EU:n tietosuoja-asetukseen valmistautuminen FCG-konsernissa ja Kuntarekry-palvelussa

Vesa Nyman 7.3.2018

EU:n tietosuoja-asetus (GDPR)

Mikä on henkilötietoa?

- Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja.
- Tunnistettavissa olevana pidetään luonnollista henkilöä, **joka voidaan suoraan tai epäsuorasti tunnistaa** erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella

- Henkilötietoa voivat olla esimerkiksi tieto, kuva, paikkatieto, tietojen yhdistelmä, IP-osoite jne. ja ne voivat sijaita esim. tietojärjestelmissä, tiedostoissa tai paperikopioina.

EU:n tietosuoja-asetus (GDPR)

- Tietosuoja on osa perustuslain takaamaa yksityissuojaa. Tietosuojatyössä pyritään suojelemaan luonnollisen henkilön henkilötietoja ja turvata yksilön oikeuksia omien henkilötietojen käsittelyssä.
- EU:n uusi tietosuoja-asetus (GDPR, General Data Protection Regulation) soveltaminen alkaa **25.5.2018**
- Tavoitteena tietosuoja-asetuksella on erityisesti
  - yksityishenkilöiden oikeuksien turvaaminen
  - tietosuojasääntelyn harmonisointi EU:ssa
- Tietosuoja-asetus on lainsäädäntöohje, jonka kukin jäsenvaltio toteuttaa omassa kansallisessa lainsäädännössään
  - Oikeusministeriön alainen työryhmä ehdottanut kansallista tietosuojalakia
  - Tietosuoja-asetus **korvaa** vuoden 1995 henkilötietodirektiivin (95/46/EY) ja henkilötietolain (523/1999) säännökset henkilötietojen käsittelyn osalta
- Asetus tuo **rekisterinpitäjille** ja **henkilötietojen käsittelijöille** paljon uusia velvoitteita
- Mikäli velvoitteita ei ole riittävän hyvin hoidettu, kansallisella valvontaviranomaisella on sakotusmahdollisuus: enintään 20 milj. € tai 4 % liikevaihdosta

Muutoksen vaikutusanalyysi

- Asiakasvaatimukset – Asiakkaat vaativat selvityksiä henkilötietojen käsittelystä sekä apua käyttämiensä sovelluksien tietosuoja- ja tietoturvakyvykkyyksistä
- Sopimusmuutokset – Pakollisia sopimusklausuuleja tulee lisätä ~kaikkiin sopimuksiin
- Organisointimuutokset – Nimettävä tietosuojasta vastuullisia henkilöitä liiketoimintayksiköittäin, konsernitason koulutusta lisättävä, tietosuojaan keskittyviä ryhmiä muodostettava
- Prosessimuutokset – Henkilötietojen käsittelyssä käytettäviä prosesseja muutettava, tietosuoja otettava huomioon sovelluskehityksessä, tietosuojaloukkauksille ja rekisteröityjen oikeuksien toteuttamiselle määritettävä prosessi, riski- ja vaikuttavuusarviointeja tulee tehdä selvästi aiempaa laajemmin, lisädokumentaatio
- Teknologiamuutokset – Sisäänrakennettu ja oletusarvoinen tietosuoja tulee tehokkaasti huomioida henkilötietojen käsittelyä sisältävissä toiminnoissa niiden kaikissa vaiheissa
- Dokumentointivaatimukset – GDPR sisältämän osoitusvelvollisuuden vuoksi tulee selvitettäviä asioita dokumentoida laajasti

FCG-konsernin valmistautuminen EU:n tietosuoja-asetukseen

Erilaisia liiketoimintoja, erilaisia tarpeita

- FCG-konsernissa on erilaista liiketoimintaa:
  - Kaupunkisuunnittelua
  - Konsultointia
  - Ohjelmistoliiketoimintaa
  - Koulutusta

- Toimimme näin tietosuojan osalta eri rooleissa
  - Konsultointiliiketoiminnassa toimeksiannoissa käsittelemme asiakkaiden vastuulla olevia henkilötietoja henkilötietojen käsittelijöinä
  - Konsernihallinto- ja koulutusliiketoiminta toimii rekisterinpitäjinä ja käyttää kymmeniä henkilötietojen käsittelijöitä
  - Ohjelmistoliiketoiminnassa korostuu sovelluksen tietoturva ja ominaisuudet

Käytännön valmistautuminen GDPR:ään

- GDPR:ään valmistautumisprojekti aloitettiin 07/2017.
- Projektissa
  - Tehtiin läpivientimalli eri rooleille (rekisterinpitäjä, henkilötietojen käsittelijä, sovellustoimittaja)
  - Henkilötietovarannot selvitettiin ja tunnistettiin liiketoimintojen rooli näihin liittyen
  - Omat sovellukset tunnistettiin ja tehtiin näihin liittyvät tietoturva- ja ominaisuustarpeiden kartoitukset sekä puutteiden implementointi
  - Keskitetysti muodostettiin/päivitettiin politiikkoja, toimintamalleja, prosesseja, koulutettiin henkilöstöä
  - Jalkautetaan tietosuoja jokapäiväiseen työhön

Opittua / vinkkejä

- GDPR ei anna kaikkeen selviä vastauksia. Tee päätöksiä nopeasti, älä takerru epäolennaisuuksiin!

- Yksinkertainen on kaunista: vähän rekistereitä, konsernitason prosessit käyttöön

Kuntarekry-palvelun GDPR-valmistautuminen

Kuntarekryn valmistautumistoimenpiteet

- Palvelun tietoturva käyty läpi ja otettu käyttöön uusia suojatoimia
- Palvelun ominaisuustarpeet käyty läpi ja ohjelmistokehityksessä
- Analysoitu miten rekisteröidyn oikeudet toteutuvat ja kuinka rekisteröityjen pyynnöt voidaan toteuttaa
- Palvelusta tehty GDPR-ohjeistus asiakkaille

- Sopimusmalli henkilötiedon käsittelystä tekeillä → sopimukset kaikkien asiakkaiden kanssa kevään aikana