HENKILÖTIETOJEN KÄSITTELYN TARKASTUSLISTA
(esimerkiksi ostopalvelusopimuksissa)

Tämä henkilötietojen käsittelyyn liittyvien perusasioiden tarkastuslista on laadittu eri projekteissa työskentelevien sekä sopimustekstejä laativien työntekijöiden avuksi helpottamaan henkilötietojen oikeaoppisen käsittelyn huomioimista. Lisäksi tarkastuslistasta on apua varmistettaessa, että hankittavissa tai käytettävissä tietojärjestelmissä on huomioitu tietoturvan ja tietosuojan peruslähtökohdat.

1. Onko hankkeessa/sopimuksessa määritelty, mitä eri henkilörekistereitä toiminnassa ylläpidetään ja minkälaisia henkilötietoja käsitellään?	☐ Kyllä ☐ Ei
2. Onko sopimuksessa määritelty selvästi, kuka on henkilötietolain tarkoittama rekisterinpitäjä ja mitkä ovat rekisterinpitäjän velvollisuudet ja mitä ovat toimeksisaajan velvollisuudet?	☐ Kyllä ☐ Ei
3. Sopimustyyppejä on erilaisia. Oletko huolehtinut, että heti sopimuksen alussa selviää, onko kyseessä esimerkiksi toimeksiantosopimus, jossa palveluntuottaja toimii toimeksiantajan (=tilaajan) lukuun?	☐ Kyllä ☐ Ei
4. Oletko tietoinen, että palveluntuottaja voi olla tekninen rekisterinpitäjä eli ylläpitää ja käyttää toimeksiantajan henkilörekistereitä tilaajan lukuun siinä laajuudessa, kun sopimuksessa määritellyt tehtävät edellyttävät?	☐ Kyllä ☐ Ei
5. Oletko varmistanut, että palveluntuottaja pystyy erottelemaan teknisesti omaksi loogiseksi osarekisterikseen toimeksiantajan henkilö- ja asiakastiedot ja palveluntuottamisen päättyessä pystyy tarvittaessa luovuttamaan tiedot meille takaisin ja hävittämään ne itseltään?	☐ Kyllä ☐ Ei
6. Oletko varmistanut, että henkilötietoja ei käytetä muuhun kuin hankkeessasi määriteltyyn tarkoitukseen (ei esimerkiksi mainontaan tai ulkopuolisen palveluntuottajan omaan toimintaan)?	☐ Kyllä ☐ Ei
7. Oletko huomioinut, että jos palvelussa/toiminnassa muodostuu kokonaan uusi henkilörekisteri, pitää siitä laatia henkilötietolain tarkoittama rekisteriseloste ja se pitää olla rekisteröidyn saatavilla (esimerkiksi julkaista internetsivuilla)?	☐ Kyllä ☐ Ei
8. Oletko hankkeessasi analysoinut ja laatinut kuvauksen henkilötietojen käyttöön liittyvistä toimintaprosesseista?	☐ Kyllä ☐ Ei
9. Onko hankkeessa huolehdittu henkilötietoja käsittelevän henkilökunnan kouluttamisesta erityisesti tietosuojaan liittyvissä asioissa?	☐ Kyllä ☐ Ei
10. Oletko huolehtinut henkilötietojen käsittelyn valvonnasta ja onko sopimuksessa määritelty tilaajan mahdollisuus auditoida tai käyttää kolmatta osapuolta auditoimassa palveluntuottajan toimintaa henkilötietojen käsittelyn oikeellisuudesta ja tietoturva-asioiden toteutuksesta?	☐ Kyllä ☐ Ei
11. Onko sopimuksessa määritelty rahallinen sanktio mahdollisten tietovuotojen osalta?	☐ Kyllä ☐ Ei
12. Onko käyttö- ja salassapitositoumukset tehty työntekijöiden kanssa ja niiden sisältö ja merkitys selvitetty?	☐ Kyllä ☐ Ei
13. Onko tietojen turvalliseen käsittelyyn, säilytykseen, varmuuskopiointiin ja hävittämiseen olemassa tarvittavat välineet ja toimintatavat (prosessit)?	☐ Kyllä ☐ Ei
14. Oletko varmistanut sopimuksessa, että sopimuksen tietosuojaan ja tietoturvaan liittyvät yhteyshenkilöt saavat viivyttelemättä tiedon palveluun tai sen tietotekniikkaan liittyvistä tietoturva- ja tietosuojapoikkeamista/häiriöistä/ongelmista (esim. tietovuodot, hakkeroinnit, toteutuneet merkittävät riskit yms.)?	☐ Kyllä ☐ Ei
15. Onko varmistettu, että käytettävään tietojärjestelmään ei pääse ilman asianmukaista valtuutusta?	☐ Kyllä ☐ Ei
16. Oletko huomioinut, että pääsääntöisesti kaikissa tietojärjestelmissä pitää vaatia käytettäväksi henkilökohtaista käyttäjätunnusta ja salasanaa tai muuta vahvaa tunnistamista?	☐ Kyllä ☐ Ei
17. Käyttölokitiedot: Onko mahdollista jälkikäteen todeta, kuka on katsonut, lisännyt tai poistanut tietoja järjestelmästä, koska tämä on tapahtunut, miltä tietokoneelta ja mihin tietoihin toimenpide on kohdistunut? Pääsääntöisesti käyttölokitiedot pitää olla saatavilla.	☐ Kyllä ☐ Ei
18. Onko tietojärjestelmän käyttöoikeudet rajattu vain työtehtävissä tarvittaviin tietoihin?	☐ Kyllä ☐ Ei

19. 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
20. Oletko velvoittanut, että tietojärjestelmien käyttöoikeudet poistetaan tai niitä muutetaan, jos henkilö jää pois palveluntuottajan palveluksesta tai hänen työtehtävänsä muuttuvat?	☐ Kyllä ☐ Ei
21. Onko työntekijöitä ohjeistettu, että henkilötietoja tai muuta salassa pidettävää tietosisältöä ei välitetä suojaamattomana internetin yli esimerkiksi sähköpostilla, ellei tietojen riittävästä salaamisesta ole huolehdittu?	☐ Kyllä ☐ Ei
22. Oletko varmistanut, että pääsy ohjelmointiympäristöön on rajoitettu ja sen käyttö on valvottu?	☐ Kyllä ☐ Ei
23. 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
24. Onko varmistettu, että tietoliikenteessä käytetään vain turvallisia yhteyksiä ja niiden kapasiteetti ja käytettävyys ovat riittävät (tehty esim. selvitys)?	☐ Kyllä ☐ Ei
25. Oletko varmistanut, että käytettävien palvelimien ja työasemien tietoturvallisuudesta (mm. virustorjunta ja päivitykset) huolehditaan?	☐ Kyllä ☐ Ei
26. Oletko varmistanut, että on määritelty, mitä muita välineitä kuin sähköisiä tietojärjestelmiä (paperitulosteita, CD-ROM/DVD-levyjä, USB-tikkuja, magneettinauhoja tms.) käytetään henkilötietojen tallentamiseen tai siirtämiseen ja kuinka niiden suojaamisesta ja arkistoinnista sekä hävittämisestä huolehditaan?	☐ Kyllä ☐ Ei
27. 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
28. Oletko varmistanut sopimusneuvotteluissa ja sopimuksissa, että toimeksiantaja edellyttää palveluntuottajan toimimaan voimassaolevan lainsäädännön ja tilaajan ohjeiden mukaisesti henkilötietojen käsittelyssä eikä palveluntuottaja saa luovuttaa mitään tilaajan omistamia tietosisältöjä ilman lupaa eteenpäin esimerkiksi alihankkijoilleen?	☐ Kyllä ☐ Ei
29. Oletko huolehtinut, että palveluntuottajalle on ilmoitettu tilaajan tietoturvaan ja tietosuojaan sekä rekisterinpitoon liittyvät yhteyshenkilöt?	☐ Kyllä ☐ Ei
30. Oletko huolehtinut, että palveluntuottajilla pitää olla nimetty yhteyshenkilö tietosuoja-asioihin ja mahdollisiin epäkohtiin pitää välittömästi puuttua?	☐ Kyllä ☐ Ei