EU: N TIETOSUOJA-ASETUS – OHJEITA VÄLITYSLIIKKEILLE

KÄSITTEITÄ:

Henkilötietoja ovat kaikki ne tiedot, joista voidaan suoraan tai epäsuorasti johtaa tunnistettavissa oleva luonnollinen henkilö. Henkilötietoja ovat käytännössä muun muassa henkilön nimi, valokuva, osoite, puhelinnumero, sähköposti, henkilötunnus, auton rekisterinumero, kiinteistön paikkatieto, IP-osoite jne.

Henkilötiedon käsittely voi olla mitä vain lähtien tietojen keräämisestä, tallettamisesta, järjestämisestä, käyttämisestä, siirtämisestä, luovuttamisesta, säilyttämisestä, muuttamisesta, yhdistämisestä ja suojaamisesta aina poistamiseen ja tuhoamiseen asti.

Rekisterinpitäjä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Välitysliike on käytännössä rekisterinpitäjä.

Rekisteröity tarkoittaa luonnollista henkilöä, jota tiedot koskevat. Rekisteröityjä ovat muun muassa välitysliikkeen asiakkaat ja työntekijät.

Tietojen käsittelijä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tietojen käsittelijä voi olla esimerkiksi yritys, joka tarjoaa palkkahallinnon palveluja tai IT-palvelujen toimittaja.

Rekisteröity tarkoittaa luonnollista henkilöä, jota tiedot koskevat. Rekisteröityjä ovat muun muassa välitysliikkeen asiakkaat ja työntekijät.

Tietojen käsittelijä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tietojen käsittelijä voi olla esimerkiksi yritys, joka tarjoaa palkkahallinnon palveluja tai IT-palvelujen toimittaja.

EU:n yleinen tietosuoja-asetus on jo astunut voimaan ja siirtymäaika päättyy 25.5.2018. Kun kyse on asetuksesta, tulee se sovellettavaksi kaikissa jäsenvaltioissa sellaisenaan. Asetusta tullaan täsmentämään uudella kansallisella tietosuojalailla. Lain on tarkoitus astua voimaan toukokuussa.

Tietosuoja-asetuksen piirissä ovat kaikki yritykset, jotka käsittelevät henkilötietoja eli käytännössä myös kaikki välitysliikkeet niiden koosta riippumatta. Jokaisella välitysliikkeellä on ainakin

toimeksiantopäiväkirja, välitysjärjestelmän rekisterit ja usein myös muita rekistereitä kuten markkinointirekisteri. Asetuksessa on paljon samoja asioita kuin nykyisessä henkilötietolaissa, mutta se sisältää myös monia uusia hankalasti tulkittavia ja sovellettavia velvollisuuksia ja oikeuksia. Sen vuoksi jokaisen välitysliikkeen pitää olla tietoinen uuden asetuksen sisällöstä sekä varmistua yrityksen käytäntöjen ja henkilötietojen käsittelyn asianmukaisuudesta.

> Sanktiot laiminlyönneistä ovat kovat, jopa 4% yrityksen liikevaihdosta tai 20 miljoonaa euroa sen mukaan, kumpi näistä määristä on suurempi. Koska sanktiot ovat hallinnollisia, viranomainen voi määrätä ne suoraan ilman tuomioistuinkäsittelyä.

Kentällä on ollut epätietoisuutta siitä, mitä toimia tietosuoja-asetus välitysliikkeiltä edellyttää. Vaadittavat toimet riippuvat henkilötietojen käsittelyn laajuudesta ja nykytilasta välitysliikkeessä, jonka vuoksi tyhjentävän to do-listan laatiminen on mahdotonta. Seuraavat kohdat kuitenkin ohjaavat välitysliikettä oikeaan suuntaan. Uuden tietosuojalain sekä soveltamiskäytännön myötä tulkinnat ja toimintatavat täsmentynevät ajan mittaan.

1. Vastuut ja roolit

Kaikki lähtee yrityksen johdon tietoisuudesta ja vastuullisuudesta – johdon on vietävä tietosuojaan liittyviä asioita aktiivisesti eteenpäin. Myös asenteen on oltava kohdillaan. Apua voi tarvittaessa pyytää ulkopuoliselta asiantuntijalta.

Aluksi on hyvä nimetä, kuka ottaa välitysliikkeessä käytännön tasolla vastuun tietosuojaan liittyvistä asioista. Hän voi olla esimerkiksi toimitusjohtaja tai vastaava hoitaja, mutta myös esimerkiksi välittäjä, sihteeri tai muu henkilö. Vastuullisen tehtävänä on huolehtia, että prosessit, tietosuojaselosteet yms. päivitetään sekä toimia yhteyshenkilönä johdon, asiakkaiden ja viranomaisten suuntaan. Välitysliikkeen on huolehdittava vastuullisen henkilön sekä koko henkilöstön kouluttamisesta.

Silloin kun liiketoiminnan keskeisenä osana on henkilötietojen laajamittainen ja säännöllinen seuranta, pitää yritykseen nimittää erikseen tietyt edellytykset täyttävä tietosuojavastaava. Välitysliikkeillä tällaista velvollisuutta ei todennäköisesti ole, koska edellä mainitun ei voida katsoa olevan niiden liiketoiminnan keskeinen osa.

2. Mitä henkilötietoja välitysliike käsittelee

Henkilötiedon käsite on laaja. Välitysliikkeen on hahmotettava ja kirjattava, mitä kaikkia henkilötietoja se käsittelee. Välitysliikkeet käsittelevät ainakin

- toimeksiantajien
- toimeksiantajien vastapuolten sekä
- työntekijöidensä henkilötietoja

On huomioitava, että toimeksiantoihin saattaa liittyä myös muiden kuin asiakkaiden henkilötietoja sisältäviä asiakirjoja (kuten vuokrasopimukset, perunkirjat jne.). Lisäksi välitysliike käsittelee usein

esimerkiksi esittelystä tai muuta kautta kerättyjä henkilötietoja markkinointia varten. Muista myös mahdolliset yhteistyökumppanit yms.

Henkilötietojen lähteitä taas voivat olla ainakin toimeksiantosopimukset, ostotarjoukset, yhteydenottolomakkeet nettisivuilla, esittelyt, erilaiset kilpailut ja hakuvahtia varten jätettävät yhteystiedot sekä työsopimukset ja työntekijältä itseltään tulevat tiedot.

3. Miksi henkilötietoja kerätään - henkilötietojen käsittelyn tarkoitus ja perusta

Kun käsiteltävien henkilötietojen joukko on hahmotettu, on niille määritettävä käsittelyn peruste. Lähtökohta on, että henkilötietojen käsittely on kiellettyä paitsi, jos käsittelylle on tietosuoja-asetuksen mukainen peruste. Nämä perusteet ovat:

- Rekisteröidyn suostumus
- Sopimuksen täytäntöön paneminen
- Lakisääteinen velvoite
- Elintärkeä etu
- Julkisen vallan käyttö ("yleinen etu")
- Oikeutettu etu

Asiakkaista ja muista henkilöistä saa siis kerätä vain sellaisia tietoja, jotka ovat välitysliikkeen toiminnan tai vastuiden kannalta tarpeen. Asiakassuhteen toteutuminen, mutta myös välityslainsäädäntö ja rahanpesulainsäädäntö edellyttävät, että välitysliike käsittelee asiakkaiden henkilötietoja. Esimerkiksi työntekijöiden henkilötietoja taas käsitellään työsopimussuhteen toteuttamiseksi.

Suostumuksen edellytykset ovat asetuksessa tiukentuneet ja välitysliikkeen kannattaa jatkossa arvioida kriittisesti, käyttääkö se suostumusta henkilötietojen käsittelyn perusteena. Todennäköistä on, että nykyisen lainsäädännön aikana kerättyjä suostumuksia ei kuitenkaan tarvitse uusia, kunhan ne on annettu asetuksen tarkoittamalla tavalla vapaaehtoisesti, yksilöidysti, tietoisesti ja yksiselitteisesti. Suostumusta ei voi esimerkiksi antaa valmiiksi rastitetulla ruudulla ja rekisteröidyllä on oltava oikeus peruuttaa se milloin tahansa. Lisäksi välitysliikkeen on pystyttävä osoittamaan, että suostumus on todella annettu.

4. Rekisterit ja tietoturva

Välitysliikkeen pitää myös tunnistaa edellä kerrottu huomioiden, mitä rekisterejä sillä on. Laki velvoittaa välitysliikkeitä pitämään toimeksiantopäiväkirjaa, johon merkitään mm. toimeksiantajan nimi ja osoite. Välitysliikkeellä voi olla myös erillinen rekisteri, johon tallennetaan tietoja ainakin ostotarjouksen tekijöistä. Näiden lisäksi markkinointia varten kerätyt henkilötiedot muodostavat rekisterin. Työntekijöitä varten on myös oma rekisterinsä. On huomioitava, että rekisterin muodolla ei ole merkitystä ja henkilötietojen joukko voi olla esimerkiksi tietokonejärjestelmässä, Excelissä, Wordissa tai paperilla.

Tarkista, että välitysliikkeessä käytettävät järjestelmät ja tietoturva ovat ajan tasalla sekä missä kaikkialla tietoja säilytetään (oma tietokone, pilvipalvelut, perinteinen paperiarkisto jne.). Välitysliikkeen rekistereissä saattaa olla sellaista dataa, jota siellä ei saisi olla. Siivoa kaikki tällaiset tiedot pois. Jos jonkin henkilön tietojen säilyttämiselle ei ole enää perusteita tai tiedolle määritetty säilytysaika on kulunut umpeen (kts. säilytysajoista jäljempänä), ne pitää hävittää. Rekisterien ajantasaisuuden varmistamiseksi ne kannattaa jatkossa tarkastaa määrävälein. Välitysliikkeen on syytä suunnitella, millä tavoin tiedot tarkastetaan ja miten usein tämä tehdään.

Jos välitysliikkeessä on useampia työntekijöitä, tulee miettiä, ketkä heistä käsittelevät henkilötietoja ja lisäksi, ketkä heistä saavat niitä käsitellä. Kaikki välitysliikkeen työntekijät eivät saa päästä tietoihin käsiksi automaattisesti. Oikeus pitää olla ainoastaan niillä, joilla on siihen tarve työnsä puolesta. Tietoa voidaan tarpeen mukaan rajata salasanoin, arkistojen lukituksella tai muulla tavoin.

5. Mihin henkilötietoja luovutetaan

Välitysliikkeen pitää tunnistaa, mihin eri suuntiin se luovuttaa henkilötietoja ja millä perusteella. Tällaisia tahoja voivat olla muun muassa valvova viranomainen, Verohallinto ja KVKL:n hintaseurantapalvelu kauppatietojen osalta. Lisäksi henkilötietojen käsittelyä on voitu ulkoistaa esimerkiksi palkka- ja taloushallintoon, IT-tukeen, pilvipalveluun, asiakaspalveluun ja KIVI/PDX:ään. Ulkoistamisesta huolimatta välitysliike kantaa aina viime kädessä vastuun henkilötietojen asianmukaisesta käsittelystä. Jos henkilötietojen käsittelyä on ulkoistettu, tulee ulkoistamissopimukset päivittää. Osapuolten on laadittava kirjallinen aukoton sopimus tietojen käsittelijän vastuista ja velvoitteista. Tietosuoja-asetus luettelee ne asiat, jotka sopimukseen tulee minimissään sisällyttää.

6. Rekisteröityjen oikeuksien toteuttaminen

Lähtökohtaisesti tietosuoja-asetuksen mukaiset rekisteröidyn oikeudet ovat pääosin samoja kuin nykylainsäädännössä, mutta niitä on vahvistettu. Näitä oikeuksia ovat:

- Oikeus saada tietoa
    - Välitysliikkeellä on informointivelvollisuus. Rekisteröidylle on annettava riittävästi informaatiota henkilötietojen käsittelystä siinä vaiheessa, kun henkilötiedot annetaan välitysliikkeelle eli esimerkiksi silloin kun sopimus tai tarjous tehdään. Informointi voidaan toteuttaa esimerkiksi antamalla rekisteröidylle tietosuojaseloste (kts. jäljempänä). Kun yhteystiedot jätetään internetsivuston kautta, voidaan oheen lisätä linkki tietosuojaselosteeseen. KVKL:n laki- ja lausuntovaliokunta tulee päivittämään mallilomakkeissaan olevia (toimeksiantosopimukset, ostotarjoukset ja esisopimus kiinteistön kaupasta) ehtoja tietosuoja-asetuksen perusteella. Jäsenistön on otettava malliehdot tai vastaavanlaiset ehdot käyttöönsä viimeistään toukokuussa.

- Oikeus saada pääsy tietoon
    - Jos rekisteröity tätä pyytää, pitää hänellä antaa tieto siitä, mitä kaikkia henkilötietoja hänestä on tallennettu välitysliikkeen rekistereihin. Pyyntöön on lähtökohtaisesti reagoitava kuukauden sisällä.
- Oikeus tiedon oikaisemiseen
    - Jos rekisteröidystä on tallennettu epätarkkaa tai virheellistä tietoa, on tällä oikeus pyynnöstä oikeus saada tieto oikaistuksi. Pyyntöön on lähtökohtaisesti reagoitava kuukauden sisällä.
- Oikeus tulla unohdetuksi
    - Rekisteröidyllä on oikeus pyytää hänen tietojaan poistettavaksi ilman aiheetonta viivytystä, paitsi jos on olemassa jokin laillinen peruste säilyttää ne. Muun muassa toimeksiantajien ja toimeksiantajien vastapuolten osalta tietoja ei voida pyynnöstä hävittää, koska välitysliikelaki ja rahanpesulaki velvoittavat säilyttämään tiedot tietyn ajan.
- Oikeus rajoittaa käsittelyä
    - Jos rekisteröity sitä pyytää, hänen tietojensa aktiivista käsittelyä on rajoitettava tietyissä tilanteissa. Henkilötietojen käsittelyn rajoittamista koskevia menetelmiä voivat olla esimerkiksi käyttäjien pääsyn estäminen valittuihin henkilötietoihin.
- Oikeus tiedon siirrettävyyteen ("data portability")
    - Jos henkilötietojen käsittely perustuu suostumukseen tai sopimukseen ja käsittelyä tehdään automaattisesti, rekisteröidyllä on oikeus saada välitysliikkeelle toimittamansa häntä koskevat henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle. Jos se on teknisesti mahdollista, rekisteröidyllä on oikeus saada tiedot siirrettyä suoraan rekisterinpitäjältä toiselle. Tämä oikeus tulee todennäköisesti harvemmin vastaan välitysliikkeessä.
- Oikeus vastustaa käsittelyä
    - Jos henkilötietojen käsittely perustuu rekisterinpitäjän tai kolmannen osapuolen oikeutetun edun toteuttamiseen, rekisteröidyllä on myös oikeus vastustaa häntä itseään koskevia tietojen käsittelyä tiettyyn tarkoitukseen kuten esimerkiksi suoramarkkinointiin.
- Automatisoituun päätöksentekoon ja profilointiin liittyvät oikeudet
    - Tämä oikeus tulee todennäköisesti harvemmin vastaan välitysliikkeessä, mutta voi tulla kyseeseen esim. asiakasdatan pohjalta personoidussa markkinoinnissa tai verkkopalvelussa.

Välitysliikkeen pitää selvittää, mitä rekisteröidyn oikeuksia käytössä oleviin käsittelyn perusteisiin liittyy ja miten rekisteröityjen oikeuksien toteuttaminen käytännössä toteutetaan.

7. Tietojen säilyttäminen

Uuden asetuksen lähtökohtana on, että välitysliike säilyttää mahdollisimman vähän henkilötietoja ja vain silloin, kun ne ovat tarpeellisia käsittelyn tarkoitusten kannalta. Tiedot on poistettava kokonaan, kun niiden säilyttämiselle ei ole enää perustetta. Välitysliikkeen pitää pystyä

perustelemaan miksi ja miten pitkään tiettyjä henkilötietoja säilytetään. Välitysliikkeiden on välitysliikelain edellyttämällä tavalla säilytettävä toimeksiantoon liittyviä asiakirjoja henkilötietoineen vähintään viisi vuotta. Vahingonkorvausvastuun ollessa tätä pidempi on tietoja perusteltua säilyttää pidempäänkin. Myös muuta tarkoitusta kuten pelkkää markkinointia varten kerätyille tiedoille pitää määrittää jokin perusteltu säilytysaika. Lisäksi on huomioitava, että muun muassa suoramarkkinointia varten kerätyt tiettyä henkilöä koskevat tiedot tulee lähtökohtaisesti poistaa heti, mikäli henkilö tätä pyytää.

8. Tietojen siirto EU/ETA-alueen ulkopuolelle

Nykylainsäädäntöä vastaavasti henkilötietoja voidaan siirtää EU/ETA:n ulkopuolelle ainoastaan, jos komissio on tehnyt päätöksen kyseisen maan tietosuojatason riittävyydestä taikka käytössä on asianmukaiset suojamekanismit, kuten komission hyväksymät mallisopimuslausekkeet. Lähtökohtaisesti välitysliikkeet eivät siirtäne tietoja EU/ETA-alueen ulkopuolelle. Sen vuoksi tähän teemaan ei perehdytä tässä kirjoituksessa sen tarkemmin.

On kuitenkin syytä varmistaa, missä yrityksen käyttämät erilaiset pilvipalvelut kuten Dropbox, iCloud ja Google tai IT-järjestelmät sijaitsevat, ja joko välttää henkilötiedon käsittelyä niiden palvelujen avulla, jotka sijaitsevat EU/ETA alueen ulkopuolella, tai varmistua kansainvälisten tiedonsiirtojen lainmukaisuudesta välitysliikkeessä.

9. Tietosuojaselosteet

Tietosuojaseloste ei sinällään ole mikään uusi juttu, sillä jo nykyinen henkilötietolaki on edellyttänyt rekisteriselostetta välitysliikkeeltä. Uusi asetus edellyttää kuitenkin laajempaa selostetta verrattuna aiempaan, jonka vuoksi ne on päivitettävä. Jos selosteita ei ole jostain syystä ollut aiemmin olemassa, nyt on syytä kiireen vilkkaa sellaiset laatia.

Selosteesta on asetuksen mukaan käytävä ilmi vähintään:

- Rekisterinpitäjän eli välitysliikkeen yhteystiedot
- Henkilötietojen käsittelyn oikeusperusta (UUSI)
- Käsittelyn tarkoitukset
- Henkilötietoryhmät
- Tietojen luovutus
- Tietojen siirto EU/ETA ulkopuolelle
- Säilytysajat (UUSI)
- Kaikki rekisteröidyn oikeudet (UUSI)
- Tietoturvatoimenpiteet
- Tiedot automaattisesta päätöksenteosta ja profiloinnista (UUSI)

Selosteen tai selosteiden on oltava julkisesti nähtävillä välitysliikkeen verkkosivuilla. Tietosuojaselosteet laaditaan välitysliikkeen henkilötietojen käytön perusteella. Välitysliikkeellä tulee siis lähtökohtaisesti olemaan useampia selosteita tai yksi yhdistetty seloste. KVKL:n laki- ja lausuntovaliokunta tulee päivittämään mallilomakkeissaan olevia (toimeksiantosopimukset,

ostotarjoukset ja esisopimus kiinteistön kaupasta) ehtoja tietosuoja-asetuksen perusteella. Jäsenistön on otettava malliehdot tai vastaavanlaiset ehdot käyttöönsä viimeistään toukokuussa.

10. Tietoturvaloukkausten ilmoitusvelvollisuus

Mahdollisen tietoturvaloukkauksen sattuessa välitysliikkeen on lähtökohtaisesti tehtävä siitä tietyn sisältöinen ilmoitus valvontaviranomaiselle ilman aiheetonta viivytystä heti, kun loukkaus on tullut välitysliikkeen tietoon, mahdollisuuksien mukaan 72 tunnin kuluessa. Loukkauksesta on kyse esimerkiksi silloin, jos joku ulkopuolinen henkilö pääsee käsiksi tietoihin tai tietoja luovutetaan luvattomasti. Jos ilmoitusta ei voida tehdä 72 tunnin kuluessa, välitysliikkeen on toimitettava valvontaviranomaiselle perusteltu selvitys. Ilmoituksen voi jättää tekemättä, jos loukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Ilmoitus on tehtävä esimerkiksi silloin, kun henkilötunnuksia on varastettu.

Lisäksi loukkauksesta on lähtökohtaisesti ilmoitettava niille henkilöille, joiden tietojen osalta tietosuojaa on rikottu. Ilmoitusta rekisteröidylle ei kuitenkaan tarvitse tehdä, jos rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja loukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä tai rekisterinpitäjä on toteuttanut loukkauksen johdosta toimenpiteitä, joilla varmistetaan, että korkea riski luonnollisten henkilöiden oikeuksille ja vapauksille ei enää todennäköisesti toteudu. Välitysliikkeen on dokumentoitava kaikki tietoturvaloukkaukset ja ne on tarvittaessa esitettävä valvontaviranomaiselle.

> Ilmoituksessa on kuvattava loukkaus, loukkauksen todennäköiset seuraukset ja toimenpiteet, jotka on toteutettu loukkauksen johdosta sekä yhteyshenkilö.

11. Dokumentoi!

Uusi asetus tuo mukanaan myös niin sanotun osoitusvelvollisuuden. Jatkossa ei enää riitä, että välitysliike noudattaa sääntelyä vaan sen pitää pystyä myös osoittamaan, miten tietosuoja on huomioitu toiminnan suunnittelussa ja toteutuksessa. Tämän vuoksi vastuiden selkeä kuvaus sekä henkilötietojen käsittelyprosessien ja erilaisten tietosuojatoimintojen dokumentointi on ensiarvoisen tärkeää. Laadi välitysliikkeelle tietoturvapolitiikka, jossa on määritetty keskeiset tietosuojaperiaatteet. Tietosuojasta tulee laatia myös perusohjeet, jotka sisältävät muun muassa toimintaohjeet omille työntekijöille mahdollisten tietoturvaloukkausten varalta, toimintaohjeet rekisteröityjen oikeuksien toteuttamisesta sekä ohjeet henkilötietojen säilytysajoista.

Haluatko kuulla lisää tietosuoja-asetuksesta ja esittää tarkentavia kysymyksiä? KVKL järjestää välitysliikkeille suunnatun koulutuksen 2.3.2018 Helsingissä. Lisätiedot toimisto@kvkl.fi tai www.kvkl.fi

Ilmoittaudu koulutukseen tämän linkin kautta