


Tietosuoja yhteistyön mahdollistajana

Jarkko Reittu - Tietosuojavastaava

10.12.2020

Tietosuojaa koskeva keskeinen lainsäädäntö

- EU:n yleinen tietosuoja-asetus
  - Ylintä oikeutta joka syrjäyttää kansallisen lainsäädännön (pl. perustuslaki)
- Tietosuojalaki (1050/2018)
  - Kansallinen laki, joka täydentää tietosuoja-asetusta
- Julkisuuslaki (621/1999)
  - Sääntelee viranomaisten asiakirjojen julkisuutta
- Tiedonhallintalaki (906/2019)
  - Sääntelee viranomaisten tietoaineistojen hallintaa ja tietoturvallista käsittelyä

Omavalvonnan ja olennaisten vaatimusten säädökset

- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007 (Muutoksi tulossa: HE 212/2020)
- Laki sähköisestä lääkemääräyksestä 61/2007 (Muuttumassa 2020?)
- THL:n Määräys 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset
- THL:n Määräys 2/2015: Omavalvontasuunnitelmaan sisällytettävät selvitykset ja vaatimukset
- THL:n Määräys 2/2016: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista vaatimuksista

EU:n yleinen tietosuoja-asetus eli GDPR

- Osa Euroopan unionin suurta tietosuojalainsäädännön uudistusta
- Tausta
  - Informaatioteknologian nopea kehitys
  - Jäsenvaltioiden hajanainen tietosuojasääntely ja laintulkinta
- Tavoitteena on
  - vahvistaa henkilöiden oikeuksia henkilötietoja käsiteltäessä
  - parantaa EU:n digitaalisten sisämarkkinoiden toimintaedellytyksiä

GDPR – Osa tietosuojalainsäädännön jatkumoa

- 1948 YK:n ihmisoikeuksien yleismaailmallinen julistus
- 1950 Euroopan neuvoston ihmisoikeussopimus
- 1960 – 1980 kansallinen tietosuojasääntely kehittyy
- 1973/1974 Euroopan neuvoston päätökset 73/22 ja 74/29
- 1980 OECD Guidelines on the Protection on Privacy and Transborder Flows of Personal Data
- 1981 Euroopan neuvoston Convetion for the Protection of Invididuals with regard to Automatic Processing of Personal Data ”Convention 108”
- 1995 Europan komission tietosuojadirektiivi 95/46/EC
- 2002 Sähköisen viestinnän tietosuojadirektiivi
- 2009 Lissabonin sopimus, erityisesti 8 artikla
- 2016 Rikosasioiden tietosuojadirektiivi
- 2018 EU:n yleinen tietosuoja-asetus
- Tulossa: Sähköisen viestinnän tietosuoja-asetus

Artikla 4: Rekisterinpitäjän ja henkilötietojen käsittelijän määritelmät

Rekisterinpitäjä (data controller) ja yhteisrekisterinpitäjä (joint controller)

- Osapuoli, joka yksin tai yhdessä määrittelee henkilötietojen käsittelyn tarkoitukset ja käsittelyn keskeiset keinot
- Kysymykset rekisterinpitäjän tunnistamiseksi: Kenen aloitteesta henkilötietoja käsitellään? Kuka hyötyy käsittelystä? Kuka päättää käsittelyn tarkoituksesta ja keinoista?
- Rekisterinpitäjä voidaan määritellä myös lainsäädännössä joko suoraan (esim. THL on Koronavilkun rekisterinpitäjä) tai epäsuorasti (esim. THL:n tehtävänä on ”ylläpitää alan tiedostoja ja rekistereitä”)
- Rekisterinpitäjyys määräytyy vain tietosuoja-asetuksen perusteella eikä siitä voi sopia
- Rekisterinpitäjällä ei tarvitse olla pääsyä henkilötietoihin

Henkilötietojen käsittelijä (data processor)

- Osapuoli, joka käsittelee henkilötietoja rekisterinpitäjän puolesta
  - Esim. kyselytutkimuksen toteuttaminen, näyteanalyysit, henkilötietojen tallentaminen pilvipalveluun
- Rekisterinpitäjä saa käyttää vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat tietosuoja-asetusta
- Henkilötietojen käsittelystä on sovittava aina sopimuksella (data processing agreement)
- Henkilötietojen käsittelijä ei saa käyttää rekisterinpitäjän vastuulla olevia henkilötietoja omiin tarkoituksiinsa

Artikla 4:Rekisteröity, henkilötieto ja käsittely

Rekisteröity (data subject)

- Luonnollinen (elävä) henkilö, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen perusteella

Henkilötieto (personal data)

- Kaikki tiedot, jotka liittyvät rekisteröityyn
- Henkilötietoja ovat siis muutkin tiedot kuin tunnisteelliset tiedot
- Pelkkä hypoteettinen tai häviävän pieni mahdollisuus tunnistamiseen ei tee tiedoista henkilötietoja. Tunnistaminen tulee olla toteutettavissa kohtuullisin ja laillisin keinoin.

Henkilötietojen käsittely (data processing)

- Toimenpiteet, jotka kohdistuvat henkilötietoihin

Tunnisteelliset henkilötiedot

Tieto on tunnisteellista, jos sen perusteella voidaan tunnistaa yksittäinen henkilö

- Yhden tai useamman tunnusomaisen fyysisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen tekijän perusteella
- Myös pseudonymisoidut aineistot ovat tunnisteellisia
- Vaikka aineistossa ei olisi suoria tunnisteita, mutta henkilö voidaan tunnistaa epäsuorien tunnisteiden perusteella, on kyse henkilötiedoista

Suorat tunnisteet
Tietoja, jotka yksin riittävät tunnistamiseen:
Nimi, henkilötunnus, nimen mukainen sähköpostiosoite, biometriset tunnisteet

Vahvat epäsuorat tunnisteet
Tietoja, joiden avulla henkilö voidaan tunnistaa kohtuullisen helposti:
Osoite, puhelinnumero, ip-osoite, työntekijänro, vakuutusnro, tilinro, tarkat vuosiansiot, auton rekisterinumero, harvinainen ammattinimike, harvinainen sairaus, annettu asema esim. puheenjohtajuus, valo- tai videokuva

Välilliset/epäsuorat tunnisteet
Eivät ole yksittäin riittäviä henkilön tunnistamiseksi, mutta mahdollistavat tunnistaminen yhdistettyinä muihin tietoihin:
Sukupuoli, ikä, asuinkunta, ammatti, päivämäärä (syntymäaika, kuolinaika, tapahtuma-aika)

Tietosuoja vs. tietoturva

- Tietoturva (information security) tarkoittaa **tiedon** saatavuuden, luottamuksellisuuden ja eheyden ylläpitämistä.
- Tietosuoja (data protection/data privacy) on osa perusoikeuksien takaamaan **yksityisyyden suojaa.** Tietoturva on keskeinen osa tietosuojasuojan toteutumista.
- Tietosuoja-asetuksessa tietosuoja esitellään tietosuojaperiaatteina

Artikla 5: GDPR:n tietosuojaperiaatteet

Tietosuojaperiaate	Käytännön merkitys
Lainmukaisuus, kohtuullisuus ja läpinäkyvyys	Käsittele henkilötietoja vain, kun se on tarkoituksen toteuttamisen kannalta perusteltua ja lainmukaista. Älä käsittele henkilötietoja salaa tai odottamattomalla tavalla. Informoi käsittelystä rekisteröityjä.
Käyttötarkoitussidonnaisuus	Älä käsittele henkilötietoja muuhun kuin alkuperäiseen tarkoitukseen. Poikkeusmahdollisuus: tutkimus, arkistointi ja tilastointi.
Tietojen minimointi	Käsittele vain tarkoituksen kannalta tarpeellisia henkilötietoja. Poista tarpeettomaksi osoittautuvat tiedot.
Täsmällisyys	Vanhentuneet, epätarkat tai virheelliset tiedot on korjattava tai poistettava viipymättä. Suunnittele, kuinka tämä voidaan toteuttaa käytännössä
Säilytyksen rajoittaminen	Älä säilytä henkilötietoja pidempään kuin on tarkoituksen kannalta välttämätöntä. Poista/arkistoi/anonymisoi henkilötiedot tarvittaessa.
Eheys ja luottamuksellisuus	Varmista tietojen sähköinen ja fyysinen tietoturvallisuus.

Vaatimustenmukaisuus, osoitusvelvollisuus ja riskilähtöisyys

- Rekisterinpitäjä vastaa siitä, että henkilötietojen käsittelyssä toteutuu GDPR:n tietosuojaperiaatteet ja vaatimukset
- Rekisterinpitäjän on kyettävä osoittamaan, että henkilötietojen käsittely on tietosuoja-asetuksen mukaista
  - Käytännössä vaatii kirjallista dokumentaatiota
- Henkilötietojen käsittely tulee suunnitella perustuen riskiarvioon
- Tietosuojavaltuutetun sanktiot mahdollisia mm. hallinnollinen seuraamusmaksu ja käsittelykielto

Suomen sanktiokäytäntöä

100 000 euron sakko Postille
- Puutteita informointivelvollisuuden toteuttamisessa

72 000 euron sakko Taksi Helsingille
- Taksit tallensivat ääntä ilman perustetta ja kertomatta siitä

16 000 euron sakko Kymen Vesi Oy:lle
- Tietosuojaa koskeva vaikutustenarviointi oli jäänyt tekemättä

12 500 euron sakko Yritys X:lle
- Yritys keräsi työntekijöidensä tietoja tarpeettomasti

Määräys muuttaa käsittely lainmukaiseksi
- Henkilötunnusta ei saa laittaa sairaanhoitopiirin potilaslaskulle tai kirjallisiin hallintopäätöksiin

Artikla 6: Lainmukainen käsittelyperuste

- Henkilötietojen käsittely edellyttää aina lainmukaista käsittelyperustetta
- Tietosuoja-asetuksen 6 artiklassa on 6 yhdenvertaista perustetta:
  - Suostumus
  - Sopimuksen täytäntöönpano
  - Lakisääteisen velvoitteen noudattaminen
  - Rekisteröidyn tai toisen elintärkeä etu
  - Yleisen edun mukaisen tehtävän suorittaminen tai julkisen vallan käyttäminen
  - Oikeutettu etu (ei sovellu viranomaisiin)
- Käsittelyperusteen valinta vaikuttaa erityisesti rekisteröidyn oikeuksiin
- Erityisiin henkilötietoryhmiin kuuluvien tietojen käsittely edellyttää lisäksi erityisehtojen täyttymistä

Artikla 9: Erityisiin henkilötietoryhmiin kuuluvat tiedot eli ns. arkaluonteiset henkilötiedot

- Tietosuoja-asetuksen mukaan erityisiin henkilötietoryhmiin kuuluvat:
  - Rotu tai etninen alkuperä
  - Poliittiset mielipiteet
  - Uskonnolliset tai filosofiset uskomukset
  - Ammattiliiton jäsenyys
  - Geneettinen tieto sellaisenaan
  - Biometrinen tieto, kun tarkoituksena on tunnistaa henkilö esim. valvontakamerakuvat
  - Terveydentilaa koskevat tiedot
  - Seksuaalisen suuntautuminen
  - Seksuaalielämää koskevat tiedot
  - Rikostuomioita tai rikkomuksia koskevat tiedot
- Tietosuoja-asetus: näiden tietojen käsittely on lähtökohtaisesti kielletty!
- Käsittely on mahdollista vain tietosuojalain 6 §:n tai GDPR 9 artiklan mukaisten erityisehtojen täyttyessä

Suostumus viranomaistoiminnassa

- Tietosuoja-asetuksen mukaan suostumus ei voi toimia käsittelyperusteena, kun osapuolet ovat epäsuhtaisessa asemassa, erityisesti kun toinen osapuoli on viranomainen
- Perustuslakivaliokunta
  - Suostumukseen perustuvat perusoikeuksien rajoitukset ovat valtiosääntöoikeudellisesti ongelmallisia
  - Oikeusvaltioperiaatteiden mukaisesti viranomaisen toiminnasta on säädettävä lailla
- Lainmukainen käsittelyperuste voi olla esim. lakiin perustuvan yleisen edun mukaisen tehtävän suorittaminen, mutta suostumus voi silti toimia ylimääräisenä suojatoimenpiteenä
  - Esim. Koronavilkku ja tapauskohtaisesti tieteelliset tutkimukset

Rekisteröidyn oikeudet

- Henkilötietojen käsittelyn lainmukainen käsittelyperuste määrittää sen, millaisia oikeuksia rekisteröidyllä on
  - oikeudet ovat laajimmillaan silloin, kun käsittely perustuu suostumukseen
  - oikeuksien käyttämistä koskeviin pyyntöihin vastattava kuukauden sisällä
- Oikeuksien käyttäminen on tehtävä mahdollisimman helpoksi
- Oikeuksista voidaan poiketa tietyissä tilanteissa
- Poikkeuksia on tulkittava rajoitetusti

III Luku: Rekisteröidyn oikeudet

- Rekisteröidyllä on lähtökohtaisesti oikeus
  - saada tietoa henkilötietojensa käsittelystä eli oikeus läpinäkyvään informaatioon (12-14 artikla)
  - saada pääsy tietoihin ml. Kopio omista tiedoista (15 artikla)
  - oikaista vääriä tietoja (16 artikla)
  - poistaa tiedot ja tulla unohdetuksi (17 artikla)
  - rajoittaa tietojen käsittelyä (18 artikla)
  - siirtää tiedot järjestelmästä toiseen (20 artikla)
  - vastustaa tietojen käsittelyä (21 artikla)
  - olla joutumatta automaattisen päätöksenteon kohteeksi (22 artikla)
- Oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi
- Henkilötietojen käsittelyä koskeva asia voidaan viedä käräjäoikeuteen riita-asiana
- Henkilötietojen käsittelyä koskevan hallintopäätöksen riitauttaminen HAO:ssa

12-14 Artikla: Läpinäkyvä informointi

- Aikaisemmin henkilötietolain mukaan laadittava mm.
  - Rekisterikohtainen rekisteriseloste
- Nyt tietosuoja-asetuksen mukaan
  - Voidaan ilmoittaa laajemmin, eikä ole sidottu rekisteriin tai tiettyyn käsittelyyn
  - Sisältö vaihtelee tapauskohtaisesti, mutta tietyt minimivaatimukset on täytettävä
  - Ei ole muotovaatimusta
  - Haaste: tiivis, läpinäkyvä, ymmärrettävä ja selkeä, helposti saatavilla, ei kuitenkaan liian yleisluonteisesti, huomioitava kohderyhmä
  - Kerroksittainen informointi on suositeltavaa
    - Kerrotaan aluksi keskeisimmät tiedot
    - Tarjotaan lisätietoja esim. verkkosivuilla

12-14 Artikla: Läpinäkyvä informointi

- Milloin tiedot on annettava?
  - Kun tiedot kerätään rekisteröidyltä itseltään: **Keräämisen yhteydessä**
  - Kun tiedot kerätään muualta: **Käytännössä viimeistään 30 pv kuluessa** (poikkeusmahdollisuus)
- Kun tiedot on kerätty rekisteröidyltä itseltään:

  ”Jos rekisterinpitäjä aikoo käsitellä henkilötietoja edelleen muuhun tarkoitukseen kuin siihen, johon henkilötiedot kerättiin, rekisterinpitäjän on ilmoitettava rekisteröidylle ennen kyseistä jatkokäsittelyä tästä muusta tarkoituksesta ja annettava kaikki asiaankuuluvat lisätiedot”
  - Ei poikkeusmahdollisuutta, rikkomisessa mahdollisuus maksimisanktioon

Artikla 32: Käsittelyn turvallisuus

- Tehtävä riskiarvio, jonka perusteella on toteutettava asianmukaiset organisatoriset ja tekniset toimenpiteet riskien lieventämiseksi ja riittävän turvallisuustason varmistamiseksi
- Mm. käsittelyn luonne, tarkoitus ja laajuus vaikuttavat riskiarvion laajuuteen ja asianmukaisiin toimenpiteisiin
- Riskiarviossa on kiinnitettävä erityisesti huomiota henkilötietojen vahingossa tai laittomasti tapahtuvaan tuhoamiseen, häviämiseen, muuttamiseen, luvattomaan luovuttamiseen tai henkilötietoihin pääsyyn

Artikla 35: Tietosuojaa koskeva vaikutustenarvionti (DPIA)

- Tietosuojaa koskeva vaikutustenarvionti on tehtävä, kun:
  - Käsitellään laajamittaisesti arkaluonteisia henkilötietoja tai rikostuomioita koskevia tietoja
  - Käsitellään arkaluonteisia henkilötietoja tai rikostuomioita koskevia tietoja henkilön arvioimiseksi tai pisteyttämiseksi
  - Arkaluonteisia henkilötietoja sovitetaan yhteen tai yhdistetään muihin tietokokonaisuuksiin
  - Käsitellään laajamittaisesti sijaintitietoja
  - Yleisölle avointa aluetta valvotaan järjestelmällisesti ja laajamittaisesti
  - Henkilötietoja käsitellään ilmiantojärjestelmien eli ns. whistleblowing-järjestelmien yhteydessä
  - Rekisteröidyn informoinnista poiketaan 14 artiklan 5 b -kohdan perusteella
- Tarkoituksena on arvioida riskejä, joita suunniteltu henkilötietojen käsittely aiheuttaa rekisteröidylle
- ”On pyydettävä neuvoja tietosuojavastaavalta”

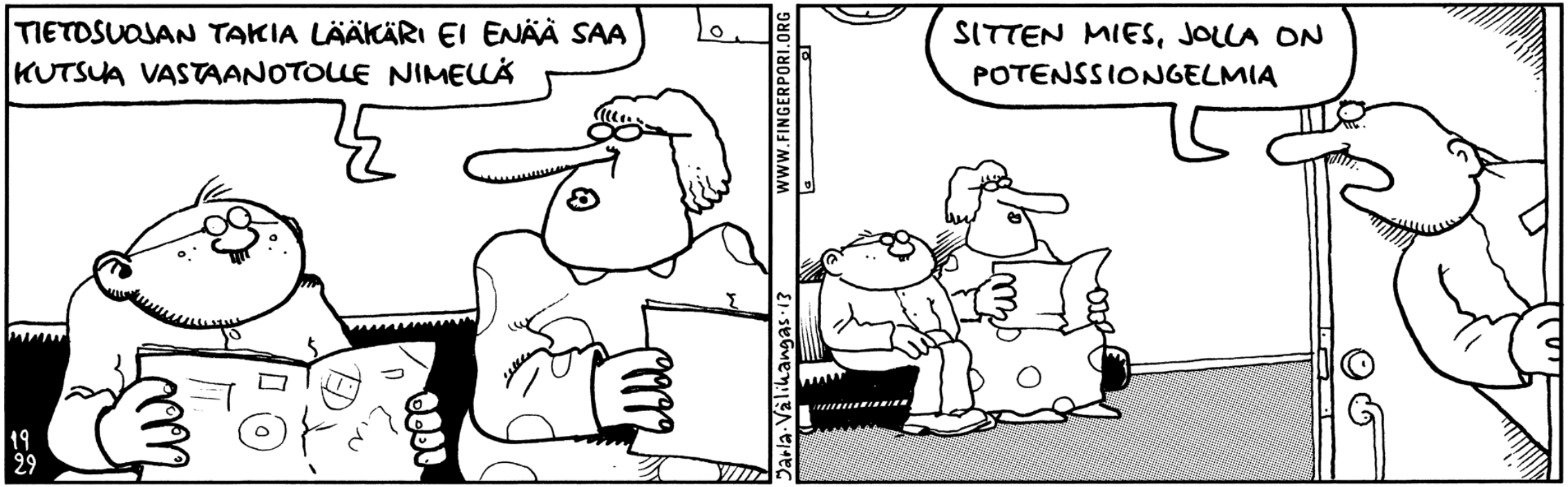
Mitä tehdä käytännössä?

1. Suunnittele henkilötietojen käsittely etukäteen
   - Käsitelläänkö henkilötietoja?
   - Tunnista käsiteltävät tiedot, käsittelyn tarkoitus ja oikeusperuste
   - Kuinka informoidaan rekisteröityjä?
   - Tunnista eri osapuolten roolit sekä määritä vastuut ja velvollisuudet
   - Siirretäänkö tietoja EU/ETA-alueen ulkopuolelle?
   - Varaudu poikkeustilanteisiin ja tietoturvaloukkauksiin
   - Rekisteröityjen oikeudet ja niistä poikkeaminen
   - Mitä tiedoille tapahtuu käsittelyn päätyttyä?
2. Tee riskiarvio ja tarvittaessa tietosuojaa koskeva vaikutustenarviointi
3. Toteuta riittävät organisatoriset ja tekniset toimenpiteet
4. Laadi riittävä tietosuojadokumentaatio
5. Huolehdi henkilöstön osaamisesta: ohjeista ja kouluta

Vaadittava tietosuojadokumentaatio pähkinänkuoressa

- Rekisteröidyille annettava informaatio
- Tietosuojaa koskeva vaikutustenarviointi tarvittaessa
- Seloste henkilötietojen käsittelytoimista (30 artikla)
- Suostumukset tarvittaessa
- Sopimukset
  - Sopimukset rekisterinpitäjien välillä
  - Sopimukset henkilötietojen käsittelystä
  - Komission vakiolausekkeet tietojen siirtomekanismina
- Huomioi erityislainsäädännön vaatimukset, esim.
  - Tiedonhallintalain asettamat vaatimukset
  - Omavalvontasuunnitelmat ja sote-tiedonhallinnan määräykset

Kiitos mielenkiinnosta!



Lähde: Helsingin sanomat 5.6.2013