VAHTI-hyvät käytännöt tukimateriaali

5.11.2021

**Hankinnan muistilista tietosuoja-asioissa**

Sisällysluettelo

[1 Yleistä 3](#_Toc87031329)

[2 Muistilistan versionhallinta 4](#_Toc87031330)

[3 Hankinnan muistilista tietosuoja-asioissa 4](#_Toc87031331)

Hankinnan muistilista tietosuoja-asioissa

# Yleistä

Tämä asiakirja on tarkoitettu vapaasti hyödynnettäväksi ja sovellettavaksi tietosuojan hankintojen muistilistan muodostamisen tukimateriaalina. Jokaisen organisaation tulee tarkistaa ja sovittaa tämä sen omaan toimintaan, sitä ei tule ottaa käyttöön sellaisenaan.

Toivomme, että annat palautetta tästä tukimateriaalista:

<https://response.questback.com/dvv/digiturvahyvatkaytannotpalaute>

Muut yhteydenotot koskien tätä tukimateriaalia:
digiturva@dvv.fi

Tämän tukimateriaalin tuottamisesta on vastannut VAHTI tietosuojan kehittäminen työryhmän asiantuntijat.

# Muistilistan versionhallinta

|  |
| --- |
| Version hallinta |
| versio nro | mitä tehty | pvm/henkilö |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Hankinnan muistilista tietosuoja-asioissa

## Hankinnan suunnittelu

Suunnitellessasi hankintaa käy vähintään seuraavat kysymykset läpi:

1. Käsitelläänkö henkilötietoja
	* Kyllä (jatka muistilistan läpikäyntiä)
	* Ei (muistilistan läpikäyntiä ei tarvitse jatkaa)
2. Mitä [henkilötietoja](https://tietosuoja.fi/mika-on-henkilotieto) käsitellään?
	* Luettele eri henkilötietoryhmät
	* Huomioi, että erityisiin henkilötietoryhmiin (mm. rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveyttä koskevia tietoja, seksuaalinen suuntautuminen, geneettisiä ja biometrisia tietoja henkilön tunnistamista varten) kuuluvien henkilötietojen käsittely on lähtökohtaisesti kiellettyä. Pohdi erityisen tarkkaan löytyykö näiden tietojen käsittelemiseksi [käsittelyperuste](https://tietosuoja.fi/kasittelyperusteet) kuten henkilön suostumus tai lakisääteinen velvoite.
3. Varmista saako edellä luettelemia henkilötietoja siirtää EU/ETA-alueen ulkopuolelle
	* Organisaatiolla voi olla linjaus, että esimerkiksi erityisiä henkilötietoja ei saa siirtää EU/ETA-alueen ulkopuolelle. Voit varmistaa asia organisaation tietosuojavastaavalta, joka huomioi EU/ETA-alueen ulkopuolisissa siirroissa organisaation linjauksen lisäksi [tietosuojan riittävän tason päätökset](https://tietosuoja.fi/siirto-tietosuojan-riittavyytta-koskevan-paatoksen-perusteella).
	* Huomio organisaation linjaus ja tietosuojavastaavan neuvonta tarjouspyynnössä
4. Oletko tehnyt arvion tarpeesta tehdä vaikutustenarviointi uutta toimintaa, prosessia, järjestelmään käyttöönotettaessa?
	* Täytä vaikutustenarvioinnin alkukartoitus (organisaatiosi oma dokumentti tai tarvittaessa [VAHTI dokumentti](https://dvv.fi/vahti))
	* Jos vaikutustenarvioinnin alkukartoitus ohjaa laatimaan varsinaisen vaikutustenarvioinnin, ota yhteys tietosuojavastaavaan ohjauksen saamiseksi ja vaikutustenarvioinnin laatimiseksi yhteistyössä.
5. Oletko ollut yhteydessä tietosuojavastaavaan henkilötietojen käsittelyyn liittyvissä kysymyksissä?
6. Oletko varmistanut, vaatiiko henkilötietojen käsittely erityisiä tietoturvamenettelyitä?
	* Huomioi organisaatiosi tietoturvalinjaukset (esim. käsitellään henkilötunnuksia jolloin käsittely oltava salattua) ja konsultoi tietoturvamenettelyistä tarvittaessa tietoturvavastaavaa

## Tarjouspyynnön tekeminen

1. Huomioi hankinnan suunnitteluvaiheessa esille nousseet rajoitukset henkilötietojen käsittelyyn liittyen ja nosta nämä osaksi tarjouspyyntöä
	* Rajoituksia voi olla esimerkiksi tietojen siirrossa ulkomaille (EU/ETA-alueen ulkopuolelle) ja teknisissä ja organisatorisissa suojatoimissa
2. Muista lisätä tarjouspyyntöön lause laatuvaatimusten painotuksesta (tietosuoja ja tietoturva)
	* Organisaatio voi linjata, että tietoturva ja tietosuojan erityisistä suojatoimista tai organisaation tietosuojaliitteen sisällöstä saa laatupisteitä kilpailutuksessa
	* Linkitä esimerkki hankintavaatimukset & pisteytys dokumentista
3. Laadi tarkemmat tietosuojan ja tietoturvan hankintavaatimukset
	* Huomioi ehdottomat vaatimukset
	* Varmista, että sisäänrakennetun ja oletusarvioisen tietosuojan vaatimukset toteutuvat hankittavassa kokonaisuudessa (organisaatiosi oma dokumentti tai tarvittaessa [VAHTI dokumentti](https://dvv.fi/vahti))
4. Liitä henkilötietojen käsittelyehdot tarjouspyyntöön

## Vuoropuhelu toimittajien kanssa

1. Varmista, että ehdottomat vaatimukset on huomioitu jo tarjouspyyntövaiheessa
2. Huomioi tarveharkinnan mukaisesti hankinnassa täydentävät ehdot/ lisäehdot
	* voit esimerkiksi hyödyntää [Kyberturvallisuuskeskuksen julkaisemia hankintamateriaaleja lisäehtojen määrittelyssä](https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja)

## Tarjousten käsittely

1. Tietosuojan tason arviointi
	* Tarjouksen tekijän toimittaman dokumentaation läpikäynti
	* Arvioi, vaikuttaako tarjouksen tekijä sellaiselta, joka pystyy noudattamaan tietosuojasäännöksiä asianmukaisesti? Vain sellaisia henkilötietojen käsittelijöitä saa käyttää, jotka pystyvät täyttämään tietosuoja-asetuksen vaatimukset ja varmistamaan rekisteröidyn oikeuksien toteutumisen.
2. Laadi tarvittaessa vaikutustenarviointi
	* + Laadi organisaatiosi ohjeiden mukaisesti vaikutustenarviointi.
		+ Osallista henkilötietojen käsittelijä mukaan vaikutustenarvioinnin laatimiseen
		+ Konsultoi tarvittaessa tietosuojavastaavaa ja pyydä ohjausta

## Kilpailun jälkeen

1. Tee tarvittavat sopimukset ja varmista sujuva yhteistyö tietosuoja-asioissa.
2. Varmista, että henkilötietojen käsittelijä on nimennyt yhteyshenkilön tietosuoja-asioihin liittyen
3. Varmista, että vaikutustenarviointi on laadittu
4. Tarkista, että voiko henkilötietoja luovuttaa tietopyynnön tehneelle?
* Käänny tietosuojavastaavan puoleen