GDPR tööriistakast

TARK

GDPR - ???

Mis on GDPR?

- ✓ GDPR on ELi isikuandmete kaitse üldmäärus (*general data protection regulation, GDPR*), mille rakendamine algab üleeuroopaliselt **25. mail 2018**. GDPRi põhieesmärk on anda inimestele tagasi kontroll oma isikuandmete üle ning ühtlustada isikuandmete kaitse regulatsiooni ELis.

Kellele GDPR kohaldub?

- ✓ GDPR kohaldub sisuliselt kõigile (vastutavatele töötlejatele ja volitatud töötlejatele), kes töötlevad füüsilise isiku ehk inimese kohta käivaid andmeid. Isegi juhul kui vastutav või volitatud töötleja asub väljaspool ELi, kohaldub talle GDPR, kui ta töötleb ELi elanike andmeid.

Mis on isikuandmed?

- ✓ Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise isiku ehk inimese kohta.
- ✓ Näiteks nimi, aadress, ID kood, pildid, e-posti aadress, andmed inimese asukoha kohta jne.

Mis on isikuandmete eriliigid?

- ✓ Isikuandmed, mis annavad teavet inimese rassi või etnilise päritolu, poliitiliste veendumuste, usuliste või filosoofiliste veendumuste või ametiühingusse kuulumise kohta.
- ✓ Isikuandmete eriliigid hõlmavad ka geneetilisi ja biomeetrilisi andmeid (nt sõrmejälgi või näopilte), terviseandmeid, seksuaalelu või seksuaalset orientatsiooni puudutavaid andmeid.
- ✓ Nõusolek selliste andmete töötlemiseks peab olema selgesõnaline.

Mis on töötlemine?

- ✓ Töötlemine on igasugune isikuandmetega tehtav toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine. Töötlemine võib toimuda käsitsi või automatiseeritult.

Kes on vastutav kes volitatud töötleja?

- ✓ Vastutav töötleja on isik, kes otsustab, kuidas ja miks isikuandmeid töödeldakse.
- ✓ Volitatud töötleja on isik, kes töötleb isikuandmeid vastutava töötleja nimel, näiteks ettevõtte IT- või raamatuspidamisteenuse pakkuja.

Millised on peamised muudatused?

Andmetöötluse põhimõtted ja töötlemise tingimused jäävad laias laastus samaks, kuid on ka palju uut:

- ✓ Nagu varemgi tuleb isikuandmete töötlemisel järgida kuut üldpõhimõtet[1]. Uueks nõudeks on see, et peab olema võimeline tõendama põhimõtete täitmist.
- ✓ Isikult tema andmete töötlemiseks kehtiva nõusoleku saamine muutub keerulisemaks, sest nõuded nõusolekule on karmimad.
- ✓ Pea kõik andmetöötlejad peavad pidama registrit andmetöötlustoimingute kohta.
- ✓ Inimestel on teatud tingimustel õigus nõuda oma andmete ülekandmist endale või nt teisele teenuse osutajale.
- ✓ Isikuandmete töötlemine peab olema läbipaistev ning seetõttu tuleb inimest põhjalikult teavitada tema andmete töötlemisega seotud asjaoludest.
- ✓ Uued nõuded vastutava ja volitatud töötleja vahelistele andmetöötlust reguleerivatele lepingutele.

[1] Vaata ülevaadet 6 üldpõhimõtte kohta lisast 1.

- ✓ Suured karistused GDPRi nõuete rikkumise korral – teatud rikkumiste puhul võidakse rakendada trahve, mille maksimumsumma on 20 miljonit eurot või 4% ettevõtte ülemaailmsest käibest.

Andmekaitsespetsialist - JAH või EI?

GDPR kohustab andmekaitsespetsialisti määrama järgmisi andmetöötlejaid:

- ✓ kelle põhitegevuseks on ulatuslik andmesubjektide korrapärane ja süstemaatiline jälgimine (näitena on Andmekaitse Inspektsioon välja toonud ka hotellid)
- ✓ kelle põhitegevuseks on andmete eriliikide ulatuslik töötlemine.

- ✓ Isegi juhul, kui ettevõte ei pea määrama andmekaitsespetsialisti, on soovitatav määrata andmekaitse eest vastutav isik, sest isikuandmete kaitsega tuleb tegeleda jooksvalt.

Mis on andmesubjekti õigused?

- ✓ GDPR annab inimesele seoses tema andmete töötlemisega 7 põhiõigust[2].

Kuidas andmesubjektide õigused ettevõtet mõjutavad?

- ✓ Andmetöötleja peab olema teadlik, kelle isikuandmeid ta töötleb ja dokumenteerima andmete töötlemisel tehtavad toimingud.

- ✓ Ettevõte peab olema valmis vastu võtma ning täitma andmesubjekti poolt esitatavaid taotlusi.

Mida peavad ettevõtted andmete turvalisuse tagamiseks tegema?

- ✓ GDPR nõuab, et ettevõtted rakendaksid turvalisuse tagamiseks sobivaid tehnilisi ja organisatsioonilisi meetmeid, arvestades olemasolevat tehnoloogiat, rakendamise kulusid ja töötlemise iseloomu, ulatust, konteksti ning eesmärke. Tänased turvameetmed tuleks üle vaadata ja hinnata nende vastavust GDPRi nõuetele.

- ✓ Isikuandmetega seotud rikkumisest tuleb teatud juhtudel teavitada Andmekaitse Inspektsiooni ning andmesubjekte.

Kas vastutava ja volitatud töötleja vahel peab olema leping?

- ✓ JAH – GDPR näeb ette miinimumtingimused, mida andmetöötlusleping peab sisaldama.

- ✓ Vaadake üle kõik andmetöötluslepingud, ilmselt ei vasta need GDPRi nõuetele ja seetõttu peate uued tingimused teenuse pakkujaga läbi rääkima ja neis kokku leppima.

- ✓ Kandke kõik ettevõtte nimel isikuandmeid töötlevad volitatud töötlejad isikuandmete registrisse.

Kas võib andmeid edastada väljapoole ELi?

- ✓ GDPR keelab isikuandmete edastamise väljapoole ELi, v.a juhul, kui on täidetud teatud tingimused.

Mida teha, et 25. maiks GDPRi vormis olla?

- ✓ Kaardistage andmevood ja nende liikumine – kelle ja milliseid andmeid töötlete, miks te andmeid kogute, kust andmeid saate, kus ja kuidas säilitate, kellega jagate, kui kaua säilitate, kuidas kustutate/hävitate, milliseid turvameetmeid andmete kaitseks kasutate?

- ✓ Püüdke tuvastada, kas praegune andmetöötlus ja sellega seotud protsessid vastavad GDPRi nõuetele.

- ✓ Arutage erinevate osakondadega eeltoodud teemasid ja koostage tegevuskava GDPRi nõuetele vastavuse saavutamiseks.

- ✓ Tooge välja põhiprotsessid, mida võib olla vaja muuta ja koostage nende muudatuste rakendamise ajakava.

- ✓ Täitke Isikuandmete register.

- ✓ Viige läbi isikuandmetega kokku puutuvate töötajate andmekaitsealane koolitus.

[2] Andmesubjekti õiguste kohta vaata lisast 1.

Tööriistakomplekt

Mida see tööriistakomplekt sisaldab?

Sellest tööriistakomplektist leiate järgmiste dokumentide mallid:

- Ettevõtte privaatsuspoliitika
- Privaatsusteate töötajatele
- Privaatsusteate klientidele
- Isikuandmetega seotud rikkumistele reageerimise protseduur
- Andmesubjekti õiguste ja taotluste protseduur
- Andmekaitse standardklauslid andmetöötluslepingutesse
- Isikuandmete register

✓ Olenevalt ettevõtte tegevusala spetsiifikast ja andmetöötluse mahus võib olla vajadus täiendavate reeglite ja protseduuride järgi.

Mis on ettevõtte privaatsuspoliitika?

✓ *Privaatsuspoliitika* on ettevõte isikuandmete töötlemise üldisi ja peamisi põhimõtteid kajastav dokument.

✓ Privaatsuspoliitika on eelkõige ettevõtte sisemine dokument, tutvumiseks ja järgimiseks ettevõtte juhtkonnale ning töötajatele.

Millal ja kellele tuleb esitada privaatsusteade?

✓ *Privaatsusteade* tuleb esitada inimesele (nt töötajale, kliendile) tema andmete saamisel või esimesel võimalusel pärast seda.

✓ Privaatsusteade annab informatsiooni inimese andmetega seonduvatest peamistest asjaoludest nagu töötlemise eesmärgid, õiguslikud alused, säilitamise kriteeriumid, jne.

Miks on vaja isikuandmetega seotud rikkumistele reageerimise protseduuri?

✓ Isikuandmete rikkumise kahtluse korral, sh näiteks andmete kaotsimineku või lubamatu juurdepääsu puhul, annab *isikuandmetega seotud rikkumistele reageerimise protseduur* ettevõtte töötajatele tegevusjuhised, kuidas nad sellises olukorras käituma peavad.

✓ Protseduuris täpsustatakse, millistest rikkumistest tuleb teavitada Andmekaitse Inspektsiooni ja andmesubjekte.

✓ Ettevõte peaks ka veenduma, et töötajad suudaksid rikkumise ära tunda ning teaksid, millal, kuidas ning kellele rikkumisest teatada.

Mis on andmesubjekti õiguste ja taotluste protseduur?

✓ *Andmesubjekti õiguste ja taotluste protseduur* on juhendav dokument, kus selgitatakse:

- millised on inimese õigused seoses tema isikuandmetega, mis on ettevõtte valduses
- kuidas inimene neid õigusi kasutada saab
- kuidas peaks ettevõte tegelema inimese taotlusega oma õigusi kasutada.

Millal on vaja andmekaitse standardklausleid?

✓ GDPR nõuab, et ettevõtted sõlmiksid ettevõtte nimel isikuandmeid töötlevate isikutega kirjalikud andmetöötluse kokkulepped ning näeb ette mõned kohustuslikud tingimused, mis sellistes lepingutes peavad sisalduma.

✓ Selles tööriistakomplektis sisalduvate *andmekaitse standardklauslite* abil saate olemasolevaid andmetöötluslepinguid muuta, sõlmides andmekaitset reguleeriva lisa või uue lepingu.

✓ Andmekaitse standardklauslid peaksid edaspidi olema iga andmetöötlust käsitleva lepingu kohustuslikuks osaks.

Isikuandmete register

Dokumenteerib ettevõtte andmetöötluse põhiprotsessid erinevate andmekogumite (*dataset*) kaupa.

PRIVAATSUSPOLIITIKA

Selles privaatsuspoliitikas („**privaatsuspoliitika**”) kirjeldame, kuidas [*ettevõtte nimi*] („**ettevõte**”) töötleb oma töötajate, klientide või ettevõttega muul moel koostööd tegevate inimeste isikuandmeid ning milliseid meetmeid me isikuandmete kaitsmiseks rakendame.

Isikuandmeid töödeldakse isikuandmete kaitse üldmääruse (määrus (EL) 2016/679) ning muude siseriiklike ja Euroopa privaatsusseaduste ning regulatsioonide (ühiselt „**andmekaitseseadus**”) kohaselt.

Selles privaatsuspoliitikas kasutatud mõisted on defineeritud 2. leheküljel.

1. ULATUS

Käesolev privaatsuspoliitika kohaldub kõigile isikuandmetele, mida vastutava töötlejana töötleme.

Ettevõte töötleb näiteks töötajate, ajutiste töötajate, füüsilisest isikust ettevõtjate, töö- ja ametikohale kandideerijate, tarnijate kontaktisikute, klientide ja külaliste ja muude koostööpartnerite isikuandmeid.

2. EESMÄRK

Selle privaatsuspoliitika eesmärk on selgitada, milliseid isikuandmeid me töötleme ning kuidas ja miks seda teeme. Lisaks kirjeldab see privaatsuspoliitika meie kohustusi ja vastutust andmete kaitsmisel.

See privaatsuspoliitika ei kajasta meie andmekaitsealaseid tegevusi ammendavalt, erinevates valdkondades, nagu nt turvalisus, sätestatakse täpsemad reeglid ja juhendid, millest mõistlikus ulatuses ettevõtte siseselt ka teavitame.

MÕISTED

Selles privaatsuspoliitikas kasutatakse mõisteid järgmises tähenduses:

EMP – Euroopa majanduspiirkond (hetkel kehtiva regulatsiooni kohaselt kuuluvad EMPsse kõik Euroopa Liidu liikmesriigid ning Norra, Island ja Liechtenstein).

GDPR – on ELi isikuandmete kaitse üldmäärus (*general data protection regulation*, (EU) 2016/679), mille rakendamine algab 25. mail 2018.a.

Isikuandmed – on igasugused andmed ja teave, mis on seotud füüsilise isiku ehk inimesega ja mis võimaldavad selle inimese isikut tuvastada. Isik on tuvastatav, kui tema isikut saab andmete põhjal ebaproportsionaalse pingutuseta mõistlikus ulatuses tuvastada. Tuvastamise aluseks võib olla näiteks nimi, isikukood, asukohateave, võrguidentifikaator või füüsiline, füsioloogiline, geneetiline, vaimne, majanduslik, kultuuriline või sotsiaalne tunnus või selliste tunnuste kombinatsioon.

Isikuandmete eriliigid – on isikuandmed, millest ilmneb inimese rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, aga ka geneetilised andmed, inimese kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed, terviseandmed või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta.

Isikuandmetega seotud rikkumine – on turberikkumine, mille tagajärg on edastatavate, talletatavate või muul viisil töödeldavate isikuandmete tahtmatu või ebaseaduslik hävimine, kaotsiminek, muutmine, lubamatu avaldamine või lubamatu juurdepääs neile andmetele.

Klient – on füüsiline isik, kellele ettevõte seoses oma majandustegevusega osutab teenuseid ja/või pakub kaupu.

Kolmas isik – on füüsiline või juriidiline isik, avaliku sektori asutus, amet või organ, välja arvatud andmesubjekt, vastutav töötleja või volitatud töötleja ja isikud, kes võivad isikuandmeid töödelda vastutava töötleja või volitatud töötleja otseses alluvuses.

Koostööpartner – füüsiline isik, kes on ettevõtte tarnija või muu juriidilisest isikust koostööpartneri töötaja/esindaja/kontaktisik.

Külastajakaardi andmed – turismiseaduses nõutud andmed majutusettevõtte külastaja kohta: nimi, sünniaeg, kodakondsus ja aadress; temaga koos majutatava abikaasa ja alaealise nimi, sünniaeg ja kodakondsus; majutusteenuse osutamise aeg; kui tegemist ei ole Eesti, EMP lepinguriigi või Šveitsi kodaniku või Eestis elamisloa või elamisõiguse alusel elava välismaalasega, siis ka: reisidokumendi liik, number ja selle välja andnud riik.

Profiilianalüüs – on igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud selle füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega.

Töötlemine – on isikuandmetega tehtav toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine. Töötlemine võib toimuda käsitsi või automatiseeritud süsteeme, näiteks IT-süsteeme, kasutades.

Töövõtja – on füüsiline isik (st mitte ettevõte), kellega ettevõte on sõlminud töövõtulepingu (teenuse osutamise leping), siia kuuluvad ka ettevõtte juhtorganite liikmed.

Vastutav töötleja – on isik, kes otsustab, miks ja kuidas (st mis eesmärkidel ja viisidel) isikuandmeid töödeldakse. Vastutava töötleja kindlakstegemisel võib olla abi järgmistele küsimustele vastamisest.

- Kes otsustab, milliseid isikuandmeid säilitatakse?
- Kes otsustab, mis eesmärkidel isikuandmeid kasutatakse?
- Kes otsustab, mis viisil isikuandmeid töödeldakse?

Kui isik otsustab ise tema valduses olevate isikuandmete töötlemise üle ja on nende eest vastutav, siis on ta vastutav töötleja.

Volitatud töötleja – on isik, kes töötleb isikuandmeid vastutava töötleja nimel. Kui isikuandmed on isiku valduses või ta töötleb neid, kuid tal ei ole voli nende töötlemise üle otsustamiseks, st ta töötleb neid vastutava töötleja juhiseid järgides, siis on see isik volitatud töötleja. Volitatud töötlejaks võib olla nt teenuse osutaja (näiteks palgaarvestusteenuse osutaja).

1. ISIKUANDMETE KATEGOORIAD

1.1 Töötajad ja töövõtjad

Ettevõte töötleb oma töötajate, töö- ja ametikohtadele (nt juhatuse liikmed) kandideerijate ja töövõtjate kohta, samuti endiste töötajate ja endiste töövõtjate kohta.

Need isikuandmed hõlmavad järgmist:

- isiklikud andmed, nagu nimi, sünniaeg, pangakonto andmed, lähisugulased, sotsiaalmeedia konto andmed, viisa-/passi-/ID kaardi andmed või vastava dokumendi koopia;
- kontaktandmed, nagu aadress ja telefoninumber, e-posti aadress;
- personalifaili andmed, muu hulgas: töösuhte tingimused, koolitusandmed, töötulemuste hindamised/hinnangud, edutamised, isiklikud arenguplaanid, käitumis- ja distsiplinaarandmed, töö asukoht, palgaandmed, pangakonto andmed ning maksukohustuslase number ja isikukood;
- töösuhete ajaloo / kandideerimise andmed, näiteks hariduse ja varasemate töösuhete ajalugu;
- pereliikmete andmed, näiteks laste sünniajad ja nimed (need on asjakohased näiteks juhul, kui inimene taotleb vanemapuhkust);
- ametiühingu liikmesust puudutavad andmed;
- tööalase sooritusega seotud andmed, näiteks töötajate iga-aastane palga ülevaatamine, psühhomeetrilised testid jne.
- [*vajadusel muutke ja täiendage ülaltoodut*]
- Isikuandmete eriliigid: meditsiinilised andmed, näiteks arstitõendid ja haiguslehed; [*milliseid isikuandmete eriliike te veel töötajate puhul töötlete*]

Ülaltoodud loetelu ei ole ammendav, kuid hõlmab kõige sagedamini kogutavaid, kasutatavaid ja muul viisil töödeldavaid isikuandmeid.

1.2 Kliendid

Ettevõte töötleb ka oma klientide isikuandmeid. Need isikuandmed võivad hõlmata järgmist:

- isiklikud andmed, nagu nimi, sünniaeg/isikukood;
- kontaktandmed, näiteks aadress ja telefoninumber, e-posti aadress;
- külastajakaardi andmed;
- krediitkaardi andmed nagu kaardi number, kehtivusaeg, CVV
- isiklikke eelistusi puudutavad andmed, nagu […].
- [*vajadusel muutke ja täiendage ülaltoodut*]
- Isikuandmete eriliigid: [*nimetage, milliseid isikuandmete eriliike te klientide puhul töötlete*]

1.3 Koostööpartnerid

Ettevõte töötleb oma koostööpartnerite isikuandmeid. Selliseid isikuandmed võivad hõlmata järgmist:

- isiklikud andmed, näiteks nimi, ametinimetus, ametikoht, tööalased identifitseerimisnumbrid, osakond, äriüksus (sh koolituse/kontrollimise jaoks kogutavad kontaktandmed);
- kontaktandmed, näiteks meiliaadress, telefoninumbrid ja töö asukoht;
- maksuandmed, näiteks käibemaksu-/maksukohustuslase numbrid.

- [*vajadusel muutke ja täiendage ülaltoodut*]

2. ANDMETE TÖÖTLEMISE EESMÄRGID

Ettevõte töötleb isikuandmeid nendel eesmärkidel, milleks isikuandmed on kogutud.

Töötajate isikuandmeid töötleme näiteks järgmistel eesmärkidel:
- töölepinguseaduses ettevõttele sätestatud tööandja kohustuste täitmine;
- palga ja hüvitiste haldamine;
- personalitegevuste, soorituse ja talendi juhtimine;
- siseauditid;
- [*vajadusel muutke ja täiendage ülaltoodut*]

Klientide ja koostööpartnerite isikuandmeid töötleme näiteks järgmistel põhjustel:
- turismiseaduses sätestatud majutusettevõtte kohustuste täitmine (nt külastajakaardi täitmine ja säilitamine 2.a. jooksul;
- kliendi/koostööpartneriga sõlmitud lepingu ettevalmistamine ja selle täitmine;
- turundus ja avalikud suhted;
- ettevõtte toodete ja teenuste täiustamine;
- uurimistöö ja statistiline analüüs;
- ettevõtte äristrateegia kujundamine;
- ettevõtte või meie klientide ja töötajate suhtes ebaseadusliku ja/või kuritegeliku käitumise vältimine ja tuvastamine.
- [*vajadusel muutke ja täiendage ülaltoodut*]

Aeg-ajalt võime töödelda isikuandmeid ka muudel põhjustel. Ettevõte püüab tagada inimeste teavitamise nende isikuandmete töötlemise eesmärkidest isikuandmete saamise ajal. Kui see pole võimalik või mõistlik, siis üritame inimesi teavitada esimesel võimalusel pärast isikuandmete saamist või muul viisil töötlemist.

3. PROFIILIANALÜÜS

Ettevõte teeb erinevate inimeste (nt töötajate, töövõtjate ja töö- või ametikohale kandideerijate aga ka klientide) osas profiilianalüüsi. Ettevõte tegeleb järgmist tüüpi profiilianalüüsiga:
- [*Näited: talendijuhtimiseks ja tööjõu hindamiseks;*
- *kohaloleku ja soorituse analüüsimiseks;*
- *kliendi eelistuste analüüsimiseks*]

Ettevõte töötleb selliseid andmeid, kui: a) see on seadustega sõnaselgelt lubatud; b) see on vajalik lepingu sõlmimiseks või täitmiseks või c) inimene on andnud selleks nõuetekohase nõusoleku.

Juhul, kui teeme automatiseeritud otsuseid, sealhulgas profiilianalüüsi, siis teavitame inimesi kasutatavast loogikast ja sellest, milline on sellise töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks.

4. ANDMESUBJEKTI ÕIGUSED

Inimestel on andmekaitseseaduse alusel oma isikuandmetega seonduvalt teatud õigused.

4.1. Õigus andmetega tutvuda – teil on õigus teada, milliseid andmeid teie kohta säilitatakse ja kuidas neid töödeldakse.

4.2. Õigus andmete parandamisele – teil on õigus nõuda oma isikuandmete parandamist, juhul kui need on ebaõiged.

4.3. Õigus andmete kustutamisele („õigus olla unustatud“) – teil on teatud juhtudel õigus nõuda, et me teie isikuandmed kustutaksime (nt kui meil ei ole neid enam vaja, te võtate tagasi meile andmete töötlemiseks antud nõusoleku, jne).

4.4. Õigus töötlemise piiramisele – teil on teatud juhtudel õigus keelata või piirata oma isikuandmete töötlemist teatud ajaks (nt kui olete esitanud vastuväite andmetöötluse osas).

4.5. Õigus esitada vastuväiteid – konkreetsest olukorrast lähtuvalt on teil õigus esitada oma isikuandmete töötlemise osas vastuväiteid kui teie andmete töötlemine toimub meie õigustatud huvist lähtudes või avalikust huvist lähtudes. Otseturunduse eesmärgil isikuandmete töötlemisele võib esitada vastuväiteid igal ajal.

4.6 Õigus andmete ülekandmisele – Juhul, kui isikuandmete töötlemine põhineb inimese nõusolekul või ettevõttega sõlmitud lepingul ja andmeid töödeldakse automatiseeritult, siis on inimesel õigus saada teda puudutavaid isikuandmeid, mida ta on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul ning õigus edastada need andmed teisele vastutavale töötlejale. Samuti on tal õigus nõuda, et ettevõte edastaks andmed otse teisele vastutavale töötlejale, *kui see on tehniliselt teostatav*.

4.7. Automaatse otsuste tegemine (sh profiilianalüüs) – juhul, kui olete teid teavitanud, et teostame automatiseeritud töötlusel põhinevat otsustamist (sh profiilianalüüsi), mis toob kaasa teid puudutavaid õiguslikke tagajärgi või avaldab teile märkimisväärset mõju, siis võite nõuda, et otsust ei tehtaks üksnes automatiseeritud töötluse alusel.

Andmesubjekti õiguste ja taotluste protseduuris on selgitatud, kuidas eespool nimetatud õigustega seotud taotlusi saab esitada ja kuidas ettevõte selliseid taotlusi haldab.

5. TURVE

5.1 Turbemeetmed

Ettevõttes on kehtestatud füüsilised, tehnilised ja organisatsioonilised meetmed isikuandmete kaitsmiseks ebaseadusliku või omavolilise hävitamise, kaotsimineku, muutmise, avaldamise, omandamise või neile lubamatu juurdepääsu eest.

Ettevõtte kasutab näiteks järgmisi füüsilisi andmeturbe meetmeid:

- isikuandmeid sisaldavaid paberkandjal dokumente hoitakse lukustatud ruumides ja kappides, millele on ligipääs vaid teatud töötajatel oma tööülesannete täitmiseks;
- andmete töötlemise ruumid ja IT-süsteemid on piisavalt kaitstud tule, ülekuumenemise, vee, voolukõikumiste ja voolukatkestuste eest;
- [*vajadusel muutke ja täiendage ülaltoodut*]

Tehniliste turbemeetmetena on ettevõttes kasutusel näiteks:

- videovalve;
- kõik tööarvutid on töötaja lahkumisel parooliga ekraanisäästjaga kaitstud;
- on tagatud, et IT-süsteem ei võimalda uusi sisenemiskatseid ja lukustab kasutajatunnuse, kui ebaõnnestunud sisenemiskatsete arv ületab teatud piiri;

- on tagatud, et eriti ohustatud süsteemid (nt sülearvutid, nutitelefonid) on piisavalt hästi kaitstud (kasutades näiteks krüpteerimist või muid viise);
- [*vajadusel muutke ja täiendage ülaltoodut*]

Organisatsiooniliste turbeneetmetena kasutame:
- juurdepääsud olulistele IT süsteemidele ja ruumidele on reguleeritud;
- kõigile IT süsteemide kasutajatele on määratud rollid ja profiilid;
- on kindlaks määratud, millistele andmetele millised kasutajad ligi pääseda tohivad ning ligipääsuõigused vastavad töötaja tööülesannetest tulenevatele vajadustele;
- on tagatud, et ligipääsuõigused tühistatakse töötaja lahkumisel ettevõttest;
- on tagatud, et avalikult kasutatavatest ruumidest ei pääse ilma volituseta ruumidesse, mida kasutatakse isikuandmete töötlemiseks;
- ettevõtte külastajate (st mitte avalikult kasutatavate ruumide külastajate) tarvis on koostatud külastuskord ning külastajate andmed, saabumis- ja lahkumisajad registreeritakse saabumisel ja lahkumisel;
- ruumid, kus asuvad IT-süsteemile ligipääsu võimaldavad arvutid ja ruumid, kus hoitakse isikuandmeid sisaldavaid dokumente, on kontrolli/valve all ka peale tööaja lõppu;
- [*vajadusel muutke ja täiendage ülaltoodut*]

5.2 Isikuandmetega seotud rikkumised

Ettevõtte tegeleb isikuandmetega seotud rikkumistega vastavalt isikuandmetega seotud rikkumisele reageerimise protseduuris sätestatule. Juhised isikuandmetega seotud rikkumiste tuvastamise ja sellest teatamise kohta leiate isikuandmete rikkumisele reageerimise protseduurist.

6. ISIKUANDMETE AVALDAMINE

Ettevõte võib aeg-ajalt isikuandmeid kolmandatele isikutele avaldada või neil ettevõttes töödeldavatele isikuandmetele juurde pääseda (näiteks kui õiguskaitseasutus või Andmekaitse Inspektsioon esitab kehtiva nõude isikuandmetele juurdepääsemiseks).

Ettevõte võib jagada isikuandmeid ka: a) teise ettevõttega samasse kontserni kuuluva isikuga (nt emaettevõte ja tütarettevõtted, kontserni lõplik kasusaaja ja selle tütarettevõtted); b) valitud muude osapooltega, sh äripartnerid, tarnijad ja töövõtjad; c) muude osapooltega, kui müüme või ostame teisi ettevõtteid või varasid (st tehingute tegemisel), või d) kui ettevõttel on seaduslik kohustus isikuandmeid avaldada (see hõlmab teabevahetust teiste ettevõtete ja organisatsioonidega pettuste vältimiseks).

Kui ettevõte sõlmib muude osapooltega lepinguid isikuandmete töötlemiseks ettevõtte nimel, tagab ta sobivate lepinguliste kaitsemeetmete olemasolu isikuandmete kaitsmiseks, kasutades muuhulgas andmekaitse standardklausleid, mis on välja töötatud ettevõtte nimel andmeid töötlevate isikutega sõlmitavatesse lepingutesse lisamiseks.

Ettevõte avaldab isikuandmeid või annab neile juurdepääsu järgmiste isikute kategooriatele allpool selgitatud eesmärkidel:

- sideteenuste osutajad – töötajate kõne- ja andmesideteenuste korraldamiseks;
- palgaarvestuse teenuse osutajad – töötajate palgaarvestuse pidamiseks;
- töötervishoiuteenuse osutajad – töötajate töötervishoiu korraldamiseks;
- värbamisagentuurid – uute töötajate/töövõtjate leidmiseks;
- turundusettevõtted – ettevõtte poolt nimetatud klientidele otseturunduse tegemiseks;

- kindlustusvahendajad ja kindlustusandjad – ettevõtte töötajate reisi-, õnnetusjuhtumi-, vms sellise kindlustuse tegemiseks;
- [*vajadusel muutke ja täiendage*]

7. ANDMETE SÄILITAMINE

Ettevõte säilitab isikuandmeid ainult seni, kuni selliste isikuandmete säilitamist peetakse vajalikuks eesmärkidel, milleks neid isikuandmeid koguti. Isikuandmeid säilitatakse asjakohaste seaduste ja ettevõtte põhimõtete kohaselt.

Ettevõte lähtub isikuandmete säilitamisel järgmistest kriteeriumidest:

- kui kaua kui on vaja isikuandmeid säilitada selleks, et pakkuda oma teenuseid
- kui isikul on ettevõtte juures kliendikonto või kliendikaart, siis säilitame isikuandmeid terve konto/kaardi aktiivsusaja või nii kaua kui neid on vaja isikule teenuste osutamiseks
- kui ettevõttel on seadusest tulenev, lepinguline või muu sarnane kohustus isiku andmete säilitamiseks, siis seni kuni on vajalik sellise kohustuse täitmiseks
- peale lepingulise suhte lõppemist säilitame teatud andmeid nii kaua, kui kaua on isikul (andmesubjektil) või ettevõttel endal õigus esitada lepingu alusel nõudeid teise poole vastu

Mõned näited:

- Külastajakaardi andmeid säilitame turismiseaduse nõuete kohaselt 2 aastat alates kaardi täitmisest.
- Töölepingu kirjalikke dokumente säilitame töölepingu seaduse nõuete kohaselt 10 aastat töölepingu lõppemisest.
- Krediitkaardiandmeid säilitame kuni meievahelise majutusteenuse lepingu nõuetekohase täitmiseni. [kui on põhjuseid krediitkaardi andmeid kauem hoida, siis selgitage miks ja kui kaua]

Täpsemad kriteeriumid sätestatakse ettevõtte *isikuandmete registris*.

8. ANDMEEDASTUS VÄLJASPOOLE EMPd

Aeg-ajalt võib ettevõttel olla vaja edastada isikuandmeid väljaspoole EMPd. Selline edastus toimub kehtiva andmekaitseseaduse kohaselt[1]. Ettevõte võtab tarvitusele mõistlikke abinõusid tagamaks, et isikuandmeid koheldakse EMPst väljapoole edastamisel turvaliselt ja selle privaatsuspoliitika kohaselt.

[1] GDPR artiklid 45-49 sätestavad millal ja mis tingimustel on andmete edastamine lubatud. GDPRi artikkel 45 kohaselt võib isikuandmeid EList väljapoole edastada siis, kui Euroopa komisjon on teinud otsuse, et selline kolmas riik, territoorium või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme. Selliseks edastamiseks ei ole vaja eriluba. Sellised riigid, territooriumid või rahvusvahelised organisatsioonid avaldatakse *Euroopa Liidu Teatajas* ja komisjoni veebilehel.

Ettevõte edastab isikuandmeid järgmistesse asukohtadesse väljaspool EMPd allpool nimetatud eesmärkidel, kasutades järgmisi meetmeid isikuandmete kaitseks:

- [*riik, kuhu andmeid edastatakse - edastamise eesmärk – tagatiste kirjeldus*]

[Selgituseks, tagatiseks võib olla, nt siduvad kontsernisised eeskirjad, standardsed andmekaitseklauslid Euroopa komisjoni poolt vastu võetud vormis, jne (vt GDPR Art. 46-49)]

9. VASTUTUSALAD

Ettevõte vastutab isikuandmete töötlemise eest. Üldine vastutus selle privaatsuspoliitika järgimise eest ettevõttes lasub ettevõtte juhtkonnal, kes määrab peamise kontakti seoses i) ettevõtte töötajate ja töövõtjate isikuandmete töötlemise; ii) klientide ja koostööpartnerite isikuandmete töötlemise ja iii) ettevõttes töödeldavate isikuandmete turvalisusega.

Kõigil ettevõtte töötajatel, kes puutuvad kokku isikuandmete töötlemisega on kohustus järgida kõige ajakohasemat avaldatud versiooni sellest privaatsuspoliitikast.

10. SEOTUD REEGLID JA PROTSEDUURID

Seda privaatsuspoliitikat tuleb lugeda koos järgmiste reeglite ja protseduuridega:

- Isikuandmetega seotud rikkumistele reageerimise protseduur
- Andmekaitse standardklauslid andmetöötluslepingutesse
- Andmesubjekti õiguste ja taotluste protseduur
- Privaatsusteade (töötajatele, klientidele)
- Isikuandmete register
- [*täiendage, kui teil on olemas või töötate välja täiendavaid reegleid*]

Kuupäev: […]

PRIVAATSUSTEADE

[*ettevõtte nimi*] (edaspidi “meie”) hindab kõrgelt iga oma kliendi (edaspidi „teie“) privaatsust. Selles privaatsusteates selgitame, milliseid andmeid me teie kohta kogume, miks me seda teeme ja mida me teie andmetega teeme.

1. **Kes me oleme?**
2. **Mis andmeid me teie kohta kogume ja kellelt me neid saame?**
3. **Miks meil teie andmeid vaja on? Mis juhtub, kui te andmeid ei esita?**
4. **Millisel õiguslikul alusel me andmeid töötleme?**
5. **Kellega me teie andmeid jagame?**
6. **Kui kaua me teie andmeid säilitame?**
7. **Millised on teie õigused seoses oma andmetega?**

Kes me oleme?

[Lühike kirjeldus ja kontaktandmed ettevõtte kohta ja kui asjakohane, siis andmekaitsespetsialisti kontaktandmed. Kui kuulute suuremasse gruppi/ketti, siis tooge ka see välja].

Me rakendame vajalikke tehnilisi, füüsilisi ja organisatsioonilisi turvameetmeid, et kaitsta teie isikuandmeid kadumise, hävimise ja omavolilise juurdepääsu eest.

Kui teil tekib privaatsusteates toodud info osas küsimusi, siis võtke meiega ühendust: [e-posti aadress]

Mis andmeid me teie kohta kogume ja kellelt me neid saame?

Me kogume teie kohta järgmisi andmeid:

- ✓ isiklikud andmed: nagu nt ees- ja perekonnanimi, sünniaeg/isikukood
- ✓ kontaktandmed: nagu nt elukoha aadress, telefoninumber, e-posti aadress
- ✓ külastajakaardi andmed: need on turismiseaduses nõutud andmed majutusettevõtte külastaja kohta – nt kodakondsus, külastajaga koos majutatava abikaasa ja alaealise nimi, sünniaeg ja kodakondsus, majutusteenuse osutamise aeg, jne
- ✓ krediitkaardi andmed: nagu nt kaardi number, omaniku nimi, kehtivusaeg
- ✓ turvakaamera salvestised – juhul kui külastate meie majutusasutust või muid ruume, kus asuvad turvalisuse kaalutlustel video või muud elektroonilised või digitaalsed jälgimissüsteemid või seadmed
- ✓ andmed isiklike eelistuste kohta: nagu nt […]

[ülaltoodud loetelu on näitlik – vajadusel muutke ja täiendage seda; kontrollige, kas kõiki andmeid, mida kogute on ka tegelikult vaja]

Üldjuhul saame andmed otse teilt, kui teete broneeringu või päringu meie veebilehe kaudu, telefoni või e-maili teel või ostate teenuseid otse, meie juurde kohale tulles.

Samuti edastavad teie andmeid meile reisiettevõtjad, broneerimisettevõtjad ning muud majutusteenuse vahendamisega tegelevad isikud, kellelt olete majutuse ja/või muud teenused meie juures tellinud. Juhul, kui me ei ole andmeid saanud otse teilt esitame privaatsusteate teile esimesel võimalusel peale andmete saamist.

Miks meil teie andmeid vaja on? Mis juhtub, kui te andmeid ei esita?

Kasutame teie andmeid teie poolt tellitud majutus- ja/või muude teenuste osutamiseks, samuti meie tegevust reguleerivate seadustega meile pandud kohustute täitmiseks ning üldistel ärilistel eesmärkidel, nagu näiteks:

- ✓ isiklikud andmed – neid andmeid vajame teie isikusamasuse tuvastamiseks, mis omakorda on oluline, et tagada teenuse osutamine isikule, kes selle tegelikult tellis
- ✓ kontaktandmed – neid andmeid vajame teiega ühenduse võtmiseks. Eelkõige võtame ühendust telefoni või e-posti vahendusel, kuid teatud juhtudel võib olla vajalik ka elukoha aadressi kasutamine (nt juhul, kui muude sidevahendite kaudu ühendust ei saa).
- ✓ külastajakaardiandmed – neid andmeid on meil kohustus küsida turismiseadusest tulenevalt. Eesmärgiks on ära hoida ohtu, mis võib peituda näiteks illegaalses immigratsioonis.
- ✓ krediitkaardi andmed – neid andmeid vajame juhul, kui tulenevalt meie [üldtingimustest] [majutusteenuse lepingust] on meil õigus teie krediitkaardilt kinni pidada teatud summa teie poolt tellitud teenuste eest tasumiseks või tehtud kulutuste hüvitamiseks.
- ✓ andmed isiklike eelistuste kohta – kui me neid andmeid küsime või kui te omal valikul meile selliseid andmeid avaldate, siis kasutame neid selleks, et osutada teile paremat, teie soovidest ja huvidest lähtuvat teenust.

  [ülaltoodud loetelu on näitlik – vajadusel muutke ja täiendage seda; kontrollige, kas kõiki andmeid, mida kogute on ka tegelikult vaja]

Kui te meile külastajakaardiandmeid ei esita, siis ei ole meil võimalik teile majutusteenust osutada.

Millisel õiguslikul alusel me teie andmeid töötleme?

Teie andmete töötlemisel tugineme erinevatele õiguslikele alustele:

- ✓ vajadus luua teiega lepinguline suhe või täita teiega sõlmitud lepingut
- ✓ teie nõusolek - *kui tugineme isikuandmete töötlemisel teie nõusolekule, siis teadke, et teil on õigus igal ajal oma nõusolek tagasi võtta*
- ✓ vajadus täita meile seadusega pandud kohustusi (nt külastajakaardi täitmine ja säilitamine 2 aasta jooksul)
- ✓ vajadus teostada meie õigustatud huvisid, sh ettevõtte juhtimine ja üldise äritegevuse elluviimine; seaduserikkumiste ja pettuste avastamine
- ✓ vajadus kaitsta teie või mistahes teise inimese elulisi huvisid (nt avaldades teie andmed õnnetusjuhtumi korral kiirabitöötajale)
- ✓ muul seadusega lubatud alusel.

Kellega me teie andmeid jagame?

Me ei jaga teie poolt meile usaldatud andmeid, väljaarvatud piiratud juhtudel, mida on kirjeldatud allpool ja juhul, kui see on selles privaatsusteates kirjeldatud eesmärkide saavutamiseks vajalik:

- ✓ Meie tütar ja sidusettevõtted: võime teie isikuandmeid jagada oma tütar- või sidusettevõtetega, mis kõik asuvad Euroopa Liidus.
- ✓ Teenusepakkujad: nagu mitmed teised firmad võime tellida andmete töötlemise teenuseid usaldusväärsetelt kolmandatelt teenusepakkujatelt, näiteks IT ja konsultatsiooniteenuseid;
- ✓ Avaliku võimu organid ja valitsusasutused: me võime jagada andmeid asutustega, kui me oleme seadusega kohustatud andmeid jagama või andmete jagamine on vajalik meie õiguste kaitseks;
- ✓ Professionaalsed nõustajad ja muud: me võime jagada teie andmeid professionaalsete nõustajatega nagu audiitorid, advokaadid, raamatupidajad ja muud nõustamisteenust pakkuvad isikud;
- ✓ Kolmandad isikud seoses ettevõtte tehingutega: Aeg-ajalt võime jagada teie andmeid kolmandate isikutega korporatiivse tehingu, näiteks ettevõtte või selle osa müügi raames teisele ettevõttele. Samuti ettevõtte ümberkorraldamise, ühisettevõtte loomise, ühinemise või muul viisil ettevõtte vara või aktsiate ümberpaigutamise raames.

  [ülaltoodud loetelu on näitlik – vajadusel muutke ja täiendage seda]

Juhul kui jagame teie andmeid ülaltoodud isikutega, siis tagame teie andmete kaitse meie ja sellise isiku vahel sõlmitavas andmetöötluslepingus.

Me ei säilita ega saada teie isikuandmeid väljaspoole Euroopa majanduspiirkonda ega riikidesse, mille kohta ei ole direktiivi 95/46/EÜ artikli 25 lõike 6 või selle järglasdokumendiks oleva määruse (EL) 2016/679 artikli 45 lõike 1 alusel kaitse piisavuse otsust tehtud.

Kui kaua me teie andmeid säilitame?

Säilitame teie andmeid niikaua kuni see on vajalik erinevate andme töötlemise eesmärkide täitmiseks.

Ettevõte lähtub isikuandmete säilitamisel järgmistest kriteeriumidest:

- nii kaua kui on vaja isikuandmeid säilitada selleks, et pakkuda oma teenuseid
- kui isikul on ettevõtte juures kliendikonto või kliendikaart, siis säilitame isikuandmeid terve konto/kaardi aktiivsusaja või nii kaua kui neid on vaja isikule teenuste osutamiseks
- kui ettevõttel on seadusest tulenev, lepinguline või muu sarnane kohustus isiku andmete säilitamiseks, siis seni kuni on vajalik sellise kohustuse täitmiseks
- peale lepingulise suhte lõppemist säilitame teatud andmeid nii kaua, kui kaua on isikul (andmesubjektil) või ettevõttel endal õigus esitada lepingu alusel nõudeid teise poole vastu

Näiteks, külastajakaardi andmeid säilitame turismiseaduse nõuete kohaselt 2 aastat alates kaardi täitmisest. Krediitkaardiandmeid säilitame ainult niikaua kuni meievahelise majutusteenuse lepingu nõuetekohase täitmiseni. [kui on põhjuseid krediitkaardi andmeid kauem hoida, siis selgitage miks ja kui kaua]

Kui olete meile andud nõusoleku otseturustusmaterjalide edastamiseks, siis säilitame teie kontaktandmeid seni kuni olete nõusoleku tagasi võtnud.

Millised on teie õigused seoses oma andmetega?

Teil on andmesubjektina järgmised õigused:

1. Õigus andmetega tutvuda – teil on õigus teada, milliseid andmeid teie kohta säilitatakse ja kuidas neid töödeldakse.

2. Õigus andmete parandamisele – teil on õigus nõuda oma isikuandmete parandamist, juhul kui need on ebaõiged.

3. Õigus andmete kustutamisele („õigus olla unustatud“) – teil on teatud juhtudel õigus nõuda, et me teie isikuandmed kustutaksime (nt kui meil ei ole neid enam vaja, te võtate tagasi meile andmete töötlemiseks antud nõusoleku, jne).

4. Õigus töötlemise piiramisele – teil on teatud juhtudel õigus keelata või piirata oma isikuandmete töötlemist teatud ajaks (nt kui olete esitanud vastuväite andmetöötluse osas).

5. Õigus esitada vastuväiteid – konkreetsest olukorrast lähtuvalt on teil õigus esitada oma isikuandmete töötlemise osas vastuväiteid kui teie andmete töötlemine toimub meie õigustatud huvist lähtudes või avalikust huvist lähtudes. Otseturunduse eesmärgil isikuandmete töötlemisele võib esitada vastuväiteid igal ajal.

6. Andmete ülekandmise õigus – teil õigus nõuda enda poolt meile edastatud andmete ülekandmist endale masinloetaval kujul. Võite nõuda andmete ülekandmist ka otse teisele vastutavale töötlejale, kuid seda ainult juhul, kui see on tehniliselt teostatav. Ülekandmise õigus kehtib ainult nende andmete puhul, mida me töötleme teie nõusoleku alusel või teiega sõlmitud lepingu täitmiseks.

7. Automaatse otsuste tegemine (sh profiilianalüüs) – juhul, kui olete teid teavitanud, et teostame automatiseeritud töötlusel põhinevat otsustamist (sh profiiilianalüüsi), mis toob kaasa teid puudutavaid õiguslikke tagajärgi või avaldab teile märkimisväärset mõju, siis võite nõuda, et otsust ei tehtaks üksnes automatiseeritud töötluse alusel.

Kui teil tekib selles teates toodud info osas küsimusi või soovite esitada taotlust andmesubjekti õiguste teostamiseks, siis võtke meiega ühendust e-posti aadressil [...].

Me teeme oma parima, et adresseerida teie taotlusi ja soove aegsasti ja ilma tasuta, välja arvatud juhtudel, kus sellega kaasneks ebaproportsionaalne kulu. Kui te ei ole rahul meie poolt antud vastusega, siis on teil võimalik pöörduda kaebusega Andmekaitse Inspektsiooni poole.

PRIVAATSUSTEADE (TÖÖTAJATELE)[1]

[ettevõtte nimi] (edaspidi ka „meie“) hindab kõrgelt oma töötajate (sh tööle kandideerijate) (edaspidi „teie“) privaatsust. [ettevõtte nimi] privaatsuspoliitika kirjeldab, kuidas me erinevate füüsiliste isikute, sh teie, isikuandmeid töötleme. Privaatsuspoliitikas on muuhulgas kirjas meie põhimõtted nii teie kui ka teiste füüsiliste isikuandmete kogumise, kasutamise, edastamise, avaldamise ja muu töötlemise aga ka kohaldatavate turvameetmete osas.
Palun viige end kurssi meie privaatsuspoliitika tingimustega, mille leiate siseveebist: [lisage viide, link] [selle koopia on teile edastatud].

Mis tüüpi isikuandmeid me töötleme?

Isikuandmed, mida teie kohta töötleme, hõlmavad teie isiklikke andmeid nagu nt nimi, isikukood; kontaktandmeid nagu telefoninumber aga ka muid vajalikke isikuandmeid, kui: a) kui see on vajalik seoses teie töösuhtega; b) kui kohalduvad seadused seda meile lubavad või nõuavad või c) see on meie äritegevuse jaoks vajalik.

Miks me teie isikuandmeid töötleme?

Nagu privaatsuspoliitika ette näeb, kasutame teie isikuandmeid mitmesugustel põhjustel, muu hulgas:

- ✓ seadusest tulenevate nõuete täitmiseks, nagu näiteks dokumentide säilitamine ja aruandlus, lepinguliste kohustuste ja/või tervishoiukohustuste täitmine;
- ✓ üldisteks ärilisteks eesmärkideks, näiteks palgaarvestusega seotud toimingud, töölähetuste korraldamine ja/või toodete ning teenuste täiustamine;
- ✓ selleks, et hõlbustada teie ja teie nimetatud kontaktisikutega suhtlemist hädaolukorras ning töötajate ja muude isikute tervise ja ohutuse kaitsmiseks.

Millisel õiguslikul alusel me teie andmeid töötleme?

Töösuhetes tugineme isikuandmete töötlemisel eelkõige järgmistele õiguslikele alustele:

- ✓ vajadus luua teiega lepinguline suhe või täita teiega sõlmitud lepingut
- ✓ vajadus täita meile seadusega pandud kohustusi (nt töölepingu sõlmimine ja säilitamine 10 aasta jooksul)
- ✓ vajadus teostada meie õigustatud huvisid, sh ettevõtte juhtimine ja üldise äritegevuse elluviimine, seaduserikkumiste ja pettuste avastamine
- ✓ muul seadusega lubatud alusel.

Töösuhetes me reeglina isikuandmete töötlemisel töötaja nõusolekule ei tugine. Kui selleks peaks siiski vajadus tekkima, *siis teadke, et teil on õigus igal ajal oma nõusolek tagasi võtta.*

Teatud erandlikel juhtudel võib isikuandmete töötlemise õiguslikuks aluseks olla vajadus kaitsta teie või mistahes teise inimese elulisi huvisid (nt avaldades teie andmed õnnetusjuhtumi korral kiirabitöötajale).

[1] Selgituseks ettevõttele: Ettevõtte uute töötajate puhul võib privaatsusteate punktid lisada ka temaga sõlmitavasse töölepingusse.

Teie isikuandmete turvalisus

Niivõrd kui see on mõistlikult võimalik, on meil kehtestatud sobivad juriidilised, organisatsioonilised, füüsilised ja tehnilised meetmed isikuandmete kaitsmiseks. Lisaks, kui kasutame ettevõtte väliseid teenusepakkujaid, sõlmime sellise teenuse osutajaga andmetöötluslepingu, milles kohustame teenus osutajat: a) võtma tarvitusele sobivaid meetmeid isikuandmete konfidentsiaalsuse ja turvalisuse kaitsmiseks ja ii) töötlema isikuandmeid vastavate seaduse nõuetele.

Isikuandmete avaldamine ja edastamine

Ettevõtte töötajatel on juurdepääs teie tööalastele kontaktandmetele, nt nimi, ametikoht, telefoninumber ja meiliaadress. Lisaks nendele tööalastele kontaktandmetele on juurdepääs muudele isikuandmetele ning nende töötlemine on üldjuhul lubatud ainult neile inimestele, kellel on neid andmeid vaja tööülesannete täitmiseks (nn *need-to-know basis*). Selliste inimeste hulka võivad kuuluda teie otsene ülemus ja teised tema poolt määratud inimesed ning [personali-, IT-,raamatupidamis-, finants- ning siseauditite] osakonna töötajad.

Aeg-ajalt võime teha isikuandmeid kättesaadavaks teistele meie kontserni üksustele ja muudele osapooltele, nt õiguskaitse- ja reguleerivatele asutustele, välistele professionaalsetele nõustajatele (nt advokaadid, audiitorid, jne) ja teenusepakkujatele (nt palgaarvestuse, kindlustuse, personaliteenuste, IT-süsteemide ja -toe pakkujatele ning muudele osapooltele, kes meid äritegevuses aitavad).

Aeg-ajalt võime jagada teie andmeid kolmandate isikutega korporatiivse tehingu, näiteks meie ettevõtte või selle osa müügi raames teisele ettevõttele. Samuti meie ettevõtte ümberkorraldamise, ühisettevõtte loomise, ühinemise või muul viisil ettevõtte vara või aktsiate ümberpaigutamise raames.

Juhul kui jagame teie andmeid ülaltoodud isikutega, siis tagame teie andmete kaitse meie ja sellise isiku vahel sõlmitavas andmetöötluslepingus.

[Me ei säilita ega saada teie isikuandmeid väljaspoole Euroopa majanduspiirkonda ega riikidesse, mille kohta ei ole direktiivi 95/46/EÜ artikli 25 lõike 6 või selle järglasdokumendiks oleva määruse (EL) 2016/679 artikli 45 lõike 1 alusel kaitse piisavuse otsust tehtud.]

Teie õigused

Teil on meie juures oma isikuandmete töötlemisega seoses teatud õigused, muu hulgas õigus:

Õigus andmetega tutvuda – teil on õigus teada, milliseid andmeid teie kohta säilitatakse ja kuidas neid töödeldakse.
Õigus andmete parandamisele – teil on õigus nõuda oma isikuandmete parandamist, juhul kui need on ebaõiged.
Õigus andmete kustutamisele – teil on teatud juhtudel õigus nõuda, et me teie isikuandmed kustutaksime (nt kui meil ei ole neid enam vaja, te võtate tagasi meile andmete töötlemiseks antud nõusoleku)
Õigus töötlemise piiramisele – teil on teatud juhtudel õigus keelata või piirata oma isikuandmete töötlemist teatud ajaks (nt kui olete esitanud vastuväite andmetöötluse osas).
Õigus esitada vastuväiteid – konkreetsest olukorrast lähtuvalt on teil õigus esitada oma isikuandmete töötlemise osas vastuväiteid kui teie andmete töötlemine toimub meie õigustatud huvist lähtudes või avalikust huvist lähtudes.
Automaatse otsuste tegemine (sh profiilianalüüs) – juhul, kui oleme teid teavitanud, et teostame automatiseeritud töötlusel põhinevat otsustamist (sh profiilianalüüsi), mis toob kaasa

teid puudutavaid õiguslikke tagajärgi või avaldab teile märkimisväärset mõju, siis võite nõuda, et otsust ei tehtaks üksnes automatiseeritud töötluse alusel.

Palun pange tähele, et tulenevalt töösuhte spetsiifikast ning kohalduvatest seadustest ei pruugi need õigused teatud isikuandmete või isikuandmete teatud töötlusviiside puhul kehtida.

Kui soovite mõnda eespool nimetatud õigust kasutada, palun pöörduge meie personaliosakonna poole, kes teid selles protsessis juhendab.

Teie kohustused

Teie ülesanne on hoida oma isikuandmeid ajakohasena, teavitades meid olulistest muudatustest oma isikuandmetes.

Samuti on teie kui töötaja kohus teiste inimeste isikuandmete kaitseks järgida kõiki kohaldatavaid seadusi ja/või ettevõttesiseseid poliitikaid, norme ja protseduure, arvestades neis aeg-ajalt tehtavaid muudatusi. Täpsemalt tohite isikuandmetele juurde pääseda ja kasutada neid ainult seoses oma tööülesannetega, ja ainult vajalikul määral.

Teie kohustus hoida teiste inimeste isikuandmeid konfidentsiaalsena on jõus ka pärast meiega töösuhte lõpetamist.

Teatis

Palume teil allkirjastada ja tagastada **lisas** olev teatis, mis kinnitab, et olete lugenud privaatsuspoliitikat ja tingimusi, mis puudutavad eespool nimetatud isikuandmete töötlemist, kinnitades, et mõistate oma seonduvaid õigusi ja kohustusi.

LISA
Isikuandmete kaitse teatis

Mina, [ees- ja perekonnanimi], kinnitan käesolevaga, et olen **lugenud ja mõistan** privaatsusteates sätestatud isikuandmetega seotud tingimusi. Samuti olen **lugenud ja mõistan** ettevõtte privaatsuspoliitikat

Saan aru, et ettevõte töötleb minu isikuandmeid, kui: a) see on ettevõtte äritegevuse jaoks vajalik; b) kui kohalduvad seadused seda lubavad või nõuavad või c) kui see on vajalik seoses meievahelise töösuhtega.

Lisaks mõistan, et minu kohus on tagada oma isikuandmete õigsus ja et mul on õigus:

- oma isikuandmetega tutvuda, nõuda nende muutmist, nende töötlemist piirata, nõuda teatud juhtudel kustutamist või nende kasutamisele vastuväiteid esitada;
- küsida teavet selle kohta, millisel alusel minu isikuandmeid töödeldakse, ja/või
- juhul kui minu isikuandmete töötlemine tugineb minu nõusolekule, võtta oma nõusolek oma valikul tagasi.

Samuti nõustun käesolevaga järgima töösuhte kestel töötlema teiste inimeste isikuandmeid vastavalt ettevõtte privaatsuspoliitikale (sh mis tahes selle hilisematele versioonidele).

Allkirjastanud: ..... Kuupäev: .....

ISIKUANDMETEGA SEOTUD RIKKUMISTELE REAGEERIMISE PROTSEDUUR

1. SISSEJUHATUS

See isikuandmetega seotud rikkumistele reageerimise protseduur („**protseduur**") kirjeldab isikuandmetega (defineeritud allpool) seotud rikkumistest või rikkumiskahtlusest teatamise ja registreerimise protsessi.

Selle protseduuri eesmärk on tagada, et ettevõte tegeleks ja kõrvaldaks igasuguse isikuandmetega seotud rikkumise sündmuse kiiresti, et selle mõju oleks minimaalne ning et kõik seadusest tulenevad kohustused teavitada isikuandmetega seotud rikkumisest Andmekaitse Inspektsiooni („**AKI**") ja/või rikkumisest mõjutatud isikut/isikuid kooskõlas isikuandmete kaitse üldmäärusega (määrus (EL) 2016/679) („**GDPR**")) saaks õigeaegselt täita.

2. MIS ON ISIKUANDMED?

Isikuandmed on igasugused andmed, mis puudutavad ELis asuvat inimest ja mille alusel on võimalik seda inimest tuvastada („**isikuandmed**"). Isik on tuvastatav, kui tema isikut saab andmete põhjal ebaproportsionaalse pingutuseta mõistlikus ulatuses tuvastada. Tuvastamise aluseks võib olla näiteks nimi, isikukood, asukohateave, võrguidentifikaator või füüsiline, füsioloogiline, geneetiline, vaimne, majanduslik, kultuuriline või sotsiaalne tunnus või selliste tunnuste kombinatsioon.

3. MIS ON ISIKUANDMETEGA SEOTUD RIKKUMINE?

GDPRi definitsiooni kohaselt on isikuandmetega seotud rikkumine „*on turberikkumine, mille tagajärg on edastatavate, säilitatavate või muul viisil töödeldavate isikuandmete tahtmatu või ebaseaduslik hävimine, kaotsiminek, muutmine, lubamatu avaldamine või lubamatu juurdepääs neile andmetele*" („**isikuandmetega seotud rikkumine**").

Isikuandmetega seotud rikkumine leiab aset siis, kui isikuandmeid loata või kogemata avaldatakse, need kaotsi lähevad või kui neid mis tahes muul viisil omavoliliselt, kogemata või ebaseaduslikult kogutakse, kasutatakse, registreeritakse, talletatakse või jagatakse. Isikuandmetega seotud rikkumise näited on: isikuandmeid sisaldava sülearvuti või mobiiltelefoni kaotsiminek või vargus; (kaitsmata) isikuandmeid sisaldava Exceli faili saatmine vastuvõtuks õigustamata isikule; palgaandmete printimine ja nende printerisse jätmine; isikuandmeid sisaldavasse süsteemi häkkimine ja/või failide kaotsiminek või vargus jne.

Igasugust andmeturbe rikkumisega seotud juhtumit nimetatakse „**andmekaitsejuhtumiks**". Kui andmekaitsejuhtum ei hõlma isikuandmeid, pole tegemist isikuandmete rikkumisega. Lisaks pole mitte kõik isikuandmeid hõlmavad andmekaitsejuhtumid isikuandmetega seotud rikkumised. Näiteks ei pruugi isikuandmete kaotsiminek olla isikuandmetega seotud rikkumine, kui: i) isikuandmed on krüpteeritud või anonüümseks muudetud; ii) isikuandmetest on tehtud täielik ajakohane varukoopia ning iii) juurdepääsu isikuandmetele jälgitakse. Seetõttu tuleb juhtumipõhiselt otsustada, kas andmekaitsejuhtum kujutab endast isikuandmetega seotud rikkumist.

4. MILLAL SEDA PROTSEDUURI KOHALDATAKSE?

Kui andmekaitsejuhtum *ei hõlma* isikuandmeid, siis ei ole vaja seda protseduuri järgida. Kui andmekaitsejuhtum *hõlmab* isikuandmeid, võib olla tegemist isikuandmetega seotud rikkumisega ja seda protseduuri kohaldatakse. Kahtluste korral, kas on toimunud isikuandmetega seotud rikkumine, peaks ettevõte olukorda hindama ja vajadusel küsima nõu ka vastava valdkonna spetsialistidelt väljastpoolt ettevõtet.

5. KUIDAS ISIKUANDMETEGA SEOTUD RIKKUMISEST TEATADA?

On tähtis, et kõigist tegelikest või arvatavatest isikuandmetega seotud rikkumistest teatataks kohe järgmiste juhiste kohaselt.

5.1 Esialgne teatamine

Kui saate teada tegelikust või arvatavast isikuandmetega seotud rikkumisest, tuleb sellest teatada kohe ettevõtte tegevjuhile ja olemasolu korral andmekaitsespetsialistile või ettevõttes andmekaitse eest vastutavale isikule (edaspidi mõlema kohta „**andmekaitsespetsialist**“).

5.2 Lahenduskava koostamine

Kui on toimunud isikuandmetega seotud rikkumine, koostab ettevõtte tegevjuht koostöös andmekaitsespetsialistiga plaani isikuandmetega seotud rikkumise lahendamiseks. Selle protseduuri lisas 1 on voodiagramm isikuandmete rikkumise lahendamiseks.

Asjakohase lahenduskava koostamisel arvestab lahendusega tegelev meeskond järgmist:

- isikuandmetega seotud rikkumise teatises saadud andmeid;
- vajalikke toiminguid, mis on vaja isikuandmetega seotud rikkumise peatamiseks kohe teha;
- kas on vajalik teavitada AKI´t isikuandmetega seotud rikkumisest ja kui on, siis millest tuleb teatada;
- isikuandmetega seotud rikkumisest tulenevad võimalikud tagajärjed ettevõttele ja mõjutatud isikutele;
- meetmed, mida ettevõte sellel ajal rakendab ja/või saab rakendada, et mõjutatud isikute kahju vähendada;
- viis, kuidas rikkumisest mõjutatud isikuid isikuandmete rikkumisest teavitatakse, kas see on antud olukorras kohane; ja meetmed, mida inimesed saavad rakendada edasise kahju leevendamiseks;
- kas isikuandmetega seotud rikkumisega võib kaasneda ettevõtte vastutus või muude osapoolte (nt volitatud töötleja) vastutus;
- ettevõtte sisene (ja vajaduse korral väline) kommunikatsioon ja sellise kommunikatsiooni ajastus;
- kas lisaks AKI´le tuleks teavitada ka muid huvirühmi; ja
- mida saab isikuandmetega seotud rikkumisest õppida ja milliseid meetmeid rakendada, et püüda konkreetse rikkumise kordumist ja sarnaseid rikkumisi vältida.

5.3 Kas AKI teavitamine on nõutav?

Igast isikuandmetega seotud rikkumisest pole vaja AKI´t teavitada. Näiteks pole vaja AKI´t teavitada, kui isikuandmete rikkumisega ei kaasne tõenäoliselt ohtu ühelegi inimesele. Kui AKI´t siiski on vaja teavitada, teeb seda ettevõtte tegevjuht kui on teavitamise vajadust andmekaitsespetsialistiga arutanud.

Seega peab ettevõte hindama, millal on tegu ohuga füüsiliste isikute õigustele ja vabadustele. GDPRi põhjenduspunktid 75, 76 ja 85 selgitavad, et erineva tõenäosuse ja tõsidusega ohud füüsiliste isikute õigustele ja vabadustele võivad tuleneda isikuandmete töötlemisest, mille tulemusel võib tekkida füüsiline, materiaalne või mittemateriaalne kahju, eelkõige juhtudel, kui:

- töötlemine võib põhjustada diskrimineerimist, identiteedivargust või -pettust, rahalist kahju, maine kahjustamist, pseudonümiseerimise loata tühistamist või mõnda muud tõsist majanduslikku või sotsiaalset kahju;
- andmesubjektid võivad jääda ilma oma õigustest ja vabadustest või kontrollist oma isikuandmete üle;
- töödeldakse isikuandmete eriliike (delikaatseid isikuandmeid);
- tegeletakse profileerimisega;
- töödeldakse kaitsetute füüsiliste isikute, eriti laste isikuandmeid;
- töötlemine hõlmab suurt hulka isikuandmeid ning mõjutab paljusid andmesubjekte.

Andmesubjekti õigustele ja vabadustele tekkiva ohu tõenäosus ja tõsidus tuleks teha kindlaks lähtudes andmetöötluse laadist, ulatusest, kontekstist ja eesmärkidest. Ohtu tuleks hinnata objektiivse hindamise põhjal, millega tehakse kindlaks, kas andmetöötlustoimingutega kaasneb oht või suur oht.

Teade AKI´le tuleb edastada tarbetu viivituseta ja võimaluse korral hiljemalt 72 tundi pärast isikuandmetega seotud rikkumisest teadasaamist. Kui teadet ei edastata 72 tunni jooksul, tuleb esitada AKI´le selgitustega põhjendus viivituse kohta.

5.4 Lahendamine

Pärast AKI teavitamist ja AKI poolt tehtud tähelepanekute kaalumist peab ettevõtte tegevjuht andmekaitsespetsialistiga isikuandmetega seotud rikkumise käsitlemise ja lahendamise teemal nõu, lähtudes asjakohasest isikuandmetega seotud rikkumise lahenduskavast.

6. MILLEST ON VAJA AKI´t TEAVITADA?

Aruandes AKI´le tuleb teavitada järgmisest:

- isikuandmetega seotud rikkumise iseloom, muu hulgas puudutatud isikuandmete kategooriad ja inimeste kategooriad (nt töötajad või kliendid), mõjutatud inimeste arv ja ohustatud isikuandmete hulk;
- isikuandmetega seotud rikkumise eeldatavad tagajärjed;
- meetmed, mis on võetud või mida plaanitakse võtta tarvitusele isikuandmetega seotud rikkumise kõrvaldamiseks;
- meetmed, mida rikkumisest mõjutatud inimesed saavad tarvitusele võtta, et piirata isikuandmetega seotud rikkumisest tulenevaid kahjulikke tagajärgi; ja
- ettevõtte kontaktisiku nimi ja kontaktandmed lisateabe saamiseks isikuandmetega seotud rikkumise kohta.

NB! Rikkumisteadete edastamise hõlbustamiseks on AKI´l kavas oma võrgulehele luua vastav veebiteenus.

7. ISIKUANDMETEGS SEOTUD RIKKUMISEST TEATAMINE MÕJUTATUD INIMESTELE

Isikuandmetega seotud rikkumisest mõjutatud inimest tuleb teavitada ainult juhul, kui isikuandmete rikkumisega kaasneb tõenäoliselt suur oht selle inimese õigustele ja

vabadustele. Isikuandmete rikkumisest teatamine mõjutatud isikutele peab toimuma vastava lahenduskava kohaselt.

Töötlemistoimingute liigid, mis kujutavad oma laadi, ulatuse, konteksti ja eesmärkide poolest tõenäoliselt suurt ohtu füüsiliste isikute õigustele ja vabadustele on näiteks:

- uue tehnoloogia kasutamine. *See ei pea ilmtingimata olema ajalises plaanis uus, vaid võib olla näiteks tark- või riistvara, mis on turul juba mõnda aega olnud kättesaadav, kuid mida andmetöötleja ei ole seni kasutanud, kuid plaanib kasutusele võtta*;
- andmetöötlustoimingud on uut tüüpi ja vastutav töötleja ei ole nende osas varem andmekaitsealast mõjuhinnangut teostanud. *Näiteks uute toodete või teenuste arendamine ning pakkumine*;
- ulatuslikud isikuandmete töötlemise toimingud, mille eesmärk on töödelda suurt hulka isikuandmeid piirkondlikul, riiklikul või rahvusvahelisel tasandil ja mis võivad mõjutada paljusid andmesubjekte;
- avalike alade ulatuslik jälgimine, eriti kui kasutatakse elektroonilisi optikaseadmeid (nt videokaamerad korrakaitse või valve eesmärgil).

Andmesubjekti teavitamise eesmärk on lisaks ettevõttele võimaldada ka andmesubjektil endal võtta vajalikke ettevaatusabinõusid ohu leevendamiseks. Teates tuleks kirjeldada isikuandmetega seotud rikkumise olemust, samuti tuleks anda asjaomasele füüsilisele isikule soovitusi võimaliku kahjuliku mõju leevendamiseks.

Rikkumisest mõjutatud isikutele saadetav teavitus peab sisaldama vähemalt järgmist:
- isikuandmetega seotud rikkumise iseloom ja ulatus;
- meetmed, mis on isikuandmetega seotud rikkumise negatiivsete tagajärgede piiramiseks tarvitusele võetud;
- nii isikuandmetega seotud rikkumise tegelike kui ka eeldatavate tagajärgede kirjeldus; ja
- meetmed, mida ettevõte on tarvitusele võtnud või kavatseb isikuandmetega seotud rikkumise tagajärgede leevendamiseks rakendada.

Inimeste teavitamine pole vajalik, kui:
- ettevõte on rakendanud sobivaid tehnilisi ja organisatsioonilisi meetmeid, mis muudavad isikuandmed loetamatuks kõigile, kellel puudub õigus neile juurde pääseda, näiteks krüpteerimise kaudu;
- ettevõte on võtnud tarvitusele edasisi meetmeid, mis tagavad selle, et suur oht inimestele tõenäoliselt ei realiseeru; või
- see nõuaks ebaproportsionaalseid jõupingutusi. Sellisel juhul tehakse avalik teadaanne või võetakse tarvitusele muud sarnased meetmed, et rikkumisest puudutatud isikuid võrdselt teavitada.

Juhul kui ettevõte ei pea vajalikuks andmesubjekte informeerida, annab GDPRi artikkel 34(4) AKI´le siiski õiguse ettevõttelt vastavat teavitamist nõuda.

8. RIKKUMISTE REGISTER

Ettevõte peab pidama isikuandmetega seotud rikkumiste registrit, milles dokumenteeritakse kõik isikuandmetega seotud rikkumised („**register**").

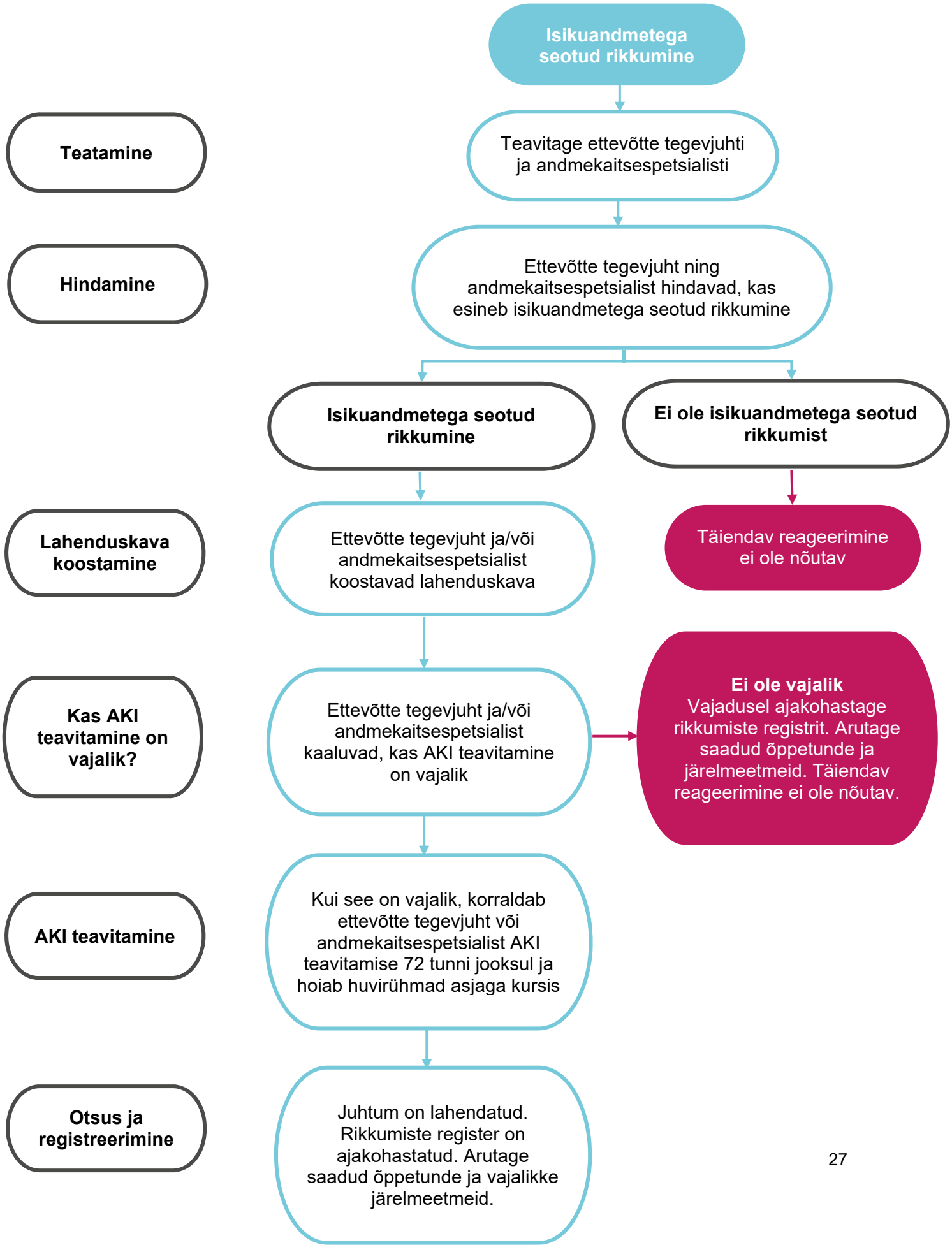
Registri eesmärk on: i) õppida isikuandmete rikkumisest ja sellest, kuidas sellega toime tuldi; ii) suuta anda täpseid vastuseid rikkumisest mõjutatud isikutelt ja/või AKI´lt saadud küsimustele ning iii) luua võimalus, et vajadusel AKI´le tõendada isikuandmetega seotud rikkumise menetlemiseks GDPR´is ettenähtud nõuete täitmist.

Iga isikuandmetega seotud rikkumise kohta kantakse registrisse järgmised andmed:

- isikuandmete rikkumisest teadasaamise/teavitamise kuupäev ja kellaaeg;
- mõjutatud isiku(te) nimi ja kontaktandmed;
- faktid ja üksikasjad isikuandmetega seotud rikkumise iseloomu kohta;
- isikuandmetega seotud rikkumise mõjude kirjeldus;
- kellele isikuandmete rikkumisest on teatatud ja miks; ning
- järelmeetmed pärast isikuandmete rikkumise avastamist (nt meetmed, mis takistavad isikuandmete rikkumise kordumist jne).

LISA 1

Isikuandmetega seotud rikkumise protseduuri voodiagramm



ANDMESUBJEKTI ÕIGUSED JA TAOTLUSED

Isikuandmete kaitse üldmäärus („**GDPR**") annab inimestele seoses nende isikuandmetega väga laialdased õigused („**andmesubjekti õigused**"). Sellest lähtuvalt võivad inimesed esitada taotlusi oma isikuandmetega tutvumiseks, andmete muutmiseks, kustutamiseks, parandamiseks või ülekandmiseks ning esitada andmete töötlemisele vastuväiteid.

Selle dokumendi eesmärk on selgitada: 1) millised õigused andmesubjektil on ja 2) kuidas käsitleda taotlusi („**taotlus**") selliste andmesubjekti õiguste kasutamiseks kooskõlas GDPRi või muude kohalduvate seadustega. Voodiagramm selle dokumendi lisas 1 aitab illustreerida nimetatud taotluste käsitlemise protseduuri.

1. ANDMESUBJEKTI ÕIGUSED

Andmesubjektil on GDPRist tulenevalt järgmised õigused.

A. Juurdepääsuõigus

Kui isik esitab isikuandmetega seotud taotluse tuleb mõistlikke vahendeid kasutades tuvastada taotlust esitava isiku identiteet, et andmeid ei avaldataks õigustamata isikule. Näiteks, tuleb kontrollida, kas taotlus on edastatud andmesubjekti tavapäraselt e-posti aadressilt, mille ta ise oma kontaktandmete all avaldanud on.

[*Kommentaar: GDPR soovitab võimalusel luua isikutele nö kaugjuurdepääs turvalisele iseteenindussüsteemile, mis annab isikule otseligipääsu oma andmetele ja nende muutmisele*.]

Kui isik esitab vastavasisuise taotluse, peab ettevõte vastutava töötlejana:

- kinnitama, kas ta töötleb selle inimese isikuandmeid;
- kui ettevõte isikuandmeid töötleb on inimesel õigus tutvuda isikuandmetega ja saada järgmist teavet:
  - mis on töötlemise eesmärk
  - mis liiki isikuandmeid töödeldakse
  - vastuvõtjad (või nende kategooriad), kellele isikuandmeid avalikustatakse või avalikustatakse, eelkõige kolmandates riikides olevad vastuvõtjad või rahvusvahelised organisatsioonid;
  - kui võimalik, siis kavandatav isikuandmete säilitamise ajavahemik või selle määramise kriteeriumid;
  - teave õiguse kohta taotleda vastutavalt töötlejalt andmesubjekti puudutavate isikuandmete parandamist, kustutamist või töötlemise piiramist või esitada vastuväide sellisele isikuandmete töötlemisele;
  - teave õiguse kohta esitada kaebus järelevalveasutusele;
  - kui isikuandmeid ei ole saadaud andmesubjektilt, siis teave andmete allika kohta;
  - teave automatiseeritud otsuste, sealhulgas profiilianalüüsi tegemise kohta ning sisuline teave kasutatava loogika ja selle kohta, millised on sellise töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks.
- edastama inimesele isikuandmete koopia. Kui inimene esitab taotluse elektrooniliselt, siis esitatakse ka teave elektroonilises vormis.

B. Õigus andmete parandamisele

Inimestel on õigus nõuda isikuandmete parandamist, kui andmed on ebaõiged või mittetäielikud. Ettevõte kui vastutav töötleja peab sellisel juhul parandama isikuandmed põhjendamatu viivituseta.

Kui selliseid isikuandmeid on jagatud kolmanda isikuga, peab selliseid isikuid võimalusel parandamisest teavitama. Samuti tuleb teavitada inimest nendest kolmandatest isikutest, kellele on tema isikuandmeid edastatud.

C. Õigus andmete kustutamisele (ka „õigus olla unustatud")

Andmesubjektil on õigus nõuda, et ettevõte, kes tema isikuandmeid vastutava töötlejana töötleb kustutaks põhjendamatu viivituseta teda puudutavad isikuandmed ja ettevõte on kohustatud seda tegema, kui kehtib üks järgmistest asjaoludest:

- isikuandmeid ei ole enam vaja sellel eesmärgil, millega seoses need on kogutud;
- andmesubjekt võtab töötlemiseks antud nõusoleku tagasi (st andmetöötlus toimub nõusoleku alusel) ning puudub muu õiguslik alus isikuandmete töötlemiseks;
- andmesubjekt esitab vastuväite isikuandmete töötlemise suhtes GDPR artikli 21 lõike 1 või 2 kohaselt;
- isikuandmeid on töödeldud ebaseaduslikult;
- isikuandmed peab kustutama selleks, et täita vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega ette nähtud juriidilist kohustust;
- isikuandmeid koguti seoses lapsele osutatud infoühiskonna teenuste pakkumisega (GDPR artikkel 8(1)).

Kui ettevõte on jaganud isikuandmeid mõne muu isikuga (nt volitatud töötlejaga, nagu palgaarvestuse teenuse osutaja), peab ettevõte teavitama ka seda isikut inimese andmete kustutamisest.

Ettevõte võib keelduda isikuandmete kustutamisest, kui isikuandmeid töötlemine on vajalik:

- sõna- ja teabevabaduse õiguse teostamiseks;
- selleks, et täita ettevõtte juriidilist kohustust, mis näeb ette isikuandmete töötlemise, või täita avalikes huvides olevat ülesannet;
- rahvatervise valdkonnas avaliku huviga seotud põhjustel;
- avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil;
- õigusnõuete koostamiseks, esitamiseks või kaitsmiseks.

C. Piiramise õigus

Inimesel on ka õigus nõuda ka, et ettevõte piiraks tema isikuandmete töötlemist järgmistel juhtudel:

- kui andmesubjekt vaidlustab oma isikuandmete õigsuse, siis ajaks, mis võimaldab ettevõttel isikuandmete õigsust kontrollida;
- kui isikuandmete töötlemine on ebaseaduslik, kuid andmesubjekt ei taotle isikuandmete kustutamist, vaid kasutamise piiramist;
- vastutav töötleja ei vaja isikuandmeid enam töötlemise eesmärkidel, kuid need on andmesubjektile vajalikud õigusnõuete koostamiseks, esitamiseks või kaitsmiseks,

- kui andmesubjekt on esitanud isikuandmete töötlemise suhtes GDPR artikli 21 lõike 1 kohaselt vastuväite, siis ajaks, kuni kontrollitakse, kas ettevõtte õiguspärased põhjused kaaluvad üles andmesubjekti põhjused.

Isikuandmete töötlemise piiramise meetodid võivad muu hulgas hõlmata valitud isikuandmete ajutist ümberpaigutamist teise töötlemissüsteemi, valitud isikuandmete muutmist kasutajatele kättesaamatuks või avaldatud andmete ajutist kõrvaldamist veebisaidilt. Automaatsetes andmete kogumites tuleks isikuandmete töötlemise piiramine tagada üldjuhul tehniliste vahenditega selliselt, et isikuandmeid enam edasi ei töödelda ja neid ei saa enam muuta. Asjaolu, et isikuandmete töötlemine on piiratud, tuleks süsteemis selgelt määratleda.

Kui töötlemine on piiratud, on ettevõttel lubatud isikuandmeid säilitada, kuid mitte neid muul viisil edasi töödelda, enne kui asi on lahendatud. Erandiks edasitöötlemise keelule on andmesubjekti nõusolek, õigusnõuete koostamise/esitamise/kaitsmise vajadus või teiste juriidiliste või füüsiliste isikute õiguste kaitsmine.

Kui ettevõte on jaganud isikuandmeid mõne kolmanda isikuga (nt volitatud töötlejaga, nagu palgaarvestuse teenuse osutaja), peab ettevõte teavitama seda kolmandat isikut vastava inimese andmete töötlemisele kehtestatud piirangutest edasise teatamiseni.

Piirangu eemaldamisest tuleb teavitada andmesubjekti ja samuti eelpool nimetatud kolmandat isikut.

D. Vastuväidete esitamise õigus

Konkreetsest olukorrast lähtuvalt on inimesel õigus esitada vastuväiteid sellisele andmete töötlemisele, mille aluseks on avalik huvi või andmetöötleja õigustatud huvi. Vastuväite esitamisel peab ettevõte lõpetama selle isiku isikuandmete töötlemise, v.a juhul kui tal on võimalik tõendada, et andmeid töödeldakse mõjuval õiguspärasel põhjusel (see otsustatakse juhtumipõhiselt).

GDPRi nõuete kohaselt tuleb Inimesi teavitada vastuväidete esitamise õigusest esmasel ühenduse võtmisel ja privaatsusteates. Sellele õigusele peab juhtima sõnaselgelt isiku tähelepanu ning see teave peab olema esitatud selgelt ja eraldiseisvalt muust informatsioonist.

Kui ettevõte töötleb andmeid otseturunduse eesmärgil, siis võib vastuväite esitada ka igasuguse põhjenduseta ja igal ajal. Otseturunduse eesmärgil andmete töötlemine tuleb lõpetada koheselt vastava vastuväite saamisel. Keeldumiseks ei näe GDPR ette erandeid ega õiguslikke aluseid.

E. Automatiseeritud otsused

GDPR reguleerib:
- automatiseeritud otsustamist – so otsuse langetamine puhtalt automatiseeritult, ilma inimsekkumiseta; ja
- profiilianalüüsi – so igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud asjaomase füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega. Profiilianalüüs on sageli osa automatiseeritud otsustamisest.

Andmesubjektil on õigus, et tema kohta ei tehtaks otsust, mis põhineb üksnes automatiseeritud töötlusel, sealhulgas profiilianalüüsil, mis toob kaasa teda puudutavaid õiguslikke tagajärgi või avaldab talle märkimisväärset mõju.

Eeltoodut ei kohaldata, kui automatiseeritud otsus: a) on vajalik andmesubjekti ja vastutava töötleja vahelise lepingu sõlmimiseks või täitmiseks; b) on lubatud vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega, milles on sätestatud ka asjakohased meetmed andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks, või c) põhineb andmesubjekti selgesõnalisel nõusolekul.

F. Andmete ülekandmise õigus

Isikuandmete ülekandmise õigus kohaldub ainult:

- isikuandmetele, mille inimene on ise vastutavale töötlejale andnud;
- juhul, kui andmetöötluse õiguslikuks aluseks on andmesubjekti nõusolek või ettevõttega sõlmitud lepingu täitmise vajadus; ja
- juhul, kui andmetöötlus toimub automatiseeritult.

Kui isik esitab andmete ülekandmise taotluse ja ülaltoodud tingimused on täidetud, peab ettevõte inimesele andmed edastama struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul. Masinloetav tähendab seda, et informatsioon on struktureeritud selliselt, et tarkvaral on võimalik eraldada spetsiifilised andmeelemendid ning see võimaldab teistel ettevõtetel andmeid kasutada. Informatsioon tuleb esitada tasuta.

Kui andmesubjekt seda nõuab ja kui see on tehniliselt teostatav, peab ettevõte olema valmis edastama andmeid otse teisele vastutavale töötlejale (nt ettevõttega sarnase teenuse pakkujale), kui see on tehniliselt teostatav. See ei tähenda siiski seda, et ettevõte peaks kasutusele võtma töötlussüsteemid, mis tehniliselt ühilduvad teiste ettevõtetega.

Kui isikuandmed puudutavad rohkem kui ühte inimest, tuleb hinnata, kas andmete ülekandmine seaks ohtu teiste isikute õigused. Samuti peab hindama, kas andmete ülekandmine võib kahjustada ettevõtte enda huvisid ja õigusi, nt oht avaldada äri- ja tootmissaladusi). Andmete ülekandmisega ei tohi teiste isikute õigusi ja vabadusi kahjustada.

2. ANDMESUBJEKTI TAOTLUSTE HALDAMINE

A. Taotlusele vastamine

Ettevõte peab suhtlema taotluse esitanud inimese ja muu osapoolega, kellega isikuandmeid on jagatud, kui muutmine, kustutamine või piiramine on läbi viidud.

Inimestele nende taotluse vastusena saadetav teave või suhtlus peab olema:

- konkreetne, selge, hõlpsasti mõistetav ja hõlpsasti kättesaadavas vormingus ning arusaadavas sõnastuses;
- kirjalik (nt kirja või meili teel); ja
- kui inimene esitab taotluse elektrooniliselt (nt meili teel), peab ka vastuse edastama võimaluse korral elektrooniliselt, kui inimene teisiti ei soovi.

B. Taotlusele vastamise tähtaeg

Pärast nõuetekohase taotluse kättesaamist tuleb vastus saata põhjendamatu viivituseta, kuid igal juhul mitte hiljem kui 1 kuu pärast taotluse saamist. Seda ühe kuu pikkust perioodi võib pikendada vajaduse korral veel kahe kuu võrra, arvestades esitatud taotluste keerukust ja arvu. Ettevõte peab teavitama inimest tähtaja pikendamisest esimese kuu jooksul arvates taotluse saamisest, lisades viivituse/pikendamise põhjused.

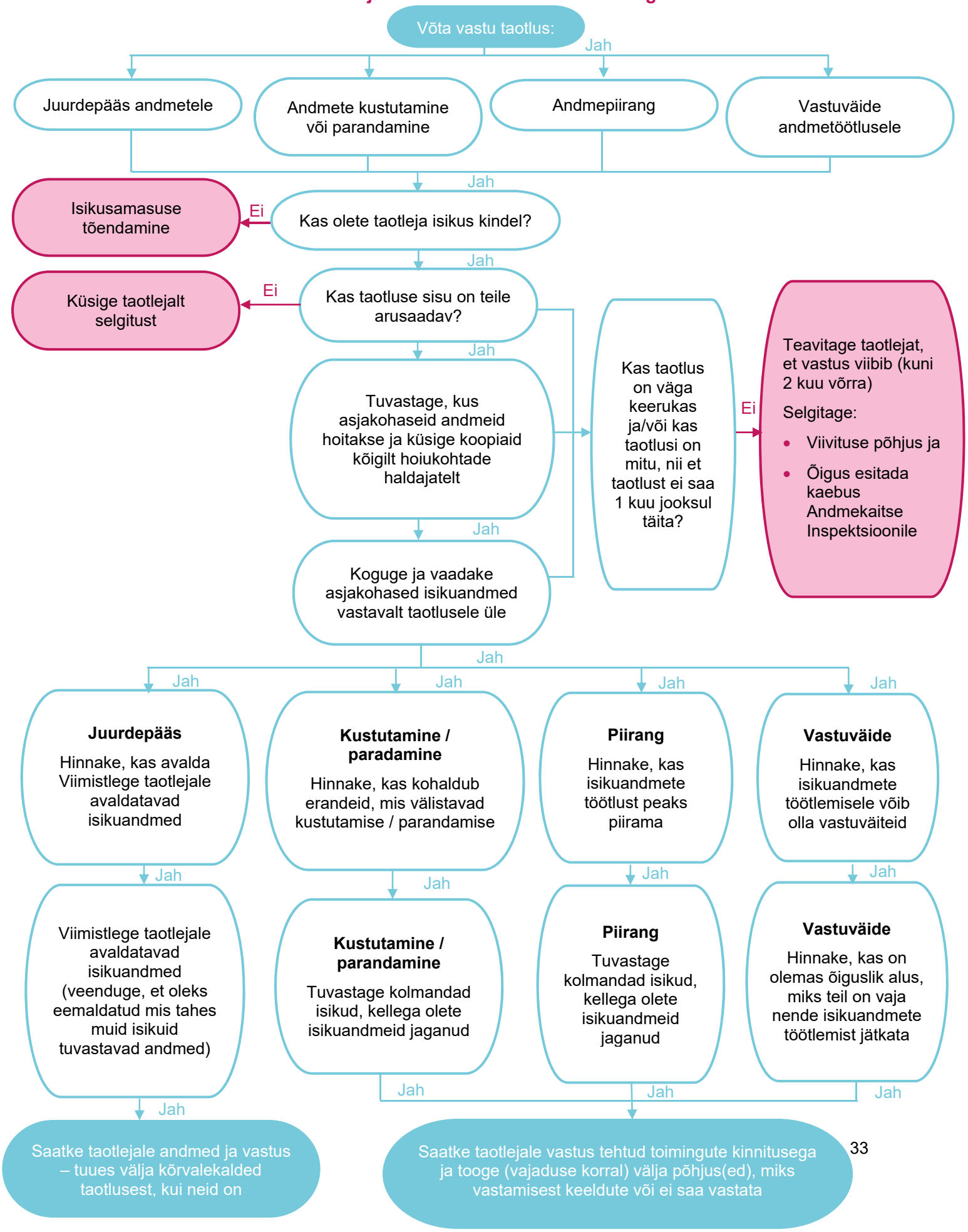
Kui ettevõttel on mõjuv ja seaduslik põhjus taotlusele ettenähtud aja jooksul või üldse mitte vastata, peab ettevõte: a) teavitama inimest viivituseta põhjustest, miks ta midagi ei tee, kuid igal juhul hiljemalt 1 kuu pärast taotluse saamist, ja b) teavitama inimest tema õigusest esitada kaebus vastavale andmekaitseasutusele.

C. Taotlusele vastamise kulud

Igasugune ettevõtte poolt antav teave/suhtlus seoses andmesubjekti poolt esitatud taotlusega peab olema tasuta, v.a juhul, kui inimese taotlus on selgelt põhjendamatu või liialdatud (näiteks korduvate taotluste korral), millisel juhul ettevõte võib: a) võtta inimeselt mõistlikku tasu või b) keelduda taotlusest.

LISA 1

Andmesubjekti taotluste haldamise voodiagramm



ANDMEKAITSE STANDARDKLAUSLID[1]

1. See andmekaitset reguleeriv lisa (edaspidi **lisa**) on lisa [lepingu nimi] lepingule [*ettevõtte nimi*] **(**edaspidi **ettevõte**) ja [*ettevõtte nimel isikuandmeid töötleva isiku nimi*] (edaspidi **teenuse osutaja**) vahel kuupäevaga [*lepingu kuupäev*] (edaspidi **leping**).

Kui selle lisa ja lepingu vahel on vastuolusid kehtivad selle lisa sätted. Selguse huvides, selles lisas hõlmab viide lepingule ka seda lisa ennast.

Ettevõte ja teenuse osutaja lepivad kokku järgmises:

2. Definitsioonid

Andmekaitsejuhtum – turberikkumine, mille tagajärg on edastatavate, säilitatavate või muul viisil töödeldavate isikuandmete tahtmatu või ebaseaduslik hävimine, kaotsiminek, muutmine, omavoliline avaldamine või juurdepääs neile andmetele.

Andmekaitseseadused – tähendab järgmisi õigusakte:
2.1 ELi andmekaitsedirektiiv 95/46/EÜ;
2.2 ELi e-privaatsuse direktiiv 2002/58/EÜ (**e-privaatsuse direktiiv**);
2.3. ülalnimetatud õigusaktide mis tahes järglas- või asendusakte, muu hulgas selle jõustumisel isikuandmete kaitse üldmäärust (määrus (EL) 2016/679) (**GDPR**) ja e-privaatsuse direktiivi järglasdokumenti ning kõiki muid kohalduvaid isikuandmete töötlemist reguleerivad seaduseid, määruseid ja käitumiskoodeksid (arvestades neisse aeg-ajalt tehtavate muudatustega).

EMP – Euroopa majanduspiirkond (hetkel kehtiva regulatsiooni kohaselt kuuluvad EMPsse kõik Euroopa Liidu liikmesriigid ning Norra, Island ja Liechtenstein).

Lepinguga hõlmatud isikuandmed – on kõik isikuandmed, mida ettevõte edastab teenuse osutajale seoses lepingu ja/või teenustega või mida teenuse osutaja ettevõtte jaoks või nimel seoses lepingu ja/või teenustega saab, kogub, loob või muul viisil töötleb.

---

[1] Kõik selles dokumendis sisalduvad joonealused märkused on selgitused ettevõttele ja tuleb koos tekstisiseste viidetega enne lepingus või selle lisas kasutamist kustutada.
Andmetöötluse lisa eesmärgid ja roll: *järgmised andmekaitsealase kokkuleppe punktid tuleks lisada maksimaalses võimalikus ulatuses kõigisse isikuandmete töötlemist puudutavatesse lepingutesse. Siin toodud lepingupunte võib kasutada, 1) lisades need andmekaitse kokkuleppena kõigisse uutesse lepingutesse, mida parajasti koostatakse/arutatakse; ja 2) need võib lisada olemasolevatele lepingutele muudatuse kaudu, st pooled lepivad kokku, et andmekaitset reguleerivast lisast saab olemasoleva lepingu osa. Lisajuhised on antud allpool.*
Vastutavale töötlejale soodne: *see andmekaitse lisa / need andmekaitse klauslid on koostatud vastutavale töötlejale (st teie ettevõttele) soodsal viisil. Soovitame kasutada neid klausleid kõikidel juhtudel, kus ettevõte tegutseb vastutava töötlejana.*
Kasutamine lisana*. Seda dokumenti võib kasutada (olemasoleva või uue) lepingu lisana, mis sisaldab GDPRis nõutud sätteid ettevõtte poolt teenuse osutaja kaasamiseks.*
Kasutamine punktidena*. Selle dokumendi sisu võib kasutada lepingu põhiosasse lisatavate punktidena. Kui soovite kasutada seda dokumenti andmekaitse punktidena ja integreerida selle sisu olemasolevasse lepingusse, tuleb punkt 2 lisada lepingu jaotisse „Mõisted" ja punkti 3 võib lisada uue punktina lepingu põhiosasse. 1. punkti võib välja jätta.*
Muud asjad, mida tähele panna. *Lepingupunktid, mis võib olla vaja üle vaadata, on järgmised:*
• Mõiste „kahju" definitsioon: vastutav töötleja/teie ettevõte peaks kaaluma „andmekadu" ja muude sarnaste kahjude lisamist korvatavate kahjude hulka, nii et teenuse osutaja vastutaks sellise kahju eest (et see ei jääks teenuse osutaja vastutuse ulatusest välja) ja
• Vastutus: ettevõtte ja teenuse osutaja vahel peab risk olema sobival viisil jagatud, arvestades võimalikke trahve, mida GDPRi alusel võidakse rakendada.

Teenused – on [*teenuste loetelu*].[2]

3. Andmetöötlus

3.1 Selles punktis 3 on mõistetel **andmesubjekt** ja **töötlemine** andmekaitseseaduses kasutatav tähendus ning ettevõte on käsitletav **vastutava töötlejana** ja teenuse osutaja **volitatud töötlejana** andmekaitseseaduse tähenduses.

3.2 Lepinguga hõlmatud isikuandmete töötlemisel teenuse osutaja või teenuse osutaja töötajate ja/või alltöövõtjate poolt lepingu alusel või sellega seoses, kohustub teenuse osutaja (ja kohustub tagama, et teenuse osutaja töötajad ja/või alltöövõtjad teeks sama):

(a) töötlema lepinguga hõlmatud isikuandmeid ainult sellises ulatuses, mis on vajalik teenuste osutamiseks lepingu tingimuste kohaselt või muul viisil ettevõtte dokumenteeritud juhiste kohaselt;

(b) mitte muutma lepinguga hõlmatud isikuandmete sisu ega avaldama või lubama avaldada lepinguga hõlmatud isikuandmeid ühelegi muule osapoolele (sh alltöövõtjale), v.a juhul, kui ettevõte on selleks konkreetse kirjaliku nõusoleku andnud;

(c) rakendama sobivaid tehnilisi ja organisatsioonilisi meetmeid, muuhulgas GDPR artiklis 32(1) nimetatuid (kui see on asjakohane), et:
   (i) kaitsta lepinguga hõlmatud isikuandmeid loata või ebaseadusliku töötlemise ja juhusliku või ebaseadusliku kaotsimineku, hävimise, kahjustumise, muutmise või avaldamise eest,
   (ii) tagada andmekaitseseaduste järgimine; ja
   (iii) tagada andmesubjekti õiguste kaitse.

   Eelkõige tuleb rakendada juurdepääsukontrolli, lepinguga hõlmatud isikuandmete mis tahes allalaadimine kaasaskantavasse seadmesse või andmekandjale või elektrooniline edastamine peab olema krüpteeritud.

(d) tagama, et lepinguga hõlmatud isikuandmetele on juurdepääs üksnes teenuse osutaja töötajatel, kes vajavad juurdepääsu neile andmetele oma tööülesannete täitmiseks, ning neil töötajatel on asjaomaste andmete töötlemiseks sobiv väljaõpe;

(e) veenduma, et kõik teenuse osutaja töötajad, kes teenuste osutamisega seotud on, oleksid sõlminud teenuse osutajaga konfidentsiaalsuslepingu ja tagama lisaks, et sellised töötajad teaksid ja järgiksid teenuse osutaja kohustusi selle lepingu alusel seoses isikuandmete turbe ja kaitsega*;*

(f) töötlema lepinguga hõlmatud isikuandmeid kooskõlas kohalduvate andmekaitseseadustega ja mitte lubama ühtegi tegevust, mis võiks tekitada mingil viisil olukorra, kus ettevõte rikuks andmekaitseseadusi;

(g) esitama kirjalikke tõendeid selle kohta, et teenuse osutaja järgib andmekaitseseadusi, kui ettevõte seda nõuab;

(h) tegema koostööd ja osutama abi, mida ettevõte soovib, ning kehtestama sobivad tehnilised ja organisatsioonilised meetmed, mis võimaldaksid ettevõttel täita andmesubjekti taotlusi andmesubjektile andmekaitseseaduste alusel kuuluvate õiguste

[2] Täitke vastavalt sellele, milliseid teenuseid lepingu alusel osutatakse või vastavalt seal toodud definitsioonile. Pange tähele, et teenuse kirjeldus peab sisaldama järgmist: töötlemise teema ja kestus, töötlemise iseloom ja eesmärk, isikuandmete liik ja seotud andmesubjektide kategooriad.

kasutamisel (muu hulgas seoses andmesubjekti isikuandmete väljavõtte saamise ja/või kustutamisega);

(i) mitte töötlema lepinguga hõlmatud isikuandmeid väljaspool EMPi ilma ettevõtte eelneva kirjaliku nõusolekuta (ja kui andmeid edastatakse väljapoole EMPi, siis sõlmides mis tahes dokumendi või lepingu, mis on ettevõtte mõistliku hinnangu kohaselt lepinguga hõlmatud isikuandmete selliseks edastamiseks vajalik, et tagada lepinguga hõlmatud isikuandmete kaitse);

(j) [ettevõtte või pädeva reguleeriva või järelevalveasutuse soovil võimaldama auditeerida teenuse osutaja poolt lepingu alusel tehtavaid töötlemistoiminguid (ja seotud vahendeid); auditi viivad läbi ettevõte, tema volitatud esindajad (keda seob konfidentsiaalsuskohustus) ja/või asjakohase reguleeriva või järelevalveasutuse esindajad][3].

3.3 Teenuse osutaja teavitab ettevõtet niipea kui see on mõistlikult võimalik, ja igal juhul kahekümne nelja (24) tunni jooksul järgmisest:

(a) ettevõtte poolt lepinguga hõlmatud isikuandmete töötlusemiseks antud instruktsioon rikub teenuse osutaja hinnangul andmekaitseseaduse sätteid;

(b) mis tahes õiguskaitseorgani või muu pädeva asutuse esitatud juriidiliselt siduvast lepinguga hõlmatud isikuandmete avaldamise nõudest, kui ettevõtte teavitamine pole seadusega keelatud;

(c) mis tahes otse andmesubjektilt saadud nõudest, ise sellisele nõudele vastamata, v.a juhul, kui see on seadusega nõutav või kui ettevõte on lubanud teenuse osutajal seda teha;

(d) vastavalt andmekaitseasutuselt või muult reguleerivalt asutuselt või isikult mis tahes lepinguga hõlmatud isikuandmetega seotud kirjavahetuse, teatise või muu teabe saamisest suuliselt või kirjalikult ja/või

(e) selle punkti 3 rikkumisest teadasaamisest.

3.4 Olenemata muudest käesoleva lepingu sätetest võib ettevõte mõistliku etteteatamisega nõuda teenuse osutajalt üksikasjalikku kirjalikku kirjeldust järgmise kohta: i) teenuse osutaja ja tema alltöövtjate (kui neid on) poolt kasutatavad tehnilised ja organisatsioonilised meetmed lepinguga hõlmatud isikuandmete töötlemiseks ja/või ii) töötlemistoimingud, mida teenuse osutaja ettevõtte nimel teostab, sisaldades vähemalt niisugusel hulgal infot, nagu nõuab GDPRi artikkel 30(2). Kümne (10) päeva jooksul pärast seda, kui teenuse osutaja on saanud kätte ettevõtte kirjaliku taotluse (mis sisaldab ettevõtte nõudmiste üksikasjalikku kirjeldust), edastab teenuse osutaja ettevõttele kirjaliku aruande, mille põhjal peab olema võimalik mõistlikult järeldada, kas vastavaid lepinguga hõlmatud isikuandmeid on töödeldud andmekaitseseaduste ja lepinguga kooskõlas.

---

[3] Töötlejad on tõenäoliselt selle punkti lisamise vastu. Selles kontekstis pange tähele, et GDPR paneb vastutavale töötlejatele ehk teie ettevõttele järgmised kohustused:
• *vastutavad ja teenuse osutajad peavad nõudmisel tegema järelevalveasutusega koostööd (punkt 31) ja*

• *teenuse osutajad peavad tegema vastutavale töötlejale kättesaadavaks kogu teabe, mis on vajalik punktis 28 nimetatud kohustuste täitmise demonstreerimiseks, ja lubama viia läbi auditi ning osalema selles, sh vaatlused, mida viib läbi vastutav töötleja või vastutava töötleja määratud teine audiitor (punkt 28(3)).*

Lepingu punkt 3.2(i) kajastab neid kohustusi (vastutava töötleja kasuks).

3.5 Olenemata teistest selle punkti 3 sätetest, kui teenuse osutaja või mõni teenuse osutaja töötaja või alltöövõtja saab teada mõnest andmekaitsejuhtumist, kohustub teenuse osutaja kohe (kuid igal juhul kahekümne nelja (24) tunni jooksul teadasaamisest) teavitama ettevõtet telefoni ja e-posti teel. E-posti teel edastatav teade peab võimaluse korral sisaldama andmekaitsejuhtumiga hõlmatud andmeliikide kirjeldust, andmesubjektide arvu ja ettevõtte andmekirjete ligikaudset arvu, ülevaadet andmekaitsejuhtumi võimalikust mõjust ja tagajärgedest ettevõttele ning teenuse osutaja poolt ette võetavatest parandusmeetmetest. Kui teenuse osutaja nimetatud teavet 24 tunni jooksul ei esita, peab ta viivitust ettevõttele põhjendama.

3.6 Teenuse osutaja kohustub ilma igasuguse lisakuluta ettevõttele (kuivõrd andmekaitsejuhtum oli seotud käesolevast punktist 3 tulenevate teenuse osutaja kohustuste rikkumisega) tagama kõik ressursid, abi ja koostöö, mida ettevõte vajab, et: (i) teavitada asjakohast andmekaitseasutust andmekaitsejuhtumist, (ii) edastada teavet, mida võidakse sellise andmekaitsejuhtumi kohta nõuda ja/või (iii) teavitada vastavaid andmesubjekte sellisest andmekaitsejuhtumist vajalikul viisil.

3.7 Teenuse osutaja võtab viivitamata ja oma kulul (kuivõrd andmekaitsejuhtum oli seotud käesolevast punktist 3 tulenevate teenuse osutaja kohustuste rikkumisega) kõik andmekaitsejuhtum põhjuste kõrvaldamiseks vajalikud meetmed ning peab eelnevalt ettevõttega heas usus nõu, millised parandusmeetmed võivad olla vajalikud ja teeb ettevõttega mõistlikku koostööd seoses kõikide ettevõtte poolsete parandusmeetmetega.

3.8 Teenuse osutaja kohustub ilma igasuguse lisakuluta ettevõttele tagama kõik ressursid, abi ja koostöö, mida ettevõte soovib, et ettevõte saaks täita oma GDPRi artiklitest 35 ja 36[4] tulenevad kohustused, muu hulgas esitades ettevõtte nõudmisel viivitamatult teavet mis tahes andmekaitse mõju hindamise kohta, mida ettevõtte läbi viib.

3.9 Kui teenuse osutaja kasutab ettevõtte nimel teatud lepinguga hõlmatud isikuandmete töötlustoimingute tegemiseks ettevõtte nõusolekul alltöövõtjat, teeb ta seda üksnes alltöövõtjaga sõlmitud kirjaliku lepingu alusel, millega alltöövõtja kohustub lepinguga hõlmatud isikuandmete töötlemisel järgima vähemalt käesolevas punktis 3 sätestatud tingimustega samaväärseid andmekaitsetingimusi ning teenuse osutaja kohustub ettevõtte nõudmisel esitama koopia või kokkuvõtte nimetatud tingimustest. Igal juhul jääb teenuse osutaja ettevõtte ees täielikult vastutavaks oma esindajate, töötajate ja alltöövõtjate tegevuse või tegevusetuse eest.

3.10 Pärast konkreetse teenuse osutamise lõppu või ettevõttelt vastava kirjaliku nõude saamisel lõpetab teenuse osutaja kõik lepinguga hõlmatud isikuandmetega seonduvad toimingud ning tagastab vastavalt ettevõtte juhistele ja poolte vahel kokku lepitud vormis ja/või kustutab taastamatult kõik lepinguga hõlmatud isikuandmed, mida teenuse osutaja on lepingu alusel töödelnud, ning kohustab ka oma alltöövõtjaid seda tegema. Kui teenuse osutaja riigi õigusaktid või kohalik reguleeriv asutus piiravad lepinguga hõlmatud isikuandmete hävitamist või tagastamist, hoiab teenuse osutaja lepinguga hõlmatud isikuandmeid konfidentsiaalsetena ega töötle neid mis tahes muul eesmärgil.

3.11 Kui eeltoodust ei tulene teisiti, tagastab ja/või kustutab teenuse osutaja lepinguga hõlmatud isikuandmed 60 päeva jooksul alates lepingu lõppemisest või lõpetamisest

[4] *Selgituseks: GDPRi artiklid 35 ja 36 sätestavad järgmise:*
Art. 35 (Andmekaitse mõju hindamine) sätestab andmekaitse mõju hindamise kohustuse teatud olukordades.
Art. 36 (Eelnev teavitamine) sätestab eelneva nõu pidamise kohustuse andmekaitseasutusega seoses teatud andmekaitsealaste mõjuhindamistega.

3.12 Käesolevas punktis 3 kokkulepitu kehtib tähtajatult kuni kokkuleppe lõpetamiseni poolte volitatud esindajate poolt.

3.13 Teenuse osutaja vabastab ettevõtte vastutusest ning vastutab ettevõtte ning tema töötajate, esindajate ja temaga seotud isikute asemel mis tahes kulutuste, kohustuste ja nõuete eest, mis esitatakse ettevõttele ja/või temaga seotud isikute vastu seoses teenuse osutaja, tema töötajate või alltöövõtjate rikkumiste, hooletuse, vigade, eksimuste või tegevusetusega käesoleva punkti 3 täitmisel.

ISIKUANDMETE REGISTER

Mis on isikuandmete register?

See on tsentraalne register kõigi isikuandmete kogumite kohta, mis on ettevõtte valduses, nt töötajate, klientide ja koostööpartnerite, alltöövõtjate, külaliste jne kohta, mis on nende inimeste põhised ja mida saab kasutada nende otseseks või kaudseks tuvastamiseks. Isikuandmed võivad olla elektroonilises või füüsilises (nt paberkujul) vormis. Neid võidakse hoida ettevõttes või teiste, ettevõtteväliste isikute juures (nt arhiivi teenuse osutaja juures).

Ettevõttes säilitatavad isikuandmed võivad muu hulgas olla tööle kandideerimise avaldused, külaliste logid, CCTV materjal, soodustuste platvormid, palgaarvestuse süsteemid, kulude süsteemid, kliendihalduse süsteemid, skanneeritud dokumentide hoidla, asukoha jälgimise andmed või failikapid.

Miks see vajalik on?

GDPRi üks läbivaid eesmärke on andmetöötleja vastutustundlikkus. See tähendab, et andmetöötlejad peavad olema võimelised aru saama kogu andmetöötlusahelast, tagades inimeste suhtes seadusliku, õiglase ning läbipaistva andmetöötlusprotsessi. Selle nõude täitmist aitab tagada see, kui andmetöötleja dokumenteerib ja säilitab informatsiooni tema vastutusalasse kuuluvate isikuandmete töötlemise toimingute kohta.

Andmetöötlustoimingute registreerimine on GDPRi uus nõue ja see aitab andmetöötlejatel paremini mõista isikuandmete kaitse olemust, kaardistada oma tegevusi ning paremini planeerida isikuandmete kaitsega seonduvat.

Isikuandmete registri abil on võimalik näidata, et ettevõte on andmete töötlemise viisi ja põhjuse seisukohast vastutustundlik ning läbipaistev. Samuti aitab registri pidamine ettevõttel välja selgitada, milliseid andmeturbemeetmeid on vaja, andmesubjekti õigustega seotud taotluste täitmiseks ja tuvastada, milliste ettevõtteväliste andmetöötlejate lepingute puhul on vaja kohaldada andmekaitse standardtingimusi.

Isikuandmete registri mall

Selle tööriistakasti juurde kuulub isikuandmete registri mall, mis on Excel formaadis tabel. Isikuandmete registri mall sisaldab võrreldes GDPRi nõuetega pisut rohkem andmeväljasid, kuid aitab seeläbi anda ettevõttele endale parema arusaama isikuandmete töötlemisest ning on heaks abivahendiks nõuetele vastavuse tõendamisel.

Kuidas isikuandmete registrit kasutada?

- Vaadake üle ettevõtte isikuandmete registri mall ja määrake vastutusalad selle täitmiseks ning haldamiseks.
- Analüüsige ettevõtte olemasolevaid protsesse ja nende tulemusena hoitavaid isikuandmeid.
- Iga välja täitmise kohta leiate juhised isikuandmete registri mallist.

- Kui teatud registri lahtrid ei ole ettevõtte suurust või spetsiifikat silmas pidades asjakohased jätke need tühjaks.

- Mõelge isikuandmetele, mida hoitakse või edastatakse väljaspoole ettevõtet (nt pilve kaudu) ja lisage need registri teisele vahekaardile.

- Kaasake registri täitmisse personali-, kliendi-, IT- ja hankeosakonnad/meeskonnad.

- Veenduge, et ettevõtte isikuandmete registrit ajakohastataks regulaarselt (sh täiendage vajadusel malli ennast, nt uute väljade lisamisega, kui see on ettevõtte tegevusest lähtuvalt vajalik)

Lisa 1

GDPR – isikuandmete töötlemise põhimõtted

Vastutav töötleja peab tagama, et isikuandmete töötlemine vastaks kõigile kuuele töötlemise põhimõttele ning peab olema võimeline nende põhimõtete täitmist tõendama:

1. Seaduslikkus, õiglus ja läbipaistvus – isikuandmeid tuleb töödelda seaduslikult, õiglaselt ja andmesubjektile läbipaistvalt.

2. Eesmärgi piirang – isikuandmeid töödeldakse kindlaksmääratud, selgel ja õiguspärasel eesmärgil ning neid ei tohi hiljem töödelda viisil, mis on esialgselt määratud eesmärkidega vastuolus (v.a avalikkuse huvi korral, teaduslikul, ajaloolisel või statistilisel eesmärgil).

3. Võimalult väheste andmete kogumine – isikuandmed peavad olema asjakohased, olulised ja piiratud sellega, mis on nende töötlemise eesmärgist lähtuvalt vajalik.

4. *Õigsus* – isikuandmed peavad olema õiged ja vajaduse korral ajakohastatud. Ebaõiged isikuandmed tuleks parandada või kustutada.

5. *Säilitamise piirang* – isikuandmeid ei tohi hoida identifitseeritaval kujul kauem, kui vajalik (v.a avalikkuse huvi, teadusliku, ajaloolise või statistilise eesmärgi korral).

6. *Usaldusväärsus ja turvalisus* – isikuandmeid tuleb töödelda selliselt, et oleks tagatud nende asjakohane turvalisus.

GDPR´i alusel on andmesubjektil 7 põhiõigust:

1. Õigus andmetega tutvuda ehk juurdepääsuõigus – inimesel on õigus teada, milliseid andmeid nende kohta säilitatakse ja kuidas neid töödeldakse.

2. Õigus andmete parandamisele – inimesel on õigus nõuda isikuandmete parandamist, kui need on ebatäpsed või mittetäielikud.

3. Õigus andmete kustutamisele („õigus olla unustatud“) – inimese õigus nõuda oma isikuandmed teatud juhtudel (nt neid ei ole enam vaja, andmesubjekt võtab nõusoleku tagasi, jne) kustutada.

4. Õigus töötlemise piiramisele – inimese õigus teatud juhtudel keelata või takistada oma isikuandmete töötlemist teatud ajaks.

5. Andmete ülekandmise õigus – inimese õigus nõuda enda poolt vastutavale töötlejale edastatud andmete ülekandmist endale või teisele vastutavale töötlejale masinloetaval kujul (kehtib ainult siis, kui andmetöötluse aluseks on inimese nõusolek või vastutava töötlejaga sõlmitud leping).

6. Õigus esitada vastuväiteid – konkreetsest olukorrast lähtuvalt on inimesel õigus esitada vastuväiteid sellisele andmete töötlemisele, mille aluseks on avalik huvi või andmetöötleja õigustatud huvi. Otseturunduse eesmärgil töötlemise osas võib vastuväite esitada igal ajal.

7. Automaatse otsuste tegemine (sh profiilianalüüs) – inimesel on õigus nõuda, et otsust, mis toob kaasa teda puudutavaid õiguslikke tagajärgi, ei tehtaks üksnes automatiseeritud töötluse (sh profiilianalüüsi alusel).