



TIETOTURVAN JA TIETOSUOJAN PERUSASIOIDEN TARKASTUSLISTA HANKINNOISSA JA PROJEKTEISSA

Tämä tarkastuslista on laadittu yhteistyössä Espoon, Kuopion, Oulun ja Tampereen kaupunkien kanssa projekteja, vaatimusmäärittelyitä, hankkeita, sopimustekstejä yms. valmistelevien ja toteuttavien työntekijöiden avuksi. Kaikki listan kohdat eivät sovellu kaikkialle, koska esimerkiksi sopimuksia ei ole kaikissa projekteissa.

Normaalisti listan kaikista asioista pitäisi olla huolehdittu eli vastaus tarkastuslistan kohtiin pitäisi olla ”Kyllä”. Mahdollisia ”Ei” kohtia on syytä selvittää ja tarvittaessa kysyä lisätietoja tietoturva- ja tietosuoja-asiantuntijoilta tai selvittää asia organisaation ohjeistuksesta.

Projektin/hankinnan tmv. nimi:

Täyttäjän nimi, tehtävänimike ja yksikkö:

Pvm:

TIETOSUOJA		HUOM
1. Oletko selvittänyt liittyykö käsittelemääsi asiaan erityislainsäädäntöä, jossa säädetään erityisesti kyseiseen toimintaan liittyen henkilötietojen käsittelystä?	Kyllä Ei	
2. Oletko kartoittanut tietosuojaan (henkilötietojen käsittelyyn) liittyvät riskit, tehnyt riittävät riskienhallintatoimenpiteet ja laatinut riskeihin liittyen varautumissuunnitelmat? Tämä on erityisen tärkeää isorisessä henkilötietojen käsittelyssä. Lisätietoa löydät EU:n yleisestä tietosuoja-asetuksesta (2016/679) ja siihen liittyvästä ohjauksesta.	Kyllä Ei	
3. Oletko varmistanut, että palveluntuottaja pystyy erottelemaan teknisesti omaksi loogiseksi osarekisterikseen kaupungin/rekisterinpitäjän henkilö- ja asiakastiedot ja palveluntuottamisen päättyessä pystyy tarvittaessa luovuttamaan tiedot meille takaisin ja hävittämään ne sovitusti itseltään? Tämä on tärkeää, jos palveluntuottaja käyttää omia tietojärjestelmiään rekisterinpitäjän henkilö/asiakastietojen hallinnassa.	Kyllä Ei	
4. Oletko huomionnut, että jos palvelussa/toiminnassa muodostuu kokonaan uusi henkilörekisteri, pitää siitä laatia tietosuojaseloste (rekisterinpitäjän informaatio rekisteröidylle), joka pitää olla rekisteröidyn saatavilla (esimerkiksi julkaista internetsivuilla)?	Kyllä Ei	
5. Oletko hankkeessasi analysoinut ja laatinut kuvauksen henkilötietojen käyttöön liittyvistä toimintaprosesseista?	Kyllä Ei	
6. Onko hankkeessa huolehdittu henkilötietoja käsittelevän henkilökunnan kouluttamisesta henkilötietojen oikeaoppiseen käsittelyyn?	Kyllä Ei	

Tietoturva	Huom
7. Onko hankkeessasi tietojen turvalliseen käsittelyyn, säilytykseen, varmuuskopiointiin ja hävittämiseen olemassa tarvittavat välineet ja toimintatavat (prosessit)?	Kyllä Ei
8. Onko varmistettu, että käytettävään tietojärjestelmään tai tietoihin ei pääse käsiksi ilman asianmukaista käyttöoikeutta?	Kyllä Ei
9. Oletko huomionnut, että pääsääntöisesti kaikissa tietojärjestelmissä pitää vaatia käytettäväksi henkilökohtaista käyttäjätunnusta ja salasanaa tai muuta vahvaa tunnistamista?	Kyllä Ei
10. Lokitiedot: Oletko varmistanut, että hankittava järjestelmä mahdollistaa henkilötietojen käsittelyn osalta jälkikäteen todentamisen, kuka on katsonut, lisännyt tai poistanut tietoja järjestelmästä, milloin tämä on tapahtunut, miltä tietokoneelta ja mihin tietoihin toimenpide on kohdistunut? Huom! SOTE-palveluissa lakisääteistä.	Kyllä Ei
11. Oletko varmistanut, että käyttöoikeuden (myös pääkäyttäjäoikeudet) saaminen järjestelmään tai sen muuttaminen edellyttää kirjallista pyyntöä ja järjestelmän käyttöoikeudet vastaavat käyttäjän työtehtävien mukaisia tarpeita päästä järjestelmään?	Kyllä Ei
12. Onko toimeksiantosopimuksessa veloitettu, että tietojärjestelmien käyttöoikeudet poistetaan tai niitä muutetaan, jos henkilö jää pois ulkoisen palveluntuottajan palveluksesta tai hänen työtehtävänsä muuttuvat?	Kyllä Ei
13. Oletko varmistanut, että pääsy ohjelmointiympäristöön tai koko järjestelmää koskeviin asetuksiin on rajoitettu ja sen käyttö on valvottu?	Kyllä Ei
14. Oletko varmistanut, että palvelun ja siihen liittyvän tietotekniikan riskienhallinnasta ja sen suunnittelusta huolehditaan ja kuka sen tekee? (Onko esim. tietojärjestelmiä varten varajärjestelmät sekä jatkuvuus- ja toipumissuunnitelmat olemassa?)	Kyllä Ei
15. Onko varmistettu, että tietoliikenteessä käytetään vain turvallisia yhteyksiä ja niiden kapasiteetti ja käytettävyydet ovat riittävät (esim. www-sovelluksessa pitää olla https käytössä, jos järjestelmään kirjaudutaan käyttäen salasanaa tai järjestelmällä käsitellään salassa pidettäviä tietoja)?	Kyllä Ei
16. Oletko varmistanut, että käytettävien palvelimien ja muiden laitteiden tietoturvasuudesta (mm. päivitykset ja haittaohjelmien torjunta) huolehditaan?	Kyllä Ei
17. Oletko varmistanut, että on määritelty, mitä muita välineitä kuin sähköisiä tietojärjestelmiä (paperitulosteita, CD-ROM/DVD-levyjä, USB-tikkuja tms.) käytetään henkilötietojen tallentamiseen tai siirtämiseen ja kuinka niiden suojaamisesta ja arkistoinnista sekä tietoturvalisistä hävittämisestä huolehditaan?	Kyllä Ei
18. Oletko varmistanut, että järjestelmästä ei oteta tarpeettomasti paperisia tulosteita ja että järjestelmästä otettavien tulosteiden käsittelystä on annettu riittävät ohjeet ja määräykset? (Kaiken tietosuojattavan jätteen hävityksen on oltava kunnossa!)	Kyllä Ei

SOPIMUKSET JA ULKOPUOLINEN PALVELUNTARJOAJA	HUOM
19. Jos kyseessä on toimeksiantosopimus, niin onko siinä määritelty, mitä eri henkilörekistereitä toiminnassa ylläpidetään ja minkälaisia henkilötietoja käsitellään?	Kyllä Ei
20. Onko sopimuksessa määritelty selvästi, kuka on lain tarkoittama rekisterinpitäjä ja mitkä ovat rekisterinpitäjän velvollisuudet? Huom! On tärkeää erottaa juridinen rekisterinpitäjä (data controller) ja käsittelijä (data processor), joka käyttää tietoja toimeksiantajan lukuun.	Kyllä Ei
21. Oletko varmistanut, että mikäli kyseessä on henkilötietojen käsittelyn ulkoistaminen, pitää sopimuksella varmistaa EU:n yleisen tietosuoja-asetuksen (2016/679) velvoitteiden noudattaminen "kuten henkilötietojen käsittelyyn liittyvien ehtojen sopiminen kirjallisesti?"	Kyllä Ei
22. Oletko varmistanut, että jos sosiaalihuollon palveluntuottaja käyttää palvelun toteuttamiseksi alihankkijaa, on sen varmistuttava siitä, että alihankkijana toimiva palveluntoteuttaja noudattaa sosiaalihuollon asiakastietojen käsittelyssä sosiaalihuollon asiakasasiakirjoista annetun lain (254/2015) 25 §:n 1 momentissa tarkoitettua sopimuksen ehtoja ja 24 §:n 3 momentissa säädettyjä velvoitteita?	Kyllä Ei
23. Oletko varmistanut sopimusteitse, että henkilötietoja ei käytetä muuhun kuin hankkeessasi määriteltyyn tarkoitukseen (esimerkiksi ulkoisen palveluntuottajan tekemään kaupalliseen mainontaan)?	Kyllä Ei
24. Onko sopimuksessa määritelty mahdollisuus auditoida tai käyttää kolmatta osapuolta auditoimassa ulkoisen palveluntuottajan toimintaa henkilötietojen käsittelyn oikeellisuudesta ja tietoturva-asioiden toteutuksesta?	Kyllä Ei
25. Onko sopimuksessa määritelty rahallinen sanktio mahdollisten tietovuotojen osalta?	Kyllä Ei
26. Onko Tietojen ja tietojärjestelmien käyttö- ja salassapitositoumukset tehty ulkopuolisen toimijan työntekijöiden kanssa ja niiden sisältö ja merkitys selvitetty? Tai onko vastaavat asiat edellytetty sopimuksessa ja sopimuksessa velvoitettu toinen osapuoli huolehtimaan työntekijöidensä perehdytyksestä ja sitoumuksien ottamisesta?	Kyllä Ei
27. Oletko varmistanut sopimuksessa, että kaupungin tietosuojaan ja tietoturvaan liittyvät yhteyshenkilöt saavat viivyttämättä tiedon palveluun tai sen tietotekniikkaan liittyvistä tietoturva- ja tietosuojapoikkeamista/häiriöistä/ongelmista (esim. tietovuodot, hakkeroinnit, toteutuneet merkittävät riskit yms.)?	Kyllä Ei
28. Onko hankkeeseesi liittyen esim. ulkopuolisen palveluntuottajan työntekijöitä ohjeistettu, että henkilötietoja tai muuta salassa pidettävää tietosisältöä ei välitetä suojaamattomana internetin yli esimerkiksi sähköpostilla, ellei tietojen riittävästä salaamisesta ole huolehdittu?	Kyllä Ei
29. Oletko huolehtinut, että palveluntuottajilla pitää olla nimetty yhteyshenkilö tietosuoja-asioihin ja mahdollisiin epäkohtiin pitää välittömästi puuttua?	Kyllä Ei
30. Onko hankkeesi hankintoihin liitetty asiantuntijoiden kanssa laaditut vaatimusmäärittelyt tietoturvasta ja tietosuojasta?	Kyllä Ei

Lisätietoja:

- Oman organisaatiosi tietoturva- ja tietosuojaohjeet
- (VAHTI) ohjeet <https://www.vahiohje.fi/>
- Hankintoihin liittyviä ohjeita ja valmiita sopimusliitemalleja löytyy osoitteesta <https://www.hankinnat.fi/>
- Henkilötietojen käsittelyn ratkaisuja löytyy tietosuojavaltuutetun toimiston sivuilta <https://www.tietosuoja.fi/>