

PÄIVITETTY 29.10.2018

TILINTARKASTAJA JA EU:N TIETOSUOJA-ASETUS – KYSYMYKSIÄ JA VASTAUKSIA

SUOMEN TILINTARKASTAJAT RY:N SUOSITUKSIA 1/2018



Sisällys

1 Mitä henkilötiedot ovat ja käsittelevätkö tilintarkastajat henkilötietoja?.....	3
2 Milloin tilintarkastaja on rekisterinpitäjä ja milloin henkilötietojen käsittelijä?.....	3
3 Mikä on tilintarkastajan rooli erityyppisissä toimeksiannoissa?	4
4 Pitääkö lakisääteisessä tilintarkastustoimeksiannossa sopia henkilötietojen käsittelemisestä?	5

Suomen Tilintarkastajat ry on tilintarkastajia edustava edunvalvontajärjestö. Jäsenemme ovat tilintarkastuslain mukaisesti hyväksytyjä HT-, KHT-, JHT- ja JHTT-tilintarkastajia sekä tilintarkastusalan ja taloushallinnon asiantuntijoita. Tavoitteenamme on auttaa tilintarkastajien ammattikuntaa menestymään sekä tuomaan lisäarvoa elinkeinoelämälle ja yhteiskunnalle. Taloudellista raportointia ja alan käytäntöjä edistämällä olemme mukana rakentamassa perustaa suomalaisen yhteiskunnan kilpailukyvyille ja hyvinvoinnille. Yhdistykseen kuuluu yli 90 % Suomessa toimivista hyväksytyistä tilintarkastajista.

Ohje on julkaistu alun perin 15.5.2018 ja sitä on päivitetty 29.10.2018 kohdalla 4:

Kysymys: Pitääkö lakisääteisessä tilintarkastustoimeksiannossa sopia henkilötietojen käsittelemisestä?

Vastaus: Ei tarvitse, koska lakisääteisessä tilintarkastuksessa tilintarkastaja on rekisterinpitäjä.

Euroopan unionin tietosuoja-asetus¹ (jäljempänä myös ”tietosuoja-asetus”) on herättänyt kysymyksiä niin tilintarkastajissa kuin tarkastuskohteissa. Suomen Tilintarkastajat ry on tunnistanut tilintarkastajien ja tarkastuskohteiden tarpeen kansalliselle ohjeistukselle.

Tässä Q&A:ssa esitetyt tulkinnat ja soveltamisohjeet ovat Suomen Tilintarkastajat ry:n laatimia. Kotimaista soveltamiskäytäntöä tietosuoja-asetuksesta ei vielä ole, joten esitetyt tulkinnat voivat kehittyä ja muuttua ajan myötä. Tietosuoja-asetusta ja uutta kansallista tietosuojalakia sovelletaan 25.5.2018 alkaen.

1 Mitä henkilötiedot ovat ja käsittelevätkö tilintarkastajat henkilötietoja?

Tietosuoja-asetus koskee henkilötietojen käsittelyä. Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tyypillisiä henkilötietoja ovat henkilötunnus, nimi ja osoite, mutta myös kuvat ja evästeet (cookiet) luetaan henkilötietoihin, jos ne ovat yhdistettävissä tiettyihin luonnollisiin henkilöihin.

Henkilötietojen käsittely tarkoittaa esimerkiksi tietojen keräämistä, muokkaamista, jäsentämistä tai poistamista. Se kattaa henkilötietojen kaikenlaisen käyttämisen, ja käsitteen tulkinta on laaja.

Tilintarkastajat käsittelevät esimerkiksi asiakashallintaansa ja palveluntarjoajiinsa liittyviä henkilötietoja sekä omia työntekijöitään koskevia henkilötietoja. Lisäksi tilintarkastajat käsittelevät toimeksiantajensa suorittamisen yhteydessä esimerkiksi asiakkaidensa työntekijöitä ja sopimuskumppaneita koskevia henkilötietoja. Henkilötietoja käsitellään toimeksiannoissa vaihtelevassa laajuudessa toimeksiannon luonteen mukaan, ja joissakin toimeksiannoissa ei mahdollisesti käsitellä lainkaan henkilötietoja.

2 Milloin tilintarkastaja on rekisterinpitäjä ja milloin henkilötietojen käsittelijä?

Tietosuoja-asetuksen mukaisia keskeisiä rooleja ovat rekisterinpitäjä ja henkilötietojen käsittelijä.

¹ Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta

Rekisterinpitäjä määrittelee, mitä henkilötiedoille pitää tai saa tehdä ja millä tavoin, ts. mitä tarkoitusta varten tietoja käsitellään ja kuinka käsittely tapahtuu. Rekisterinpitäjän on huolehdittava siitä, että tietosuoja-asetuksen periaatteita noudatetaan ja että rekisteröidyt voivat käyttää oikeuksiaan. Rekisterinpitäjällä on myös yleinen vastuu siitä, että käsittelystä aiheutuvista tietojen eheyteen liittyvistä riskeistä johtuen suoritetaan asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta varmistetaan ja pystytään osoittamaan, että käsittely tapahtuu tietosuoja-asetuksen mukaisesti.

Rekisterinpitäjällä on tietosuoja-asetuksessa määritelty tiedonantovelvollisuus rekisteröityjä kohtaan. Rekisterinpitäjän pitää lisäksi valvoa, että heidän käyttämänsä henkilötietojen käsittelijät käsittelevät henkilötietoja tietosuoja-asetuksen mukaisesti. Rekisterinpitäjän on myös käsiteltävä tietoturvaloukkauksia koskevat ilmoitukset. Rekisterinpitäjän on tiedotettava henkilötietojen käsittelystä, kun tietoja kerätään, mutta myös rekisteröidyn sitä pyytäessä. Tietosuoja-asetuksessa määrätään yksityiskohtaisesti, mitä tietoja rekisteröidylle on annettava hänen henkilötietojensa käsittelystä².

Henkilötietojen käsittelijä käsittelee hänelle käsittelyä varten luovutettuja henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä ei itse päättä käsittelyn tietosuoja-asetuksen tarkoitetusta oikeudellisesta perusteesta/perusteista eikä käsittelyn tarkoituksesta tai tarkoituksista, vaan käsittelijän on noudatettava käsittelystä rekisterinpitäjän antamia ohjeita. Tämä tarkoittaa, ettei henkilötietojen käsittelijä saa itse päättää, mitä tarkoituksia varten tai kuinka henkilötietoja käsitellään. Lisäksi henkilötietojen käsittelijä on velvollinen avustamaan rekisterinpitäjää täyttämällä omat velvoitteensa rekisteröityjä ja valvontaviranomaista kohtaan. Käsittelijällä ei kuitenkaan ole tiedonantovelvollisuutta rekisteröityjä kohtaan, vaan tämä velvollisuus on rekisterinpitäjällä. Henkilötietojen käsittelijällä on itsenäinen velvollisuus toteuttaa asianmukaisia teknisiä ja organisatorisia toimenpiteitä henkilötietojen suojaamiseksi.

3 Mikä on tilintarkastajan rooli erityyppisissä toimeksiannoissa?

3.1 *Asiakkaiden ja toimeksiantojen hyväksymistä ja käsittelyä koskevat tiedot sekä asiakasrekisteri (TTL 4:9 §):* Tilintarkastajat ovat rekisterinpitäjiä käsiteltäessä henkilötietoja näitä tarkoituksia varten, koska tällainen käsittely tapahtuu tilintarkastajan omia asiakashallintaan liittyviä tarkoituksia varten.

3.2 *Tilintarkastus:* Tilintarkastajat ovat tilintarkastustoimeksiannoissa rekisterinpitäjiä toimeksiannon suorittamisen yhteydessä hankkimiensa henkilötietojen osalta. Tämä johtuu tilintarkastajan itsenäisestä roolista ja siitä, että tilintarkastaja suorittaa toimeksiannon voimassa olevien lakien ja hyvän tilintarkastustavan mukaisesti. Tällöin tilintarkastaja päättää, mitä henkilötietoja tilintarkastustoimeksiannossa käsitellään ja kuinka käsittely tapahtuu.

3.3 *Muut lakiin tai asetukseen perustuvat tarkastustoimeksiannot kuin tilintarkastus:* Nämä toimeksiannot ovat varsin samanlaisia kuin tilintarkastustoimeksiannot ja tilintarkastajilla on usein itsenäinen rooli päätettäessä, mitä toimenpiteitä tehdään ja

² Tarkemmat tiedot mm. rekisteröidyn oikeuksista löytyvät tietosuojavaaluttetun oppaasta:

http://www.tietosuoja.fi/material/attachments/tietosuojavaaluttettu/tietosuojavaaluttetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf



mitä henkilötietoja on tarpeellista käsitellä. Tällaisissa toimeksiannoissa henkilötietoja käsittelevät tilintarkastajat ovat yleensä rekisterinpitäjiä toimeksiannon yhteydessä hankkimiensa henkilötietojen osalta.

3.4 Tilintarkastajan muut palvelut, joissa tilintarkastaja käsittelee henkilötietoja:

Toimeksiannon sisältäessä itsenäistä harkintavaltaa henkilötietojen käsittelystä tilintarkastaja on pääsääntöisesti rekisterinpitäjä (ks. edellä rekisterinpitäjää koskeva kohta). Jos tilintarkastaja saa yksityiskohtaiset ohjeet siitä, mitä toimenpiteitä suoritetaan sekä mitä ja miten henkilötietoja käsitellään, eikä tilintarkastajalla ole tarvetta hankkia tietoja itsenäisesti (mukaan lukien henkilötiedot), tilintarkastaja voi olla henkilötietojen käsittelijä.

4 Pitääkö lakisääteisessä tilintarkastustoimeksiannossa sopia henkilötietojen käsittelemisestä?

Ei tarvitse, koska lakisääteisessä tilintarkastuksessa tilintarkastaja on rekisterinpitäjä.