Anne Hirsiniemi / ABa

1.12.2017

Talonrakennusteollisuus ry:n jäsenyrityksille

Uusi tietosuojasääntely

EU:ssa on astunut voimaan tietosuoja-asetus ja henkilötietojen käsittelyn on oltava tietosuoja-asetuksen mukaista 25.5.2018 alkaen. Muutoksia Suomen lainsäädäntöön valmistellaan parhaillaan, mutta niiden sisältöä ei ole vielä julkistettu. Alla on selostettu asetuksen sisältö pääpiirteissään sekä sen vaikutuksia käytännössä. Lisätietoja asiaan saa RT:n nettisivuilta www.rakennusteollisuus.fi/tietosuoja, joita päivitetään sitä mukaa kun asetuksen tulkinnasta ja lainsäädäntömuutoksista saadaan lisätietoa.

Ketä ja mitä tietosuoja-asetus koskee?

Tietosuoja-asetus koskee kaikkia, jotka käsittelevät henkilötietoja. Asetusta sovelletaan sekä yksityisellä että julkisella sektorilla riippumatta esim. henkilötietojen käsittelyn laajuudesta, käsiteltävien henkilötietojen luonteesta tai käytetystä teknologiasta. Käytännössä jokaisessa yrityksessä käsitellään henkilötietoja ja muodostetaan niistä rekistereitä ja käsittelijöitä voi olla kaikissa henkilöstöryhmissä.

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen tekijän perusteella.

Rekisterillä tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein. Kaikki rekisterit kuuluvat tietosuoja-asetuksen piiriin riippumatta toteuttamistavasta tai siitä, miten rekisteriä ylläpidetään. Esim. työntekijöistä ylläpidettävä excel-taulukko on henkilörekisteri, koska se sisältää henkilötietoja. Myös asiakas- tai markkinointirekisterit ovat henkilörekistereitä, jos niihin on tallennettu henkilötietoja. Samaan henkilörekisteriin kuuluvat kaikki samaa käyttötarkoitusta varten kerätyt henkilötiedot. Samaan rekisteriin sisältyviä tietoja voi olla osittain sähköisesti ja osittain paperilla ja niitä voi olla myös eri paikoissa tai eri henkilöiden hallussa.

Mitä yrityksen tulee tehdä?

Yrityksen on ennen 25.5.2018 huolehdittava, että henkilötietojen käsittely on tietosuoja-asetuksen mukaista.

1. Kartoita henkilötietojen käsittelyn nykytila
Kartoituksen voi käytännössä tehdä esim. tietotilinpäätöksen ja rekisteriselosteiden avulla, joihin ohjeet ja mallit löytyvät mm. tietosuojavaltuutetun nettisivuilta. RT avaa lähiaikoina tie-

tosuoja-asetusta koskevan nettisivun, johon tulevat linkit edellä mainittuihin. Jos kartoituksessa ilmenee puutteita suhteessa tietosuoja-asetukseen ja lainsäädäntöön, tulee puutteet korjata sekä käytännössä että dokumentoituna tietotilinpäätökseen ja rekisteriselosteisiin.

2. Toteuta tietosuoja-asetuksen vaatimukset ja osoita se

Asetuksen yleisperiaatteiden mukaan henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidylle läpinäkyvästi sekä tiettyä laillista tarkoitusta varten (käyttötarkoitussidonnaisuus), henkilötietojen tulee olla asianmukaisia ja olennaisia sekä täsmällisiä ja tarvittaessa päivitettyjä, henkilötietoja saa säilyttää vain niin kauan kuin tarpeen ja niitä on käsiteltävä turvallisesti (suojaaminen luvattomalta ja lainvastaiselta käytöltä).

Käsittelylle on aina oltava jokin alla luetelluista asetuksen mukaisista perusteista:

- rekisteröidyn suostumus yhtä tai useampaa tarkoitusta varten;
- sopimuksen täytäntöönpano tai sopimusta edeltävien toimenpiteiden toteuttaminen rekisteröidyn pyynnöstä;
- lakisääteisen velvoitteen noudattaminen;
- rekisteröidyn tai muun henkilön elintärkeän edun suojaaminen;
- yleistä etua koskevan tehtävän suorittaminen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen tai
- rekisterinpitäjän/kolmannen osapuolen oikeutetun edun toteuttaminen (esim. asiakas- tai palvelusuhde), paitsi jos rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät ne.

Tietojen suojaamisesta on huolehdittava niiden keräämisvaiheesta tuhoamiseen saakka. Suojaaminen edellyttää myös käsittelyn seuraamista ja valvontaa. Suojatoimenpiteitä ovat mm. henkilöstön koulutus/ohjaus/määräykset, salassapitositoumukset, tila- ja käytönvalvontaa, tietojärjestelmien tietoturva sekä tietojen käytönvalvonta ja salaus. Suojaustoimenpiteiden taso riippuu käsiteltävien henkilötietojen luonteesta, laajuudesta, asiayhteydestä, tarkoituksesta ja käsittelyyn liittyvistä tietosuojariskeistä.

Tietosuoja-asetuksen myötä yrityksillä on velvollisuus kirjallisesti osoittaa, että asetuksen säännöksiä noudatetaan yrityksessä (osoitusvelvollisuus) eikä pelkkä noudattaminen siis enää riitä. Käytännössä yrityksen on suunniteltava ja dokumentoiva henkilötietojen käsittely (esim. kirjalliset rekisteriselosteet ja tietotilinpäätös) ja sen tietoturvallisuus (tekniset ja organisatoriset suojatoimenpiteet).

3. Toteuta rekisteröidyn oikeudet

Asetuksessa on aiempaa enemmän säännelty oikeuksia rekisteröidylle, jotka rekisterinpitäjä tulee pystyä toteuttamaan:

- Informointi henkilötietojen käsittelystä niiden keruun yhteydessä;
- Pyynnöstä toimitettava henkilötietojen käsittelyä koskevat tiedot konekielisesti;
- Oikeus oikaista tietonsa ja saada tietonsa poistetuksi (oikeus tulla unohdetuksi);
- Oikeus käsittelyn rajoittamiseen ja vastustamiseen;
- Oikeus siirtää tietonsa järjestelmästä toiseen;
- Oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta.

4. Arvioi mahdolliset riskit
Tietosuoja-asetus velvoitteet yritykset perusteellisesti arvioimaan henkilötietojen käsittelyynsä liittyvät riskit. Riskeillä tarkoitetaan henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja esimerkiksi silloin, kun käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen. Rekisterinpitäjän ja henkilötietojen käsittelijän on käytettävissä olevin keinoin toimittava näiden riskien lieventämiseksi ja poistamiseksi.

5. Sopimusehdot luovutettaessa henkilötietoja yrityksen ulkopuolelle
Oikeuden luovuttaa henkilötietoja tulee sisältyä johonkin kohdassa 2. luetelluista asetuksen mukaisista henkilötietojen käsittelyn perusteista ja luovutuksesta on ilmoitettava rekisteröidylle. Sopimukseen jonka johdosta luovutus tapahtuu, tulee asetuksen mukaan sisällyttää käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät ja käsittelijän on sitouduttava alla oleviin velvoitteisiin:

1) käsittelemään henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti;
2) noudattamaan käsittelyssä salassapitovelvollisuutta;
3) toteuttamaan turvallisuustasoltaan kyseisten henkilötietojen käsittelyn riskiä vastaavat tekniset ja organisatoriset tietoturvatoimenpiteet;
4) velvoittamaan kaikki henkilötietoja käsittelevät noudattamaan samoja tietosuojavelvoitteita kuin rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa on sovittu;
5) auttamaan rekisterinpitäjää teknisin ja organisatorisin toimenpitein täyttämään rekisteröityjen pyynnöt koskien henkilötietojensa käsittelyä;
6) auttamaan rekisterinpitäjää varmistamaan asetuksen velvollisuuksien noudattamisen;
7) poistamaan/palauttamaan käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä kaikki henkilötiedot ja poistamaan olemassa olevat jäljennökset, paitsi jos unionin oikeudessa tai jäsenvaltion lainsäädännössä vaaditaan säilyttämään henkilötiedot;
8) saattamaan rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen em. velvollisuuksien noudattamisen osoittamista varten, ja sallii rekisterinpitäjän tai muun rekisterinpitäjän valtuuttaman auditoijan suorittamat auditoinnit asiassa sekä osallistuu niihin.

6. Ilmoitusvelvollisuus tietoturvaloukkauksista
Rekisterinpitäjällä on asetuksen mukaan velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle. Tietoturvaloukkauksella tarkoitetaan henkilötietojen vahingossa tapahtuvaa tai lainvastaista tuhoamista, häviämistä, muuttamista, luvatonta luovuttamista tai pääsyä tietoihin. Rekisterinpitäjän on tehtävä loukkausta koskeva ilmoitus valvontaviranomaiselle mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta. Ilmoituksen voi jättää tekemättä ainoastaan, mikäli loukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.

Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset ja kaikki niihin liittyvät seikat, loukkauksen vaikutukset ja toteutetut korjaavat toimet.
Osana henkilötietojen käsittelyn suunnittelua tulisi suunnitella prosessit myös mahdollisten tietoturvaloukkausten varalle niiden tunnistamiseen, ilmoittamiseen, selvittämiseen ja dokumentointiin sekä ohjeistaa nämä henkilötietojen käsittelijöille.

7. Tietosuojavastaava

Yrityksen on nimettävä tietosuojavastaava, jos yrityksen ydintehtävät muodostuvat henkilötietojen käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. RT selvittää parhaillaan, kuuluuko rakennusalan toiminta velvoitteen piiriin. Tietosuojavastaava voi olla yrityksen palveluksessa työskentelevä henkilö tai ulkopuolelta hankittu palvelu, jolla on erityisasiantuntemusta tietosuojalainsäädännöstä ja alan käytänteistä ja joka valvoo riippumattomasti tietosuoja-asetuksen noudattamista. Vaikka asetus ei velvoittaisi nimeämään tietosuojavastaavaa, kannattaa yrityksessä kuitenkin nimetä tietty yhteyshenkilö tietosuoja-asioissa.

Käytännössä

Selvitä ja toteuta seuraavat asiat:

- Mitä henkilötietoja kerätään ja käsitellään ja muodostuuko niistä rekistereitä.
- Millä perusteella henkilötietoja kerätään ja käsitellään ja mahdollisesti luovutetaan yrityksen ulkopuolelle.
- Miten huolehdittu tietoturvasta sekä riskien arvioinnista ja minimoinnista.
- Tarvitaanko tietosuojavastaava. Nimeä jos tarvitaan.
- Miten toteutetaan yllä 3. kohdassa mainitut rekisteröityjen oikeudet.
- Miten toteutetaan ilmoitus tietoturvaloukkauksista.
- Tietoturvavelvoitteet sopimuksiin luovutettaessa henkilötietoja yrityksen ulkopuolelle.

Dokumentoi edellä mainitut esim. tietotilinpäätöksen ja rekisteriselosteiden avulla ja perehdytä/kouluta henkilötietoja käsittelevät työntekijät asetuksen mukaiseen käsittelyyn.

Muuta

Tietosuoja-asetuksessa on erikseen säädetty velvoitteista siirrettäessä henkilötietoja EU:n ulkopuolelle. Tietosuojavaltuutettu valvoo asetuksen noudattamista ja antaa sanktioita sen rikkomisesta tai laiminlyönnistä. Määrättävä sanktio arvioidaan kussakin tapauksessa erikseen ja niitä 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.

Lisätietoja asiaan saa RT:n nettisivuilta, joita päivitetään sitä mukaa kun asetuksen tulkinnasta ja lainsäädäntömuutoksista saadaan lisätietoa. Samoin tietosuojavaltuutetun nettisivuilta löytyy hyödyllistä jatkuvasti päivittyvää tietoa asiasta. Sieltä löytyvät myös ohjeet ja mallit jäsenkirjeessä mainittujen rekisteriselosteiden ja tietotilipäätöksen tekemiseen, joita tietosuojavaltuutettu tullee päivittämään.

Lisätietoja Anne Hirsiniemi, puh. 040 759 2950
anne.hirsiniemi@rakennusteollisuus.fi