Digitaalisen turvallisuuden teemakuukausi

Tietosuojapäivä 9.10.2018

Chatin kautta tulleita kysymyksiä ja vastauksia tietosuojasta

Vastaukset ovat tietosuojavaltuutetun toimiston asiantuntijoiden laatimia, ellei vastauksen yhteydessä toisin mainita. Ne ovat yleistä ohjausta, eivät kannanottoja yksittäistapauksiin (TSA 57 1 b).

Kysymykset on käsitelty Juhta/VAHTI työpajassa #17, läpikäynnin helpottamiseksi tiettyjä kohtia on alleviivattu. Alleviivaukset on tehnyt Kuntaliitosta Tuula Seppo.

Ketkä ovat sellaisia itsenäisiä rekisterinpitäjiä joiden ei tarvitse tehdä muiden kanssa tietosuojasopimuksia ja liitteitä? Esim. vakuutusyhtiö jonka järjestelmään teemme lakisääteiset tapaturmailmoitukset väittää, että emme tarvitse kaupungin ja vakuutusyhtiön välistä sopimusta, onko näin?

Kysymykseen ei voi ottaa kantaa yksiselitteisesti tuntematta sen yksityiskohtia. Esimerkiksi jos kyse on kaupungin työntekijöistä, kaupunki on työntekijöidensä henkilötietojen osalta rekisterinpitäjä. Vakuutusyhtiö vakuuttaessaan työntekijät on myös rekisterinpitäjä, koska vakuutusyhtiö käsittelee tietoja omiin tarkoituksiinsa. Luovuttaessaan tietoja toiselle rekisterinpitäjälle kaupungin tulee varmistaa mm., että tietojen luovutus on mahdollinen, noudattaa huolellisuusvelvollisuutta ja että siitä on informoitu rekisteröityjä (eli että työntekijät ymmärtävät, että tiedot tallentuvat vakuutusyhtiölle). Varsinaista käsittelijän ja rekisterinpitäjän välistä sopimusta ei kuitenkaan tehtäisi, vaikka asiasta ja toimintatavoista muutoin sovittaisiin.

Henkilötietojen käsittelijästä on kyse silloin, kun käsittelijä tekee rekisterinpitäjän puolesta jonkun toimen rekisterinpitäjän ohjeiden mukaisesti. Käsittelijä ei voi käyttää tietoja omiin tarkoituksiinsa, vaan ainoastaan siihen tarkoitukseen, josta on sovittu esim. ulkoistussopimuksella.

Tivi uutisoi juuri, että Ruotsissa tulossa ensimmäiset GDPR-tuomiot – tutkinnassa 66 yritystä. Miten Suomessa? Ja juuri ruotsalaisten on kerrottu suhtautuvan asetukseen suurpiirteisesti, omia väljiä tulkintoja tehden

Reijo Aarnio kommentoi puheenvuorossaan 9.10. Ruotsin GDPR-tuomioita: Suomessa on noin 3 000 vireille tullutta asiaa tähän mennessä. Koska tietosuoja-asetus on koko EU:n yhteinen, yksi maa ei voi pitkällä aikavälillä tulkita sitä poikkeuksellisen väljästi tai tiukasti, siihen puuttuvat muut jäsenmaat.

Menikö ilmoitus tietosuojavastaavista tämän hankkeen kautta tietosuojavaltuutetulle? Olin jostain lukevinani näin? Vai pitääkö tehdä vielä erillinen ilmoitus?

Tietosuojavaltuutetulle pitää tehdä erillinen ilmoitus tietosuojavastaavasta.

Millaisia tietoturvaloukkausilmoituksia tietosuojavaltuutettu on saanut?

Reijo Aarnio kommentoi puheenvuorossaan 9.10. tietoturvaloukkauksia: Tietoturvaloukkauksia tulee noin 10 päivässä eli 4 kk:ssa toistatuhatta ilmoitusta ja niiden aiheet vaihtelevat yksittäisiä kansalaisia koskevista ylikansallisiin loukkauksiin. Tietosuojavaltuutetun toimisto yrittää toimia niin, että tietoturvaloukkausilmoituksen tekeminen olisi palvelu, jonka avulla voidaan selvittää, millaisia ongelmatapauksia käytännön arjessa ilmenee ja ilmoitus olisi myös toiminnan kehittämisen väline.

PeV arvioi tietosuojalakia koskevassa lausunnossaan (24/2018) kriittisesti ehdotettua seuraamuskollegiota. Näetkö tästä huolimatta, että ehdotus menee sellaisenaan syksyn aikana läpi?

Reijo Aarnion mukaan sanktion määräämiseen liittyvä järjestelmään mentiin maksimien kautta (20 milj. / 4 % liikevaihdosta). Samalla unohtui asetuksen hienoin piirre eli harmonisointi. Sanktioista on päätettävä EU:ssa yhteisesti, ei yksittäisen valvontaviranomaisen toimesta. Euroopan tietosuojaneuvostolla on työryhmä, joka käy läpi sanktioihin ja niiden määräämiseen liittyviä asioita.

Koskeeko asetus myös Ahvenmaan postimyyntiyrityksiä

Kyllä koskee.

Tuleeko tietoturvaloukkausten sähköiseen ilmoituslomakkeeseen mahdollisuus ilmoittaa myös tietojen saatavuutta koskevista tietoturvaloukkauksista? Käsittääkseni nämäkin tulisi ilmoittaa.

Tietoturvaloukkausten sähköistä ilmoituslomaketta ollaan päivittämässä lähiaikoina, ja siihen ollaan lisäämässä myös mahdollisuus ilmoittaa tietojen saatavuutta koskevasta loukkauksesta.

Miten pohjoismaisiin tietosuojakäytäntöihin ym. vaikuttaa se, että kaikki Pohjoismaat eivät ole EU:n jäseniä?

Pohjoismaat, jotka eivät kuulu EU:hun, noudattavat yleistä tietosuoja-asetusta ETA-sopimuksen perusteella.

Sosiaali- ja terveydenhuollolla ja apteekeilla tulee Kuntaliiton elokuussa annetun ohjeen mukaan olla oma tietosuojavastaavansa ja heitä koskevat myös asetuksen tietosuojavastaavia koskevat säännökset. Moni kunta on luopunut sosiaali- ja terveydenhuollon tietosuojavastaavasta ja nimennyt esim. tietosuojan yhteyshenkilöitä asetuksen mukaisen tietosuojavastaavan lisäksi. Eikä tämä ole ristiriidassa tuon Kuntaliiton ohjeen kanssa? Miten TSV suhtautuu tähän malliin? Kanta-palvelut edellyttävät valvontaa ja seurantaa tekemään organisaation oman tietosuojavastaavan ja tästä tulisi olla Omavalvontasuunnitelman mukaan sopimus, jolla varmistetaan, että tietosuojavastaava saa hänelle kuuluvan roolin ja aseman organisaatiossa, jotta hän voi hoitaa tehtäviään tarkoituksenmukaisesti.

Tietosuoja-asetus mahdollistaa sen, että erityislainsäädännössä säädetään velvollisuudesta nimittää tietosuojavastaava. Sosiaali- ja terveydenhuollon palveluntarjoajille ja apteekeille on säädetty tällainen velvollisuus. Nimittämisvelvollisuus on edelleen olemassa.

Myös sosiaali- ja terveydenhuollon sekä apteekkien tietosuojavastaavien asema ja tehtävät tulevat tietosuoja-asetuksesta. Tämä tarkoittaa muun muassa sitä, että rekisterinpitäjän on varmistettava tietosuojavastaavalle riittävät toimintaedellytykset, jotta tietosuojavastaava pystyy toteuttamaan kaikki hänelle kuuluvat tehtävät. Tehtäviä on kuvattu esimerkiksi verkkosivuillamme (https://tietosuoja.fi/tietosuojavastaavat) tai kysymyksessä mainitussa Kuntaliiton ohjeessa (https://www.kuntaliitto.fi/yleiskirjeet/2018/tietosuojavastaavan-nimittaminen-tehtavat-ja-asema).

Onko tähän videoon jotain linkkiä, jos vaikka laittaisimme tämän intran sivuille ja henkilökunnalle katsottavaksi?

Video löytyy eOppivan koulutusmateriaaleista. Video pyritään julkaisemaan tämän vuoden aikana myös kuntien henkilöstölle.

Onko Tietosuojan ABC tulossa myös englanniksi ja/tai ruotsiksi?

Videona Tietosuojan ABC on toistaiseksi julkaistu vain suomenkielisenä. Vastaava ruotsinkielinen aineisto tekstinä (PDF) löytyy eOppivan kurssialueelta samasta paikasta kuin linkki suomenkieliseen videoon.

Miten WhatsApp -sovelluksen käyttö esim. koulun ja päiväkodin viestinnässä? Pysyykö henkilötiedot EU:n / ETA:n sisäpuolella? Onko turvallista?

Henkilötietojen käsittelyssä on noudatettava henkilötietojen käsittelyä koskevaa lainsäädäntöä. EU:n yleisen tietosuoja-asetuksen lisäksi henkilötietojen käsittelyyn tullaan soveltamaan parhaillaan eduskunnassa käsiteltävänä olevaa tietosuojalakia (HE 9/2OI8), joka tulee täydentämään ja täsmentämään tietosuoja-asetusta. Lisäksi henkilötietojen käsittelyyn voi vaikuttaa toimialakohtainen lainsäädäntö (esim. varhaiskasvatuslaki, perusopetuslaki) sekä viranomaisten toiminnan julkisuudesta annettu laki (julkisuuslaki) yleislakina, jos sitä sovelletaan toimintaan. Unionin oikeuden etusijaperiaatteen mukaisesti kansallista lainsäädäntöä ei voi soveltaa siten, että se olisi ristiriidassa tietosuoja-asetuksen kanssa.

Henkilötieto on määritelty tietosuoja-asetuksen 4 artiklan 1 kohdassa. Tietosuoja-asetuksen yhtenä periaatteena on riskiperusteinen lähestymistapa ja riskiarvio tehdään rekisteröidyn näkökulmasta. Arviossa huomioidaan henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset.

Osa päivähoidon ja opetuksen järjestämisessä käsiteltävistä lapsia ja oppilaita koskevista tiedoista on salassa pidettäviä, mikä vaikuttaa riskin arviointiin. WhatsApp-sovelluksen käytössä tulisi selvittää tarkemmin esimerkiksi, minkälaisia tietoja siellä tultaisiin käsittelemään, miten tiedot on suojattu ja millaiset käyttöehdot palvelussa on. WhatsApp on maailmanlaajuisesti käytössä oleva palvelu, joka voi mahdollisesti siirtää henkilötietoja EU:n ulkopuolelle. Rekisterinpitäjän (eli tässä tapauksessa päivähoidon tai opetuksen järjestäjä) tulee ottaa edellä mainitut asiat ja niihin liittyvä lainsäädäntö huomioon, kun se arvioi, onko sovellus mahdollista ottaa käyttöön.

Tietosuoja-asetuksessa säädetään rekisterinpitäjän osoitusvelvollisuudesta, joka on asetuksen keskeinen periaate (ks. tietosuoja-asetuksen 5 artiklan 2 kohta, 24 artiklan 2 kohta, 25 artikla ja 30 artikla). Se tarkoittaa, että rekisterinpitäjän on pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä.

Lisätietoja: www.tietosuoja.fi

Onko valvova viranomainen laatinut luettelon käsittelytoimista jolloin pitää tehdä vaikutustenarviointi (DPIA)

Kyllä, yhteensä 22 jäsenmaata on laatinut Euroopan tietosuojaneuvostolle kansalliset luettelot, niiden mukana Suomi.

Mistä löytyy ne esimerkit mistä tehdään tietoturvaloukkausilmoitus

Tietosuojavaltuutetun toimiston verkkosivuilla osoitteessa https://tietosuoja.fi/tietoturvaloukkaukset

Jos tutkimuksen rekisterinpitäjä, esim. väitöskirjatyössä, on yksittäinen rekisterinpitäjä ja käsitellään laajamittaisesti erityisiä henkilötietoryhmiä koskevaa aineistoa, tietosuojavastaava on nimettävä. Voitko tutkija olla itse myös tietosuojavastaava?

Jos tutkija on rekisterinpitäjä, ei se voi samanaikaisesti olla tietosuojavastaava. Tietosuojavastaavan on oltava riippumaton, eikä hänellä voi olla eturistiriitoja tietosuojavastaavan tehtävien kanssa. Koska jokainen organisaatio on erilainen, eturistiriitoja on tarkasteltava tapauskohtaisesti.

Tietosuojavastaava ei voi olla sellaisessa asemassa tai tehtävässä, jossa hänen on määritettävä henkilötietojen käsittelyn tarkoitukset ja keinot. Henkilötietojen käsittelyn tarkoitusten ja keinojen määrittely on rekisterinpitäjälle kuuluva tehtävä. Eturistiriitoja voi syntyä, jos tietosuojavastaavaksi on nimetty esimerkiksi tietoturvavastaava tai ylimmän johdon edustaja.

Voiko työntekijäasemassa oleva (esim. tutkija) olla rekisterinpitäjänä?

Jos tutkimushankkeeseen osallistuu useampia tahoja, on tunnistettava eri toimijoiden roolit. Se, että tutkija on työntekijä asemassa, ei estä sitä, että hänelle voisi muodostua rekisterinpitäjän rooli. Lopullinen analyysi rooleista on kuitenkin tehtävä tapauskohtaisten tunnusmerkkien ja tietosuoja-asetuksen rekisterinpitäjä määritelmän pohjalta.

Tietosuoja-asetuksen mukaan rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot (TSA 4 artikla 7 kohta).

Tietosuoja-asetus tunnistaa myös yhteisrekisteripitäjyyden. Yhteisrekisteripitäjyydessä on kysymys silloin, toimijat määrittelevät yhdessä henkilötietojen käsittelyn tarkoitukset ja keinot sekä jakavat rekisterinpitäjän vastuun. Tällöin yhteisrekisterinpitäjien tulee tietosuoja-asetuksen 26 artiklan mukaisesti määritellä keskinäisellä järjestelyllä ja läpinäkyvällä tavalla kunkin vastuualueet tietosuoja-asetuksessa olevien velvoitteiden noudattamiseksi. Tehtävänjaon rekisteröidyn oikeuksien käytön sekä rekisteröidyn informoinnin osalta on oltava selkeä. Järjestelystä on käytävä asianmukaisesti ilmi yhteisten rekisterinpitäjien todelliset roolit ja suhteet rekisteröityihin nähden. Järjestelyn keskeisten osien on oltava rekisteröidyn saatavilla.

Voiko arkaluonteisia tietoja käyttää Microsoftin pilvipalveluissa, esim. Yammer?

Yrityksen tai organisaation saattaa olla hankala tai jopa mahdoton näyttää toteen esimerkiksi GDPR:n 32 artiklan vaatimukset käsittelyn tietoturvallisuudelle. Esimerkiksi Yammer yleensä postittaa keskustelut

sähköpostilla niille ryhmän jäsenille, jotka eivät ole keskustelun aikana aktiivisesti läsnä, mutta on esimerkiksi mainittuna keskustelussa. Mobiiliudessa ja pilvipalveluiden käytössä kannattaa huomioida, että käsiteltävä tieto saattaa levitä hallitsemattomasti organisaation ulkopuolisiin laitteisiin.

Henkilötietojen määritelmä esitettiin muodossa identifioivat henkilötiedot. Mitkä kaikki ovat henkilötietoja?

Henkilötietojen määritelmä löytyy tietosuojavaltuutetun toimiston verkkosivuilta osoitteesta https://tietosuoja.fi/mika-on-henkilotieto

Julkisen terveydenhuollon puolen palautekyselyt: Jos palautteessa mainitaan lääkärin tai sairaanhoitajan nimi, tuleeko se pseudonymisoida tai anonymisoida palautteista.

Henkilötietoja tulee aina käsitellä vain siinä määrin, kuin se on tarpeellista. Jos siis kyselystä saatavia palautteita käsitellään sellaisiin tarkoituksiin, joissa työntekijän yksilöinti ei ole tarpeen, on yksilöivät tiedot syytä poistaa palautteesta. Työntekijöiden henkilötietojen käsittelyssä tulee lisäksi ottaa huomioon, mitä yksityisyyden suojasta työelämässä on säädetty.

Olisiko tietosuojan työkirjasta esimerkkiä?

Ei toistaiseksi ole.

IP-osoite ja eväste. Kannattaako niistä kovin vauhkoilla? IP osoite, joka näkyy, ei ole minun (välttämättä) vaan palomuurin tai koulun/kirjaston tietokoneen -> ei henkilötieto

IP-osoite: Eri laitteet käyttävät IP-osoitteita, kun ne kommunikoivat tietoverkoissa, esimerkiksi internetissä. Osa IP-osoitteista on niin sanotun yksityisverkon osoitteita, jolloin julkiseen internetiin näkyy vain palvelun tarjoajan yhdyskäytävän julkinen IP-osoite. Esimerkiksi puhelimet ja koti-adsl-reitittimet saattavat taas käyttää hyvin pitkiä aikoja samaa julkista IP-osoitetta, jolloin laitteen käyttämä internet-yhteys pystytään kohdistamaan käyttäjään. Esimerkiksi IP-osoite jää www-palvelimien lokitietoihin, joissa taas näkyvät myös www-palvelimelta pyydetyt sivut tai www-palvelimelle lähetetyt tiedot. IP-osoite on henkilötieto ja se voidaan monissa tapauksissa liittää käyttäjään. Erityisen tarkkaan kannattaisi miettiä, antaako sijaintitietojaan (esimerkiksi selaimen kysymiä), koska yhdessä IP-osoitteen kanssa voidaan myös henkilön liikkumista paikantaa. Tulee kuitenkin huomioida, että laitteet jotka on yhdistetty tietoverkkoon, tarvitsevat toimiakseen IP-osoitteita, sen käyttöä ei voida estää.

Evästeet: Toiminnallisuuden kannalta evästeet ovat välttämättömyys www-sivuille. Usein evästeisiin liittyvä huoli liittyy niin sanottuihin kolmannen osapuolen evästeisiin, jotka taas eivät ole välttämättömyys. Kolmannen osapuolen evästeillä seurataan eri internet-sivujen käyttöä ja kohdennetaan mainontaa automaattisesti evästeiden muodostaman tiedon perusteella. Kolmannen osapuolen evästeet voivat kerätä paljonkin henkilötietoja henkilöstä. Evästeistä on tulossa syksyn aikana ohjeistusta tietosuoja.fi-sivustolle.

Miten verohallinnossa todennetaan tietopyynnön tekijän henkilöllisyys?

Tällä hetkellä verohallinnolla ei ole sähköistä tunnistautumista, tämä korjautuu, kun OmaVero-palvelu otetaan käyttöön.

Miten ohjeistaa tutkimusyhteistyötä kiinalaisten kanssa?

Kysymyksen epämääräisyydestä johtuen joudun antamaan vastauksen erittäin yleisellä tasolla. Jos tutkimusyhteistyössä tapahtuva henkilötietojen käsittely kuuluu tietosuoja-asetuksen soveltamisalaan, tulee tutkimustyössä huomioida tietosuoja-asetuksesta sekä sitä täydentävästä kansallisesta laista tulevat vaatimukset. Mikäli henkilötietoja on tarkoitus siirtää Kiinaan, on huomioitava myös henkilötietojen ulkomaille siirtoa koskevat säännökset. Yleisen tietosuoja-asetuksen ((EU) 2016/679) 44 artiklassa ilmaistun siirtoja koskevan yleisen periaatteen mukaan henkilötietoja saadaan siirtää kolmannessa maassa tapahtuvaa henkilötietojen käsittelyä varten vain, jos tietosuoja-asetuksen V luvussa vahvistettuja edellytyksiä noudatetaan ja jos tietosuoja-asetuksen muista säännöksistä ei muuta johdu.

Kameravalvonta: nauhat säilyy 14 pv. Asiakkaalle (henkilö kuvassa) pitää vastata 1 kk kuluessa. Eli ei ole mitään näytettävää kuvamateriaalia. Onko laillinen menettely?

Tietosuoja-asetuksen 15 artiklan mukaan rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja jos näitä henkilötietoja käsitellään, oikeus saada pääsy henkilötietoihin.

Tietosuoja-asetus 5 artiklan 1.c -kohdan mukaan henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään (”tietojen minimointi”). Jos rekisterinpitäjä on määritellyt kameratallenteiden säilytysajaksi 14 pv, asiakkaalle vastataan ettei ko. tallennetta enää ole.

Onko Espoossa käytössä joku sähköinen työkalu organisaation tietoturvapoikkeamien ilmoittamiselle? Jos on niin mikä?

Ei ole (vastaajana Espoon kaupungin tietosuojavastaava Juho Nurmi).

Onko vaikutusten arvioinnista tulossa suomalaista mallia vrt. Ranskan tietosuojaviranomaisten PIA?

Ranskalaisten tuottama DPIA-työkalu on käännetty suomeksi ja sitä hyödynnetään jatkossa myös meillä.

Tuleeko vaikutustenarviointi tehdä, jos rekisterinpitäjä (ei terveydenhuollon palvelujen tuottaja) käsittelee arkaluonteisia henkilötietoja?

Enemmän tietoa siitä, milloin vaikutustenarviointi tulee tehdä, on tietosuojavaltuutetun toimiston verkkosivuilla https://tietosuoja.fi/vaikutustenarviointi. Samalla sivulla on linkki myös esimerkkitapauksiin.

Onko aineiston omistajuus ja se kuka on rekisterinpitäjä eri asia?

Tietosuojan yhteydessä ei tunneta immateriaalioikeuden kaltaista omistajuuden käsitettä. Rekisterinpitäjä on se, joka hallinnoi tietoa.

Näyttää siltä, ettei Espoossa ole sosiaali- ja terveystoimessa tietosuojavastaavaa? Eikä työterveyshuollossa? On tietosuojan yhdyshenkilöitä. Eikö terveyspalveluissa ole pakko olla seurantaa ja valvontaa varten nimitetty lakisääteinen tietosuojavastaava? Vai hoitaako Espoon kaupungin tietosuojavastaava myös terveydenhuollon ja työterveyshuollon sähköisen valvonnan ja muut tehtävät? Melkoisen iso kakku yhdelle ihmiselle, jos aikaa riittää tuon kokoisessa kaupungissa hoitamaan myös nuo lakisääteiset tietosuojavastaavien tehtävät.

Espoossa on työterveyshuollossa tietosuojavastaava. Sosiaali- ja terveystoimessa tietosuojavastaavan rooli on jaettu lakimiesten (juridinen puoli) ja järjestelmäasiantuntijan (lokitietojen tarkastuspyynnöt) kesken. On kyllä alustavasti keskusteltu, voisiko tietosuoja-asetuksen edellyttämä tietosuojavastaava kattaa koko organisaation. Tietenkin tekninen valvonta säilyisi edelleen sote-puolella (vastaajana Espoon kaupungin tietosuojavastaava Juho Nurmi).

Jos työkännykkä häviää, tai varastetaan, siitä tehdään rikosilmoitus. Miten on, pitääkö tietosuojan nimissä tehdä jotain?

Työkännykän tai muun henkilötietoja sisällä pitävän välineen hävitessä tulee pohtia, onko tapauksessa syntynyt tietoturvaloukkaus. Tietoturvaloukkauksen sattuessa rekisterinpitäjän on noudatettava tietosuoja-asetuksen 33 artiklan mukaista velvoitetta ilmoittaa loukkauksesta valvontaviranomaiselle.

Lisäksi rekisterinpitäjän on arvioitava, aiheuttaako kyseinen loukkaus korkean riskin rekisteröidylle. Arvioinnissa tulee ottaa huomioon esimerkiksi henkilötietojen laatu ja määrä, tunnistamisen helppous, ovatko sivulliset käyttäneet tietoja, onko indikaatioita laittomasta käsittelystä ja mahdollisten seurauksien vakavuus.

Asetuksen mukaan henkilötiedoilla tarkoitetaan tietoja, jotka LIITTYVÄT tunnistettuun tai tunnistettavissa olevaan henkilöön. Ei siis edellytä, että henkilötiedon perusteella henkilö voitaisiin tunnistaa?

Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Tunnistettavissa oleva luonnollinen henkilö on henkilö, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen tai verkkotunnistetietojen perusteella.

Henkilötietoja voi olla talletettuna esimerkiksi sähköisissä tiedostoissa, tietokannoissa, paperilla, kortistossa, mapeissa tai ääni- tai kuvatallenteella.

Erilaisia käsityksiä on esimerkiksi siitä, milloin on kyse tietosuoja-asetuksen mukaisesta rekisteröidyn omia tietoja koskevasta pyynnöstä. Puhutaan tarkastuspyynnöistä sisällyttäen näihin vain pyynnöt, jossa henkilö pyytää nähtäväkseen kaiken, mitä organisaatiolla on hänestä kerättynä. Eikö kuitenkin myös yhteen tiettyyn esim terveystietoon kohdistuva pyyntö ole aivan yhtä lailla TsA:ssa tarkoitettua pääsyä omiin tietoihin?

Rekisteröity voi pyytää jotain tiettyä asiaa tai sitten kaikkia tietojaan kyseisen yrityksen henkilötietokannoista.

Pitääkö sotun loppuosa antaa palveluntarjoajalle tunnistautumiseksi? Vai onko sotulla enää mitään suurempaa merkitystä?

Mahdollisesti.

Henkilötunnus on yksilöimiskeino. Henkilötunnusta ei ole tarkoitettu henkilöiden tunnistamiseen. Tietosuoja-asetuksessa henkilötunnus ei kuulu 9 artiklan erityisiin henkilötietoryhmiin. Kansallisen henkilötunnuksen käsittelystä säädetään tietosuoja-asetuksen 87 artiklassa. Kyseisessä artiklassa säädetään, että ”Jäsenvaltiot voivat määritellä tarkemmin erityiset kansallisen henkilönumeron tai muun yleisen tunnisteen käsittelyn edellytykset. Tässä tapauksessa kansallista henkilönumeroa tai muuta yleistä tunnistetta on käytettävä ainoastaan noudattaen rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia tämän asetuksen mukaisesti”.

Tietosuojalakiehdotus (HE 9/2018) on vielä valmistelussa eduskunnassa. Lakiehdotus sisältää pykälän henkilötunnuksen käsittelystä ja käsittelyn edellytyksistä.

Lisätietoa henkilötunnuksen käytöstä saatte https://tietosuoja.fi/usein-kysyttya-henkilotunnus -sivustolta.

Pitääkö allekirjoitukset pöytäkirjoista nyt poistaa/mustata, koska on henkilötietoa? Onko eroa organisaation edustaja, nimenselvennyksen kanssa/ilman? Allekirjoitushan on helppo kopioida (identiteettivarkaus).

Kysymykseen ei voi yksiselitteisesti ottaa kantaa tuntematta sen yksityiskohtia. Allekirjoituksella vahvistetaan tai hyväksytään allekirjoitetun asiakirjan sisältö, ja virallisissa asiakirjoissa on yleensä oltava allekirjoitukset. Joissain tapauksissa, jos asiakirjaa käytetään asiayhteydessä, joka ei suoraan liity allekirjoittajaan, hänen allekirjoituksensa voi olla syytä mustata.

Miksi "työnantajaorganisaatio" omistaa työntekijöiden rekisteritiedot ja on siksi rekisteripitäjä eikä esim. Palkeet, joka kuitenkin käsittelee tiedot palkkojen maksua varten. Ja tiedot on toimitettava nimenomaan palkeiden määrittämällä tavalla.

Rekisterinpitäjä on se taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Henkilötietojen käsittelijä on se taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Rekisterinpitäjä voi ulkoistaa henkilötietojen käsittelyn, esimerkiksi palkan maksun. Tässä tilanteessa kyse voi olla henkilötietojen käsittelemisestä rekisterinpitäjän lukuun.

Pitääkö kunnan tietosuojavastaavalla olla oikeudet kaikkiin asioihin ja asiakirjoihin vai riittääkö, että ne lisätään hänelle tarvittaessa? Meillä pyytää oikeudet sote-asioihin, vaikka niihin ei liittyisi tietosuojaongelmia tms.

WP29 on tietosuojavastaavia koskevassa ohjeessa todennut, että tietosuojavastaavan läsnäolo on suositeltavaa tehtäessä päätöksiä, joilla on vaikutusta tietosuojaan. Tietosuojavastaavalle tulee toimittaa kaikki olennaiset tiedot, jotta tämä voi antaa asianmukaisia neuvoja.

Tietosuojavastaavalle tulee ohjeen mukaan järjestää tarvittaessa pääsy muihin palveluihin /esim. henkilöstöresurssit, oikeudellinen neuvonta, tietotekniikka), jotta hän voi saada niistä olennaista tukea ja tietoa.

Ohjeissa ei ole mainittu mitä asiakirjoja tietosuojavastaavalle tulee toimittaa tai mihin tietoihin sillä on oltava oikeudet ja pääsy.

Kunnan työntekijöitten puhelinluettelotiedot on Elisan konesalissa. Kunta syöttää tiedot Elisan järjestelmään. Onko Elisa rekisterinpitäjä vai Kunta vai molemmat. Kumpi informoi asiakasta henkilötietojen käsittelystä pyydettäessä? Vai eikö puhelinluettelo ole edes henkilörekisteri vaan yhteystieto (joka sisältää henkilötietoja)?

Henkilötiedolla tarkoitetaan kaikkia tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistetiedoiksi voidaan katsoa esimerkiksi nimi, henkilötunnus, sijaintitieto ja verkkotunnistetieto.

Tietosuoja-asetuksen 4 artiklan mukaan rekisterinpitäjä on se taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjän vastuulla on informoida rekisteröityjä henkilötietojen käsittelystä. Henkilötietojen käsittelijä puolestaan on se taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.