Haaga-Helia
ammattikorkeakoulu Oy

Yksityisyyden suoja asioiden internetissä

Ulla Tiikkaja

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma 2016

Haaga-Helia ammattikorkeakoulu Oy

Tiivistelmä

14.05.2016

Tekijä
Ulla Tiikkaja

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Yksityisyyden suoja asioiden internetissä

Sivu- ja liitesivumäärä
35 + 7

Opinnäytetyön otsikko englanniksi
Internet of Things privacy

Tässä opinnäytetyössä selvitettiin yksityisyydensuojaa asioiden internetissä sekä rekisteröidyn että rekisterinpitäjän kannalta. Lisäksi tutkittiin yritysten käytäntöjä tietojen keräämisessä. Tutkimus rajattiin koskemaan yksityisyydensuojaa asioiden internetissä.

Tutkimus toteutettiin kvalitatiivisena tutkimuksena jakautuen kahteen osaan: teoriaan ja haastatteluihin. Haastattelut tehtiin marraskuun 2015 ja tammikuun 2016 välisenä aikana.

Tietosuojavaltuutetun haastattelussa selvisi, että yksityisyydensuoja on perusoikeus, joka on turvattu Suomen perustuslaissa, EU:n perusoikeuskirjassa ja EU:n ihmisoikeussopimuksessa. Vuonna 2018 voimaan tulevan EU:n tietosuoja-asetuksen myötä yksityisyydensuojan käytännöt yhdenmukaistuvat kaikille EU: n jäsenvaltioille. Uudistuksen pyrkimyksenä on parantaa rekisteröityjen tietoturvaa ja luottamusta internetiin.

Yrityshaastattelussa kävi ilmi, että laitteiden keräämät tiedot tallentuvat alihankkijoiden palvelimille, mutta palvelinten sijainti ei välttämättä ollut yrityksen tiedossa. Lisäksi tieto siitä, milloin yrityksen keräämät tiedot kuuluvat henkilötietolain piiriin ja rekisteri-ilmoitus tulee täyttää, oli joissakin tapauksissa epäselvää.

Tutkimuksessa selvisi myös, että osa aktiivisuusrannekkeiden valmistajista käyttää amerikkalaisia palvelimia tietojen tallentamiseen ja että he toimivat Yhdysvaltojen lakien mukaan, vaikka he myyvät rannekkeita Euroopassa. Tämän seurauksena yksityisyydensuoja heidän tuotteitaan käyttävillä asiakkailla saattaa olla heikompi kuin Euroopassa yleensä.

Asiasanat
Esineiden internet, yksilösuoja, tietosuoja

HAAGA-HELIA
University of Applied Sciences

Abstract

14.05.2016

Author
Ulla Tiikkaja

Degree programme
Business Information Technology

Report/thesis title
Internet of Things privacy

Number of pages and appendix pages
35 + 7

The objective of this research was to study the Internet of Things privacy both from registered person's and the data controller's point of view. Additionally the aim was to study the practices of data collection. The research was limited to privacy issues associated with the Internet of Things.

This research was carried out as a qualitative study and was split into two parts, namely, the theoretical background and interviews. The interviews were conducted between November 2015 and January 2016.

In the interview with the data protection supervisor it turned out that privacy is a privilege that is protected by the Constitution of Finland, Charter of Fundamental Rights of the European Union and in the European Convention on Human Rights. Europe Data Protection rules will be renewed. The data protection reform that will come into effect during 2018 will be equal for all member states of the European Union. The aim of this reform is to improve registered data security and confidence in the Internet.

The interviewed company revealed that the data was collected on the servers of subcontractors and therefore the actual location of the servers was not always known. Also it was in some cases unclear, when the collected was subject to the privacy law and an application of registration had to be filled in.

The study also reveals that some of the activity wristband manufacturers use American servers for data storage, and that they are operating under the laws of the United States, even if they sell wristbands in Europe. As a result the privacy of the customers using their products may be weaker than in Europe, in general.

Keywords
Internet of Things, privacy, data protection

Sisällys

1 Johdanto 1

1.1 Tutkimuksen tavoitteet 2

1.2 Käsitteiden määrittely 2

2 Asioiden internet 4

3 Yksityisyydensuoja 5

3.1 Henkilötietojen käsittely rekisteröidyn kannalta 6

3.1.1 Sopimus vai suostumus 6

3.1.2 Oikeudet 7

3.2 Henkilötietojen käsittely rekisterinpitäjän kannalta 8

3.2.1 Yleistä 8

3.2.2 Ilmoitusvelvollisuus 8

4 Yksityisyyden suojaa koskevat säännökset 9

4.1 Henkilötietolaki 9

4.1.1 Lain soveltaminen 9

4.1.2 Määritelmät 10

4.1.3 Henkilötietojen käsittely 11

4.1.4 Rekisteriseloste 12

4.1.5 Arkaluontoiset tiedot 13

4.1.6 Henkilötunnuksen käsittely 13

4.1.7 Suoramarkkinointi ja muut osoitteelliset lähetykset 14

4.1.8 Henkilötietojen luovutus EU:n ja ETA:n ulkopuolelle 14

4.1.9 Rekisteröidyn oikeudet 15

4.1.10 Ilmoitus tietosuojavaltuutetulle 17

4.2 Erityislainsäädäntö 18

4.3 Julkisuuslaki 18

4.4 Työelämän tietosuojalaki 20

4.5 Tietoyhteiskuntakaari 20

4.6 Direktiivit ja asetukset 20

5 Tietosuojavastaaville tärkeät eurooppalaiset sopimukset 21
5.1 Euroopan ihmisoikeussopimus 21
5.2 Euroopan neuvoston yleissopimus 108 22
5.3 Euroopan unionin perusoikeuskirja 22
6 EU:n tietosuojauudistus 23
7 Tutkimustulokset 24
7.1 Tietosuojavaltuutettu Reijo Aarnion haastattelu 24
7.1.1 Henkilötietojen käsittely 24
7.1.2 Direktiivit 25
7.1.3 Tietojen jakaminen 26
7.1.4 Haasteet 26
7.1.5 Selvitettäviä tapauksia 26
7.1.6 Tietojen säilyttäminen 27
7.1.7 EU:n ulkopuolelta tulevat yritykset 27
7.1.8 Mistä apua yrityksille? 27
7.2 Yrityshaastattelu 27
7.3 Aktiivisuusrannekkeiden valmistajien yksityisyyden suoja 28
7.3.1 Henkilötiedot 28
7.3.2 Muut kuin henkilötiedot 30
7.3.3 Evästeet ja muut tekniikat 31
7.3.4 Tietojen säilytysaika 31
7.3.5 Tietojen luovuttaminen 32
7.3.6 Tietojen suojaaminen 32
7.3.7 Palvelimien sijainti 33
8 Johtopäätökset 34
Lähteet 36
Liite 1. Kysymykset tietosuojavaltuutetulle Reijo Aarniolle 41
Liite 2. Kysymykset yritykselle 42

1 Johdanto

Asioiden internet (Internet of Things= IoT) kytkee älylaitteita verkkoon (Cisco). Arvioiden mukaan vuonna 2020 noin 50 miljardia laitetta olisi kytkettynä internetiin (Cisco). Tulevaisuudessa vaa'an voisi synkronoida internetin kanssa, jolloin henkilö voisi seurata painoaan internetissä. Mutta kuka muu kuin asianosainen saisi tietää tästä? Haluaisitko, että naapurisi tai vaikkapa vakuutusyhtiösi saisi tietää painosi? Yksityisyydensuoja ja tietoturva ovat kasvavia huolenaiheita asioiden internetissä, mitä enemmän langattomia laitteita sitä enemmän tietoturvariskejä. (Deutsche Welle 2015.)

IoT-laitteet tulevat helpottamaan elämäämme, mutta sensoreiden avulla saadaan myös tietoa, joka joutuessaan ulkopuolisiin käsiin, voi paljastaa meistä asioita, joita emme välttämättä halua jakaa. Esimerkiksi aktiivisuusranneke Fitbit mittaa askeleet ja poltetut kalorit, mutta siihen saa myös manuaalisesti lisättyä liikunta-aktiivisuuden mukaan lukien seksuaalisen aktiivisuuden. Aikaisemmin Fitbit -käyttäjän profiili ja aktiivisuudet olivat oletuksena julkisia, mutta kun selvisi että Google – hakukoneella pystyttiin saamaan jopa 200 Fitbit -käyttäjän seksuaalinen aktiivisuus näkyviin, niin Fitbit piilotti aktiivisuudet. Nykyään aktiivisuudet eivät näy muille kuin käyttäjälle, olivat käyttäjän asetukset mitkä tahansa. (Hill, K 2011.)

Asioiden internet ei suinkaan ole uusi asia. Ubiquitos Computing, jota myös sanotaan Jokapaikan tekniikaksi, on termi, jota käytettiin nykyisen esineiden internetin tilalla (Aarnio, R. 9.11.2015). Vuonna 2006 HIIT (Helsinki Institute of Information technology) teki taustaselvityksen ubiikin yhteiskunnan haitoista, eduista, hyödyistä ja riskeistä Liikenne- ja viestintäministeriölle (Tietosuojavaltuutetun toimisto 2006). Jo silloin tuli selväksi, että yksityisyydensuojan turvaaminen tulee aiheuttamaan haasteita. Nyt, 10 vuotta myöhemmin, olemme edelleen samojen kysymysten äärellä eli miten pystyä turvaamaan tietosuoja ja oikeus yksityisyyteen.

1.1 Tutkimuksen tavoitteet

Tässä opinnäytetyössä selvitettiin yksityisyydensuojaa asioiden internetissä sekä rekisteröidyn että rekisterinpitäjän kannalta. Lisäksi tutkittiin yritysten käytäntöjä tietojen keräämisessä. Tutkimus rajattiin koskemaan yksityisyydensuojaa asioiden internetissä.

Tutkimus toteutettiin kvalitatiivisena tutkimuksena jakautuen kahteen osaan: teoriaan ja haastatteluihin. Haastattelut tehtiin marraskuun 2015 ja tammikuun 2016 välisenä aikana.

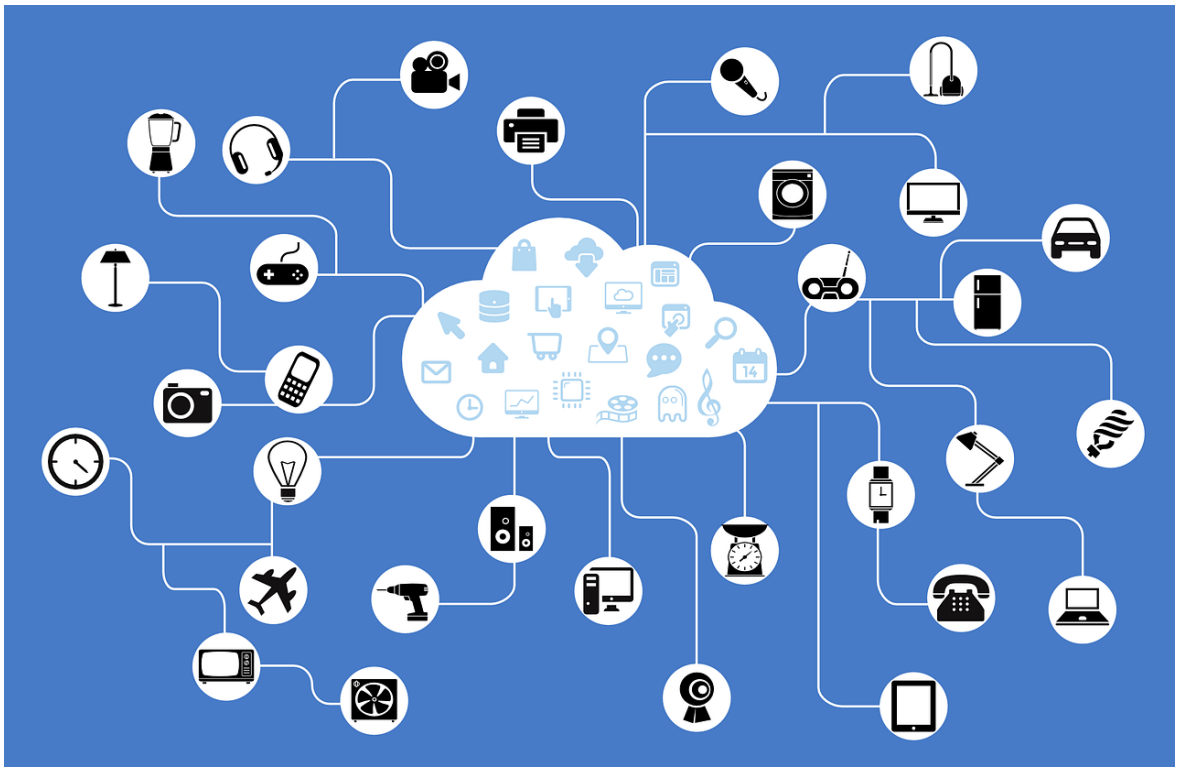
1.2 Käsitteiden määrittely

Demografinen	Väestöllinen (Suomisanakirja 2015)
Eväste	Pieni tekstitiedosto, jonka internetselain tallentaa käyttäjän laitteelle (Viestintävirasto 2015a).
Henkilötiedot	Henkilötiedot ovat tietoja, josta voi tunnistaa yksittäisen käyttäjän (Garmin 2016).
Henkilötietolaki	Peruslaki henkilötietojen käsittelystä (Tietosuojavaltuutetun toimisto 2013b).
IoT	Internet of Things, asioiden/esineiden internet
Rekisterinpitäjä	yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöön henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty. (Tietosuojavaltuutetun toimisto 2015a)
Rekisteröity	Henkilö, jota henkilötieto koskee (Tietosuojavaltuutetun toimisto 2015a)

Ubiquitos computing Jokapaikan tietotekniikka eli huomaamatta kaikkialla tapahtuva tietotekniikka (Talouselämä 2009).

Web-bug Sähköpostiin tai WWW-sivuille upotettu näkymätön kuva, joka kertoo, että käyttäjä on avannut sähköpostiviestin tai sivun (Rouse M, 2009).

2 Asioiden internet



Kuvio 1. Asioiden internet (Internet of Things)

Asioiden internet (kuvio 1) on järjestelmä, jonka avulla laitteet, kuten fyysiset esineet, palvelut, järjestelmät tai jopa ihmiset, joilla on omat sensorit, pystyvät yhdistymään internetiin ja siirtämään tietoa ilman, että ihmisen tarvitsee olla osana prosessia. (Rouse, M. 2014).

Ensimmäinen laite, joka yhdistettiin internetiin, oli Coca-Cola -kone Carnegie Mellon-nimisessä yliopistossa 1980–luvun alussa. Ohjelmoijat ottivat yliopistossa yhteyttä koneeseen internetin välityksellä tarkistaakseen, oliko koneessa kylmiä juoma valmiina, etteivät he turhaan kävelisi monta kerrosta alas. (Rouse, M. 2014).

Tällä hetkellä löytyy markkinoilta muun muassa älykelloja, aktiivirannekkeita ja älyhuonekaluja, joille kaikille on yhteistä se, että ne keräävät tietoja kuluttajasta. Älysänky esimerkiksi kerää tietoa unen laadusta ja reagoi jopa sairaskohtauksiin patjan alla olevien sensoreiden avulla (Tivi 2016), toimistopöytä muuttaa korkeuttaan käyttäjän pituuden mukaan ja säilytyslokeroiden ja neuvotteluhuoneiden käyttöastetta voidaan mitata. Älylaitteiden lisääntyessä ja kerätyn tiedon kasvaessa huoli yksityisyydensuojasta kasvaa.

3 Yksityisyydensuoja

Yksityisyydensuoja sekoitetaan helposti tietoturvaan. Tietoturvalla tarkoitetaan lähinnä teknisiä ja hallinnollisia toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys. Tietoturvallisella toiminnalla siis pyritään vahvistamaan yksityisyydensuojaa. (Viestintävirasto 2015b.)

Yksityisyyden suoja on perusoikeus, joka on turvattu Suomen perustuslaissa, EU:n perusoikeuskirjassa ja EU:n ihmisoikeussopimuksessa (Aarnio, R. 9.11.2015). Oikeus yksityisyyden suojaan säädettiin vuonna 1985 (Tietosuojavaltuutetun toimisto 2013a).

Kuviossa 2 on kuvattu yksityisyyden suojaa koskevat säännökset:

1. Henkilötietolaki on yleislaki, jota sovelletaan kaikkeen henkilötietojen käsittelyyn, ellei muissa laeissa ole vastaavia erityissäännöksiä.
2. Henkilötietojen käsittelyä koskevaa erityislainsäädäntöä on eri aloja koskevissa laeissa. Ne saattavat koskea esimerkiksi oikeutta henkilötietojen keräämiseen ja tallettamiseen tai henkilörekisterien tietosisältöä.
3. Julkisuuslakia sovelletaan silloin, kun henkilötietojen luovutetaan viranomaisten henkilörekisteristä.
4. Työelämän tietosuojalakia sovelletaan kun on kyse yksityisyyden suojasta työelämässä.
5. Tietoyhteiskuntakaari turvaa yksityisyyden suojaa ja viestinnän luottamuksellisuutta.
6. Direktiivit ja asetukset sisältävät Euroopan unionin antamia tietosuojaa koskevia kansainvälisiä normeja ja ohjeita. (Tietosuojavaltuutetun toimisto 2015e.)

Nämä säännökset selitetään tarkemmin kohdassa: 4. Yksityisyyden suojaa koskevat säännökset.

Kuvio 2. Yksityisyydensuojaa koskevat säännökset

3.1 Henkilötietojen käsittely rekisteröidyn kannalta

3.1.1 Sopimus vai suostumus

Henkilötietojen käsittely edellyttää suostumusta. Määritelmällisesti suostumus on yksipuolinen oikeustoimi, joka pitää aina olla ilman haitallisia seuraamuksia peruutettavissa. Sopimus on kaksipuoleinen oikeustoimi, joka sitoo molempia osapuolia. (Aarnio, R. 9.11.2015.)

Internetissä henkilön solmiessa sopimuksen palveluntarjoajan kanssa hänellä on kaksi vaihtoehtoa; joko hän hyväksyy sopimuksen ja saa käyttää palveluntarjoajan palveluja tai kieltäytyy hyväksymästä, jolloin hän ei voi käyttää palveluntarjoajan palveluja. On kuitenkin syytä tarkistaa seuraavat asiat ennen kuin hyväksyy sopimuksen (Viestintävirasto 2014.):

:

- mitä tietoja kerätään
- tietoon liittyvät oikeudet
- sovellettava lainsäädäntö
- minne tieto tallennetaan
- tietojen käyttötarkoitus (mihin ja miten tietoja hyödynnetään)
- tietojen luovuttaminen ja jakaminen kolmansille osapuolille
- markkinointi
- onko tieto julkista tai yksityistä
- miten tieto suojataan
- tietojen säilytysaika
- mitä tapahtuu tiedoille, kun sopimus päättyy.

3.1.2 Oikeudet

Rekisteröidyllä on oikeus selvittää, mitä tietoja hänestä on kerätty ja talletettu ja tarvittaessa pyytää asia tutkittavaksi. Ensisijaisesti tulee kääntyä rekisterinpitäjän puoleen, mutta mikäli asiaa ei saa selvitettyä rekisterinpitäjän kanssa, voi ottaa yhteyttä tietosuojavaltuutetun toimistoon. Henkilötietolaissa rekisteröidylle säädettyjä oikeuksia ovat (Tietosuojavaltuutetun toimisto 2014g):

- tiedonsaantioikeus
- tarkastusoikeus
- oikeus saada tietonsa korjatuiksi
- kielto-oikeus

Mikäli rekisteröity haluaa mahdollisimman kattavan kielto-oikeuden saa, kun kieltää Väestörekisterikeskusta ja Liikenteen turvallisuusvirastoa Trafi luovuttamasta osoitetietoja (Tietosuojavaltuutetun toimisto 2013c). Oikeuksista lisää kohdassa 4.1.9 rekisteröidyn oikeudet.

3.2 Henkilötietojen käsittely rekisterinpitäjän kannalta

3.2.1 Yleistä

Henkilötietojen käsittelyn tulee olla henkilötietolain (523/1999) 2 luvun 6 § mukaan asiallisesti perusteltua. Käsittelyn tarkoitukset, mistä henkilötiedot hankitaan sekä mihin niitä luovutetaan, on määriteltävä ennen henkilötietojen keräämistä tai muodostamista henkilörekisteriksi. Käsittelyn tarkoitusta ei myöhemmin saa muuttaa tieteellistä tai tilastotarkoitusta varten vaan sen tulee olla yhteensopiva alkuperäisten käsittelyn tarkoitusten kanssa. (HTL 2:6 §.) Lisää henkilötietojen käsittelystä kohdassa 4.1.3.

3.2.2 Ilmoitusvelvollisuus

Henkilötietolain 36 ja 37 pykälässä on säädetty, milloin rekisterinpitäjän on tehtävä ilmoitus tietosuojavaltuutetun toimistolle (Tietosuojavaltuutetun toimisto 2014f). Tarkemmin näistä pykälistä kohdassa 4.1

Velvollisuus tehdä **toimintailmoitus** koskee perintätoimistoja, mielipide- ja markkinatutkimustoimintaan elinkeinona harjoittavia yrityksiä, tietojenkäsittelypalveluja tuottavia yrityksiä ja henkilöarviointiyrityksiä, jotka tekevät työtään asiakkailleen, asiakkailtaan saamiensa toimeksiantojen mukaisesti, mikäli he käyttävät tai käsittelevät henkilörekisterissä olevia tietoja. (Tietosuojavaltuutetun toimisto 2014f.)

Automaattisesta henkilötietojen käsittelystä täytyy tietyissä laissa erikseen säädetyissä tapauksissa tehdä **rekisteri-ilmoitus** tietosuojavaltuutetulle. **Lisäksi ilmoitus tulee tehdä aina, kun tietojenkäsittelypalvelut hankitaan ulkopuolisilta yrityksiltä.** (Tietosuojavaltuutetun toimisto 2015a.)

Siirrettäessä tai luovuttaessa henkilötietoja ulkomaille ilmoitusvelvollisuus koskee lähinnä tietojen siirtämistä Euroopan Unionin ulkopuolisiin maihin, jolloin tehdään **henkilötietojen ulkomaille luovutusta koskeva ilmoitus** (Tietosuojavaltuutetun toimisto 2015a ja 2014f).

4 Yksityisyyden suojaa koskevat säännökset

Suomessa on yleislaki, joka koskee kaikkea henkilötietojen käsittelyä. Henkilötietojen käsittelyyn liittyvät ohjeet ovat erilaiset riippuen siitä, onko kyseessä esimerkiksi pankinjohtaja, työnantaja vai viranomainen. Pankinjohtajahan ei saa kysyä, paljonko sairaslomia asiakkaalla on ollut, kun taas työnantajan pitää kerätä työntekijän sairaslomatiedot. (Aarnio, R. 9.11.2015.)

Tietosuoja määrittää rekisteröidyn ja rekisterinpitäjän välisen oikeussuhteen. Suomessa kahden rekisterinpitäjän suhdetta arvioitaessa on huomioitava, että mikäli toinen on viranomainen, sitä määrittää julkisuuslaki eli silloin ei tietosuojaa sovelleta. (Aarnio, R. 9.11.2015.)

4.1 Henkilötietolaki

Suomen lainsäädännöstä henkilötietolaissa säädetään henkilötietojen käsittelyn edellytyksistä. (Viestintävirasto, 2014). Henkilötietolain (523/1999) 1 luvun 1 pykälän (§) mukaan lain tarkoituksena on turvata yksityisyyden suoja sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

4.1.1 Lain soveltaminen

Henkilötietolain (523/1999) 1 luvun 2 § mukaan lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Lisäksi sitä sovelletaan silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. Jos kuitenkin henkilötietojen käsittely on pelkästään yksityiseen käyttöön, henkilötietolakia ei sovelleta.

4.1.2 Määritelmät

Henkilötietolain (523/1999) 1 luvun 3 § kohdassa 1 määritellään henkilötiedot:

> Tässä laissa tarkoitetaan:
>
> 1) *henkilötiedolla* kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi; (HTL 1:3 § kohta 1).

Henkilötietolain (523/1999) 1 luvun 3 § kohdan 2 mukaan henkilötietojen käsittelyllä tarkoitetaan henkilötietoihin kohdistuvia toimenpiteitä:

> Tässä laissa tarkoitetaan:
> 2) *henkilötietojen käsittelyllä* henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä (HTL 1:3 § kohta 2).

Henkilötietolain (523/1999) 1 luvun 3 § kohdan 3 mukaan henkilörekisteri on henkilötietoja sisältävä tietojoukkoa, jota käsitellään automaattisen tietojenkäsittely avulla tai joka on järjestetty kortistoksi, luetteloksi tai muulla tavalla, siten että henkilöä koskevat tiedot voidaan löytää helposti:

> Tässä laissa tarkoitetaan:
> 3) *henkilörekisterillä* käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta (HTL 1:3 § kohta 3).

Henkilötietolain (523/1999) 1 luvun 3 § kohdassa 4 on määritetty rekisterinpitäjä, jolla tarkoitetaan henkilöä, yhteisöä laitosta tai säätiötä, joka kerää henkilötiedot:

> 4) *rekisterinpitäjällä* 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 (HTL 1:3 § kohta 4).

Henkilötietolain (523/1999) 1 luvun 3 § kohdan 5 mukaan rekisteröity tarkoittaa henkilöä, jota henkilötieto koskee.

4.1.3 Henkilötietojen käsittely

Henkilötietolain (523/1999) 2 luvun 8 § mukaan henkilötietoja saa käsitellä ainoastaan rekisteröidyn henkilön antamalla suostumuksella. Käsiteltävien tietojen tulee olla käsittelyn tarkoituksen kannalta tarpeelliset. Virheellisiä, epätäydellisiä ja vanhentuneita tietoja ei saa käsitellä. Henkilötietojen luovuttaminen voi tapahtua vain, jos se kuuluu tavanomaisena osana kyseisen toiminnan harjoittamista edellyttäen, että se sopii yhteen henkilötietojen käsittelyn tarkoituksen kanssa ja voidaan olettaa rekisteröidyn olevan tietoinen henkilötietojen luovuttamisesta. (HTL 2:8 §.)

> Henkilötietoja saa käsitellä ainoastaan:
>
> 1) rekisteröidyn yksiselitteisesti antamalla suostumuksella;
>
> 2) rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöönpanemiseksi, jossa rekisteröity on osallisena, taikka sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
>
> 3) jos käsittely yksittäistapauksessa on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi;
>
> 4) jos käsittelystä säädetään laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta;

5) jos rekisteröidyllä on asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan (*yhteysvaatimus*);

6) jos kysymys on konsernin tai muun taloudellisen yhteenliittymän asiakkaita tai työntekijöitä koskevista tiedoista ja näitä tietoja käsitellään kyseisen yhteenliittymän sisällä;

7) jos käsittely on tarpeen rekisterinpitäjän toimeksiannosta tapahtuvaa maksupalvelua, tietojenkäsittelyä tai muita niihin verrattavia tehtäviä varten;

8) jos kysymys on henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavista yleisesti saatavilla olevista tiedoista ja näitä tietoja käsitellään rekisterinpitäjän tai tiedot saavan sivullisen oikeuksien ja etujen turvaamiseksi; tai

9) jos tietosuojalautakunta on antanut käsittelyyn 43 §:n 1 momentissa tarkoitetun luvan.

Henkilötietojen luovuttaminen voi tapahtua 1 momentin 5 kohdan nojalla vain, jos henkilötiedon luovuttaminen kuuluu tavanomaisena osana kysymyksessä olevan toiminnan harjoittamiseen edellyttäen, että tarkoitus, johon tiedot luovutetaan, ei ole yhteensopimaton henkilötietojen käsittelyn tarkoituksen kanssa ja että rekisteröidyn voidaan olettaa tietävän henkilötietojen tällaisesta luovuttamisesta. (HTL 2:8 §.)

4.1.4 Rekisteriseloste

Rekisterinpitäjän rekisteriselosteessa on henkilötietolain (523/1999) 2 luvun 10 § mukaan oltava rekisterinpitäjän tai tämän edustajan tiedot, mihin tarkoitukseen henkilötietoja kerätään, kuvaus rekisteröityjen kohderyhmästä, mihin tietoja luovutetaan ja siirretäänkö tietoja EU:n tai ETA alueen ulkopuolelle.

Rekisterinpitäjän rekisteriselosteessa on oltava rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot, henkilötietojen käsittelyn tarkoitus, kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä, mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle sekä kuvaus rekisterin suojauksen periaatteista. (HTL 2:10 §.)

4.1.5 Arkaluontoiset tiedot

Henkilötietolain (523/1999) 3 luvun 11 § mukaan arkaluonteisten henkilötietojen käsittely on kielletty:

> Arkaluonteisten henkilötietojen käsittely on kielletty. Arkaluonteisina tietoina pidetään henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan:
>
> 1) rotua tai etnistä alkuperää;
>
> 2) henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista;
>
> 3) rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta;
>
> 4) henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia;
>
> 5) henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka
>
> 6) henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.(HTL 3:11 §.)

Henkilötietolain (523/1999) 3 luvun 12 § mukaan arkaluontoisia henkilötietoja voidaan kerätä, mikäli rekisteröity antaa suostumuksensa, tai jos rekisteröity itse on saattanut vakaumuksensa tai ammattiliittoon kuulumista julkiseksi tai mikäli tietojen käsittely on tarpeen rekisteröidyn tai jonkun toisen henkilön elintärkeän edun suojaamiseksi. Arkaluontoiset tiedot on poistettava rekisteristä välittömästi kun käsittelylle ei ole enää perustetta. Perustetta ja käsittelyn tarvetta on arvioitava vähintään viiden vuoden välein, ellei laista tai 1 momentin 13 kohdassa tarkoitetusta tietosuojalautakunnan luvasta muuta johdu. (HTL 3:12 §.)

4.1.6 Henkilötunnuksen käsittely

Henkilötunnusta saa henkilötietolain (523/1999) 13 § mukaan käsitellä vain rekisteröidyn luvalla tai jos siitä säädetään laissa. Tämän lisäksi henkilötunnusta saa käsitellä, mikäli on tärkeää, että rekisteröity yksilöityy laissa säädetyn tehtävän suorittamiseksi, oikeuksien ja velvollisuuksien toteuttamiseksi tai historiallista tai tieteellistä tutkimusta tai tilastointia varten. (HTL 3:13 §.)

Rekisterinpitäjän on huolehdittava siitä, että henkilötunnusta ei merkitä tarpeettomasti henkilörekisterin perusteella asiakirjoihin (HTL 3:13 §).

4.1.7 Suoramarkkinointi ja muut osoitteelliset lähetykset

Henkilörekisteriä saa henkilötietolain (523/1999) 4 luvun 19 pykälän mukaan käyttää suoramarkkinointiin, mielipide- tai markkinatutkimukseen tai muihin näihin rinnastettaviin osoitteellisiin lähetyksiin, jollei rekisteröity ole kieltänyt henkilötietojen keräämistä ja tallettamista tähän tarkoitukseen. Edellytyksenä näille osoitteellisille lähetyksille on, että henkilörekisteriä käytetään lyhytaikaiseen ja ennakolta yksilöityyn toimeen eikä se vaaranna rekisteröidyn yksityisyyden suojaa. Henkilörekisteri saa sisältää vain rekisteröidyn nimen, arvon, ammatin, iän, äidinkielen ja sukupuolen, yhden tunnistetiedon ja yhteystiedot yhteydenottoa varten. Mikäli henkilörekisteriä käytetään rekisteröidyn työtehtäviin liittyvään informaation lähettämiseen, henkilörekisteri saa sisältää tietoja jotka koskevat hänen tehtäviään ja asemaa elinkeinoelämässä tai julkisessa tehtävässä. (HTL 4:19 §.)

4.1.8 Henkilötietojen luovutus EU:n ja ETA:n ulkopuolelle

Henkilötietoja voidaan siirtää EU:n ja ETA:n ulkopuolelle vain, jos taataan riittävä tietosuojan taso kyseisessä maassa. Riittävä tietosuojan taso riippuu henkilötietolain (523/1999) 5 luvun 22 § mukaan tietojen luonteesta, luovuttamisen tarkoitusperästä ja kestoajasta, alkuperämaassa ja kohdemaassa voimassa olevista yleisistä ja alakohtaisista oikeussäännöistä sekä käytännesäännöistä ja noudatettavista turvatoimista. (HTL 5:22 §.)

Jos yllä olevat ehdot eivät täyty, mutta rekisteröity on antanut suostumuksensa tai rekisteröidyn ja rekisterinpitäjän välillä on jokin olemassa oleva sopimus, jota ei voi toteuttaa ilman siirtoa, rekisteröidyn henkilötiedot saa siirtää luvun 23 mukaan. Myös mikäli henkilötietojen siirto on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi tai yleisen edun turvaamiseksi tai jos se on oikeusvaateen kannalta tärkeä. (HTL 5:23 §.)

Safe Harbor on Euroopan yhteisöjen komission vuonna 2000 hyväksymä järjestely, jota käyttäen yritykset ja asiakkaat ovat saaneet siirtää henkilötietoja Euroopasta Yhdysvaltoihin. Lokakuussa 2015 EU tuomioistuimen tekemän päätöksen mukaan Safe Harbor – järjestely ei takaa riittävää henkilötietosuojaa ja uusien siirtomenettelyjen neuvottelut ovat vielä kesken. (Tietosuojavaltuutetun toimisto, 2015c.)

Yritysten on siis selvitettävä voiko henkilötietojen siirtoa jatkaa muiden tietojensiirtoperusteiden nojalla vai onko esimerkiksi palveluntarjoajalla mahdollisuus säilyttää tiedot EU:n sisäpuolella, kunnes päästään sopimukseen uusista korvaavista siirtomenettelyistä Euroopan komission ja Yhdysvaltojen hallinnon välillä. (Tietosuojavaltuutetun toimisto, 2015b.)

Euroopan komissio julkaisi 29.2.2016 EU-U.S Privacy –järjestelyn dokumentit, joiden avulla järjestelyn toimeenpaneminen voidaan toteuttaa. Tämä uusi järjestely, joka sisältää vahvoja ja riittäviä suojamekanismeja, tulee, astuessaan voimaan, korvaamaan Safe Harbor –järjestelyn, joka todettiin riittämättömäksi henkilötietosuojan kannalta. (Tietosuojavaltuutetun toimisto, 2016)

4.1.9 Rekisteröidyn oikeudet

Rekisteröidyn oikeudet on säädetty henkilötietolain (523/1999) 6 luvussa. 24 pykälän mukaan rekisterinpitäjän tulee kerätessään henkilötietoja huolehdittava siitä, että rekisteröity voi saada tiedon rekisterinpitäjästä tai sen edustajasta, henkilötietojen käsittelyn tarkoituksesta ja siitä, mihin tietoja luovutetaan säännönmukaisesti sekä rekisteröityjen oikeuksien käyttämisestä henkilötietojen käsittelyssä (HTL 6:24 §).

Henkilötietolain (523/1999) 6 luvussa 25 § mukaan suoramarkkinoinnissa ja markkina- ja mielipidetutkimuksen kyselyssä ja muussa osoitteellisessa kyselyssä rekisteröidylle on ilmoitettava sen henkilörekisterin nimi ja rekisterinpitäjä ja tämän yhteystiedot, joista rekisteröidyn nimi- ja puhelintiedot on hankittu. Puhelinmyynnissä vastaavat tiedot on annettava pyynnöstä. (HTL 6:25 §).

Jokaisella on oikeus tarkastaa, mitä häntä koskevia tietoja henkilörekisterissä on tai ettei rekisterissä ole häntä koskevia tietoja. Samalla on rekisterinpitäjän ilmoitettava säännönmukaiset tietolähteet sekä mihin rekisterin tietoja käytetään ja mihin säännönmukaisesti luovutetaan. Jos on kyse automatisoidusta päätöksestä, rekisteröidyllä on oikeus saada tieto myös automaattiseen käsittelyyn liittyvistä toimenpiteistä.

26 pykälän 3 momentin mukaan tietojen tarkastaminen tulee olla ilmaista, jos edellisestä pyynnöstä on kulunut enemmän kuin yksi vuosi. Jos edellisestä pyynnöstä on kulunut vähemmän kuin vuosi, rekisterinpitäjä saa periä kohtuullisen korvauksen, joka ei saa ylittää tiedon antamisesta aiheutuvia välittömiä kustannuksia. (HTL 6:26 §).

Henkilötietolain (523/1999) 6 luvun 27 § 1 momentin mukaan tarkastusoikeutta ei ole, jos tiedon antaminen saattaisi:

- vahingoittaa valtion turvallisuutta, puolustusta tai yleistä järjestystä ja turvallisuutta taikka haitata rikosten ehkäisemistä tai selvittämistä
- aiheuttaa vakavaa vaaraa rekisteröidyn terveydelle tai hoidolle taikka jonkun muun oikeuksille

Tarkastusoikeutta ei myöskään ole, jos henkilötietoja käytetään yksinomaan historiallista tai tieteellistä tutkimusta taikka tilastointia varten tai jos rekisterissä olevia henkilötietoja käytetään valvonta- ja tarkastustehtävissä ja tiedon antamatta jättäminen on välttämätöntä Suomen tai Euroopan unionin tärkeän taloudellisen tai rahoituksellisen edun turvaamiseksi. Jos vain osa tiedoista on sellaisia, että ne jäävät tarkastusoikeuden ulkopuolelle, rekisteröidyllä on oikeus tietää muut hänestä tallennetuista tiedoista. (HTL 6:27 §.)

Mikäli rekisteröity haluaa tarkastaa itseään koskevat tiedot, hänen on henkilötietolain (523/1999) 6 luvussa 28 § mukaan esitettävä pyyntö rekisterinpitäjälle omakätisesti allekirjoitetussa tai sitä vastaavalla tavalla varmennetussa asiakirjassa tai henkilökohtaisesti rekisterinpitäjän luona. Rekisterinpitäjän tulee ilman aiheetonta viivytystä varata rekisteröidylle tilaisuus tutustua tietoihin tai rekisteröidyn niin pyytäessä, annettava ne kirjallisessa muodossa.

Jos rekisterinpitäjä kieltäytyy antamasta tietoja, hänen on annettava tästä kirjallinen todistus. Kieltäytymisen veroiseksi katsotaan myös, mikäli rekisterinpitäjä ei ole vastannut kirjallisesti kolmeen kuukauteen pyynnön esittämisestä. Rekisteröity voi saattaa asian tietosuojavaltuutetun käsiteltäväksi. (HTL 6:28 §.)

Henkilötietolain (523/1999) 6 luvussa 29 § mukaan rekisterinpitäjän on ilman aiheetonta viivytystä oma-aloitteisesti tai rekisteröidyn vaatimuksesta oikaistava, poistettava tai täydennettävä rekisterissä oleva, käsittelyn tarkoituksen kannalta virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto. Rekisterinpitäjän on myös estettävä tällaisen tiedon leviäminen, jos tieto voi vaarantaa rekisteröidyn yksityisyyden suojaa tai hänen oikeuksiaan. Mikäli rekisterinpitäjä kieltäytyy, hänen tulee antaa kirjallinen todistus siitä, jonka rekisteröity voi saattaa tietosuojavaltuutetun käsiteltäväksi. (HL 6:29 §.)

Henkilötietolain (523/1999) 6 luvussa 30 § mukaan rekisteröidyllä on oikeus kieltä rekisterinpitäjää käsittelemästä häntä itseään koskevia tietoja suoramainontaa, etämyyntiä ja muuta suoramarkkinointia sekä markkina- ja mielipidetutkimusta samoin kuin henkilömatrikkelia ja sukututkimusta varten. (HTL 6:30 §.)

4.1.10 Ilmoitus tietosuojavaltuutetulle

Henkilötietolain (523/1999) 8 luvun 36 §:n mukaan rekisterinpitäjän on ilmoitettava henkilötietojen automaattisesta käsittelystä tietosuojavaltuutetulle lähettämällä tälle rekisteriseloste. Lisäksi rekisterinpitäjän on ilmoitettava tietosuojavaltuutetulle henkilötietojen siirrosta Euroopan unionin jäsenvaltioiden alueen tai Euroopan talousalueen ulkopuolelle, jos tietoja siirretään 22 §:n nojalla tai 23 §:n 6 tai 7 kohdassa tarkoitetuilla perusteilla eikä siirrosta ole laissa säädetty sekä 31 §:ssä tarkoitetun automatisoidun päätöksentekojärjestelmän käyttöönotosta. (HTL 8:36 §.)

Joka harjoittaa elinkeinona perimistoimintaa tai markkina- tai mielipidetutkimusta taikka hoitaa toisen lukuun henkilöstön valintaan ja soveltuvuuden arviointiin liittyviä tehtäviä tai tietojenkäsittelytehtäviä ja tässä toiminnassa käyttää tai käsittelee henkilörekistereitä ja niissä olevia tietoja, on velvollinen tekemään ilmoituksen toiminnastaan tietosuojavaltuutetulle. (HTL 8:36 §.)

Ilmoitus on henkilötietolain (523/1999) 8 luvun 37 § mukaan tehtävä riittävän ajoissa, kuitenkin viimeistään 30 päivää ennen henkilörekisteriin talletettaviksi aiottujen henkilötietojen keräämistä ja tallettamista tai muuhun ilmoitusvelvollisuuden aiheuttavaan toimenpiteeseen ryhtymistä.

4.2 Erityislainsäädäntö

Erityislakien henkilötietojen käsittelyä koskevat säännökset vaikuttavat myös henkilötietojen käsittelyyn. Erityislainsäädäntöä sovelletaan ensisijaisena yleislakiin nähden, paitsi henkilötietolain yleisvelvoitteiden osalta, joita ei erityislainsäädännössä ole mainintaa. Henkilötietolain yleisvelvoitteita ovat esimerkiksi vaatimus määritellä käsiteltävien henkilötietojen keräämisen tarkoitus ja tarpeellisuus sekä huolellisuus- ja suojaamisvelvoitteet. Henkilötietolakeihin nähden kaikkia toimialoja koskevia erityislakeja tai -säännöksiä ovat laki sähköisen viestinnän tietosuojasta sekä laki yksityisyyden suojasta työelämässä. Yksityisen sektorin rekisterinpitoon vaikuttavia lakeja ovat esimerkiksi laki luottolaitostoiminnasta, vakuutustoimintaa koskevat lait, työeläkelait ja työterveyshuoltolaki. (Tietosuojavaltuutetun toimisto 2014a.)

4.3 Julkisuuslaki

Henkilötietojen luovutus viranomaisten henkilörekisteristä määräytyy viranomaisten toiminnan julkisuudesta annetun lain mukaan, paitsi tilanteet, joissa erityislain säännös oikeuttaa jonkin viranomaisen luovuttamaan tai saamaan henkilötietoja. Henkilötietoja luovuttava viranomainen joutuu selvittämään lainmukaisuuden sekä julkisuuslain että henkilötietolain perusteella. (Tietosuojavaltuutetun toimisto 2014b.)

Julkisuuslain mukaan jokaisella on oikeus saada tieto itseään koskevista viranomaisen asiakirjaan sisältyvistä tiedoista. Jos on kyse henkilörekisteriin sisältyvästä tiedosta, joudutaan arvioimaan suhdetta henkilötietolaissa säädettyyn rekisteröityjen tarkastusoikeuteen. (Tietosuojavaltuutetun toimisto 2014b.)

Henkilötietojen käsittelyyn on julkisuuslaissa salassapitoa koskevia säännöksiä. Säännökset ovat pääosin julkisuuslain 24 pykälässä (Tietosuojavaltuutetun toimisto 2014b). Tässä poimintoja julkisuuslain (621/1999) 6 luvusta 24 pykälästä:

> Salassa pidettäviä viranomaisen asiakirjoja ovat, jollei erikseen toisin säädetä:
>
> henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista (Laki viranomaisten toiminnan julkisuudesta 6:24 § kohta 7.)
>
> 31) asiakirjat, jotka sisältävät tiedon henkilön ilmoittamasta salaisesta puhelinnumerosta tai tiedon matkaviestimen sijaintipaikasta, samoin kuin asiakirjat, jotka sisältävät tiedon henkilön kotikunnasta ja hänen siellä olevasta asuinpaikastaan tai tilapäisestä asuinpaikastaan samoin kuin puhelinnumerosta ja muista yhteystiedoista, jos henkilö on pyytänyt tiedon salassapitoa ja hänellä on perusteltu syy epäillä itsensä tai perheensä terveyden tai turvallisuuden tulevan uhatuksi;(30.11.2001/1151) (Laki viranomaisten toiminnan julkisuudesta 6:24 § kohta 31.)
>
> 32) asiakirjat, jotka sisältävät tietoja henkilön poliittisesta vakaumuksesta tai tietoja henkilön yksityiselämän piirissä esittämistä mielipiteistä taikka tietoja henkilön elintavoista, osallistumisesta yhdistystoimintaan tai vapaa-ajan harrastuksista, perhe-elämästä tai muista niihin verrattavista henkilökohtaisista oloista; asiakirjat, jotka sisältävät tietoja henkilön toimimisesta poliittisessa tai muussa luottamustehtävässä tai henkilön pyrkimisestä sellaiseen tehtävään samoin kuin henkilön osallistumisesta poliittisen puolueen perustamiseen ja rekisteröintiin tai valitsijayhdistyksen perustamiseen vaaleja varten, ovat kuitenkin julkisia. (Laki viranomaisten toiminnan julkisuudesta 6:24 § kohta 32.)

4.4 Työelämän tietosuojalaki

Työelämän tietosuojalain on tarkoitus vastata yksityiselämän suojaa koskeviin kysymyksiin työelämän alueella. Laki koskee vain työntekijän ja työnantajan välistä suhdetta. (Tietosuojavaltuutetun toimisto 2014e.)

Kun työnantaja kerää työntekijöidensä henkilötietoja omiin tarpeisiinsa, työntekijällä on oikeus tietää ja päättää omien henkilötietojensa käsittelystä ja sisällöstä. Työelämän tietosuojalaissa säädetään mm. henkilötietojen käsittelystä, huumausaineiden käyttöä koskevien tietojen käsittelystä, kameravalvonnasta työpaikalla sekä työnantajille kuuluvien sähköpostiviestien käsittelystä. (Työ- ja elinkeinoministeriö 2016.)

Tämän erityislain ohella myös henkilötietolaissa ja tietoyhteiskuntakaaressa on yleisiä tietosuojaan liittyviä säännöksiä, joita sovelletaan työelämässä. Tätä lakia valvovat työsuojeluviranomaiset ja tietosuojavaltuutetun toimisto. (Työ- ja elinkeinoministeriö 2016.)

4.5 Tietoyhteiskuntakaari

Suomessa henkilötietolain lisäksi toinen tärkeä laki yksityisyydensuojan kannalta on tietoyhteiskuntakaari, joka astui voimaan 1.1.2015. Tällä lailla kumottiin sähköisen viestinnän tietosuojalaki. Tietoyhteiskuntakaari sisältää keskeiset sähköistä viestintää koskevat säädökset. (Tietosuojavaltuutetun toimisto 2015e.)

Lain tarkoituksena on edistää sähköisen viestinnän palvelujen tarjontaa ja käyttöä. Lisäksi sen tavoitteena on varmistaa, että viestintäpalvelut ja viestintäverkot on kohtuullisin ehdoin jokaisen saatavilla koko maassa ja että ne ovat teknisesti laadultaan hyviä ja toimintavarmoja. Tämän lain tarkoituksena on myös turvata radiotaajuuksien häiriötön käyttö ja edistää kilpailua. (Tietosuojavaltuutetun toimisto 2015f.)

4.6 Direktiivit ja asetukset

Direktiivit ovat Euroopan unionin parlamentin ja neuvoston laatimia lainsäädäntöohjeita.

Ne osoittavat halutun lopputuloksen, mutta lainsäädännön muodot ja keinot ovat jäsenvaltioiden valittavissa. Direktiivin täytäntöönpano tapahtuu kansallisella lainsäädännöllä. Asetukset ovat taas sellaisenaan sovellettavissa ilman täytäntöönpanotoimia. (Tietosuojavaltuutetun toimisto 2015d.)

Tietosuojan kannalta keskeisimmät direktiivit ovat henkilötietodirektiivi ja sähköisen viestinnän tietosuojadirektiivi. Suomessa henkilötietolaki on saatettu vastaamaan henkilötietodirektiiviä ja tietoyhteiskuntakaari sähköisen viestinnän tietosuojadirektiiviä. (Tietosuojavaltuutetun toimisto 2015d.)

Henkilötietojen käsittelyä koskevia säädöksiä voi olla myös kansainvälisissä sopimuksissa. Sopimus sitoo allekirjoittamaata, kun se on kansallisesti saatettu voimaan, yleensä säätämällä laki, jota sopimus koskee. . (Tietosuojavaltuutetun toimisto 2015d.)

5 Tietosuojavastaaville tärkeät eurooppalaiset sopimukset

Tietosuojavastaaville tärkeitä sopimuksia ovat Euroopan Ihmisoikeussopimus (kannattaa opetella ulkoa), Euroopan neuvoston yleissopimus 108 ja voimassa oleva Euroopan perusoikeussopimus, jonka 7 ja 8 artiklaa erityisesti valvotaan. (Aarnio, R. 9.11.2015.)

5.1 Euroopan ihmisoikeussopimus

Euroopan ihmisoikeussopimuksen (63/1999) mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta (8 artikla 1 momentti).

8 artiklan 2 momentin mukaan viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi jos yleinen turvallisuus, rikollisuuden tai epäjärjestyksen estäminen, terveyden ja moraalin suojaaminen tai muiden henkilöiden oikeuksien ja vapauksien turvaaminen niin vaatii ja laki sen sallii.

Sukupuoleen, rotuun, ihonväriin, kieleen, uskontoon, poliittisiin tai muihin mielipiteisiin, kansalliseen tai yhteiskunnalliseen alkuperään, kansalliseen vähemmistöön kuulumisen, varallisuuteen, syntyperään tai muuhun asemaan perustuva syrjintä on kielletty (14 artikla).

5.2 Euroopan neuvoston yleissopimus 108

Euroopan neuvoston yleissopimus 108 on yleissopimus henkilötietojen automaattisessa tietojenkäsittelyssä. Kaikki EU:n jäsenvaltiot ovat vahvistaneet sen.
Se on ainoa oikeudellisesti sitova kansainvälinen sopimus tietosuojan alalla ja sitä sovelletaan sekä yksityisellä että julkisella sektorilla. (Euroopan neuvosto 2014.)

Tässä sopimuksessa annetaan henkilötietojen keruuseen ja käsittelyyn liittyviä ohjeita mm. kieltämällä arkaluontoisten henkilötietojen käsittelyn ilman riittäviä oikeudellisia suojatoimia. Yksilön oikeus saada tietää hänestä tallennetuista tiedoista ja tarvittaessa saada korjata tietoja vahvistetaan tässä sopimuksessa. Näitä oikeuksia voidaan rajoittaa vain mikäli välttämätön etu, kuten valtion turvallisuus tai puolustus, sitä vaatii. . (Euroopan neuvosto 2014.)

Yleissopimuksessa mahdollisestaan henkilötietojen vapaa siirto sopimuspuolena olevien jäsenvaltioiden välillä, mutta maihin joissa ei ole vahvistettu riittävää suojaa asetetaan tiettyjä rajoituksia. . (Euroopan neuvosto 2014.)

5.3 Euroopan unionin perusoikeuskirja

Riippumaton viranomainen valvoo Euroopan unionin perusoikeussopimuksen 7 ja 8 artiklan noudattamista (Aarnio, R. 9.11.2015). 7 artiklassa sanotaan, että jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan. 8 artiklassa sanotaan, että jokaisella on oikeus henkilötietojensa suojaan, ja että tietojenkäsittelyn on oltava asianmukaista ja tapahduttava tiettyä tarkoitusta varten ja henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua kerättyihin tietoihin ja saada ne oikaistuiksi. (EUR-Lex., 2000.)

6 EU:n tietosuojauudistus

Euroopan parlamentti, komissio ja neuvosto ovat päässeet sopuun uudesta tietosuoja-asetuksesta. Se on tarpeen, koska rajat ylittävä verkkokauppa on lisääntynyt voimakkaasti ja teknologia kehittynyt. Näiden myötä myös henkilötietoja kerätään yhä enemmän. (Tietosuojavaltuutetun toimisto 2015c.)

Uudessa tietosuoja-asetuksessa henkilötietojen käsittely on kaikille kansalaisille EU:ssa yhdenmukainen. Tämä parantaa henkilöiden luottamusta internetin tarjoamiin palveluihin. Se myös helpottaa rekisterinpitäjää, joka toimii monessa jäsenvaltiossa. Tähän asti yritys on joutunut selvittämään jokaisen maan tietosuojasäännökset erikseen. Tietosuojan yhdenmukaisuuden varmistamiseksi tullaan perustamaan Euroopan tietosuojaneuvosto. (Tietosuojavaltuutetun toimisto 2015c.)

EU:n tietosuojauudistus helpottaa myös kuluttajan mahdollisuuksia kilpailuttaa palveluntarjoajia, sanoo tietosuojavaltuutettu Reijo Aarnio Turun Sanomien tekemässä haastattelussa. Uudistuksen myötä tulee olemaan nykyistä helpompaa siirtää tietonsa tietokannasta toiseen. (Sairanen, M. 2016.)

Rekisteröidyn oikeudet tulevat olemaan aika lailla samat kuin nykyäänkin eli oikeus tarkastaa henkilötiedot pysyy (3.1.2) ja rekisterinpitäjän on oikaistava virheelliset, tarpeettomat ja vanhentuneet henkilötiedot. Lakisääteisiin rekistereihin henkilöllä ei ole oikeutta saada omia tietojansa poistettua. Uutena oikeutena rekisteröity voi pyytää itseään koskevia tietoja sähköisesti, julkisella sektorilla siirto-oikeutta ei kuitenkaan sovelleta. (Tietosuojavaltuutetun toimisto 2015c.)

Alle 16-vuotiaan henkilötietojen käsittely on kiellettyä ilman vanhempien lupaa, mikä tarkoittaa sitä, ettei alle 16–vuotias esimerkiksi saa käyttää sosiaalisen median palveluja ilman vanhempien lupaa. Tosin ikäraja on sovittavissa jäsenmaakohtaisesti kuitenkin niin, että alin ikäraja on 13 vuotta. Oleellinen muutos yrityksille on velvollisuus nimittää tietosuojavastaava. Nykyään esimerkiksi apteekeilla ja terveydenhuoltoyrityksillä on velvollisuus nimetä tietosuojavastaava. (Tietosuojavaltuutetun toimisto 2015c.)

Yrityksen on pystyttävä osoittamaan, että tietosuojasäännökset huomioidaan sen toiminnassa. Tietoturvaloukkauksista on ilmoitettava tietosuojaviranomaiselle. (Tietosuojavaltuutetun toimisto 2015c.)

Tietosuoja-asetusta tullaan soveltamaan sellaisenaan Suomessa nykyisen EU:n henkilötietodirektiivin sijaan. Suomen lainsäädäntöä joudutaan kuitenkin muuttamaan jonkin verran, sillä jäsenvaltiot voivat antaa asetusta tarkentavaa lainsäädäntöä erityisesti julkisella sektorilla. (Tietosuojavaltuutetun toimisto 2015c.)

7 Tutkimustulokset

Tutkimus toteutettiin kvalitatiivisena eli laadullisena tutkimuksena kahdessa osassa; ensimmäisessä osassa tutkin viranomaisen näkökulmasta, mitkä lait ja direktiivit koskevat henkilötietojen keräilyä haastattelemalla tietosuojavaltuutettu Reijo Aarniota; toisessa osassa tutkin yritysten näkökulmasta, mitä tietoja he keräävät ja mitä he tekevät näillä tiedoilla haastattelemalla yhtä yritystä ja tutkimalla kahden eri aktiivirannekkeita myyvien yritysten käyttöehtoja.

7.1 Tietosuojavaltuutettu Reijo Aarnion haastattelu

7.1.1 Henkilötietojen käsittely

Henkilötietojen käsittely edellyttää suostumusta. Määritelmällisesti suostumus on yksipuolinen oikeustoimi, joka pitää aina olla ilman haitallisia seuraamuksia peruutettavissa. Sopimus on kaksipuoleinen oikeustoimi, joka sitoo molempia osapuolia. (Aarnio, R. 9.11.2015.) Lisää kohdassa 3.1.

Suomessa on yleislaki, joka koskee kaikkea henkilötietojen käsittelyä. Henkilötietojen käsittelyyn liittyvät ohjeet ovat erilaiset riippuen siitä, onko kyseessä esimerkiksi pankinjohtaja, työnantaja vai viranomainen. Pankinjohtajahan ei saa kysyä, paljonko sairaslomia asiakkaalla on ollut, kun taas työnantajan pitää kerätä työntekijän sairaslomatiedot. (Aarnio, R. 9.11.2015.)

Tietosuoja määrittää rekisteröidyn ja rekisterinpitäjän välisen oikeussuhteen. Suomessa kahden rekisterinpitäjän suhdetta arvioitaessa on huomioitava, että mikäli toinen on viranomainen, sitä määrittää julkisuuslaki eli silloin ei tietosuojaa sovelleta. (Aarnio, R. 9.11.2015.)

Tietosuojavastaaville tärkeitä eurooppalaisia sopimuksia ovat Euroopan ihmisoikeussopimus (kannattaa opetella ulkoa), Euroopan neuvoston yleissopimus 108 ja voimassa oleva Euroopan perusoikeussopimus, jonka 7 ja 8 artiklaa erityisesti valvotaan. (Aarnio, R. 9.11.2015.) Lisätietoa kohdassa 5.

7.1.2 Direktiivit

Suomessa Suomen lait ja EU:n lait sitovat. Jos EU:n lait ja Suomen laki määrittää saman asian eri tavalla komissio haastaa jäsenvaltiot EU:n tuomioistuimeen, jossa päätetään, onko direktiivi lainvastainen vai onko Suomen lakia muutettava. Esimerkkinä Mandatory datory tension – nimellä kulkeva sähköisen tietojärjestelmän pakkotallennusdirektiivi 206/46 todettiin laittomaksi 12.3.2014. (Aarnio, R. 9.11.2015.)

Henkilötietodirektiivin mukaan tietojenkäsittelyjärjestelmät on tarkoitettu palvelemaan ihmistä ottaen huomioon ihmisten perusoikeudet, erityisesti oikeus ihmisen yksityisyyteen. Tietojenkäsittelyjärjestelmien on edistettävä kansainvälistä kauppaa, hyvinvointia ja yhteistoimintaa. (Aarnio, R. 9.11.2015.)

Kun puhutaan direktiiveistä, valitustie kulkee kansainvälisen tuomioistuimen kautta EU tuomioistuimeen, mutta ihmisoikeusrikkomuksissa tie menee ihmisoikeustuomioistuimeen. (Aarnio, R. 9.11.2015.) Lisää direktiiveistä kohdassa 4.6.

Esimerkkitapauksena voidaan pitää sairaalan potilastietojärjestelmän tietoturvaominaisuutta arvioitaessa I vastaan Suomi heinäkuun 17, 2008, jossa arvioitiin, oliko se ihmisoikeussopimuksen mukainen. Todettiin, ettei se ole. (Aarnio, R. 9.11.2015.)

Tapauksessa oli kysymys potilaan yksityisyyden suojan loukkauksesta, kun ei ollut järjestetty riittäviä takeita siitä, ettei potilasrekisteriin pääsisi muut kuin potilasta hoitanut henkilöstö. Valittaja oli työskennellyt sairaanhoitajana silmätautien poliklinikalla. Samaan aikaan hän kävi tartuntatautien poliklinikalla, kun hänet oli todettu HIV-positiiviseksi.

Hänellä oli herännyt epäilys siitä, että työtoveritkin tiesivät hänen sairaudestaan. Siihen aikaan sairaalan henkilökunnalla oli vapaa pääsy potilasrekistereihin. Lopputulos: Euroopan ihmisoikeustuomioistuin oli yksimielinen siitä, että Euroopan ihmisoikeussopimuksen 8 artiklaa oli rikottu, kun potilastietoja oli päässyt vuotamaan rekisterijärjestelmän puutteiden vuoksi. (Finlex 2008.)

7.1.3 Tietojen jakaminen

Kun jakaa kolmansille osapuolille tietoa, niin pitää olla oikeus siihen ja oikeus määräytyy erilaisten seikkojen perusteella kuten laki ja käsittelyn tarkoitus. Rekisterinpitäjän tulee antaa selvitys oikeudesta ryhtyä tietoja käsittelemään ja miten niitä aiotaan suojata**.** Rekisterinpitäjälle tietosuojavaltuutetun toimiston julkaisema **Ota oppaaksi henkilötietolaki!** (Aarnio, R. 9.11.2015.)

7.1.4 Haasteet

Asioiden internetin kasvu tuo tullessaan useita haasteita, kuten esimerkiksi lainsäädännön ajan tasalla pitäminen. Vientituotteeksi tuotteistamisessa täytyy ottaa huomioon sekä eurooppalainen että maailmanlaajuinen kehikko. Lisäksi omat haasteensa tuo teknologian suuri vaikutus ihmisten sosiaaliseen käyttäytymiseen ja taloudelliseen hyvinvointiin. Asioiden internet saattaa johtaa valtavaan ihmisten valvontaan, joka ei meille länsimaisille ihmisille ole tuttua. (Aarnio, R. 9.11.2015.)

7.1.5 Selvitettäviä tapauksia

Asioiden internetiin selvitettäviä tapauksia ei varsinaisesti ole ollut, mutta esimerkiksi radiotaajuustekniikkaan liittyvät kysymykset ovat olleet selvitettävänä. Aikoinaan ensimmäiset biometriset passit (etäluettavalla sirulla olevat RFID -passit) herättivät pelkoa ihmisissä siitä, miten käy yksityisyyden suojan. Lisäksi poliittisella tasolla hallituksella on ollut digiloikka, jossa mennään kohti tietointensiivistä taloutta. (Aarnio, R. 9.11.2015.)

7.1.6 Tietojen säilyttäminen

Henkilötietoja voi säilyttää niin kauan, kun on asiallinen peruste niitä säilyttää. Eri tilanteissa on erilainen tallennusaika, esimerkiksi työnantaja ei saa säilyttää niitä kauan aikaa, kun taas sairaalan tulee tallentaa ne pysyvästi. Organisaation tulee etukäteen määritellä kauanko he säilyttävät tietoja. (Aarnio, R. 9.11.2015.)

7.1.7 EU:n ulkopuolelta tulevat yritykset

Yrityksen toimiessa EU:ssa yrityksen tulee aina noudattaa EU:n lakeja henkilötietojen käsittelyn osalta (Aarnio, R. 9.11.2015).

Tapauksessa Google Spain vastaan Colteja tutkittiin, milloin yhdysvaltalainen yritys oikeasti on EU:n markkinoilla (Aarnio, R. 9.11.2015). Colteja valitti Google Spainille hakukoneen tuloksista, koska se loukkasi hänen yksityisyyttään ja tieto oli vanhentunut. Google Spain laittoi valituksen eteenpäin Kaliforniassa sijaitsevalle Google Incille, joka oli vastuussa hakukoneesta. Tapaus meni EU:n tuomioistuimelle, koska Google Inc. oli mielestään oikeassa noudatettuaan amerikkalaista näkemystä. EU:n tuomioistuin ratkaisi tapauksen Costejan hyväksi. (Euroopan tuomioistuin, 2014.).

7.1.8 Mistä apua yrityksille?

Tietosuojavaltuutetun toimisto antaa yleisellä tasolla ohjausta niin paljon kuin ehtivät. Asioiden internetiä koskevaan yksityiskohtaiseen ohjaamiseen ei ole valmiuksia; tilanteet vaihtelevat niin paljon, että ohjausta voidaan antaa vain yleisellä tasolla, mutta tietosuojayhteisö on ohjeistanut sovellusten osalta todeten, että niihin sovelletaan rekisterinpitäjän velvoitteita ja vastaavasti kuluttajan oikeuksia. (Aarnio, R. 9.11.2015.)

7.2 Yrityshaastattelu

Haastattelemani yritys myy IoT-ratkaisuja omille asiakasyrityksilleen. Henkilötunnuksia ei kerätä, mutta jokainen loppukäyttäjä saa käyttäjätunnuksen.

Asiakkaista kerätään vain liiketoiminnalle hyödyllisiä tietoja eli esimerkiksi tietyn laitteen käyttöastetta. Tietoja säilytetään ulkopuolisen tietoyrityksen pilvessä ainakin puoli vuotta, mutta käytännössä tiedot saattavat olla siellä ikuisesti. Lakeja, joita yritys on ottanut huomioon IoT-toiminnassaan, on laki yksityisyydensuojasta ja henkilötietolaki. (Yritys x, 7.1.2016.)

Laitteiden keräämät tiedot tallentuvat alihankkijoiden palvelimille, mutta palvelinten sijainti ei välttämättä ollut yrityksen tiedossa. Tiedettiin kuitenkin, että ne olivat EU:n rajojen sisäpuolella. Lisäksi tieto siitä, milloin yrityksen keräämät tiedot kuuluvat henkilötietolain piiriin ja rekisteri-ilmoitus tulee täyttää, oli joissakin tapauksissa epäselvää. (Yritys x, 7.1.2016.)

7.3 Aktiivisuusrannekkeiden valmistajien yksityisyyden suoja

Haastattelemani yrityksen lisäksi vertasin aktiivisuusrannekkeita myyvien yritysten toimintatapoja. Yritykset, joita tutkin, olivat Fitbit, Garmin ja Polar.

7.3.1 Henkilötiedot

Tarjotakseen palveluja Polar saattaa kysyä henkilötietoja, jotka tallennetaan asiakastietokantaan. Yritys saattaa kerätä myös teknistä tietoa liittyen ostettuun tuotteeseen, lisätarvikkeisiin ja ohjelmiin sekä näiden käyttöön. Näitä tietoja saatetaan käyttää ohjelmapäivityksiin, tuotetuen ja mahdollisten muiden palvelujen tarjoamiseen. Lisäksi näitä tietoja voidaan käyttää markkinointi- ja myynninedistämistarkoituksiin ja tutkimus- ja tuotekehitystarkoituksiin. Mikäli ei halua, että näitä tietoja käytetään, tulee lähettää kirjallinen pyyntö asiasta. Ilman lupaa yritys ei saa jakaa asiakkaan antamia henkilötietoja kolmannelle osapuolelle, muualle kuin yrityksen omalle maahantuojalle asiakkaan maassa, mikäli pyynnön toteuttaminen tätä edellyttää. Koska tietosuojalain mukaan virheellisiä tietoja ei saa kerätä, yritykset pyrkivätkin poistamaan epätäydelliset, väärät ja vanhentuneet tiedot. Asiakkaalla on oikeus tarkistaa ja korjata itseään koskevia tietoja ja asiakkaan tuleekin varmistaa, että yhteys- sekä muut tiedot ovat oikein ja ajan tasalla. (Polar Electro 2016)

Kun käyttäjä käy Garmin-sivustolla ja luo tilin sinne, Garmin saattaa kerätä henkilötietoja, kuten käyttäjän nimi-, postiosoite-, puhelinnumero-, sähköpostiosoite- ja maksukortin tiedot. Garmin International Inc. saattaa kerätä ja säilyttää käyttäjän henkilökohtaisia tietoja Yhdysvalloissa eli jos käyttäjä ei asu Yhdysvalloissa, pitää huomioida, että Yhdysvaltain tietojen suojausta ja yksityisyyttä koskevat lait eivät välttämättä ole yhtä kattavia kuin asuinmaan laki. Garmin saattaa käyttää henkilökohtaisia tietoja sisäisiin tilastointi-, markkinointi- tai toimintatarkoituksiinsa, kuten luotaessa myyntiraportteja ja mitattaessa asiakkaiden väestötietoja, kiinnostusta, ostokäyttäytymistä ja muita trendejä. Garminin sivustot saattavat sisältää palveluja, kuten keskustelupalstoja, foorumeita, chat-toimintoja ja blogeja, joissa käyttäjät voivat julkaista tietoja ja materiaaleja. Näillä sivustoilla julkaistut käyttäjien tiedot saattavat muuttua julkisiksi ja saattavat olla sivustojen käyttäjien ja suuren yleisön käytettävissä. Käyttäjien tulee siis harkita tarkasti henkilötietojen tai minkä tahansa tietojen julkaisemista Garminin sivustoissa. Garmin ei vastaa henkilötietojen käytöstä, kun käyttäjä on ilmoittanut niitä vapaaehtoisesti sivustoissaan. (Garmin 2016b.)

Käyttäjän aktivoidessa Fitbit – laitteensa, häneltä kysytään henkilötietoja, kuten pituutta, painoa ja sukupuolta. Laitteet tallentavat tietoja kuten askeleet, painon, unenlaadun (riippuen laitteesta) ja lähettävät nämä tiedot Fitbitille. Kun käyttäjä luo Fitbit-tilin, Fitbit kerää henkilökohtaisia tietoja kuten sähköpostiosoitteen ja syntymäajan. Mikäli käyttäjä käyttää Facebookia tai Google+ tiliä luodakseen Fitbit -tilin, Fitbit kysyy lupaa toisen tilin tietoihin kuten nimeen, profiilikuvaan ja kaverilistaan. Fitbit ei takaa yksityisyysuojan olevan tällä tavalla kirjautuneena yhtä hyvä kuin Fitbitin sivuille suoraan kirjautuessa. Toisen tilin tietojen jakamisen voi aina estää estämällä Fitbitin pääsyn tuolle tilille. Fitbitillä on pääsy puhelimen yhteystietoihin, jotta käyttäjä pystyy tunnistamaan tuttavat, jotka käyttävät Fitbitiä. Fitbit ei kuitenkaan tallenna puhelimen yhteystietoja, vaan ne poistetaan välittömästi, kun niitä on käytetty tähän tarkoitukseen. Mikäli käyttäjä lisää ruokamerkintöjä tai valokuvia, osallistuu keskusteluihin tai lähettää viestejä Fitbit –ystävilleen, nämä tiedot kerätään ja tallennetaan käyttäjän muiden tilitietojen kanssa. (Fitbit 2014.)

7.3.2 Muut kuin henkilötiedot

Polar kerää teknisiä tietoja kuten aktiviteettien jäljittäminen IP-osoitteeseesi tai viimeksi selaamaasi internet-sivustojen avulla. Näitä tietoja käytetään kokonaisuutena ja niiden avulla lasketaan sivujen vierailumääriä, keskimääräistä vierailun pituutta, selailtuja sivuja ja muuta teknistä tietoa. Polar kerää myös tietoja sivulatauksista ja – hauista, mukaan lukien mahdolliset kiinnostuksen kohteet ja demografiset tiedot. Näitä tietoja voidaan luovuttaa kolmansille osapuolille kuitenkin, niin etteivät kenenkään henkilötiedot ole tunnistettavissa (Polar Electro 2016.)

Garminin yksityisyystiedotteen mukaan ”muut tiedot” ovat tietoja, joista ei voi tunnistaa käyttäjän henkilöllisyyttä tai jotka eivät liity suoraan yksittäisiin henkilöihin, kuten selain- ja laitetiedot, sovellusten käyttötiedot, evästeiden, pikselitunnisteiden ja muiden tekniikoiden avulla kerätyt tiedot, väestötiedot ja muut käyttäjän ilmoittamat tiedot sekä kootut tiedot. Ellei sovellettava laki toisin edellytä, Garmin saattaa käyttää ja ilmoittaa muita tietoja mihin tahansa tarkoituksiin. Jos Garminin on kohdeltava muita tietoja henkilötietoina sovellettavan lain mukaan, Garmin käyttää niitä henkilötietoina. Sijaintitiedot kerätään nimettömästi muodossa, josta ei voi tunnistaa käyttäjää. Mikäli käyttäjä antaa suostumuksensa, Garmin saattaa jakaa tai myydä muita tietoja myös kolmansille osapuolille nimettöminä muodossa, josta yksittäistä käyttäjää ei voi tunnistaa. Suoritustietoja, kuten juoksu- ja kävelylenkkejä, askelia ja suoritusaikoja, Garmin ei siirrä eikä myy millekään muulle osapuolelle ilmoittamatta asiasta käyttäjälle ja pyytämättä käyttäjän lupaa. Käyttäjä voi hallita näiden tietojen näkyvyyttä sivustojen ja sovellusten yksityisyysasetuksista. Mainostiedoista Garmin kerää napsautustiheydet ja niihin liittyvien toimintojen (kuten etusetelin tallennus) käyttämistiheydestä. (Garmin 2016b.)

Fitbit kerää myös teknisiä tietoja (lokitietoja), kuten IP-osoitteet selailluilta sivuilta, käyttöjärjestelmätiedot ja mitä selainta on käytetty sekä URL-tietoja. Fitbit käyttää näitä tietoja, jotta käyttäjä saa vain hänen alueelleen oleelliset tiedot ja että käyttäjän sivusto toimii kunnolla. Synkronoidessa laitteen aktiviteetit siirretään Fitbitin palvelimelle. Lisäksi tallennetaan synkronointiaika, laitteen paristotaso ja IP-osoite, jota käytetty synkronoidessa. Fitbit, kuten Garmin ja Polarkin, ei jaa ulkopuolisille tietoja, joista voisi tunnistaa käyttäjän. (Fitbit 2014.)

7.3.3 Evästeet ja muut tekniikat

Kun asiakas käy Polarin nettisivuilla, yritys voi palvelimeltaan lähettää päätelaitteelle evästeitä, joiden avulla kerätään päätelaitettasi koskevia tietoja, jolla yritys voi parantaa sivustojaan. Evästeitä ei talleteta eikä niistä kerätä henkilötietoja, mutta mikäli asiakas ei halua näitä evästeitä, hän voi kieltäytyä niistä. Myös selainohjelmasta voi estää evästeiden latautumista. (Polar Electro 2016.)

Garmin saattaa käyttää evästeitä, pikselitunnisteita, web-bugeja, GIF -tiedostoja tai muita työkaluja sivustoissaan ja sähköpostiviesteissään, joilla he pystyvät seuraamaan sivuston käyttöä ja mainosten tehoa. Lisäksi Garmin käyttää Google Analyticsiä tilastotietojen ja käyttäjien väestötietojen, mielenkiinnon kohteiden ja toiminnan seuraamiseen. Tiedot kerätään nimettömästi tavalla, josta käyttäjää ei voi tunnistaa. Jos käyttäjä ei halua, että tietoja kerätään näillä tekniikoilla, ne voi kieltää automaattisesti useimmissa selaimissa tai niitä voi estää tai sallia halutessaan. Jos käyttäjä lisäksi asuu alueella, jossa edellytetään käyttäjän lupaa evästeiden käyttämiseen Garminin sivustoissa, käyttäjä voi määrittää evästeasetuksensa sivustoissa. Osa evästeistä on kuitenkin pakollisia sivuston keskeisten toimintojen käyttämiseksi, joten niitä ei voi poistaa käytöstä. (Garmin 2016b.)

Fitbit käyttää evästeitä kuten Garmin ja Polarkin. Fitbitin käyttämät evästeet ovat AppNexus, DataXu, DoubleClick ja DoubleClick Floodlight sekä Google Adwords Conversion. Fitbit käyttää Mixpanel Google Analytics ja Optimizely analytics toiminnan ja mielenkiinnon seuraamiseen. Käyttäjä voi estää kaikki nämä tekniikat.

7.3.4 Tietojen säilytysaika

Kaikki kolme yritystä säilyttävät henkilötietoja niin kauan kuin yksityisyystiedotteessa määritetyt tarkoitukset edellyttävät, ellei laki edellytä tai salli sitä pidempää säilytysaikaa. Käytännössä se tarkoittaa sitä, että henkilökohtaiset tiedot säilytetään niin kauan kuin käyttäjä on asiakkaana yrityksessä.

7.3.5 Tietojen luovuttaminen

Garmin saattaa jakaa käyttäjän Garminille toimittamia henkilökohtaisia tietoja tytäryhtiöiden kanssa maailmanlaajuisesti yksityisyystiedotteessa määritettyihin tarkoituksiin. Vuosiraportista voi tarkistaa yritykseen liittyvien toimijoiden luettelo. Toimijoiden on suojattava käyttäjien henkilötiedot yksityisyystiedotteen mukaisesti. Garmin International Inc. Yhdysvalloissa vastaa yhteiskäytössä olevien henkilötietojen hallinnasta. Jos käyttäjä ei asu Yhdysvalloissa, pitää huomioida, että Yhdysvaltain tietojen suojausta tai yksityisyyttä koskevat lait eivät välttämättä ole yhtä kattavia kuin asuinmaan lait. Kolmannen osapuolen palveluntarjoajat saattavat avustaa liiketoiminnassa ja sivustojen toiminnassa tai hallita Garminin puolesta toimintoja, kuten maksukorttien käsittelyä ja tuotteiden toimitusta, joten Garmin saattaa jakaa käyttäjien henkilötietoja, kuten maksukorttitietoja, näiden kolmansien osapuolten kanssa, jotta ne voivat toimittaa näitä palveluja. Garmin saattaa myös luovuttaa käyttäjien henkilötietoja muille, jos heillä on siihen käyttäjän lupa sovellettavan lain muodossa. Fuusiossa, myynnissä tai konkurssissa Garmin saattaa siirtää tietoja tytäryhtiölle tai kolmannelle osapuolelle. (Garmin 2016b).

Fitbitillä ja Polarilla periaate tietojen luovuttamiselle on sama kuin Garminillakin eli ulkopuolisille luovutetaan vain tietoja, joista ei pysty tunnistamaan yksittäistä henkilöä.

7.3.6 Tietojen suojaaminen

Garmin noudattaa PCI-DSS-standardia ja käyttää monenlaisia tekniikoita, kuten UTM (Unified Threat Management) -järjestelmiä ja salausta, jotka turvaavat käyttäjän maksutiedot. Garmin pitää palvelimet aina ajan tasalla suojaus- ja käyttöjärjestelmäpäivityksillä. (Garmin 2016a.)

Polar käyttää kaikkia tarkoituksenmukaisiksi katsomiaan keinoja henkilötietojen suojaamiseksi ja estääkseen oikeudettoman tietoihin käsiksipääsyn ja tietojen sopimattoman käytön. (Polar 2016.)

Fitbit käyttää teknillisiä ja hallinnollisia turvatoimia käyttäjän tietojen suojaamiseen. (Fitbit 2014.)

7.3.7 Palvelimien sijainti

Fitbitin ja Garminin palvelimet sijaitsevat Yhdysvalloissa. Molemmat noudattavat vain Amerikan lakeja, joten yksityisyydensuoja ei välttämättä ole yhtä hyvä kuin Euroopan unionin tarjoama yksityisyydensuoja. Polar noudattaa enintään Suomen lakia (Polar 2016), mutta palvelimen sijaintia ei ole kirjoittajan tiedossa. (Fitbit 2014, Garmin 2016b.)

8 Johtopäätökset

Tutkimuksessa opin, kuinka läheisesti tietoturva liittyy yksityisyydensuojaan, sillä ilman tietoturvaa yksityisyydensuojaakaan ei ole. Tietoturvan pitäminen kunnossa on erittäin tärkeää yksityisyydensuojan kannalta.

Suomen lainsäädännössä erityisesti henkilötietolaissa ja tietoyhteyskuntakaaressa säädetään henkilötietojen käsittelyn edellytyksistä, mutta yksityisyydensuojaa käsitellään myös muissa laissa. Erityislainsäädäntöä sovelletaan ensisijaisesti yleislakiin nähden, paitsi henkilötietolain yleisvelvoitteiden osalta, koska niitä ei erityislainsäädännössä mainita. Työelämän tietosuojalaki vastaa yksityisyyden suojaa koskeviin kysymyksiin työelämän alueella. Laki koskee vain työntekijän ja työnantajan välistä suhdetta. Julkisuuslakia sovelletaan, kun toinen osapuoli on viranomainen. Lisäksi yksityisyydensuojaa käsitellään kansainvälisissä direktiiveissä, jotka pitää vahvista jäsenmaan lainsäädännössä, ja asetuksissa, jotka ovat sellaisenaan voimassa.

EU:n uusi tietosuoja-asetus astuu voimaan vuonna 2018. Sen mukaan rekisterinpitäjällä pitää olla oma tietosuojavastaava. Lisäksi henkilötietojen käsittely uudessa asetuksessa on yhdenmukaistettu EU:n sisällä. Uudistuksen pyrkimyksenä on parantaa rekisteröityjen tietoturvaa ja luottamusta internetiin. Rekisterinpitäjälle **Ota oppaaksi henkilötietolaki!** on hyvä opas siihen, mitä tietoja saa kerätä.

Yrityshaastattelussa kävi ilmi, että laitteiden keräämät tiedot tallentuvat alihankkijoiden palvelimille, mutta palvelinten sijainti ei välttämättä ollut yrityksen tiedossa. Lisäksi tieto siitä, milloin yrityksen keräämät tiedot kuuluvat henkilötietolain piiriin ja rekisteri-ilmoitus tulee täyttää, oli joissakin tapauksissa epäselvää.

Tutkimuksessa selvisi myös, että osa aktiivisuusrannekkeiden valmistajista käyttää amerikkalaisia palvelimia tietojen tallentamiseen ja että he toimivat Yhdysvaltojen lakien mukaan, vaikka he myyvät rannekkeita Euroopassa. Tämän seurauksena yksityisyydensuoja heidän tuotteitaan käyttävillä asiakkailla saattaa olla heikompi kuin Euroopassa yleensä.

Tämän tutkimuksen perusteella kannattaa aina ensimmäisenä tarkistaa yksityisyysasetukset sovelluksesta, ennen kuin alkaa käyttää aktiivisuusranneketta. Ennen aktiivisuusrannekkeen ostoa suositeltavaa olisi myös ottaa selvää, minkä lain alaisuudessa yritys toimii. Kirjautumisessa kannattaa aina rekisteröityä saman yrityksen tunnuksilla eikä käyttää jonkun muun palvelun kuten Facebookin tai Google+ tunnuksia, koska yksityisyydensuoja saattaa olla heikompi asiakkaan käyttäessä niitä.

Aiheena tämä oli haastava, sillä uutisia EU:n tietosuojauudistuksesta, tietojen siirtämisestä EU:n ulkopuolelle ja asioiden internetistä yleisesti tulee viikoittain. Jatkotutkimuksessa voisi selvittää tietoturvaa asioiden internetissä.

Lähteet

Aarnio, R. 9.11.2015. Tietosuojavaltuutettu. Tietosuojavaltuutetun toimisto. Haastattelu. Helsinki.

Cisco. Internet of Things. Luettavissa: http://www.cisco.com/web/solutions/trends/iot/portfolio.html. Luettu: 23.05.2015.

Deutsche Welle. 2015. Internet of things holds promise but sparks privacy. Luettavissa: http://www.dw.com/en/internet-of-things-holds-promise-but-sparks-privacy-concerns/a-15911207. Luettu: 04.10.2015.

EUR-Lex, 7.12.2000. Luettavissa:http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A12012P%2FTXT. Luettu: 8.3.2016.

Euroopan ihmisoikeussopimus 20.5.1999/63

Euroopan neuvosto 2014. Käsikirja Euroopan tietosuojaoikeudesta. Euroopan neuvoston yleissopimus 108, s. 15. Luettavissa: http://www.echr.coe.int/Documents/Handbook_data_protection_FIN.pdf. Luettu 11.05.2016.

Euroopan tuomioistuin, 2014. Lehdistötiedote nro 70/14. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. Luettavissa: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf. Luettu 10.04.2016.

Finlex 2008. I. v. Finland-tapaus – Yksityiselämän suoja – Potilasasiakirjat. Luettavissa: http://www.finlex.fi/fi/oikeus/eurooppa/feit/2008/20083456?search[type]=pika&search[pika]=X%20vastaan%20suomi. Luettu 12.05.2016.

Fitbit 2014. Fitbit Privacy Policy. Luettavissa: https://www.fitbit.com/uk/legal/privacy. Luettu: 4.10.2015.

Garmin 2016a. Garmin ja tietoturva. Luettavissa: https://www.garmin.com/fi-FI/legal/security. Luettu: 12.05.2016.

Garmin 2016b. Yksityisyystiedote. Luettavissa: https://www.garmin.com/fi-FI/legal/privacy-statement. Luettu: 12.05.2016.

Henkilötietolaki 22.4.1999/523

Hill, K. 2011. Fitbit moves quickly after users sex stats exposed. Luettavissa: http://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/#55837aa679e7. Luettu: 15.04.2016.

Ihmisoikeussopimus 20.05.1999/63

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621 (Julkisuuslaki)

Polar Electro, 2016. Käyttöehdot. Luettavissa: http://www.polar.com/fi/kayttoehdot#acceptance. Luettu:8.3.2016.

Rouse, M. 2014. IoT Agenda. Internet of Things. Luettavissa: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. Luettu: 28.02.2016.

Sairanen M. 2016. Turun Sanomat. Tietosuojavaltuutettu: Uudistus helpottaa kilpailuttamista. Luettavissa: http://www.ts.fi/uutiset/kotimaa/854597/Tietosuojavaltuutettu+Uudistus+helpottaa+kilpailuttamista. Luettu: 7.4.2016.

Suomisanakirja, 2015. Demografinen. Luettavissa: http://www.suomisanakirja.fi/demografinen. Luettu 16.04.2016.

Talouselämä 2009. Ubiikkiyhteiskunta hiipii huomaamatta. Luettavissa: http://www.talouselama.fi/uutiset/ubiikkiyhteiskunta-hiipii-huomaamatta-3405194. Luettu 16.04.2016.

Tietosuojavaltuutetun toimisto 2006. Toimintakertomus. Luettavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/tehtavat/toimintakertomus/4JfSGuQyN/2006.pdf. Luettu: 15.11.2015.

Tietosuojavaltuutetun toimisto 2013a. Henkilötietolain taustaa. Luettavissa: http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/henkilotietolaintaustaa.html. Luettu: 6.5.2016.

Tietosuojavaltuutetun toimisto 2013b. Henkilötietolaki. Luettavissa: http://www.tietosuoja.fi/fi/index/lait/Henkilotietolaki.html. Luettu: 15.11.2015

Tietosuojavaltuutetun toimisto 2013c. Kielto-oikeus. Luettavissa: http://www.tietosuoja.fi/fi/index/rekisteroidylle/rekisteroidynoikeudet/kielto-oikeus.html. Luettu: 12.05.2016.

Tietosuojavaltuutetun toimisto 2014a. Erityislainsäädäntö. Luettavissa: http://www.tietosuoja.fi/fi/index/lait/erityislainsaadanto.html. Luettu: 05.03.2016

Tietosuojavaltuutetun toimisto 2014b. Julkisuuslaki. Luettavissa: http://www.tietosuoja.fi/fi/index/lait/julkisuuslaki.html. Luettu 6.5.2016.

Tietosuojavaltuutetun toimisto 2014c. Sähköisen viestinnän tietosuojalaki. Luettavissa: http://www.tietosuoja.fi/fi/index/lait/sahkoisenviestinnantietosuojalaki.html. Luettu: 5.4.2016.

Tietosuojavaltuutetun toimisto 2014d. Tietoyhteiskuntakaari. Luettavissa: http://www.tietosuoja.fi/fi/index/lait/sahkoisenviestinnantietosuojalaki.html. Luettu 16.4.2016.

Tietosuojavaltuutetun toimisto 2014e. Työelämän tietosuojalaki. Luettavissa: http://www.tietosuoja.fi/fi/index/lait/tyoelamantietosuojalaki.html. Luettu 10.05.2016.

Tietosuojavaltuutetun toimisto 2014f. Ilmoitusvelvollisuus. Luettavissa: http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/ilmoitusvelvollisuus.html Luettu 10.03.2016. Luettu 11.05.2016.

Tietosuojavaltuutetun toimisto 2014g. Rekisteröidyn oikeudet. Luettavissa: http://www.tietosuoja.fi/fi/index/rekisteroidylle/rekisteroidynoikeudet.html. Luettu: 12.05.2016.

Tietosuojavaltuutetun toimisto 2015a. Ota oppaaksi henkilötietolaki. Luettavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfq8WnQ7/Ota_oppaaksi_henkilotietolaki.pdf. Luettu: 15.11.2015.

Tietosuojavaltuutetun toimisto 2015b. Safe Harbor –tiedote5. Luettavissa: http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2015/10/safeharbor-tiedote5.html. Luettu: 24.02.2015.

Tietosuojavaltuutetun toimisto 2015c. EU:n tietosuojauudistus. Luettavissa: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html. Luettu: 1.3.2016.

Tietosuojavaltuutetun toimisto 2015d. Kansainväliset normit ja ohjeet. Luettavissa: http://www.tietosuoja.fi/fi/index/lait/kansainvalisetnormitjaohjeet.html. Luettu: 9.5.2016

Tietosuojavaltuutetun toimisto 2015e. Lait. Luettavissa: http://www.tietosuoja.fi/fi/index/lait.html. Luettu: 10.05.2016.

Tietosuojavaltuutetun toimisto 2015f. Sähköisen viestinnän tietosuojalaki. Luettavissa: http://www.tietosuoja.fi/fi/index/lait/sahkoisenviestinnantietosuojalaki.html. Luettu 09.05.2016.

Tietosuojavaltuutetun toimisto 2016. Safe Harbor –tiedote 8 – Privacy Shield . Luettavissa:http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2016/03/safeharbor-tiedote8.html. Luettu 10.05.2016.

Tivi 2016. Älysänky tarkkailee vuorokauden ympäri ja antaa elintapavinkkejä. Luettavissa: http://www.tivi.fi/Kaikki_uutiset/alysanky-tarkkailee vuorokauden-ympari-ja-antaa-elintapavinkkeja-6244650. Luettu: 2.5.2016.

Työ- ja elinkeinoministeriö 2016. Yksityisyyden suoja työelämässä ja lasten kanssa työskentely. Työelämän tietosuoja. Luettavissa: http://www.tem.fi/?s=2313. Luettu: 9.5.2016.

Viestintävirasto 2014. Yksityisyydensuoja internetpalveluiden sopimuksissa. Luettavissa:https://www.viestintavirasto.fi/attachments/tietoturva/Sopimukset_ja_yksityisyyden_suoja_20141028.pdf. Luettu 1.10.2015.

Viestintävirasto 2015a. Evästeet. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/palveluidenturvallinenkaytto/evasteet.html. Luettu 10.05.2016.

Viestintävirasto 2015b. Yksityisyydensuoja. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/05/ttn20150507 1519.html. Luettu 10.4.2015.

Rouse M, 2009. Web-bug. Luettavissa: http://searchsoa.techtarget.com/definition/Web-bug. Luettu 13.05.2016.

Yritys X, 7.1.2016. Haastattelu. Helsinki.

Liite 1. Kysymykset tietosuojavaltuutetulle Reijo Aarniolle

Mitä kaikkea pitää ottaa huomioon esineiden internetissä (IoT) yksityisyydensuojan kannalta?

Mitä tietoja ei saa/saa kerätä?

Mitä haasteita IoT on tuonut tullessaan?

Onko ollut jo selvitettäviä tapauksia koskien IoTia? Millaisia?

Kun jakaa dataa kolmannelle osapuolelle, mitä pitää ottaa huomioon?

Euroopan tasolla henkilötietojen suojana on kaksi direktiiviä: "Data Protection Directive" ja "Directive on privacy and electronic communications"

Suomessa pitää ottaa huomioon henkilötietolaki ja tietoyhteiskuntakaari..
Onko muita lakeja, joita pitäisi ottaa huomioon koskien asioiden internetiä?

Mitkä lait ovat vahvempia: EU:n lait vai Suomen?

Minkä maan lait pätevät, jos yritys sijaitsee USA:ssa? Voiko USA:ssa oleva yritys vain "ohittaa" Suomen ja EU:n lait
jollain tavalla?

Nyt kun Safe Harborin -sopimuksen nojalla ei saa siirtää tietoja EU:sta USA:han, niin mitä vaikeuksia tämä aiheuttaa?

Jos loppuasiakas hyväksyy yrityksen ehdot, onko hänellä enää mitään oikeuksia?

Kuinka kauan tietoja voidaan säilyttää?

Liite 2. Kysymykset yritykselle

1) Minkälaista IoT -toimintaa teillä on ja mitä asiakkaan tietoja kerätään?

2) Missä tietoja säilytetään? Oletteko tätä varten hankkineet palveluja ulkopuolisilta?

3) Kuinka kauan tietoja säilytetään?

4) Mihin tarkoitukseen tietoja käytetään?

5) Jaetaanko tietoja kolmannelle osapuolelle ja jos kyllä, minkälaista tietoa jaatte?

6) Miten turvaatte säilyttämänne tiedot?

7) Mitä eri lakeja teidän täytyy ottaa huomioon, kun keräätte tietoja, mitä erityissäännöksiä otatte huomioon?