VAHTI-hyvät käytännöt tukimateriaali

5.11.2021

**Sisäänrakennetun ja oletusarvioisen tietosuojan periaatteiden läpikäynti hankinnoissa**

Sisällysluettelo

[1 Yleistä 3](#_Toc87032051)

[2 Sisäänrakennetun ja oletusarvioisen tietosuojan periaatteiden läpikäynti 4](#_Toc87032052)

# Yleistä

Tämä asiakirja on tarkoitettu vapaasti hyödynnettäväksi ja sovellettavaksi tukimateriaalina tietosuojan huomioimiseksi hankinnoissa. 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.

# Sisäänrakennetun ja oletusarvioisen tietosuojan periaatteiden läpikäynti

* + 1. Läpinäkyvyys
			- Onko kaikki käsittelytoimet kuvattu tarpeeksi selkeästi, niin että kaikki käsittely on kerrottavissa selkeästi rekisteröidyille?
			- Esim. julkiset Tietosuojailmoitukset tai käsittelytoimien kuvaukset siitä miten tietoja käsitellään. Toimittaako toimittaja nämä vai tuleeko hankintaa tekevän tehdä ne itse?
		2. Käyttötarkoitussidonnaisuus
			- Mitä teknisiä tai muita menetelmiä on käytössä, joilla varmistetaan, ettei tietoja käytetä muihin tarkoituksiin
			- Esim. toimittajan omat tarkoitukset, tuotekehitys, testaaminen ja niihin käytettävät työmenetelmät ja niiden kuvaukset
		3. Tietojen minimointi
			- Miten varmistutaan siitä, että ei kerätä sellaisia tietoja, joita ei tarvita käyttötarkoitukseen
			- Onko tiedot helposti poistettavissa järjestelmistä käyttäjän omin toimin, ohjaako järjestelmä tai palvelu keräämään vain tarpeellisia tietoja, jne?
		4. Täsmällisyys
			- Onko tarpeen varmistaa erityisesti tietojen täsmällisyyttä ja miten ne järjestelmässä huomioidaan?
			- Esimerkiksi automaattiset postitukset tai kuittaukset voivat vaatia sitä, että osoitetietoja tai yhteystietoja on tarkistettava säännöllisesti esimerkiksi väestörekisterikeskukselta tai rekisteröidyiltä suoraan. Onko tällaiseen automatiikkaa, vai vaatiiko se manuaalista työtä ja keneltä?
		5. Säilytyksen rajoittaminen
			- Henkilötietoja saa säilyttää vain niin kauan kuin käyttötarkoitus edellyttää.
			- Voidaan järjestelmän tai palvelun osalta käyttää teknistä automatiikkaa vanhentuneiden tietojen poistamiseen. Vaatiiko se manuaalityötä, jos niin keneltä?
		6. Eheys ja luottamuksellisuus
			- Onko tiedot yhdessä paikassa, rakenteisessa muodossa ja onko niistä riittävät varmuuskopiot
			- Onko salauksesta huolehdittu aina kun tietoja siirretään tai niiden loppusäilytyspaikassa. Jos, niin miten tämä on toteutettu?