TIETOSUOJAVALTUUTETUN TOIMISTO

MALLI HENKILÖTIETOJEN KÄSITTELYN / HENKILÖREKISTERIN REKISTERITOIMINTOJEN ANALYSOIMISEKSI

Päivitetty 27.07.2010

www.tietosuoja.fi

Malli henkilötietojen käsittelyn/henkilörekisterin rekisteritoimintojen analysoimiseksi

Huom!
- Tämä mallilomake on kopioitavissa/tulostettavissa tietosuojavaltuutetun toimiston kotisivuilta (www.tietosuoja.fi). Kopioitua mallia voidaan muokata tarpeen mukaan.

- **Täyttöohjeet oheisessa liitteessä (Liite 1)**. Numerot viittaavat ohjeiden vastaaviin kohtiin.

Yleisohjeeksi kuvauksen laatijalle:

Käy läpi ja arvioi henkilötietojen eri käsittelyt ja käsittelyvaiheet, sekä rekisteröityjen oikeuksien toteuttamistavat. Eli laadi kunkin eri tehtävän prosessien kuvaukset. Arvioi henkilötietojen käsittelyn laillisuus henkilötietolain ja mahdollisen asiaa koskevan erityislainsäädännön kannalta (**suunnitteluvelvollisuus**). Huomioi kuvauksessa kaikkien käsittelyjen osalta myös toimintaan tai tietojen käsittelyyn liittyvät ostopalvelut. Toimeksiantopalvelujen (rekisterinpitäjän lukuun tapahtuva toiminta) osalta tilaaja on rekisterinpitäjä. Palvelujen tuottajan vastuu määräytyy sopimusvastuuna. Arvioi myös miten toiminta ja henkilötietojen lainmukaisuus varmistetaan sopimussuhteen syystä tai toisesta päättyessä.

1. REKISTERINPITÄJÄ

_____

_____

_____ (lisää kirjoitusrivejä tarpeen mukaan)

2. REKISTERIN VASTUUHENKILÖ

_____

_____

3. HENKILÖTIETOJEN KÄSITTELYN / REKISTERIN KÄYTTÖTARKOITUS

_____

4. HENKILÖTIETOJEN KÄSITTELYN / REKISTERIN PITÄMISEN PERUSTE

5. REKISTERIN NIMI

6. REKISTERIN TIETOSISÄLTÖ

6a. REKISTERIN TIETOLÄHTEET / SÄÄNNÖNMUKAISET TIETOLÄHTEET

7. HENKILÖTIETOJEN LUOVUTUKSET / SÄÄNNÖNMUKAISET LUOVUTUKSET

8. REKISTERIEN SISÄINEN KÄYTTÖ

8a. REKISTERIN SUOJAAMINEN

9. REKISTERIEN YHDISTÄMINEN

10. HENKILÖREKISTERIEN JA REKISTERITIETOJEN SÄILYTYS, ARKISTOINTI JA HÄVITTÄMINEN

11. REKISTERÖIDYN INFORMOINTI

12. REKISTERÖIDYN TARKASTUSOIKEUS

13. TIEDON KORJAAMINEN

14. REKISTERIHALLINNON JÄRJESTÄMINEN

15. NIMETÄÄN REKISTERIASIOITA HOITAVA HENKILÖ

15a. rekisteriselosteen laatiminen ja saatavillapitotapa

16. SISÄISET REKISTERITOIMINNAN OHJEET JA KOULUTUS

17. SEURANNAN JÄRJESTÄMINEN, ONGELMISTA JA PUUTTEISTA ILMOITTAMINEN

Malli henkilötietojen käsittelyn/
henkilörekisterin rekisteritoimintojen
analysoimiseksi/ (Liite 1)

Henkilötietojen käsittelyn/rekisteritoimintojen kuvauksen täyttöohje

Huom!
- Numerot viittaavat kuvauslomakkeen vastaaviin kohtiin
- Ohjeessa mainitut tietosuojavaltuutetun esitteet löytyvät Internetistä osoitteesta (www.tietosuoja.fi)
- Lyhenne HetiL = Henkilötietolaki (523/1999)

1. REKISTERINPITÄJÄ

Määritellään kyseistä tehtävää varten perustettavan / perustetun henkilörekisterin rekisterinpitäjä HetiL 3 § 4 kohdan mukaisesti. (Kts. myös tietosuojavaltuutetun esite: ”Kunnat ja henkilötietolaki”)

2. REKISTERIN VASTUUHENKILÖ

Määritellään se henkilö, joka asemaansa liittyen vastaa siitä, että rekisteritoiminnot suunnitellaan ja toteutetaan säännösten ja määräysten sekä annettujen yleisohjeiden mukaisesti ja jonka asiana on määrätä tai todeta eri rekisteritoimintoja koskeva päätösvalta sekä rekisterinpidon tehtäviin osallistuvat. Rekisterin vastuuhenkilö on yleensä asianomaisista toiminnoista vastaava henkilö.

3. HENKILÖTIETOJEN KÄSITTELYN / REKISTERIN KÄYTTÖTARKOITUS

Määritellään ja kuvataan, minkä tehtävän hoitamista varten (= käsittelyn/rekisterin käyttötarkoitus) / rekisteri perustetaan / on perustettu (looginen rekisteri HetiL 3 § 3 kohta, 6 § ja 7 §)

Loogiseen rekisteriin kuuluvat kaikki kussakin tehtävässä käytettävät, teknisesti erikseenkin pidettävät osarekisterit tai tiedostot. Esim. päivähoitorekisteriin voivat kuulua osarekistereinä mm. päivähoitohakemukset, laskutus ja päiväkotikohtaiset tiedot.

Arvioidaan käyttötarkoituksen lainmukaisuus eli täyttyykö henkilötietolain edellyttämä asianmukaisuusvaatimus. (HetiL 6 §)

4. HENKILÖTIETOJEN KÄSITTELYN / REKISTERIN PITÄMISEN PERUSTE

Arvioidaan, määritellään ja perustellaan oikeus henkilötietojen käsittelyyn / rekisterin perustamiseen / pitämiseen HetiL:n 8, 12 §:n 14-20 §:ien perusteella.

Esimerkiksi:
- lainsäädännöstä johtuva peruste (nimetään säännökset)
- rekisteröidyn suostumus (määritellään suostumuksen muotoa koskevat vaatimukset (HetiL 3.1, kohta 7))
- muu asiallinen yhteys rekisterinpitäjän ja rekisteröidyn välillä (esim. jäsenyys-, palvelus-, asiakas- tai potilassuhde).

5. REKISTERIN NIMI

Määritellään rekisterille nimi. Nimen tulisi kuvata hoidettavia tehtäviä / siihen rekisteröityjä henkilöitä.

6. REKISTERIN TIETOSISÄLTÖ

Suunnitellaan / kuvataan, arvioidaan ja perustellaan henkilörekisterin tietosisältö sekä sen lainmukaisuus (HetiL 9 §, 11-20 §)

Tietosisältö määritellään ja arvioidaan osarekistereittäin
- arvioidaan ja perustellaan tietosisällön lainmukaisuus
    - selvitetään tietosisältöä koskevat erityissäännökset
    - selvitetään
        - täyttyykö tarpeellisuusvaatimusedellytys
        - onko arkaluonteisten tietojen kerääminen ja tallettaminen lainmukaista
        - ovatko rekisterin tiedot virheettömiä

- suunnitellaan ja määritellään, millä tavoin tietojen virheettömyys varmistetaan.
- suunnitellaan ja määritellään, onko ja mitkä rekisterit ja tiedot tarkoituksenmukaista ja tietosuojan kannalta perusteltua tallettaa atk:lle vai manuaalisesti.
- suunnitellaan tietojärjestelmien tietoarkkitehtuuri mm. toiminnan tarpeiden, luovutusten, suojausvaatimusten ja mahdollisten salassapitosäännösten kannalta.

6a. REKISTERIN TIETOLÄHTEET / SÄÄNNÖNMUKAISET TIETOLÄHTEET

Määritellään, arvioidaan, kuvataan ja perustellaan rekisterin tietolähteet, niiden lainmukaisuus sekä tietojen hankkimisessa noudatettavat menettelytavat.

Tietolähteet selvitetään ja määritellään sekä perustamis- että ylläpitovaiheen osalta
- mistä tietoja hankitaan
- mitä tietoja hankitaan ja voidaan lainmukaisesti hankkia
- millä perusteella tietoja voidaan saada (säännös, suostumus, suostumusmallit)
- miten tiedot hankitaan – menettelytavat
- millä tavoin tiedot pyydetään – malli
- millä tavoin rekisteröityjä informoidaan rekisteriin talletetuista, muualta kuin häneltä itseltään hankituista tiedoista
- millä tavoin tietolähteitten käyttö kirjataan

7. HENKILÖTIETOJEN LUOVUTUKSET / SÄÄNNÖNMUKAISET LUOVUTUKSET

Määritellään, arvioidaan, kuvataan ja perustellaan henkilötietojen luovutukset sekä luovutusten lainmukaisuus. (Kts. ”Henkilötietojen luovuttaminen viranomaisten henkilörekistereistä”).

- määritellään, ovatko tiedot salassa pidettäviä
- selvitetään, onko henkilötietojen luovuttaminen tarpeellista
- määritellään
    - mihin tai kenelle tietoja luovutetaan
    - mitä tietoja voidaan lainmukaisesti luovuttaa (ml. tarpeellisuusvaatimus)
    - millä perusteella tietoja luovutetaan (säännös, suostumus)
    - millä tavoin tiedot luovutetaan
        - luovutusta pyytäviltä vaadittavat selvitykset ja pyynnön muotovaatimukset

- luovutusten menettelytavat, niiden asianmukaisuus ja suojaus
- Huomioi erityisesti sähköiseen tiedonsiirtoon liittyvät tietosuoja- ja tietoturvavaatimukset!

- määritellään mahdollisesti kysymykseen tulevan kielto-oikeuden toteutus
- selvitetään mahdollinen henkilötietojen luovuttaminen ulkomaille, arvioidaan luovuttamisen edellytykset ja siihen liittyvät menettelyt, ml. ilmoitusvelvollisuus
- suunnitellaan, miten rekisteristä on luovutettavissa vain tilastotiedot.

8. REKISTERIEN SISÄINEN KÄYTTÖ

Suunnitellaan, kuvataan ja arvioidaan henkilörekisterin sisäinen käyttö ja sen lainmukaisuus. Myös rekisterin sisäinen käyttö suunnitellaan aina osarekistereittäin

- määritellään asiaa koskevat säännökset ja niiden merkitys sisäisessä käytössä
    - käyttötarkoitussidonnaisuus (HetiL 7 §)
    - salassapitosäännökset (esim. HetiL 33 §, L viranomaisten toiminnan julkisuudesta 24 §)
    - huolellisuusvelvoite (HetiL 5 §)
    - suojaamisvelvoite (HetiL 32 §)
    - mahdolliset erityissäännökset
- määritellään rekisterin käyttötarkoituksen pohjalta rekisterien erilaiset käyttötavat
    - suunnitellaan tarvittavat tulosteet sekä niiden jakelu
        - henkilötietoja sisältävät tulosteet
        - tilastot ym.
        - henkilötunnuksen merkitseminen asiakirjaan/tulosteisiin (HetiL 13 §)
- määritellään tietojen suojaamisen ja turvaamisen lähtökohdat ja perusvaatimukset

8a. REKISTERIN SUOJAAMINEN

Määritellään rekisterinpidon turvaamisen periaatteet ja suunnitellaan tietojen suojaamisen toteutustavat ja ratkaisut sekä atk-rekisterien että manuaalisten rekisterien osalta, mm.

- määritellään rekisterinpidon suojaamisen, tietoturvallisuuden ja näiden valvonnan vastuut
- arvioidaan rekisterin tietojen arkaluonteisuus ja salassa pidettävyys sekä rekisterinpidon tietosuojariskit sekä häiriöiden seuraukset
- määritellään henkilötietojen käytön ja mahdollisen tiedon siirron tarpeiden pohjalta järjestelmän rakenteet ja tietoryhmät
- suunnitellaan ja järjestetään henkilöstön valmiudet ja työolot turvallisen rekisterinpidon edellyttämälle tasolle
- laaditaan ohjelmistojen ja laitteiden käyttöä ja muuttamista sekä sijaintia koskevat ohjeet ja kuvaukset
- huolehditaan tietoturvallisuuden toteutumisesta kaikissa käsittelyvaiheissa ja kaikkien laitteiden ja ohjelmien osalta
- laaditaan rekisterin käyttöä ja käyttövaltuuksia sekä niiden muuttamista koskevat ohjeet ja säännöt
    - määritellään käyttöoikeuksien perusteet
    - määritellään käyttäjätunnusten ja salasanojen käytön periaatteet

- laaditaan rekisterinpidon valvontaa ja rekisterien käytön valvontaa koskevat ohjeet ja säännöt
    - määritellään käytön rekisteröinnin ja valvonnan periaatteet
    - määritellään käyttäjien (myös ATK-henkilöstön) valvonnan periaatteet

- laaditaan tietovälineiden käsittelyä (ml. hävittäminen) koskevat ohjeet
- laaditaan ohjeet ja säännöt henkilörekisterin käsittelylle tietoverkossa ja tietoliikenteen välityksellä
- suunnitellaan ja laaditaan ohjeet rekisterien fyysistä suojaamista varten (tilat, lukitukset, kulunvalvonta yms.)
- suunnitellaan ja laaditaan ohjeet tietojen luovutusmenettelyistä sekä sisäisessä kuljetuksessa ja muussa sisäisessä toiminnassa noudatettavista menettelyistä
- varmistetaan sopimuksin riittävä turvallisuus, kun muut kuin rekisterinpitäjä pitävät, kuljettavat, säilyttävät ym. rekisterien tietoja
- pyydetään henkilöstöltä erillinen salassapitositoumus, jossa on todettava myös mahdollinen lainsäädäntöön perustuva salassapitovelvollisuus.

9. REKISTERIEN YHDISTÄMINEN

Selvitetään, määritellään ja kuvataan rekisterien yhdistämistarve ja yhdistämisen lainmukaisuus HetiL:n 8 ja 12, 14-20 §:n perusteella

- määritellään yhdistettäväksi aiotut rekisterit
- arvioidaan yhdistämisen lainmukaisuus HetiL:n 8, 12 ja 14-20 §:n perusteella — tähän liittyen arvioidaan yhdistämisen tuloksena syntyneen rekisterin lainmukaisuus.
- suunnitellaan yhdistämisen toteutustapa

10. HENKILÖREKISTERIEN JA REKISTERITIETOJEN SÄILYTYS, ARKISTOINTI JA HÄVITTÄMINEN

Suunnitellaan, arvioidaan ja kuvataan rekisterien ja niiden sisältämien henkilötietojen säilyttämisajat ja niiden lainmukaisuus.

- määritellään asiaa koskevat säännökset ja määräykset: mihin säilyttäminen ja mahdollinen arkistointi perustuu (HetiL:n 12. 2, 34, 35 §:t; viranomaisten osalta arkistolaki ja mahdolliset erityissäännökset)
- arvioidaan, miten pitkään henkilörekisteri ja sen eri tiedot ovat **toiminnan kannalta tarpeellisia**
- selvitetään, onko rekisteri ja sen tiedot — sen jälkeen kun ne toiminnan kannalta eivät ole enää tarpeellisia — arkistoitava, sekä miten pitkäksi aikaa rekisterit ja sen eri tiedot voidaan ja tulee arkistoida.
    - yksityinen toiminta: arkistointilupa HetiL:n 35.2 §
    - viranomaisten toiminta: arkistolaki

- suunnitellaan ja kuvataan, millä tavoin ja missä tiedot arkistoidaan
- suunnitellaan ja kuvataan, miten henkilörekisterit ja niiden tiedot hävitetään, mm.
    - päivittäistoiminnassa syntyvän aineiston hävittäminen
    - arkistoidun aineiston hävittäminen
    - hävittämistä koskevat sopimukset

11. REKISTERÖIDYN INFORMOINTI

Suunnitellaan
- mistä informoidaan
- milloin informoidaan
- miten informointi toteutetaan: määritellään menettelytavat / lomakkeet
- mahdolliset poikkeukset toiminnasta, perustelut (Kts. ”Rekisterinpitäjän yleinen informointivelvollisuus”, ”Malli sosiaalihuollon asiakkaiden informoinnista”, ”Malli julkisen terveydenhuollon potilaiden informoinnista”)

12. REKISTERÖIDYN TARKASTUSOIKEUS

Suunnitellaan ja kuvataan rekisteröityjen tarkastusoikeus sekä sen toteutus henkilötietolain 26-28 §:ien tai mahdollisten erityissäännösten mukaisesti

- selvitetään asiaa koskevat säännökset
    - selvitetään, onko rekisteriin tarkastusoikeutta
    - määritellään ja kuvataan ne tilanteet, joissa tarkastusoikeus tapauskohtaisesti voidaan mahdollisesti evätä
    - määritellään miten tarkastusoikeus toteutetaan rekisteröidyn pyynnöstä
    - toimittaako rekisterinpitäjä tiedot oma-aloitteisesti?
    - suunnitellaan, missä ajassa tarkastusoikeus toteutetaan
    - suunnitellaan tarkastusoikeuden esittämiseen, organisointiin ja toteuttamiseen liittyvät menettelytavat
        - tarkastuspyynnön muotovaatimukset (Laadi mallilomakkeet) *
        - kuka vastaanottaa pyynnöt, kuka päättää, kuka ja miten toteutetaan
        - tarkastusoikeuden epäämisestä annettava todistus
- selvitetään tarkastusoikeuden suhde ja ero muihin tiedonsaantioikeutta koskeviin säännöksiin, ohjeistetaan asia

(* Voit käyttää tietosuojavaltuutetun laatimia mallilomakkeita, kts. www.tietosuoja.fi)

13. TIEDON KORJAAMINEN

Suunnitellaan ja kuvataan virheen oikaisun toteutus

- selvitetään asiaa koskevat säännökset
- suunnitellaan, millä tavoin tietojen virheettömyydestä ja niiden korjaamisesta huolehditaan oma-aloitteisesti sekä tietojen virheettömyyden varmistamismenettelyt
- suunnitellaan ja kuvataan, millä tavoin ja miten virhe korjataan
    - normaalin ylläpitomenettelyn yhteydessä
    - muulla tavoin, miten
    - missä ajassa virhe korjataan
    - millä tavoin virhe korjataan
- suunnitellaan, millä tavoin virheen korjaaminen organisoidaan ja toteutetaan: kuka vastaanottaa pyynnöt *, kuka päättää, kuka toteuttaa

(* Voit käyttää tietosuojavaltuutetun laatimia mallilomakkeita, kts. www.tietosuoja.fi)

14. REKISTERIHALLINNON JÄRJESTÄMINEN

Määritellään, kuka/ketkä käyttää/käyttävät rekisteritoiminnoissa päätösvaltaa
Määritellään, kuka/ketkä toteuttaa/toteuttavat rekisteritoiminnot

15. NIMETÄÄN REKISTERIASIOITA HOITAVA HENKILÖ

Nimetään ja määritellään se henkilö, jonka puoleen voi kääntyä saadakseen tarkempia tietoja rekisteristä sekä oikeudesta saada tarkastaa ja saada korjatuksi itseään koskevat tiedot. Tämä henkilö merkitään myös rekisteriselosteeseen rekisteriasioita hoitavaksi henkilöksi.

15a. rekisteriselosteen laatiminen ja saatavillapitotapa

Jokaisesta henkilörekisteristä tulee laatia rekisteriseloste. Selosteen tietosisältö määritellään HetiL:n 10 §:ssä. Selosteeseen on tarkoituksenmukaista merkitä myös HetiL:n 24 §:ssä tarkoitetut informointi-tiedot.

Rekisteriseloste tulee pitää jokaisen saatavilla rekisterinpitäjän toimipaikassa. Suositeltavaa on laittaa esimerkiksi palveluihin liittyvät rekisteriselosteet rekisterinpitäjän kotisivuille.

16. SISÄISET REKISTERITOIMINNAN OHJEET JA KOULUTUS

Laaditaan sisäiset rekisterin käyttöä koskevat ohjeet henkilöstölle.

Tavoitteena on, että kuvaus voisi toimia myös tietosuojan ohjeena organisaatiossa

Järjestetään riittävä koulutus henkilöstölle. Koulutuksen tulisi sisältyä aina myös toimintoja koskevaan koulutukseen.

Suunnitellaan, millä tavoin ohjeet ja koulutus pidetään ajan tasalla.

17. SEURANNAN JÄRJESTÄMINEN, ONGELMISTA JA PUUTTEISTA ILMOITTAMINEN

Suunnittele ja organisoi tapa, jolla tieto mahdollisista puutteista, ongelmista ym. saadaan viipymättä eri vastuuhenkilöille.