

Tugiteenuste osutamise kokkulepe Lisa 2 ANDMETÖÖTLUSE LEPING

Käesolev lisa (edaspidi: **lisa**) on lahutamatu osa sõlmitud tugiteenuste osutamise kokkuleppest (edaspidi: **leping**), mis sõlmitakse Rahandusministeeriumi (edaspidi: **vastutav töötleja**) ja Riigi Tugiteenuste Keskuse (edaspidi: **volitatud töötleja**) vahel, teostamaks kokkuleppes nimetatud tegevustega seotud andmesubjektide (edaspidi: **andmesubjektid**) isikuandmete töötlemist.

1. Lisa eesmärk

1.1. Käesoleva lisa eesmärk on kokku leppida volitatud töötleja õigustes ja kohustuses isikuandmete töötlemisel, millest pooled lepingu täitmisel juhinevad. Käesolev lisa kujutab endast isikuandmete töötlemist puudutavat andmetöötlemise lepingut vastavalt Euroopa Liidu isikuandmete kaitse üldmäärusele (2016/679) (edaspidi: **üldmäärus**).

1.2. Andmesubjektide kategooriad ja isikuandmete liigid, mida lepingu täitmisel töödeldakse (edaspidi: **isikuandmed**), isikuandmete töötlemise kestus, iseloom ja eesmärgid ning vastutava töötleja antud juhised on välja toodud lepingus, sh selle juurde kuuluvates dokumentides. Vajadusel võib vastutav töötleja anda isikuandmete töötlemiseks täiendavaid dokumenteeritud juhiseid.

1.3. Pooled kohustuvad järgima kõiki kohalduvaid andmekaitsealaseid õigusakte, sh juhendeid ja tegevusjuhiseid, mis on väljastatud isikuandmete kaitse eest vastutava kohaliku ja/või Euroopa Liidu asutuse poolt ning seoses kõikide isikuandmetega, mida lepingu alusel töödeldakse.

2. Mõisted

2.1. Käesolevas lisa olevate mõistete sisustamisel lähtutakse üldmääruses sätestatust, sealhulgas:

2.1.1. „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;

2.1.2. „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 ühendamise, 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 töötleva isikuandmeid vastavalt käesolevas lisa nimetatud ja teistele asjakohastele õigusaktidele, juhenditele ja lepingule (sh vastutava töötleja antud dokumenteeritud juhistele) ning ainult sellisel määral, mis on vajalik lepingu täitmiseks. Kui see on lepingu täitmiseks seondult vajalik, võib volitatud töötleja andmesubjektide isikuandmeid töödelda ka järgmistel eesmärkidel:

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

3.2. 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 kõigist avastatud vastuoludest dokumenteeritud juhiste ja käesolevas lisa nimetatud õigusaktide või juhendite vahel.

3.3. Volitatud töötleja võib isikuandmete töötlemiseks kasutada teisi volitatud töötlejaid (edaspidi: **teine volitatud töötleja**) üksnes vastutava töötleja eelneval nõusolekul, mis on antud vähemalt kirjalikku taasesitamist võimaldavas vormis. Ilma vastutava töötleja kirjalikku taasesitamist võimaldava nõusolekuta võib volitatud töötleja kasutada isikuandmete töötlemiseks teisi volitatud töötlejaid üksnes juhul, kui see on vajalik volitatud töötleja info- ja sidesüsteemide hoolduseks, kui hoolduse läbiviimine ilma isikuandmeid töötlemata pole võimalik.

3.3.1. Volitatud töötleja vastutab kõigi teiste volitatud töötlejate tegevuse eest nagu enda tegevuse eest ning sõlmib teise volitatud töötlejaga isikuandmete töötlemiseks kirjalikud lepingud vastavalt üldmääruse artikli 28 lõikele 4, mis on käesolevas lepingus sätestatuga vähemalt samaväärsed.

3.3.2. Kui vastutav töötleja on andnud volitatud töötlejale loa kasutada lepingust tulenevate kohustuste täitmiseks teisi volitatud töötlejaid, on lepingust tulenevatele küsimustele vastamisel kontaktisikuks vastutavale töötlejale üksnes volitatud töötleja ning volitatud töötleja tagab selle, et kõnealune teine volitatud töötleja täidab lepingu nõudeid ja on sellega seotud samal viisil nagu volitatud töötleja ise. Vastutav töötleja võib igal ajahetkel võtta tagasi volitatud töötlejale antud loa kasutada teisi volitatud töötlejaid.

3.4. Volitatud töötleja kohustub hoidma lepingu täitmise käigus teatavaks saanud isikuandmeid konfidentsiaalsena ning mitte töötleva isikuandmeid muul kui lepingus sätestatud eesmärgil. Samuti tagama, et isikuandmeid töötleva volitatud isikud (sh teised volitatud töötlejad, volitatud töötleja töötajad jt, kellel on ligipääs lepingu täitmise käigus töödeldavatele isikuandmetele) järgivad konfidentsiaalsusnõuet.

3.5. Volitatud töötleja kohustub rakendama asjakohaseid turvalisuse tagamise meetmeid, muu hulgas tehnilisi ja korralduslikke, viisil, et isikuandmete töötlemine vastaks üldmääruse artikli 32 nõuetele, sealhulgas:

3.5.1. vältima kõrvaliste isikute ligipääsu isikuandmete töötlemiseks kasutatavatele andmetöötlusseadmetele;

3.5.2. ära hoidma andmekandjate omavolilist teistsaldamist;

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

3.6. Volitatud töötleja aitab võimaluste piires vastutaval töötlejal asjakohaste tehniliste ja korralduslike meetmete abil täita vastutava töötleja kohustusi vastata üldmääruse tähenduses kõigile andmesubjekti taotlustele oma õiguste teostamisel, muu hulgas edastades kõik andmesubjektidelt saadud andmete kontrollimise, parandamise ja kustutamise, andmetöötluse keelamise ja muud taotlused vastutavale töötlejale viivitamatult nende saamisest alates.

3.7. Volitatud töötleja aitab vastutaval töötlejal täita üldmääruse artiklites 32–36 sätestatud kohustusi, võttes arvesse isikuandmete töötlemise laadi ja volitatud töötlejale kättesaadavat teavet.

3.8. Vastutav töötleja võib viia läbi auditeid, taotledes volitatud töötlejalt kirjalikku taasesitamist võimaldavas vormis asjakohast teavet eesmärgiga kontrollida volitatud töötleja käesolevast lisast tulenevate kohustuste täitmist. Pooled on kokku leppinud, et:

3.8.1. vastutava töötleja auditeid võib viia kas vastutav töötleja ja/või kolmas isik, keda vastutav töötleja on selleks volitanud;

3.8.2. volitatud töötlejal on kohustus anda vastutavale töötlejale teavet, andmeid ja dokumente, mida on vaja selleks, et tõendada käesoleva lisa nõuetekohast täitmist;

3.8.3. vastutav töötleja käsitleb kogu volitatud töötleja poolt auditi raames saadud teavet konfidentsiaalsena.

3.9. Volitatud töötleja suunab kõik järelevalveasutuste päringud otse vastutavale töötlejale, kuna suhtluses järelevalveasutustega pole volitatud töötlejal õigust vastutavat töötlejat esindada ega tema nimel tegutseda. Volitatud töötleja teeb vastutava töötlejaga koostööd volitatud töötlejat puudutavates küsimustes või toimingutes järelevalveasutusele vastamisel.

4. Isikuandmete töötlemine väljaspool Euroopa Liitu ja Euroopa Majanduspiirkonda

4.1. Käesoleva lepingu esemeks olevaid isikuandmeid ei tohi töödelda väljaspool Euroopa Liitu ega Euroopa Majanduspiirkonda, sh ei tohi nimetatud isikuandmeid edastada kolmandale riigile või rahvusvahelisele organisatsioonile.

4.2. Juhul, kui käesoleva lepingu esemeks olevate isikuandmete töötlemine väljaspool Euroopa Liitu ja Euroopa Majanduspiirkonda, sh nende edastamine kolmandale riigile või rahvusvahelisele organisatsioonile, on vajalik lepingu täitmiseks, lepivad pooled sellises andmetöötluses eelevalt kirjalikult kokku. Kirjalikku kokkulepet ei ole vaja sõlmida, kui volitatud töötleja on kohustatud isikuandmeid kolmandale riigile või rahvusvahelisele organisatsioonile edastama volitatud töötleja suhtes kohaldatava Euroopa Liidu või liikmesriigi õiguse alusel. Sellisel juhul teatab volitatud töötleja sellise õigusliku aluse olemasolust enne isikuandmete töötlemist vastutavale töötlejale, kui selline teatamine ei ole olulise avaliku huvi tõttu kõnealuse õigusega keelatud.

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 teada isikuandmete töötlemisega seotud rikkumisest või on alust kahelda, et selline rikkumine on aset leidnud.

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

5.3. Volitatud töötaja teeb vastutava töötajaga igakülgset koostööd selleks, et välja töötada ja täita tegevusplaan isikuandmetega seotud rikkumiste kõrvaldamiseks. Volitatud töötaja peab tegema kõik võimaliku, et edasist rikkumist ära hoida ning kahju vähendada.

5.4. Vastutav töötaja vastutab järelevalveasutuse teavitamise eest.

6. Vastutus

6.1. Lisaks lepingus sätestatud vastutusele:

6.1.1. vastutab volitatud töötaja kahju eest, mida ta on tekitanud vastutavale töötajale, andmesubjektidele või muudele kolmandatele isikutele isikuandmete töötlemise tagajärjel, mis on tekitatud käesoleva lisa nõudeid, mh kõiki selles mainitud õigusnorme ja dokumenteeritud juhiseid, rikkudes.

6.1.2. kohustub volitatud töötaja, kui ta on isikuandmete töötlemise nõudeid rikkunud ja selle tagajärjel on vastutav töötaja kohustatud maksma hüvitist või trahvi, hüvitama vastutavale töötajale sellega seoses kantud kulud.

6.1.3. kui volitatud töötaja rikub oluliselt käesolevas lisas sätestatud isikuandmete töötlemise nõudeid, muuhulgas isikuandmete kaitse üldmääruse või muude kohaldatavate õigusnormide sätteid isikuandmete kaitse valdkonnas, on vastutaval töötajal õigus leping ette teatamata üles öelda. Oluline lepingurikkumine on eelkõige, kui:

6.1.3.1 isikuandmete töötlemise põhimõtete täitmist kontrolliva järelevalveasutuse või kohtu menetluses selgub, et volitatud töötaja või teine volitatud töötaja ei täida isikuandmete töötlemise põhimõtteid;

6.1.3.2 vastutav töötaja leiab käesoleva lisa kohaselt läbiviidud auditis, et volitatud töötaja või teine volitatud töötaja ei täida isikuandmete töötlemise põhimõtteid, mis tulenevad käesolevast lisast või kohaldatavatest õigusnormidest.

7. Muud sätted

7.1. Volitatud töötaja kohustub lepingu lõppemisel tagastama vastutava töötajale kõik andmesubjektide isikuandmed või kustutama või hävitama isikuandmed ja nende koopiad vastavalt vastutava töötaja antud juhistele.

7.2. Volitatud töötaja väljastab vastutavale töötajale volitatud töötaja esindusõigusega isiku kirjaliku kinnituse, et tema ja kõik tema kasutatud teised volitatud töötajad on teinud eelnevas punktis nimetatud toimingud.

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

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

Vastutav töötaja

Volitatud töötaja

/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)

☐ 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 juhtus (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 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 andmetöötleja 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

☐ Sotsiaalselt 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):
