ASIAA TIETOSUOJASTA 4/1999
7.6.1999

HENKILÖTIETOLAKI HENKILÖTIETOJEN KÄSITTELYN OHJAAJANA

Tietosuojavaltuutetun tehtävänä on antaa henkilötietojen käsittelyä koskevaa ohjausta ja neuvontaa. Tämä esite sisältää käyttöönne tietosuojavaltuutetun yleisohjausta otsikkoasiassa. Tutustu myös muihin julkaisuihimme ja kotisivuumme Internetissä.

Henkilötietolaki on Sinua varten, käsitteletpä sitten henkilötietoja tai olet käsittelyn kohteena.

TIETOSUOJAVALTUUTETUN TOIMISTO

Albertinkatu 25, 00180 Helsinki
Puhelin: vaihde (09) 16003
Telefax (09) 1606 7835
www.tietosuoja.fi

HENKILÖTIETOLAINSÄÄDÄNTÖ YKSITYISYYDEN TURVAAJANA

HENKILÖTIETOLAIN TARKOITUS JA TAVOITTEET

Henkilötietolaki (523/1999) on säädetty toteuttamaan yksityiselämän suojaa sekä muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistämään hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Rekisteröityjen yksityisyyden ja heidän etujensa ja oikeuksiensa suojaaminen ei ole erillinen velvoite, vaan se kuuluu olennaisena osana hyvään hallintotapaan ja palveluun. Rekisteröidyn, esimerkiksi asiakkaan yksityisyyden suojan huomioiminen ja hänen oikeuksistaan kertominen lisää luottamusta rekisterinpitäjän ja rekisteröidyn välillä sekä edistää näin myös toiminnallisia tavoitteita.

Henkilötietolaissa säädetyt henkilötietojen käsittelyn yleiset edellytykset perustuvat rekisterinpitäjän toiminnan tarpeisiin. Kussakin rekisterinpitäjän tehtävässä (käsittelyn tarkoitus) tarpeellisia ja virheettömiä tietoja voidaan käsitellä, muttei muita. Laissa säädetty henkilötietojen kaikkiin käsittelyvaiheisiin ulottuva tarpeellisuusvaatimus sekä huolellisuusvaatimus tukevat myös toiminnan tavoitteita. Laki ohjaa säännöksillään hyvään tietohuoltoon ja tiedonhallintatapaan. Henkilötietolainsäädännön keskeisenä tarkoituksena on erityisesti ehkäistä tietotekniikan ja uuden teknologian käyttöön liittyviä tietosuojariskejä. Lain säännöksillä on keskeinen merkitys esimerkiksi käsiteltävien tietojen virheettömyyden takaajana on. Tosiasiassa rekisterinpitäjän toiminnalliset ja yksityisyyden suojan edellyttämät tavoitteet ovat lähes yhteneväiset.

Henkilötietolain mukaan henkilötietojen käsittely voi eräiltä osin perustua myös muuhun lainsäädäntöön. Sen vuoksi myös henkilötietojen käsittelyä koskevalla erityislainsäädännöllä voi olla olennainen merkitys sekä toiminnan tarpeiden että yksityisyyden suojan toteutumisessa. Jos kysymys on esimerkiksi rekisteröityjä koskevista arkaluonteisista tiedoista, tietojen salassapitoperusteet on arvioitu ja niistä on säädetty ensisijaisesti kyseisiä toimintoja koskevassa lainsäädännössä. Viranomaisten toiminnan osalta salassapitoperusteet määräytyvät viranomaisten asiakirjojen ja toiminnan julkisuutta koskevan lain säännösten pohjalta.

HENKILÖTIETOLAIN KEINOT TAVOITTEIDEN SAAVUTTAMISEKSI

Henkilötietolain tavoitteiden toteutuminen perustuu siihen, että rekisterinpitäjä (yritys, yhteisö. viranomainen, laitos ym.) arvioi henkilötietojen käsittelyn laissa säädettyjen vaatimusten perusteella. Lain vaatimukset voidaan huomioida vain

* määrittelemällä käsiteltävien henkilötietojen tarkoitus (rekisterin käyttötarkoitus).

* suunnittelemalla henkilötietojen käsittely ensijaisesti osana kyseisen toiminnan ja tehtävien sekä tietojärjestelmien suunnittelua, arvioimalla käsittelyn tarpeellisuus ja muu lainmukaisuus henkilötietolain ja mahdollisten asiaa koskevien erityislakien säännösten

perusteella sekä varmistumalla henkilötietojen käsittelyn ja tietojärjestelmien huolellisesta toteutuksesta.

* määrittelemällä henkilötietojen eri käsittelyvaiheisiin ja käsittelyyn liittyvät vastuut. Henkilötietojen käsittelyn vastuut ovat osa ko. toiminnan ja tehtävien vastuita. Rekisterinpitäjän voi olla lisäksi tarkoituksenmukaista määrätä organisaatioonsa erikseen tietosuojasta vastaava henkilö, joka huolehtii muun muassa tietosuojan suunnittelun, toteutuksen, ohjauksen ja koulutuksen koordinoinnista.

* suunnittelemalla, millä tavoin rekisteröityjen oikeudet huomioidaan ja millä tavoin ne voivat tukea tehtävien hoitoa ja palvelujen toteuttamistapaa.

MITÄ SUUNNITTELU KÄYTÄNNÖSSÄ EDELLYTTÄÄ

Kun suunnittelet henkilötietojen keräämistä, Sinun on siten syytä käydä läpi ainakin seuraavat toimenpiteet.

1) Määrittele ja yksilöi, mitä tehtävää varten aiot kerätä ja tallettaa henkilötietoja (käsittelyn tarkoitus/rekisterin käyttötarkoitus)

* Henkilötietojen käsittelyn tarkoitus määritellään siten, että siitä ilmenee, minkä rekisterinpitäjän tehtävää varten tietoja kerätään ja käsitellään. Tiettyä tehtävää varten perustettuun henkilörekisteriin kuuluvat kaikki tiedot, joita kyseisessä tehtävässä kerätään ja käsitellään, vaikka tietoja pidettäisiin teknisesti erillisissä osarekistereissä (looginen rekisteri). Nämä osarekisterit voivat olla atk:lla tai manuaalisesti ylläpidettyjä. Käytännössä osarekisterit ja niiden sisältämät tiedot muotoutuvat tehtävien hoidon organisoinnin perusteella. Esimerkkinä voidaan mainita palvelussuhteen hoitoa varten muodostettu henkilöstörekisteri, jossa osarekistereitä voivat organisointitavasta riippuen olla esimerkiksi henkilöstöluettelo, palkanlaskennan osarekisteri, koulutusluettelo, poissaololuettelot yms.

* Arvioi, edellyttääkö tehtävän hoito henkilöiden tunnistamistietojen keräämistä, vai riittäisivätkö ilman tunnisteita olevat tiedot.

2) Analysoi ja kirjaa ylös ko. tehtävän edellyttämät toiminnot (kuvaa toimintaprosessit) ja arvioi, mitä tietoja , mitä tarkoitusta varten ja millä tavoin eri toiminnan vaiheissa henkilötietoja on tarpeen kerätä, käyttää, luovuttaa tai muutoin käsitellä. Määrittele jo tässä yhteydessä, miten pitkään eri tietoja tarvitaan toisaalta ko. toiminnan tarpeisiin ja miten pitkään niitä mahdollisesti on tarpeen muun lainsäädännön nojalla säilyttää sekä miten tiedot eri käsittelyvaiheissa hävitetään. Muutostilanteissa toimintaprosessit on arvioitava uudelleen. Selvitä myös erityisesti atk:n käyttöä suunniteltaessa, millä tavoin esimerkiksi tilasto- ja suunnittelukäyttöön, johdon tarpeisiin sekä sisäiseen ja tarvittaessa myös ulkoiseen tiedottamisen voidaan tuottaa tietoja ilman henkilöiden tunnistetietoja. Arvioi myös tietosuojariskit ja varmista, miten tietojen suojaamisesta ja tietoturvasta voidaan huolehtia.

*Selvitä ja arvioi jo tässä yhteydessä, onko tehtävän hoidossa tarpeen hankkia palveluja ulkopuolisilta, missä ominaisuudessa nämä toimivat palvelujen ostajaan nähden sekä mitä ja millä tavoin henkilötietoja ko. palvelun yhteydessä käsitellään. Mikäli palvelu hankitaan toimeksiantona (palvelut hankkivan lukuun), vastaa rekisterinpitäjä myös palvelujen

tuottajan henkilötietojen käsittelyn lainmukaisuudesta. Palvelujen tuottajan vastuu määräytyy tällöin pelkästään sopimusvastuuna, ellei muussa laissa ole erikseen säädetty palvelujen tuottajille velvollisuuksia. Esimerkiksi henkilötietolaissa säädetyt suojaamis- ja huolellisuusvelvoitteet koskevat myös toimeksiantotehtäviä suorittavia. On tärkeää, että palvelujen ostamisesta tehdään riittävän selvät kirjalliset sopimukset ja että sopimuksessa määritellään myös henkilötietojen käsittelyyn liittyvistä vastuista ja velvoitteista sekä niihin liittyvistä menettelyistä. On myös tärkeää, että ennen sopimuksen tekemistä - ja riippumatta sopimuksen luonteesta - muun ohella varmistutaan siitä, että sopimuksen tarkoittaman toiminnan edellyttämä henkilötietojen käsittely hoidetaan lain vaatimusten mukaisesti.

3) Arvioi henkilötietolain eri säännösten ja mahdollisten henkilötietojen käsittelyä koskevien erityissäännösten perusteella, onko henkilötietojen käsittelylle olemassa lain vaatimat edellytykset.

* Arvioi erikseen kaikkien käsittelyvaiheiden laillisuus: kerääminen, tietosisältö, käyttö omassa toiminnassa, luovuttaminen, säilyttäminen, suojaaminen, hävittäminen ja muu käsittely.

Arvioinnin tuloksena syntyy kuvaus henkilötietojen eri käsittelyvaiheista (rekisteri-kuvaus). Kuvausta voidaan käyttää tietojen käsittelyä ja tietosuojaa koskevien ohjeiden pohjana.

Erityisen tärkeää on, että lainmukaisuuden arvio tehdään kyseisen toiminnon tai tehtävän sekä tietojärjestelmien ja tiedonsiirron suunnittelun ja toteutuksen yhteydessä. Virheellisesti toteutettujen tietojärjestelmien korjaaminen on kallista ja voi johtaa sekä toiminnan että yksityisyyden suojan kannalta merkittäviin haittoihin ja vahinkoihin.

4) Huomaa, että kaikissa käsittelyn vaiheissa keräämisestä aina säilyttämiseen ja hävittämiseen on sekä toiminnan että tietosuojan kannalta tarpeen varmistaa, että käsitellään vain kussakin tarkoituksessa ja tehtävässä/osatehtävässä tarpeellisia ja virheettömiä tietoja, ettei rekisteröityjen yksityisyyttä perusteettomasti vaaranneta ja että kaikessa käsittelyssä ja käsittelyvaiheissa huomioidaan tietojen suojaamiselle asetettavat vaatimukset. Tietojärjestelmien rakenteet ja toteutus, järjestelmien käyttöoikeudet, asiakirjojen laatiminen ja tietosisältö samoin kuin atk-tulosteiden sisältö ja jakelu arvioidaan tältä pohjalta.

5) Selvitä, mitä oikeuksia rekisteröidyillä on saada tietoja itsestään ja henkilötietojen käsittelystä sekä suunnittele ja organisoi se tapa, jolla oikeuksien toteuttaminen käytännössä hoidetaan. Mieti, millä tavalla oikeuksien toteuttaminen voi tukea ko. toiminnan tavoitteita sekä millä tavoin oikeuksien toteuttamiseen liittyviä menettelyjä voidaan yksinkertaistaa ja sisällyttää osaksi ko. toimintaa ja tietojärjestelmiä. Tietotekniikkaa voidaan hyödyntää myös sisällyttämällä ohjelmistoihin ja sovelluksiin erilaisia toimintaa ja rekisteröityjen yksityisyyden suojaa ohjaavia ominaisuuksia. Rekisteröityjen keskeisimmät oikeudet ovat

* yleinen tiedonsaantioikeus rekisterinpidosta
  (rekisteriselosteen laatiminen ja saatavillapitovelvollisuus).
* informointivelvoite henkilötietojen käsittelystä
* tarkastusoikeus ja virheen oikaisu

* kieltomahdollisuus tietyissä tilanteissa

6) Selvitä, onko henkilötietojen käsittelystä tehtävä ilmoitus tietosuojavaltuutetulle. Tee tarvittaessa ilmoitus.

7) Huolehdi siitä, että henkilötietojen käsittelyvastuut on määritelty, että henkilöstöllä on riittävät ohjeet ja tiedot henkilötietojen käytön ja käsittelyn edellytyksistä sekä tietojärjestelmien toimintaperiaateista. Ylläpidä ohjeistusta ja koulutusta jatkuvasti. Perusohjeistus muodostuu rekisterikuvauksen laatimisen yhteydessä.

8) Huolehdi siitä, että käytön ja käsittelyn lainmukaisuutta voidaan valvoa ja valvotaan. Määrittele myös sanktiot määräysten ja säännösten vastaisesta käytöstä.

9) Seuraa osana toimintaa ja tehtävien hoitoa henkilötietojen käsittelyyn liittyvien asioiden toimivuutta ja ryhdy tarvittaessa toimenpiteisiiin havaittujen epäkohtien korjaamiseksi. Muista, että kysymys on ennen muuta myös toiminnan edellytysten varmistamisesta .