

TIETOSUOJAVALTUUTETUN TOIMISTO

TYÖELÄMÄN TIETOSUOJA NS. WHISTLEBLOWING ILMIANTOJÄRJESTELMISSÄ

Päivitetty 27.07.2010

www.tietosuoja.fi

SISÄLLYS:

Huonetaulu …….. 3

1. Johdanto …….. 3

2. Henkilötietolain ja työelämän tietosuojalain velvoitteet …… 4

3. Informointi …… 7

4. Yhteistoimintamenettelyt …….. 7

5. Tarkastusoikeudesta, virheen korjaamisesta ja muista oikeusturvakeinoista 8

5. 1 Tarkastusoikeus 8

5.2 Virheen korjaaminen …… 9

5. 3 Muita oikeusturvakeinoja …… 9

6. Tietosuojavaltuutetun valvonta …… 10

7. Säilytysajoista …….... 10

8. Ulkomaille luovutukset ja siirrot …….. 10

9. Ilmoitusvelvollisuudesta …….... 11

10. Lopuksi …….. 11

Liitteet ja ohjausmateriaali …… 12

Material and Publications in English …… 13

Huonetaulu

Tarkastuslista whistleblowing –ilmiantojärjestelmiä toteutettaessa työpaikalla

0. Varmista, että yhtiösi kuuluu Sarbanes-Oxley-Act:in piiriin
1. Suunnittele huolellisesti – nimeä tietosuojavastaava
2. Käytä apuna rekisteriselostetta / tietosuojaselostetta
3. Määritä sallittu käsittelyn tarkoitus – älä käytä muuhun
4. Muista, että työoikeudellinen sääntely koskee myös ilmiantojärjestelmiä
5. Tee päätös järjestelmän käyttöönotosta työpaikan yhteistoimintamenettelyssä
6. Informoi henkilökuntaa
7. Älä koskaan käytä päätöksentekoon työntekijää kuulematta
8. Huolehdi tietojen laadusta ja oikeellisuudesta
9. Toteuta rekisteröidyn oikeudet
10. Toteuta korkea tietosuojan ja tietoturvan taso

1. Johdanto

Työelämässä ja yritystoiminnassa esiintyy erilaisia vihje- tai ilmiantojärjestelmiä, jotka voivat olla sähköisiä tietojärjestelmiä, esim. sähköposti- tai puhelinjärjestelmiä. Tässä oppaassa annetaan ohjeistusta siitä, miten edempänä esitettyjä organisaatioiden sisäisiä ilmiantojärjestelmiä voidaan käyttää ja samalla noudattaa direktiiviin 95/46/EY sisältyviä EU:n tietosuojasääntöjä sekä suomalaisen henkilötietolain (523/1999) ja laki yksityisyyden suojasta työelämässä (759/2004) eli työelämän tietosuojalain säännöksiä. Tässä oppaassa otetaan myös erityisesti huomioon 29 Artikla – Tietosuojatyöryhmän laatima ohjaus WP 117, 1.2.2006, EU:n tietosuojasääntöjen soveltamista sisäisiin ilmiantojärjestelmiin kirjanpidon, sisäisten kirjanpitotarkastusten, tilintarkastusten, lahjonnan torjumisen sekä pankki- ja talousrikosten alalla koskeva lausunto 1/2006.

Eräs tällainen ilmiantojärjestelmä on yhdysvaltalainen ns. whistleblowing –ilmiantojärjestelmä, jolla tarkoitetaan yhdysvaltalaisesta ns. Sarbanes-Oxley-Act laista johtuvaa velvollisuutta ja jonka pyrkimyksenä on rahoitusmarkkinoiden ja elinkeinotoiminnan turvaaminen sisäisten ilmiantojärjestelmien avulla kirjanpidon, sisäisten kirjanpitotarkastusten, tilintarkastusten, lahjonnan torjumisen sekä pankki- ja talousrikosten alalla. Laki koskee Yhdysvaltain pörssiin julkisesti noteerattuja yhtiötä ja mm. niiden EU:hun sijoittautuneita tytäryrityksiä. Tämä tietosuojavaltuutetun oppaan näkemys koskee ainoastaan Sarbanes-Oxley-Act laista johtuvia ns. whistleblowing –ilmiantoärjestelmiä.

Yhdysvaltain kongressi hyväksyi Sarbanes-Oxley-lain vuonna 2002 erilaisten yritysmaailman rahoitusskandaalien jälkeen. Kyseisessä laissa vaaditaan yhdysvaltalaisia julkisesti noteerattuja yhtiöitä ja niiden EU:hun sijoittautuneita tytäryrityksiä sekä muita kuin yhdysvaltalaisia yhtiöitä, jotka ovat listautuneet johonkin Yhdysvaltain pörssiin, ottamaan tilintarkastuskomiteassaan käyttöön menettelyt, jotka koskevat liikkeeseenlaskijan kirjanpitoa, sisäisiä kirjanpitotarkastuksia tai tilintarkastusta koskevien valitusten vastaanottoa, tallentamista ja käsittelyä sekä liikkeeseenlaskijan työntekijöiden mahdollisuutta tuoda ilmi luottamuksellisesti ja nimettömänä kirjanpidon tai tilintarkastusten alalla epäilyttäviä seikkoja. Lisäksi Sarbanes-Oxley-lain 806 pykälässä vahvistetuilla säännöksillä pyritään varmistamaan, että julkisesti noteerattujen yhtiöiden työntekijöitä, jotka esittävät todisteita petoksista, suojataan kostotoimenpiteiltä, joita heihin saatettaisiin kohdistaa ilmoitusjärjestelmään turvautumisen vuoksi.

Arvopaperimarkkinoiden valvontaviranomainen (Securities and Exchange Commission, SEC) vastaa Yhdysvalloissa Sarbanes-Oxley-lain soveltamisen valvonnasta. Nämä säännökset on otettu huomioon Nasdaqin ja New Yorkin pörssin (NYSE) säännöissä. Nasdaqiin tai NYSEen listautuneiden yhtiöiden on vuosittain varmennettava pörssille tilinsä. Tämä varmennusmenettely merkitsee, että yhtiöt voivat osoittaa noudattavansa tiettyjä sääntöjä, myös ilmiantamista koskevia sääntöjä.

Jos yhtiöt eivät noudata ilmiantoon liittyviä vaatimuksia, Nasdaq, NYSE tai SEC voivat määrätä raskaita seuraamuksia ja rangaistuksia. Koska ei ole varmuutta siitä, ovatko ilmiantojärjestelmät EU:n tietosuojasääntöjen mukaisia, EU:n tietosuojaviranomaiset saattavat määrätä yhtiöille seuraamuksia, jos ne eivät noudata EU:n tietosuojasääntöjä, ja toisaalta Yhdysvaltain viranomaiset voivat määrätä seuraamuksia, jos yhtiöt eivät noudata Yhdysvaltain asettamia sääntöjä.

Yhdysvalloissa tutkitaan parhaillaan, voidaanko joitakin Sarbanes-Oxley-lain säännöksiä soveltaa yhdysvaltalaisten yhtiöiden eurooppalaisiin tytäryrityksiin ja Yhdysvaltain pörsseihin listautuneisiin eurooppalaisiin yhtiöihin. Vaikka on epäselvää, voidaanko kaikkia Sarbanes-Oxley-lain säännöksiä soveltaa Eurooppaan sijoittuneisiin yhtiöihin, sellaiset yhtiöt, joihin Sarbanes-Oxley-lakia sovelletaan kyseisen säädöksen selkeiden ekstraterritoriaalisten säännösten nojalla, haluavat kuitenkin noudattaa Sarbanes-Oxleylain erityisiä ilmiantoa koskevia säännöksiä.[1]

2. Henkilötietolain ja työelämän tietosuojalain velvoitteet

Silloin kun Suomessa toimiva yritys joutuu toiminnassaan soveltamaan em. yhdysvaltalaista lainsäädäntöä, Sarbanes-Oxley-Act:ia, ja siihen liittyviä ilmiantojärjestelmiä, joutuu yritys rekisterinpitäjänä myös arvioimaan henkilötietojen käsittelyn lainmukaisuutta henkilötietolain ja työelämän tietosuojalain sekä muun suomalaisen lainsäädännön valossa.[2]

Sisäisten ilmiantojärjestelmien tavoitteena on yleensä varmistaa, että yhtiöiden päivittäisessä hallinnossa noudatetaan asianmukaisesti päätöksenteko- ja valvontajärjestelmän (corporate governance) periaatteita. Ilmianto on tarkoitettu lisäkeinoksi, jonka avulla työntekijät voivat erityiskanavaa apunaan käyttäen ilmoittaa sisäisesti rikkomuksista. Se täydentää organisaation tavanomaisia tiedotus- ja ilmoituskanavia, joita ovat esimerkiksi työntekijöiden edustajat, linjajohto, laadunvalvonnasta vastaava henkilöstö ja sisäiset tarkastajat, joiden tehtävänä nimenomaisesti on tällaisista rikkomuksista ilmoittaminen. Ilmianto pitäisi nähdä toissijaisena sisäiseen hallintoon nähden, ei sen korvaajana.

Artikla 29 - Tietosuojatyöryhmä korostaa, että ilmiantojärjestelmissä on noudatettava EU:n tietosuojasääntöjä. Ilmiantojärjestelmissä käsitellään useimmissa tapauksissa henkilötietoja (eli jonkun yksilöidyn tai yksilöitävissä olevan henkilön tietoja kerätään ja tiedot rekisteröidään, tallennetaan, luovutetaan ja tuhotaan), mikä tarkoittaa, että tietosuojasääntöjä on sovellettava.[3]

[1] 29 Artikla – Tietosuojatyöryhmä, WP 117, 1.2.2006, s. 11, perustelu lausunnon soveltamisen rajaamiselle.
[2] Henkilötietolain 4 §:n mukaan lakia sovelletaan sellaiseen henkilötietojen käsittelyyn, jossa rekisterinpitäjän toimipaikka on Suomen alueella tai muutoin Suomen oikeudenkäytön piirissä.
[3] WP 117, s. 6. Ilmoitusjärjestelmän välityksellä syytetyn suojelun korostuminen tietosuojasäännöissä.

Ilmiantojärjestelmien käytössä työpaikoilla on otettava huomioon henkilötietolaista ja työelämän tietosuojalaista johtuvat velvoitteet. Henkilötietolain 6 §:n mukaan henkilötietojen käsittely tulee suunnitella etukäteen. Henkilötietojen käsittelyn tulee olla asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Henkilötietojen käsittelyn tarkoitukset sekä se, mistä henkilötiedot säännönmukaisesti hankitaan ja mihin niitä säännönmukaisesti luovutetaan, on määriteltävä ennen henkilötietojen keräämistä tai muodostamista henkilörekisteriksi. Henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään.

Tietosuojavaltuutetun ratkaisukäytännössä on katsottu, että henkilötietojen käsittely, jolla loukataan jotain toista oikeutta, ei ole henkilötietolain 6 §:n tarkoittamalla tavalla asiallisesti perusteltua, ellei se perustu nimenomaiseen lainsäännökseen. Esimerkiksi työsopimuslaissa (55/2001) säädettyä työsopimusoikeudellista työn johto- ja valvontaoikeutta ei saa käydä ylittämään whistleblowing- järjestelmien ja niiden yhteydessä kerättävien tietojen takia.

Henkilötietolain 7 §:n käyttötarkoitussidonnaisuuden mukaisesti henkilötietoja saa käyttää tai muutoin käsitellä vain tavalla, joka ei ole yhteensopimaton edellä tarkoitettujen ennalta määrättyjen käsittelyn tarkoitusten kanssa.

Henkilötietolain 8 §:n 1 mom. 5 kohdan mukaan työnantajalla (rekisterinpitäjä) on oikeus käsitellä työntekijän (palvelussuhde) tai asiakkaan tai muun niihin verrattavan suhteen vuoksi, jos näillä rekisteröidyillä on asiallinen yhteys rekisterinpitäjän toimintaan (yhteysvaatimus).

Henkilötietolain 8 §:n 1 mom. 6 kohdan mukaan työnantajalla (rekisterinpitäjä) on oikeus käsitellä henkilötietoja, jos kysymys on konsernin tai muun taloudellisen yhteenliittymän työntekijöitä tai asiakkaita koskevista tiedoista ja näitä tietoja käsitellään kyseisen yhteenliittymän sisällä.

Edellä mainitun lisäksi on huomioitava erikseen henkilötietojen siirtoa ulkomaille koskevat säännökset. Ks. tarkemmin kappale 8. Ulkomaille luovutukset ja siirrot, s. 10.

Lisäksi asiassa on otettava huomioon työelämän tietosuojalain säännökset. Lain 3 §:n mukaan työnantaja saa käsitellä vain työntekijän työsuhteen kannalta välittömästi tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen ja työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta. Tästä tarpeellisuusvaatimuksesta ei voida poiketa edes työntekijän suostumuksella. Lain välitön tarpeellisuusvaatimus rajoittaa työnantajan oikeuksia käsitellä työntekijöiden henkilötietoja.

Työelämän tietosuojalain 4 §:ssä säädetään työntekijän henkilötietojen keräämisen yleisistä edellytyksistä ja työnantajan tiedonantovelvollisuudesta. Työnantajan on kerättävä työntekijää koskevat henkilötiedot ensi sijassa työntekijältä itseltään. Jos työnantaja kerää henkilötietoja muualta kuin työntekijältä itseltään, työntekijältä on hankittava suostumus tietojen keräämiseen. Suostumus ei kuitenkaan ole tarpeen silloin, kun viranomainen luovuttaa tietoja työnantajalle tämän laissa säädetyn tehtävän suorittamiseksi tai kun työnantaja hankkii henkilöluottotietoja tai rikosrekisteritietoja työntekijän luotettavuuden selvittämiseksi.

Hallituksen esityksen 75/2000 4 §:n perusteluiden mukaan tietojen keräämisellä työelämässä tarkoitetaan sellaista järjestelmällistä toimintaa, jonka tarkoituksena on manuaalisen käsittelyn avulla muodostaa työntekijöistä henkilörekisteri tai sen osa tai käsitellä tietoja automaattisen tietojenkäsittelyn avulla. Henkilötiedot olisi ensi sijassa kerättävä työntekijältä itseltään. Työnantajan kerätessä henkilötietoja muualta kuin työntekijältä itseltään, olisi pääsääntöisesti hankittava tämän suostumus. Jos työntekijä ei anna suostumusta tai sitä on asian laatu huomioonottaen mahdotonta pyytää häneltä, olisi työnantajalla oikeus hankkia tietoja ilman suostumustakin kahdella edellytyksellä. Ensinnäkin tietoja voidaan hankkia vain silloin, kun ne olisivat välittömästi työsuhteen kannalta tarpeellisia lain 3 §:n mukaisesti. Toiseksi henkilötietojen hankintaan olisi oltava selvä peruste, joka liittyisi työntekijän luotettavuuden selvittämiseen. Työntekijän luotettavuutta koskevat tiedot voisivat olla tarpeellisia mm. tehtävissä, joissa henkilö olisi välittömästi taloudellisessa vastuussa työnantajan omaisuudesta tai kun työsuhde vaatisi muutoin erityistä luottamusta. Laissa määritellään näin henkilötietolakia tarkemmin työnantajan oikeus kerätä työntekijän suostumuksetta ulkopuolisilta henkilötietoja ottaen erityisesti huomioon työelämän lähtökohdat ja työntekijöiden suojelun tarve.

Lain perusteluissa todetaan myös muita asiallisesti perusteltuja tietojen keräämistapoja muualta kuin työntekijältä itseltään, kuten esim. ulkopuolisen asiakaspalautteen kerääminen työntekijöistä. Nykyisin yritykset ja yhteisöt keräävät palvelunsa kehittämiseksi asiakaspalautetta. Työnantajat saattavat kerätä tietoja varmistaakseen laadunvalvonnan, asiakaspalvelun, omaisuuden suojelun sekä työprosessin organisoimisen. Kirjallisiin asiakaskyselyihin voi liittyä myös kysymyksiä, joiden vastausten perusteella yksittäinen työntekijä saattaa olla tunnistettavissa. Tällaiset tiedot voitaisiin tässä tapauksessa rinnastaa työntekijän luotettavuuden selvittämiseen. Työnantajat voisivat siten hankkia työntekijän suostumuksetta tällaista asiakaspalautetta, jos näin saatavat tiedot muutoin täyttävät lain 3 §:ssä tarkoitetun tarpeellisuusvaatimuksen.[4]

Erityistä tarpeellisuusvaatimusta sekä selvää perustetta työntekijän luotettavuuden selvittämiseksi arvioidaan tässä tapauksessa ns. whistleblowing –säännösten mukaan. Tietosuojadirektiivin 95/46/EY mukaisesti henkilötietojen käsittelyn on oltava asianmukaista ja lainmukaista, henkilötiedot on kerättävä tiettyä nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä tämän tarkoituksen kanssa yhteensopimattomalla tavalla. Lisäksi käsiteltyjen tietojen on oltava asianmukaisia, olennaisia eikä liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja missä niitä myöhemmin käsitellään. Näihin viimeksi mainittuihin sääntöihin viitataan joskus yhteisesti ”suhteellisuusperiaatteena”. Lisäksi on toteutettava aiheelliset toimenpiteet sen varmistamiseksi, että virheelliset tai puutteelliset tiedot poistetaan tai oikaistaan. Näiden olennaisten tietosuojasääntöjen soveltamisella on lukuisia vaikutuksia siihen tapaan, jolla organisaation työntekijät voivat tehdä ilmoituksia ja jolla kyseinen organisaatio voi näitä tietoja käsitellä.[5]

Henkilötietolain 6 §:n mukaan henkilötiedot kerätään tiettyä nimenomaista ennalta määrättyä ja asiallisesti perusteltua käyttötarkoitusta varten. Henkilötietojen on oltava asianmukaisia ja olennaisia eikä liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja mihin tarkoitukseen niitä tullaan myöhemmin käsittelemään. Ilmoitusjärjestelmän tarkoituksena on varmistaa päätöksenteko- ja valvontajärjestelmän asianmukaisuus, joten ilmoitusjärjestelmässä olisi kerättävä ja käsiteltävä ainoastaan tätä päämäärää palvelevia tietoja. Tällaisia järjestelmiä perustaessaan yritysten olisi selkeästi määriteltävä, minkä tyyppisiä tietoja järjestelmässä voidaan käsitellä ja luovuttaa, ja rajattava tiedot koskemaan kirjanpitoa, sisäisiä kirjanpitotarkastuksia tai tilintarkastuksia, pankki- ja talousrikoksia ja lahjonnan torjuntaa.[6]

[4] HE 75/2000 vp: 4 §:n yksityiskohtaiset perustelut ja yleisperustelut, 1.4. Kansainvälisen työjärjestön (ILO) ohjeisto.
[5] WP 117, s. 9, 2. Tietojen laadun ja oikeasuhteisuuden periaatteiden soveltaminen (tietosuojadirektiivin 6 artikla).
[6] WP 117, s. 11, iv) Kerättyjen ja käsiteltyjen tietojen oikeasuhteisuus ja virheettömyys.

Näin ollen työnantajan rekisterinpitäjänä on huolehdittava ilmiantojärjestelmien kautta kerättävien tietojen laadusta. Tietojen tulee olla virheettömiä ja niiden tulee olla välittömästi tarpeellisia työsuhteeseen, ts. työnantajan ja työntekijän oikeuksiin ja velvollisuuksiin liittyen. Työnjohto- ja valvontaoikeutta ei siis saa ylittää kerättävien tietojen osalta. Tietojen on liityttävä ilmiantojärjestelmän asiallisesti perusteltuun käsittelyn tarkoitukseen, eivätkä ne saa muilta osin loukata tietosuojaa ja työntekijöiden yksityisyyden suojaa. Asiassa on otettava huomioon erityisesti työelämän tietosuojalain 1 §[7] ja 3 § sekä henkilötietolain em. 6 § ja 9 §[8].

Rekisterinpitäjän on myös huolehdittava riittävän korkeasta tietosuojan ja tietoturvan tasosta. Tällöin on otettava huomioon henkilötietolain tarkoittama huolellisuusvelvoite[9] sekä etukäteinen suunnitteluvelvoite.[10] Erityisesti on kiinnitettävä huomiota tietojen suojaamisvelvoitteeseen[11] ja vaitiolovelvollisuuteen[12]. Ilmiantojärjestelmässä olevat henkilötiedot on suojattava sivullisten asiattomalta pääsyltä tietoihin sekä huolehdittava siitä, ettei tietoja ilman laissa säädettyä perustetta luovuteta sivullisille. Säännönmukaiset luovutukset tulee suunnitteluvelvoitteen mukaan määritellä etukäteen. Rekisterinpitäjän tulee myös toteuttaa riittävän korkea fyysinen ja tietotekninen tietoturva.[13] Niillä henkilöillä, jotka rekisterinpitäjän etukäteisen määrittelyn mukaisesti käsittelevät ilmiantojärjestelmässä olevia henkilötietoja, on vaitiolovelvollisuus käsittelyn yhteydessä saamistaan tiedoista, jotka koskevat mm. henkilön ominaisuuksia, henkilökohtaisia oloja tai taloudellista asemaa.

Rekisterinpitäjän tulee laatia kaikista henkilörekistereistä henkilötietolain 10 §:n tarkoittama rekisteriseloste ja pitää se jokaisen saatavilla. Tietosuojaselosteeseen voidaan lisäksi merkitä, miten rekisteröidyn tarkastusoikeus ja virheenkorjaamisoikeus toteutetaan. Edellä mainittu velvoite rekisteriselosteen laatimisesta tulee ottaa huomioon ilmiantojärjestelmiä suunniteltaessa ja käyttöön otettaessa. Rekisteriselosteeseen tulee merkitä myös

---

[7] Työelämän tietosuojalain 1 §: Lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. Lisäksi lain tarkoituksena on edistää hyvän tietojenkäsittelytavan noudattamista ja kehittämistä käsiteltäessä sekä työnhakijoiden että työntekijöiden henkilötietoja työelämässä.

[8] Henkilötietolain 9 §: Tietojen laatua koskevat periaatteet. Käsiteltävien henkilötietojen tulee olla määritellyn henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia (tarpeellisuusvaatimus). Rekisterinpitäjän on huolehdittava siitä, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja käsitellä (virheettömyysvaatimus). Rekisterinpitäjän velvollisuutta arvioitaessa on otettava huomioon henkilötietojen käsittelyn tarkoitus sekä käsittelyn merkitys rekisteröidyn yksityisyyden suojalle.

[9] Henkilötietolain 5 §: Rekisterinpitäjän tulee käsitellä henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa sekä toimia muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta. Sama velvollisuus on sillä, joka itsenäisenä elinkeinon- tai toiminnanharjoittajana toimii rekisterinpitäjän lukuun.

[10] Henkilötietolain 6 §:n suunnittelu- ja 32 §:n suojaamisvelvoitteeseen liittyy vaatimus määritellä etukäteen organisaatiossa ne henkilöt, joiden tehtäviin kuuluu henkilörekistereissä ja tietojärjestelmissä olevien henkilötietojen käsittely.

[11] Henkilötietolain 32 §: Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.

[12] Henkilötietolain 33 §:n vaitiolovelvollisuus. Joka henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessaan on saanut tietää jotakin toisen henkilön ominaisuuksista, henkilökohtaisista oloista tai taloudellisesta asemasta, ei saa tämän lain vastaisesti sivulliselle ilmaista näin saamiaan tietoja.

[13] Mm. lukitut tilat, järjestelmien käyttöoikeuksien määrittely, käyttäjätunnukset ja salasanat, järjestelmien käyttäjien lokitietojen hallinnointi, palomuurit, virustorjunta, luottamukselliset ja salatut viestintäyhteydet.

rekisteriasioista vastaava henkilö ja/tai rekisterinpitäjän edustaja, jonka tulee huolehtia rekisteröityjen oikeuksien toteutumiseen liittyvistä palveluista. Rekisterinpitäjän tulee siis nimetä ns. tietosuojavastaava.

Ks. Tietosuojavaltuutetun toimiston esitteet: Tietosuoja- ja rekisteriselosteet. Oppaat ja lomakkeet. Tietosuojavastaavan toimenkuva, tehtävät ja asema. Tietosuojan ja tietoturvan Tee se itse –tarkastus.

3. Informointi

Henkilötietolain 24 §:n mukaisesti rekisterinpitäjän on henkilötietoja kerätessään huolehdittava siitä, että rekisteröity voi saada tiedon rekisterinpitäjästä ja tarvittaessa tämän edustajasta, henkilötietojen käsittelyn tarkoituksesta sekä siitä, mihin tietoja säännönmukaisesti luovutetaan, samoin kuin ne tiedot, jotka ovat tarpeen rekisteröidyn oikeuksien käyttämiseksi asianomaisessa henkilötietojen käsittelyssä. Tiedot on annettava henkilötietoja kerättäessä ja talletettaessa tai, jos tiedot hankitaan muualta kuin rekisteröidyltä itseltään ja tietoja on tarkoitus luovuttaa, viimeistään silloin kun tietoja ensi kerran luovutetaan. Mikäli rekisteröity on jo saanut nämä tiedot, voidaan informointivelvoitteesta poiketa 24 §:n 2 momentin 1 kohdan mukaisesti.

Työelämän tietosuojalain 4 §:n 2 momentti asettaa työnantajalle erityisen informointivelvollisuuden. Mikäli työnantaja hankkii työntekijästä tietoja tämän luotettavuuden selvittämiseksi, tulee työnantajan kertoa tällaisten tietojen hankkimisesta etukäteen. Mikäli työnantaja on kerännyt henkilötietoja muualta kuin työtekijältä itseltään, on työnantajan kerrottava työntekijälle kerätyistä tiedoista ja niiden sisällöstä, ennen kuin tietoja käytetään työntekijää koskevaan päätöksentekoon. Työnantaja on velvollinen informoimaan työntekijää oma-aloitteisesti. Säännös velvoittaa työnantajaa toimimaan aktiivisesti ja informoimaan työntekijää myös henkilötiedon sisällöstä ennen työntekijää koskevan päätöksen tekemistä.

4. Yhteistoimintamenettelyt

Työelämän tietosuojalaki säätää yhteistoimintamenettelystä työpaikoilla. Lain 4 §:n 3 momentin mukaan henkilötietojen kerääminen työsuhteen aikana sekä työhön otettaessa kuuluu yhteistoiminnasta yrityksissä annetussa laissa (334/2007) tarkoitetun yhteistoimintamenettelyn piiriin.

Lain 21 § säätää yhteistoimintavelvoitteen tietoverkon käytön järjestämisessä. Työpaikan sähköpostin ja muun tietoverkon käyttö kuuluvat yhteistoiminnasta yrityksissä annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi edellä mainituista asioista. Yhteistoiminta- tai kuulemismenettelyn jälkeen työnantajan on määriteltävä tietoverkkojen ja sähköpostin käyttösäännöt ja tiedotettava työntekijöille sähköpostin ja tietoverkon käytöstä.

Työnantajan tulee neuvotella henkilöstön edustajien kanssa päättäessään uusien henkilötietojärjestelmien ja tietojärjestelmien käyttöönotosta ja niiden sisällöstä, kuten muistakin kerättävistä tiedoista. Yhteistoimintamenettelyssäkään ei voida sopia sellaisten tietojen keräämisestä, jotka eivät täytä lain tarpeellisuusvaatimusta tai lain säännöksiä

muutoin. Ennen kuin ns. whistleblowing -järjestelmä voidaan ottaa yrityksessä käyttöön, tulee asianmukaiset yhteistoimintamenettelyt henkilöstön kanssa käydä läpi. Yhteistoimintamenettely palvelee myös osaltaan rekisterinpitäjän informointivelvoitteen toteutumista.

5. Tarkastusoikeudesta, virheen korjaamisesta ja muista oikeusturvakeinoista

Rekisterinpitäjän tulee etukäteen suunnitella ns. whistleblowing -järjestelmien osalta, miten henkilötietolain tarkoittama tarkastusoikeus ja virheenkorjaamisoikeus tullaan ko. järjestelmässä olevien tietojen osalta toteuttamaan. Ks. myös tarkemmat ohjeet WP 117[14].

5. 1 Tarkastusoikeus

Henkilötietolain tarkoittamasta tarkastusoikeudesta säädetään lain 26 § - 28 §:ssä. Jokaisella on salassapitosäännösten estämättä oikeus tiedon etsimiseksi tarpeelliset seikat ilmoitettuaan saada tietää, mitä häntä koskevia tietoja henkilörekisteriin on talletettu tai, ettei rekisterissä ole häntä koskevia tietoja. Rekisterinpitäjän on samalla ilmoitettava rekisteröidylle rekisterin säännönmukaiset tietolähteet sekä, mihin rekisterin tietoja käytetään ja säännönmukaisesti luovutetaan. Henkilötietolain 27 §:ssä säädettyjä tarkastusoikeuden poikkeuksia tulee tulkita suppeasti. Henkilötietolain tarkoittama tarkastusoikeus tarkoittaa oikeutta saada tiedot kirjallisessa muodossa ja on kerran vuodessa maksuton.

Ns. whistleblowing –järjestelmien osalta tietosuojavaltuutettu toteaa, että henkilötietolain tarkastusoikeus koskee ainoastaan rekisteröityä (työntekijää) itseään koskevia henkilötietoja. Näin ollen ilmoituksen tai ilmiannon tehnyttä henkilöä koskevat tiedot eivät kuuluisi ilmiannon kohteen (rekisteröity) tarkastusoikeuden piiriin. Ilmoittajalla tai ilmiannon tehneellä on puolestaan itseään koskeviin tietoihin tarkastusoikeus henkilötietolain mukaisesti.

Rekisterinpidon ja henkilötietojen käsittelyn perusperiaatteisiin kuuluu kuitenkin määritellä etukäteen tietolähteet. Rekisteröidyllä on oikeus tietää ne tietolähteet, mistä henkilötiedot on kerätty. Näin ollen ilmoituksen kohteella (työntekijällä) on oikeus saada tietää ilmoituksen tehnyt tietolähde, ellei tätä oikeutta laissa erikseen rajoiteta. Rekisteröidylle tulee antaa ymmärrettävässä muodossa tieto siitä, mistä tai keneltä häntä koskeva tieto on peräisin henkilötietolain avoimuusperiaatteen mukaisesti.[15] Mikäli järjestelmä on tarkoitettu sellaiseksi, että ilmiantoja on mahdollista tehdä anonyymisti nimettömänä, ei em. tiedonsaantioikeutta voi luonnollisestikaan tällaisissa yhteyksissä käyttää.[16] Väärien ilmoitusten välttämiseksi ja luotettavien tietolähteiden käyttämisen varmistamiseksi rekisterinpitäjän tulisi tuoda ilmoittajalle julki, että rekisteröidyllä eli ilmoituksen kohteella on pääsääntöisesti oikeus saada tietoonsa käytetyt tietolähteet.

---

[14] WP 117, s. 13, i) oikeus saada tietää tietojen keräämisestä, ii) oikeus tietojen saantiin, oikaisuun ja poistamiseen.
[15] Ks. Tietosuojavaltuutetun kannanotto 19.3.2001, dnro 1196/523/2000 http://www.tietosuoja.fi -> ratkaisut
[16] WP 117, s. 10, iii) Mieluummin omalla nimellä esitettyjä ja luottamuksellisia ilmoituksia kuin nimettömiä ilmoituksia

5.2 Virheen korjaaminen

Henkilötietolain 29 §:ssä säädetään virheen korjaamisesta. Rekisterinpitäjän on ilman aiheetonta viivytystä oma-aloitteisesti tai rekisteröidyn vaatimuksesta oikaistava, poistettava tai täydennettävä rekisterissä oleva, käsittelyn tarkoituksen kannalta virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto. Rekisterinpitäjän on myös estettävä tällaisen tiedon leviäminen, jos tieto voi vaarantaa rekisteröidyn yksityisyyden suojaa tai hänen oikeuksiaan.

Jollei rekisterinpitäjä hyväksy rekisteröidyn vaatimusta tiedon korjaamisesta, hänen on annettava asiasta kirjallinen todistus. Todistuksessa on mainittava myös ne syyt, joiden vuoksi vaatimusta ei ole hyväksytty. Rekisterinpitäjän on ilmoitettava tiedon korjaamisesta sille, jolle rekisterinpitäjä on luovuttanut tai jolta rekisterinpitäjä on saanut virheellisen henkilötiedon. Ilmoitusvelvollisuutta ei kuitenkaan ole, jos ilmoittaminen on mahdotonta tai vaatii kohtuutonta vaivaa.

Tietosuojavaltuutetun ohjauksen mukaisesti tietojen täydentäminen on eräs tietojenkorjaamistapa. Näin menetellen rekisteristä ilmenee rekisterinpitäjän kannan lisäksi rekisteröidyn käsitys. Kun rekisterinpitäjä ja rekisteröity ovat eri mieltä tietojen oikeellisuudesta, eikä rekisterinpitäjä katso voivansa oikaista tai poistaa tietoja, on mahdollista liittää rekisteritietoihin rekisteröidyn näkemys.[17]

Artikla 29 - Tietosuojatyöryhmä toteaa, että EU:n tietosuojasääntöjen soveltaminen ilmiantojärjestelmiin merkitsee erityisen huomion kiinnittämistä syytetyn henkilön suojelemiseen. Tässä suhteessa työryhmä korostaa, että ilmiantojärjestelmiin sisältyy hyvin vakava riski syytetyn leimaamisesta ja syyllistämisestä organisaatiossa, johon hän kuuluu. Kyseinen henkilö altistuu tällaisille riskeille jo ennen kuin hän on tietoinen esitetyistä syytöksistä ja ennen kuin epäilyksenalaiset seikat on tutkittu sen määrittelemiseksi, onko niille perusteita. Työryhmä katsoo, että kun tietosuojasääntöjä sovelletaan asianmukaisesti ilmiantojärjestelmiin, lievitetään edellä mainittuja riskejä. Se myös katsoo, että sääntöjen soveltamisella ei estetä järjestelmien asianmukaista toimintaa vaan myötävaikutetaan siihen.

5. 3 Muita oikeusturvakeinoja

Henkilöstöä tulee informoida ns. whistleblowing –järjestelmän asianmukaisesta käyttötarkoituksesta ja tietojen tarpeellisuusvaatimuksesta. ”Pelisääntöjen” tulee olla selvät. Suomen lainsäädännöstä löytyy myös muita säännöksiä epäasiallisten ilmoitusten tai pahansuovassa ja kiusaamistarkoituksessa tehdyn väärän ilmiannon osalta. Kysymykseen voi tulla työturvallisuuslain (738/2002) 18 §:n ja 28 §:n tarkoittama häirintä ja epäasiallinen kohtelu työpaikalla, johon työantajan on puututtava. Työsuojelupiirit valvovat työturvallisuuslain noudattamista. Sovellettavaksi voivat myös tulla rikoslain säännökset esim. kunnian loukkaamisesta tai yksityiselämää loukkaava tiedon levittämisestä.[18]

Toisaalta myös ilmiantajien suojelu tulisi varmistaa ja ilmiantajille tulisi antaa takeet siitä, että he eivät joudu kostotoimenpiteiden kohteeksi (syrjintä tai kurinpitotoimet). Sarbanes-Oxley-lain 806 pykälässä vahvistetuilla säännöksillä pyritään varmistamaan, että julkisesti

[17] Tsv:n opas: Henkilörekisteriin talletetun tiedon korjaaminen, s. 5, http://www.tietosuoja.fi

[18] Rikoslaki (39/1889) 24 luku: 8 §: yksityiselämää loukkaava tiedon levittäminen, 9 §: kunnianloukkaus, 10 § törkeä kunnianloukkaus.

noteerattujen yhtiöiden työntekijöitä, jotka esittävät todisteita petoksista, suojataan kostotoimenpiteiltä, joita heihin saatettaisiin kohdistaa ilmoitusjärjestelmään turvautumisen vuoksi.[19]

[19] WP 117, s. 5, s. 8, s. 11.

6. Tietosuojavaltuutetun valvonta

Henkilötietolain 38 §:n mukaan tietosuojavaltuutettu antaa henkilötietojen käsittelyä koskevaa ohjausta ja neuvontaa sekä valvoo henkilötietojen käsittelyä tämän lain tavoitteiden toteuttamiseksi ja käyttää päätösvaltaa siten kuin tässä laissa säädetään.

Tietosuojavaltuutetun on edistettävä hyvää tietojenkäsittelytapaa sekä ohjein ja neuvoin pyrittävä siihen, että lainvastaista menettelyä ei jatketa tai uusita. Tarvittaessa tietosuojavaltuutetun on saatettava asia tietosuojalautakunnan päätettäväksi taikka ilmoitettava se syytteeseen panoa varten.

Tietosuojavaltuutetun on ratkaistava asia, jonka rekisteröity on saattanut henkilötietolain 28 ja 29 §:n nojalla hänen käsiteltäväkseen. Tietosuojavaltuutettu voi antaa rekisterinpitäjälle määräyksen rekisteröidyn tarkastusoikeuden toteuttamisesta tai tiedon korjaamisesta.

Työelämän tietosuojalain 22 §:n mukaan lain noudattamista valvovat työsuojeluviranomaiset yhdessä tietosuojavaltuutetun kanssa.

7. Säilytysajoista

Henkilötietolain 9 §:ssä säädetään tietojen laatua koskevat periaatteista. Käsiteltävien henkilötietojen tulee olla määritellyn henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia (tarpeellisuusvaatimus). Rekisterinpitäjän on huolehdittava siitä, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja käsitellä (virheettömyysvaatimus). Rekisterinpitäjän velvollisuutta arvioitaessa on otettava huomioon henkilötietojen käsittelyn tarkoitus sekä käsittelyn merkitys rekisteröidyn yksityisyyden suojalle. Lisäksi työelämän tietosuojalain 3 §:n välitön tarpeellisuusvaatimus rajaa työnantajan oikeutta käsitellä ja säilyttää työntekijöiden henkilötietoja.

Henkilötietolain 34 § säätää henkilörekisterin hävittämisestä. Henkilörekisteri, joka ei ole enää rekisterinpitäjän toiminnan kannalta tarpeellinen, on hävitettävä, jollei siihen talletettuja tietoja ole erikseen säädetty tai määrätty säilytettäviksi tai jollei rekisteriä siirretä arkistolaissa tarkoitetulla tavalla arkistoon (vain arkistolaissa määritellyt organisaatiot).

Whistleblowing –järjestelmien osalta rekisterinpitäjän tulee määritellä tietojen säilytysajat. Käsittelyn kannalta tarpeettomat tiedot tulee välittömästi poistaa henkilötietolain ja työelämän tietosuojalain tarpeellisuusvaatimuksen mukaisesti. Mikäli tiedot johtavat oikeuskäsittelyyn tai toimenpiteisiin työnantajan taholta, tulee tiedot säilyttää niin kauan kuin ne ovat esim. oikeuskäsittelyn kannalta tarpeellisia ja muutoksenhakumahdollisuutta ei enää ole. Ks. tarkemmat ohjeet WP 117, jossa suositellaan maksimissaan 2 kuukauden säilytysaikaa.[20]

8. Ulkomaille luovutukset ja siirrot

Vaikka whistleblowing –järjestelmien yhteydessä olisi olemassa luovutusperuste esim. konsernin tai taloudellisen yhteenliittymän sisäisesti tapahtuvaan työntekijöiden

[20] WP 117, s. 12, v) tiukat määräajat tietojen säilyttämiselle.

henkilötietojen käsittelyyn, on lisäksi asiassa otettava huomioon henkilötietolain 22 ja 23 §:n säännökset EU:n ja ETA:n ulkopuolelle kolmansiin maihin siirrettävien henkilötietojen osalta.

Henkilötietoja voidaan siirtää Euroopan unionin jäsenvaltioiden alueen tai Euroopan talousalueen ulkopuolelle siltä osin kuin Euroopan yhteisöjen komissio on henkilötietodirektiivin, 3 artiklan ja 25 artiklan 6 kohdan mukaisesti todennut, että kyseisessä maassa taataan tietosuojan riittävä taso. Tällainen siirtoperuste esimerkiksi on, jos henkilötietojen vastaanottaja on Yhdysvaltoihin sijoittautunut yritys, joka on liittynyt yksityisyyden suojaa koskevaan ns. Safe Harbor –järjestelmään. Siirtoperusteena voidaan myös käyttää henkilötietodirektiivin 26 artiklan 4 kohdassa tarkoitettuja komission hyväksymiä mallisopimuslausekkeita.

Siirtoperusteena voidaan käyttää myös sopimusta tietojen siirrossa riittävän turvan varmistamiseksi, kun rekisterinpitäjä siirtää tietoja EU:n tai ETA:n ulkopuolelle sellaiseen kolmanteen maahan, jossa yleinen suoja on riittämätön. Henkilötietolain 23 §:n 7 kohdan mukaan siirto on mahdollinen, jos rekisterinpitäjä antaa sopimuslausekkein tai muulla tavoin riittävät takeet henkilöiden yksityisyyden ja oikeuksien suojasta, eikä komissio ole henkilötietodirektiivin mukaisesti todennut takeita riittämättömiksi. Tällaisesta siirrosta on ilmoitusvelvollisuus tietosuojavaltuutetulle.

Ks. tarkempaa ohjausta tietosuojavaltuutetun opas: Henkilötietojen siirto ulkomaille henkilötietolain mukaan.[21]

9. Ilmoitusvelvollisuudesta

Rekisterinpitäjällä ei ole pääsääntöisesti ilmoitusvelvollisuutta tietosuojavaltuutetulle henkilötietolain 8 §:n 1 mom. 5 kohdan mukaisesta henkilötietojen käsittelystä, joka perustuu palvelussuhteeseen (asiallinen yhteys) tai 8 §:n 1 mom. 6 kohdan mukaisesta konsernin tai taloudellisen yhteenliittymän sisällä tapahtuvasta työntekijöiden henkilötietojen käsittelystä.

Edellä mainituissa ulkomaille siirroissa ilmoitusvelvollisuutta tietosuojavaltuutetulle ei ole, mikäli siirto tapahtuu laissa säädetyin perustein, esim. Safe Harbor-järjestelyin tai komission hyväksymiä, muuttamattomia mallisopimuslausekkeita käyttäen. Muissa ulkomaille siirroissa saattaa ilmoitusvelvollisuus täyttyä. Ks. tarkemmin tietosuojavaltuutetun opas: Henkilötietojen siirto ulkomaille henkilötietolain mukaan.

Mikäli tietojenkäsittely tai tietojenkäsittelypalvelut on tarkoitus ulkoistaa toimeksiannonsaajalle henkilötietolain 8 §:n 1 mom. 7 kohdan mukaisesti, on tästä ilmoitusvelvollisuus tietosuojavaltuutetulle.

Ks. tarkemmin ilmoitusvelvollisuudesta tietosuojavaltuutetun oppaasta: Henkilötietolain mukainen ilmoitusvelvollisuus.[22] Ks. myös opas: Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset.

---

[21] http://www.tietosuoja.fi
[22] http://www.tietosuoja.fi

10. Lopuksi

Edellä mainittujen säännöksien noudattaminen rajaa työantajan oikeuksia käsitellä työntekijöiden henkilötietoja sekä antaa whistleblowing –ilmiantojärjestelmien henkilötietojen käsittelylle asianmukaiset käsittelyn perusteet.

Työelämässä mahdollisesti esiintyviä muita ilmiantojärjestelmiä tai ilmiantopuhelimia on arvioitava erikseen. Työturvallisuuslaissa säädetään ilmoitusvelvollisuudesta työnantajalle, työsuojeluvaltuutetulle ja työsuojeluviranomaiselle työturvallisuutta vaarantavissa asioissa, esim. työpaikalla tapahtuvasta häirinnästä. Työturvallisuuslakia valvovat työsuojeluviranomaiset (työsuojelupiirit) siten kuin laissa työsuojelun valvonnasta ja työpaikan työsuojeluyhteistoiminnasta (44/2006) säädetään. Työelämän tietosuojalain valvonta kuuluu tietosuojavaltuutetulle yhdessä työsuojeluviranomaisten kanssa.

Liitteet ja ohjausmateriaali

29 Artikla – Tietosuojatyöryhmän ohjaus WP 117, 1.2.2006, EU:n tietosuojasääntöjen soveltamista sisäisiin ilmiantojärjestelmiin kirjanpidon, sisäisten kirjanpitotarkastusten, tilintarkastusten, lahjonnan torjumisen sekä pankki- ja talousrikosten alalla koskeva lausunto 1/2006.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_fi.pdf

Henkilötietolaki (523/1999)
http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Laki yksityisyyden suojasta työelämässä (759/2004)
http://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Ajantasainen lainsäädäntö.
http://www.finlex.fi/fi/laki/ajantasa/

Työelämän tietosuoja –opas
http://www.tem.fi/?C=98249&s=2691&xmid=4220

Tietosuojavaltuutetun toimiston kotisivut www.tietosuoja.fi

- Lomakkeet: Tietosuoja- ja rekisteriselosteet
- Oppaat: Tietosuojavastaavan toimenkuva, tehtävät ja asema.
- Oppaat: Tietosuojan ja tietoturvan Tee se itse –tarkastus.
- Oppaat: Henkilörekisteriin talletettujen tietojen tarkastaminen.
- Oppaat: Henkilörekisteriin talletetun tiedon korjaaminen.
- Oppaat: Henkilötietojen siirto ulkomaille henkilötietolain mukaan.
- Oppaat: Henkilötietolain mukainen ilmoitusvelvollisuus.
- Oppaat: Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset.

Material and Publications in English

ARTICLE 29 Data Protection Working Party,
WP 117, Adopted on 1 February 2006
Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf

The Office of the Data Protection Ombudsman – Data Protection in Finland
http://www.tietosuoja.fi -> English

- Data Protection Legislation
- Publications on Data Protection
- Description of the file
- Transfer of Personal Data to a Foreign Country according to the Personal Data Act

Personal Data Act (523/1999)
http://www.finlex.fi/fi/laki/kaannokset/1999/en19990523

Act on the Protection of Privacy in Working Life (759/2004)
http://www.finlex.fi/en/laki/kaannokset/2004/20040759

Data Protection in Working Life – Brochure
http://www.mol.fi/mol/en/99_pdf/en/92_brochures/8013e_data_protection.pdf