



Tietosuojaohje

Mitä tietosuojasta tulee tietää julkisissa hankinnoissa

Tekijät:

Eeva-Riitta Högnäs Julkisten hankintojen neuvontayksikkö

Susan Hindström valtiovarainministeriö

Haastatellut organisaatiot:

Lapinjärven kunta, Työterveyslaitos ja Satakunnan hyvinvointialue

Julkaistu 10 / 2024

1. Johdanto	3
2. Tietosuoja sääntelyn roolit julkisessa hankinnassa	4
3. Mitä ovat henkilötiedot julkisessa hankinnassa?	6
4. Hankintayksikön henkilötiedon maantieteellinen sijainti	8
5. Tietosuoja hankintamenettelyssä	10
5.1. Tietosuoja hankinnan valmistelussa	10
5.2. Tietosuoja hankintamenettelyssä	12
5.2.1. Hallinnolliset ja toiminnalliset vaatimukset	12
5.2.2. Tietosuoja sopimusluonnos	13
5.2.3 Sopimusneuvottelut	15
5.2.4 Tietosuojan arviointi useissa hankinnoissa samalta toimittajalta	15
6. Tietosuoja hankinnan sopimuskaudella	16
7. Hankintoja koskeva tietosuoja seloste	17
Hyödyllisiä linkkejä	18

1. Johdanto

Tämä ohje on tarkoitettu hankintojen tekijän tueksi tietosuoja-asioiden ymmärtämiseksi. Tietosuojan tavoitteena on varmistaa, että yksityisten henkilöiden tietoja käsitellään lainsäädännön vaatimusten mukaisesti ja läpinäkyvästi. Oikeudellisen sääntelyn avulla toteutetaan henkilötietojen sallitun käsittelyn rajat ja edellytykset.

Euroopan unionin yleisessä tietosuoja-asetuksessa (GDPR, General Data Protection Regulation) säädetään tietosuojasta. Kansallinen tietosuojalaki (1050/2018) täydentää ja täsmentää EU:n yleistä tietosuoja-asetusta ja sitä sovelletaan yleisen tietosuoja-asetuksen rinnalla. Yleinen tietosuoja-asetus on suoraan sovellettavaa oikeutta ja se koskee kaikkia rekisterinpitäjiä ja käsittelijöitä, jotka käsittelevät henkilötietoja.

Ohje ei huomioi kaikkia tietosuoja-asetuksen velvoitteita tai riskejä taikka kerro tietosuoja-asetuksen mahdollistamista yksityishenkilön oikeuksista. Tämän ohjeen ja kilpailutuksesta vastaavan hankinta-asiantuntijan hankintaan liittyvän arvion lisäksi saattaa yksittäistapauksissa olla aiheellista konsultoida asiantuntijaa, joka nimenomaisesti on perehtynyt tietosuojasääntelyyn.

Ohjeen lähtökohta on julkisissa hankinnoissa yleisin tilanne, jossa hankintayksikkö toimii rekisterinpitäjänä ja toimittaja toimii tietojen käsittelijänä. Rekisterinpitäjänä toimiminen tarkoittaa yksinkertaistettuna, että henkilötiedot ovat hankintayksikön keräämiä tai saamia ja tallentamia, ja tiedot annetaan jonkinlaisesta

rekisteristä toimittajalle. Toimittajan rooli on kuitenkin arvioitava hankintakohtaisesti. Mikäli toimittajan rooli hankinnan toteuttamisessa on monitahoisempi, aiheesta tulee konsultoida tietosuoja-asiantuntijaa.

Tietosuojalainsäädäntö perustuu yksityishenkilön (rekisteröidyn) oikeuteen omin tietoihinsa. Julkisen hankinnan tekijä harvemmin päätyy kosketuksiin yksityishenkilöiden tietopyyntöjen tai tietojen kanssa, joten tämä ohje ei käsittele yksityishenkilön asemaa tietosuojan näkökulmasta.

Ohje on kirjoitettu oletusarvoisesti palveluhankintojen näkökulmasta. Tästä huolimatta ohjetta voi soveltaa myös urakka- tai tavarahankinnoissa. Lisäksi hankintakohtaisesti on otettava huomioon muu sääntely esimerkiksi asiakastiedoista. Esimerkiksi sosiaali- ja terveydenhuollon hankinnoissa on erikseen varmistettava asiakastiedon oikea käsittely, eli salassapito, kirjaamiskäytännöt ja käyttöoikeudet, sekä käsittelyyn käytettävien järjestelmien tietoturva.

2. Tietosuojasääntelyn roolit julkisessa hankinnassa

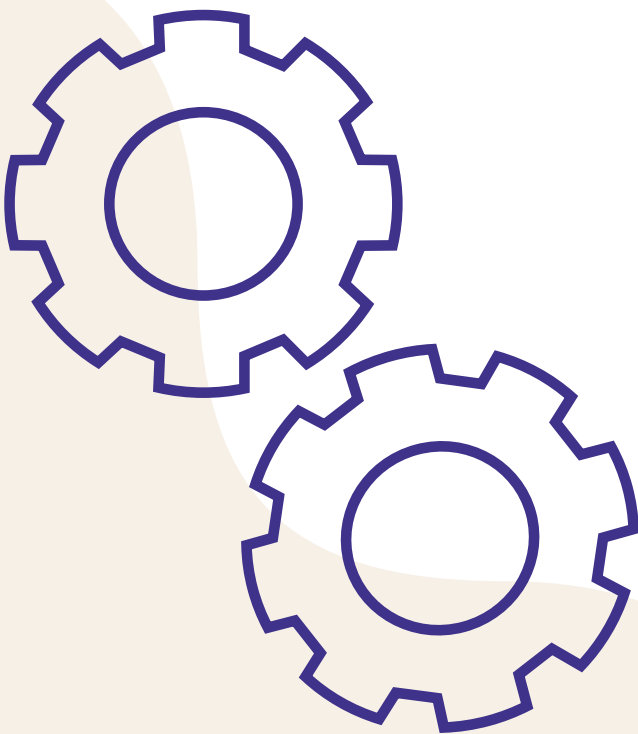
Julkisen hankinnan sopimusoapuolet ovat hankintayksikkö tilaajana ja toimittaja palveluntuottajana. Tietosuojalainsäädännön osapuolet ovat rekisterinpitäjä ja tietojen käsittelijä. Nämä roolit asettuvat useimmiten selkeästi yhteen hankintayksikön ollessa rekisterinpitäjä ja toimittajan toimiessa tietojen käsittelijänä.

Rekisterinpitäjänä hankintayksikkö:

- Antaa toimittajalle henkilötietoja, joita sen on saatava tuottaakseen tilatun palvelun
- Määrittää tietoisesti hankinnan kohteen rajataakseen tietojen antamisen ja käsittelyn välttämättömyyden
- Määrää, mitä tiedoilla saa tehdä, mihin niitä saa käyttää ja kuinka kauan.
- Määrittelee käsittelyn sisällön sopimuksella tai muualla asiakirjalla, esim. vakiosopimuslausekkeet.

Tietojen käsittelijänä toimittaja:

- Vastanottaa välttämättömät henkilötiedot rekisterinpitäjältä
- Noudattaa tietojen käsittelyssä yleistä tietosuoja-asetusta sekä hankintayksikön ohjeita
- Hävittää henkilötiedot, kun se ei enää tarvitse niitä palvelun tuottamiseksi.

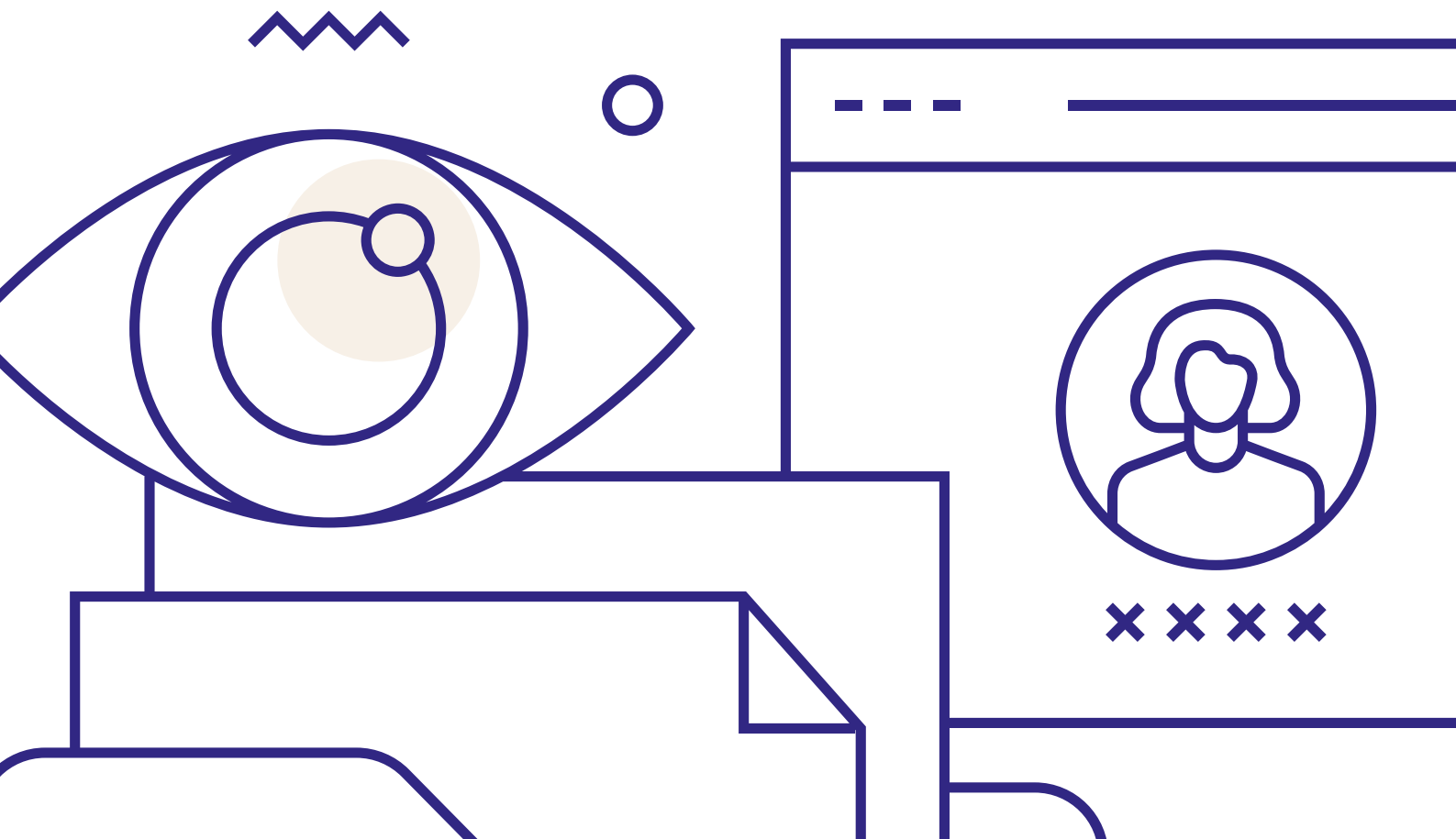


Rekisterinpitäjän eli hankintayksikön rooli henkilötietojen osalta on keskeinen. Julkisen hankinnan tarjouspyynnössä hankintayksikkö määrittelee henkilötietojen käsittelyn laajuuden ja keston. Rekisterinpitäjä kantaa vastuun siitä, että sen rekisteristä lähtöisin olevia henkilötietoja käsitellään asianmukaisesti. Jos henkilötiedoille tapahtuu jotakin (esim. tietovuoto), hankintayksikkö on rekisterinpitäjänä vastuussa seurauksista.

Palveluntuottaja on hankinnoissa useimmiten tietojen käsittelijän roolissa. Rooli on sama riippumatta siitä, kenen omistamassa tai hallinnoimassa järjestelmässä henkilötietoja käsitellään. Palveluntuottaja toimii useimmiten henkilötietojen käsittelijänä, vaikka se tallentaisi tai käsittelee henkilötietoja omassa tai hankintayksikön järjestelmässä.

Mikäli toimittaja käyttää hankinnassa alihankintaa, on hankintakohtaisesti arvioitava alihankkijan rooli henkilötietojen näkökulmasta. Kussakin hankinnassa on arvioitava, tarvitseeko toimittajan alihankkijan käsitellä henkilötietoja päävastuullisen toimittajan lisäksi. Siten, vaikka toimittaja tarvitsisi tilaajan rekisteristä peräisin olevia henkilötietoja palvelun toteuttamiseksi, saattaa hankinta olla mahdollista suunnitella siten, että toimittajan alihankkijan ei tarvitse niitä käsitellä. Tämä tulee ottaa huomioon hankinnan kohdetta määriteltäessä.

Mikäli alihankkijan on tarpeen käsitellä palvelun tuottamisessa tilaajan henkilötietoja, on toimittajan varmistuttava sopimusteitse, että alihankkija käsittelee tilaajan henkilötietoja ainoastaan hankintayksikön määrittämässä laajuudessa ja ohjeiden mukaan. Toimittaja vastaa alihankkijan tietojen käsittelystä kuin omasta toiminnastaan.



3. Mitä ovat henkilötiedot julkisessa hankinnassa?

Organisaatiot, muiden ohella hankintayksiköt, keräävät ja käsittelevät paljon erilaisia yksityishenkilöihin liittyviä tietoja. Ne saattavat kerätä tietoa internetsivujensa kävijöistä, pitää yllä työntekijöihinsä liittyviä tietoja, järjestää tapahtumia, joista kerätään osallistujatietoja taikka tuottaa lakisääteisiä tai muita palveluita, joista kertyy asiakastietoa. Kaikista edellä mainituista henkilötietokokonaisuuksista kertyy henkilörekisteri. Rekisteri saattaa käytännössä olla esimerkiksi asiakastietojärjestelmän sisältö, tilaisuuteen osallistujista

koottu excel-tiedosto tai internetsivun seurantasovellus. Henkilötietorekisterin olemassaolosta, siihen kertyvistä tiedoista ja siitä, mihin tietoa käytetään hankintayksikön toiminnassa, tulee kertoa henkilöille, joiden tietoja kerätään. Tiedottaminen tapahtuu usein käsittelytoimista laaditun selosteen muodossa, joka löytyy esimerkiksi organisaation internetsivulta tai linkistä ilmoittautuessa tapahtumaan.

Henkilötieto on mikä tahansa tieto, joka voidaan kohtuullisella vaivalla yhdistää yksityishenkilöön.

Henkilötietoja ovat muun muassa:

- Nimi
- Henkilötunnus, käyttäjätunnus
- Sijaintitieto, osoite, sähköpostiosoite
- Valokuva
- Sormenjälki
- Verkkotunnistetieto (kuten IP-osoite)
- Fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä



Tietosuoja-asetus asettaa erityisen suojelun kohteeksi erityiset henkilötietoryhmät, eli tiedot, jotka ovat luonteeltaan erityisen arkaluonteisia ja joiden käsittely on lähtökohtaisesti kielletty. Tällaisia tietoja ovat esimerkiksi terveyteen, etniseen alkuperään, uskontoon tai seksuaalisuuteen liittyvät tiedot. Näiden tietojen käsittely on sallittua vain tietosuoja-asetuksessa (9 artikla) tarkasti rajatuissa tilanteissa. Tietyissä julkisen sektorin palveluissa on kuitenkin tarve ja peruste käsitellä tällaisia tietoja. Mikäli hankinnassa käsitellään erityisiä henkilötietoryhmiä, muiden ohella asiakastietoja asiakastietolain mukaisesti, tulee hankintayksikön kiinnittää erityistä huomiota sen varmistamiseen, että tietojen käsittelylle on olemassa tietosuoja-asetuksen mukainen peruste. Lisäksi tulee kiinnittää huomiota tietojen käsittelyn rajoittamiseen sekä käsittelijän ohjeistukseen.

Julkisessa hankinnassa olennainen henkilötieto on tieto, jota toimittaja tarvitsee palvelun tuottamiseen, ja jonka käytöstä hankintayksikkö toimittajaa ohjeistaa. Yleensä kyse on suoraan hankintayksikön henkilökisteristä annettavasta tiedosta, eli tiedosta, jonka hankintayksikkö lähettää jossakin tiedosto- tai muussa muodossa sopimuskauden alettua toimittajalle. Kysymys voi myös olla henkilötiedoista, joita toimittaja kerää hankintayksikön puolesta. Tällöin hankintayksikön ja toimittajan tulee tehdä tietojen käsittelystä tietosuojasopimus.

Jos hankinnassa ei liiku tietoa hankintayksikön rekisteristä toimittajalle tai toimittaja ei muutoin esimerkiksi itse kerää henkilötietoja hankintayksikön puolesta, ei tietosuoja ole tarpeen huomioida hankinnassa.

Jos hankinnassa ei anneta erityisesti tietoa henkilökisteristä, mutta toimittaja näkee sopimusyhteistyössä sopimusyhteyshenkilön ja tämän kahden kollegan sähköpostiosoitteen hankintaa koskevissa sähköposteissa, tuleeko tietosuojasopimus tehdä?

Ei tarvitse. Kysymyksessä ei ole henkilötieto, jonka hankintayksikkö on rekisterinpitäjänä kerännyt tiettyyn tarkoitukseen.



4. Hankintayksikön henkilötiedon maantieteellinen sijainti

EU:n tietosuoja-asetus on yhtenäistänyt Euroopan talousalueen (ETA-alue) tietosuojasääntelyn. Siten kaikki EU- ja ETA-maat soveltavat samaa tietosuojasääntelyä, ja tietojen käsittelystä sopiminen tällä maantieteellisellä alueella on yhdenmukaista. Tämä tarkoittaa sitä, että toimittajan tai tämän alihankkijan sijainti esimerkiksi toisessa EU-maassa ei muodosta erityistä riskiä, johon erikseen olisi reagoitava.

Sähköisten tietojen käsittelyssä hankalaa on kuitenkin se, että vaikka hankintayksikön sopimustoimittaja on sijoittunut esimerkiksi Irlantiin tai Viroon, tiedot saattavat tietoverkkoja pitkin liikkua ETA-alueen ulkopuolelle.

Hankintayksikön tulee hankintaa suunnitellessaan tiedostaa, missä hankinnan kohdetta toimittavat toimittajat maantieteellisesti käsittelevät henkilötietoja. Tämä selviää esimerkiksi markkinavuoropuhelun avulla. Mitä kriittisempi hankinta on kyseessä ja mitä arkaluontoisempia tietoja hankinnassa käsitellään, sitä kriittisemmin hankinnan kohteen suunnittelussa tulee suhtautua tietojen käsittelyyn ETA-alueen ulkopuolella. Käsittely ETA-alueen ulkopuolella on toki sallittua perustellusta syystä ja erillisen sopimuskirjoituksen perusteella.

Hankinnassa voidaan oletusarvoisesti edellyttää, että hankintayksikön tietoja käsitellään ETA-alueella, tai toisin sanoen, että tietoja ei saa käsitellä ETA-alueen ulkopuolella. Hankintayksikön tulee kuitenkin varmistaa, että markkinalla on tarjoajia, jotka täyttävät vaatimuksen.



Esimerkiksi markkinavuoropuhelussa hankintayksikön on aiheellista selvittää, missä hankintayksikön rekisterin henkilötietoja tullaan käsittelemään. Termi ”tietojen käsittely” saattaa antaa virheellisen kuvan siitä, että ETA-alueen ulkopuolinen tietojen käsitteleminen toimittajan toimesta olisi jollakin tavoin aktiivinen toimi. Pelkästään se, että toimittajan organisaatiossa joku voi potentiaalisesti päästä käsiksi hankintayksikön henkilörekisteristä peräisin olevaan tietoon ETA-alueen ulkopuolella johtaa siihen, että ETA-alueen ulkopuolisesta tietojen käsittelystä tulee erikseen sopia toimittajan kanssa ja käsittelyn asianmukaisuus varmistaa.

Tietojen ”käsittelyllä” tarkoitetaan mm. toimintoja, joita kohdistetaan henkilötietoihin automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, säilyttämistä, muokkaamista, hakua, kyselyä, katselua, käyttöä, tietojen luovuttamista siirtämällä, tietojen yhdistämistä tai tuhoamista.

Tietojen käsittelemisestä ETA-alueen ulkopuolella tulee erikseen sopia hankintayksikön ja tarjoajan välillä. Tämä johtuu siitä, että tietosuojan taso muissa kuin ETA-alueen maissa ei välttämättä vastaa EU:n tietosuoja-asetuksen tasoa. Siirron seurauksena yksityishenkilöiden (rekisteröityjen) tietojen suojaamisen taso

voi vaarantua. Henkilötietojen siirroille on lisäksi oltava tietosuoja-asetuksessa määritelty siirtooperuste. Siirtooperusteen tehokkuus ja täydentävien suojatoimien tarve on arvioitava tapauskohtaisesti, joten kilpailutuksesta vastaavan asiantuntijan on suositeltavaa konsultoida tietosuoja-asiantuntijaa jokaisesta ETA-alueen ulkopuolisesta tietojen siirrosta.

Tietosuoja-asetuksessa on määritelty siirtooperusteita, jonka perusteella tietojen käsittely on mahdollista ETA-alueen ulkopuolella. Siirtooperuste voi olla esimerkiksi Euroopan komission päätös tietyn valtion riittävästä tietosuojan tasosta. Tällaisia valtioita ovat esimerkiksi Iso-Britannia, Sveitsi, Japani ja Uusi-Seelanti. Toinen esimerkki siirtooperusteesta on hankintayksikön ja tarjoajan välillä allekirjoitettava sopimuspaketti, jota kutsutaan komission vakiolausekkeiksi. Vakiolausekkeitä voidaan käyttää sopimiseen yksinään tai hankintayksikön vakiotietosuojaehtojen lisäksi. Komission vakiolausekkeet ovat käyttäjälle raskas ja vaikeaselkoinen kokonaisuus siinä käytettävän tietosuojaterminologian vuoksi, joten sen käytössä suositellaan käytettävän asiantuntijaa myös hankinta-yksikön apuna.

Komission vakiolausekkeet (sopimus pohjat) ja niihin liittyvää tietoa löytyy [täältä](#).

5. Tietosuoja hankintamenettelyssä

5.1. Tietosuoja hankinnan valmistelussa

Kun kilpailutuksesta vastaava asiantuntija aloittaa hankinnan valmistelun, on suositeltavaa, että tämä rutiininomaisesti varmistaa hankinnasta vastaavalta substanssiosaajalta, käsitelläänkö hankinnassa henkilötietoja. Vaikka kilpailutuksesta vastaavan asiantuntijan tulee auttaa tunnistamaan hankinnat, joissa käsitellään henkilötietoja, vastuu tietosuojan toteutumisesta on kuitenkin lähtökohtaisesti substanssiosaajalla.

Annammeko henkilötietoja rekisteristämme palveluntarjoajalle?

Kerääkö palveluntarjoaja henkilötietoja pyynnöstämme osana palvelua?

Kilpailuttamisesta vastaavan asiantuntijan on myös tarpeen varmistaa henkilötietojen siirtämisen välttämättömyys. Toisinaan substanssiasiantuntija saattaa vastata yllä olevaan ensimmäiseen kysymykseen myöntävästi vanhasta tottumuksesta, kun niin on ennenkin saatettu tehdä. Tietosuojalainsäädäntö kuitenkin edellyttää, että henkilötietoja käsitellään vain, kun se on välttämätöntä. Siten kilpailutusasiantuntijan on aiheellista varmistaa tarpeen lisäksi myös käsittelyn kesto.

Onko tietojen antaminen toimittajalle välttämätön osa palvelun toteuttamista?

Mitkä ovat olennaiset ja välttämättömät henkilötiedot suhteessa hankinnan toteuttamiseen (ns. tietojen minimointi)?

Voidaanko henkilötiedon käsittelemistä rajoittaa ajallisesti esimerkiksi vain sopimuskauden alkuun, vai onko käsittely tarpeen koko sopimuskauden?



Mikäli hankinnan kohteena olevassa palvelussa käsitellään henkilötietoja, se tulee ottaa huomioon tarjouspyyntömateriaalin laatimisessa. Tarjouspyyntömateriaaliin tulee vähintäänkin liittää henkilötietojen käsittelysopimuksen tai sopimusliitteen luonnos. Tämän lisäksi on usein tarpeen, että hankintayksikkö asettaa myös henkilötietojen käsittelemiseen liittyviä pakollisia vaatimuksia.

Kilpailutuksesta vastaavan asiantuntijan on tärkeää osallistua hankintayksikön tietosuoja-asioiden toteutumiseen seuraavasti:

- Tunnistaa, käsitelläänkö hankinnassa henkilötietoja
- Varmistaa henkilötietojen käsittelyn välttämättömyys ja laajuuden raja
- Jos henkilötietoja liikkuu hankinnassa, liittää tarjouspyyntömateriaaliin organisaation tietosuojaa koskevat malliehdot
- Varmistaa, että substanssiasiantuntija on tarkistanut malliehtojen soveltumisen
- Varmistaa, että tietoturva-vaatimuksissa on huomioitu henkilötietojen riittävä suojaus, ellei näitä ole huomioitu jo hankintayksikön tietosuojaa koskevilla malliehdoissa.

Koska henkilötietojen käsittelyyn liittyvät ehdot tulevat osaksi hankinnan materiaaleja ja hankinnan vaatimuksia, kilpailutuksesta vastaavan tulee varmistua hankinnan muiden vaatimusten kaltaisesti, että henkilötietoja koskevat tulkinnat on tehty oikein. Tämän tulisi tapahtua yhteistyössä substanssiosaajan ja tietosuojaosaajien kanssa. Kilpailutuksesta vastaavan ei luonnollisesti tarvitse tehdä päätöksiä tai ottaa kantaa epäselvissä tilanteissa henkilötietojen käsittelyn suhteen, mutta tämän tulee huomauttaa epäselvyyksistä. Henkilötietojen käsittelyyn liittyvien määrittelyjen ollessa epäselviä tai tulkinnanvaraisia, tulisi kilpailutuksesta vastaavan joko itse kysyä tai vastuuttaa substanssiasiantuntija kysymään tietosuojamäärittelyistä tietosuoja-asiantuntijalta.

Kysy henkilötiedoista - Varmista epäselvät - Liitä ehdot - Delegoi vastuu

Hankinnan kohteesta riippuen hankintayksikön saat-
taa olla aiheellista selvittää tarjoajien henkilötietojen-
käsittelyprosesseja tai henkilötietojen käsittelypaikkaa
(sijainti ETA-alueella). Hankintayksikön on hankinnan
kohteen määrittelyssään harkittava, voidaanko tieto-
jen sijainti rajoittaa ETA-alueelle, ja missä tilanteissa
tietojen siirto alueen ulkopuolelle on mahdollistetta-
va riittävän kilpailun aikaansaamiseksi hankinnassa.
Kilpailun lisäksi harkinnassa on otettava huomioon
ainakin myös henkilötietojen määrä ja luonne hankin-
nan kohteena olevassa palvelussa.

5.2. Tietosuoja hankintamenettelyssä

5.2.1. Hallinnolliset ja toiminnalliset vaatimukset

Jos hankinnan kohteena olevaan palveluun liittyy henkilötietojen käsittelyä, tarjouspyyntömateriaaliin on usein aiheellista sisällyttää pakollisia vaatimuksia tietoturvan ja tietosuojan toteuttamisesta. Vaatimusten laatiminen on usein substanssiasiantuntijan vastuulla, mutta organisaatiossa on hyvä laatia pohjat vaatimuksille, joita olisi helppo käyttää. Seuraavat vaatimusehdot ovat esimerkkejä mahdollisiksi vaatimuksiksi, joita tulee muokata organisaation tarpeiden ja hankinnan kohteen perusteella:

Järjestelmän tulee noudattaa ja mahdollistaa kaikkien rekisteröityjen oikeuksien toteuttaminen, kuten voimassa olevassa EU:n ja Suomen lainsäädännössä on määritelty.

Toimittajan käsittelyjärjestelmien ja palveluiden tulee varmistaa tehokkaasti henkilötietojen käsittelyn turvallisuus ja luottamuksellisuus.

Toimittajan tulee välittömästi toimittaa hankintayksiköille kaikki pyynnöt muuttaa, poistaa tai kieltää henkilötietojen käsittelyä. Hankintayksikön pyynnöstä toimittajan täytyy tukea hankintayksikköä rekisteröityjen toimittamien pyyntöjen täyttämisessä. Toimittaja ei itse vastaa näihin pyyntöihin.

Hankintayksikön omistamia henkilötietoja ei tule käyttää toimittajan omien palveluiden kehittämiseen tai testaamiseen tai muihin toimittajan omiin käyttötarkoituksiin.

Toimittajalla on kyvykkyys tarjota hankintayksikön tietosuojaseloste sekä ehdot hankintayksikön loppukäyttäjille sovitulla tavalla.

Toimittajan tulee dokumentoida kaikki sovitut ja toteutetut suojatoimet ja varmistaa, että kaikki dokumentit ovat ajan tasalla. Toimittaja ja hankintayksikkö arvioivat yllä mainitut tekniset ja organisaatiotason suojatoimet ja niiden riittävyyden säännöllisesti.

Toiminnallisten vaatimusten asettaminen tulee asettaa myös palveluntarjoajien kypsyystason mukaan. On selvää, että erityisten henkilötietoryhmien käsittely edellyttää edistyneempiä tietosuojavaatimuksia. On kuitenkin huomattava, että mitä pienempi tarjoajayritys on, sen tärkeämpää on asettaa aivan perustavanlaatuisiakin vaatimuksia henkilötietojen käsittelylle, jotta tarjoaja ymmärtää velvoitteensa. Esimerkiksi yksin toimivalla toiminimiyrittäjällä ei välttämättä ole tietoturvallisia järjestelmiä ennestään. Tällöin tietojen käsittelyn edellytykset saattaa olla tarpeen suunnitella eri tasolla kuin isompien yritysten kanssa toimiessa.

5.2.2. Tietosuoja sopimusluonnos

Hankintayksikön on suositeltavaa laatia luonnos henkilötietojen käsittelysopimukseksi tai henkilötietojen käsittelyä koskevaksi sopimusliitteeksi. Organisaatiokohtaiset sopimusmekanismit henkilötietojen käsittelyä edellyttävissä hankinnoissa harvoin vaihtelevat suuresti hankinnan kohteesta toiseen, vaikka tapauskohtainen arvio ehtojen soveltumisesta onkin tehtävä.

Sopimusehdot, jotka koskevat henkilötietojen käsittelyä kilpailutetussa hankinnassa, laitetaan tarjouspyynnön liitteeksi. Ne ovat olennainen osa hankinnan ehtoja, sillä toisinaan pelkät tietosuojaan liittyvät ehdot vaikuttavat tarjoajan päätökseen osallistua kilpailutukseen.

Tietosuojaa koskevissa sopimusehdoissa on yleensä kaksi osaa:

1. Pysyvät, melko muuttumattomat organisaatiossa tarpeellisiksi määritetyt ehtolausekkeet, mukaan lukien hankintayksikön ohjeet sen henkilötietojen käsittelemisestä.
2. Hankintakohtaisesti täytettävät kohdat, joissa määritellään, mitä tietoja juuri kyseisessä hankinnassa liikkuu sekä mihin tietoja saa käyttää ja milloin.

Pysyvissä ehtokohdissa määritetään usein:

- Osapuolten roolit (taho, joka on rekisterinpitäjä ja taho, joka on käsittelijä) ja rekisterinpitäjän lähtökohtainen vastuu lainsäädännön noudattamisesta
- Toimittajan velvollisuudet (toimittaja noudattaa yleisen tietosuoja-asetuksen vaatimuksia ja hankintayksikön ohjeita, on toteuttanut tarkoituksenmukaiset tekniset ja organisatoriset toimet henkilötietojen asianmukaiseksi käsittelemiseksi, nimeää tietosuojasta vastaavan henkilön, ilmoittaa hankintayksikölle pyynnöistä ja loukkauksista, avustamisvelvollisuus)
- Tilaajan velvollisuudet (ylläpitää ja tiedottaa ohjeista, nimeää tietosuojasta vastaavan henkilön)
- Henkilöstön ja alihankkijan tietosuojatietoisuuden varmistaminen ja vastuiden vyöryttäminen edelleen alihankkijalle, hankintayksikön lupa alihankkijan käyttöön
- Palvelun paikka
- Henkilötietojen käsittelyn päättyminen

Pysyvissä ehtokohdissa hankintayksikkö voi myös organisaatiokohtaisesti määrittää käytäntöjä esim. tietosuojaan liittyvien virhe- tai sopimusrikkomustilanteiden varalle erityisten purku- tai irtisanomisehtojen tai sopimussakkojen ja vahingonkorvauksen suhteen. Ehtoja käytettäessä tulee ottaa huomioon tarjoajien

halu tarjota hankinnassa, jos ehdot ovat poikkeuksellisen tiukkoja. Mikäli hankinnassa määriteltäisiin esimerkiksi purkuehto sopimusrikkomuksen tilanteessa, tulee hankintayksikön ennakolta pohtia, miten palvelu voidaan sopimuspurun jälkeen järjestää, mukaan lukien uudelleenkilpailutusaika. Hankintayksikön tulee

siten aina varmistaa varasuunnitelman olemassa olo tilanteessa, jossa se tiukasti vaatii tilaajamyönteisen sopimuksen noudattamista.

Pysyvissä ehtokohdissa voidaan ottaa myös kantaa mahdollisiin toimittajan yritysjärjestelyihin sopimuskaudella. Hankintasopimuksen muuttaminen yritysjärjestelytilanteessa on julkisista hankinnoista ja käyttö-oikeussopimuksista annetun lain (1397/2016) 136 §:n 2 momentin 4 kohdan mukaan usein mahdollista, ja arviointi tulee tehdä tapauskohtaisesti. Vaikka sopimuskumppanin vaihdos olisi sallittu sopimusmuutos, tietosuoja koskevissa ehdoissa voidaan sopia esimerkiksi tietosuojasopimuksen uudelleen neuvottelusta yritysjärjestelytilanteessa.

Käytännössä hankintakohtaisesti määritetyt yksityiskohdat voivat olla hankintayksikön sopimus pohjissa joko luetellen erilaiset vaihtoehdot, jolloin hankintaan soveltuvat valitaan esimerkiksi ruksimalla, tai kysymys voi olla avoimeksi jätetyistä täytettävistä sopimuskohdista.

Hankintasopimuksessa tulee sopia varsinaisen hankintasopimuksen ja sen liitteiden välisestä suhteesta, eli soveltamisjärjestyksessä. Tietosuojaliitteen tulisi olla soveltamisjärjestyksessä ensisijainen muihin liitteisiin nähden, kun sopimuksen tulkinnassa tulee epäselvyyttä tietosujanäkökulmasta. Asiasta voi kirjata sopimukseen esimerkiksi virkkeen: *”Jos sopimuksen liitteenä on Tietosuojasopimus/-liite, sovelletaan sitä ensisijaisesti muihin liitteisiin nähden.”*

Hankinnan kohteen substanssiasiantuntijan tulee osallistua tietosuojaehtojen **hankintakohtaisten** ehtojen määrittelyyn. Osaan täytetään esimerkiksi:

Henkilötietojen tyypit ja rekisteröityjen ryhmät

- » Täytettävään kohtaan täytetään, minkä henkilötietoryhmän tietoja käsitellään hankinnassa (esim. hankintayksikön työntekijät tai hankintayksikön asiakkaat) sekä mitä tietoja hankinnassa liikkuu (esim. työntekijän nimi ja käyttäjätunnus tai asiakkaan nimi, henkilötunnus ja kuva)

Henkilötietojen käsittelyn luonne ja tarkoitus

- » Täytettävään kohtaan täytetään, miksi ja miten toimittaja käsittelee henkilötietoja, esimerkiksi: ”Hankintayksikkö tilaa toimittajalta tietokoneiden asennuspalvelua, minkä vuoksi toimittajan on käsiteltävä hankintayksikön työntekijöiden tietoja tietokoneiden käyttäjäkohtaisen asennuksen loppuunsaattamiseksi.

Henkilötietojen käsittelyn kesto

- » Täytettävään kohtaan täytetään, kuinka kauan ja missä vaiheessa sopimuskautta toimittaja käsittelee henkilötietoja, esimerkiksi: ”Tietokoneiden asennuksen ajan, jonka jälkeen toimittaja tuhoaa henkilötiedot” tai ”Sopimuskauden ajan”.

Henkilötietojen käsittelyyn liittyvät erityiset riskit ja tarvittavat suojatoimet

- » Täytettävään kohtaan täytetään, mitä riskejä tilanteeseen liittyy, miten turvallisuustaso varmistetaan ja miten esim. estetään henkilötietojen väärinkäyttö tai lainvastainen pääsy tietoihin.

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivustolla on julkaistu tietosuojasopimus pohja sekä käsittelyliite pohja, joita hankintayksiköt voivat muokaten käyttää muun ohella hankinnoissaan. Vaihtoehtoisesti pohjia voi käyttää oman mallipohjan taustamateriaalina. Ohjeet löytyvät Digi- ja väestötietoviraston verkkosivujen otsikon Työkalut ja mallipohjat alta ("Tietosuojaliite" (docx, 5/2023) ja "Henkilötietojen käsittelytoimien kuvaus" (docx, 5/2023): <https://dvv.fi/digiturvajulkaisut>

Myös Julkisen hallinnon tietoturvallisuuden arviointikriteeristön (Julkri) suosituksissa otetaan lyhyemmin kantaa henkilötietojen käsittelyyn: Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) : Suositus ja kriteeristö - [Valto \(valtioneuvosto.fi\)](https://valtioneuvosto.fi)

5.2.3 Sopimusneuvottelut

Toisinaan tietosuoja-asiat nousevat sopimusneuvotteluissa erityisen keskustelun kohteeksi. Toimittajan organisaatiossa tietosuojasopimusluonnos saattaa päätyä tietosuoja-asiantuntijan kommenteille vastan jälkeen, kun toimittaja on hankintapäätöksellä valittu hankinnan toimittajaksi. Tällaisessa tapauksessa toimittaja saattaa pyrkiä esittämään laajojakin kommentteja tietosuojasopimusluonnokseen jälkikäteen.

Hankintayksikön on muistettava, että tietosuojaan liittyvät sopimuslausekkeet ovat olleet osa tarjouspyyntömateriaalia ja ovat olleet kaikkien tarjoajien nähtävillä. Tarjoajat ovat tehneet tarjouspyyntöön perustuvat tarjouksensa muun ohella tietosuolausekkeet huomioon ottaen. Siten hankintayksikön tulee suhtautua varovaisesti edes tietosuojasopimuslausekkeista neuvottelemiseen. Kun tarjoaja on tarjouksessaan sitoutunut tarjouspyynnön mukaiseen toimittamiseen, ei sillä tulisi olla perustetta muuttaa tarjousta edes tietosuojalausekkeiden osalta. Hankintayksikön on taasen kiellettyä muuttaa tarjouspyyntömateriaaliaan

kilpailutuksen päätyttyä siinä määrin olennaisesti, että sillä voisi olla vaikutusta kilpailutuksen lopputulokseen. Esimerkiksi jos henkilötietojen käsittely ei ole sallittu tarjousvaiheessa, tästä joustaminen ja muutoksen mahdollistaminen tarjousajan päätyttyä muodostaisi todennäköisesti olennaisen ja kielletyn sopimusmuutoksen. Kun sopimusehdot ovat olleet mukana tarjouskilpailussa, jokin tarjoaja on esimerkiksi saattanut jättää tarjoamatta, ja toinen ottaa jonkin riskin huomioon osana hinnoitteluaan. Tällöin ehtojen muuttamisen hyväksyminen olisi voinut muuttaa tarjouskilpailun lopputuloksen, ja voi siten muodostaa kielletyn olennaisen muutoksen hankintaan.

5.2.4 Tietosuojan arviointi useissa hankinnoissa samalta toimittajalta

Toisinaan hankintayksiköt hankkivat palveluita usealla eri sopimuksella samalta toimittajalta. Tilanne saattaa tulla vastaan esimerkiksi saman toimittajan voittaessa useamman kilpailutuksen. Tällöin tietosuoja-asiat tulee arvioida ja sopia jokaisen sopimuksen osalta erikseen.

Tarve sopia tietosuoja-asioista hankintakohtaisesti johtuu siitä, että eri hankinnoissa voivat liikkua erilaiset henkilötietojen tyypit (esimerkiksi yhdessä työntekijöiden käyttäjätunnuksia ja sähköpostiosoitteita ja toisessa asiakkaiden nimiä ja IP-osoitteita) tai henkilötietoja saattavat käsitellä eri toimijat (esimerkiksi yhdessä hankinnassa toimittajalla ei ole alihankkijaa ja toisen toteutuksessa on). Siten tietyn toimittajan kanssa solmittu tietoturvasopimus ei kata mitään muuta hankintaa kuin yhden tietyn hankinnan kohteen. Tietoturvasopimus ei ole yleissopimus kaikista hankintayksikön ja tietyn tarjoajan välisistä tietojensiirroista, vaan hankintakohtainen määrittely rekisterinpitäjän tietojen asianmukaisesta käsittelystä juuri siinä hankinnassa.

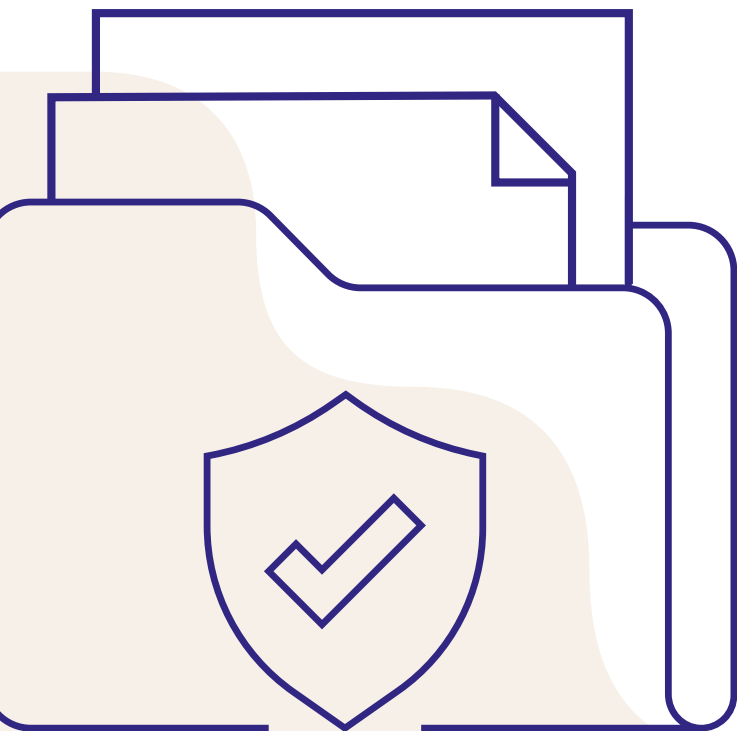
6. Tietosuoja hankinnan sopimuskaudella

Hankinta-asiantuntijan tietosuojaan liittyvät tehtävät päättyvät usein sopimuskauden alkuun. Kuten hankinnan suunnittelun ja kilpailutuksenkin ajanakin, sopimuskauden käynnistyessä ja sen aikana vastuuhenkilöinä tietosuoja-asioissa toimivat substanssi- ja mahdolliset tietoturva-asiantuntijat. On kuitenkin hyvä ymmärtää, että tietosuoja-asiat ovat aktiivisia usein koko sopimuskauden ajan.

Sopimuksen käyttöönottovaiheessa hankintayksikkö ja toimittaja yhteistyössä luovat ja käynnistävät tietosuojaan liittyvät käytännön prosessit (kuka tekee, missä järjestelmässä ja mitä), sopivat käytännön raportointivastuiden toteuttamisen ja hallinnollisten yhteistyöelinten työn.

Sopimuskauden aikana tietosuojatilanteita on aktiivisesti seurattava ja järjestelyitä kehitettävä. Sopimuskauden aikana on mahdollista herättää käyttöön käytännön toimintatapoja osapuolten vastuiden toteuttamiseksi. Hankintayksikön saattaa olla tarpeen myös auditoida, eli tarkastaa, toimittajan tietosuoja-prosesseja.

Sopimuskauden päättyessä toimittajan tulee lopettaa hankintayksikön henkilötietojen käsittely ja hallitusti päättää tietoihin liittyneet toimenpiteet. Toimittajan tulee luovuttaa takaisin hankintayksikölle sen henkilötiedot. Käytännössä tämä tapahtuu tietojen hävittämiselle toimittajan tallennustiloista. palvelun luonteesta riippuen toimittajalla saattaa kuitenkin olla erilaisia lakisääteisiä tai muita perusteita säilyttää tietoja säilytysaikavaatimusten mukaisesti myös palvelun päättymisen jälkeen.



7. Hankintoja koskeva tietosuojaseloste

Hankintayksikön tulee laatia ja asettaa yleisesti verkkosivuille saatavaksi tietosuojaseloste julkisia hankintoja koskevien henkilötietojen käsittelystä. Tietosuojaseloste on julkinen asiakirja, jolla rekisterinpitäjä kertoo rekisteröidyille, mitä tietoja heistä kerätään, miksi ja millaisin periaattein. Rekisterinpitäjä on se, joka määrittää henkilötietojen käsittelyn tarkoitukset

Tietosuoja-asetuksessa ei mainita sanaa tietosuojaseloste, mutta GDPR-asetuksessa määrätään rekisterinpitäjän informaatiovelvollisuudesta rekisteröityjä kohtaan (12-14 artiklat) sekä velvollisuudesta ylläpitää selostetta vastuullaan olevista käsittelytoimista (30 artikla).

EU:n tietosuoja-asetuksen 6 artiklan 1 mukaan henkilötietojen käsittely on lainmukaista, kun vähintään yksi kohdan edellytyksistä täyttyy:

6 artikla

1. Käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy:
 - a. rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten;
 - b. käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
 - c. käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;

- d. käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;
- e. käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi;
- f. käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suoja edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

Hankintayksiköissä yleinen oikeusperuste, joka tietosuojaselosteessa hankinnan henkilötietojen käsittelylle esitetään, on lakisääteinen velvoite (artikla 6 kohta 1 c). Sitä käytetään esimerkiksi, kun käsitellään henkilötietoja hankintojen toteuttamiseksi kilpailuttamalla hankintalain mukaisesti, tarkastellaan rikosrekisteriotteita tai suoritetaan pakotteisiin liittyviä tarkastuksia.

Oikeusperuste voi olla myös esimerkiksi yleinen etu (artikla 6 kohta 1 e). Sitä voidaan käyttää esimerkiksi, kun käsitellään henkilötietoja sellaisten hankintojen toteuttamiseksi, joita ei hankintalain mukaisesti ole kilpailutettava (kuten pienhankinnat tai poikkeukset hankintalain soveltamisalasta), tai kun käsitellään henkilötietoja markkinakartoitusten toteuttamiseksi.

Tietosuojaselosteessa esitettävä käsittelyperuste hankinnassa esitettävien henkilötietojen käsittelyyn voi vaihdella organisaatiokohtaisesti perustuen hankintayksikön organisaation toimintaan tai velvollisuuksiin.

Hyödyllisiä linkkejä

- [Tietosuojaohjeita organisaatioille](#) | Tietosuojavaaltuutetun toimisto
- Mallipohjat tietosuojasopimukselle ja henkilötietojen käsittelytoimille:
[Tietosuojaoliite](#) (5/2023)
[Henkilötietojen käsittelytoimien kuvaus](#) (5/2023)
- [Julkisen hallinnon tietoturvallisuuden arviointikriteeristö](#) (Julkri): Suositus ja kriteeristö
- [Komission hyväksymät vakiolausekkeet](#) | Tietosuojavaaltuutetun toimisto

