



# VASTAVUS ISIKUANDMETE KAITSE ÜLDMÄÄRUSEGA



## Mis on isikuandmed?

Isikuandmed on teave inimese kohta, mille abil saab teda otse või kaudselt tuvastada: nimi, isikukood, asukohateave, samuti füüsilised, geneetilised, vaimsed, majanduslikud, kultuurilised ja mis tahes muud tuvastamist võimaldavad tunnused ja nende kombinatsioonid.

Seega on isikuandmete määratlemisel oluline küsida: kas nende andmete põhjal on võimalik füüsilist isikut otseselt või kaudselt tuvastada? Isikuandmete kaitse reeglid ei kehti, kui teave ei võimalda inimest mõistlike pingutustega tuvastada.

## Siin on mitteamendav loetelu isikuandmetest, mille kaudu on isik tuvastatav:

- ees- ja perekonnanimi, isikukood, sünniaeg;
- telefoninumber;
- isikut töendava dokumendi number;
- foto ja videosalvestised;
- telefonikõnede audiosalvestised;
- andmed kliendi omaduste kohta;
- CV-d, märkmed kandideerijate kohta
- inimese hääl.

IKÜM toob eraldi välja ka eriliiki isikuandmed. Eriliiki isikuandmete töötlemine väärrib suuremat hoolsust.

Eriliiki isikuandmete mitteammendav loetelu on välja toodud siin:

- terviseandmed;
- biomeetrilised andmed;
- ametiühingusse kuulumine;
- poliitilised ja usulised veendumused;
- geneetilised andmed;
- rassiline või etniline päritolu.



Isikuandmete kaitse üldmäärust ei kohaldata juriidiliste isikute andmete töötlemisel, näiteks juriidilise isiku nime või kontaktandmete kasutamisel.

## Miks on vaja isikuandmeid kaitsta?

Andmekaitsereeglid ei ole pelgalt juriidilise kohtustuse täitmiseks, vaid on oluline osa inimeste õiguste ja vabaduste kaitsmisest ning läbipaistva ja usaldusväärse ühiskonna alusest. Maailmas toimuva valguses tuleb nentida, et andmete kaitse on muutunud ka oluliseks julgeolekuküsimuseks.

Inimestele tuleb tagada kindlus, et nende kohta käivat teavet kogutakse ja kasutatakse ausalt, õigesti ja turvaliselt. Inimese eraelu puutumatus ja vabadust ei tohi lubamatult riivata ja inimestele tuleb tagada võimalus oma õiguseid teostada, s.h saada selgitusi isikuandmete töötlemise seaduspärasuse kohta.

**Ettevõtetel tuleb juba eos juurutada põhimõte, et kogutud isikuandmeid on vajalik käsitleda samasuguse hoolsusega kui näiteks ettevõtte finantsvarasid. Kui ettevõtte kasutab oma finantsvahendeid, teab ta ju samuti, mis eesmärgil ja alusel neid kasutatakse. Miks peaks see isikuandmete puhul teisiti olema?**

## Mis on isikuandmete kaitse üldmäärus?

2018. aasta 25. maist kohaldatakse Euroopa Liidu liikmesriikidele, sh Eestile, isikuandmete kaitse üldmäärust (IKÜM).

Isikuandmete kaitse üldmäärusega tagatakse inimeste õigus isikuandmete kaitsele. IKÜM-is on kirjas nii füüsiliste isikute õigused kui andmetöötlejatele kehtestatud kohustused isikuandmete töötlemisel. Eestis hoolitseb isikuandmete töötlemise teadlikkuse kasvatamise ning IKÜM-i kohase täitmise eest Andmekaitse Inspeksioon (AKI).

IKÜM-i ametlik inglisekeelne nimi on General Data Protection Regulation ehk lühendatult GDPR. Isikuandmete kaitse üldmäärus on eestikeelne tõlge.

Andmekaitse Inspeksioon on informatsiooni, s.h kontakteerumise viisid, koondanud oma veebilehele [www.aki.ee](http://www.aki.ee).

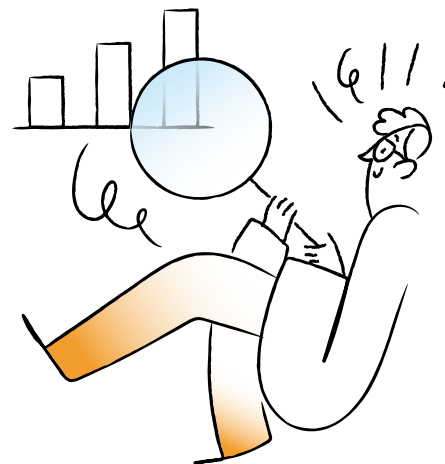
## Korrektseks isikuandmete töötlemiseks tuleb ettevõtetel järgida järgmisi isikuandmete töötlemise põhimõtteid.



1. Isikuandmete töötlemiseks peab olema selge eesmärk ja õiguslik alus.
2. Isikuandmete töötlemine peab olema läbipaistev ja inimesele arusaadav.
3. Isikuandmeid tohib koguda täpselt nii palju ja nii kaua, kui on vajalik eesmärgi saavutamiseks.
4. Ettevõtte peab veenduma, et isikuandmed oleksid ajakohased ning õiged. Ebaõiged isikuandmed tuleb kohe parandada või kustutada.
5. Isikuandmeid võib töödelda viisil, mis tagab isikuandmete konfidentsiaalsuse ja turvalisuse ning selleks kasutatakse asjakohaseid tehnilisi ja korralduslikke meetmeid.

## Mis on isikuandmete töötlemine?

Isikuandmete töötlemine on isikuandmetega tehtav mistahes toiming: kogumine, korrastamine, säilitamine, muutmine, lugemine, kasutamine, edastamine, ühendamine, kustutamine, päringute tegemine, avalikustamine ja muud võimalikud tegevused.



## Kes vastutab isikuandmete töötlemise eest?

Ettevõtte, kes töötleb isikuandmeid, vastutab nende töötlemise õiguspärasuse eest.

Isikuandmete töötlejad peavad lähtuvalt sellest, kuidas andmeid töödeldakse, määratlema, kas ollakse vastutav, volitatud või kaasvastutav töötleja.

Selleks, et hinnata, kas isikuandmete töötlemine ettevõttes vastab IKÜM-ile, tuleb vastata järgmistele küsimustele. Kui vastate kõikide küsimustele jaatavalt, siis vastab ettevõtte reeglitele. Kui mõnele küsimusele on vastus eitav, siis tuleb ettevõtetel veelkord oma tegevused läbi mõelda.



Kas olen teinud kindlaks, <u>kas ettevõtte töötleb isikuandmeid?</u>	<input type="radio"/>	<input type="radio"/>	- Kui ettevõtte töötleb isikuandmeid (sh näiteks kui neil on vähemalt üks töötaja või klient), tuleb järgida IKÜM-ist tulenevaid reegleid ning vastata järgnevale küsimustele kontrollnimekirjas.
Kas olen läbi analüüsinud ja rakendanud isikuandmete <u>töötlemise põhimõtteid?</u>	<input type="radio"/>	<input type="radio"/>	Ettevõtte peab isikuandmeid töötlemata a) läbipaistvalt, b) ainult kindlal eesmärgil, c) nii vähe kui võimalik, d) täpselt ja õigesti, e) ainult nii kaua kui vaja, f) turvaliselt, g) vastutustundlikult.
Kas olen koostanud ettevõttes töödeldavate isikuandmete kohta <u>töötlemisülevaate?</u>	<input type="radio"/>	<input type="radio"/>	Töötlemisülevaates on kirjas informatsioon ettevõttes töödeldavatest isikuandmetest.
Kas olen taganud <u>turvalise isikuandmete töötlemise?</u>	<input type="radio"/>	<input type="radio"/>	Et tagada isikuandmete töötlemise turvalisus ja konfidentsiaalsus, tuleb rakendada asja- ja ajakohaseid tehnilisi ja korralduslikke turvameetmeid.
Kas olen sõlminud isikuandmete töötlemist puudutavad lepingud ettevõtte koostööpartneritega?	<input type="radio"/>	<input type="radio"/>	Kolmandate ettevõtete teenuste (näiteks raamatupidamine) kasutamisel tuleb sõlmida isikuandmete töötlemist puudutavad kokkulepped.
Kas olen rakendanud <u>lõimitud ja vaikimisi andmekaitse?</u>	<input type="radio"/>	<input type="radio"/>	Andmekaitsele tuleb mõelda enne, kui uus teenus või süsteem valmis tehakse. Andmete kaitsmisele pööratakse tähelepanu kogu protsessis. Vaikimisi kogutakse ainult neid andmeid, mida tõesti vaja on ning milleks on olemas õiguslik alus.
Kas olen hinnanud vajadust teha <u>mõjuhinnang?</u>	<input type="radio"/>	<input type="radio"/>	Andmekaitse mõjuhinnangu peavad tegema ettevõtted, kelle isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärgi arvestades tekib tõenäoliselt inimestele <u>suur oht</u> . Mõjuhinnanguga hinnatakse andmetöötluse mõju inimese vaatenurgast. Eestis on siseriikliku mõjuhinnangu ulatuslikkuse kriteeriumid järgnevad: 1) eriliiki või süüteoandmed 5000 ja enama inimese kohta, 2) suurt ohtu põhjustavaid andmeid 10 000 ja enama inimese kohta, 3) ülejäänud isikuandmed 50 000 ja enama inimese kohta. Ettevõttel on kasulik teha mõjuhinnang ka siis, kui esmapilgul ei tundu tõenäoline, et suur oht realiseeruks.
Kas jälgin <u>kolmandatesse riikidesse isikuandmete edastamise nõudeid?</u>	<input type="radio"/>	<input type="radio"/>	- Kui isikuandmete edastamine toimub Euroopa Liidu siseselt, siis peab selleks olema <u>õiguslik alus</u> , nagu seda on vaja igaks andmetöötluse toiminguks, kuid täiendavaid kaitsemeetmeid (nt taotleda inspeksiooni kooskõlastus) rakendada ei pea. - Kui isikuandmete edastamine toimub välisriikidesse väljaspool Euroopa Liitu, siis tuleb uurida, millisele andmekaitsetasemele riik vastab ja vastavalt sellele nõudeid järgida. Üldreegel on see, et andmeid võib edastada juhul, kui on rakendatud nõuetekohased kaitsemeetmed ning on olemas õiguslik alus vastavalt IKÜM-i artiklitele 6 või 9. Oluline informatsioon isikuandmete edastamise kohta, sh millised on mittepääsava turvalisusega riigid, on <u>AKI veebilehel</u> vastavas rubriigis.
Kas olen valmis vajadusel <u>andmekaitse spetsialisti määrama?</u>	<input type="radio"/>	<input type="radio"/>	Andmekaitse spetsialist tuleb määrata järgmistel juhtudel: 1) eriliiki andmeid või süüteoandmeid 5000 ja enama inimese kohta, 2) suurt ohtu põhjustavaid andmeid 10 000 ja enama inimese kohta (näiteks identiteedivarguse või pettuse oht), 3) isikuandmeid 50 000 ja enama inimese kohta; on tegemist avaliku sektori asutusega. Kui AKS on määratud, tuleb sellest teada anda nii avalikkusele kui Andmekaitse Inspeksioonile. Mõlemat ühekorraga saab ettevõtte teha <u>äriregistri</u> kaudu.
Kas olen valmis Andmekaitse Inspeksiooni ja <u>inimesi rikkumisest teavitama?</u>	<input type="radio"/>	<input type="radio"/>	Ettevõttel tuleb juhinduda järgnevalt: 1) dokumenteerida kõik isikuandmetega seotud rikkumised, mis on ettevõttes toimunud, sh asjaolud, mõju ja parandusmeetmed, 2) teavitada isikuandmetega seotud rikkumisest AKI-t 72 tunni jooksul, 3) teavitada viivitamatult inimest tema andmetega seotud rikkumisest, kui see kujutab endast suurt ohtu.