on teie peamine tegevuskoht? (palun kirjuta riigi nimi): _____

Rikkumisest on puudutatud ka teiste EL riikide isikud:

Ei

Jah (palun täpsusta, milliste riikide ning tooge välja isikute arv riikide lõikes. Kui puudutatud isikuandmete koosseis on riigiti erinev, tooge ka see välja):
