OULUN SEUDUN
AMMATTIKORKEAKOULU

Riikka Junttila

Lain asettamat vaatimukset henkilörekistereille ohjelmistoprojektissa

OULUN SEUDUN
AMMATTIKORKEAKOULU

Lain asettamat vaatimukset henkilörekistereille ohjelmistoprojektissa

Riikka Junttila
Opinnäytetyö
Kevät 2013
Liiketalouden ko
Oulun seudun ammattikorkeakoulu

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Liiketalouden koulutusohjelma, oikeuden- ja hallinnon suuntautumisvaihtoehto

Tekijä: Riikka Junttila
Opinnäytetyön nimi: Lain asettamat vaatimukset henkilörekistereille ohjelmistoprojektissa
Työn ohjaaja: Katja Sankala
Työn valmistumislukukausi ja -vuosi: Kevät 2013 Sivumäärä: 42+9 liitesivua

Henkilötiedot ovat joukko tietoja, joiden avulla ihminen voidaan yksilöidä. Useamman ihmisen tietojen ollessa samassa tietokannassa muodostuu henkilörekisteri. Näitä rekistereitä säädellään lainsäädännöllä. Lainsäädännön tavoitteena on, että henkilötietoja ei voi kerätä ilman perustetta.

Opinnäytetyössä käsitellään henkilörekistereihin liittyvää lainsäädäntöä. Opinnäytetyö on tehty toimeksiantona. Toimeksiantajana on talkootyönä toimivan ohjelmistoprojektin taustaorganisaatio. Ohjelmistoprojektin tarkoituksena on rakentaa uusia tietojärjestelmiä toimeksiantajalle, ja yhtenä osana projektissa ovat henkilörekisterit. Ohjelmistoprojektissa on tarkoitus rakentaa yksi laajempi henkilörekisteri. Koska toimeksiantaja on pieni organisaatio, ei toimihenkilöillä usein ole tarvittavaa lainopillista tietämystä toimiakseen oikealla tavalla. Tiedon hankkiminen ja ajan tasalla pitäminen on aikaa vievää ja asiaan perehtymättömälle vaikeaa.

Opinnäytetyön tarkoituksena on tutkia, miten lainsäädännöllä ohjataan henkilörekistereitä. Työn tavoitteena on laatia ohjeistus henkilörekistereiden lain asettamista vaatimuksista rekistereiden suunnittelussa, ylläpidossa ja hävittämisessä eli koko henkilörekisterien elinkaaren ajan. Opinnäytetyössä pyritään löytämään vastauksia kysymyksiin, mitä oikeuksia on rekisteröidyllä, mitä velvollisuuksia on rekisterinpitäjällä ja miten henkilötietoja tulee käsitellä.

Opinnäytetyö on toiminnallinen ja tutkimusmenetelmänä on lainoppi. Ensisijaisesti lähteenä on käytetty voimassaolevaa lainsäädäntöä ja hallituksen esityksiä. Lainkäytön havainnollistamiseksi on työssä esitelty oikeuden ratkaisuja sekä tietosuojavaltuutetun kannanottoja. Lisäksi lähteinä on käytetty oikeuskirjallisuutta sekä viranomaisen antamaa ohjeistusta. Käytännön näkökulmaa työhön on tuotu tarkastelemalla toimeksiantajan rekistereitä ja hyödyntämällä toimeksiantajan työntekijöiden osaamista. Opinnäytetyön tuloksena syntyi Ohjeistus henkilörekistereiden suunnittelusta, ylläpidosta ja hävittämisestä.

Tutkimuksen johtopäätöksenä voidaan todeta, että henkilörekistereitä ohjaa ensisijaisesti henkilötietolaki, mutta rekisteristä riippuen myös muu lainsäädäntö ja ohjeistus. Rekisteröidyllä on paljon oikeuksia, jotka on otettava huomioon henkilörekisterin koko elinkaaren ajan. Henkilörekistereiden käyttötarkoitukseen on syytä kiinnittää huomiota, koska käyttötarkoituksella määrätään koko henkilörekistereiden käyttö. Rekistereille on syytä luoda selkeä ohjeistus sisäiseen käyttöön, jotta jokainen tietää henkilörekistereiden merkityksen ja käytön. Henkilörekistereiden käyttöoikeuksia on syytä miettiä tarkoin, turhia käyttöoikeuksia on syytä välttää. Tietoturvakysymykset ovat sitä tärkeämpiä, mitä suurempia rekisterit ovat ja mitä enemmän henkilötietoja kerätään internet-palveluiden kautta.

Asiasanat: henkilötieto, henkilörekisteri, henkilötietolaki, rekisteriseloste

ABSTRACT

Oulu University of Applied Sciences
School of Business and Information Management, Option of Law and Administration

Author: Riikka Junttila
Title of thesis: Demands to the person registers set by the law in a software project
Supervisor: Katja Sankala
Term and year when the thesis was submitted: Spring 2013 Number of pages: 42+9 enc.

Personal data is a set of information that can help a person to be identified. Date of several forms in the same database prisons of a person register. Law shall regulate these files. Aim of the legislation is that personal data cannot be collected without justification.

The thesis deals with Personal Data Act. This thesis was written as an assignment. The principal is a host organization doing software project with volunteers. The software project is to build new systems for principal and a part of the project is the person registers. The software project is to create the system for one larger person register. Since the client is a small organization, clerical personnel often do not have the necessary legal dogmatic in order to act correctly. To collect information and keeping it up to date is a time-consuming and difficult for the unfamiliar.

Purpose of this thesis is to investigate the Personal Data Act and the aim is to draw up guidelines what the law requires from registers in definition, maintenance and destruction phase covering the whole life cycle. The thesis seeks the answers what are rights of a registered person and what obligations are imposed for registrar and how personal data the shall processed.

This thesis is functional and the method is jurisprudence. The existing legislation and the government's proposals are used as the primary source. The legal decision and statements from Data Protection Ombudsman are presented to illustrate the application of the law. In addition, the legal literature and the guidance provided by the authorities are used sources as well. Studying the principal's registers and utilizing the principal's knowledge bring the practical aspect of the thesis. The thesis result is a collection of guidelines how to define, maintain and destroy the person registers.

As a conclusion of the thesis can be said that person registers are primarily controlled by Personal Data Act, but depending on the register by other legislation and guidelines also. The registers have rights, which have to be taken into account during the whole life cycle of the person register. Attention must be paid to the purpose of use of person registers because with the purpose of use the use of the whole person registers is determined. For internal use, on shall create a clear guidance such that everyone knows the significance and the usage of the register. The user rights of the person registers shall be considered thoroughly, and unnecessary user rights shall be avoided. The larger the registers are and the more personal information is gathered the Internet services, the more important the issues selected to information security are.

Index terms: personal data, person register, law of personal date, file description

SISÄLLYS

LYHENTEET

HAO	Hallinto-oikeus
HE	Hallituksen esitys
HTL	Henkilötietolaki 22.9.1999/523
KP-sopimus	Kansalaisoikeuksia ja poliittisia oikeuksia koskeva yleissopimus
PerL	Suomen perustuslaki 11.6.1999/731
SopS	Sopimussarja
SVTSL	Sähköisen viestinnän tietosuojalaki 16.6.2004/516
TSS-sopimus	Taloudellisia, sosiaalisia ja sivistyksellisiä oikeuksia koskeva yleissopimus
YK	Yhdistyneet kansakunnat

1 JOHDANTO

Jokaisesta meistä on tiedot yhdessä tai useammassa henkilörekisterissä. Emme edes usein tule ajatelleeksi, mihin tietomme annamme tai mitä oikeuksia meillä on näihin tietoihin ja rekistereihin. Meistä kuitenkin yhä useampi on tietoisempi meille kuuluvista oikeuksista ja tulevaisuudessa varmasti vielä useampi, toivottavasti. Rekisterinpitäjät ovat myös tietoisempia heitä koskevista velvollisuuksista henkilötietoja kohtaan. Maailmamme muuttuminen yhä enemmän tietoteknilliseksi luo haasteita siihen, miten tietomme pysyvät vain niiden käytössä, joiden käyttöön ne on annettu. Henkilötiedot ovat nousset esille viime aikoina yhä useammin uutisotsikoissa. Näen taustalla ihmisten tietoisuuden omista oikeuksistaan ja tiedon nopean leviämisen internetin välityksellä. Tietoturvakysymyksiä en voi painottaa liikaa.

Tämän opinnäytetyön tarkoituksena on tutkia lain asettamia vaatimuksia henkilörekistereissä ohjelmistoprojektissa. Toimeksiantaja on projektiluonteisesti toimiva organisaatio, joka pysyy tässä opinnäytetyössä anonyyminä. Ohjelmistoprojekti toimii talkoovoimin, ja sen tehtävänä on rakentaa uusia tietoteknillisiä palveluja taustaorganisaatiolle. Tässä työssä toimeksiantajana toimii ohjelmistoprojektin taustaorganisaatio. Toimeksiantajalla on useita henkilörekistereitä, joita ollaan tarkastelemassa, muuttamassa, hävittämässä ja yhdistämässä. Toimeksiantaja halusi tietää, mitä vaatimuksia laki asettaa henkilörekistereille. Opinnäytetyön toimeksiantaja on siis rekisterinpitäjä.

Opinnäytetyön aihe muotoutui toimeksiantajan tarpeista ja ohjaajan kanssa käydyn keskustelun pohjalta. Tavoitteena oli löytää vastaukset seuraaviin tutkimuskysymyksiin: Millaisia oikeuksia laki säätää henkilörekisteriin rekisteröidylle? Mitä velvollisuuksia henkilörekisterin pitäjällä on lain mukaan? Miten henkilötietoja on lain mukaan käsiteltävä? Tavoitteena oli luoda ohjeistus, jonka avulla toimeksiantajan on helpompi suunnitella, ylläpitää ja tehdä henkilörekisterinsä. Tämän vuoksi opinnäytetyö on toiminnallinen työ, jonka tuotoksena on syntynyt ohjeistus. Ohjeistuksen avulla toimeksiantaja pystyy kehittämään henkilötietojen käsittelyä turvallisemmaksi ja luotettavammaksi. Opinnäytetyössä ei käsitellä kuitenkaan erityislakien, kuten arkistolain, vaikutusta henkilörekistereiden käsittelyyn.

Opinnäytetyön tutkimusmenetelmä on lainoppi, jonka ensisijaisena tietoperustana on henkilötietolaki (22.9.1999/523). Lähteenä on käytetty myös hallituksen esitystä sekä tietosuojavaltuutetun

antamia ohjeistuksia ja alan kirjallisuutta. Lähteitä on pyritty käyttämään monipuolisesti. Ohjeistuksen tekemiseen saatiin tukea toimeksiantajalta, keskustelemalla työntekijöiden kanssa, tutustumalla rekistereihin ja työympäristöön. Oma työkokemus yrityksissä, joissa henkilötietoja käsitellään päivittäin, on auttanut ymmärtämään henkilötietojen käsittelyn merkitystä, syvyyttä ja monipuolisuutta.

Keskeisimpinä käsitteinä tässä opinnäytetyössä ovat henkilötieto, henkilörekisteri, rekisteröity ja rekisterinpitäjä. Nämä käsitteet on avattu tarkemmin luvussa kolme. Toisessa luvussa käsitellään yksityisyyttä ja sitä, mihin yksityisyys perustuu. Tämä osio antaa taustaa sille, millaiset oikeudet meillä jokaisella on omiin tietoihimme sekä siihen, miten tätä oikeutta suojellaan lainsäädännöllä. Kolmas luku käsittelee rekisteröidyn oikeuksia ja neljäs luku rekisterinpitäjän velvollisuuksia. Etenkin tietotekniikan kehittymisen myötä tärkeimpiä kysymyksiä ovat tietosuoja- ja tietoturvakysymykset. Näihin kysymyksiin kiinnitetään huomiota viidennessä luvussa.

2 YKSITYISYYS HENKILÖREKISTEREISSÄ

Henkilörekisterien ja sähköisen liiketoiminnan suunnittelussa ja tietojärjestelmien käytössä on kunnioitettava yksilöiden perusoikeuksia ja vapauksia. Yksityisyyden suoja on Suomessa perusoikeus. Suomen perustuslaissa taataan jokaiselle yksityiselämän, kunnian ja kotirauhan turva (Suomen perustuslaki 11.6.1999/731 2:10.1 §). Tässä samassa mainitaan myös, että henkilötietojen suojasta säädetään tarkemmin lailla, eli Suomen perustuslaki sisältää näin ollen lainsäädäntötoimeksiannon, johon henkilötietolaki ja muu lainsäädäntö henkilötietojen suojaamisesta perustuu (PerL 2:10.1 §). Yksityisyyttä suojataan myös ihmisoikeutena sekä Euroopan unionin antamin direktiivien ja perusoikeuskirjalla (Vanto 2011, 18).

2.1 Rekisteröidyn yksityisyys

Yksityisyyden määrittely on hyvin vaikeaa. Asiaan liittyy monia näkökulmia, ristiriitaisia tavoitteita ja kansallisia arvoja. Yksityisyyden käsite ei ole maailmanlaajuinen, vaan se on sidoksissa siihen kulttuuriin ja yhteiskuntaan, jossa kukin yksilö elää (Järvinen 2010, 14). Yksityisyyden määrittelyn vaikeus ja suhteellisuus johtuneekin siitä, että yksityisyys on jokaisen henkilökohtainen kokemus, johon vaikuttavat ainakin kyseisen henkilön tiedot, kokemustausta, ympäristö ja elämäntilanne, jotka eivät voi olla kenelläkään täysin samoja. (Salminen 2009, 16.)

Lähtökohtana henkilötietojen käsittelyssä voidaan pitää periaatetta, että henkilö itse on tietolähteenä antamilleen tiedoille. Toisin sanoen henkilö itse voi paljastaa itsestään tietoja sivulliselle ja julkisuuteen. Viranomainen ei saa luovuttaa näitä tietoja muille. Toisaalta kuitenkin se, joka tietää toisen yksityiselämästä muuten kuin viranomaistoiminnan kautta, saa kertoa muille nämä tiedot. (Pesonen 2008, 46.) Voidaankin sanoa, että yksityisyyden suoja muodostuu yksilön oikeuksista tietää ja vaikuttaa omien henkilötietojen käsittelyyn sekä rekisterinpitäjän henkilötietojen käsittelyyn liittyvistä velvollisuuksista. Lainsäädännöllä ei suojata tietoja, vaan yksilöä ja hänen oikeuttaan omiin tietoihin. (Salminen 2009, 15.)

Tämä yksilön oikeus omiin henkilötietoihinsa on ihmisen perusoikeus. Näin ollen yksilö itse voi näihin oikeuksiin perustuen käyttää omiin tietoihinsa liittyvää niin sanottua tiedollista itsemäärää-

misoikeuttaan suhteessaan rekisterinpitäjään, joka hänen tietojaan käsittelee (Salminen 2009, 16.)

2.2 Henkilötietolain taustaa

Yksityisyyden suojan lähtökohtana voidaan pitää YK:n ihmisoikeussopimuksia. Suomi on liittynyt useisiin kansainvälisiin ihmisoikeussopimuksiin. Merkittävimpiä näistä sopimuksista ovat YK:ssa sovitut yleismaailmalliset ihmisoikeussopimukset kuten kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus vuodelta 1966 sekä taloudellisia, sosiaalisia ja sivistyksellisiä oikeuksia koskeva kansainvälinen yleissopimus, TSS-sopimus, vuodelta 1966. (Salminen 2008, 66.) Suomalaisten kannalta tärkeitä ihmisoikeussopimuksia on hyväksynyt myös Euroopan neuvosto. Näistä tärkeimpiä ovat Euroopan ihmisoikeussopimus vuodelta 1953 sekä Euroopan neuvoston perusoikeuskirja (30.3.2010 EUVL C 83). (Salminen 2008, 68.) Kansainväliset sopimukset luovat pohjan oikeudelle yksityisyyteen.

Kansainväliset yleissopimukset kansalaisoikeuksista ja poliittisista oikeuksista sekä taloudellisista, sosiaalisista ja sivistyksellisistä oikeuksista luovat valtioille pohjan yksilön vapauteen ja oikeuksiin omassa valtiossaan. KP-sopimusta luonnehditaan vapauspainotteiseksi ihmisoikeussopimukseksi, sillä tämä sopimus suojaa ensimmäisen ja vanhimman sukupolven oikeuksia, kuten oikeutta elämään ja sananvapautta. KP-sopimus velvoittaa valtiota olemaan rajoittamatta yksilön vapautta. Näitä ihmisoikeussopimuksia valvoo YK:n ihmisoikeuskomitea (Yhdistyneiden kansakuntien peruskirja, 16.12.1966, SopS 8, 2 artikla; Salminen 2008, 68). TSS-sopimus puolestaan on oikeuspainotteinen, eli se velvoittaa valtioita toimimaan niin, että tietyt oikeudet toteutuvat, kuten oikeus sosiaaliturvaan ja riittävään elintasoon. TSS-sopimus ei niin ikään velvoita kansalaista itseään. (Salminen 2008, 70.)

EU on tehnyt ratkaisevan askeleen sopimalla Euroopan unionin perusoikeuskirjasta. Euroopan unionin perusoikeuskirjan 8 artiklassa taataan jokaiselle oikeus henkilötietojensa suojaan. Henkilötietojen käsittelyn on perusoikeuskirjan mukaan oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn perusteen nojalla. Jokaisella on myös oikeus tutustua hänestä kerättyihin tietoihin ja saada ne tarvittaessa oikaistua. (Euroopan unionin perusoikeuskirja, 30.3.2010 EUVL C 83, 30.3.2010. 8.)

Suomessa yksityisyyden suoja lähtee Suomen perustuslain 2. luvun 10. § mukaan siitä, että jokaisen yksityiselämä, kunnia ja kotirauha on turvattava. Lisäksi laissa säädetään, että ihmiset ovat yhdenvertaisia lain edessä. Tällä taataan jokaiselle perussuoja, ja samalla toimeksianto säätää tarkemmin henkilötiedoista. (PerL 2:10 § ja 2:6 §.)

Tärkein tietosuojaa ja yksityisyyttä koskeva laki on Suomen lainsäädännössä yleislakina sovellettava henkilötietolaki. Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä (HTL 1:1 §). On kuitenkin huomioitava, että globalisoituminen ja teknologian kehitys ovat mullistaneet henkilötietojen käsittelyä ja tapaa kerätä tietoja. Euroopan komissiossa onkin menneillään tietosuojadirektiivin uudistaminen tasolle, jossa yksilön oikeudet voidaan taata myös tulevaisuudessa (Euroopan komissio, hakupäivä 20.2.2013).

3 REKISTERÖIDYN OIKEUDET

Henkilötietojen käsittelyä, tallentamista, käyttämistä ja siirtämistä erilaisissa rekistereissä on tarkoin säädelty laissa. Lähtökohtana on, että yksilöllä itsellään on päätösvalta siihen, miten häntä koskevia tietoja saa käyttää, ellei lainsäädännöllä ole toisin määrätty. (HE 96/1998, 33.) Lain tarkoituksena on suojata yksityiselämää ja yksityisyyden suojaa henkilötietojen käsittelyssä sekä auttaa hyvän tietojenkäsittelytavan kehittymistä ja noudattamista (Henkilötietolaki 1:1 §).

Henkilötietolakia sovelletaan silloin, jos muualla laissa ei toisin säädetä, eli henkilötietolaki on yleislakina henkilötietojen käsittelylle. Henkilötietolakia sovelletaan aina, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. Sillä ei ole merkitystä käsitelläänkö henkilötietoja ATK-käsittelyssä vai manuaalisesti (HTL 2:1-2 §). Hallituksen esityksessä on tarkennettu, että kaikki henkilötietoja sisältävä tietojoukko, jota käsitellään automaattisen tietojenkäsittelyn avulla, on aina pidettävä henkilörekisterinä (HE 96/1998, 33–34).

3.1 Määritelmät

Henkilötiedolla tarkoitetaan kaikkia luonnollisesta henkilöstä tai hänen ominaisuuksistaan tai elinolosuhteistaan tehtyjä merkintöjä, jotka voidaan tunnistaa häntä, hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi (HTL 1:3 § 1 k.). Tämä määritelmä on hyvin laaja ja niin se pitäisikin ymmärtää. Voidaankin ajatella, että henkilötieto yksinkertaisimmillaan on sormenjälki tai henkilötunnus, nimi tai puhelinnumero, sillä ne voidaan tunnistaa yhtä luonnollista henkilöä koskevaksi. Toinen tekijä arvioitaessa sitä, onko kyseessä henkilötietolaissa tarkoitettu henkilötieto, on se, onko henkilö tunnistettavissa tiedon perusteella. (Vanto 2011, 22.) Henkilötiedoiksi luetaan siis kaikki tiedot, joista henkilö voidaan tunnistaa epäsuorasti johonkin toiseen tietoon yhdistämällä (Järvinen 2010, 255).

Henkilötietojen käsittelyllä tarkoitetaan henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietotoihin kohdistuvia toimenpiteitä (HTL 1:3.1§ 2 k.). Käytännössä mikä tahansa henkilötietoihin kohdistuva toimenpide on henkilötietolain tarkoittamaa käsittelyä ja silloin on noudatettava henkilötietolakia (Vanto 2011, 28).

Henkilörekisteri on tietojoukko, joka muodostuu käyttötarkoituksensa vuoksi yhteenkuuluvista henkilötiedoista, joita käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla tai joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla. Tiettyä henkilöä koskevat tiedot voidaan näin ollen löytää helposti ja ilman kohtuuttomia kustannuksia. (HTL 1:3 § 3 k.) Keskeistä henkilötietorekisteri-käsitteen määrittämiseksi on looginen rekisterikäsite. Tämä merkitsee sitä, että samaan henkilörekisteriin luetaan kuuluvaksi kaikki tiedot, joita käytetään samassa käyttöyhteydessä riippumatta siitä, miten ja mihin ne on tallennettu. Kun tietoja käsitellään ja niistä muodostuu lyhytaikaisia tiedostoja ja tallenteita, niitä ei pidetä eri henkilörekistereinä silloin, kun ne ovat rekisterinpitäjän hallussa ja niitä käytetään henkilörekisterissä määritellyn käsittelyn tarkoituksen mukaisesti. (HE 96/1998, 34.) Tietosuojalautakunnan tekemän päätökseen mukaan pelkästään se, että jokin henkilötietoja sisältävä luettelo laaditaan pelkästään tekstinkäsittelyn avulla, ei tee siitä laissa tarkoitettua automaattisen tietojenkäsittelyn avulla ylläpidettävää henkilörekisteriä. Oleellista on, onko näiden henkilötietojen avulla ihminen tunnistettavissa näistä tiedoista ja mihin tietoja käytetään. (Tietosuojalautakunnan päätös 7/26.3.1990.)

Rekisterinpitäjä on henkilö, yhteisö tai yritys, jonka käyttöön rekisteri on perustettu ja joka vastaa käytön lainmukaisuudesta (HTL 1:3 § 4 k.). Vastuullinen taho yrityksen henkilörekisterissä on yritys itse, viime kädessä kuitenkin sen toimiva johto. Käytännön työn voi kuitenkin tehdä nimetty henkilö, jonka vastuulle rekisterin käyttö on annettu (Järvinen 2010, 256). Keskeistä rekisterinpitäjä-käsitteen kannalta on oikeus määrätä henkilörekisterin käytöstä. Rekisterinpitäjä voi määrätä, mihin henkilötietoja käytetään henkilötietolain sallimissa rajoissa. (Vanto 2011, 31.)

Rekisteröity on henkilö, jonka tietoja rekisteri sisältää (HTL 1:3 § 5 k.). Rekisteröidyllä on aina tiettyjä oikeuksia hänestä oleviin tietoihin, koska hänen tietonsa ovat tallennuksen kohteena (Järvinen 2010, 256).

Sivullinen on jokin muu henkilö, yhteisö tai yritys kuin rekisterinpitäjä, rekisteröity, henkilötietojen käsittelijä tai henkilötietoja rekisterinpitäjän lukuun tekevä henkilö (HTL 1:3 § 6 k.). Sivullinen voi olla esimerkiksi työnantajan lukuun työntekijöiden henkilötietoja käsittelevä palveluntarjoaja kuten palkkatoimisto. Tällöin rekisterinpitäjä on antanut esimerkiksi omien työntekijöiden henkilötiedot tilitoimistolle palkanmaksua varten. (Vanto 2011, 32.)

3.2 Informointi tietojen käsittelystä

Rekisterinpitäjän on huolehdittava henkilötietoja kerätessään, että rekisteröity voi saada tiedon rekisterinpitäjästä ja tarvittaessa tämän edustajasta. Rekisteröidyn täytyy saada pyydettäessä tieto henkilötietojen käsittelyn tarkoituksesta sekä siitä, mihin tietoja säännönmukaisesti luovutetaan. Rekisteröidyllä on oikeus saada ne tiedot, jotka ovat tarpeen rekisteröidyn oikeuksien käyttämiseksi asianomaisessa henkilötietojensa käsittelyssä. Nämä tiedot on annettava henkilötietoja kerätessä ja talletettaessa tai jos tiedot hankitaan muualta kuin rekisteröidyltä itseltään ja tietoja on tarkoitus luovuttaa muualle. (HTL 6:24.1 §.) Rekisterinpitäjän informointivelvollisuudella pyritään turvaamaan rekisteröidyn tietoisuus itseään koskevien henkilötietojen käsittelystä. Näin rekisteröity voi parantaa oikeuksiaan henkilötietojen käsittelyssä sekä arvioida henkilötietojen käsittelyn laillisuutta ja asianmukaisuutta. (HE 96/1998, 59.)

Tiedonantovelvollisuudesta voidaan poiketa, jos rekisteröity on saanut jo nämä tiedot. Tiedonantovelvollisuudesta voidaan poiketa myös, mikäli se on välttämätöntä valtion turvallisuuden, puolustuksen tai yleisen järjestyksen ja turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi taikka verotukseen tai julkiseen talouteen liittyvän valvontatehtävän vuoksi. Tiedonantovelvollisuudesta voidaan poiketa lisäksi, jos tietoja kerätään muualta kuin rekisteröidyltä itseltään tai jos tiedon antaminen rekisteröidylle on mahdotonta tai vaatii kohtuutonta vaivaa. Tiedonantovelvollisuudesta voidaan poiketa, jos tiedonantaminen aiheuttaa rekisteröidylle tai tietojenkäsittelyn tarkoitukselle mittavaa vahinkoa tai haittaa eikä talletettavia tietoja käytetä rekisteröityä koskevan päätöksentekoon. Jos tietojen keräämisestä, tallettamisesta tai luovuttamisesta on nimenomaisesti säädetty toisin, voidaan myös poiketa tiedonantovelvollisuudesta. (HTL 6:24.2 §.)

Rekisteröidyn ilmoittaessa tietoja verkon kautta hänellä on informointivelvoitteen mukaan oikeus saada lain edellyttämä informointi rekisterinpitäjän verkkosivuilta jo ennen tietojen antamista. Tästä on hyvä ja tarkoituksenmukaista sisällyttää tieto rekisteriselosteeseen, jolloin asiakirja nimetään tietosuojaselosteeksi. Tietosuojaseloste olisi hyvä löytyä internetistä. (Tietosuojavaltuutettu c, hakupäivä 5.12.2012.) Tietosuojaselosteessa olisi hyvä ilmoittaa rekisteröidylle informaatiovelvoitteen täyttämiseksi vaaditut tiedot. Rekisteriseloste ja tietosuojaseloste eroavat toisistaan niin, että rekisteriseloste on oltava kaikkien saatavilla, kun taas tietosuojaselosteen vaatimuksena on, että rekisteröidylle informoidaan henkilökohtaisesti. (Salminen 2007, 39.) Mikäli internetpalvelussa käytetään evästeitä, on siitä informoitava verkkopalvelun yhteydessä. Laissa on myös poikkeus evästeiden käytön informoinnille. Kyse on poikkeustapauksista, kun evästeiden ainoana

käyttötarkoituksena on teknisesti helpottaa palvelun käyttöä tai jos käyttäjä on nimenomaan pyytänyt evästeiden käyttöön perustuvaa palvelua. (Sähköisen viestinnän tietosuojalaki 516/2004 2:7 §.) Tämä voidaan toteuttaa liittämällä tietosuojaselosteeseen oma evästeiden käyttöä koskeva osuus (Tietosuojavaltuutettu c, hakupäivä 25.3.2013).

3.3 Tarkastusoikeus

Jokaisella on oikeus tarkistaa itseään koskevat henkilötiedot. Henkilötietolain mukaan jokaisella on salassapitosäännösten estämättä oikeus saada tietää, mitä häntä koskevia henkilötietoja henkilörekisteriin on tallennettu tai ettei rekisterissä ole häntä koskevia tietoja. Rekisterinpitäjän on samalla ilmoitettava rekisteröidylle rekisterin säännönmukaiset tietolähteet sekä mihin henkilörekisterin tietoja käytetään ja säännönmukaisesti luovutetaan. (HTL 6:26.1 §.) Tarkastusoikeus koskee niin jokaista itseään kuin huollossa olevaa lastakin, jos tiedot on tallennettu rekisteriin ja tiedot koskevat tietojen pyytäjää tai hänen huollossaan olevaa lasta. Myös alaikäisellä, alle 18-vuotiaalla, on tarkastusoikeus. Rekisterinpitäjän arvion varaan jää, täyttääkö alaikäinen lapsi itsemääräämisoikeuden kriteerit, eli jos alaikäinen ikäänsä, kehitystasoonsa ja asian laatuun nähden ymmärtää asian merkityksen, hän voi käyttää tarkastusoikeutta. (Lapsen oikeuksien yleissopimus 20.11.1989/44 3 artiklan 1. kohta ja 12. artikla; PerL 6.3 §; 106 §; Tietosuojavaltuutettu a, hakupäivä 29.11.2012.)

Tarkastusoikeutta hyödynnetään yllättävän vähän, vaikka oikeus on hyvin vahva (Järvinen 2010, 265). Tiedot on annettava rekisteröidylle ilman aiheetonta viivytystä, ymmärrettävässä muodossa ja kirjallisesti, mikäli niin pyydetään (HTL 6:28.2 §; Tietosuojavaltuutettu a, hakupäivä 29.11.2012). Tiedot on annettava maksutta kerran vuodessa, jos rekisteröity käyttää tarkastusoikeutta. Mikäli tarkastusoikeutta käytetään useamman kerran vuoden sisällä, saa rekisterinpitäjä periä kohtuullisen korvauksen tiedonannosta, mutta ei enempää kuin mitä tiedon antamisesta on aiheutunut välittömiä kustannuksia. (HTL 6:26.3 §.)

Tarkastusoikeus edellyttää rekisterinpitäjän huolehtivan, että rekisteröity saa tiedon hänelle kuuluvista tiedoista. Rekisteröidylle on annettava mahdollisuus esittää tarkastuspyyntöjä, ja rekisterinpitäjän on järjestettävä pyyntöjen käsittely. On myös päätettävä, missä muodossa vastaukset toimitetaan. Tarkastusoikeudesta on hyvä informoida esimerkiksi rekisteriselosteessa. (Salminen 2009, 79.)

Kaikkia tietoja ei kuitenkaan tarvitse luovuttaa rekisteröidylle. Tarkastusoikeuden ulkopuolelle on muun muassa rajattu tiedot, joiden luovuttaminen voisi vaarantaa yleistä turvallisuutta, rikosten selvittämistä, jonkun toisen oikeuksia tai Euroopan unionin tärkeää taloudellista ja rahoituksellista etua (HTL 6:27 §). On hyvä huomioida, että vaikka osa tiedoista olisi sellaisia, joita ei tarvitse luovuttaa, on muut tiedot annettava (He 96/1998, 61). Rekisteröity voi aina pyytää tietoja ja mahdollinen kieltävä päätös on perusteltava aina kirjallisesti (HTL 6:28.2 §). Jos rekisterinpitäjä ei anna tietoja kolmen kuukauden kuluessa siitä, kun tietoja on pyydetty, rekisteröity voi saattaa asian tietovaltuutetun käsiteltäväksi (HTL 6:28.2 §).

Hämeenlinnan hallinto-oikeus on antanut selventävän ratkaisun, milloin henkilöllä ei ollut oikeutta tarkistaa itseään kokevia tietoja.

> Y:tä koskevassa sosiaalitoimistossa tehdyssä lastensuojelun huoltoselosteessa oli X:ää koskevia merkintöjä. Näistä tiedoista ei ollut annettu jäljennöksiä tarkastusoikeuden nojalla X:llä. Tietoja ei ollut annettu, koska tiedon antamisesta saattaisi aiheutua vakavaa vaaraa Y:n oikeuksille. Nämä tiedot oli Y:n luottamuksella kertomia asioita. (HAO 3.11.2000/00/369/3, Finlex.)

3.4 Tiedon korjaaminen

Virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto on viipymättä joko rekisterinpitäjän oma-aloitteisesti tai rekisteröidyn vaatimuksesta korjattava, poistettava tai täydennettävä. Jos yksityisyyden suoja tai rekisteröidyn oikeudet ovat vaarassa, on rekisterinpitäjän estettävä tällaisen tiedon leviäminen. (HTL 6:29.1 §.) Rekisteröidyn ei tarvitse perustella tiedon korjaamista, ja tieto on aina korjattava mahdollisimman pian (HE 96/1998, 63–64). Tietosuojavaltuutetun kannanoton mukaan rekisterinpitäjän ei tarvitse suostua tiedon korjaamiseen, jos asiakas vaatii nimensä kirjoittamista sellaisilla merkeillä, joita rekisterinpitäjällä ei ole keskustietokoneellaan. Tällöin nimi voidaan kirjoittaa alkuperäistä nimeä vastaavalla tavalla suomen kielen mukaan. On kuitenkin kiinnitettävä huomiota siihen, miten kyseinen henkilö voidaan erottaa muista rekisteröidyistä eli yksilöidä yksiselitteisesti tietyksi henkilöksi. (Tietosuojavaltuutetun kannanotto, Dnro 649/41/2001.)

Mikäli rekisterinpitäjä ei hyväksy rekisteröidyn pyyntöä tiedon korjaamisesta, on rekisterinpitäjän annettava kirjallinen todistus tästä perusteluineen. Rekisteröity voi halutessaan viedä asian tietosuojavaltuutetun käsiteltäväksi. (HTL 6:29.2 §.) Tämän vuoksi perusteluissa olisi oltava rekiste-

rinpitäjän nimi, osoite, henkilötietojen käsittelyn tarkoitus, rekisteröidyn nimi ja rekisteröidyn vaatima muutos henkilötietoihin sekä perustelut vaatimukseen (HE 96/1998, 64). Tietosuojavaltuutettu painottaa, että mitä yksilöidympi, perustellumpi ja selkeämpi korjausvaatimus on, sitä paremmin rekisterinpitäjä pystyy sitä käsittelemään (Tietosuojavaltuutettu a, hakupäivä 29.11.2012). Oikeutta saada tiedot korjatuksi voidaan pitää rekisterinpitäjään kohdistuvan virheettömyysvaatimuksen peilikuvana (Vanto 2011, 134).

Jos rekisterinpitäjä on luovuttanut tai saanut henkilötietoja, on sen ilmoitettava korjattavasta tiedosta sille, jolle rekisterinpitäjä on luovuttanut tai jolta se on virheellisen tiedon saanut. Ilmoittamista ei tarvitse tehdä, mikäli se on mahdotonta. (HTL 6:29.3 §.) Hallituksen esityksessä ei määritellä tarkemmin, mitä mahdottomuudella tarkoitetaan (HE 96/1998 64).

3.5 Kielto-oikeus

Rekisteröity voi halutessaan kieltää rekisterinpitäjää käsittelemästä häntä koskevia tietoja suoramainontaa, etämyyntiä ja muuta suoramarkkinointia sekä markkina- ja mielipidetutkimusta että henkilömatrikkelia ja sukututkimusta varten (HTL 6:30 §). Mikäli rekisteröity haluaa kieltää osoitetietojensa käyttämisen tai luovuttamisen suoramarkkinointitarkoituksiin, on hänen ilmoitettava kiellosta rekisterinpitäjälle. Tiedon voi ilmoittaa joko puhelimitse tai kirjallisesti. Kielto-oikeuden käyttäminen on rekisteröidylle aina maksutonta. (Tietosuojavaltuutettu a, hakupäivä 29.11.2012.)

Suoramarkkinoinnin osalta on huomioitava, että ei-sähköisessä muodossa tapahtuva, esimerkiksi postin kautta toimitettava mainonta, voidaan kieltää, kun rekisteröity sitä pyytää. Tällaista suoramarkkinointia voidaan tehdä niin kauan kunnes rekisteröity kieltää sen. Sähköistä suoramarkkinointia puolestaan säädellään tietosuojalaissa, jossa pääsääntö on, että sähköistä suoramarkkinointia saa kohdistaa ainoastaan henkilöihin, jotka ovat antaneet siihen ennalta suostumuksensa. (SVTSL16.6.2004/516 7:26.1 §; Vanto 2011, 135.)

3.6 Automatisoitu päätös

Automatisoidulla päätöksellä tarkoitetaan rekisteröidyn ominaisuuksien, kuten ammatillisen suoriutumisen, luottokelpoisuuden, luotettavuuden tai käyttäytymisen arviointia sekä tiedoista tehtyä päätöstä, joka tehdään täysin automatisoidun tietojenkäsittelyn avulla. Automatisoituun päätök-

seen ei saa vaikuttaa inhimillinen myötävaikutus, jos päätöksestä syntyy oikeudellisia vaikutuksia rekisteröidylle tai jos se vaikuttaa muuten rekisteröityyn merkittävällä tavalla. (HTL 6:31.1 §; HE 96/1998, 65.) Tällaiset päätökset ovat sallittuja vain silloin, kun siitä on laissa säädetty tai päätös tehdään sopimuksen tekemisen tai täytäntöönpanon yhteydessä. Tällainen päätös edellyttää kuitenkin, että rekisteröidyn oikeudet suojataan tai rekisteröidyn sopimuksen tekeminen tehdään tai täytäntöönpanoa koskevaan pyyntöön vastataan. (HTL 6:31.1 §.)

Tietosuojavaltuutetulle on ilmoitettava, mikäli automatisoitua päätöksentekoa käytetään. Tällä halutaan taata rekisteröidyn oikeuksien toteutuminen. (HTL 8:36.1 §.) Lisäksi rekisterinpitäjän on ilmoitettava tietosuojavaltuutetulle, jos tietoja siirretään Euroopan unionin jäsenvaltioiden rajojen tai Euroopan talousalueen ulkopuolelle (HTL 8:36.2 §).

4 REKISTERINPITÄJÄN VELVOLLISUUDET

4.1 Henkilötietojen käsittelyä koskevat yleiset periaatteet

Rekisterinpitäjällä on monia velvollisuuksia. Rekisterinpitäjän on huolehdittava mahdollisuuksien mukaan käsiteltävien henkilötietojen oikeellisuudesta ja ajantasaisuudesta. Virheellisiä, vanhentuneita tai epätäydellisiä tietoja ei saa käsitellä. (Innanen & Saarimäki 2012, 87.) On huomioitava, että kaikkien rekisterinpitäjän velvollisuuksien on toteuduttava yhtä aikaa (Salminen 2007, 30).

4.1.1 Huolellisuusvelvoite

Henkilötietolaki asettaa rekisterinpitäjälle huolellisuusvelvoitteen, mikä tarkoittaa, että henkilötietojen käsittelyssä on noudatettava lakia, huolellisuutta ja hyvää tietojenkäsittelytapaa. Rekisterinpitäjän on toimittava niin, että rekisteröidyn yksityiselämän suojaa ja muita yksityisyydensuojan turvaavia perusoikeuksia ei rajoiteta ilman laissa säädettyä perustetta. Tämä sama sääntö koskee myös niitä, jotka toimivat rekisterinpitäjän lukuun, kuten alihankkijoita. (HTL 2:5 §.) Kenenkään yksityisyyttä ei siis saa vaarantaa eikä loukata. (Salminen 2007, 34.)

Huolellisuusvelvoite tietosuojalainsäädännön periaatteena luo pohjan hyvään tiedonhallintatapaan sekä rekisterinpidon itseohjautuvuuteen. Rekisterinpitäjän on oma-aloitteisesti huolehdittava siitä, että henkilötietoja käsitellään niin, että otetaan huomioon yksityisyydensuojan säännökset ja muut periaatteet. Rekisterinpitäjän on siis tunnettava lain säännökset sekä huolehdittava henkilötietoja käsittelevien henkilöiden riittävästä koulutuksesta ja luotava menettelytavat, jotka täyttävät lain vaatimukset. (HE 96/1998, 37.) Viime aikoina otsikoihin on noussut Sisäministeriön selvityspyyntö poliisihallinnon henkilötietojen käsittelystä ja huolellisuusvelvoitteen tärkeydestä. Erityisesti tässä nousee esille, että on huolehdittava sisäisestä ohjeistuksesta ja valvottava henkilötietojen käsittelyä. (Sisäasiainministeriö, hakupäivä 12.4.2013.) Hyvä rekisteritapa on joustava käsite, mikä täsmentyy ja konkretisoituu lain soveltamisen kautta. Soveltamisessa on kuitenkin toimialakohtaisia vaihteluita. Hyvä rekisteritapa on jatkuvassa muutoksessa, ja se koostuu lähes kokonaan sellaisista asioista, joista ei ole laissa erikseen säädetty. (Salminen 2007, 35.)

Myös tietosuojavaltuutettu toteaa ohjeistuksessaan, että hyvä tietojenkäsittelytapa edellyttää, ettei kenenkään yksityisyyttä saa perusteettomasti loukata eikä vaarantaa (Tietosuojavaltuutettu d, hakupäivä 29.11.2012). Tämä merkitsee sitä, että henkilötunnuksen keräämisen tarve ja vaihtoehtoisten yksilöintitietojen käyttömahdollisuudet tulee selvittää aina jo suunnitteluvaiheessa kaikkien käsittelyvaiheiden kannalta (Vanto 2011, 39).

Huolellisuusvelvoitteen huomioiminen tietojenkäsittelyssä on hyvin monivaiheinen ja jatkuva prosessi. Tämä prosessi koostuu henkilötietolain vaatimusten läpiviennistä rekisterinpitäjän organisaatiossa. Erityistä huomiota on kiinnitettävä henkilötietojen käsittelyn suunnitteluun kaikessa toiminnassa. (Vanto 2011, 40.) Erityisesti internet-palveluissa on sen toimintaympäristön monimuotoisuuden vuoksi kiinnitettävä huomiota palveluiden toimivuuteen ja teknillisiin ominaisuuksiin. Henkilötietojen käsittely internet-palveluissa liittyykin hyvin kiinteästi tekniseen toteutukseen. (Salminen 2007, 36.)

4.1.2 Suunnitteluvelvollisuus

Henkilötietolain mukaan henkilötietojen käsittelyn täytyy olla asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta (HTL 2:6 §). Asianmukaisuusvaatimus kohdistuu sekä rekisterinpidon tarpeellisuuteen yleensä että rekisterin käyttötarkoitukseen (HE 96/1998, 37–38). Lähtökohtana henkilötietojen käsittelylle on se, että rekisterinpitäjän on voitava perustella, miksi kyseisten tietojen käyttö sen toiminnassa on tarpeellista ja asiallista. Näin ollen tarpeettomien henkilötietojen käsittely rekisterinpitäjän toiminnassa ei ole henkilötietolain mukaan oikein. (Vanto 2011, 41.)

Asianmukaisuusvaatimus perustuu tietosuojadirektiivin 6. artiklan ensimmäiseen kohtaan. Siinä vaaditaan jäsenmaita säätämään, että henkilötietoja käsitellään asianmukaisesti ja laillisesti. (Euroopan parlamentin ja neuvoston direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla, 12.7.2002, 2002/58/EY, 6.)

Ennen henkilötietojen keräämistä tai muodostamista henkilörekisteriksi on määriteltävä henkilötietojen käsittelyn tarkoitukset sekä se, mistä henkilötiedot säännönmukaisesti hankitaan, ja mihin niitä säännönmukaisesi luovutetaan. Henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisen rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään. (HTL 2:6 §.) Hallituksen esityksessä (HE 96/1998, 38) tarkennetaan vielä, että henkilörekisteriä saa ja

pitää käyttää niin, että toiminta täyttää asiallisuuden ja yleisen mittapuun mukaan arvioituna myös hyväksyttävyyden kriteerit. Rekisterinpitäjän on arvioitava toimintaa kokonaisvaltaisesti sekä otettava huomioon toiminnan kaikki osa-alueet ja henkilötietojen käsittelyn tarve ja käyttötarkoitus näillä osa-alueilla. (Vanto 2011, 41-42.) Suunnitteluvelvoite edellyttää rekisterinpitäjän toiminnan ja tietojärjestelmäkokonaisuuden kuvaamista ja suunnittelemista, sillä näin henkilötietojen käsittely voidaan perustella asiallisesti toiminnan kannalta (Salminen 2007, 36).

4.1.3 Käyttötarkoitussidonnaisuus

Käyttötarkoitussidonnaisuusperiaate tarkoittaa sitä, että henkilötietoja voi käsitellä vain tavalla, joka ei ole suunnitteluvelvoitteen perusteella määritellyn käsittelyn tarkoituksen vastaista. Rajoitus ei kuitenkaan lainkohdan mukaan koske henkilötietojen käyttöä tieteellistä tutkimusta tai tilastotarkoitusta varten. (HTL 2:7 §.) Käsiteltävien tietojen tarpeellisuus ja henkilötietojen käsittelyn tarkoitus rekisterinpitäjän toiminnan kannalta riippuvat siis rekisterinpitäjän tehtävän luonteesta, erityisesti sen sisällöstä, toiminnallisuuksista ja liiketoimintamallista (Salminen 2007, 43–44). Tietosuojavaltuutetun mukaan on kuitenkin muistettava, että jos henkilötietoja käytetään edellä mainittuun käyttöön, on salassapitosäännökset muistettava (Tietosuojavaltuutettu a, hakupäivä 29.11.2012). Tällä tarkoitetaan sitä, että jos esimerkiksi asiakkaan matkapuhelinnumero on määritelty kerättäväksi asiakkaan tilaaman palvelun suorittamistarkoituksessa, ei sitä myöhemmin voi käyttää markkinointitarkoitukseen (Vanto 2011, 43).

Hallituksen esityksessä henkilötietojen käsittelyn tarkoitus sekä säännönmukaiset tietojen siirrot voidaan myöhemmin määritellä uudelleen, jos rekisterinpitäjän toiminnan olosuhteet muuttuvat ja uudelleen määrittely on näin ollen tarpeen. Tässä on kuitenkin otettava huomioon se, että näin määritelty tarkoitus ei saa olla yhteen sopimaton alkuperäisen käsittelyn tarkoituksen kanssa. (HE 96/1998, 38.)

4.1.4 Käsittelyn yleiset edellytykset

Käsittelyn yleiset periaatteet on otettava huomioon koko käsittelyn elinkaaren ajan henkilötietojen keräämisestä niiden tuhoamiseen asti. Nämä periaatteet ohjaavat rekisterinpitäjää valitsemaan henkilörekisterin suunnittelussa, rakentamisessa ja ylläpitämisessä toimintatavat, joiden avulla henkilötietolain tarkoitus toteutuu. (Laaksonen, Nevasalo & Tomula 2006, 38.) Rekisterinpitäjän

on muistettava yleisten edellytysten lisäksi asiallisen perustelun vaatimus sekä henkilötietojen käyttötarkoitussidonnaisuus (Vanto 2011, 44).

Henkilötietolain 2:8. §:ssä on säädetty käsittelyn yleisistä edellytyksistä yhdeksän asian lista. Henkilötietoja saa käsitellä aina rekisteröidyn suostumuksella (HTL 2:8.1 § 1 k.). Hallituksen esityksessä määritellään tarkemmin, että henkilötietojen käsittelyn tulisi lähtökohtaisesti perustua rekisteröidyn suostumukseen, sillä tällöin toteutuu parhaiten henkilön tiedollinen itsemääräämisoikeus ja rekisterinpidon avoimuus (HE 96/1998, 38). Henkilötietolaissa ja henkilötietojen käsittelyssä suostumuksella on hyvin keskeinen rooli, ja siksi onkin hyvä ymmärtää pätevän suostumuksen edellytykset. Henkilötietojen käsittely on kielletty ilman pätevää suostumusta, ellei tiedossa ole muuta laissa mainittua yleistä edellytystä käsittelylle. (Vanto 2011, 44.) Suostumuksen tulee olla vapaaehtoinen, yksilöity ja tietoinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn (HTL 1:3 § 7 k.). Tässä on hyvin tärkeää muistaa, että suostumuksen nimenomaisuus ja asiakkaan riittävän tietoisuuden syntyminen edellyttävät asiakkaan kattavaa informaatiota siitä, mihin hän suostumuksensa antaa. Yleensä tämä edellyttää rekisteröidyltä aktiivista toimenpidettä. (Salminen 2009, 55.)

Hallituksen esityksessä mainitaan suostumuksesta vielä, että sen olisi oltava rekisteröidyn yksiselitteisesti antama (HE 96/1998, 39). Tietosuojavaltuutetun kannanotossa (1218/45/2000), joka käsittelee sitä, saako ammattiyhdistys julkaista internet-sivuillaan jäsentensä tiedossa olevia sähköpostiosoitteita, painotetaan, että tähän on oltava jäsenten suostumus. Tietoja saa käyttää vain yhdistystoiminnassa eli tietojen käyttötarkoitussidonnaisuus on otettava huomioon. (Tietosuojavaltuutettu e, hakupäivä 4.2.2013.) Rekisteröidyn suostumus voidaan internetissä pyytää rekisteröitymisen yhteydessä eli samalla, kun hän antaa tietoja rekisterinpitäjän käyttöön. Tämä vaatii käytännössä rekisteröidyn toimenpiteitä suostumuksen ilmaisemiseksi, kuten suostumuksen ilmaisevan merkin merkitsemistä rekisteröitymisen yhteydessä tietojen merkitsemislomakkeen kohtaan, jossa suostumuksen sisältö on yksilöity riittävän yksiselitteisesti. Toisaalta myös pelkkä asiakastietojen antaminen voi olla suostumus, mutta tällöin rekisteröityä täytyy selkeästi informoida asiasta. (Salminen 2007, 31.) Suostumukselle asetetut vaatimukset määräytyvät kuitenkin tapauskohtaisesti, ja merkitystä on myös kerättävän tiedon laadulla. Viime kädessä suostumuksen olosta syntyneessä kiistassa todistustaakka on rekisterinpitäjällä. Tämän vuoksi rekisterinpitäjän olisi syytä tallentaa rekisteröidyn suostumus. (HE 96/1998, 39.)

Rekisterinpitäjä saa käsitellä henkilötietoja rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osallisena. Rekisterinpitäjä voi käsitellä henkilötietoja myös sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä. (HTL 2:8.1 § 2 k.) Tällaista henkilötietojen käsittelyä voi olla esimerkiksi matkapuhelinliittymän avaamista varten tarvittavien henkilötietojen käsittely (Vanto 2011, 46).

Jos kysymyksessä on rekisteröidyn elintärkeän edun suojaaminen yksittäistapauksessa, voidaan henkilötietoja käsitellä ilman rekisteröidyn suostumusta (HTL 3:8.1 § 3 k.). Tässä keskeisintä on, että kysymyksessä on rekisteröidyn elintärkeä etu. Tällainen tilanne voi olla esimerkiksi, kun on kysymys rekisteröidyn hengen tai terveyden pelastamisesta ja se edellyttää häntä koskevien tietojen käsittelyä eikä hänen suostumustaan käsittelyyn ole saatavilla. Tällöin täytyy muistaa, että kysymyksessä on oltava yksittäistapaus. (HE 96/1998, 39.)

Henkilötietoja voi lisäksi käsitellä, mikäli käsittelystä on säädetty laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta (HTL 3:8.1 § 4 k.). Hallituksen esityksessä tarkennetaan vielä, että henkilötietojen käsittely ei tältä osin voi perustua asetukseen tai asetuksen nojalla määrättyyn tehtävään tai velvoitteeseen (HE 96/1998, 39). Esimerkki henkilötietojen käsittelyä koskevasta sääntelystä on laki terveydenhuollon valtakunnallisista henkilörekistereistä. Siinä on lailla velvoitettu eri viranomaiset antamaan heidän rekisterissään olevat henkilötiedot valtakunnalliseen henkilörekisteriin. (Laki terveydenhuollon valtakunnallisista henkilörekistereistä 9.6.1989/556 3 §.) On hyvä muistaa, että henkilötietolakia sovelletaan yleislakina myös sellaiseen henkilötietojen käsittelyyn, josta on säädetty muussa laissa, ellei erityislaissa toisin säädetä (Vanto 2011, 47).

Henkilötietoja saa käsitellä, jos rekisteröidyllä ja rekisterinpitäjällä on asiallinen yhteys rekisterinpitäjän toimintaan tai yhteys perustuu asiakas- tai palvelusuhteeseen, jäsenyyteen tai muuhun niihin rinnastettavaan suhteeseen (HTL 2:8.1 § 5 k.). Asiakassuhdeperusteen osalta on hyvin tärkeää, että rekisterinpitäjä pystyy asiallisesti perustelemaan henkilötietojen käsittelyn yleensä. Asiakassuhdeperusteen osalta on määriteltävä, kuinka asiakassuhde syntyy ja kuinka se päättyy kyseisessä toiminnassa. (Salminen 2009, 56–57.) Internet-palveluissa asiakassuhde voi syntyä tuotetta tai palvelua ostettaessa sekä päättyä, mikäli palveluita ei enää käytetä tietyn ajan kuluttua tai kun tuote on toimitettu rekisteröidylle. Asiakassuhde voi siis olla myös määräaikainen. (Salminen 2009, 31.) Henkilötietojen luovuttamisen on oltava tavanomaista toiminnan harjoittami-

sessa ja nimenomaan henkilörekisterin tarkoituksen mukaista. On myös huomioitava, että rekisteröidyn voidaan olettaa tietävän tällaisesta tietojen luovuttamisesta. (HTL 2:8.2 §.)

Henkilötietoja saa käsitellä myös silloin, kun kysymyksessä on konsernin tai muun taloudellisen yhteenliittymän asiakkaita tai työntekijöitä koskevista tiedoista ja näitä tietoja käsitellään kyseisen yhteenliittymän sisällä (HTL 2:8.1 § 6 k.). Hallituksen esityksessä täydennetään asiallisen yhteyden vaatimusta tilanteissa, joissa konsernit ylläpitävät yhteisrekistereitä eikä rekisteröidyllä ole asiallista yhteyttä kaikkiin konserniin kuuluviin yhtiöihin. Yhdellä konserniyhtiöllä on kuitenkin oltava henkilötietolain vaatima asiallinen yhteys rekisteröityyn. (HE 96/1998, 39.)

Henkilötietoja voidaan lisäksi käsitellä, mikäli käsittely on tarpeen rekisterinpitäjän toimeksiannosta tapahtuvaa maksupalvelua, tietojenkäsittelyä tai muita niihin rinnastettavia tehtäviä varten (HTL 2:8.1 § 7 k.). Toimeksiantajalla ei ole itsenäistä oikeutta käsitellä tietoja, vaan hänen oikeutensa perustuu aina rekisterinpitäjän oikeuteen. Tällöin toimeksisaaja käsittelee tietoja rekisterinpitäjän lukuun ainoastaan saamansa maksupalvelu-, tietojenkäsittely- tai muun näihin rinnastettavan toimeksiannon puitteissa. (HE 96/1008, 39.)

Jos kysymyksessä on henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavista yleisesti saatavilla olevista tiedoista ja näitä käsitellään rekisterinpitäjän tai tiedot saavan sivullisen oikeuksien ja etujen turvaamiseksi, saa henkilötietoja käsitellä (HTL 2:8.1 § 8 k.). Hallituksen esityksen mukaan tämä säännös mahdollistaa esimerkiksi ammatin- ja elinkeinonharjoittajan luottotietojen käsittelyn. Yleisesti saatavilla olevilla tiedoilla tarkoitetaan laissa muun ohella oikeusrekisterikeskuksen pitämään liiketoimintakieltorekisteriin sekä konkurssi- ja yrityssaneerausrekisteriin ja kaupparekisteriin sisältyviä tietoja, jotka ovat julkisia. Tämä mahdollistaa henkilötietojen käsittelyn, jos käsittely on tarpeen rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun intressin toteuttamiseksi. Tämä edellyttää, etteivät yksityisyyden suojaa turvaavat edut syrjäytä näitä rekisterinpitäjän tai sivullisen intressejä. Voidaan katsoa, etteivät henkilön yksityisyyden suojaa turvaavat edut edellä mainitussa henkilötietolain kohdassa tarkoitetuissa tilanteissa syrjäytä rekisterinpitäjän tai sivullisen intressejä, koska kysymys on henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavista tiedoista, jotka ovat yleisesti saatavilla. (HE 96/1998, 40.)

Henkilötietoja saa käsitellä, jos tietosuojalautakunta on antanut luvan käsittelyyn. Lain pykälässä viitataan jäljempänä olevaan lain kohtaan. (HTL 2:8.1 § 9 k.) Kyseisessä pykälässä ja momentissa säädetään, että

> Tietosuojalautakunta voi antaa luvan henkilötietojen käsittelylle, jos käsittely on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi muussa kuin yksittäisessä tapauksessa taikka yleistä etua koskevan tehtävän suorittamiseksi tai sellaisen julkisen vallan käyttämiseksi, joka kuuluu rekisterinpitäjälle tai sivulliselle, jolle tiedot luovutetaan. Lupa voidaan myöntää myös rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun edun toteuttamiseksi edellyttäen, ettei tietojen tällainen käsittely vaaranna henkilön yksityisyyden suojaa ja oikeuksia. (HTL 9:43.1 §.)

4.1.5 Tiedon laatua koskevat periaatteet

Rekisterinpitäjän on pidettävä huoli siitä, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja käsitellä, eli kysymyksessä on niin sanottu virheettömyysvaatimus (HTL 2:9.2 §). Tämän säännöksen kannalta on keskeistä, että henkilötietojen käsittelyn tarkoitus on määritelty, kuten henkilötietolaissa siitä tarkemmin säädetään (HTL 2:5.2 §). Sen jälkeen, kun käyttötarkoitussidonnaisuus on määritelty, tulee miettiä mitä tietoja rekisteröidystä tarkoitusten saavuttamiseksi tarvitaan (Vanto 2011, 52). Tietojen tulee siis olla tarpeellisia käyttötarkoituksen mukaisesti, eikä määriteltyihin käyttötarkoituksiin kuulumattomia tietoja saa käsitellä edes asiakkaan suostumuksella (Salminen 2009, 65). Sen lisäksi, että liian laajoja henkilötietoja ei saa kerätä, ei myöskään saa käsitellä virheellisiä, epätäydellisiä tai vanhentuneita asiakastietoja. Keinot tiedon laadun ja henkilötietojen virheettömyyden varmistamiseksi on suunniteltava ennen tietojen keräämistä. Tiedon laatu ja virheettömyys voidaan varmistaa esimerkiksi niin, että aina kun rekisteröity on yhteydessä rekisterinpitäjään, hänen perustietonsa tarkistetaan. Täydellinen tiedon virheettömyyden vaatimus on useimmiten käytännössä mahdotonta, eikä lakikaan sitä vaadi. (Salminen 2009, 65.)

Rekisterinpitäjän velvollisuutta arvioitaessa on otettava huomioon henkilötietojen tarkoitus sekä käsittelyn merkitys rekisteröidyn yksityisyyden suojalle (HTL 2:9.2 §). Rekisterinpitäjän yksityisyyden suojaa koskevalla velvollisuudella tarkoitetaan sitä, että käsiteltäessä henkilötietoja tutkimus- tai tilastotarkoituksiin velvoite ei edellytä yhtä laajoja toimia kuin, jos kysymys on sellaisesta henkilötietojen käsittelystä, jossa tietoja käytetään yksityistä henkilöä koskevassa päätöksenteossa. (HE 96/1998, 42.)

4.2 Rekisteriseloste

Rekisteriselosteen avulla pyritään tietojenkäsittelyn avoimuuteen rekistereissä. Henkilötietolain velvoittaa rekisterinpitäjän laatimaan henkilörekisteristä rekisteriselosteen, jonka on oltava jokaisen saatavilla rekisterinpitäjän toimipaikassa (HTL 2:10.1 §). Mikäli rekisterinpitäjällä on useita toimipaikkoja, on rekisteriseloste oltava rekisterinpitäjän kaikissa toimipaikoissa. Rekisteröity voi halutessaan pyytää rekisteriselosteen nähtäväksi rekisterinpitäjältä. Jos rekisteröity ei saa rekisteriselostetta nähtäväksi, voi rekisteröity kääntyä tietosuojavaltuutetun puoleen. (Tietosuojavaltuutettu a, hakupäivä 29.11.2012.) Voidaan todeta, että rekisteriselosteen yksi tarkoitus on, että rekisterinpitäjä on pohtinut riittävästi rekisterin tarkoitusta, suojausta ja tietojen luovuttamista (Järvinen 2010, 258).

Rekisteriseloste on osa henkilötietolaissa tarkoitettua henkilötietojen käsittelyn suunnittelua (HTL 2:6 §). Rekisteriseloste on laadittava, oli sitten kyse automaattisen tietojenkäsittelyn avulla ylläpidettävästä henkilörekisteristä tai manuaalisesta rekisteristä. (HE 96/1998, 42.) Tästä velvollisuudesta voidaan poiketa ainoastaan, jos se on välttämätöntä valtion turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi tai verotukseen tai julkiseen talouteen liittyvän valtion tehtävän vuoksi (HTL 2:10.2 §). Rekisteriselosteen tulee olla saatavilla internetissä, mikäli henkilörekisteri on tietoverkossa (HE 96/1998, 42).

Henkilötietolain mukaan rekisteriselosteesta on tultava esiin

1. rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot
2. henkilötietojen käsittelyn tarkoitus
3. kuvaus rekisteröidyn ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä
4. mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle
5. kuvaus rekisterin suojauksen periaatteista (HTL 2:10 §.)

Nämä rekisteriselosteen vaatimukset ovat hyvin suppeat eli rekisteriselosteelta ei vaadita paljon (Vanto 2011, 55). Rekisteriselosteen tietojen ei tarvitse olla yksityiskohtaisia. Henkilörekisterin epävirallisia nimiä tai tietotyyppejä ei tarvitse erikseen eritellä. Ei myöskään tarvitse kuvata yksityiskohtaisesti käytettyjä palomuureja tai tietoturvaohjelmia, eli tietojen kuvaaminen yleisellä,

ymmärrettävällä tasolla riittää. Jos esimerkiksi teknisiä suojauksia kuvaa kovin tarkkaan, se voi olla jopa tietoturvariski. (Järvinen 2010, 258.)

4.3 Arkaluonteiset tiedot ja henkilötunnus

Jo henkilörekisteriä suunniteltaessa on otettava huomioon arkaluonteisten tietojen ja henkilötunnuksen käsittely. Henkilötietolain mukaan nämä tiedot vaativat erityistä perustelua. Käytännössä kyseisiä tietoja ei saa käsitellä lainkaan, ellei niiden käsittely ole toiminnan kannalta välttämätöntä. Myös muiden henkilötietolain asettamien yleisten periaatteiden toteutuminen kannattaa varmistaa arkaluonteisten tietojen ja henkilötunnuksen osalta huolellisesti. (Järvinen 2010, 262.)

4.3.1 Arkaluonteiset henkilötiedot

Lain mukaan tietojenkäsittelyn lähtökohtana on, että arkaluonteisten henkilötietojen käsitteleminen on kielletty. Henkilötietolain mukaan seuraavia tietoja on pidettävä arkaluonteisina:

1. rotu tai etninen alkuperä
2. henkilön yhteiskunnallinen, poliittinen tai uskonnollinen vakaumus tai ammattiliittoon kuuluminen
3. rikollinen teko, rangaistus tai muu rikoksen seuraamus
4. henkilön terveydentila, sairaus tai vamma tai häneen kohdistunut hoitotoimenpide tai näihin verrattava toimi
5. henkilön seksuaalinen suuntautuminen tai käyttäytyminen
6. henkilön sosiaalihuollon tarve tai hänen saamat sosiaalihuollon palvelut, tukitoimet tai muu sosiaalihuollon etuus (HTL 2:11 §.)

Näiden tietojen käsittely on siis lähtökohtaisesti kielletty, mutta henkilötietolaissa on lueteltu poikkeusperusteet, jotka mahdollistavat arkaluonteisten tietojen käsittelyn. Arkaluonteisia tietoja saa siis käsitellä vain henkilötietolaissa erikseen säädetyissä tilanteissa. (HTL 3:12 §.) Poikkeukset koskevat myös viranomaisten henkilörekistereissä olevien arkaluonteisten tietojen käsittelyä ja siten myös tietojen luovuttamista viranomaisten rekistereistä. (Salminen 2009, 75.)

Henkilötietolain mukaan arkaluonteisia tietoja saa käsitellä, jos rekisteröity on antanut käsittelylle nimenomaisen suostumuksensa (HTL 3:12.1 § 1 k.). Tällainen nimenomainen suostumus edellyttää kirjallista suostumusta, jossa ilmenee minkälaiseen käsittelyyn lupa on annettu (HE 96/1998, 43). Tässäkin on hyvä muistaa, että rekisterinpitäjällä on todistustaakka suostumuksen olemassaolosta, mikäli tarve sille tulee (Vanto 2011, 58).

Arkaluonteisten tietojen käsittelykielto ei estä sellaisen henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista koskevia tietoja, jotka rekisteröity on itse saattanut julkisuuteen (HTL 3:12.1 § 2 k.). Tässä on otettava huomioon se, että useimmiten näiden tietojen julkisuuteen tulo on henkilön omankin edun mukaista, esimerkiksi poliittiset luottamustehtävät (HE 96/1998, 43). Hyvä kysymys on kuitenkin se, saako arkaluonteista tietoa käsitellä silloin, kun henkilö on itse tuonut tiedon julkisuuteen esimerkiksi sosiaalisessa mediassa.

Arkaluonteisia tietoja saa käsitellä, mikäli tieto on tarpeen rekisteröidyn tai jonkun toisen henkilön elintärkeän edun suojaamiseksi ja rekisteröity on estynyt antamasta suostumustaan (HTL 3:12.1 § 3 k.). Tämä peruste tulee kysymykseen erityisesti rekisteröidyn terveydentilaan liittyvissä tilanteissa, kuten ensiaputilanteissa (HE 96/1998, 43).

Jos tietojen käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi, arkaluonteisten tietojen käsittely on sallittua (HTL 3:12.1 § 4 k.). Hallituksen esityksen mukaan (HE 96/1998, 43) tämä pykälä helpottaa muun muassa asianajajien ja yleisten oikeusaputoimistojen oikeutta käsitellä vastapuolta koskevia rikostietoja ja muita asian ajamisessa tarvittavia arkaluonteisia tietoja. On kuitenkin muistettava, että henkilötietojen käsittelyn on oltava asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. (Vanto 2011, 60.)

Kielto käsitellä arkaluonteisia tietoja ei koske laissa säädettyä käsittelyä tai jos käsittely johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä (HTL 3:12.1 § 5 k.). Hallituksen esityksessä tarkennetaan, että arkaluonteisten tietojen kerääminen tai jos rekisterinpitäjä käsittelee tietoja tehtävänsä perusteella, ei tämän lain kohdan mukaan ole mahdollista, jos henkilörekisteristä on säädetty vain asetuksessa (HE 96/1998, 44). Esimerkiksi perusopetuslain mukaan opetuksen järjestäjillä on oikeus saada oppilaistaan tiedot salassapitosäännösten estämättä sosiaali- ja terveydenhuoltoviranomaiselta, muulta sosiaalipalvelun tai terveydenhuollon palvelujen tuottajalta sekä terveydenhuollon ammattihenkilöltä (Perusopetuslaki 21.8.1998/628 8:41.4 §).

Arkaluonteisten tietojen käsittelykielto ei estä tietojen käsittelyä historiallista tai tieteellistä tutkimusta taikka tilastointia varten (HTL 3:12.1 § 6 k.). Hallituksen esityksessä viitataan henkilötietolain 14. ja 15. §:ään, missä säädetään ne tilanteet, joissa henkilötietojen käsittely on historiallista tai tieteellistä tutkimusta tai tilastointia varten sallittua (HE 96/1998, 44).

Arkaluonteisten tietojen käsittelykielto ei estä uskonnollista, poliittista tai yhteiskunnallista vakaumusta koskevien tietojen käsittelyä tällaista vakaumusta edustavien yhdistysten ja muiden yhteisöjen toiminnassa. Tietoja voidaan käsitellä, jos ne koskevat näiden yhdistysten tai yhteisöjen jäseniä tai henkilöitä, joilla on säännölliset yhdistysten ja yhteisöjen tarkoituksiin liittyvät yhteydet, eikä tietoja luovuteta sivullisille ilman rekisteröidyn suostumusta (HTL 3:12.1 § 7 k.). Tämä lainkohta sallii siis yhdistysten ja yhteisöjen käsitellä jäsentensä henkilötietoja, sillä heidän jäsenyytensä yhdistyksessä tai yhteisössä jo sinällään luo olettamuksen henkilötietojen arkaluonteisuudesta (Vanto 2011, 61).

Arkaluonteiset tiedot on poistettava välittömästi rekisteristä sen jälkeen, kun käsittelylle ei ole momentissa mainittua perustetta (HTL 3.12.2 §). Tämä tarkoittaa käytännössä sitä, että rekisteröity on antanut kirjallisen suostumuksen arkaluonteisten tietojen käsittelylle, mutta jos rekisteröity peruuttaa myöhemmin suostumuksen, on kaikki häntä koskevat tiedot välittömästi poistettava rekisteristä. Myös silloin, kun rekisteröity eroaa poliittisesta puolueesta tai uskonnollisesta yhteisöstä, on kaikki häntä koskevat tiedot poistettava tietojärjestelmistä. (Vanto 2011, 67.)

4.3.2 Henkilötunnuksen käsitteleminen

Lähtökohtaisesti myös henkilötunnuksen käsittelyä tulee välttää, ellei sen käsittely ole välttämätöntä. Henkilötunnuksen liian laaja käyttö voi muodostaa tietoturvallisuusriskin rekisteröidylle ja aiheuttaa välillisesti riskejä myös rekisterinpitäjälle. On myös huomioitava, että vaikka rekisterinpitäjällä on lupa käsitellä henkilötunnuksia, niitä ei saa merkitä tarpeettomasti esimerkiksi tulosteisiin. (HTL 3:13.4 §; Laaksonen yms. 2006, 41.)

Henkilötunnuksen käsittely on sallittua rekisteröidyn yksiselitteisesti antamalla suostumuksella tai jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää laissa säädetyn tehtävän suorittamiseksi, rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi tai historiallista tai tieteellistä tutkimusta

tai tilastointia varten. (HTL 3:13.1 §.) Perusedellytyksenä on, että rekisteröidyn yksiselitteinen yksilöiminen on tärkeää lainkohdassa mainitun tehtävän suorittamiseksi. Pelkkä laissa säädetyn tehtävän helpompi tai nopeampi suorittaminen henkilötunnuksen avulla ei oikeuta henkilötunnuksen käsittelyä, vaan käsittely on sallittua ainoastaan silloin, kun rekisteröidyn yksiselitteinen yksilöiminen on tärkeää tehtävästä suoriutumiseksi. (HE 96/1998, 48.) Henkilötiedot tulee suojata hyvin, ja näitä tietoja saa käsitellä vain niihin oikeutettu henkilö (Pesonen 2008, 146).

Henkilötunnusta saa käsitellä lain mukaan luotonannossa tai saatavan perinnässä, vakuutus-, luottolaitos-, maksupalvelu-, vuokraus- ja lainaustoiminnassa, luottotietotoiminnassa, terveydenhuollossa, sosiaalihuollossa ja muun sosiaaliturvan toteuttamisessa sekä virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa (HTL 3:13.2 §). Nämä ovat erityisiä tilanteita, joissa rekisteröidyn yksiselitteinen yksilöiminen on erityisen tarpeellista ja usein myös välttämätöntä jo rekisteröidyn oikeusturvankin kannalta (HE 96/1998, 48).

Henkilötunnusta saa käsitellä myös osoitetietoja päivitettäessä tai moninkertaisen postilähetyksen välttämiseksi suoritettavan tietojenkäsittelyn vuoksi, jos henkilötunnus jo on luovutuksensaajan käytettävissä (HTL 3:13.3 §). Tällä voidaan välttää monia turhia työvaiheita rekistereissä ja yritysten toiminnassa (Vanto 2011, 68).

Sähköisissä palveluissa on usein hyvä käyttää henkilötunnusta asiakkaan yksilöintiin. Tällöin henkilötunnuksen käyttötarkoitus on erotella asiakkaat asiakasrekistereissä, mutta pelkkää henkilötunnusta ei saa käyttää tunnistamiseen rekisteröitymisen yhteydessä. Myöskään henkilötunnuksen käyttö käyttäjätunnuksena ei ole sallittua. Henkilötunnuksen käytön kanssa kannattaa olla hyvin tarkka, jotta vältytään henkilötunnuksen turhalta käytöltä. (Salminen 2009, 76.)

5 TIETOTURVALLISUUS JA TIETOJEN SÄILYTTÄMINEN

Tietosuojan ydinaluetta ovat yksityisyyden suojaaminen ja henkilötietojen käsittelyn toimintatavat. Tietoturvaan puolestaan kuuluu erityisesti tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistaminen. (Innanen & Saarimäki 2012, 112.)

5.1 Tietojen suojaaminen

Tietojen suojaamisen lähtökohtana on, että rekisterinpitäjän on huolehdittava riittävästä teknisestä ja organisatorisesta henkilötietojen suojaamisesta. Asiattomilla ei saa olla pääsyä tietoihin. Vahingossa tai laittomasti tapahtuvaa tietojen hävittämistä, muuttamista, luovuttamista, siirtämistä tai muuta käsittelyä ei saa tapahtua. Riittävän tietosuojan turvaamiseksi on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta. (HTL 7:32.1 §.) Tietosuoja ja tietoturva eivät ole siis sama asia, vaan tietosuojalla tarkoitetaan nimenomaan tiedon luottamuksellisuuden säilymistä. Tietoturvalla pyritään puolestaan toteuttamaan tietosuojaa. (Innanen & Saarimäki 2012, 112.) On hyvä huomata, että henkilötietojen tietoturvasta huolehtiminen ei tarkoita pelkästään jälkikäteisiä toimenpiteitä, vaan tietoturvanäkökohdat tulisi ottaa huomioon myös palvelun suunnittelussa (Innanen 2009, 8).

Henkilötietolaissa ei oteta kantaa siihen, mikä on riittävä tekninen suojaustaso, koska tekniikan kehittymistä on vaikea arvioida. Suojaustasoa arvioitaessa on siis toisaalta kiinnitettävä huomiota riittäviin teknisiin keinoihin ja niiden aiheuttamiin kustannuksiin. Toisaalta suojauksen tasoon vaikuttavat käsiteltävien henkilötietojen sisältö. Jos rekisterinpitäjä käsittelee arkaluonteisia tietoja, on sen kiinnitettävä aivan erityisellä tavalla suojaukseen huomiota. (HE 96/1998, 66.) Tietojen laadun lisäksi on otettava huomioon tietojen määrä ja ikä. Rekisterinpitäjän velvollisuus on määritellä tietojen käyttöoikeudet ja käsittelyyn oikeuttavat tavat, kuten tallennus, muuttaminen, haku ja tuhoaminen (HE 96/1998, 66). Voidaankin sanoa, että tämä johtuu osittain teknologiariippumattomasta lainsäädäntötavasta. Tällä mahdollistetaan se, että laki on ajan tasalla teknologian kehittyessäkin. (Salminen 2007, 36.)

Rekisterinpitäjät voivat erilaisilla salasanajärjestelmillä tai vastaavin turvajärjestelmin varmistaa, että tietoja pääsevät käsittelemään vain henkilöt, joilla on siihen oikeus. Samalla voidaan luoda menettelytavat, joiden avulla voidaan seurata tietojen käsittelyä, kuten esimerkiksi sitä, kuka tietoja on käsitellyt ja mitä tiedoille on tehty. Järjestelmän pitäisi olla sellainen, että jos tietoja pääsee käsittelemään laittomasti, se aiheuttaa rekisterinpitäjälle välittömästi hälytyksen. Laittoman yrityksen alkuperä olisi pystyttävä jäljittämään mahdollisuuksien mukaan. (HE 96/1998, 66.)

Jos henkilötietoja on siirrettävä, on varmistettava, että siirto ei aiheuta muutoksia tietojen sisältöön eikä tietoja häviä (HE 96/1998, 66). Henkilötietolaissa tarkennetaan vielä, että mikäli rekisterinpitäjä luovuttaa henkilötietoja teknisin käyttöyhteyksin sille, joka toimii rekisterinpitäjän lukuun tai jollekin muulle taholle, on ennen tietojen luovuttamista annettava riittävät ja asianmukaiset selvitykset tietojen suojaamisesta (HTL 7:21.2 §).

5.2 Vaitiolovelvollisuus ja henkilörekisterin hävittäminen

Jokaista henkilötietojen käsittelijää koskee vaitiolovelvollisuus. Jos käsittelijä on saanut tietää jotakin toisen henkilön ominaisuuksista, henkilökohtaisista oloista tai taloudellisesta asemasta, ei hän saa antaa näitä tietoja ulkopuoliselle (HTL 7:33 §). Tämä vaitiolovelvollisuus koskee käytännössä kaikkia, jotka käsittelevät henkilötietoja. On kuitenkin muutamia poikkeustilanteita, joissa tietoja voidaan antaa sivulliselle. Tällaisia tilanteita ovat esimerkiksi sellaiset, joissa sivullisen ja rekisteröidyn väliseen suhteeseen soveltuu jokin henkilötietojen käsittelyn yleisistä edellytyksistä, kuten rekisteröidyn elintärkeä etu. (Vanto 2011, 154.)

Tämä velvollisuus on voimassa, vaikka salassapito- tai vaitiolosopimusta ei olisikaan erikseen tehty. Erillisellä sopimuksella voidaan toki laajentaa velvollisuutta koskemaan muitakin aloja. Monilla aloilla erityislainsäädäntö puolestaan vaatii salassapito- ja vaitiolovelvoitteet, kuten pankkisalaisuus ja terveydenhuollon ammattihenkilöitä koskevat salassapitovelvollisuudet. (Salminen 2009, 83.)

Rekisterinpitäjän on hävitettävä sellaiset rekisterit, jotka ovat sen toiminnan kannalta tarpeettomia. Mikäli rekisteriin on tallennettu tietoja, jotka on määrätty säilytettäväksi tai niitä ei siirretä arkistoitavaksi, ei rekisteriä tarvitse hävittää. (HTL 7:34 §.) Toisin sanoen kaikki tarpeettomat, virheelliset tai vanhentuneet henkilötiedot on hävitettävä, ellei puutteita voida oikaista. Tämän

lisäksi henkilötietojen hävittäminen edellyttää, että rekisterinpitäjä huolehtii henkilötietojen suojaamisesta vahingossa tai laittomasti tapahtuvalta käsittelyltä. (Salminen 2009, 66.) Tämä säännös asettaa rekisterinpitäjälle velvollisuuden säännölliseen tietohuoltoon. Rekisterinpitäjän on myös arvioitava henkilötietojen käsittelyä toiminnan kehittyessä. Tarpeellisuusvaatimus jo velvoittaa rekisterinpitäjän arvioimaan tietojen tarpeellisuutta nykyhetken mukaan. Kukaan ei pysty arvioimaan tulevaisuutta, joten senkin vuoksi tietohuoltoa on syytä tehdä. (Vanto 2011, 155.) Henkilötietoja ei saa säilyttää sen varalta, että niitä voidaan joskus tarvita. Kun henkilörekisteri hävitetään, on varmistettava, että henkilötiedot häviävät kokonaan. Myös varmuuskopiot on hävitettävä (Vanto 2011, 155.)

Rekisterinpitäjän on jo ennen henkilötietojen käsittelyn aloittamista määriteltävä henkilötietojen säilyttämisen oikeudelliset perusteet sekä henkilötietojen hävittämisen määräajat. Henkilötiedot on hävitettävä, kun niiden käsittelyn oikeudellinen peruste lakkaa tai niiden käsittely muutoin muuttuisi laittomaksi. Asiakassuhteen päättymisen tavat sekä asiakkaan suostumuksen peruuntuminen on syytä huomioida tietojen hävittämistä suunniteltaessa. (Salminen 2009, 66.)

6 OHJEISTUKSEN LAATIMINEN JA JOHTOPÄÄTÖKSET

Toimeksiantaja on pieni organisaatio, jonka työntekijöillä ei ole käytännössä tarvittavaa tietoa henkilötietolainsäädännöstä. Tiedon hakeminen ja ajan tasalla pitäminen on aikaa vievää ja asiaan perehtymättömälle vaikeaa. Opinnäytetyöraportissa haettiin vastausta tutkimusongelmiin: Millaisia oikeuksia laki säätää henkilörekisteriin rekisteröidylle? Mitä velvollisuuksia henkilörekisterin pitäjällä on lain mukaan? Miten henkilötietoja on lain mukaan käsiteltävä?

Opinnäytetyö on rakenteeltaan toiminnallinen ja tietoperustan tutkimusmenetelmänä on lainoppi. Tarpeen ja kokonaisuuden selvittämiseksi on keskusteltu toimeksiantajan työntekijöiden kanssa ja tutustuttu jo olemassa oleviin henkilörekistereihin. Näin on kartoitettu tarvetta ja henkilörekistereiden laajuutta. Opinnäytetyön tutkimusongelmiin löydettiin vastaukset tarkastelemalla keskeisintä lainsäädäntöä, lain esitöitä, oikeuskäytäntöä ja aihetta käsittelevää oikeuskirjallisuutta sekä alan asiantuntijoiden tekemiä oppaita ja tietosuojavaltuutetun toimiston ohjeistuksia. Keskeisimmäksi asiaksi tutkimusongelmien kannalta nousi luonnollisesti henkilötietolain tarkastelu.

Toimeksiantajalla on menneillään iso projekti, jossa luodaan uusia sekä yhdistetään ja hävitetään vanhoja henkilörekistereitä. Jo olemassa olevista henkilörekistereistä löytyy rekisteriselosteet, mutta ne eivät ole täysin ajan tasalla. Henkilörekistereitä on toimeksiantajalla yli kymmenen. Suurin osa niistä on hyvin selkeitä. Niissä kerätään henkilötietoina nimi, osoite ja puhelinnumero. Joukkoon mahtuu kuitenkin henkilörekistereitä, joissa on henkilötunnuksia ja muita arkaluonteisia tietoja. Toimeksiantajan henkilörekisterit ovat aktiivisessa käytössä koko ajan, mutta niiden ohjeistus on jäänyt muutosten keskellä päivittämättä. Henkilörekisterit on siirretty vuorollaan atk-järjestelmiin, jolloin tietoturvakysymykset ovat nousseet tärkeälle sijalle. Käyttötarkoitus ei ole henkilörekistereissä vuosien varrella muuttunut, mutta tietojen keräämistapa on.

Opinnäytetyön tuloksena on tehty ohjeistus. Toimeksiantajan toiveesta ohjeistuksesta tehtiin kattava ja hyvin selkeä. Ohjeistuksen rakentaminen lähti siitä, mitä täytyy ottaa huomioon henkilörekisterin suunnittelussa, ylläpidossa ja hävittämisessä. Ohjeistuksen pohjana ovat rekisteröidyn oikeudet, mutta koko ajan myös lain asettamat rekisterinpitäjän velvollisuudet, koska ne eivät sulje toisiaan pois, vaan päinvastoin täydentävät toisiaan. On hyvä tiedostaa, että rekisteröidyllä on paljon oikeuksia, joihin on rekisterinpitäjän pystyttävä vastaamaan.

Ohjeistuksessa on pyritty etenemään loogisesti alkaen henkilötietorekisterin perustamisesta päättyen henkilörekisterin rekisterinpitäjän sisäiseen ohjeistukseen (ks. liite 1). Henkilörekisterin aloittamisvaiheessa on määritettävä rekisterinpitäjä ja vastuuhenkilö. Vastuuhenkilöksi on hyvä määritellä sellainen henkilö, joka työtehtäviinsä ja asemaansa liittyen vastaa siitä, että rekisteritoiminnot suunnitellaan ja toteutetaan säännösten ja määräysten mukaisesti. Vastuuhenkilö toimeksiantajalla tulee siis olemaan eri henkilörekistereissä eri henkilö. Näin voidaan saavuttaa henkilörekistereiden lainmukaisuus ja toimivuus parhaalla mahdollisella tavalla. Henkilörekisterille on myös pyrittävä antamaan nimi, joka kuvaa rekisteriä mahdollisimman kattavasti.

Henkilötietojen käsittelyn yleiset periaatteet on pyritty huomioimaan koko ohjeistuksessa. Tärkeimpänä periaatteena ja lähtökohtana onnistuneelle henkilörekisterille on sen hyvä ja perusteellinen suunnittelu. Suunnitteluvelvollisuuden lähtökohtana on henkilötietojen keräämisen ja käsittelyn tarkoitus eli se, mitä rekisterinpitäjän tehtävää varten henkilötietoja kerätään ja tallennetaan. Tähän kiteytyy henkilörekisterin tarve ja olemassaolo. On hyvä muistaa, että loogiseen henkilörekisteriin kuuluvat kaikki erikseen pidettävät osarekisterit ja tiedostot. Toimeksiantajalla on esimerkiksi yksi isompi henkilörekisteri, jota ylläpitää useampi henkilö omilla alueillaan. He ottavat käyttöön osan henkilörekisteristä muokatakseen ja ylläpitääkseen sitä, ja kun se on valmis, he korjaavat tiedot isoon henkilörekisteriin. Kyseessä on tällöin henkilörekisteri, johon kuuluu osarekistereitä.

Henkilötietojen käsittelyn tarkoitusta mietittäessä on hyvä pohtia, riittäisivätkö tiedot ilman tunnistamistietoja. Tilastointia ja tutkimusta varten voidaan aina käyttää henkilötietoja, vaikka sitä ei olisi henkilörekisterin käyttötarkoituksessa erikseen mainittukaan. Käyttötarkoitusta voidaan myöhemmin muuttaa, mutta se ei missään nimessä saa olla sopimaton tai ristiriidassa alkuperäisen käsittelyn tarkoituksen kanssa. Tämä ei tule olemaan ongelma, mikäli henkilörekisterit ovat selkeitä ja turhia henkilörekistereitä pyritään välttämään.

Laissa henkilötietojen käsittelylle asetettujen yleisten edellytysten tarkoituksena on luoda perusta henkilötietojen käsittelylle. Kun rekisteröity antaa suostumuksensa tietojensa käsittelylle, henkilötietoja voidaan lähtökohtaisesti käsitellä. Tässä on kuitenkin tärkeä muistaa, että rekisteröidyllä on aina itsemääräämisoikeus, eli tietojen antaminen perustuu vapaaehtoisuuteen. Tietojen antaminen on tietoinen tahdonilmaisu ja yksilöity. Rekisteröidyllä täytyy olla tarpeeksi tietoa, mihin hän antaa suostumuksensa ja mihin hänen tietojaan käytetään. Viime kädessä rekisterinpitäjällä on todistustaakka siitä, että rekisteröidyn suostumus on saatu. Rekisteröidyn suostumus on keskei-

senä osana toimeksiantajan henkilörekistereitä. Internet-palveluissa suostumuksen saaminen voidaan saada edellyttämällä rekisteröityä merkitsemään rekisteröitymisen yhteydessä tietojenkeruulomakkeen kohta, jossa suostumuksen sisältö on riittävän yksiselitteisesti yksilöity. Käytännössä suostumuksen saaminen ei edellytä kovinkaan suuria toimenpiteitä, mutta toivon, että tähän kiinnitetään huomiota. Toimeksiantajan muut henkilötietojen käsittelyn edellytykset tulevat kysymykseen silloin, kun se hoitaa lakiin perustuvaa toimeksiantoa. Näitä henkilörekistereitä ei ole kuin muutama, ja tällöinkin toimeksiantajalla on mahdollisuus saada rekisteröidyltä suostumus.

Asiallisen yhteyden syntyminen rekisteröidyn ja rekisterinpitäjän välillä on luonteva tapa käsitellä henkilötietoja. Kysymys on tällöin asiakassuhteesta. Tällainen tilanne voi syntyä esimerkiksi verkkokaupassa, kun asiakas tilaa tuotteen ja antaa siinä henkilötiedot laskuttamista ja tilauksen toimittamista varten. Erillistä suostumusta ei tällöin tarvita. Henkilötietojen käsittely on sallittua myös silloin, kun rekisterinpitäjä antaa tiedot toimeksiantona kolmannen osapuolen hoidettavaksi, esimerkiksi palkanmaksua varten. Tähän ei tarvita rekisteröidyn erillistä suostumusta. Muut käsittelyn yleisten edellytysten kohdat eivät tule kysymykseen toimeksiantajan kohdalla.

Rekisterinpitäjän on mietittävä, miten hän kerää henkilötiedot henkilörekisteriin. Yleisimpiä tapoja on kerätä tiedot rekisteröidyltä itseltään. Tietoja voidaan toki täydentää myöhemmin, mutta silloin on muistettava, että tästä on informoitava rekisteröityä. Toimeksiantajan henkilötiedot kerätään pääsääntöisesti rekisteröidyiltä itseltään.

Tiedon laatua koskevat edellytykset ovat henkilötietojen tarpeellisuus ja virheettömyys. Suurena haasteena toimeksiantajalla on, miten tietoja päivitetään henkilörekisteriin, ja tehdäänkö päivitys kaikkiin henkilörekistereihin. Atk-järjestelmiin tietoja kirjatessa on varmistettava tarpeellisesta tietosuojauksesta. Tietojärjestelmien arkkitehtuurilla voidaan omalta osaltaan varmistaa tiedon virheettömyys ja tarpeellisuus (ks. liite1). Virheelliset tiedot tulee saada korjatuksi. On hyvä miettiä, miten saavutetaan oma-aloitteisesti mahdollisimman virheettömät tiedot sekä miten virheet korjataan. Riittääkö, että virheet korjataan, kun rekisteröity ottaa yhteyttä vai tehdäänkö tarkastuksia säännöllisesti? On hyvä miettiä etukäteen aikataulu ja antaa vastuuhenkilön tehtäväksi virheiden korjaaminen. Henkilötietojen virheettömyys voidaan nähdä myös rekisteröidyn oikeutena laadukkaaseen tietoon ja toimintaan.

Henkilötunnusten ja arkaluonteisten tietojen kanssa on oltava hyvin tarkka eikä niitä saa kerätä kuin muutamissa tapauksissa lain säätämissä puitteissa. Toimeksiantaja kerää näitä tietoja muutamissa henkilörekistereissä ja niissä molemmissa tämä perustuu lakiin. Henkilötunnusten ja arkaluonteisten tietojen perusteesta on hyvä olla maininta rekisteriselosteessa. Yleisin syy henkilötunnusten keräämiseen on laskutukseen liittyvä tarve. Arkaluonteisten tietojen keräämiseen puolestaan terveyteen liittyvien tietojen tarve. Tällaisissa tilanteissa erityislainsäädäntö mahdollistaa näiden tietojen keräämisen ja käyttämisen.

Rekisteriselosteen laatiminen on laaja ja merkittävä osa informointia rekisteröidylle. Rekisteriselosteesta ja tietosuojaselosteesta on toimeksiantajan pyynnöstä erillinen ohje (ks. liite 2). Rekisteriselosteissa on ilmennyt puutteita toimeksiantajalla. Rekisteriselosteet olisi hyvä tarkistaa, jotta ne ovat ajan tasalla ja täyttävät lain asettamat vaatimukset. Ohjeistuksessa on pyritty ottamaan huomioon rekisteriselosteiden tarve ja korostettu niiden tärkeyttä. Lakihan kuitenkin antaa selkeät minimivaatimukset rekisteriselosteille. Useissa rekistereissä pelkkä rekisteriseloste ei riitä vaan tarvitaan tietosuojaseloste, koska toimeksiantaja toimii internetissä.

Ohjeistuksessa on otettu kantaa tietojen luovuttamiseen, vaikka toimeksiantaja ei tässä vaiheessa luovuta tietoja eteenpäin, eli tietoja käytetään vain omaan toimintaan. Rekisteriselosteessa on oltava maininta, luovutetaanko tietoja eteenpäin. Toimeksiantaja käyttää tietoja omaan mainontaansa, mutta siihen pyydetään lupa rekisteröidyltä. Varsinaiseen suoramarkkinointiin tietoja ei luovuteta. Mikäli tietoja luovutettaisiin suoramarkkinointiin, rekisteröity voisi käyttää kielto-oikeuttaan.

Henkilötietojen käsittelystä ja keräämisestä on informoitava tarpeeksi rekisteröityvää. On mietittävä, mistä informoidaan, mitä informoidaan ja miten informoidaan. On tärkeä muistaa, että mikäli käyttötarkoitusta muutetaan, on siitä informoitava rekisteröityjä. Informointi täytyy olla osa henkilörekistereiden toimintaa. Informointi on yksi rekisteröidyn oikeuksista, eikä sitä voi olla korostamatta liikaa. Sama koskee myös tarkastusoikeutta. Tarkastusoikeus on jokaisen rekisteröidyn oikeus, mutta tätä käytetään yllättävän vähän. Siitä huolimatta siihen on hyvä varautua. Tarkastusoikeutta ei toimeksiantajan kohdalla ole tähän mennessä vielä kukaan käyttänyt eikä siihen ole varauduttu. Koska henkilörekistereitä on paljon, olisi syytä laatia ohje, miten tarkastusoikeuteen vastataan. Tarkastuspyynnöstä voidaan laatia valmis lomake, jonka rekisteröity täyttää käyttäessään tarkastusoikeutta. Tarkastusoikeuden suhde muihin tiedonsaantioikeuksiin on syytä tiedos-

taa, sillä tarkastusoikeudesta voidaan periä kohtuullinen hinta, mikäli rekisteröity käyttää sitä useamman kerran vuodessa.

Tietosuoja on osa tietoturvallisuutta ja keskeinen osa henkilörekistereitä. Ohjeistuksessa on otettu huomioon niin tietoturvallisuus kuin tietosuojakin. Lisäksi on keskitytty käymään läpi myös henkilörekisterien sisäistä käyttöä, henkilörekisterien säilyttämistä, hävittämistä ja yhdistämistä sekä henkilörekisterien hallinnointia (ks. liite 1). Henkilörekisterien suojaamisessa on tärkeää pyrkiä mahdollisimman laajaan ja hyvään tietoturvallisuuteen. Tärkeintä on pyrkiä suojaamaan mahdollisimman hyvin rekisteröidyn yksityisyyttä. Suojaamisen tasoon vaikuttaa rekistereiden tietojen arkaluonteisuus: rekisterit, jotka sisältävät arkaluonteisia tietoja tai henkilötunnuksen, on suojattava paremmin. Tietoturvakysymykset ovat toimeksiantajalla hyvin tiedossa ja hallinnassa, mutta mielestäni niitä ei koskaan korosteta liikaa. Suurin tietoturvariski on kuitenkin yleensä ihmiset, jotka tietoja käsittelevät. Ohjeistus toivottavasti kiinnittää toimeksiantajan huomiota siihen, että henkilöstöä on koulutettava ja heille on laadittava riittävä ohjeistus tietoturvakysymyksistä. Näin pystytään varmistamaan riittävä ja hyvä tietoturva. Ei riitä, että henkilörekistereiden käyttö on kunnossa, kun asioidaan rekisteröityjen kanssa, vaan on otettava huomioon myös henkilörekistereiden sisäinen käyttö. Näen tämän yhtenä suurena tietoturvariskinä, koska käyttäessämme tietoja unohdamme helposti, että nämä tiedot on annettu meille tiettyä toimintaa varten. Ohjeistuksessa käsitellään myös henkilörekistereiden sisäistä käyttöä, johon on pyritty poimimaan koko henkilötietolain keskeisimmät vaatimukset, kuten käyttötarkoitussidonnaisuus, huolellisuusvelvoite, suojaamisvelvoite, salassapitosäännökset ja muut mahdolliset säännökset, koska nämä asettavat henkilörekistereille ja henkilötiedoille omia vaatimuksia. Myös sisäisessä käytössä on huomioitava tulosteiden tietosuojakysymykset.

Henkilörekisterien ja ennen kaikkea henkilötietojen säilyttäminen, arkistointi ja hävittäminen ovat iso osa henkilörekistereiden tietoturvallisuutta. Ohjeistuksessa on pyritty ottamaan useampi näkökulma henkilötietojen säilyttämiseen ja arkistoitiin (ks. liite 1). Onko kaikkia tietoja edes tarpeen säilyttää ja arkistoida? Henkilörekistereissä on hyvin monenlaisia tietoja, mihin vaikuttaa useampi lainsäädäntö. Yhtä oikeaa vastausta ei ole, vaan jokaista henkilörekisteriä ja niiden tietoja on arvioitava kunkin henkilörekisterin kannalta erikseen. Tavoite on kuitenkin, että mitään tietoja ei säilytettäisi kauempaa kuin on tarpeen.

Joskus tullaan tilanteeseen, jossa mietitään ja nähdään tarpeelliseksi yhdistää henkilörekistereitä. Toimeksiantajalla on mietitty tätä vaihtoehtoa hyvinkin pitkään. Tärkeintä tässä on määritellä ja

arvioida tarkkaan, mikä on saatu hyöty, ja muistaa säilyttää henkilörekistereiden lainmukaisuus. Laki ei kiellä henkilörekistereiden yhdistämistä, eikä lainsäädännöllä ole estetty tai ohjeistettu henkilörekistereiden yhdistämistä. Henkilörekistereiden käyttötarkoitussidonnaisuus ja rekisteröityjen informointi on kuitenkin tässä tärkeää huomioida.

Opinnäytetyön tuotoksena syntyneet ohjeistukset tulevat toimeksiantajan jokapäiväiseen käyttöön. Opinnäytetyö on ajankohtainen ja tarpeellinen sellaisille, jotka kamppailevat lainsäädännön tulkinnanvaraisuuden vuoksi. Opinnäytetyön rajauksen vuoksi työ ei ole kovin laaja ja jättää ulkopuolelle useita mielenkiintoisia ja tärkeitä asioita kuten arkistoinnin ja tietojen säilyttämisen arvioinnin.

Opinnäytetyön tuotoksena syntyneiden ohjeistusten toteuttamisen lähtökohtana oli toimeksiantajan todellinen tarve. Toimeksiantajani tarvitsee selkeän ohjeistuksen, johon on kerätty toimeksiantajan toimihenkilöitä varten keskeinen lainsäädäntö. Ohjeistuksen sisältö rakentui opinnäytetyön rakenteen ympärille, noudattaen samaa asioiden käsittelyjärjestystä. Ohjeistuksessa on käytetty lisäksi lähteenä toimeksiantajan omia sisäisiä periaatteita, jotka eivät sisälly tämän työn teoriaosuuteen. Ohjeistuksen ensisijainen käyttötarkoitus on ohjelmistoprojektin toteuttajien sekä toimeksiantajan toimihenkilöiden käsikirjana toimiminen. Tämän vuoksi ohjeistuksen on tärkeää olla asiallinen. Sovimme myös, että tekstin raskaslukuisuuden vuoksi tekstistä jätetään lähdeviittaukset pois. Tarkemmat tiedot käytetyistä lähteistä ovat kuitenkin löydettävissä tämän opinnäytetyön teoriaosuuden yhteydestä.

Pääsääntöisesti ohjeistusta ei kuitenkaan ole tarkoitettu pikaoppaaksi, vaan tuhdiksi työvälineeksi henkilörekisterien ylläpitämiseen, suunnitteluun ja hävittämiseen. Ohjeistuksen sisällöllisenä lähtökohtana haluttiin pitää vahva lainsäädännöllinen ote. Ohjeistukseen on poimittu opinnäytetyön teoriaosuudesta keskeisimmät asiat, ja tietoja on yhdistetty toimeksiantajan oman sääntelyn kanssa. Ohjeistuksesta tulee olemaan suuri hyöty henkilörekisterilainsäädäntöä tuntemattomalle ja muutenkin lainsäädäntöön perehtymättömälle.

Lopullisena yhteenvetona voisi todeta, että henkilötietolaki kuitenkin onnistuu säätelemään henkilörekisterien toimintaa riittävästi. Henkilötietolain vähimmäisvaatimukset pitävät toimeksiantajan oman harkintavallan juuri riittävän väljänä, mutta kuitenkin tarpeeksi yhtenäisenä. Se on aivan riittävän tarkka, jotta kaikki erilaiset rekisterinpitäjät pystyvät joustavasti toimimaan omalla alallaan.

7 POHDINTA

Aiheen opinnäytetyölleni sain toimeksiantajalta useista ja hyvin erilaisista vaihtoehdoista. Mietimme sekä toimeksiantajan että ohjaajani kanssa, mikä aihe olisi koulutukseni ja toimeksiantajan kannalta järkevin. Kokonaisuudeltaan, laajuudeltaan ja järkevyydeltään päädyimme tähän aiheeseen.

Tämän tutkimuksen myötä on avartunut oma näkemykseni henkilörekistereiden merkityksestä toimeksiantajalla. Laki asettaa selkeitä ohjeita, mutta jättää paljon vastuuta myös rekisterinpitäjälle, etenkin tietoturvallisuuteen ja tietosuojaan nähden. Ohjeistuksen rakentaminen oli minulle tärkein ja avartavin kokemus koko opinnäytetyöprojektissa. Ohjeistuksen tekemisen myötä jouduin altistamaan itseni näkemään enemmän kuin tietoperusta mahdollisti, miettimään kokonaisuutta ja myös uusia mahdollisuuksia koko organisaation kannalta.

Mielenkiintoisinta oli rakentaa ohjeistus, joka palvelisi yksinkertaisuudellaan toimeksiantajaa mahdollisimman hyvin. Jouduin soveltamaan tietoperustaa kokonaisuudeksi, jossa on otettu huomioon niin toimeksiantajan sisäinen rekistereiden käyttö kuin myös rekistereiden käyttö ulospäin. Ohjelmistoprojektin myötä ollaan suunnittelemassa uutta kokonaisuutta, jossa päästään luomaan kokonaan uutta henkilötietojärjestelmää. Ohjeistuksen olisi kuitenkin palveltava myös jo voimassaolevia rekistereitä. Näin tämän todelliseksi haasteeksi, mutta onnistuin mielestäni siinä hyvin.

Oma aiempi työkokemukseni eri yritysten asiakaspalvelutehtävissä on ollut suureksi avuksi hahmottaessani kokonaisuutta ja henkilötietojen käsittelyn merkitystä. Etenkin tietosuoja- ja tietoturvakysymykset ovat oman työkokemukseni kautta olleet helpommin ymmärrettävissä. Asiakaspalvelu on lähellä sydäntäni ja sen tuoma työkokemus auttaa ymmärtämään haasteita, joita kohdataan tietojen antamisessa ja asiakkaan varmistamisessa puhelimitse ja sähköpostitse.

Tutkimukseni tekeminen toimeksiantajan tiloissa on auttanut ymmärtämään työn merkityksen ja hahmottamaan laajaa projektia. Rekistereiden laajassa viidakossa niiden merkitys on saanut uuden suunnan. Tutkimukseni on tuonut selkeyttä ja kaivattua ohjeistusta siitä, mitä kaikkea on otettava huomioon rekistereitä suunniteltaessa ja ylläpidettäessä. Henkilötietojen hävittäminen ja rekistereiden läpikäynti auttavat rekistereiden tietoturvallisuutta. Tulen jatkamaan projektia vielä

opinnäytetyön valmistumisen jälkeen ja pääsen näkemään työn merkityksen ja toimivuuden käytännössä. Olisikin mielenkiintoista myöhemmin tutkia, miten ohjeistus on toiminut käytännössä sekä perehtyä arkistointilakiin ja tietoturvallisuuskysymyksiin laajemmin ja yksityiskohtaisemmin.

Aikataulullisesti opinnäytetyöni aloitus kesti kauan, mutta varsinaisen työn tekeminen onnistui varsin nopeasti, kun pääsin tekemään työtäni toimeksiantajan tiloihin. Aloitusta hidasti kokonaisuuden hahmottamisen vaikeus ja töiden liiallinen tekeminen opinnäytetyön ohessa. On ollut kuitenkin ilo huomata, miten työ on tuonut paljon uusia ajatuksia ja ideoita ja herättänyt minussa tutkijan esiin. Välillä motivaatiota on toki haettu kovasti, mutta työn merkitys toimeksiantajalle on antanut motivaatiota ja auttanut työssä eteenpäin.

LÄHTEET

EU vahvistaa yksityisyyden suojaa verkkoympäristössä 2012. Euroopan komissio. Hakupäivä 20.2.2013. http://ec.europa.eu/news/business/120125_fi.htm.

Euroopan parlamentin ja neuvoston direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla, 12.7.2002, 2002/58/EY.

Euroopan unionin perusoikeuskirja, 30.3.2010 EUVL C 83, 30.3.2010.

Hallituksen esitys Eduskunnalle laiksi henkilötietolain muuttamisesta. HE 96/1998. Hakupäivä 23.11.2012. http://www.finlex.fi

Henkilötietolaki 22.9.1999/523

Hämeenlinnan HAO 3.11.2000/00/369/3. Finlex.

Innanen, A. 2009. Internetin yhteisöpalveluihin sovellettavasta lainsäädännöstä. Hakupäivä 5.2.2013. http://www.edilex.fi.ezp.oamk.fi:2048/lakikirjasto/6610.pdf

Innanen, A. & Saarimäki, J. 2012. Internetoikeus. Porvoo: Bookwell Oy.

Järvinen, P. 2010. Yksityisyys, turvaa digitaalinen kotirauhasi. Jyväskylä: WSOYpro Oy.

Koskinen S., Alapuronen L., Heino A-M & Salli M. 2005. Henkilötietojen käsittely työelämässä. Edita Publishing Oy.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Laki terveydenhuollon valtakunnallisista henkilörekistereistä 9.6.1989/556.

Lapsen oikeuksien yleissopimus 20.11.1989/44.

Perusopetuslaki 21.8.1998/628

Pesonen, P. 2008. Viestintäoikeuden käsikirja. Helsinki: Edita.

Salminen, J. 2008. Näkökulmia Perusoikeuksiin. Helsinki: Hakapaino Oy.

Salminen, M. 2009. Tietosuoja sähköisessä liiketoiminnassa. Talentum.

Sisäministeriö. Sisäministeriö pyytää Poliisihallitukselta selvitystä poliisiyksiköiden välisistä yhteistyöongelmista ja henkilötietojen käsittelystä, 2013. Hakupäivä 12.4.2013. http://www.intermin.fi/fi/ajankohtaista/uutiset/1/1/sisaministerio_pyytaa_poliisihallitukselta_selvitysta_poliisiyksikoiden_valisista_yhteistyoongelmista_ja_henkilotietojen_kasittelysta_2

Suomen Perustuslaki 11.6.1999/731

Sähköisen viestinnän tietosuojalaki 16.6.2004/516.

Tietosuojavaltuutettu a. Tietosuojavaltuutetun toimisto. Hakupäivä 29.11.2012. http://www.tietosuoja.fi/index.htm.

Tietosuojavaltuutettu b. Henkilörekisteriin talletettujen tietojen tarkastaminen. Hakupäivä 20.2.2013. http://www.tietosuoja.fi/uploads/xu4bctu2f6n0kq.pdf

Tietosuojavaltuutettu c. Laadi tietosuojaseloste. Hakupäivä 25.3.2013. http://www.tietosuoja.fi/uploads/azf9gjle_1.pdf.

Tietosuojavaltuutettu d. Tietoa rekisterinpitäjälle. Hakupäivä 29.11.2012. http://www.tietosuoja.fi/1698.htm#kohta8.

Tietosuojavaltuutettu e. Tietosuojavaltuutetun kannanotto ammattiyhdistyksen jäsenten sähköpostiosoitteen julkaiseminen Internetissä. Hakupäivä 4.2.2013. Http://www.tietosuoja.fi/13807.htm.

Tietosuojavaltuutetun kannanotto 16.8.2000. Dnro 649/41/2000. http://www.tietosuoja.fi/13805.htm

Tietosuojalautakunnan päätös 7/26.3.1990.

Vanto, J. 2011. Henkilötietolaki käytännössä. WSOYpro Oy.

Yhdistyneiden kansakuntien peruskirja, 16.12.1966.

LIITTEET

LIITE 1 Ohjeistus henkilörekistereille

LIITE 2 Rekisteriseloste ja tietosuojaselosteen ohjeistus

Opinnäytetyö löytyy osoitteesta www.theseus.fi

LIITE 1 OHJEISTUS HENKILÖREKISTEREILLE

Ohjeistus henkilörekistereille

1. Rekisterinpitäjä ja rekisterin vastuuhenkilö
    - henkilö, yhteisö tai säätiö, jonka käyttöä varten ko. rekisteri perustetaan
    - rekisterinpitäjän nimi, on kuvattava rekisterin käyttötarkoitusta
    - vastuuhenkilö määrää rekisterin käytöstä
    - vastuuhenkilö vastaa rekisterin suunnittelusta ja toteutuksesta säännösten, määräysten yleisohjeiden mukaisesti
    - vastuuhenkilölle voidaan esittää tiedusteluja, esim. tarkastusoikeus
2. Rekisterin nimi
    - on kuvattava hoidettavia tehtäviä
3. Suunnitteluvelvollisuus
    - tärkein vaihe!
    - rekisteri on asiallisesti perusteltava, eli miksi ko. rekisteri tarvitaan, rekisterin oltava asianmukainen
    - mietittävä, mistä tiedot hankitaan ja mitä tietoja kerätään
    - mihin tietoja luovutetaan
    - rekisterin tarkoitus, katso tarkemmin seuraava kohta
4. Henkilötietojen käsittelyn tarkoitus
    - henkilötietojen käsittelyn tarkoitus on määriteltävä siten, että määrittelystä käy ilmi, minkä rekisterinpitäjän tehtävää varten tietoja kerätään ja käsitellään
    - loogiseen rekisteriin kuuluvat kaikki kussakin tehtävässä käytettävät, teknisesti erikseenkin pidettävät osarekisterit ja tiedostot
    - asianmukaisuusvaatimus
    - arvioitava ennen määrittelyä, edellyttäkö tehtävän hoito henkilöiden tunnistamistietojen keräämistä, vai riittäisivätkö ilman tunnisteita olevat tiedot
    - ei saa olla suunnitteluvelvoitteen käsittelyn tarkoituksen vastainen (katso kohta 3)
    - henkilötietoja voidaan käyttää tilastointiin tai tieteelliseen tutkimukseen, ilman että sitä on määritelty erikseen
    - voidaan määritellä uudelleen, jos rekisterinpitäjän toiminnan olosuhteet muuttuvat ja on näin ollen tarpeen, mutta ei saa olla yhteen sopimaton alkuperäisen tarkoituksen kanssa
5. Henkilötietojen käsittelyn yleiset edellytykset
    - määriteltävä ja perusteltava oikeus henkilötietojen käsittelyyn rekisterin perustamiseen ja ylläpitämiseen
    - rekisteröidyn suostumus
        - rekisteröidyllä itsemääräämisoikeus
        - avoimuus (rekisteriseloste)
        - tarvitaan pätevä suostumus
            - vapaaehtoinen
            - yksilöity
            - tietoinen tahdon ilmaisu

        - edellyttää laajaa informaatiota, eli mihin rekisteröity antaa suostumuksen
        - viime kädessä todistustaakka rekisterinpitäjällä
        - tiedon laadulla merkitys
    - säännökset: omat, että muualta tulevat ohjeet, esim. perustuu lakiin
    - voi perustua myös asiakassuhteeseen, eli kyseessä on rekisteröidyn ja rekisterinpitäjän välillä oleva asiallinen yhteys, esim. verkkokauppa
6. Rekisterin tietolähteet
    - mitkä ovat rekisterin tietolähteet, niiden lainmukaisuus sekä tietojen hankkimisessa noudatettavat menettelytavat
    - tietolähteet selvitettävä ja määriteltävä sekä perustamis- että ylläpitovaiheen osalta
        - mistä tietoja hankitaan
        - mitä tietoja hankitaan ja voidaanko lainmukaisesti hankkia
        - millä perusteella tietoja voidaan saada (säännös, suostumus, suostumusmallit, katso kohta 5)
        - miten tietot hankitaan – menettelytavat
        - millä tavoin tiedot pyydetään
        - millä tavoin rekisteröityjä informoidaan rekisteriin talletetuista, muualta kuin häneltä itseltään hankituista tiedoista
        - millä tavoin tietolähteitten käyttö kirjataan
7. Rekisterin tietosisältö (tiedon laatua koskevat edellytykset)
    - suunniteltava ja perusteltava henkilörekisterin tietosisältö sekä sen lainmukaisuus
    - tarpeellisuusvaatimus on täytyttävä
    - onko arkaluonteisten tietojen, esimerkiksi terveystiedot, rotu, rikollinen teko, ja henkilötunnuksen kerääminen ja tallentaminen lainmukaista
    - ovatko rekisterin tiedot virheettömiä, ja miten virheettömyys varmistetaan
    - suunniteltava ja määriteltävä, onko kaikki rekisterit ja tiedot tarkoituksenmukaisia ja tietosuojan kannalta perusteltua tallettaa atk:lle vai manuaalisesti
    - suunniteltava tietojärjestelmien tietoarkkitehtuuri mm. toiminnan tarpeiden luovutusten, suojausvaatimusten ja mahdollisten salassapitosäännösten kannalta
8. Rekisteriselosteen laatiminen ja saatavilla pitotapa
    - jokaisesta henkilörekisteristä tulee laatia rekisteriseloste
    - rekisteriseloste tulee pitää jokaisen saatavilla rekisterinpitäjän toimipaikassa
    - suositeltavaa on laittaa rekisteriseloste rekisterinpitäjän kotisivuille
    - erillinen ohje
9. Henkilötietojen luovutukset, kielto-oikeus
    - määriteltävä ja perusteltava henkilötietojen luovutukset sekä luovutusten lainmukaisuus
    - onko henkilötietojen luovuttaminen tarpeellista
    - määriteltävä
        - mihin tai kenelle tietoja luovutetaan
        - mitä tietoja voidaan lainmukaisesti luovuttaa (ml. tarpeellisuusvaatimus)
        - millä perusteella tietoja luovutetaan (säännös, suostumus)
        - onko tiedot salassa pidettäviä
        - millä tavoin tiedot luovutetaan

        - luovutusta pyytäviltä vaadittavat selvitykset ja pyynnön muotovaatimukset
        - luovutusten menettelytavat, niiden asianmukaisuus ja suojaus
        - huomio erityisesti sähköiseen tiedonsiirtoon liittyvät tietosuoja- ja tietoturvavaatimukset
    - määriteltävä mahdollisesti kysymykseen tulevan kielto-oikeuden toteutus
        - koskee suoramainontaan, etämyyntiä, markkina- ja mielipidetutkimusta, henkilömatrikkelia ja sukututkimusta
10. Rekisteröidyn informointi
    - suunniteltava
        - mistä informoidaan
        - milloin informoidaan
        - miten informointi toteutetaan: määritellään menettelytavat/lomakkeet
        - mahdolliset poikkeukset toiminnasta, perustelut
11. Rekisteröidyn tarkastusoikeus
    - selvitettävä asiaa koskevat säännökset
        - määriteltävä ne tilanteet, joissa tarkastusoikeus tapauskohtaisesti voidaan mahdollisesti evätä
        - määriteltävä, miten tarkastusoikeus toteutetaan rekisteröidyn pyynnöstä
        - toimittaako rekisterinpitäjä tiedot oma-aloitteisesti
        - suunniteltava, missä ajassa tarkastusoikeus toteutetaan
        - suunniteltava tarkastusoikeuden esittämiseen, organisointiin ja toteuttamiseen liittyvät menettelytavat
            - tarkastuspyynnön muotovaatimukset (hyvä laatia mallilomake)
            - kuka vastaanottaa pyynnöt, kuka päättää, kuka ja miten toteutetaan
            - tarkastusoikeuden epäämisestä annettava todistus
        - selvitettävä tarkastusoikeuden suhde ja ero muihin tiedonsaantioikeutta koskeviin säännöksiin
12. Tiedon korjaaminen
    - suunniteltava millä tavoin tietojen virheettömyydestä ja niiden korjaamisesta huolehditaan oma-aloitteisesti sekä tietojen virheettömyyden varmistamismenettelyt
    - suunniteltava, millä tavoin ja miten virhe korjataan
        - normaalin ylläpitomenettelyn yhteydessä
        - muulla tavoin, miten
        - missä ajassa virhe korjataan
        - millä tavoin virhe korjataan
    - suunniteltava, millä tavoin virheen korjaaminen organisoidaan ja toteutetaan: kuka vastaanottaa pyynnöt, kuka päättää, kuka toteuttaa
13. Rekisterin suojaaminen
    - mietittävä rekisterinpidon turvaamisen periaatteet ja suunniteltava tietojen suojaamisen toteutustavat ja ratkaisut
    - huomioitava rekisterinpidon suojaamisen, tietoturvallisuuden ja näiden valvonnan vastuut
    - huomioitava rekisterin arkaluonteiset tiedot ja salassa pidettävyys
    - määriteltävä henkilötietojen käytön ja mahdollisten tiedon siirron tarpeiden pohjalta järjestelmän rakenteet ja tietoryhmät
    - laadittava ohjelmistojen ja laitteiden käyttöä ja muuttamista sekä sijaintia koskevat ohjeet

- huolehdittava tietoturvallisuuden toteutumisesta kaikissa käsittelyvaiheissa ja kaikkien laitteiden ja ohjelmien osalta
- laadittava rekisterin käyttöä ja käyttövaltuuksia sekä niiden muuttamista koskevat ohjeet ja säännöt
    - määriteltävä käytön rekisteröinnin ja valvonnan periaatteet
    - määriteltävä käyttäjien valvonnan periaatteet
- laadittava tietovälineiden käsittelyä (ml. hävittäminen) koskevat ohjeet
- laadittava ohjeet ja säännöt henkilörekisterin käsittelylle tietoverkossa ja tietoliikenteen välityksellä
- laadittava ohjeet rekisterien fyysistä suojaamista varten (tilat, lukitukset, kuluvalvonta yms.)
- laadittava ohjeet tietojen luovutusmenettelystä sekä sisäisessä kuljetuksessa ja muussa sisäisessä toiminnassa noudatettavista menettelyistä
- pyydettävä henkilöstöltä erillinen salassapitosopimus, jossa on todettava myös mahdollinen lainsäädäntöön perustuva salassapitovelvollisuus

14. Rekisterien yhdistäminen
    - selvitettävä ja määriteltävä rekisterien yhdistämistarve ja yhdistämisen lainmukaisuus
    - määriteltävä yhdistettäväksi aiotut rekisterit
    - arvioitava yhdistämisen tuloksena syntyneen rekisterin lainmukaisuus
    - suunniteltava yhdistämisen toteutustapa
    - muistettava rekistereiden käyttötarkoitussidonnaisuus sekä rekisteröityjen informointi
15. Henkilörekisterien ja rekisteritietojen säilytys, arkistointi ja hävittäminen
    - suunniteltava ja arvioitava rekisterien ja niiden sisältämien henkilötietojen säilyttämisajat ja niiden lainmukaisuus
    - määriteltävä rekisteriä koskevat säännökset ja määräykset: mihin säilyttäminen ja mahdollinen arkistointi perustuu
    - arvioitava, miten pitkään henkilörekisteri ja sen eri tiedot ovat toiminnan kannalta tarpeellisia
    - selvitettävä, 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
    - suunniteltava, millä tavoin ja missä tiedot arkistoidaan
    - suunniteltava, miten henkilörekisterit ja niiden tiedot hävitetään
        - päivittäistoiminnassa syntyvän aineiston hävittäminen
        - arkistoidun aineiston hävittäminen
        - hävittämistä koskevat sopimukset
16. Rekisterin sisäinen käyttö
    - määriteltävä rekistereiden sisäisen käytön säännökset ja niiden merkitys sisäisessä käytössä –käyttötarkoitussidonnaisuus
    - salassapitosäännökset
    - huolellisuusvelvoite
    - suojaamisvelvoite
    - mahdolliset erityissäännökset
        - määritellään rekisterin käyttötarkoituksen pohjalta rekisterien erilaiset käyttötavat
    - suunnitellaan tarvittavat tulosteet sekä niiden jakelu
        - henkilötietoja sisältävät tulosteet

        - tilastot yms.
        - henkilötunnuksen merkitseminen asiakirjaan/tulosteisiin
    - määritellään tietojen suojaamisen ja turvaamisen lähtökohdat ja perusvaatimukset
    - laaditaan sisäiset rekisterin käyttöä koskevat ohjeet henkilöstölle
    - tavoitteena on, että kuvaus voisi toimia myös tietosuojan ohjeena organisaatiossa
    - järjestettävä riittävä koulutus henkilöstölle
    - suunniteltava, millä tavoin ohjeet ja koulutus pidetään ajan tasalla
17. Nimetään rekisteriasioitava hoitava henkilö
    - nimettävä ja määriteltävä henkilö, jonka puoleen voi kääntyä saadakseen tarkempia tietoja rekisteristä sekä oikeudesta saada tarkastaa ja saada korjatuksi itseään koskevat tiedot
    - tämä henkilö merkitään myös rekisteriselosteen rekisteriasioita hoitavaksi henkilöksi
18. Seurannan järjestäminen, ongelmista ja puutteista ilmoittaminen
    - suunniteltava ja organisoitava tapa, jolla tieto mahdollisista puutteista, ongelmista ym. saadaan viipymättä eri vastuuhenkilöille

LIITE 2 REKISTERISELOSTEEN JA TIETOSUOJASELOSTEEN OHJEISTUS

Rekisteriseloste

Rekisteriselosteen on oltava kaikkien saatavilla, informoidaan rekisteröityjä siitä, mihin he antavat omat tietonsa.

1. Rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot
    - henkilö, yhteisö tai säätiö, jonka käyttöä varten ko. rekisteri perustetaan
    - määrä rekisterin käytöstä
    - yhteyshenkilölle voidaan esittää henkilörekisteriä koskevia tiedusteluja, esim. tarkastusoikeus
    - rekisterille annetaan nimi, joka kuvaa rekisterin käyttötarkoitusta
2. Henkilötietojen käsittelyn tarkoitus
    - kertoo minkä tehtävien hoitoon kyseinen rekisteri on perustettu
3. Kuvaus rekisteröidyn ryhmästä tai rymistä ja näihin liittyvistä tiedoista tai tietoryhmistä
    - ne tiedot tai tietotyypit, joita rekisteröidystä voidaan tallettaa
    - yksilöintitiedot eritellään (nimi, syntymäaika, yhteystiedot)
    - tietotyypeistä riittää kuvaus (esim. asiakkaan tilaamat palvelut)
    - kuvaus myös siitä, mistä tiedot säännönmukaisesti saadaan
        - rekisterinpitäjän omasta toiminnasta
        - rekisteröidyltä itseltään
        - luovutuksena muualta (ilmoitettava, millä perusteella luovutus tapahtuu)
4. Mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle
    - luovutetaanko henkilötietoja, jos luovutetaan, niin kenelle
    - mitä tietoja luovutetaan
    - mihin luovuttaminen perustuu (esim. suostumus tai laki)
5. Kuvaus rekisterin suojauksen periaatteista
    - miten tiedot on suojattu organisaation ulkopuolisilta sekä miten käyttöoikeudet on rajattu organisaation sisällä
    - yleiset periaatteet riittää

- hyvä mainita, että henkilötiedot on määrätty salassa pidettäväksi

Tietosuojaseloste

Kaikkiin verkkopalveluihin, joissa kerätään henkilötietoja on liitettävä rekisteröidyn informoimiseksi ja yksityisyyden suojaamiseksi tarpeellinen tietosuojaseloste.

1. Saa olla täysin vapaamuotoinen
2. Tiedot rekisterinpitäjästä ja tarvittaessa tämän edustajasta
3. Tiedot henkilötietojen käsittelyn tarkoituksesta
4. Mitä tietoja kerätään
5. Tietojen säilyttäminen ja hävittäminen
6. Suojaus verkossa
    - Esim. Annetuista tiedoista syntyvää rekisteriä suojataan…
7. Tiedot säännönmukaisista tietojen luovutuksista
8. Tiedot, jotka ovat tarpeen rekisteröityjen oikeuksien käyttämiseksi asianomaisessa henkilötietojen käsittelyssä
    - tarkastusoikeus
    - tiedonkorjaamisoikeus
    - kielto-oikeus
9. Maininta mistä rekisteriseloste löytyy
10. Informoinnin sisältö määräytyy viimekädessä kuitenkin aina tapauskohtaisesti