TIETOSUOJAVALTUUTETUN TOIMISTO

PORTAALITOIMINNAN SUUNNITTELU JA TOTEUTUS

Päivitetty 14.04.2011

www.tietosuoja.fi

PORTAALITOIMINNAN SUUNNITTELU JA TOTEUTUS

Ohjeen tarkoitus

Tämän esitteen tarkoituksena on kuvata henkilötietolain vaatimuksien huomioimista portaalien suunnittelussa ja toteutuksessa. Ohjeistuksessa tarkastellaan portaalien henkilötietojen käsittelyn erityispiirteitä erityisesti rekisterinpitäjän velvollisuuksien näkökulmasta. Portaaleissa voidaan toteuttaa hyvinkin erilaisia liiketoimintamalleja, jotka johtavat erilaiseen vastuiden ja sopimusten kokonaisjärjestelyyn. Tässä ohjeistuksessa pyritään auttamaan portaaleissa toimivia rekisterinpitäjiä tunnistamaan lain asettamat velvollisuudet sekä helpottamaan portaali toiminnan suunnittelua ja toteutusta tietosuojan näkökulmasta. Tarkastelussa ei oteta kantaa sähköisen viestinnän tietosuojalain tarkoittamaan viestintään tai tunnistamistietojen käsittelyyn internet- ja viestintäyhteyksien muodostamisessa. Myös portaalien sisältöön ja palveluiden toimittamiseen liittyvät tekijänoikeus- ja kuluttajansuoja kysymykset on rajattu tarkastelun ulkopuolelle.

Mikä on portaali?

Portaalia on yleisesti kuvattu väyläksi yhden tai useamman organisaation tarjoamiin tuotteisiin, palveluihin, asiointipalveluihin ja tietopalveluihin. Internetissä portaali tarkoittaa siis verkkopalvelua, joka omien toimintojensa lisäksi voi tarjota pääsyn ja yhtenäisen käyttöliittymän useisiin muihin verkkopalveluihin. Portaali auttaa saamaan yhteyksiä eri toimijoiden, kuten palvelujen tuottajien ja asiakkaiden välillä.

Huolehtimalla portaalitoiminnassa kuluttajien yksityisyyden turvaamisesta, suunnittelemalla ja toteuttamalla portaalitoiminta tietosuoja huomioiden, yritykset voivat saavuttaa kilpailuetua lisääntyneen luottamuksen kautta. Luottamus internetissä tarjottaviin palveluihin ja niiden tietoturvallisuuteen on yksi kriittisimmistä palveluiden käyttämisen edellytyksistä kuluttajan näkökulmasta.

Henkilötietolaki ja portaalitoiminta

Henkilötietolain kannalta portaalitoiminnassa tulee määritellä osapuolten roolit ja vastuut sekä näiden tehtävät henkilötietojen käsittelyssä; kuka on portaalissa käsiteltävien henkilötietojen rekisterinpitäjä, mitä eri käyttötarkoituksiin perustettujen

henkilörekisterien tietoja portaalissa käsitellään ja miten varmistetaan portaalissa käsiteltävien henkilötietojen käsittelyn laillisuus. Rekisterinpitäjä (esim yritys, viranomaisorganisaatio yms) voi ylläpitää itse portaalia tai rekisterinpitäjä voi hankkia portaalipalvelut ulkopuoliselta palvelujen tuottajalta (toimeksisaajalta). Samassa liiketoiminnallisessa tai teknisessä portaalikokonaisudessa voidaan käsitellä yhden tai useamman rekisterinpitäjän rekistereiden tietoja. Jos rekisterinpitäjä hankkii portaalipalvelun ulkopuolisilta palvelujen tuottajilta, rekisterinpitäjälle asetetaan erityisiä vaatimuksia varmistaa omaan määräysvaltaansa kuuluvien henkilötietojen käsittelyn lisäksi se, ettei toiminnassa muodostu toisten rekisterinpitäjien tietojen kanssa laittomia tietoyhdistelmiä. Tällöin on etukäteen pyydettävien selvityksin ja sopimuksin varmistuttava siitä, ettei esimerkiksi tietyn rekisterinpitäjän luovuttamia tietoja yhdistetä ko portaalitoiminnassa muiden rekisterinpitäjien tietoihin laittomasti.

Rekisterinpitäjien ja toimeksiannosta henkilötietoja käsittelevien toimeksisaajien roolit voi tunnistaa vaikkapa seuraavankaltaisella yksinkertaisella menettelyllä:

1. Tunnista ketkä toimijat käsittelevät portaalitoiminnassa **henkilötietoja** ja syntyykö henkilötietojen käsittelyssä (HetiL 3 § 1 momentin 3 kohdan tarkoittama) **henkilörekisteri**. Jos syntyy niin,
2. Arvioi kunkin toimijan rooli erikseen:
    a. Mikäli henkilötietoja käsittelevä toimija on (HetiL 3 § 1 momentin 4 kohdan tarkoittama) **rekisterinpitäjä**, koskee tätä suoraan kaikki henkilötietolain vaatimukset.
    b. Mikäli toimija käsittelee henkilötietoja jonkin rekisterinpitäjän toimeksiannosta, perustuu **toimeksisaajan** oikeus käsitellä henkilötietoja (HetiL 8 § i momentin 7 kohdan mukaisesti) kyseisen rekisterinpitäjän oikeuteen, jota rekisterinpitäjän tulee kontrolloida sopimuksin.

Esimerkiksi:

- Portaalin liiketoiminta on kokonaan yhden yrityksen vastuulla, mutta palveluiden tuotantoon osallistuu yrityksiä jotka myös käsittelevät henkilötietoja. Tällöin portaalin liiketoimintaa harjoittava yritys on rekisterinpitäjä. Koska kyseinen

rekisterinpitäjä hankkii sopimukseen perustuen tietojenkäsittelypalveluita muilta yrityksiltä, jotka portaalin palveluiden tuottamiseksi käsittelevät myös henkilötietoja, ovat nämä muut toimijat toimeksisaajia. Toimeksisaajat käsittelevät henkilötietoja perustuen toimeksiantosopimukseen liiketoimintaa harjoittavan rekisterinpitäjän kanssa.

- Mikäli samassa liiketoiminnallisessa ja teknisessä portaalin palvelukokonaisuudessa toimii kaksi tai useampia portaalipalvelun tarjoajia (joilla voi olla toisiaan korvaavia tai täydentäviä tuotteita), mutta yritykset toimivat itsenäisinä yhtiöinä ja keräävät kukin henkilötietoja vain omaan käyttöönsä, on kyseessä ns. usean rinnakkaisen rekisterinpitäjän tilanne. Tällöin kukin omiin käyttötarkoituksiinsa henkilötietoja keräävä yritys on itsenäinen rekisterinpitäjä ja kunkin rekisterinpitäjän tulee itsenäisesti huolehtia, että asiakkaita informoidaan henkilötietojen käsittelystä.

Portaalia käyttävän henkilön (rekisteröidyn), kuten portaalin asiakkaan, tulee saada tietää, kenen ja keiden rekisterinpitäjien kanssa hän asioi ja kuka käyttää määräysvaltaa portaalin toiminnassa tapahtuvassa henkilötietojen käsittelyssä. Portaalia käyttävän henkilön tulee osata kääntyä asiassaan oikean rekisterinpitäjän puoleen. Portaalipalveluja suunnittelevan ja toteuttavan rekisterinpitäjän on siten suunniteltava rekisterinpitonsa ja siihen liittyvässä portaalitoiminnassa tapahtuva henkilötietojen käsittely siten, että hän voi esittää rekisteröidyille ko. tiedot laatimassaan rekisteri- ja tietosuojaselosteessa. Tämän henkilötietolain edellyttämän informoinnin on oltava käyttäjän saatavilla näkyvästi internetin kautta toteutettavan palvelun yhteydessä. Käyttäjän tulee siis voida antaessaan henkilötietoja tietää, kuka rekisterinpitäjä hänen tietojaan käsittelee, missä tarkoituksessa se tapahtuu, miten hän voi käsittelyyn liittyviä oikeuksiaan toteuttaa sekä luovutetaanko hänen tietojaan säännönmukaisesti jonnekin. Myös tietojen suojaamista koskevat tiedot ovat olennaisia tietojaan antavan henkilön kannalta. Jos portaalipalvelut hankitaan

ulkopuolisilta palveluntuottajilta, informointi on tarpeen suunnitella yhdessä portaalin toimijoiden kesken.

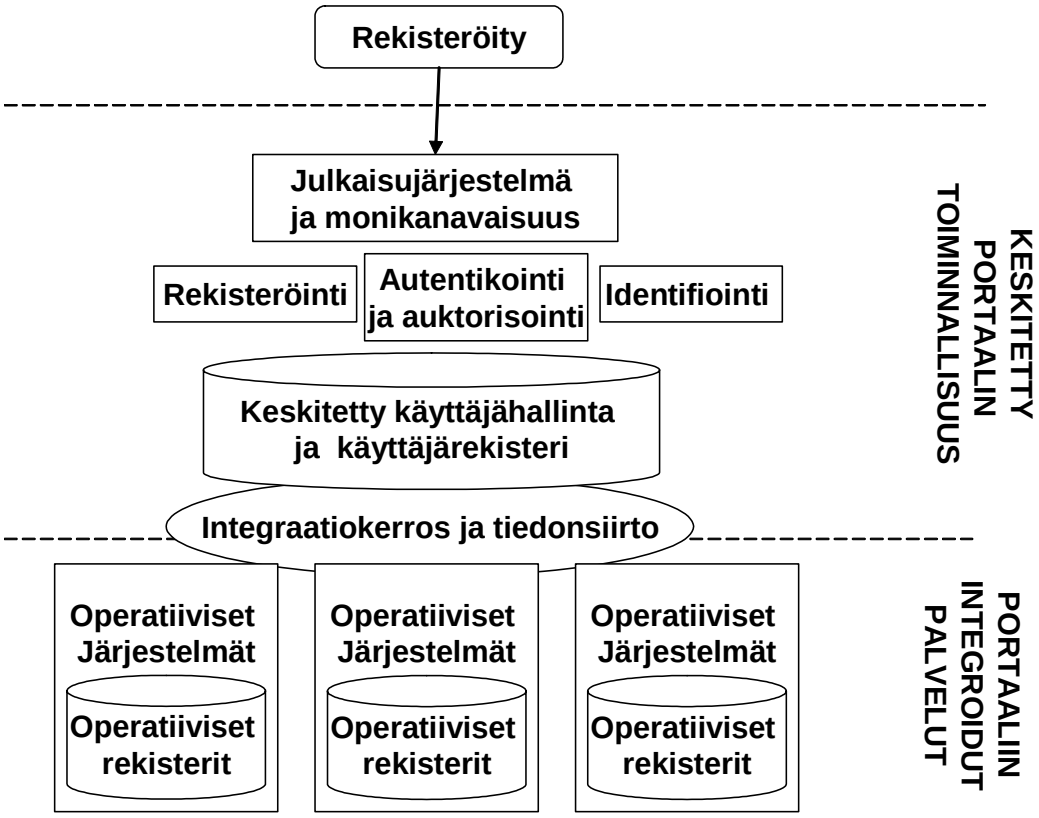
Mitä portaalilla tarkoitetaan tässä ohjeessa?

Seuraavassa käsitellään esimerkinomaisesti yhden yrityksen (rekisterinpitäjän) yhtä sähköistä palvelukanavaa. Portaalin avulla yritys tarjoaa yhdenmukaisella käyttöliittymällä asiakkaille keskitetyyn portaalirakenteeseen integroituja useiden palveluntuottajien (toimeksisaajien) palveluita. Esimerkkinä on käytetty kuluttajaliiketoiminnassa toimivaa yritystä. Ohjetta voidaan kuitenkin käyttää soveltuvin osin julkisia palveluita tarjottaessa. Portaali on siis tässä yrityksen internetpalvelu, jossa kuluttaja-asiakas voi kohdata yrityksen tarjoamat palvelut ja tuotteet. Ohjeistuksessa tarkastellaan esimerkkinä tyypillistä suuren yrityksen keskitettyä portaalipalvelua, jossa portaalin perustoiminnot tuotetaan keskitetysti ja portaalissa tarjottavat ns. operatiiviset palvelut tuotetaan portaaliin integroitujen palvelusovellusten avulla.

Esitetty portaalin rakenne yksinkertaistaa portaalin toimintakokonaisuutta ja korostaa tarkoituksella niitä toimintoja, joilla on suora yhteys henkilötietojen käsittelyyn. Portaalin rakennetta tarkasteltaessa on huomattava että pienempimuotoisissa internetsovelluksissa koko toimintakokonaisuus saattaa olla toteutettu yhdelläkin sovelluksella.

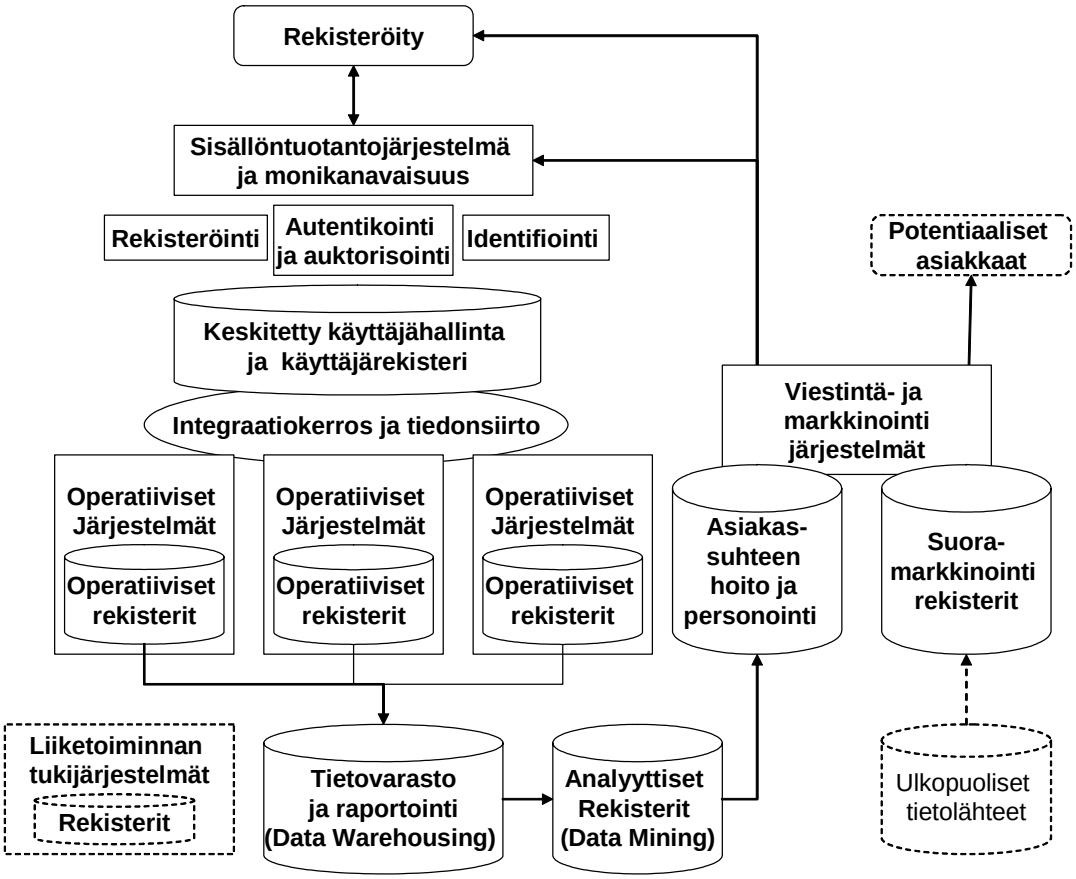
Portaalitoimintakokonaisuus on usein monen toimijan yhteistyön tulos. Samassa teknisessä portaalissa voi siis olla useita toimijoita, kuten portaalin liiketoiminnasta kokonaisuudessaa vastaava yritys, portaalin teknistä toimintaa tai sen osakokonaisuuksia kehittävät ja ylläpitävät yritykset, portaalin eri palveluita tuottavat yritykset, sovelluksia tai laitteistoja toimittavat yritykset, tietoliikenneyhteyksien tarjoajat tai vaikkapa portaalissa tuotteitaan markkinoivat yritykset. Portaalin toiminnan tekninen toteutus, ylläpito ja kehittäminen on usein jakautunut monen eri toimijan kesken. Teknisen ympäristön osalta henkilötietolaki ei ota kantaa millaisella teknisellä ympäristöllä portaalitoiminta tulisi toteutettaa. Samalla teknisellä portaalialustalla voidaan tuottaa useita itsenäisiä portaaleja tai portaaliliiketoimintoja, jotka saattavat olla kukin henkilötietolain näkökulmasta erillisiä tehtäväkokonaisuuksia.

Portaalin keskitettyjä palveluita tässä yksinkertaistetussa esimerkissä ovat internetsisällöntuotanto, käyttäjän rekisteröitymis-, autentikointi-, auktorisointi-, identifiointi- sekä integrointipalvelut. Internetsisällöntuotantojärjestelmällä voidaan muodostaa internetsivustoja, mutta mahdollisesti monikanavaisesti käyttöliittymiä myös muihin sähköisiin viestimiin, kuten matkapuhelimiin. Rekisteröitymispalvelu tarjoaa portaalipalveluun komponentin, jonka avulla portaalin asiakkaat voivat rekisteröityä portaalipalveluun antamalla tietoja itsestään sekä hyväksymällä tarpeelliset ehdot palvelun käytöstä. Rekisteröinnin yhteydessä asiakas voi tutustua yleensä myös muuhun palveluntarjoajan antamaan informaatioon. Autentikoinnilla, auktorisoinnilla ja identifioinnilla tarkoitetaan portaalin käyttäjänhallintaa, liittyen käyttäjän tunnistamiseen, käyttöoikeuksien myöntämiseen ja käyttäjän yksilöintiin portaalipalvelussa. Integrointipalveluilla tarkoitetaan rajapintoja ja komponentteja, jotka mahdollistavat useiden erilaisten palvelusovellusten toiminnan portaalin osana. Portaalipalvelukokonaisuuden tuottamiseen osallistuu esimerkissä keskitetyn portaalitoiminnallisuuden ohessa useita palvelua tuottavia ns. operatiivisia sovelluksia. Keskitetyn portaalin toiminnallisuuden avulla käyttäjälle tarjotaan eri portaalin operatiiviset palvelut siten että palveluiden käyttäjä ei välttämättä huomaa eroa siirtyessään sovelluksesta toiseen ja kokee käyttävänsä vain yhtä yhtenäistä portaalia. Portaalin tekninen palvelukokonaisuus voi muodostua siis useista erilaisista sovelluksista, joita voidaan tuottaa eri palveluiden tuottajien toimesta hajautetusti, mutta joiden palvelutarjooma voidaan koostaa keskitetysti yhteen portaalikäyttöliittymään. Portaalin keskitettyä teknistä toimintakokonaisuutta on havainnollistettu kuvassa 1.



Kuva 1. Esimerkki yhden rekisterinpitäjän portaalin keskitetystä portaaliratkaisusta ja palveluiden integroinnista.

Operatiivisten sovellusten lisäksi laajemmissa yrityksen portaaliratkaisussa voi portaaliin olla integroitu myös asiakastietojen tietovarastointi-, analysointi- tai markkinointijärjestelmiä, joissa käsitellään henkilötietoja. Henkilötietoja käsitellään yleensä myös liiketoiminnantuki-, toiminnanohjaus-, laskutus- ja viestintäjärjestelmissä sekä toimistosovelluksissa. Henkilötietojen käsittelyn näkökulmasta myös nämä järjestelmät on huomioitava osana tietosuojan järjestämistä, silloin kun niissä käsitellään henkilötietoja osana rekisterinpitäjän toimintaa. Portaalin laajennettua toimintakokonaisuutta on havainnollistettu kuvassa 2. Toiminnassa on kyettävä erottelemaan ja kuvattava eri tehtävissä tapahtuvan henkilötietojen käsittelyn tarkoitukset, joita on syytä verrata rekisterinpitäjän ja rekisteröidyn väliseen perussuhteeseen.



Kuva 2. Esimerkki yhden rekisterinpitäjän portaalin laajennetusta toimintakokonaisuudesta.

Portaaliympäristössä rekisteröidyllä tarkoitetaan HetiL 3 § 1 momentin 5 kohdan mukaan henkilöä jota henkilötieto koskee, eli kaikkia portaalia käyttäviä jotka portaalia käyttäessään tunnistetaan ja joiden tietoja portaalipalvelua toteutettaessa käsitellään. Kuluttajaliiketoiminnassa rekisteröityjä ovat käytännössä kuluttaja-asiakkaat. Rekisterinpitäjä on HetiL 3 § 1 momentin 4 kohdan mukaisesti yksi tai useampi henkilö, yhteisö, laitos tai säätiö, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty.

Portaalin liiketoiminnasta ja teknologiasta vastaava rekisterinpitäjä voi hankkia palveluita, kuten portaalin teknistä ylläpitoa, myös ulkopuoliselta palvelutoimittajalta sopimuksen perusteella. Tätä henkilötietolain HetiL 32 § 2 momentin kuvaamaa itsenäistä elinkeinonharjoittajaa, joka toimii rekisterinpitäjän lukuun, kutsutaan tässä ohjeessa **toimeksisaajaksi** ja rekisterinpitäjää vastaavasti **toimeksiantajaksi.**

Portaalin palvelukokonaisuuden muodostuessa useiden eri toimijoiden tarjoamista palveluista on erityisen tärkeää määritellä ja suunnitella, ketkä vastaavat henkilötietojen käsittelystä HetiL 3 § 4 kohdan tarkoittamana rekisterinpitäjänä ja ketkä käsittelevät henkilötietoja toimeksiannosta toimeksisaajina. Portaalin palvelutoiminnallisuuden, liiketoimintamallin ja sopimusrakenteen on oltava selkeitä ja yhteensopivia, sekä yksiselitteisesti määriteltyjä myös henkilötietojen käsittelyn roolien osalta.

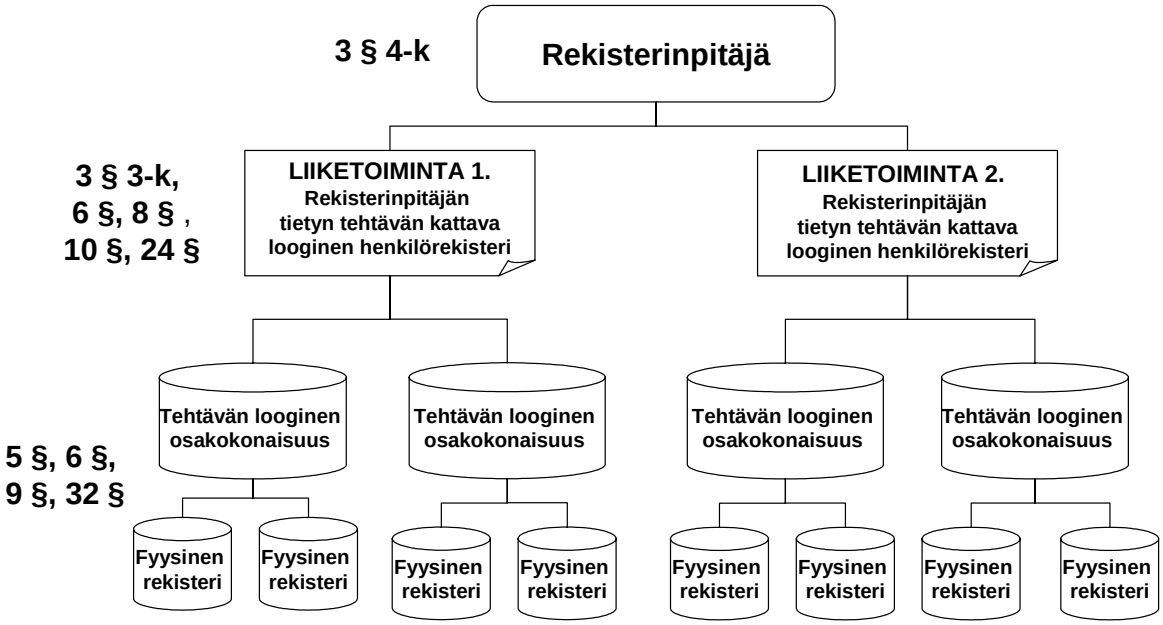
Henkilötietojen käsittelyn yleisistä edellytyksistä on säädetty HetiL 8 §:ssä. Portaalien osalta tyypillisiä HetiL 8 § mukaisia henkilötietojen käsittelyn yleisiä edellytyksiä ovat asiakkaan 1 momentin 1 kohdan mukainen rekisteröidyn yksiselitteinen suostumus ja/tai 1 momentin 5 kohdan mukainen asiallinen yhteys rekisterinpitäjän toimintaan, kuten asiakassuhde (yhteysvaatimus). Myös käsiteltävien henkilötietojen **käyttötarkoitukset** on määriteltävä HetiL 7 § käyttötarkoitussidonnaisuuden periaatteen mukaisesti siten että niistä ilmenee minkä tehtävien suorittamiseksi henkilötietoja kerätään. Käyttötarkoitukset on kuvattava loogisten kokonaisuuksien mukaisesti. Loogisella rekisterillä tarkoitetaan tiettyä tehtävää varten perustettua henkilörekisteriä, johon kuuluvat kaikki tiedot, joita kyseisessä tehtävässä kerätään ja käsitellään, vaikka tietoja pidettäisiin teknisesti erillisissä rekistereissä. HetiL:n käyttötarkoitussidonnaisuusvaatimus merkitsee, ettei henkilörekisterin talletettuja henkilötietoja saa käyttää muuhun kuin määriteltyyn käyttötarkoitukseen.

Henkilötietolaki asettaa rekisterinpitäjälle **informointivelvoitteen** HetiL 10 § ja HetiL 24 § mukaisesti. Rekisteriselosteen ja muun vaadittavan informaation voi esittää verkkopalvelussa rekisteröidylle osana ns. tietosuojaselostetta. Tietosuoja-selosteessa voi, HetiL 10 § esittämän rekisteriselosteen informaation lisäksi, esittää rekisteröidylle myös muut informaatiovelvoitteen täyttämiseksi vaadittavat tiedot, kuten HetiL 24 § vaatima informaatio[1]. Tietosuojaseloste on siis apuväline, jolla rekisterinpitäjä voi osaltaan täyttää henkilötietolain asettaman rekisteröidylle ulospäin

[1] On myös huomattava, että mikäli palvelun tuotannon yhteydessä käytetään evästeitä (cookies), on niistä informoitava kuten sähköisen viestinnän tietosuojalain (516/2004) 7 § edellyttää.

näkyvän informointivelvoitteen. HetiL 10 § ja HetiL 24 § tiedonantovelvollisuudet kohdistuvat koko henkilötietojen käsittelyn tehtävään, kuten portaalin liiketoimintokokonaisuuteen. Informaatio on voitava siis antaa tehtävätasolla, erikseen kutakin eri tehtävää, kuten tiettyä liiketoiminnallista käyttötarkoitusta, varten perustetun henkilörekisterin osalta.

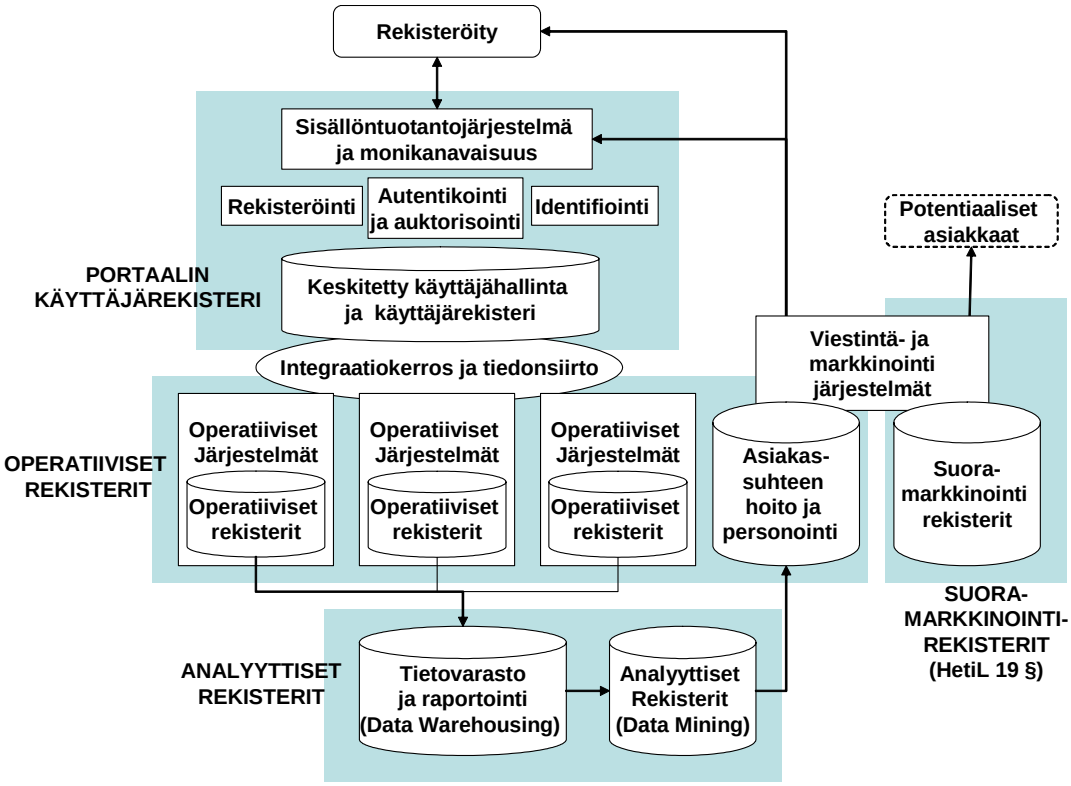
Tietoja informointivelvoitteen toteutuksesta löytyy tietosuojavaltuutetun toimiston esitteistä ”Rekisterinpitäjällä yleinen informointivelvollisuus 1.6.1999 alkaen” ja ”Laadi tietosuojaseloste**” .**



Kuva 3. Loogisten henkilörekisterien rakenne

Henkilörekisteri on siis henkilötietolain käsitteistössä looginen kokonaisuus. Rekisterinpitäjän tiettyä tehtävää, kuten tiettyä liiketoiminnallista käyttötarkoitusta, varten perustetun henkilörekisterin voi monimutkaisemmissa portaaliympäristöissä jakaa useisiin loogisiin osakokonaisuuksiin, jotta tietosuojatoiminta olisi hallittavissa ja johdettavissa. Portaaliympäristöjen tyypillisiä loogisia osakokonaisuuksia ovat esimerkiksi portaalin käyttäjärekisteri, operatiiviset rekisterit, analyyttinen rekisteri ja suoramarkkinointirekisterit. Portaalin käyttäjärekisteri on esimerkissä keskitetyn portaalitoiminnallisuuden ja erityisesti portaalin käyttäjähallinnan muodostama osakokonaisuus, jossa käsitellään henkilötietoja käyttäjän rekisteröitymistä, tunnistamista, käyttöoikeuksien hallintaa sekä yksilöintiä varten. Operatiivisten

rekisterien (kuten erilaiset portaalin palveluita tuottavat sovellukset, asiakaspalvelu- tai asiakasviestintäsovellukset) osakokonaisuuden tyypillinen käyttötarkoitus on portaaleissa palvelun tuottaminen sekä palvelutarjooman kehittäminen ja ylläpito sekä asiakassuhteen hoitaminen, hallinta ja kehittäminen. Eri operatiivisten toiminnallisuuksien ja sovellusten osalta voi myös muodostua eri erillisiä henkilötietolain tarkoittamia käyttötarkoituksia, joita voi olla syytä tarkastella omana osakokonaisuutenaan. Analyyttisessä rekisteriosakokonaisuudessa (kuten data warehousing ja data mining ratkaisuissa) jalostetaan ja yhdistellään yleensä käyttäjätietoja uudeksi, portaalin toiminnassa hyödynnettäväksi informaatioksi asiakassuhteen kehittämis-, palveluiden personointi ja markkinointi tarkoituksissa. Suoramarkkinointirekisterien käyttötarkoitukset ovat yleensä markkinointikampajoiden ja uusasiakashankinnan toteuttaminen. Liiketoiminnan tukijärjestelmiä tai toimistosovelluksia ei esimerkissä ole esitetty erikseen, mutta nekin on huomioitava toimintokokonaisuudessa. Myös tietojärjestelmissä palveluiden käytöstä syntyvät lokitiedot muodostavat mahdollisesti eri käyttötarkoituksiensa mukaisia henkilörekistereitä. Kaikki nämä rekisteritoiminnot on suunniteltava ja tarpeen kuvata henkilötietojen käsittelylle asetettujen henkilötietolain vaatimusten kannalta. Myös käsittelyjen lainmukaisuus on varmistettava kaikissa käsittelyvaiheissa. Henkilötietojen käsittelyn näkökulmasta kaikki järjestelmät on siten huomioitava osana tietosuojan järjestämistä, silloin kun niissä käsitellään henkilötietoja osana rekisterinpitäjän toimintaa. Loogisten osakokonaisuuksien suhdetta portaalin laajennettuun toimintokokonaisuuteen havainnollistetaan kuvassa 4.

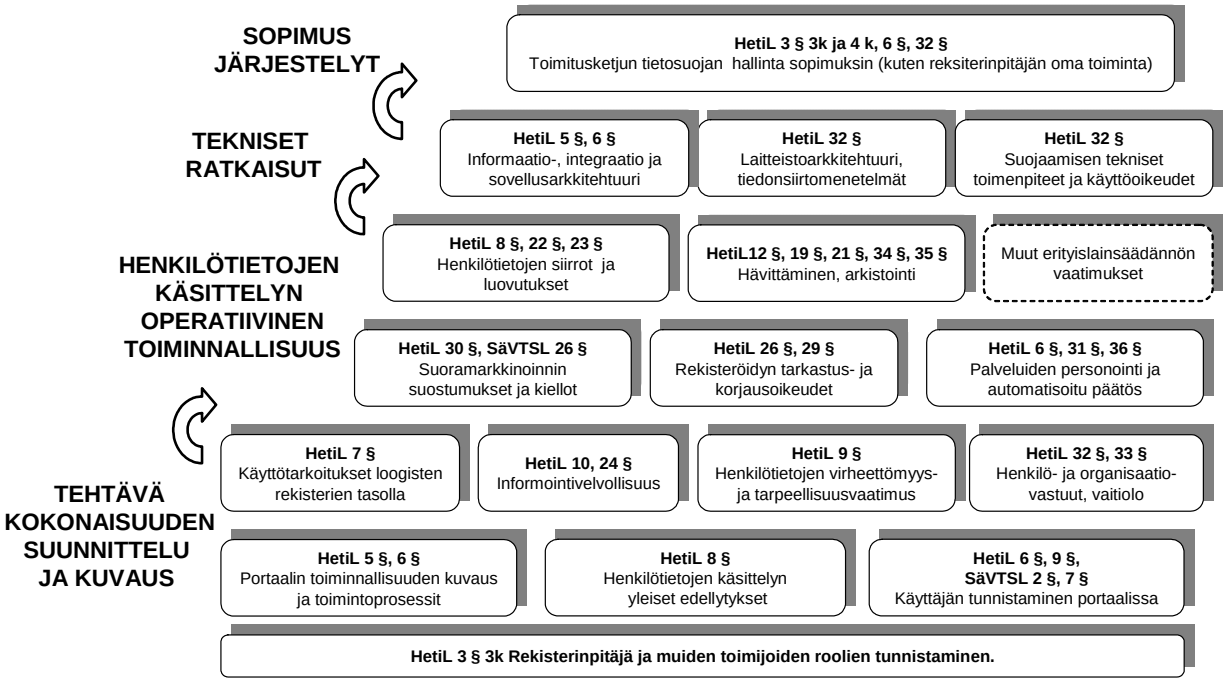


Kuva 4. Esimerkki yhden rekisterinpitäjän portaalin loogisista osakokonaisuuksista.

HetiL 6 § suunnitteluvelvoitteen ja HetiL 5§ huolellisuusvelvoitteen yhteydessä esitetyn hyvän tietojenkäsittelytavan noudattamisen kannalta tulee portaalin henkilötietojen käsittelyn toiminnallisista edellytyksistä varmistua ja rekisterinpitäjän tulee analysoida toimintansa. Koska teknisen toteutuksen osalta toimintoprosessit ja henkilötietojen käsittelyn vaiheet linkittyvät kiinteästi portaalin loogiseen informaatio-, integraatio- ja sovellustason arkkitehtuuriin, tulisi analyysissä portaalin toimintakokonaisuus ja toimintoprosessit kuvata siten, että henkilötietojen käsittelyn vaiheet ja tavat tunnistetaan.

Henkilötietojen käsittelyn suunnittelun tulee kattaa myös tekninen laitteistoarkkitehtuuri, tiedonsiirtomenetelmät sekä HetiL 32 § tarkoittamat tekniset tietosuoja- ja tietoturvaratkaisut. Portaalin suunnittelussa ja toteutuksessa tietosuojavaatimusten huomioon ottaminen etenee loogisesti toiminnan kuvaamisesta operatiivisen toiminnallisuuden kuvaamiseen. Näiden kuvausten perusteella voidaan suunnitella tekniset ratkaisut. Rekisterinpitäjän tulee lisäksi vastata myös toimeksisaajan toimeksiannosta suorittamasta henkilötietojen käsittelystä. Vasta kun

rekisterinpitäjän oma toiminta on kuvattu ja hallinnassa, on mahdollista ohjeistaa ja määrätä hallitusti sopimuksin toimeksisaajien henkilötietojen käsittelyä. Portaalin tietosuojan suunnittelun ja toteutuksen etenemisjärjestystä havainnollistetaan kuvassa 5.



Kuva 5. Portaalin tietosuojan suunnittelun ja toteutuksen etenemisjärjestys

Koska rekisteröityjä koskevilla henkilötiedoilla on huomattava merkitys portaalin ylläpitäjän palvelutuotannossa, on ne rekisterinpitäjänkin intressissä suojattava. HetiL 32 § vaatii rekisterinpitäjää lisäksi myös **organisoimaan** henkilötietojen käsittelytoimintansa siten että tietojen suojaamisesta huolehditaan. Käytännössä toiminnan organisointi tarkoittaa velvollisuutta nimetä organisaatioon vastuuhenkilöt sekä jakaa heidän vastuunsa ja tehtävänsä siten että toiminnan kokonaisuuden lainmukaisesta ja laadukkaasta hoitamisesta voidaan varmistua. Tietosuojasta huolehtiminen on selkeintä liittää mahdollisimman luontevaksi osaksi organisaation normaalia toimintaa. Henkilötietojen käsittelytoiminta ja sen mukainen tietosuojatoiminta on dokumentoitava ja siitä on laadittava henkilöstölle kattava organisaation sisäinen ohjeistus. Henkilötietoja käsittelevää, erityisesti vastuuasemissa olevaa, henkilöstöä on myös koulutettava riittävästi.

Portaalipalveluiden suunnittelun erityispiirteenä on portaalintoimintaa suunniteltaessa määriteltävä vaativatko portaalissa tarjottavat palvelut **käyttäjien tunnistamista**. Samassa portaalissakin tarjottavien eri palveluiden osalta tunnistamisen tarpeet voivat poiketa toisistaan. Palvelun käyttäjältä ei tule vaatia tunnistautumista ellei se ole perustellusti tarpeellista. Rekisterinpitäjän on määriteltävä käyttämänsä tunnistamisen tasot ja menetelmät joilla tunnistus eri tasoilla toteutetaan sekä ryhmitellä portaalissa tarjottavat palvelut tunnistamistasojen mukaan. Kyseessä on samalla henkilötietojen tietorakenteiden suunnittelu, joka vaikuttaa portaalin tekniseen toteutukseen. Yleistäen ja yksinkertaistaen portaalin käyttäjät voidaan ryhmitellä neljään käyttäjäryhmään tunnistamisen tasojen perusteella. Anonyymit käyttäjät ovat henkilötasolla tunnistamattomia sivustolla vierailijoita. Pseudonyymit käyttäjät toimivat portaalissa nimimerkillä tai muulla alias- tai nimimerkillä, ilman että heitä pystytään yleensä yhdistämään yksittäiseen henkilöön. Heikosti tunnistetut käyttäjät ovat henkilötietojaan rekisteröitymisen yhteydessä luovuttaneita, ilman että heidän henkilöllisyyttä on identifioitu. Vahvasti tunnistetut käyttäjät ovat portaalin käyttäjiä, joiden henkilöllisyys on identifioitu[2].

Toinen portaalien suunnittelun erityispiirre liittyy profilointiin ja personointiin internetpalvelussa. **Profiloinnilla** tarkoitetaan tässä asiakkaan ominaisuuksia kuvaavien uusien tietojen muodostamista jo olemassaolevien tietojen perusteella lähinnä analyyttisten tietojärjestelmien avulla. **Personoinnilla** tarkoitetaan kyseisten profiilitietojen hyödyntämistä portaalin palveluiden muodostamisessa, siten että portaalin käyttöliittymä tai palvelut muodostuvat erilaisiksi eri asiakkaille, mahdollisimman paljon heidän henkilökohtaisia tarpeitaan vastaaviksi. Personointi tuotetaan profiilien perusteella portaalin palveluita tuottavissa operatiivisissa järjestelmissä tai internetsisällöntuotantojärjestelmässä. Profilointia tai personointia ei lähtökohtaisesti ole tietosuojalainsäädännössä kielletty, mutta personoinnin ja profiloinnin osalta rekisterinpitäjän tulee olla erityisen tarkka henkilötietojen käsittelyn perusteista. Profiloinnin ja personoinnin tarpeellisuudesta, sekä erityisesti profiilien käyttötarkoitukseen nähden riittävästä virheettömyydestä, on varmistuttava ennakoivasti henkilötietolain 9 § tarpeellisuus- ja virheettömyysvaatimuksen

[2] ”Vahvaa tunnistamista tulisi vaatia sellaisissa palveluissa, joissa käsitellään luottamuksellisia tietoja, kuten henkilötietolain mukaisia arkaluonteisia tietoja tai organisaation salassa pidettäviä tietoja, tai kun käyttäjä voi tehdä sellaisia asioita, joilla on taloudellista tai oikeudellista merkitystä”. (Liikenne- ja viestintäministeriön Luoti-julkaisuja 8/2006 ”Tietoturvaopas sähköisen palvelun tarjoajalle”, s. 28. http://www.mintc.fi/web/fi/julkaisu/view/821061)

mukaisesti. Rekisteröityä on myös informoitava selkeästi HetiL 10 § ja 24 §:n henkilötietojen käsittelyn tarkoituksista ja rekisteröityihin liittyvistä käsitellyistä tiedoista tai tietoryhmistä. Personoinnin osalta on lisäksi arvioitava onko kysymyksessä HetiL 31 § mukainen automatisoitu päätös, silloin kun profiilin perusteella personoidaan automaattisesti portaalin palvelua eikä personointipäätöksen muodostamiseen osallistu henkilöitä ja automaattisesta personoinnista aiheutuu asiakkaalle oikeudellisia tai muita merkittäviä vaikutuksia. Automatisoidusta päätöksenteosta on personoinninkin osalta on ilmoitettava (Hetil 36 § 2 momentin mukaisesti) tietosuojavaltuutetulle silloin kun automatisoidun päätöksenteon järjestelmä otetaan käyttöön.

Rekisterinpitäjän toimeksiantotehtäviin liittyvä vastuu kattaa tietojenkäsittelypalvelua ostettaessa myös toimeksiannosta suoritettavan henkilötietojen käsittelyn toimeksisaajankin toiminnan osalta. Henkilötietojen käsittelyyn liittyvistä asioista on sovittava kirjallisesti. Käytännössä portaaliympäristössä tietojenkäsittelypalvelu voidaan ostaa ulkopuoliselta tekemällä toimeksiantosopimus palvelut tilaavan rekisterinpitäjän ja palvelun toimittavan toimeksisaajan välillä. Kyseinen rekisterinpitäjä vastaa tällöin toimeksiantona suoritettavan henkilötietojenkäsittelytoiminnan laillisuudesta ja toimeksisaaja vastaa edelleen henkilötietojen käsittelystä osapuolten välillä tehtävän toimeksiantosopimuksen mukaisesti. Koska tietoturva- ja tietosuojariskit osaltaan lisääntyvät ja muuttuvat toisenlaisiksi, kun tietojenkäsittelypalvelua ostetaan ulkopuoliselta yritykseltä, on tärkeää määritellä riittävän yksityiskohtaisesti mitkä tehtävät ja vastuut jäävät toimeksiantajalle. Toimeksiannoissa sopimus on väline, jonka avulla rekisterinpitäjä voi määrätä toimeksisaajien henkilötietojen käsittelystä, varmistua tietosuojan laadusta ja hallita tietosuojaan liittyviä riskejään. Tietosuojan osalta toimeksiantosopimuksessa huomioitavia seikkoja kuvataan liitteessä 1.

Toimeksiantosopimuksiin liittyviä kysymyksiä sekä asian edellyttämää suunnittelun toteutustapaa on tarkasteltu myös tietosuojavaltuutetun toimiston esitteessä; ”Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset ” .

LIITE 1.

Tarkastuslista: Mistä toimeksiantosopimuksessa on sovittava?

Rekisterinpitäjän ja toimeksisaajan on sovittava toimintaan liittyvästä henkilötietojen käsittelystä. Sopimuksen sisältö ja sopimuksen kohde riippuvat tapauskohtaisesti hankittavasta palvelusta ja sopimuksen osapuolten toimialan lainsäädännöstä ja käytännöistä. Tässä tarkastuslistassa on pyritty listaamaan olennaisia henkilötietolaista johtuvia seikkoja, jotka on huomioitava sopimusta laadittaessa henkilötietojen käsittelyn osalta. Henkilötietojen käsittelyn osalta ei tarvitse laatia erillistä sopimusta, vaan riittää että palvelusopimuskokonaisuudessa, jolla palvelu hankitaan, on huomioitu esitetyt seikat. Sopimustekniikasta riippuen osa tarkistuslistan seikoista voidaan huomioida myös toimeksisaajaa sitovassa toimeksiantajan antamassa tarkastuslistan kohdan 8. tarkoittamassa ohjeistuksessa. Dokumentti täydentää tietosuojavaltuutetun antamaa ohjeistusta toimeksiantosopimusten tekemisestä ja on soveltaen käyttökelpoinen portaalien ohella myös henkilötietojenkäsittelyn muissakin ulkoistamistilanteissa.

1. **Osapuolet:**
    - Rekisterinpitäjä/toimeksiantaja (HetiL 3 § 1mom. 4 kohta) ja rekisterinpitäjän päätösvaltainen edustaja.
    - Toimeksisaaja ja toimeksisaajan päätösvaltainen edustaja.
    - Osapuolten yhteys- ja muut vastuu henkilöt sekä heidän henkilötietojenkäsittelyyn liittyvät tehtävänsä.
2. **Henkilötietojen käsittely hankittavassa palvelukokonaisuudessa.**
   Palvelusopimuksessa tai sen liitteissä on kuvattava henkilötietojen käsittelyn vaiheet ja loogiset kokonaisuudet (loogiset rekisterit) on kuvattava ja määriteltävä mitkä tehtävät ja käsittelyvaiheet kuluvat toimeksiannon piiriin. On myös kuvattava mitä toiminta- ja menettelytapoja henkilötietojen käsittelyssä noudatetaan. Loogisten rekisterien ja loogisen sovellus-, integraatio- ja informaatioarkkitehtuurien kuvaukset sekä yksityiskohtaiset menettelytapakuvaukset voidaan liittää sopimuksen liitteeksi. Olennaista on että

toimeksiantajan ja toimeksisaajan vastuut ja tehtävät on määriteltävä käsittelyvaiheittain riittävällä tarkkuudella. (HetiL 5§-6 §, 32 §)

3. **Asiakastiedon ja henkilötiedon määräysvalta.** Rekisterinpitäjällä on määräysvalta ja lain puitteissa oikeus määrätä ja käsitellä asiakastietoja. Tämä määräysvalta käsittää myös henkilötiedot jotka syntyvät toimeksiannossa toimeksisaajan toiminnassa. Tämä on henkilötietolain lähtökohta, mutta väärinymmärrysten välttämiseksi tästä voi olla hyvä mainita sopimuksessakin.
4. **Henkilötietojen suojaaminen ja tietoturva.** Toimeksisaajan on annettava toimeksiantajalle riittävät sitoumukset henkilötietojen teknisestä suojaamisesta henkilötietojen käsittelyn kaikissa vaiheissa. Sopimusehdoin on varmistuttava henkilötietojen suojaaminen asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Henkilötietojen suojaamisen ja tietoturvallisuuteen liittyviä ratkaisuja on arvioitava ja päivitettävä säännöllisesti. Rekisterinpitäjän kannattaa varata sopimuksessa mahdollisuus myös ulkopuolisen auditoijan käyttöön. (HetiL 32 §)
5. **Salassapito.** Henkilötietojen ja niiden käsittelyn salassapidosta on sovittava yritysten välillä, huomioiden myös toimeksisaajan henkilöstön salassapitositoumukset. Henkilötietoja käsitteleviltä voidaan kriittisimmissä toiminnoissa, kuten arkaluonteisten tietojen osalta, vaatia henkilökohtaiset salassapitositoumukset ennen kuin henkilö hyväksytään henkilötietoja käsittelemään. Henkilötietoja käsittelevien on lisäksi tunnettava jokaista henkilötietoja käsittelevää koskeva HetiL 33 § määräys vaitiolosta. Toimeksisaajan tulee sitoutua myös pitämään luottamuksellisina vastaanottamansa aineistot ja tiedot sekä olemaan käyttämättä niitä muihin sopimussuhteen mukaisiin tarkoituksiin. (HetiL 32 §, 33 §)
6. **Seuranta ja valvonta.** Rekisterinpitäjän tulee varmistua oikeuksistaan valvoa ja koordinoida toimeksisaajan henkilötietojen käsittelyä ja sopimuksen noudattamista. Rekisterinpitäjällä pitää olla mahdollisuus saada tietoonsa henkilötietojen käsittelyn kannalta olennaiset tiedot. Toimeksiantajan tulee seurata sovitulla tavalla toimintaa ja raportoida siitä säännöllisesti. Palvelutason seurantaa varten voidaan asettaa erillisiä palvelutason mittareita, joista voidaan sopia erikseen teknisluonteisemmassa palvelutasosopimuksessa (SLA, Service

Level Argreement) pääsopimuksen liitteenä. Myös toiminnan laadun seurannasta ulkopuolisin auditoinnein voidaan sopia. (HetiL 32 §)

7. **Dokumentaatio.** Sopimuksessa on määriteltävä millaista ja miten tietosuojaan liittyvään dokumentaatiota ja millaisia toiminnan kuvauksia ylläpidetään toimeksisaajan toimesta.
8. **Ohjeet ja määräykset.** Rekisterinpitäjällä tulee olla mahdollisuus vaikuttaa toimeksisaajan henkilötietojen käsittelyyn koko sopimussuhteen ajan sekä antaa henkilötietojen käsittelyä koskevia ohjeita ja määräyksiä. (HetiL 32 §)
9. **Henkilötietojen siirrot osapuolten välillä.** Sopimuksessa on määriteltävä millä tavoin, mitä tietoja, kuinka usein ja millä ehdoin henkilötietoja siirretään osapuolten välillä. Myös lokitietojen saatavuudesta ja siirroista on sovittava. (HetiL 8 § 2 momentti)
10. **Henkilötietojen luovutukset ulkopuolisille.** Toimeksisaaja ei saa luovuttaa henkilötietoja ulkopuolisille kuin sopimuksessa määrätyssä laajuudessa ja sopimuksessa määrätyin edellytyksin. Erityisesti henkilötietojen luovutuksista Euroopan unionin ulkopuolelle on sovittava riittävän yksityiskohtaisesti. Myös henkilötietojen siirto toimeksiantajan muiden saman toiminnan tuotantoon osallistuvien toimeksisaajien välillä on huomioitava. (HetiL 8 § 2 mom., 22 § -23 §)
11. **Rekisteröidyn informointi.** Rekisteröidyn informointi on rekisterinpitäjän velvollisuus. Sopimuksesta on käytävä ilmi, mikäli toimeksisaajalla on oikeuksia tai velvollisuuksia avustaa rekisterinpitäjää informointivelvoitteen suorittamisessa, kuten tietosuojaselosteen esillä- tai ylläpidossa. (HetiL 10 §, 24 §, 25 §)
12. **Tarkastus-, oikaisu- ja kielto-oikeus.** Sovittava mitkä tehtävät rekisteröidyn tarkastus-, oikaisu- ja kielto-oikeuksien toteuttamiseksi suoritetaan toimeksiantajan ja toimeksisaajan toimesta. Siltä osin kun tarkastettavia tai oikaistavia henkilötietoja tai markkinointikieltoja käsitellään toimeksisaajan tietojärjestelmissä on sopimuksin varmistuttava että toimeksiantajan ja toimeksisaajan toimintaprosessit ja menettelytavat ovat yhteensopivia. Toimeksiantajan tulee vastata että tarvittavat tiedot henkilötietojen korjauksia, oikaisuja tai muutoksia varten toimitetaan toimeksisaajalle, jonka velvollisuuksiin tietojen toimitusta seuraavat toimenpiteen kuuluvat. Suoramarkkinointikieltojen

osalta on lisäksi huomattava myös sähköiseen suoramarkkinointiin vaadittavan suostumuksen hallinnointi. (HetiL 26 §-28 §, 29 §, 30 § ja SäVTSL 26 §)

13. **Immateriaalioikeudet, lisenssit ja muut käyttöoikeudet.** Osapuolten oikeudet immateriaalioikeuksin suojattuihin kohteisiin kuten henkilötietojen käsittelyssä tarvittavaan kirjalliseen aineistoon tai patentteihin on varmistettava. Samoin käyttöoikeudet henkilötietojen käsittelyssä tarvittaviin ohjelmistoihin, laitteistoihin ja tiedonsiirtoverkkoihin on varmistettava molemmille osapuolille. Ennen sopimista on varmistuttava ettei mm. kyseisiä kohteita rasita kolmannen oikeus tai sopimusehto, joka aiheuttaisi esteitä henkilötietojen käsittelytoiminnasta sopimiselle.
14. **Henkilötietoja käsittelevät henkilöt.** Sopimuksessa tulee määrätä että henkilötietoja käsittelevät toimeksisaajan puolella vain ne henkilöt, joiden tehtävien hoitaminen sitä edellyttää. Toimeksiantaja ja toimeksisaaja voivat sopia myös menettelystä, jolla sopimuskauden aikana voidaan henkilötietojen käsittely ja käyttöoikeuksia antaa, valvoa ja poistaa. Erityinen huomio kannattaa kiinnittää että toimeksisaaja vastaa siitä että samoja sovelluksia ja työvälineitä käyttävät muut kuin sopimuksen perusteella hyväksytyt henkilöt eivät pääse käsiksi toimeksiantajan tietoihin.
15. **Tietojen hävittäminen.** Sopimusehdoissa on hyvä erikseen määrätä miten ja milloin toimeksisaaja hävittää vanhentuneet ja tarpeettomat henkilötiedot ja vahvistaa hävittämisen toimeksiantajalle. Sopimuksessa tulee määrittää mahdolliset tietojen ja aineistojen hävittämistavat myös sopimussuhteen päättyessä tai purkautuessa. (HetiL 9 §, 32 §)
16. **Menettelyt ongelmatilanteissa.** Menettelytavoista ja vastuista erityyppisissä vika-, häiriö- ja ongelmatilanteissa on sovittava. Menettelytapoja on arvioitava ja päivitettävä säännöllisesti.
17. **Muutoshallinta.** Toiminnan kehittyessä osapuolten toiminnan on myös muututtava. Sopimuksessa tulisi määrittää mekanismit, joiden mukaisesti osapuolet voivat ehdottaa muutoksia, päättää muutoksista ja toteuttaa niitä siten että sopimusvelvoitteet muutuvat muutosten mukaisesti. Muutokset saattavat kohdistua myös sovelluksiin ja käytettävään teknologiaan. Tällöin muutoshallinnan mekanismin tulisi olla yhteensopiva mm. sovelluskehitys ja systeemityön menettelyjen kanssa.

18. **Toimeksisaajan alihankkijoiden käyttö.** Sopimusehdoissa tulee määrätä voiko ja jos voi niin millä edellytyksillä toimeksisaaja käyttää alihankkijoita, siten ettei tietosuojaa tai tietoturvallisuutta vaaranneta.
19. **Sopimuksen päättyminen, purku ja sopimuksen siirto kolmannelle** (Exit – suunnitelmat). Sopimuksessa on jo laatimisvaiheessa sovittava miten sopimuksen normaali päättyminen, purkaminen jonkin purkuperusteen osalta tai sopimuksen siirto kolmannelle vaikuttaa henkilötietojen käsittelyyn. Mitkä ovat toimenpiteen, vastuut ja velvollisuudet myötävaikuttaa henkilötietojen käsittelyn osalta erityisesti tietojen käsittelyn siirtymäaikana. Sopimuksen purkamiseen oikeuttavat sopimusrikkomukset on määriteltävä sekä millainen on tietojärjestelmien ja tietosuojan osalta ns. ylivoimainen este. Tulee sopia myös kuinka henkilötiedot toimitetaan uudelle henkilötietojen käsittelijälle tai hävitetään. Sopimuksessa tulee määrätä saako toimeksisaaja siirtää sopimusta edelleen ja millä edellytyksillä.
20. **Vahingonkorvausvastuut ja sopimussakko.** Toimeksisaajan vahingonkorvausvelvollisuudesta sekä sen perusteista on sovittava. Vahingonkorvausvastuun laajuudesta tulee ottaa sopimukseen määräys erityisesti välittömien vahinkojen osalta. Sopimusrikkomuksista voidaan määrätä myös suoraan sopimussakkoja. Erityistä huomiota tulee kiinnittää määrittelyyn millainen on vahingonkorvauksen tai tietosuojan osalta sopimussakon laukaiseva tietosuojarikkomus ja millainen on tietojärjestelmien ja tietosuojan osalta ns. ylivoimainen este. (HetiL 47 §)
21. **Erimielisyyksien ratkaisu osapuolten välillä.** Osapuolet voivat sopimuksessa määrätä menettelyt kuinka erimielisyydet ratkaistaan osapuolten välillä henkilötietojen käsittelyyn liittyvien erimielisyyksien osalta.
22. **Oikeuspaikan valinta ja sovellettavan lain valinta.** Sopimuksessa kannattaa määrätä ratkaisuvaltainen tuomioistuin sekä henkilötietojen käsittelynosalta sovellettavat lait tai lainsäädäntökehikon myös tietosuojan osalta. Tuomioistuimien sijaan voidaan myös määrätä riidanratkaisumenettelyksi välimiesmenettely.
23. **Tietosuojalainsäädännön tuntemus.** Sopimusta laadittaessa on varmistuttava ja dokumentoitava että henkilötietojen käsittelyä koskevat lait ja viranomaisen määräykset ja ohjeet ovat molempien osapuolien tiedossa. (HetiL 32 §)