TIETOSUOJAVALTUUTETUN TOIMISTO

HENKILÖTIETOJEN KÄSITTELYN ULKOISTAMINEN, YHTEISET TIETOJÄRJESTELMÄT, VERKOTTUMINEN JA NIIHIN LIITTYVÄT SOPIMUKSET

Päivitetty 27.07.2010

www.tietosuoja.fi

SISÄLTÖ

LIITTEET

Kuvat:

HENKILÖTIETOJEN KÄSITTELYN ULKOISTAMINEN, YHTEISET TIETO-JÄRJESTELMÄT, VERKOTTUMINEN JA NIIHIN LIITTYVÄT SOPIMUKSET

I Johdanto

Henkilötietolain keskeinen tavoite on hyvän tietojenkäsittelytavan ja samalla hyvän tiedonhallinnan aikaansaaminen. Tämän tavoitteen saavuttaminen edellyttää erityisesti etukäteen tapahtuvaa huolellista suunnittelua.

Tässä esitteessä käsitellään lyhyesti esimerkein niitä henkilötietolaista johtuvia keskeisiä vaatimuksia, jotka tulee huomioida, kun henkilötietojen käsittelyä edellyttäviä tehtäviä ulkoistetaan tai tietojärjestelmiä verkotetaan, ja kun näihin liittyviä sopimuksia laaditaan. Tietojärjestelmiä ja ulkoistamista koskevat päätökset tekee viime kädessä organisaation johto. Sen vuoksi esite on kohdistettu erityisesti ko. hankkeista vastuussa olevalle johdolle, sekä toimintojen ja tietojenkäsittelyjärjestelmien kehittämiseen ja suunnitteluun osallistuvalle henkilöstölle.

II Ulkoistamisen suunnittelu ja hallinta henkilötietojen käsittelyssä

Ulkoistettaessa henkilötietojen käsittelyä edellyttäviä tehtäviä, suunnittelussa on otettava huomioon muun ohella erityisesti henkilötietolain (523/1999) vaatimukset. Käytännössä esimerkiksi henkilötietoja koskevat tietojenkäsittelypalvelut voidaan ulkoistaa palvelut hankkivan rekisterinpitäjän lukuun. Tällöin palvelujen hankkimisesta tehdään toimeksiantosopimus palvelut tilaavan rekisterinpitäjän (toimeksiantaja) ja palveluntuottajan (toimeksisaaja) välillä. Kyseinen rekisterinpitäjä vastaa tällöin tietojenkäsittelyn ja muunkin toiminnan lainmukaisuudesta. Palvelun tuottaja vastaa käsittelystä osapuolten välillä tehtävän toimeksiantosopimuksen mukaisesti. Toimeksiantajan lukuun sopimuksen perusteella tapahtuva henkilötietojen käsittely on rekisterin käyttöä. Henkilötietojen antaminen toimeksisaajalle tietojenkäsittelyä varten ei siten ole henkilötietojen luovuttamista, johon tarvittaisiin asianomaisen rekisteröidyn henkilön suostumus. Toimeksisaajalla ei ole toisaalta oikeutta käyttää toimeksiantosuhteessa saamiaan henkilötietoja omassa toiminnassaan, eikä käsitellä niitä vastoin sopimusta, eikä yhdistää tietoja muuhun hallussaan olevaan aineistoon.

> **Rekisterinpitäjällä tarkoitetaan**:
> *”yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty”* (HetiL: 3.1 kohta 4)

Tietoturva- ja tietosuojariskit osaltaan lisääntyvät ja muuttuvat toisenlaisiksi kun tietojenkäsittelypalveluja hankitaan ulkopuoliselta yritykseltä. Sen vuoksi on tärkeää, että sopimuksessa määritellään riittävän yksityiskohtaisesti, mitä eri käsittelyjä ja tehtäviä palveluntuottaja tekee ja mistä vastaa, ja mitkä tehtävät ja vastuut jäävät tilaajan tehtäväksi ja vastuulle. Yhtenä sopimukseen kuuluvana osana määritellään, miten tietoturvallisuus eri käsittelyvaiheissa varmistetaan. Henkilötietolain näkökulmasta tietoturvallisuus toteuttaa erityisesti henkilötietolaissa säädettyä suojaamisvaatimusta. Tietoturvallisuuden ja tietojen suojaamisen suunnittelu ja toteutus on henkilötietojen kaikkiin käsittelyvaiheisiin liittyvä vaatimus.

Vastuiden määrittelyn kannalta on tärkeää, että sopimuksen oikeudellinen luonne on selvästi todettu sopimuksessa (toimeksiantosopimus). Tähän liittyen on myös huomattava, että viranomaisen toiminnan julkisuudesta annetun lain (621/1999 myöhempine muutoksineen) 5.2 §:n perusteella viranomaisen toimeksiannosta laadittaviin asiakirjoihin/tietoihin sovelletaan julkisuuslakia. Tämäkin seikka on tarpeen todeta toimeksiantosopimuksessa.

Onnistuneen ulkoistamisen ja sopimuksenteon edellytyksenä on, että yritys, yhteisö, viranomainen tai muu rekisterinpitäjä tuntee ja hallitsee ulkoistettavaan tehtäväänsä liittyvät prosessit ja on arvioinut toimintaan liittyvät käsittelyt henkilötietolain vaatimuksista käsin. Tähän liittyvinä toimenpiteinä edellytetään, että

- Rekisterinpitäjä on kartoittanut ja kuvannut asiakirja-aineistonsa sekä määritellyt muun ohella tehtävissään eri käyttötarkoituksiin muodostuvat henkilörekisterit

- Rekisterinpitäjällä on kuvaus myös ulkoistettavaksi suunnitellussa tehtävässä käytettävästä henkilörekisteristä, rekisterinpitoon liittyvistä prosesseista ja tehtävän edellyttämistä henkilötietojen käsittelyistä.

- kuvaus on tehty toiminnalliset, tekniset ja lainsäädännön vaatimukset huomioon ottaen, jolloin käsittelyssä toteutuu henkilötietolain edellyttämä hyvä tietojenkäsittelytapa ja julkisuuslain edellyttämä hyvä tiedonhallintatapa. Esim. tarpeettomia ja virheellisiä tietoja ei saa kerätä eikä tallettaa, käsittelyssä on huomioitava huolellisuus- ja suojaamisvelvoitteet sekä käyttötarkoitussidonnaisuuden vaatimus ja rekisteröityjen oikeuksien toteuttaminen.

Esimerkkejä eri tehtävistä (käyttötarkoituksista), joissa muodostuu henkilörekisteri:

1. Yrityksissä, pankeissa ja vakuutuslaitoksissa muodostuu eri asiakassuhteiden hoitamisessa asiakasrekistereitä

2. kunnalle säädetyissä eri tehtävissä ja niiden edellyttämissä asiakassuhteiden hoidossa muodostuu kussakin tehtävissä eri henkilörekisterit (esim. opetuksen järjestämisessä oppilasrekisteri, sosiaalihuollon eri tehtävissä asiakasrekisterit)

3. valtion viranomaiset hoitavat lakisääteisiä tehtäviään, joissa usein edellytetään henkilötietojen keräämistä. (Esim.Valtiokonttori hoitaa laissa säädettyinä eri tehtävinään mm. valtion henkilöstön eläkeasioita ja valtion tapaturma-asioita). Kussakin tehtävässä muodostuu eri käyttötarkoitukseen ko. tehtävän hoitamista varten henkilörekisteri.

4. Sekä julkisen että yksityisen sektorin organisaatiot tarvitsevat henkilöstönsä palkkaamiseksi ja palvelusuhteeseen liittyvien tehtävien hoitamiseksi
   a) henkilöstöhallinnon rekisterin
   b) työnhaussa muodostuvat rekisterit

Suunnittelussa on hyvä huomata, että samaan henkilörekisteriin kuuluvat kaikki ne tiedot, joita käsitellään kyseisen tehtävän hoitamiseksi (rekisterin käyttötarkoitus). Hyvän tiedonhallinnan aikaansaaminen edellyttää, että kuvattuna on se kokonaisuus, joka tietyssä rekisterinpitäjän tehtävässä muodostuu (looginen henkilörekisteri). Vaikka tietojärjestelmä voidaan toteuttaa osatoiminnoittain, toiminnan ja tietojenkäsittelyn tarpeiden suunnittelu, toteuttaminen ja myös ulkoistaminen edellyttää, että suunnittelun pohjana on kokonaiskuva tehtävästä ja sen eri

osatoiminnoista, prosesseista ja työnkuluista.

> **Henkilörekisterillä tarkoitetaan:**
> *"käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta"* (HetiL 3.1. kohta 3)
>
> "***Henkilötietojen käsittelyn tarkoitus*** *tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään"* (HetiL 6 § mom. 2)

Ulkoistaminen voidaan toteuttaa eri tavoin, esim.
- viranomainen, yritys, muu yhteisö (rekisterinpitäjä) hankkii tietojenkäsittelypalveluita tai muita palveluja yksityiseltä yritykseltä
- valtion viranomainen ja kunnallinen viranomainen voivat hankkia tietojenkäsittely- ja muita palveluja toiselta viranomaiselta

Suunniteltaessa ulkoistettavia tehtäviä ja niihin liittyviä henkilötietojen käsittelyjä ulkoistaminen kuvataan osana ko. tehtävään liittyvää rekisterinpitoa.

- Tässä yhteydessä suunnitellaan yksityiskohtaisesti, mitä tehtäviä ja vastuita henkilötietojen käsittelyissä mahdollisen palveluntuottajan edellytetään hoitavan, sekä mitkä tehtävät jäävät rekisterinpitäjälle, mitä mahdollisia riskejä ja uhkia järjestelyihin liittyy, miten ne voidaan ratkaista, miten erilaiset menettelyt on tarkoitus hoitaa, sekä mitä palvelun tuottajan edellytetään ottavan huomioon tietoturvallisuuden ja tietojen suojaamisen vaatimusten täyttämiseksi käsittelyjen eri vaiheissa
- Kaikissa vaiheissa varmistetaan, ettei kenenkään yksityisyyttä perusteettomasti vaaranneta. Tämä edellyttää mm., että tietorakenteet suunnitellaan ja toteutetaan siten, että käyttöoikeudet henkilötietoihin voidaan rajata kussakin tehtävissä tarpeellisiin tietoihin ja ettei henkilötietoja luovuteta – jos se olisi lainmukaista – enempää kuin ko. tarkoituksessa on tarpeellista. Asiakirjoja, näyttöjä ja näkymiä suunniteltaessa varmistetaan, ettei niissä esitetä tarpeettomasti tietoja. (esim. henkilötunnus).
- Huolellisen suunnittelu- ja valmistelutyön pohjalta voidaan tehdä asian edellyttämät tarjouspyynnöt sekä laatia sopimukset riittävän yksityiskohtaisesti. Sopimuksissa osapuolten tehtävät ja vastuut on kuvattava ja määriteltävä riittävän yksityiskohtaisesti, jotta tiedetään mistä on sovittu ja jotta mahdollisiin sopimusrikkomuksiin voidaan puuttua
- On myös tärkeää ennakoida ja sopimuksessa määritellä sopimuksen päättymiseen liittyvät tilanteet sekä ne tehtävät ja velvoitteet, jotka osapuolten tässä yhteydessä tulee hoitaa.

Alla oleva taulukko kuvaa, millä tavoin rekisterinpitäjän on tarpeen kuvata ja arvioida rekisterinpidon toiminnallisuus ja lainmukaisuus. (Kuva 1)
Kun rekisterinpitäjä suunnittelee ulkoistusta, suunnittelu tulee toteuttaa kuvaamalla, mitkä rekisterinpitäjän tehtävistä/osatehtävistä ja niihin liittyvistä henkilötietojen käsittelytehtävistä aiotaan ulkoistaa. Jokaiseen käsittelyvaiheeseen liittyy myös tietojen suojaamisen ja tietoturvallisuuden vaatimuksia. Suunnittelu tehdään loogisen rekisterikäsitteen pohjalta siten, että kaikki ko. tehtävässä muodostuvan aineiston (atk ja manuaalinen) käsittely ja työnkulut kuvataan.

Kuva 1: Esim. YHDISTELMÄ HENKILÖTIETOJEN KÄSITTELYN KUVAUSMALLISTA

REKISTERINPITÄJÄ: (HetiL 3.1§.k 4) **Esim.** ***keskusvirasto xx***					
REKISTERIN KÄYTTÖTARKOITUS: (HetiL 3.1.§ k 3, 6 §) Esim. ***xx:n Henkilöstöhallinnon rekisteri***					
Käsittelyvaihe	**Kuvaa toiminnan edellyttämät käsittelytarpeet/ toteutus vaiheittain/ Osatehtävittäin + vastuut**	**Kuvaa ja arvioi tietosuojaan kohdistuvat uhat ja riskit käsittely-vaiheittain**	**Määrittele käsittelyn menettelytavat, tietoturvan ja tietojen suojaamisen toteutus vaiheittain/ osatehtävittäin** **- kuka tekee** **- mitä tekee** **- millä tavoin**	**Määrittele ja varmista käsittelyn ja menettelyjen oikeud. edellytykset** **- arviointi käsittelyvaiheittain HetiL:n ja mahd. erityissäännösten mukaisesti**	***Ulkoistettavassa toiminnassa palvelun-tuottajalle suunniteltu tehtävät ja vastuut***
Tietojen kerääminen/ Tietosisältö - mitä tietoja - tietolähteet/ tiedonsaannin peruste, ym.				**- HetiL 9 §** **- työelämän tietosuojalaki (TyTSL)** **- mahd. erityis-säännökset**	
Rekisterin sisäinen käyttö ja suojaaminen ml. tietoturva				**- HetiL 5 §, 32 §** **- mahd. erityis-säännökset (esim. JulkL 18 §)**	
Luovuttaminen - kenelle - mikä tarkoitus – mitä tietoja – millä perust.				**- HetiL 8 §, 12 § 5 §, 9 §, 32 §** **- mahd. erityis-säännökset (esim. JulkL 16.3 §)**	
Säilyttäminen ja hävittäminen - säilyttämisaika * aktiivi-/ passiiviaika – menettelytapa				**- HetiL 34 §, 5 § , 9 §, 32 §** **- mahd. erityis-säännökset (esim. ArkistoL)**	
Rekisteröityjen informointi				**- HetiL 24 §, 3.1 § k 7** **- TyTSL**	

- mistä – miten				**- mahd. erityis-säännökset**	
Rekisteröityjen oikeuksien toteutus – tarkastusoikeus – virheen korjaus – kielto-oikeus				**- HetiL 26-29 §,** **- mahd. erityis-säännökset**	
Muut tarpeellisten käsittely-vaiheiden kuvaukset				**- HetiL 5 §, 9 §, 32 §** **- TyTSL 16 § - 23 §**	

Kuva/Tietosuojavaltuutetun toimisto

Seuraavassa kuvassa esitetään toisesta näkökulmasta se kokonaisuus ja ne eri elementit, jotka tulee olla määriteltynä ja kuvattuna henkilötietojen käsittelyssä ja käsittelyä ylläpitävän tietojärjestelmän suunnittelussa ja toteutuksessa (Kuva 2). Samat asiat tulee arvioida palveluntuottajan toiminnan osalta, kuitenkin huomioon ottaen käsiteltäväksi annetut tehtävät ja käsittelyt.

Kuva 2:
Esimerkki XX-käyttötarkoituksessa perustetun henkilörekisterin ylläpitämiseen suunniteltavan tietojärjestelmän eri elementeistä

LOOGINEN REKISTERI =
- rekisterinpitäjäorganisaation itsensä toteuttama käsittely
- ulkopuolisen palveluntuottajan rekisterinpitäjän lukuun toimeksiantosopimuksen perusteella toteuttama käsittely
  → käsittely kuuluu rekisterinpitäjäorganisaation loogiseen

henkilörekisteriin

Rekisterinpitäjän oma toiminta:

Kaavio tietojärjestelmien suunnittelun ja toteutuksen elementeistä HetiL:n vaatimusten kannalta arvioituna:

Käyttötarkoitus, tietosisältö ja tietovirrat: Toiminta-analyysi

Henkilörekisterin käyttötarkoitus, tietosisältö ja rakenne, tietolähteet, käyttö ja luovutukset, säilyttäminen, ml. ulkopuoliset palvelut, rekisteröityjen oikeuksien toteuttaminen

Rekisterin ja sovelluksen rakenne/arkkitehtuuri

Tietorakenteet, tietotasot ja -ryhmät

Tietojen siirto-tarve (käyttö), suojaaminen ja valvonta toiminta-yksikössä eli rekisterinpitäjän omassa toiminnassa

Tietojen siirto-tarve (luovutus) kahden toiminta-yksikön ja rekisterinpitäjän välillä, tiedon luovutustavat, tiedonsiirron "auktorisointi" ja valvonta

Tietojen säilyttämis-tarpeen mukainen rakenne ja hävittäminen

Tietojen päivitys- ja korjaamismenettely

Sovellusrakenne

Laitteistoarkkitehtuuri

Laitteiston ja tiedonsiirtoverkon tekniset tietosuoja- ja tietoturvaratkaisut

Kuva/Tietosuojavaltuutetun toimisto. Laatineet M.K./R-T. P.

TOIMEKSI-ANTO-SOPIMUS

Palveluntuottajalle (toimeksisaajalle) suunnitellut tehtävät

Kuvaus ja analyysi toimeksisaajalle suunniteltavista tehtävistä ja vastuista, mm.

- henkilötietojen käyttöön ja muuhun käsittelyyn, esim. luovuttamiseen liittyvät tehtävät
  *
  *
  *

- tietoturvaan ja tietojen suojaamiseen liittyvät tehtävät,vaatimukset ja vastuut

- laitteistoon ym. liittyvät vaatimukset ja vastuut

- henkilöstöä koskevat salassapito- ym. vaatimukset
  *** käyttäjä- ja vaitiolositoumus**

- muut käsittelyyn liittyvät tehtävät ja vastuut (esim. informointi ja rekisteriselosteen saatavillapito)

Tietoturvallisuuden varmistamisen velvoite kuuluu kaikkiin käsittelyvaiheisiin ja kaikkiin tietojärjestelmän toteutuksen tasoihin ja osiin

Liitteenä 1 on toimeksiantosopimuksen sopimusrunko, ja liitteenä 2 tarkistuslista, jossa on esimerkinomaisesti lueteltu mistä /minkä tyyppisistä eri asioista toimeksiantosopimuksissa tulisi olla sopimusmääräykset.

III Yhteiset tietojärjestelmät/henkilötietojen käsittelyn verkottuminen

Yhteisellä tietojärjestelmällä tarkoitetaan tässä järjestelmiä, joissa kaksi tai useampi itsenäinen yritys, laitos, viranomainen yms. (rekisterinpitäjä) toteuttavat yhdessä tieto- tai tiedonsiirtojärjestelmän tehtäviensä ja toimintojensa hoitamiseksi.

Silloin kun tehtävien hoito edellyttää ja/tai siinä on kysymys myös henkilötietojen käsittelystä, järjestelmien toteuttamista on arvioitava aina myös henkilötietolainsäädännön kannalta. Olennaista tällöin on huomata, että yhteisten/yhteiskäyttöisten tietojärjestelmien toteuttaminen ei oikeuta yhdistämään mukaan tulevien rekisterinpitäjien henkilörekistereitä. Yhteisiin tietojärjestelmiin tai tiedonsiirtojärjestelmiin liittyminen /verkottuminen ei siten muuta yksittäisen rekisterinpitäjän vastuita henkilötietojensa käsittelystä (rekisterinpidosta). Rekisterinpitäjän, esimerkiksi viranomaisen kannalta kysymys on siitä, että käsittelyyn liittyvä toimintaympäristö ja -tekniikka sekä toimintatavat muuttuvat. Toteutettava tietojärjestelmä on apuväline, jonka avulla voidaan siirtää, ylläpitää, luovuttaa ja muulla tavoin käsitellä rekisterinpitäjän/rekisterinpitäjien pitämän henkilörekisterin tai henkilörekisterien sisältämiä henkilötietoja. (Kts. rekisterinpitäjän ja henkilörekisterin, sekä henkilötietojen käsittelyn (rekisterin) käyttötarkoituksen määrittelyistä sivuilla 3 ja 5).

Yhtä tärkeää kuin hankittaessa ulkopuolisia palveluja, on analysoida ja suunnitella etukäteen yhteisen tieto- ja tiedonsiirtojärjestelmän tai verkon käyttöön liittyvät kysymykset ja vaatimukset. Lähtökohta tässäkin on, että kukin hankkeeseen lähtevä tai liittyvä rekisterinpitäjä (viranomainen, yritys ym.) tuntee omat tehtävänsä, hallitsee tehtäviinsä liittyvät prosessit ja tietojenkäsittelyt sekä toimintatavat ja osaa siten arvioida, mitä verkottuminen oman toiminnan kannalta edellyttää. Arviointi on tehtävä sekä toiminnallisten tarpeiden että myös teknisten (mm. tietoturvakysymykset) ja oikeudellisen vaatimusten kannalta (kuva 1 sivulla 6, sekä kuva 2 sivulla 8).

Yhteisesti toteutettavat tietojärjestelmät edellyttävät myös yhteisesti tehtyjä suunnitelmia, joissa hankkeen toteutus on kuvattu ja arvioitu toiminnan, lainsäädännön ja teknisen toteutuksen sekä myös kustannusten kannalta. Tietojärjestelmää toteutettaessa on tärkeää, että mukaan tulevien rekisterinpitäjien (yritysten, yhteisöjen, viranomaisten ym.) yhteistyö ja vastuut on määritelty, toiminta on suunnitelmallista ja koordinoitua, ja asian edellyttämät sopimukset, joissa osapuolten vastuut on määritelty, on tehty. Suunnittelu edellyttää muun muassa erilliset kuvaukset paitsi jokaisen mukaan tulevan rekisterinpitäjän ao. henkilörekisteristä sekä siihen liittyvästä henkilötietojen käsittelystä, myös kuvauksen koko hankkeesta ja sen osapuolista sekä siihen liittyvästä henkilötietojen käsittelystä ja käsittelyn tarpeista. Kaikista hankkeeseen liittyvistä prosesseista ja työkuluista tulee olla asianmukainen kuvaus, jotta em. hankkeelle asetetut tavoitteet ja vaatimukset voidaan arvioida ja toteuttaa (kuva 4 sivulla 12), ja että hankkeen lainmukaisuus voidaan kaikkien käsittelyvaiheiden osalta varmistaa

Rekisterinpitäjän on tunnettava muun muassa eri tehtäviinsä liittyvät tietovirrat; mistä tietoja säännönmukaisesti ja muutoinkin hankitaan ja on tarpeellista hankkia, sekä mihin tietoja sekä mitä tietoja säännönmukaisesti on tarpeen luovuttaa ja luovutetaan, sekä millä lainsäädännöllisellä perusteella tietojen hankkiminen ja luovuttaminen voi tapahtua.

Suunniteltaessa henkilörekisteriin kuuluvien henkilötietojen luovuttamista ja siirtämistä sähköisesti verkon välityksellä toiseen organisaatioon, on huolehdittava - paitsi luovutusten oikeudellisten edellytysten täyttymisestä - erityisesti myös siitä, että tietoturvallisuus ja tietojen

suojaaminen, sekä virheettömyysvaatimus toteutuvat lainsäädännön edellytysten mukaisesti. Huomioitavaksi tulevat muun muassa henkilötietolain 5, 9 ja 32 §:ssä säädetyt huolellisuus- ja suojaamisvelvoitteet sekä tarpeellisuus - ja virheettömyysvaatimukset, viranomaisten toiminnan julkisuudesta annetun lain 18 §:ssä ja sen nojalla annetussa asetuksessa määritellyt hyvän tiedonhallinnan vaatimukset, samoin kuin myös asiaa mahdollisesti koskevan muun erityislain asettamat vaatimukset. Edellytyksenä on myös, että osapuolet ovat yhdessä määritelleet pelisäännöt, joilla varmistetaan luovutusten tai tiedonsaannin onnistuminen kyseisen toiminnan ja lain edellytysten mukaisesti. Käytännössä tämä edellyttää muun muassa yhteensopivia tietorakenteita ja yhteensopivaa teknistä toteutusta, sekä asiasta tehtyjä sopimuksia, joissa muun ohella todetaan kunkin osapuolen tehtävät ja tehtävien edellyttämät rekisterinpidon vastuut.

Yhteisen tietojärjestelmän ja tiedonsiirtojärjestelmän toteutus edellyttää usein myös ulkopuolisten tietojenkäsittelypalvelujen hankkimista. Hankkeen osapuolten on useimmiten yhdessä tarpeen suunnitella ja sopia myös ulkopuolisten palvelujen hankkimisesta, sekä siihen liittyvistä vastuista, lainsäädännön vaatimukset huomioon ottaen. Koska rekisterinpitäjän vastuut eivät muutu, palvelujen hankkiminen voidaan käytännössä toteuttaa ainoastaan siten, että ulkopuoliset palvelut hankitaan erikseen kunkin rekisterinpitäjän lukuun. Vaikka palvelujen hankkiminen ja niihin liittyvät kysymykset suunnitellaan yhdessä, jokaisen rekisterinpitäjän tulee tehdä valitun palveluntuottajan kanssa erikseen toimeksiantosopimukset omien rekisteriensä tietojen käsittelystä ja ylläpitämisestä.

Järjestelyissä voi olla myös mahdollista sopia siitä, että jokin hankkeen osapuolena olevan rekisterinpitäjä (yritys, viranomainen tm.) ylläpitää tietojärjestelmää toisten osapuolten lukuun (toimeksiannnosta). Kyseinen rekisterinpitäjä toimii tällöin kahdessa roolissa: omien rekisteriensä rekisterinpitäjänä ja erikseen muitten lukuun näiden toimeksiannosta (toimeksisaajana). Toimeksisaajalla ei ole oikeutta käyttää omassa toiminnassaan ko. toimeksiantotehtävän yhteydessä käsittelemiään tietoja eikä eri toimeksiantajien (rekisterinpitäjien) henkilörekisterien tietoja saa yhdistää.

Sähköiseen käsittelyyn ja tiedonsiirtoon siirrytään usein osatoiminnoittain. Mitä laajemmasta alueellisesta tai jopa valtakunnalliseksi tarkoitetusta tieto- ja tiedonsiirtojärjestelmästä on kysymys, sitä tärkeämpää on, että toteutus pohjautuu riittävän kattavaan kokonaiskuvaukseen. Vain tältä pohjalta on mahdollista arvioida, minkälaiseen toimintaympäristöön mahdollinen osaratkaisu tehdään ja miten se vaikuttaa ja toimii myöhemmin toteutettavissa hankkeissa ja tietojärjestelmissä. Muutoin vaarana on tietojärjestelmähankkeiden epäonnistuminen ja tarpeettomat yllätykset kehittämis- ja toteutustyön aikana sekä pahimmillaan moninkertaiset kokonaiskustannukset. Vaikkei etukäteisellä suunnittelulla voida luonnollisestikaan ratkaista kaikkia tulevia ongelmia, niiden määrää todennäköisesti voidaan merkittävästi vähentää.

Jos tietojärjestelmän avulla luovutetaan henkilötietoja rekisterinpitäjien välillä, on määriteltävä ensimmäiseksi luovutuksen oikeudelliset edellytykset sekä varmistettava, että muun muassa tietoturvallisuus, tietojen virheettömyys- ja tarpeellisuusvaatimukset ja tietojen asianmukainen suojaaminen toteutuvat *sekä luovuttavassa että myös vastaanottavassa päässä.*

Henkilötietojen henkilörekisteristä luovuttaminen voidaan toteuttaa vain lainsäädännön edellytysten mukaisesti. Keskeisimmät luovuttamista koskevat oikeudelliset edellytykset voidaan esittää seuraavasti.

<u>Viranomaisten</u> henkilörekisterien tiedot
1) julkiset tiedot: rekisteröidyn suostumus tai julkisuuslain 16.3 § tai muun lain nimenomainen

säännös,
2) salassa pidettävät tiedot: rekisteröidyn suostumus, tai asiaa koskeva nimenomainen säännös (julkisuuslain 26 §, 29 § js 16.3 §).
(Katso tietosuojavaltuutetun toimiston esite ”Henkilötietojen luovuttaminen viranomaisten henkilörekistereistä”)

Yksityiset yritykset yms.
Yksityisten rekisterinpitäjien pitämien henkilörekisterien osalta luovutukseen oikeuttaa pääsääntöisesti vain rekisteröidyn suostumus tai henkilötietolain 8 §:n mukaisesti muu luovutukseen oikeuttava lainsäännös.

Suostumuksesta henkilötietojen käsittelyssä löytyy ohjausta tietosuojavaltuutetun toimiston esitteestä ”Henkilötietojen käsittely suostumuksen perusteella”.

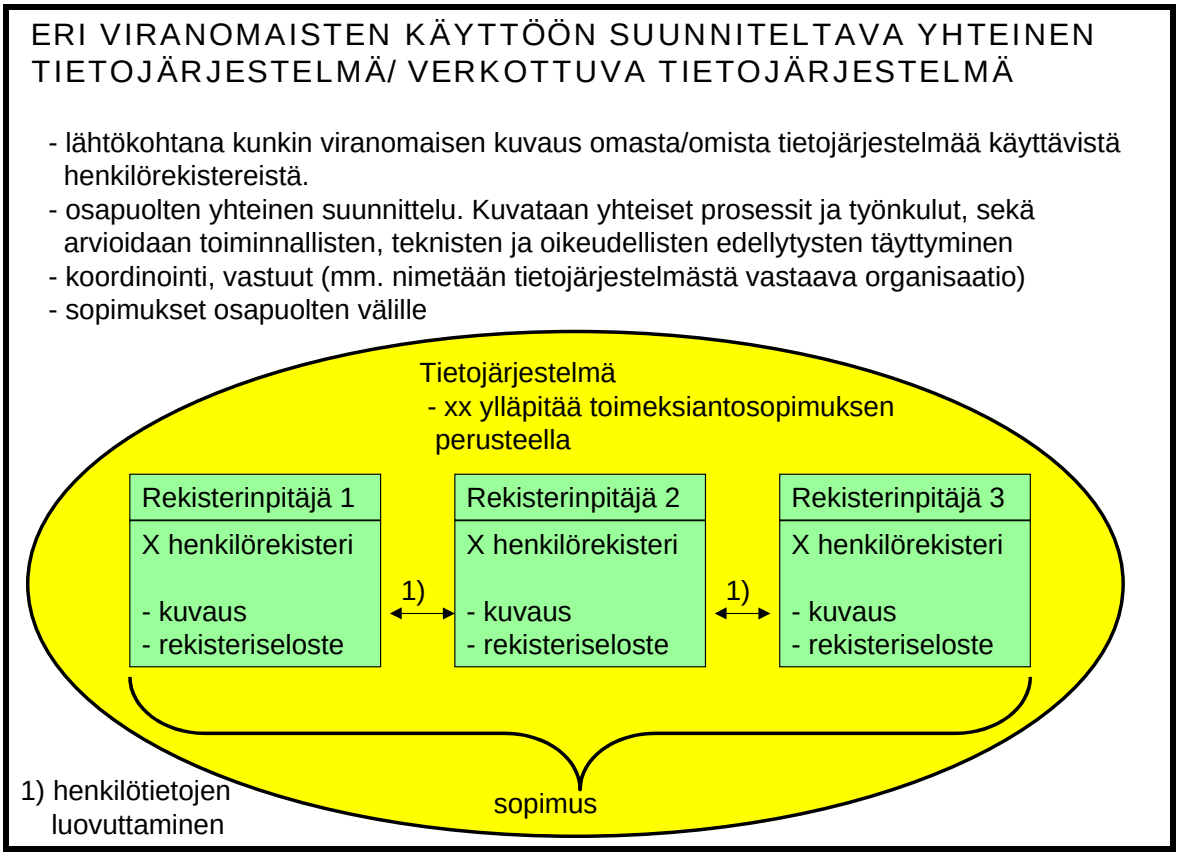
Teknisen käyttöyhteyden avaaminen merkitsee tosiasiallisesti henkilötietojen luovuttamista; esimerkiksi katseluoikeuden avaaminen sähköisen yhteyden avulla toisen viranomaisen henkilörekisterin tietoihin on henkilötietojen sähköistä luovuttamista. Tästä syystä teknisen käyttöoikeuden avaaminen esimerkiksi toisen viranomaisen tai muun rekisterinpitäjän salassa pidettäviin tietoihin edellyttää siihen nimenomaisesti oikeuttavaa lain säännöstä, minkä lisäksi luovuttamiselle on oltava lakiin perustuva oikeus (rekisteröidyn suostumus tai nimenomainen lain säännös).

> Eduskunnan perustuslakivaliokunnan lausuntojen (PeVL 12 ja 14/2002 vp) mukaan laintasoisesti onkin muun ohella säädettävä teknisen käyttöyhteyden avaamisesta toiselle rekisterinpitäjälle ja avaamisen edellytyksistä.

Useissa laeissa on erityissäännöksiä teknisen käyttöyhteyden avaamisesta ja sen edellytyksistä. Yleissäännös viranomaisen oikeudesta avata tekninen käyttöyhteys henkilörekisterien tietoihin on julkisuuslain 29 §:ssä. Vastaavaa yleissäännöstä ei ole yksityisen toiminnan osalta.

Em. säännöstenkin mukaan toteutettu katselu- tai teknisen yhteyden avaaminen ei merkitse, että kuka tahansa voi milloin tahansa saada tai katsella käyttöyhteyden avulla toisen rekisterinpitäjän henkilörekisterin tietoja. Teknisin keinoin tulee aina varmistaa tietojen suojaaminen henkilötietolain 32 §:n mukaisesti ulkopuolisilta ja asiattomilta. Lisäksi huomioon tulee ottaa henkilötietolain 7 §:n käyttötarkoitussidonnaisuus, joka merkitsee, ettei tietoja saa esimerkiksi katsella uteliaisuudesta, vaan ainoastaan, jos siihen on tehtäviin liittyvä laillinen oikeus käsitellä tietoja henkilötietolain tai muun lain nojalla. Lain nojalla tapahtunut katseluoikeuden avaaminen tai muunlainen teknisen käyttöyhteyden avulla toteutettu luovutusmahdollisuus edellyttää toisaalta myös tehokasta ja suunnitelmallista luovutusten, esim. katselujen seuranta- ja valvontajärjestelmää (lokijärjestelmä ja siihen liittyvä seuranta- ja valvontajärjestelmä). Lain vaatimusten täyttyminen tulee varmistaa osaltaan jo asiaa koskevan luvan myöntämisen/asiaa koskevan sopimuksen tekemisen yhteydessä. Henkilörekisteristä henkilötietoja luovuttava rekisterinpitäjä vastaa luovutusten lainmukaisuudesta.

Kuva 3: Eri viranomaisten käyttöön suunniteltava yhteinen tietojärjestelmä/verkottuva tietojärjestelmä



IV Esimerkkejä

1) Useat ministeriöt/hallinnonalat ovat perustaneet tai perustamassa yhteyteensä palvelukeskuksia, joiden tehtävänä on huolehtia hallinnonalansa virastojen apuna tehtävistä.

Jokainen palvelukeskuksen palveluja ja perustettavaa tietojärjestelmää käyttävä viranomainen vastaa edelleen rekisterinpitäjänä esimerkiksi omasta henkilöstöhallinnon rekisterinpidostaan. Jollei palvelukeskuksista eikä niiden tehtävistä ja vastuista ole erikseen säädetty lailla, palvelukeskus vastaa henkilötietojen käsittelystä sopimusvastuuna, minkä lisäksi sen tulee suoraan lain nojalla noudattaa henkilötietolain 5 ja 32 §:n huolellisuus- ja suojaamisvelvoitteita sekä asiaan liittyviä salassapitosäännöksiä.

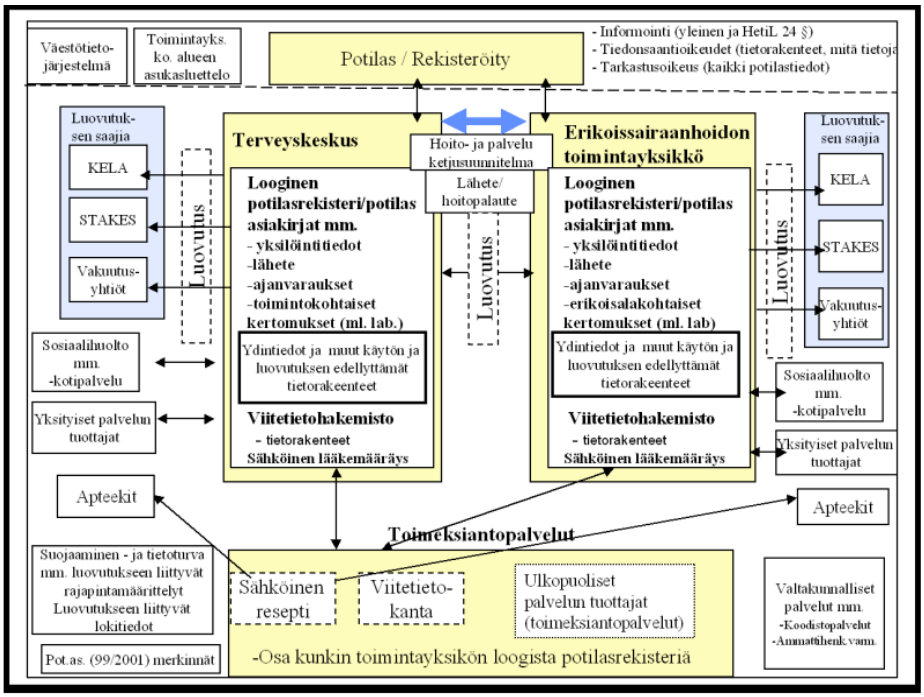
Palvelukeskuksen ja kunkin viranomaisen tulee siten tehdä erikseen toimeksiantosopimus, jossa todetaan ja määritellään ao. viranomaisen (toimeksiantaja) ja palvelukeskuksen (toimeksisaaja) tehtävät ja vastuut myös rekisterinpidossa. Hankkeen suunnittelevan ja koordinoivan viranomaisen on tarpeen tehdä palvelukeskuksen kanssa ns. palvelusopimus. Myös tarkoitukseen hankitun ja perustetun tietojärjestelmän vastuiden on oltava yksiselitteiset (ylläpito, toimivuus ym.).

2) Väestötietojärjestelmän toimivuuden vastuu on väestötietolaissa määritelty väestörekisterikeskukselle. Väestörekisterikeskus tekee ulkopuolisten palvelujen tuottajien kanssa tietojenkäsittelypalveluja koskevat tarpeelliset sopimukset. Väestötietojärjestelmässä käsiteltävien henkilötietojen käsittelyn vastuut on laissa määritelty maistraateille ja osaksi väestörekisterikeskukselle.

3) Useamman viranomaisen toteuttama tiedonsiirtoportaali voidaan toteuttaa ulkopuolisen palvelun tuottajan kanssa tehtävän sopimuksen perusteella. Jokaisen rekisterinpitäjän on varmistettava sopimuksin omien henkilörekisteriensä osalta tiedon luovutuksen tai antamisen (henkilörekisterien) lainmukaisuus henkilötietolain ja asiaa koskevien omaa toimintaansa koskevien lakien perusteella (katso kuva 1 sivulla 6, sekä kuva 2 sivulla 8). Järjestelmän toteutukseen voi kuulua myös tunnistamispalvelujen hankkiminen ulkopuolisten palvelujen tuottajalta. Jokaisen rekisterinpitäjän tulee tehdä omalla vastuullaan olevien henkilörekisteriensä osalta toimeksiantosopimukset ulkopuolisten palvelujen tuottajien kanssa. (esim. portaalin ylläpitoa ja tunnistamispalvelua koskevat sopimukset).

4) Esimerkki terveydenhuollon alueellisen tietojärjestelmän osapuolista, toimijoista ja elementeistä:

(**Kuva 4**)



Terveydenhuollon alueellisissa tietojärjestelmä- ja verkottumishankkeissa on välttämätöntä, että käytettävissä on kokonaiskuvaus hankkeen osapuolista ja heidän vastuistaan ja asemastaan hankkeessa, mahdollisista ulkopuolisista toimijoista, sekä kuvaukset kunkin osapuolen rekisterinpidosta, sekä kuvaus yhteisesti suunnitellun tietojärjestelmän toteutuksesta ja toimivuudesta. Lisäksi tulee tehdä sopimukset yhteistyöstä ja sen toteuttamistavoista. Välttämätöntä on myös, että hankkeen toteutukselle on luotu tehokas, vastuutettu ja ajantasainen seurantajärjestelmä.

Jokaisen alueellista tietojärjestelmää ja tiedonvälityspalveluja käyttävän terveydenhuollon toimintayksikön tulee erikseen tehdä toimeksiantosopimukset ulkopuolisten palveluntuottajien kanssa. Kukin terveydenhuollon toimintayksikkö (esim. terveyskeskus ja erikoissairaanhoidon toimintayksikkö) vastaa edelleen rekisterinpitäjänä omasta potilasrekisteristään ja siihen

liittyvästä tietojenkäsittelystä. Palveluntuottaja vastaa sopimusvastuuna ao. rekisterinpitäjille.
Kts.

- STM:n tuottamat terveydenhuollon sopimusmallit TSV:n verkkosivuilla → Oppaat/Muiden mallit

LIITTEENÄ 1 toimeksiantosopimuksen runkomalli
LIITTEENÄ 2 tarkistuslista, jossa on esimerkinomaisesti lueteltu mistä /minkä tyyppisistä eri asioista toimeksiantosopimuksissa tulisi olla sopimusmääräykset.

MALLI KIRJALLISEN TOIMEKSIANTOSOPIMUKSEN RAKENTEEKSI (sopimusrunko)
(sopimusmalli koskee erityisesti henkilötietojen käsittelyä edellyttäviä ulkopuolisia palveluja)

1) OSAPUOLET
*** TILAAJA, (TOIMEKSIANTAJA)**
esim. virasto xx tai yritys xx (rekisterinpitäjä)
*** TOIMEKSISAAJA (esim. yritys xx)**
- vastaa sopimuksen mukaisesti

2) SOPIMUKSEN KOHDE
esim. tietojenkäsittelypalvelujen antaminen

3) TOIMEKSIANTAJAN ASEMA, OIKEUDET JA VELVOLLISUUDET
- toimeksiantaja vastaa rekisterinpitäjänä
  * luetellaan toimeksiantajalle kuuluvat (jäävät) ko. rekisterinpitoon liittyvät tehtävät henkilötietojen käsittelyssä

4) TOIMEKSISAAJAN ASEMA, TEHTÄVÄT JA VELVOLLISUUDET
- vastuu määräytyy toimeksiantosopimuksen perusteella
  * luetellaan toimeksisaajalle kuuluvat tehtävät henkilötietojen käsittelyssä
  (esim. vastuu tietojenkäsittelyn ylläpidosta, suojaamisesta, tietoturvallisuudesta ja tietojen säilyttämisestä toimeksiantajan lukuun, sekä tarkastusoikeuden toteuttamisesta) (Kts. tarkastuslista, liite 2)
- maininta siitä, että toimeksisaajalla ei ole oikeutta käyttää tietoja omassa toiminnassaan eikä luovuttaa niitä

5) SOPIMUSYHTEISTYÖ
- mm. osapuolten vastuuhenkilöiden nimeäminen ja heidän tehtäviensä määritteleminen

6) HINTA

7) MAKSUEHDOT

8) SOPIMUKSEN VOIMASSAOLO

9) SOPIMUKSEN PÄÄTTÄMINEN/PÄÄTTYMINEN

10) SEURANTA JA VALVONTA

11) VAHINGONKORVAUS

12) SOPIMUSERIMIELISYYKSIEN RATKAISEMINEN

13) SOPIMUSKAPPALEET

14) RAPORTOINTI

15) YM. TARVITTAVIA SOPIMUSMÄÄRÄYKSIÄ

16) ALLEKIRJOITUKSET

kts. STM:n mallilomakkeet tietosuojavaltuutetun toimiston kotisivuilla (www.tietosuoja.fi)

HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVAN TOIMEKSIANTOSOPIMUKSEN TEKEMISESSÄ HUOMIOON OTETTAVIA ASIOITA (tarkistuslista).

Henkilötietolain 8 §:n 1 momentin 7 kohta oikeuttaa käsittelemään henkilötietoja rekisterinpitäjän toimeksiannosta tapahtuvaa maksupalvelua, tietojenkäsittelyä tai niihin verrattavia tehtäviä varten. Jäljempänä on listattu kysymyksiä/asioita, joita on otettava huomioon toimeksiantosopimusta tehtäessä.
(Luettelo ei ole tyhjentävä. Sopimuksen sisältö riippuu viime kädessä hankittavista palveluista)

Osapuolet:	**Huomioon sopimuksessa**
1. Kuka on rekisterinpitäjä/toimeksiantaja (henkilötietolaki 3 § 1 mom.4 kohta)	
2. Kuka on se henkilö/toimielin, jolla on oikeus rekisterinpitäjän puolesta päättää toimeksiannon tekemisestä.	
3. Kuka on toimeksisaaja (henkilö, yhteisö, yritys)	
4. Kuka on se henkilö/toimielin, jolla on oikeus tehdä sopimuksia toimeksisaajan puolesta	
5. Ketkä ovat sopijapuolten sopimusvastuuhenkilöt ja mitkä ovat heidän tehtävänsä	
Sopimuksessa määriteltäviä asioita:	
1. Henkilötietojen eri käsittelyvaiheet on kuvattava ja määriteltävä mitkä tehtävät ja käsittelyvaiheet kuuluvat toimeksiantosopimuksen piiriin. On myös sovittava mitä menettelytapoja henkilötietoja käsiteltäessä noudatetaan (Henkilötietojen käsittely voidaan määritellä tarkasti esimerkiksi palvelukuvauksessa tai vastaavassa).	
2. Toimeksiantajan ja toimeksisaajan vastuut ja tehtävät on määriteltävä käsittelyvaiheittain.	
3. Henkilötietojen käsittelyä koskevat lait ja viranomaisten antamat määräykset ja ohjeet on oltava molempien osapuolten tiedossa. Erityisesti on kiinnitettävä huomioita salassapitoa, vaitiolovelvollisuutta ja tietojen suojaamista koskeviin säännöksiin ja määräyksiin.	
4. Toimeksiantaja ja toimeksisaaja huolehtivat omalta osaltaan siitä, että tietosuojaa tai muuta salassapitoa koskevat säännökset ja viranomaisten määräykset otetaan huomioon.	
5. Toimeksisaaja antaa ennen henkilötietojen käsittelyyn ryhtymistä toimeksiantajalla riittävät sitoumukset henkilötietojen suojaamisesta tämän sopimuksen edellyttämällä tavalla. Myös toimeksisaajan henkilökuntaa koskevista salassapitositoumuksista on huolehdittava.	
6. Toimeksiantaja on henkilötietolain tarkoittama rekisterinpitäjä, jonka käyttöä varten rekisteri on perustettu ja jolla on oikeus määrätä sen käytöstä. Toimeksiantajalla on oltava mahdollisuus valvoa henkilötietojen käsittelyä ja antaa sitä koskevia määräyksiä ja ohjeita toimeksisaajalle.	
7.Toimeksiantaja ja toimeksisaaja osaltaan vastaavat henkilötietojen käytön seurannasta. On määriteltävä millä tavoin ja kuinka usein toimeksiantajalle toimitetaan loki- ja muita tietoja joita se tarvitsee valvoessaan toimeksisaajan työtä.	
8.Toimeksiantaja vastaa rekisterinpitäjänä henkilötietolain asettamista velvoitteista mukaan lukien rekisteriselosteen laatiminen ja saatavillapito, informointi sekä tarkastusoikeuden toteuttaminen. Jos toimeksisaaja avustaa rekisteröityjen oikeuksiin liittyvien toimenpiteiden toteuttamisessa on nämä tehtävät määriteltävä.	
9.Toimeksiantaja ja toimeksisaaja sopivat toimeksiannon piiriin kuuluvaan henkilötietojen käsittelyyn liittyvästä tietoturvasta ja kuinka tietoturvaan liittyviä järjestelyjä tarkistetaan ja päivitetään. Tietoturvaan liittyviä järjestelyjä on arvioitava säännöllisin määräajoin.	

10. Tietojen suojaaminen ja toimeksisaajan ohjelmistojen, sovellutusten, laitteistojen ja verkkojen käyttöoikeudet ja tietoturva toimeksiannon piiriin kuuluvissa käsittelyvaiheissa on määriteltävä ja varmistettava. Toimeksiantaja ja toimeksisaaja vastaavat siitä, että ne toteuttavat osaltaan tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomien pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta siirtämiseltä taikka muulta luvattomalta käsittelyltä.	
11. Toimeksiantaja vastaa siitä, että tietojen korjaukset, poistot ja muutokset henkilötietoihin toimitetaan toimeksisaajalle. Toimeksisaaja ottaa nämä välittömästi huomioon toimeksiannon piiriin kuuluvassa henkilötietojen käsittelyssä.	
12. Toimeksiantaja ja toimeksisaaja kartoittavat toimeksiannon toteuttamiseen liittyvät ongelmatilanteet ja niihin liittyvät menettelytavat ja vastuut.	
13. Jos toimeksisaajalla on mahdollisuus käyttää alihankkijoita tai siirtää sopimus kolmannelle osapuolelle. Mahdollisia alihankkijoita koskevat tietosuojan ja tietoturvan osalta samat vaatimukset kuin varsinaista toimeksisaajaakin. Määriteltävä myös millä ehdoilla ja mitä menettelytapoja noudattaen alihankkijoita voidaan käyttää.	
14. Toimeksisaaja ei saa käyttää tietoja hyväkseen tai luovuttaa niitä kenellekään muuten kuin sopimuksen tarkoittamassa laajuudessa ja sopimuksen mukaista tehtävää hoitaessaan. Toimeksisaaja voi käyttää tietoja vain toimeksianto-sopimuksessa määritellyillä tavoilla ja sopimuksessa määriteltyihin tarkoituksiin.	
15. Toimeksisaaja sitoutuu siihen, että henkilötietoja käsittelevät vain ne henkilöt, joiden työtehtävien hoitaminen sitä edellyttää. Toimeksiantaja ja toimeksisaaja sopivat käyttöoikeuksien antamisesta henkilötietoihin.	
16. Toimeksisaaja vastaa siitä, että samoja työvälineitä mahdollisesti käyttävät muut asiakkaat eivät pääse käsiksi toimeksiantajan tietoihin.	
17. Toimeksisaaja sitoutuu pitämään luottamuksellisina saamansa aineistot ja tiedot sekä olemaan käyttämättä niitä muihin kuin sopimuksen mukaisiin tarkoituksiin myös sopimussuhteen päättymisen jälkeenkin.	
18. Toimeksisaaja hoitaa vanhentuneet henkilötiedot sovittujen periaatteiden mukaisesti ja vahvistaa hävittämisen toimeksiantajalle. Vanhentuneen tietoaineiston osalta on määriteltävä hävittämisjankohta sekä hävittämistavat. Aineiston hävittämisessä on otettava huomioon aineiston säilyttämistä koskevat lait tai viranomaisten määräykset.	
19. Jos toimeksisaaja siirtää sopimusta tai siihen sisältyviä oikeuksia siirtää edelleen, on sovittava millä edellytyksillä niin voidaan tehdä.	
20. Millä ehdoilla sopimus voidaan peruuttaa tai sen ehtoja muuttaa ja sopimuksen päättymisen vaikutukset henkilötietojen käsittelyyn. Mitkä ovat toimenpiteet ja osapuolten vastuut toimeksiantosuhteen päättyessä.	
21. Kuinka ja missä ajassa toimeksisaajan hallussa olevat henkilötiedot toimitetaan toimeksiantajalle tai mahdolliselle uudelle toimeksisaajalle tai hävitetään	
22. Menettelytavat sopimuksen noudattamisen seurannassa ja valvonnassa	
23. Mitkä ovat sopimusrikkomusten vaikutukset ja mahdolliset vahingonkorvausvastuut ja kuinka sopimusta ja siinä sovittua henkilötietojen käsittelyä koskevat erimielisyydet ratkaistaan.	
24. Toimeksiantajan ja toimeksisaajan on huolehdittava henkilötietolain mukaisten ilmoitusten tekemisestä tietosuojavaltuutetulle - toimeksiantopalveluja hankkiva rekisterinpitäjä: rekisteri-ilmoitus - toimeksisaaja: toimintailmoitus	