Rakennusteollisuus

Tietosuoja-asetus rakennusalalla

Anne Hirsiniemi
Lakimies
Rakennusteollisuus RT ry

EU:n tietosuoja-asetus

- Euroopan parlamentti hyväksyi 15.4.2016 EU:n uuden tietosuoja-asetuksen (EU) 2016/679, joka korvaa EU:n henkilötietodirektiivin (1995).
  - Koskee kaikkien EU:n kansalaisten henkilötietojen käsittelyä ja näin yhdenmukaistaa lainsäädännön henkilötietojen käsittelystä EU:n alueella
  - Yksilöille tehokkaampi kontrolli omiin tietoihinsa
  - Dataa käsittelevien organisaatioiden velvollisuudet lisääntyvät
  - Viranomaisvalvonta ja sanktiot tehostuvat
- Soveltamisala: kaikki osin tai kokonaan automaattisessa muodossa (tietojärjestelmissä) tapahtuva henkilötietojen käsittely sekä manuaalinen henkilötietojen käsittely, joka muodostaa rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa
  - Ei koske mm. pelkästään henkilökohtaista tai kotitaloutta koskevaa henkilötietojen käsittelyä, joka ei sidoksissa ammatilliseen tai kaupalliseen toimintaan
- Siirtymäaika – voimaan Suomessa 25.5.2018.
  - Asetus on suoraan sovellettavaa lainsäädäntöä Suomessa

Asetuksen täytäntöönpano

- Oikeusministeriön työryhmä selvittänyt kansallisten lainsäädäntötoimien tarvetta yleisellä tasolla
  - Tietosuojan yleissääntely perustuu Suomessa nykyisin henkilötietolakiin (v.1999)
  - Asetuksen vaatimukset vastaavat suurelta osin henkilötietolain vaatimuksia, jonka soveltaminen käytännössä ollut kuitenkin epätarkkaa
- Tietosuoja-asetuksen johdosta säädettävä uusi kansallinen tietosuojalaki tulee korvaamaan nykyisen henkilötietolain
  - HE annettu eduskunnalle viikolla 9
  - Laista tulossa lyhyt EU:n asetusta täydentävä kansallinen laki
- Lisäksi erilliset työryhmät käyvät läpi Suomen lainsäädäntöä tietosuoja-asetuksesta johtuvien muutostarpeiden selvittämiseksi
  - TEMin työelämän tietosuojasääntelyä arvioivan työryhmän määräaika 03/2018 loppuun

Määritelmät

- **Henkilötieto** = Kaikenlaiset tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevat tiedot, jotka voidaan liittää häneen
  - Esim. henkilön nimi, postiosoite, sähköpostiosoite, henkilötunnus, syntymäaika, sukupuoli, ammatti, kuva video, tietokoneen IP-osoite, laite DI, sormenjälki, auton rekisteritunnus ovat henkilötietoja, jos tieto voidaan tunnistaa tiettyä henkilöä koskevaksi
- **Henkilötietorekisteri =** Esim. työntekijälistaukset, osallistujalistat jne.
- **Rekisteröity =** Henkilötietojen käsittelyn kohteena oleva luonnollinen henkilö
- **Rekisterinpitäjä =** Yritys/yhteisö/henkilö, jonka käyttöä varten henkilötietorekisteri perustetaan ja joka määrää rekisterin käytöstä
- **Henkilötietojen käsittelijä =** Rekisterinpitäjän lukuun toimeksiannosta työskentelevä taho, jonka tehtäviin henkilötietojen käsittely kuuluu (esim. rekisterinpitäjän työntekijä tai yritys, jolle henkilötietojen käsittely on ulkoistettu esim. ulkoistetun palkkahallinnon johdosta)

Osoitusvelvollisuus

- Velvollisuus osoittaa, että asetusta ja sen periaatteita noudatettu (käännetty todistustaakka) -> enää ei riitä, että kertoo noudattavansa
- Kattava dokumentaatio kaikista henkilötietojen käsittely- ja suojaustoimenpiteistä sekä arvio tietosuojariskeistä ja toimenpiteet niiden minimoimiseksi
- Toistaiseksi ei ole tarkkoja ohjeita siitä, miten osoitusvelvollisuus tulee käytännössä toteuttaa

  -> Tämän hetkisen tietosuojavaltuutetulta saadun tiedon mukaan voidaan toteuttaa esim. tietotilinpäätöksen, tietosuojaselosteen ja yrityksen tietosuojaohjeen avulla

Käsittelyä ja suojausta koskevia vaatimuksia

- Henkilötietojen keräämiseen ja käsittelyyn asetuksen mukainen peruste:
  - rekisteröidyn suostumus yhtä tai useampaa tarkoitusta varten (aktiivinen yksilöity tahdonilmaisu);
  - sopimuksen täytäntöönpano tai sopimusta edeltävien toimenpiteiden toteuttaminen rekisteröidyn pyynnöstä (esim. tarjouksen toimittaminen pyynnöstä tai rekrytointitilanteet);
  - lakisääteisen velvoitteen noudattaminen (esim. työntekijäluettelo työmaalla);
  - rekisteröidyn tai muun henkilön elintärkeän edun suojaaminen (esim. ICE-henkilö);
  - yleistä etua koskevan tehtävän suorittaminen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen tai
  - rekisterinpitäjän/kolmannen osapuolen oikeutetun edun toteuttaminen (esim. asiakas- tai työsuhde), paitsi jos rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät ne
- Käsittelyperusteita voidaan täsmentää kansallisella lainsäädännöllä
  - Tämän hetkisen tiedon mukaan esim. ay-liittoon kuulumista koskevan tiedon käsittelystä säädettäisiin vastaavasti kuin nykylainsäädännössä -> työnantaja voi käsitellä näitä tietoja vastaavasti kuin aiemmin

Käsittelyä ja suojausta koskevia vaatimuksia

- Arkaluonteisten tietojen käsittelyoikeus vain, jos rekisteröidyn suostumus, työlainsäädäntö sallii tai tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi
  - HOX! Työntekijän terveydentilatiedot säilytettävä erillään muista henkilötiedoista
- Lapsen henkilötietojen käsittely tietoyhteiskunnan palvelujen tarjoamiseen edellyttää vanhemman suostumusta/valtuutusta
  - Tämän hetkisen tiedon mukaan ”lapsen” ikäraja Suomessa 13 v.
- Kerääminen, käsittely ja säilytys rajoitettava vain tarpeelliseen tietoon ja aikaan -> poistettava tarpeeton ja vanhentunut tieto.
  - Ei saa kerätä ”nice to know” –tietoa, ei saa säilyttää tietoa ”varmuuden vuoksi”
  - Määräaikoja: Työsopimuslaki 5v./2v./10v., työaikalaki 2v., ilmoitusvelvollisuus 6v. -> Myös säilytysajat ja niiden perusteet dokumentoitava jatkossa
- Tietojen suojaus teknisin ja organisatorisin keinoin, esim. tietojärjestelmien tietoturva, tietojen salaus, henkilöstön koulutus ja ohjeistus, käyttäjähallinta, asiakirjojen säilytys
- Riskipohjainen lähestymistapa -> arvioitava tietosuojariskit ja ennalta ehkäistävä niitä
  - Jos kyse korkean riskin käsittelystä, tehtävä vaikutustenarviointi

Vaikutustenarviointi korkean riskin tiedoista

- Jos 2 ao. kriteereistä täyttyy, koskee ko. henkilötietoja korkea riski ja käsittelystä tehtävä vaikutustenarviointi ennen tietojen käsittelyä
  1) Rekisteröidyn työsuorituksen, taloudellisen tilanteen, terveyden, henk.koht. mieltymysten/kiinnostuksen, luotettavuuden tai käyttäytymisen, sijainnin tai liikkumisen automatisoitu arviointi, pisteytys tai profilointi
  2) Automaattinen päätöksenteko, jolla oikeus- tm. vaikutuksia
  3) Laajamittainen järjestelmällinen valvonta
  4) Arkaluonteiset tai hyvin henk.koht. tiedot (esim. terveystiedot)
  5) Tietojen laajamittainen käsittely
  6) Tietokokonaisuuksien yhteensovittaminen tai yhdistäminen
  7) Heikossa asemassa olevien rekisteröityjen tiedot (esim. työntekijä)
  8) Uusien teknisten/organisatoristen ratkaisujen innovatiivinen käyttö tai soveltaminen
  9) Käsittelytoimet estävät rekisteröityä käyttämästä oikeutta, palvelua tai sopimusta
- Asetuksen mukaan kansallisten tietosuojaviranomaisten tulee laatia lista käsittelytoimien tyypeistä, joiden osalta vaikutustenarviointi ainakin vaaditaan ao. kriteerit huomioiden -> Toistaiseksi ei saatavilla

Vaikutustenarviointi korkean riskin tiedoista

- Rakennusalalla ainakin työntekijöiden terveystiedot (4+7), kulunvalvonta sormenjälkitunnisteella (8+7)
- Menettelyä ei säännelty, mutta osoitettava dokumentoidusti, miten korkea riski huomioitu ja pyritty ennalta ehkäisemään, kukin korkean riskin tietojenkäsittelytoimi erikseen
  - Sisällettävä ainakin kuvaus käsittelytoimista ja tarkoituksesta, arvio riskeistä ja toimenpiteet niiden ennalta ehkäisyyn
  - Käytännössä kunkin korkean riskin käsittelytoimen osalta kuvataan erikseen samat prosessit kuin tietosuojaselosteessa ja tietotilinpäätöksessä + miten korkea riski huomioitu ja ennalta ehkäisty
- Voi jättää tekemättä, jos dokumentoidusti perustelee, miksei vaikutustenarviointia tarvita ja saa siihen tietosuojavaltuutetun näkemyksen
- Arvioitava ja päivitettävä jatkuvasti, ei velvollisuutta julkaista

Rekisteröidyn oikeudet laajenevat

- Nykyisen lain mukaiset velvoitteet säilyvät voimassa:
  - Informointivelvollisuus henkilötietojen käsittelystä niiden keruun yhteydessä (esim. tietosuojaselosteen avulla);
  - Rekisterinpitäjän velvollisuus oikaista virheelliset tiedot;
  - Oikeus peruuttaa suostumus;
  - Oikeus saada henkilötietonsa poistetuksi;
  - Oikeus tarkistaa itseään koskevat tiedot;
- Asetuksesta seuraavia uusia oikeuksia:
  - Oikeus saada itseään koskevat henkilötiedot rekisterinpitäjältä (konekielisesti);
  - Oikeus käsittelyn rajoittamiseen ja vastustamiseen;
  - Oikeus siirtää tietonsa järjestelmästä toiseen (vain konekieliset rekisteröidyltä saadut tiedot);
  - Oikeus tehdä valitus tietosuojavaltuutetulle
  - Oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta

Henkilötietojen käsittelyn ulkoistaminen

- Ulkoistaja rekisterinpitäjänä, vastaanottaja henkilötietojen käsittelijänä rekisterinpitäjän puolesta (esim. työntekijöiden palkkatiedot ulkoistettuun palkkahallintoon)

  -> rekisterinpitäjällä säilyy määräysvalta henkilötietoihin

- Velvollisuus laatia kirjallinen sopimus tietosuojasta
  - Voidaan käytännössä sisällyttää ulkoistetusta palvelusta laadittuun sopimukseen
- Sopimuksen sisällettävä ainakin käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi (esim. nimiä ja palkkatietoja) ja rekisteröityjen ryhmät (esim. työntekijät) sekä alla olevat rekisterinpitäjän velvollisuudet ja oikeudet:

a) henkilötietojen käsittely rekisterinpitäjän kirjallisten ohjeiden mukaisesti (yrityksen tietosuojaohjeistus);

b) henkilötietoja käsittelevien salassapitovelvollisuus (lisää salassapitosopimusten tarvetta työsuhteissa?);

c) tietosuojasta huolehtiminen asianmukaisin teknisin ja organisatorisin toimenpitein;

Henkilötietojen käsittelyn ulkoistaminen

d) alihankkijan käyttö ainoastaan rekisterinpitäjän luvalla;

e) rekisterinpitäjän auttaminen rekisteröityjen pyyntöihin vastaamiseksi rekisteröityjen käyttäessä oikeuksiaan;

f) rekisterinpitäjän auttaminen varmistamaan, että asetuksen velvollisuuksia noudatetaan (käsittelyn turvallisuus, vaikutustenarviointi, ilmoitukset tietoturvaloukkauksista aikarajoineen);

g) henkilötietojen poistaminen tai palauttaminen palveluiden tarjoamisen päätyttyä, paitsi jos lainsäädäntö velvoittaa säilyttämään henkilötiedot;

h) rekisterinpitäjän saataville tiedot tietosuojavelvoitteiden noudattamisen osoittamiseksi sekä auditointien salliminen asiassa ja osallistuminen niihin

Henkilötietojen luovuttaminen

- Luovutuksensaajasta tulee rekisterinpitäjä

  -> luovutuksensaaja saa määräysvallan henkilötietoihin

- Edellyttää, että luovuttajalla asetuksen mukainen peruste luovuttaa, luovutuksensaajalla asetuksen mukainen peruste henkilötietojen käsittelyyn ja rekisteröityä informoidaan luovutuksesta
  - Esim. työntekijöiden palkkatietojen luovuttaminen verottajalle ja henkilötietojen luovuttaminen työterveyshuollon järjestämiseksi

    ->perustuvat lakiin
  - Rekisteröidyn informointi esim. työsopimusta solmittaessa käymällä läpi tietosuojaseloste tm., voidaan myös kirjata työsopimukseen
- Luovuttamisesta voidaan laatia erillinen sopimus (ei pakko)
- Henkilötietojen siirtoihin EU:n ulkopuolelle omat säännöksensä

Tietosuojavastaava

- Asetuksen mukaan nimitettävä, jos ”rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa”.
- Kunkin yrityksen tehtävä omalta osaltaan arvio ja päätös asiassa
- Tietosuojavastaavan edellyttävää toiminta voi olla yrityksen toimiessa säännönmukaisesti päätoteuttajana yhteisillä työmailla, joilla paljon työntekijöitä -> kuukausittain raportit Verohallinnolle yhteisellä työmaalla työskennelleistä henkilöistä sekä velvollisuus pitää ajantasaista luetteloa työmaalla työskentelevistä
- Jos yritys toimii joskus päätoteuttajana yhteisellä työmaalla, toiminta todennäköisesti ei ole sen kaltaista, että tietosuojavastaavaa tulisi nimittää
  - Tehtävä arvio, kuinka paljon päätoteuttajan roolissa
- Jos yritys ei toimi lainkaan päätoteuttajana yhteisellä työmaalla, toiminta ei ole sen kaltaista, että tietosuojavastaavaa olisi velvollisuutta nimittää
- Jos yritys katsoo, ettei velvollisuutta nimittää tietosuojavastaavaa ole, ratkaisu perusteluineen on dokumentoitava (osoitusvelvollisuus)
  - Mitä enemmän henkilötietojen käsittelyä sitä tarkempi arvio ja perustelut
  - Tällöin suositeltavaa nimetä yhteyshenkilö tietosuoja-asioissa
- Tietosuojavastaavaa ei kannata nimittää vapaaehtoisesti

Tietosuojavastaava

- Yrityksen sisäinen tai ulkopuolinen henkilö ja konserni voi nimittää yhden yhteisen
- Asiantuntemusta tietosuojalainsäädännöstä sekä alan ja yrityksen toiminnasta ja valmiudet tehtävän hoitamiseen riippumattomasti (tarkentuu myöhemmin)
- Valvoo tietosuojasäännösten noudattamista -> kerää tietoa henkilötietojen käsittelytoimista, analysoi ja tarkistaa niitä sekä antaa tietoa, neuvoja ja suosituksia rekisterinpitäjälle ja henkilötietojen käsittelijälle sekä raportoi näistä ja antaa toimintakertomuksen vuosittain johdolle
  - Vastuu tietosuojasäännösten noudattamisesta säilyy aina rekisterinpitäjällä ja henkilötietojen käsittelijällä
  - Toimittaessa vastoin tietosuojavastaavan ohjeita, dokumentoitava perusteet tähän
  - Salassapitovelvollisuus tehtävää hoitaessaan

Tietosuojavastaava

- Mukaan kaikkien tietosuojakysymysten käsittelyyn mahdollisimman aikaisessa vaiheessa
  - Tarvittaviin kokouksiin ja päätöksentekoon
  - Olennaiset tiedot tietosuoja-asioihin liittyen
  - Näkemysten huomioiminen tietosuoja-asioihin ja mahdollisiin tietoturvaloukkauksiin liittyen.
- Annettava resurssit ja aikaa tehtäviensä hoitamiseen sekä pääsy henkilötietoihin ja niiden käsittelytoimiin
- Erityissuoja: ei saa erottaa tai rankaista tehtävien hoitamisen vuoksi
  - Ei siis yhtä laaja kuin luottamusmiehillä ja työsuojeluvaltuutetuilla, sillä ulottuu ainoastaan tietosuojavastaavan tehtävien hoitamista koskeviin tilanteisiin
  - Syytä kuitenkin varautua osoittamaan, ettei työsuhteen päättäminen johtunut tietosuojavastaavan tehtävien hoitamisesta
- Yhteystiedot tulee julkistaa henkilöstölle ja ilmoittaa tietosuojavaltuutetun toimistolle

Valvonta

- Tietosuojavaltuutetun toimisto valvoo lain soveltamista
  - Ilmoitusvelvollisuus nimetystä tietosuojavastaavasta ja tietoturvaloukkauksista
  - Voi määrätä sanktioita rekisterinpitäjälle/henkilötietojen käsittelijälle velvoitteiden laiminlyönneistä ja rikkomuksista
    - Arvioidaan kussakin tapauksessa erikseen
    - Sanktioita ovat mm. huomautus, varoitus, keskeytysmääräys, korjaamisvelvoite sekä sakko, jonka suuruus on 10 miljoonaa / 2 % yrityksen maailmanlaajuisesta kokonaisliikevaihdosta tai 20 miljoonaa / 4 % yrityksen maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan kumpi on suurempi.
- Kansallisesti voidaan säätää sertifiointijärjestelmästä, jonka kautta yritys voi hankkia tietosuojasertifioinnin osoituksena asetuksen velvoitteiden täyttämisestä.
  - Toistaiseksi ei tietoa, tuleeko Suomeen

Valmistautuminen tietosuoja-asetukseen

- Kartoita nykytilanne
  - Mitä henkilötietoja kerätään ja käsitellään?
  - Käyttötarkoitus ja käsittelyn peruste?
  - Onko henkilötietojen käsittelyä ulkoistettu?
  - Luovutetaanko henkilötietoja yrityksestä?
  - Henkilötietojen käsittelijät, heidän perehdytys/koulutus ja yrityksen ohjeistus?
  - Miten huolehdittu tietoturvasta ja käsittelyn rajoittamisesta määräaikoineen?
  - Miten toteutetaan rekisteröityjen oikeudet?
  - Tuleeko nimetä tietosuojavastaava?
  - Tietoturvaan liittyvien riskien arviointi (ja tarvittaessa vaikutustenarviointi) ja minimointi sekä toimenpiteet tietoturvaloukkausten yhteydessä?

    -> Korjaa mahdolliset puutteet suhteessa tietosuoja-asetuksen vaatimuksiin
- Dokumentoi edellä mainitut osoitusvelvollisuuden täyttämiseksi!!!
  - Tämän hetkisen tiedon mukaan voidaan toteuttaa esim. tietotilinpäätöksen, tietosuojaselosteen ja yrityksen tietosuojaohjeen avulla

Valmistautuminen tietosuoja-asetukseen

- Perehdytä/kouluta työntekijät, jotka käsittelevät henkilötietoja
  - Osaksi uusien perehdytystä, jos käsittelevät henkilötietoja
- Työsopimuslomakkeiden täydentäminen?
  - Maininta työntekijän perehdyttämisestä yrityksen tietosuojaohjeistukseen + salassapitolauseke?
  - Maininta työntekijän henkilötietojen käsittelystä työsuhteessa
- Seuraa viranomaisten ja RT:n ohjeistusta
  - Tietosuojavaltuutetun mukaan heidän mallinsa ja ohjeensa tietotilinpäätökseen ja tietosuojaselosteeseen käypiä, kunnes julkaisevat uudet

Rakennusteollisuus

Lisätietoja:

anne.hirsiniemi@rakennusteollisuus.fi

P. 09-1299 269