Tiedonhallintalautakunnan Suositus tietoturvallisuudesta hankinnoissa - webinaari

Tietoturvallisuusvaatimukset ja tietosuojaliite
9.10.2023 klo 8:30 – 11:30

Tietoturvapäällikkö Nina Alapuranen
Vanhempi juristi Päivi Kynkäänniemi

Tietoturvamäärittelyjen ongelmia julkisissa hankinnoissa

- Epäselvät tietoturvavaatimukset
- Väärin mitoitetut tietoturvavaatimukset
- Vanhentuneet määrittelyt
- Ei ole tarpeeksi osaamista eikä riittävästi resursseja (oma, toimittaja)
- Vaatimukset eivät sovellu hankittavaan ratkaisuun
- Integroituvuus ja yhteensopivuus ei toimi
- Puutteellinen seuranta ja auditointi
- Priorisoidaan hintaa tietoturvan kustannuksella
- Muuta, mitä?

Tarvitaan: huolellista suunnittelua, avoimuutta, yhteistyötä, vaatimusten realistisuutta, vaatimusten ajantasaisuuta ja soveltuvuutta, yhteisiä vaatimusmalleja julkiselle hallinnolle

Suosituksen sisältö

- Suositus (VM 2023:57)
  - Liite 1 a Tietoturvallisuusvaatimukset (suppea)
  - Liite 1 b Tietoturvallisuusvaatimukset (laaja)
  - Liite 2 a Hankintaehtotyökalu (uudet Excel-versiot)
  - Liite 2 b Hankintaehtotyökalu (vanhat Excel-versiot)
- Tähän liittyy myös (VAHTI- toiminnassa julkaistut)
  - Tietosuojaliite
  - Henkilötietojen käsittelytoimien kuvaus
  - DVV/digiturvajulkaisut/työkalut ja mallipohjat Digiturvajulkaisut | Digi- ja väestötietovirasto (dvv.fi)

Tiedonhallintalautakunta
Informationshanteringsnämnden

Sopimuksen tietoturvallisuusliitteet

Pääsopimukseen kirjattavat asiat

Tietoturvallisuusvaatimukset (laaja)

tai

Tietoturvallisuusvaatimukset (suppea)

Julkiset tiedot sekä vähäiset eheys- ja saatavuusvaatimukset

Hallinnollisen turvallisuuden vaatimukset
Fyysisen turvallisuuden vaatimukset
Teknisen turvallisuuden vaatimukset
Varautumisen ja jatkuvuudenhallinnan vaatimukset
Tietoturvallisuuden lisävaatimukset

Muodostetaan hankintaehtotyökalun avulla

Tietosuojaliite
Henkilötietojen käsittelytoimien kuvaus

Jos käsitellään henkilötietoja

Pääsopimukseen kirjattavat asiat, tarkista vähintään nämä:

- Oikeus tarkastaa kohteen kannalta riittävät tietoturvallisuusjärjestelyt
- Tietoturvallisuuden vastuuhenkilöt yhteystiedoissa
- Sopimuksen ja liitteiden soveltamisjärjestyksen huomiointi (erityisesti tietoturva- ja tietosuojaliitteet)
- Riittävät sakko- ja vahingonkorvauslausekkeet (myös tietoturvallisuus- ja tietosuojavaatimuksiin liittyvissä poikkeamissa
- Millainen purku- tai välittömän irtisanomisen ehto liittyy tietoturvallisuusliitteen velvoitteiden rikkomiseen
- Tietojen sijainti/käsittely Suomessa ja ETA-alueella
- Mahdollisten yrityskauppatilanteiden huomiointi

Tietoturvallisuusvaatimukset (suppea)

- Suppeaa tietoturvallisuusvaatimus liitettä 1 a voit käyttää osana sellaisia hankintoja, joissa käsitellään vain julkista tietoa ja tiedon eheyteen sekä saatavuuteen ei kohdistu normaalia korkeampia vaatimuksia.
- Vaatimuksia voidaan käyttää myös niissä tilanteissa, joissa käsitellään vain vähäisessä määrin muita kuin julkisia tietoja ja joiden paljastumisen aiheuttama vahinko on vähäinen.


Sisällysluettelo

Tietoturvallisuusvaatimukset (laaja)

- Laajempaa tietoturvallisuusvaatimukset -liitettä 1 b voi käyttää hankintoihin, joissa käsitellään salassa pidettäviä tai turvallisuusluokiteltuja (TLIV- TLI) tietoja, henkilötietoja tai hankittavien palveluiden eheyteen tai saatavuuteen kohdistuu normaalia korkeampia vaatimuksia
- Suositellaan käytettäväksi yhdessä hankintaehtotyökalun avulla muodostettavia osa-aluekohtaisten liitteiden ja tietosuojaliitteiden kanssa.

Sisällysluettelo

Huomioi nämä asiat hankinnan tietosuoja-asioita suunnitellessasi

- Dokumentissa on kohtia, jotka pitää muokata kyseiseen hankintaan sopivaksi – tätä dokumenttia ei siis voi sellaisenaan laittaa tarjouspyynnön liitteeksi.
- Tarkista, että pääsopimuksessa tai yleisissä ehdoissa oleva tarkastusoikeus kattaa myös tietosuojatarkastuksen, esim.: "Toimittaja sallii tilaajan tai sen valtuuttaman auditoijan suorittamat tarkastukset sekä osallistuu niihin."
- Mieti, miten rakennat tietoturva- ja tietosuojatyön hinnoittelun sopimuskaudella
- Kuvaa tarjoajille tarvittaessa organisaatiotasi koskeva lainsäädäntö.
- Tarkista alihankkijan tai alikäsittelijän hyväksymisen prosessi sopimuksella.
- Huomaa, että päätös siitä, saako tietoja siirtää ETA-alueen ulkopuolelle, on tehtävä ennen tarjouspyynnön lähettämistä. Huomioi tämä erityisesti hankkiessasi pilvipalveluita.
- Jos käsittelyyn liittyy erityisiin henkilötietoryhmiin kuuluvia tietoja, varmista, että hankintaehtotyökalun esiehdoissa on valittu kohdassa Henkilötiedot hankinnan kohteessa vaihtoehto "Erityisiin henkilötietoryhmiin kuuluvia tietoja".

Tietosuojaliite

- Tietosuojaliite sisältää lakisääteiset minimivaatimukset sekä ohjeita tietosuojan huomioimiseen sopimuksessa.

VAHTI hyvät käytännöt - tukimateriaali
Tietosuojaliite

1 (6)

VAHTI-sihteeristö

29.5.2023

Sisällysluettelo

Henkilötietojen käsittelytoimien kuvaus

- Henkilötietojen käsittelytoimien kuvausta voi käyttää tietosuojaliitteen alaliitteenä
- Tietosuojaliite ja Henkilötietojen käsittelytoimien kuvaus on suunniteltu toimimaan yhdessä tietoturvallisuusliitteiden kanssa

VAHTI hyvät käytännöt -tukimateriaali 1 (4)

Liite X: Henkilötietojen käsittelytoimien kuvaus

VAHTI-sihteeristö 29.5.2023

Sisällysluettelo

Tiedonhallintalautakunta
Informationshanteringsnämnden

Kiitos, kysymyksiä