



TIETOSUOJAVALTUUTETUN TOIMISTO

LAADI TIETOSUOJASELOSTE

Päivitetty 27.07.2010

www.tietosuoja.fi

Henkilötietolain mukaan kaikkiin verkkopalveluihin, joissa kerätään henkilötietoja on liitettävä tietojen antajan informoimiseksi ja yksityisyyden suojaamiseksi tarpeellinen tietosuojaseloste. Tässä oppaassa kerrotaan, minkä vuoksi informointivelvoitteet on otettu lakiin, kuinka tietosuojaseloste kannattaa laatia ja mitä informaatiota siihen tulee sisällyttää.

Henkilötietolain (523/1999) 2.2 §:n mukaan henkilötietolakia sovelletaan henkilötietojen automaattiseen käsittelyyn, mitä henkilötietojen sähköinen siirtäminen internetin verkkopalvelun kautta on. *Henkilötiedolla* tarkoitetaan ”kaikenlaisia luonnollisia henkilöitä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi” (3 § 1 kohta). Henkilötiedolla siis tarkoitetaan nimi- ja yksilöintitietojen lisäksi myös kaikenlaisia muita yksittäiseen henkilöön liitettävissä olevia tietoja. Jos verkkopalvelun kautta kerätään tietoja tai jos henkilötietoja käsitellään verkossa, tiedot muodostavat tai kuuluvat osana henkilörekisteriin. Henkilötietolain 3 §:n 3 kohdan määritelmän mukaan *henkilörekisterillä* tarkoitetaan ”käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta”. Henkilörekisteristä on aina laadittava rekisteriseloste (10 §), jonka tiedot voidaan sisällyttää myös tietosuojaselosteeseen.

Miksi tietosuojaseloste?

Henkilötietolain 24 §:n mukaan henkilötietoja kerätessä rekisteröidyn tulee aina voida olla tietoinen antamiensa tietojen tulevasta käsittelystä ja käytöstä. *Informointivelvoitteen avulla pyritään parantamaan kansalaisen mahdollisuuksia käyttää henkilötietojen käsittelyyn liittyviä oikeuksiaan sekä kasvattamaan käyttäjien luottamusta verkossa tarjottaviin palveluihin.* Henkilötietolaki on säädetty toteuttamaan Suomen perustuslaissa turvattua yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia sekä edistämään hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

Tietosuojan huomioiminen nettipalvelun yhteydessä on laissa säädetyn velvollisuuden ohella myös oleellinen osa hyvää palvelua verkkoympäristössä. Tutkimusten mukaan merkittävä osa verkon käyttäjistä kokee tietosuojaan liittyvät puutteet ongelmana asioinnin luotettavuuden ja internet-sivujen käytettävyyden kannalta. Väärin käsiin joutuneet henkilötiedot saattavat luoda uhkan tietojen kohteen eli rekisteröidyn yksityisyydelle, joten henkilötietolain säännökset pyrkivät ennaltaehkäisemään tämänkaltaisia tilanteita ohjaamalla julkishallintoa, yrityksiä, yhteisöjä ja muita rekisterinpitäjiä hyvään tietojenkäsittely- ja tiedonhallintatapaan

Käytännössä henkilötietolaki ja erityisesti sen 24 § tulee huomioida kaikilla niillä internet-sivustoilla, joilla on käytössä ns. nettilomake eli henkilötietoja kysyvä ja tallettava internet-palvelu.

Esimerkkejä verkkopalveluista tms. toiminnoista, joiden lainmukaisuus tulee arvioida myös henkilötietolain kannalta ja joihin tulee liittää tietosuojaseloste:

- 1) Tietojen kerääminen internetin kautta, esim.
 - Internetissä toteutettavat asiakaskyselyt,
 - Työpaikkahakemukset verkossa,
 - Internetissä täytettävät ilmoittautumislomakkeet,
 - Verkkokaupankäynti,
 - Palautetiedon kerääminen;
- 2) Keskustelupalstat, jotka edellyttävät rekisteröitymistä;
- 3) Muu verkkopalveluun rekisteröityminen.

Mitä tietoja tietosuojaselosteeseen tulee sisällyttää?

Rekisteröidyn oikeuksiin kuuluu henkilötietolain 24 §:n mukaan informaation saaminen antamiensa tietojen tulevasta käsittelystä. Henkilötietolain 24 §:n 1 momentin mukaan henkilötietojen keräämisen yhteydessä on annettava vähintään seuraavat tiedot:

- tiedot rekisterinpitäjästä ja tarvittaessa tämän edustajasta,
- tiedot henkilötietojen käsittelyn tarkoituksesta,
- tiedot säännönmukaisista tietojen luovutuksista,
- ne tiedot, jotka ovat tarpeen rekisteröityjen oikeuksien käyttämiseksi asianomaisessa henkilötietojen käsittelyssä (mm. 26 §:n tarkastusoikeus, 29 §:n tiedonkorjaamisoikeus ja 30 §:n suoramarkkinointitarkoituksiin tms. kerättäviä tietoja koskeva kiello-oikeus).

Lisäksi verkkopalvelun tarjoavan tahon eli rekisterinpitäjän on laadittava syntyvästä rekisteristä rekisteriseloste, joka on pidettävä jokaisen saatavilla (10 §). Lain esitöiden mukaan myös rekisteriseloste on laitettava internetiin, jos itse rekisteri on tietoverkossa (HE 96/1998, s. 43). Rekisteriseloste tai sen edellyttämä tietosisältö on siten liitettävä verkkopalvelun yhteyteen osana tietosuojaselostetta. Rekisteriselosteen edellyttämä informaatio on pitkälti yhteneväinen edellä luetellun henkilötietolain 24 §:n informointivelvollisuuden sisällön kanssa, mutta se sisältää myös yhden tärkeän lisäyksen edellyttäessään kuvausta rekisterin suojauksen periaatteista.

Tietosuojavaltuutetun toimiston laatima rekisteriselostetta koskeva ohje ja mallilomake löytyvät toimistomme verkkosivuilta osoitteesta <http://www.tietosuoja.fi/2584.htm>. 24 §:n informointivelvoitteen sisältöä kuvaava laajempi ja tätä opasta täydentävä opas (Rekisterinpitäjällä yleinen informointi velvollisuus 1.6.1999 alkaen) löytyy niin ikään tietosuojavaltuutetun toimiston verkkosivuilta osoitteesta <http://www.tietosuoja.fi/1970.htm>. Molemmat oppaat ovat tilattavissa myös postitse.

Tietosuojaselosteen suunnittelu ja laatiminen

Tietosuojaseloste on henkilötietolain 24 §:n sisältämän informointivelvoitteen ja 10 §:n rekisteriselosteen saatavillapitovelvoitteen yhdistämiseksi luotu käsite, josta huolehtimalla henkilötietoja keräävien verkkopalveluiden henkilötietolainmukaisuus voidaan varmistaa. *Tietosuojaseloste voidaan laatia täysin vapaamuotoisesti kunhan se vain sisältää henkilötietolain 10 ja 24 §:ssä edellytetyn informaation.*

Tietosuojaselosteen laatimisen lisäksi on henkilötietoja käsiteltäessä kuitenkin aina huolehdittava myös muiden henkilötietolain säännösten noudattamisesta.

HENKILÖTIETOLAIN SÄÄNNÖKSIÄ, JOTKA ON VERKKOPALVELUN YHTEYDESSÄ MYÖS OTETTAVA HUOMIOON:

- Suunnitteluvaatimus eli käyttötarkoituksen määrittely (6 §) ja muiden käsittelyvaiheiden suunnittelu ja lainmukaisuuden varmistaminen (6 §, 5 §), mm.:
 - Kerättävien henkilötietojen määrittely sekä tietolähteiden ja tietosisällön arviointi (9 §),
 - varmistuminen oikeuksista ja velvollisuuksista tietojen luovuttamiseen (8 § ja ao. erityissäännökset), säilyttämiseen (34§) sekä hävittämiseen (34 §, 32 §, 5 §),
 - rekisteröityjen oikeuksien toteutuksen suunnittelu ja varmistaminen (26-30 §);
- Koko toimintaa koskeva huolellisuusvelvoite (5 §);
- Tarpeellisuus- ja virheettömyysvaatimuksen huomioiminen kaikissa käsittelyvaiheissa (9 §);
- Tietojen suojaamisvelvoite (32 §);
- Salassapitovelvollisuus (33 § tai ao. erityissäännös).

ESIMERKKEJÄ

Asian konkretisoimiseksi tässä oppaassa esitetään internet-sivuille rekisteröitymislomakkeen yhteyteen laadittavaa tietosuojaselostetta verkkopalvelun suunnittelun ja sisällön kannalta. Internetiin sijoitetun sähköisen palvelun toteutustapa on tarpeen suunnitella ja arvioida etukäteen henkilötietolain yleisten säännösten kannalta (ks. edellisen sivun infolaatikko).

Esimerkkejä rekisteröitymistä edellyttävistä palveluista internetissä ovat esimerkiksi osallistumislomakkeet internet-kilpailuihin, käyttäjäksi kirjautumispalvelu, työnhakijaksi rekisteröityminen tai jäsenhakemuksen verkkolomake – henkilötietoja kerääviä palvelumahdollisuuksia on luke mattomia. Kaikissa näissä tapauksissa, joissa henkilötietoja pyydetään, palvelun yhteydessä täytyy antaa lain edellyttämä informaatio. Jos tietojen antaminen ei ole palvelun käyttämisen kannalta välttämätöntä, tulee myös tästä informoida.

Verkkopalvelun yhteyteen (esimerkiksi oman linkin taakse) sijoitettavan tietosuojaselosteen si-

sältö voisi olla lain asettamat vaatimukset täyttäen esimerkiksi seuraavankaltainen (huomaa, että informoinnin sisältö määräytyy kuitenkin viimekädessä aina tapauskohtaisesti).

Esimerkki: verkossa olevan lehden tilaajaksi rekisteröitymisessä muodostuva henkilö-rekisteri

Tietosuojaseloste

- **Rekisterin rekisterinpitäjä** on yritys X (*osoite*). Yhteyshenkilönä toimii henkilö X (*tarkat yhteystiedot*) [ja teknisestä toteutuksesta vastaa taho X].
- Kerättäviä henkilötietoja käytetään verkkolehtemme xxx tilaajien asiakassuhteiden ylläpitoon ja hoitoon, sekä palvelun edellyttämien yhteydenottojen mahdollistamiseen
- Rekisteriin talletetaan seuraavat tiedot:
(voit käyttää apuna myös rekisteriselostetta)
- Tietoja säilytetään asiakassuhteen jatkumisen ajan (*säilyttämisaika ja hävittäminen määriteltävä henkilötietolain 34 §:n mukaisesti*).
- Annettuja tietoja suojataan verkossa:... (*mainittava esimerkiksi, onko sähköinen yhteys SSL-suojattu = Secure Sockets Layer*)
Annetuista tiedoista syntyvää rekisteriä suojataan
(Myös tässä voidaan viitata rekisteriselosteeseen)
- Annetut yhteystietonne voidaan luovuttaa seuraaviin suoramarkkinointitarkoituksiin....., elleite ole kieltänyt luovuttamista. Kieltomahdollisuus merkittävä rekisteröintilomakkeelle
- Tilaajalla on oikeus saada tarkistaa itseään koskevat tiedot, oikeus vaatia virheellisen tiedon oikaisua, oikeus kieltää antamiensa tietojen käytön suoramarkkinointi- tms. tarkoitukseen sekä muutoinkin turvautua henkilötietolaissa turvattuihin oikeuksiinsa. Asiaa koskevat pyynnöt osoitetaan xx:lle
- Henkilötietolain 10 §:n mukainen **rekisteriseloste** on nähtävissä myös verkossa oheisen linkin X takana/muualla (*missä*).”

Palautelomakkeen suunnittelun yhteydessä täytyy mm. määritellä kerätäänkö palaute *ilman henkilön tunnistetietoja vai ei*. Tarpeettomasti henkilötietoja ei pidä koskaan kerätä.

Palautteen lähettäjä on tarpeen informoida toivotusta palautteen lähettämistavasta (anonymisti, henkilötiedoin)

Jos palaute kerätään henkilötiedoin, on suunniteltava ja arvioitava etukäteen, muodostuuko palautteista henkilötietolain soveltamisalaan kuuluva rekisteri ja mikä on palauteaineiston keräämisen ja käsittelyn tarkoitus (2.2 §, 3 § 1 kohta ja 6 §). Palautelomakkeella lähetetyt (esim. sähköpostina siirtyvät) henkilötietoja sisältävät viestit saattavat muodostaa henkilörekisterin, jos tiedot kootaan yhtenäiseksi henkilötietolain 3.1 kohdassa 3 tarkoitetuksi manuaaliseksi henkilörekisteriksi tai jos niistä sellainen syntyy palautteita automaattisen tietojenkäsittelyn avulla käsiteltäessä.

Jos palautteista muodostuu henkilörekisteri, on ryhdyttävä tietosuojaselosteen laadintaan. *Sii-näkin tapauksessa, että palaute pyydetään anonymisti, on esimerkiksi tietojen suojaamisen ta-sosta tarpeen informoida siltä varalta, jos joku haluaa kuitenkin henkilötietonsa lähettää*.

Esimerkki: internetin palautelomakkeen yhteyteen liitettävä tietosuojaseloste

Tietosuojaseloste

- Tämän xx yrityksen/viranomaisen palautejärjestelmän keräämät tiedot on tarkoitettu ai-noastaan palautteen keräämiseen X tarkoitusta varten (tarvittaessa X tarkoituksen edel-lyttämien yhteydenottojen mahdollistamiseen).
- Palautteen antaminen anonymisti on mahdollista, joten nimen- ja yhteystietojen täyttä-minen ei ole välttämätöntä.
- Jos kuitenkin halutaan antaa nimi- ja yhteystiedot, annettujen tietojen perusteella syntyy X-niminen henkilörekisteri.
- Rekisterin rekisterinpitäjä on yritys/yhteisö X (*esimerkiksi X kunnan kunnanhallitus, osoi-te X*). Yhteyshenkilönä toimii X (*tarkat yhteystiedot*).
- Rekisteri koostuu sähköisesti annettujen palautteiden sisältämistä tiedoista/ yksilöidyistä muista tiedoista/mistä?)
(Voit käyttää apuna rekisteriselostetta)
- Palaute säilytetään, kunnes asia on käsitelty (*säilyttämisaika määriteltävä henkilötietolain 34 §:n mukaisesti*).
- Palautetietoja annettaessa tiedot suojataan verkossa/tiedonsiirron aikana seuraavasti:... (*mainittava esimerkiksi, onko sähköinen yhteys SSL-suojattu = Secure Sockets Layer*)
- Palautteen tietoja ei luovuteta millekään muulle taholle.
- Palautetta lähettäneellä on oikeus saada tarkistaa lähettämänsä itseään koskevat tiedot ja oikeus vaatia virheellisen tiedon oikaisua. Asiaa koskevat pyynnöt osoitetaan xx:lle.
- Henkilötietolain 10 §:n mukainen **rekisteriseloste** on nähtävissä myös verkossa oheisen

linkin X takana/muualla (*missä*).”

Viranomaisten tarjoamien verkkopalveluiden osalta myös palautetiedon ja muun viranomaiselle toimitettavan tiedon julkisuudesta on hyvä olla maininta. Julkisuus määritellään viranomaisten toiminnan julkisuudesta annetun lain (621/1999) tai mahdollisen erityslain mukaan.

Palautteen antajalle on hyvä tarvittaessa kertoa siitä, että arkaluonteisia tietoja ei ole syytä ilmoittaa verkkopalvelun yhteydessä (ellei tietojen suojausta ole järjestetty). Muut verkkopalvelun käyttäjän kannalta tarpeelliset tiedot tulee ilmoittaa tapauskohtaisesti, toiminnan tarpeiden mukaan ja henkilötietolain yleiset säännökset huomioiden.

Jos internet-palvelun tapauksessa on kyseessä esimerkiksi verkossa tapahtuva liiketoiminta, kuten kuluttajille suunnattu **verkkokauppa** tulee henkilötietolain säädösten lisäksi huomioida myös *muiden lakien toiminnalle asettamat velvoitteet*. Näitä ovat mainitun verkkokaupankäynnin harjoittamisen yhteydessä erityisesti laki tietoyhteiskunnanpalveluiden tarjoamisesta (458/2002), jota valvoo ja ohjeistaa Viestintävirasto, sekä kuluttajansuojalain 6 luku (1072/2000), joka kuuluu Kuluttajaviraston ja kuluttaja-asiamiehen toimialaan. Kuluttajavirasto on laatinut aihetta koskevan esitteen, joka on luettavissa viraston kotisivuilla.

Tärkeää on huomata, että *eri käyttötarkoituksia varten kerättäviä tietoja varten on laadittava omat erilliset rekisteriselosteensa*. Kunkin rekisteriselosteen tiedot voidaan edellä kuvatulla tavalla sisällyttää asianomaiseen tietosuojaselosteeseen. Palveluiden käyttäjien ja lain velvoitteiden täyttymisen kannalta on oleellista, että informaatio annetaan helposti ymmärrettävässä muodossa ja palvelun käyttäjien kannalta tarkoituksenmukaisella tavalla. Tietosuojaseloste on siis syytä liittää – esim. linkkinä – kiinteästi kunkin palvelun yhteyteen.

Evästeistä informoiminen

Sähköisen viestinnän tietosuojalain (516/2004) 7 §:n mukaan myös mahdollisesta evästeiden (cookies) käyttämisestä on informoitava verkkopalvelun yhteydessä.

Tämä on toteutettavissa helposti liittämällä tietosuojaselosteeseen oma evästeiden käyttöä koskeva osuutensa. Laki sisältää informointivelvollisuudelle kuitenkin myös poikkeuksen: siinä tapauksessa, jossa evästeiden ainoana tarkoituksena on teknisesti helpottaa palvelun käyttöä tai jos käyttäjä on nimenomaan pyytänyt evästeiden käyttöön perustuvaa palvelua, evästeistä ei tarvitse tiedottaa.

Evästeet ovat internet-palvelun käyttöä kuvaavia tietoja, jotka tallentuvat esim. käyttäjän tietokoneeseen ja joita voidaan käyttää internet-selaimen ja –palvelimen väliseen yhteydenpidon ohjaamiseen. Evästeiden avulla on mahdollista tallettaa tietoa esim. käyttäjän selaamista internet-sivustoista, jotta sivu ”muistaisi” käyttäjän hänen tullessaan sivulle seuraavan kerran. Evästeet ovat välttämättömiä esim. verkkopankin ja verkkokaupan toimivuuden kannalta.

Esimerkki: lain edellytykset täyttävä evästeistä informointi

”Käytämme sivuillamme ns. cookie-toimintoa eli evästeitä. Eväste on pieni, käyttäjän tietokoneelle lähetettävä ja siellä säilytettävä tekstitiedosto, joka mahdollistaa internet-sivujen ylläpitä-

jän tunnistamaan usein sivuilla vierailevat kävijät, helpottamaan kävijöiden kirjautumista sivuille sekä mahdollistamaan yhdistelmätiedon laatimisen kävijöistä. Tämän palautteen avulla pystymme jatkuvasti parantamaan sivujemme sisältöä. Evästeet eivät vahingoita käyttäjien tietokoneita tai tiedostoja. Käytämme niitä siten, että voimme tarjota asiakkaillemme kunkin yksilöityjen tarpeiden mukaisia tietoja ja palveluita.

Mikäli sivuillamme vieraileva käyttäjä ei halua meidän saavan edellä mainittuja tietoja evästeiden avulla, useimmat selainohjelmat mahdollistavat eväste-toiminnon poiskytkemisen. Tämä tapahtuu esim. Internet Explorerä -selainohjelman "Työkalut" -valikosta löytyvän "Internet asetukset" -valikon kautta kohdasta "Suojaus".

On kuitenkin hyvä ottaa huomioon se, että evästeet voivat olla tarpeellisia joidenkin ylläpitämiemme sivujen ja tarjoamiemme palveluiden asianmukaiselle toimimiselle."

Kenellä on vastuu tietosuojaselosteen laatimisesta?

Rekisterinpitäjällä tarkoitetaan henkilötietolain määritelmän mukaan "yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiota, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty" (3 § 4 kohta). Tietosuojaselosteen laadinnasta eli informaatiovelvoitteen ja rekisteriselosteen laatimis- ja saatavillapitovelvoitteen huomioimisesta vastaa siis rekisterinpitäjänä se, joka on verkkopalvelun tarjoaja tai jonka lukuun henkilötietoja kerätään. Tämän tahon on huolehdittava lain velvoitteiden noudattamisesta ja ohjeistettava niiden teknisessä toteuttamisessa.

Velvoitteen noudattamatta jättäminen on henkilötietolain 48.2 §:n 1 kohdassa rangaistavaksi säädetty teko. Henkilötietolain noudattamista valvoo tietosuojavaltuutettu, joka voi tarvittaessa ilmoittaa asian syytteeseen panoa varten.

Evästeistä informoimista valvoo sähköisen viestinnän tietosuojalain 31 §:n nojalla Viestintävirasto. *Evästeistä informoimisen laiminlyönti on säädetty rangaistavaksi sähköisen viestinnän tietosuojalain 42.2 §:n 2 kohdassa.*

Verkkopalveluita suunniteltaessa ja tarjottaessa kannattaa huomioida, että tietosuojasta huolehtiminen lisää avoimuutta ja luottamusta sekä parantaa palvelujen käytettävyyttä. Laissa edellytettävien tietojen tuominen esille palvelun tarjoamisen yhteydessä takaa palvelulle ja kyseisille verkkosivuille mahdollisimman turvallisen käytön ja edistää siten varsinaisia toiminnallisia tavoitteita. Rekisteröityjen yksityisyyden ja heidän etujensa ja oikeuksiensa suojaamista ei tulekaan nähdä erillisenä velvoitteena, vaan se kuuluu olennaisena osana hyvään tiedonhallintatapaan ja asiakaspalveluun.

Henkilötietolaki ja muut tässä esitteessä mainitut lait pykälälineen löytyvät kokonaisuudessaan Valtion säädöstietopankista osoitteesta www.finlex.fi. Yleistä informaatiota tietosuojasta ja henkilötietolaista on saatavilla tietosuojavaltuutetun toimiston internet-sivuilta osoitteesta www.tietosuoja.fi. Sähköisen viestinnän tietosuojalakia ja evästeitä koskevaa tietoa löytyy Viestintäviraston verkkosivuilta <http://www.ficora.fi/suomi/index.html>. Verkkokaupankäyntiä koskeva Kuluttajaviraston tuottama esite "Kauppapaikka Internetissä – Verkkokauppiiaan ohje" on luettavissa Kuluttajaviraston kotisivuilla osoitteessa <http://www.kuluttajavirasto.fi>.