GDPR ei toimi

Tietosuojakäytännöt eivät noudata asetusta

VALTTERI SANKARI & MATTI WIBERG

Toimiiko GDPR[1] käytännössä? Julkisessa keskustelussa yleiseksi tietosuoja-asetukseksi kutsuttu asetus annettiin 27.4.2016, ja se astui voimaan 25.5.2018. Toimijoilla oli asetuksen antamisesta 24 kuukautta 29 päivää aikaa varmistaa, että niiden toiminta noudattaa säädöstä.

Tietosuoja ja henkilötietojen käsittely koskettavat kaikkia. Euroopan komissio (2017) arvioi tietotalouden (*data economy*) arvoksi lähes 300 miljardia euroa vuonna 2016, ja sen ennustettiin kasvavan jopa 739 miljardiin vuoteen 2020 mennessä. Säädöksen voimaan astumisen jälkeen tietosuojavaltuutetulle on tullut jo 2 700 rekisterinpitäjien ilmoitusta henkilötietojen tietoturvaloukkauksista. (Tietosuojavaltuutetun toimisto, 2019). Ovatko kansalaiset, julkisorganisaatiot ja yritykset perillä asetuksen määräyksistä?

Henkilötiedot ovat kunkin yksilön omaisuutta. Vääriin käsiin joutuneet henkilötiedot voivat aiheuttaa yksilölle taloudellista ja henkistä vahinkoa. Identiteettivarkaudessa esiinnytään toisen henkilöllisyydellä ja tarkoituksellisesti erehdytetään kolmatta osapuolta. Toisen identiteetin käyttäminen voi olla rangaistavaa myös petoksena, väärennöksenä, kunnianloukkauksena tai yksityiselämää loukkaavan tiedon levittämisenä.

Yksilöllä on oikeus yksityisyyteen ja tietosuojaan. Tietoja ei kerätä pelkästään ensisijaiseen käyttötarkoitukseensa (esim. palvelun mahdollistamiseksi) vaan myös toissijaiseen käyttötarkoitukseen (esim. mainosrekisterin ylläpitämiseen). Kaikkia tulevia käyttötarkoituksia ei vielä ole edes mahdollista hahmottaa.

EU:n aikaisempi tietosuojadirektiivi vuodelta 1995 määritteli vaatimuksia kansallisille lainsäädännöille tietosuojan toteuttamiseksi, ja tämä johti tulkintaeroihin jäsenmaiden välillä. GDPR pyrkii harmonisoimaan tietosuojalainsäädäntöä, koska asetuksena sitä sovelletaan sellaisenaan. Silti kansallisesti säännellään varsinkin viranomaisten laillisia perusteita tietojen käsittelylle. Suomessa astui voimaan 1.1.2019 Tietosuojalaki (1050/2018), jolla täsmennetään ja täydennetään asetusta.

Pitkät ja vaikeaselkoiset tietosuojaselosteet ovat arkipäivää, mutta vahvistavatko ne yksilöiden tietosuojaa. Ovatko toimijoiden käytännöt niiden omien tietosuojaselosteiden mukaisia? Voiko yksilö varmistua rekisterinpitäjien toimien lainmukaisuudesta? Yritysten tietojenkeräys- ja hyödyntämisalgoritmit ovat kilpailuvaltteja, ja niitä suojaavat liikesalaisuuslait. Pelkkä luottamus rekisterinpitäjään ei takaa yksityisyydensuojaa.

GDPR ilmentää aikamme trendejä: läpinäkyvyyttä, tilivelvollisuutta ja byrokratian vähentämistä. Ne eivät ole itseisarvoja, vaan niihin liittyvät omat ongelmansa. Niiden sisällöistä ei myöskään ole yksimielisyyttä.

Suostumus

GDPR:ssä on useita perusteita henkilötietojen lailliselle käsittelylle, ja yksi niistä on henkilön suostumus. Suostumus on yleisesti hyväksytty peruste henkilötietojen käsittelylle. Antamalla suostumuksensa henkilö luopuu osasta yksityisyydensuojaansa.

Tietosuoja on osa yksityisyydensuojaa, joka on yleisesti hyväksytty perustuvanlaatuiseksi oikeudeksi, mutta se ei ole täysin rajoittamaton. Yksityi-

1 GDPR eli General Data Protection Regulation on Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.

syydensuoja on suhteellista, ja se voi olla alisteinen muille tärkeille yhteiskunnallisille tavoitteille. Säädökset määrittelevät tietojen laillisen käsittelyn.

Jotkut asiantuntijat ja poliitikot asettavat yksityisyyden ja tietosuojan vastakkain muiden legitiimien arvojen, kuten tehokkuuden, innovaatioiden ja taloudellisen kasvun, kanssa. He siirtäisivät yksityisyydensuojasta huolehtimisen tallettajien kontolle ja vähentäisivät yksilön hallintamahdollisuuksia.

Suostumuksen tarkoituksena on voimaannuttaa yksilöitä ja antaa heille valtuudet vaikuttaa henkilötietojensa käsittelyyn. Toteutuuko tämä käytännössä? Seuraavaksi määrittelemme eräitä peruskäsitteitä:

Henkilö tarkoittaa luonnollista henkilöä, ei oikeushenkilöä tai tekoälyn avulla toimivaa järjestelmää.

Henkilötieto tarkoittaa kaikkia tunnistetun tai tunnistettavissa olevan luonnollisen henkilön tietoja.

Käsittely tarkoittaa henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin kohdistettuja automaattisia tai manuaalisia toimintoja. Tällaisia ovat esimerkiksi tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, kysely, käyttö, tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

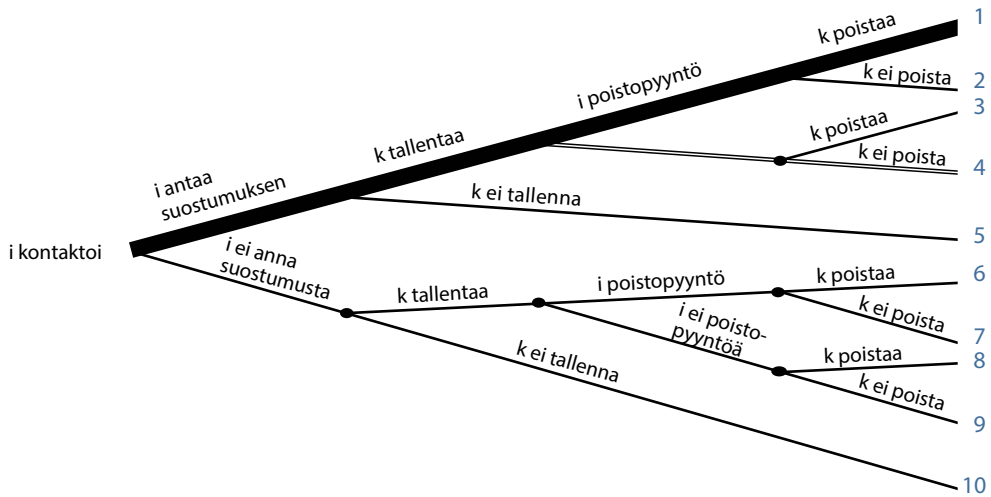
Rekisteri tarkoittaa mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.

Käsittelijä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Rekisterinpitäjä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Relevantit pelaajat ovat yksityishenkilöt, yritykset, julkisyhteisöt ja valvontaviranomaiset. Mallinnamme vuorovaikutuksen yksinkertaisimmillaan kahden toimijan, yksilön i ja käsittelijän k, pelinä (kuvio 1).

Mahdollisia polkuja on 10. Suostumuspelin polku, jossa yksilö käyttää oikeuttaan tulla unohdetuksi ja käsittelijä toteuttaa pyynnön, on lihavoitu. Käytännössä yleisin polku lienee numero 4. Tiedot pitää kuitenkin poistaa ilman eri pyyntöä, kun niitä ei enää tarvita alkuperäiseen käyttötarkoitukseen.



Kuvio 1. Suostumuspelin pelipuu.

Tiedossamme on ainakin kaksi tapausta (Specsavers, Mehiläinen), jossa asiakas ei ole antanut suostumustaan, mutta yritykset ovat silti tallentaneet hänestä tietoja eivätkä ole niitä asiakkaan nimenomaisesta kirjallisesta pyynnöstä huolimatta poistaneet (polku 7).

EU-säädöksissä on johdanto-osa ennen varsinaista säädösosaa artikloineen. Johdanto-osan teksti ei ole oikeudellisesti sitovaa, mutta siinä esitetään säädöksen tavoitteet ja perustelut. Niitä käytetään apuna artiklatekstien tulkinnassa. GDPR:n johdanto-osan kappaleessa 32 on suostumuksesta seuraavaa:

”Suostumus olisi annettava selkeästi suostumusta ilmaisevalla toimella, kuten kirjallisella, mukaan lukien sähköisellä, tai suullisella lausumalla, josta käy ilmi rekisteröidyn vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsittelyn. Toimi voisi esimerkiksi olla se, että rekisteröity rastittaa ruudun vieraillessaan internetsivustolla, valitsee tietoyhteiskunnan palveluiden teknisiä asetuksia tai esittää minkä tahansa muun lausuman tai toimii tavalla, joka selkeästi osoittaa tässä yhteydessä, että hän hyväksyy henkilötietojensa käsittelyä koskevan ehdotuksen. Suostumusta ei sen vuoksi pitäisi voida antaa vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jokin toimi toteuttamatta. Suostumuksen olisi katettava kaikki käsittelytoimet, jotka toteutetaan samaa tarkoitusta tai samoja tarkoituksia varten. Jos käsittelyllä on useita tarkoituksia, suostumus olisi annettava kaikkia käsittelytarkoituksia varten. Jos rekisteröidyn on annettava suostumuksensa sähköisen pyynnön perusteella, pyynnön on oltava selkeä ja tiiviisti esitetty eikä se saa tarpeettomasti häiritä sen palvelun käyttöä, jota varten se annetaan.”

Johdanto-osan kappaleessa 42 puolestaan on suostumuksesta seuraavaa:

”Kun tietojenkäsittely perustuu rekisteröidyn suostumukseen, rekisterinpitäjän olisi voitava osoittaa, että rekisteröity on antanut suostumuksensa käsittelytoimiin. Etenkin jos suostumus annetaan muuta seikkaa koskevan kirjallisen ilmoituksen yhteydessä, olisi varmistettava suojatoimin, että rekisteröity on tietoinen antamastaan suostumuksesta ja siitä, kuinka pitkälle menevästä suostumuksesta on kyse. Neuvoston direktiivin 93/13/ETY (10) mukaisesti rekisterinpitäjän ennalta muotoilema ilmoitus suostumuksesta olisi annettava helposti ymmärrettävässä ja helposti saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä eikä siihen pitäisi sisältyä kohtuuttomia ehtoja. Tietoisen suostumuksen antamiseksi rekisteröidyn olisi tiedettävä vähintään rekisterinpitäjän henkilöllisyys ja tarkoitukset, joita varten henkilötietoja on määrä käsitellä. Suostumusta ei voida pitää vapaaehtoisesti annettuna, jos rekisteröidyllä ei ole todellista vapaan valinnan mahdollisuutta ja jos hän ei voi myöhemmin kieltäytyä suostumuksen antamisesta tai peruuttaa sitä ilman, että siitä aiheutuu hänelle haittaa.”

GDPR:n 7. artiklassa on suostumuksesta seuraavaa:

”Suostumuksen edellytykset

1. Jos tietojenkäsittely perustuu suostumukseen, rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn.
2. Jos rekisteröity antaa suostumuksensa kirjallisessa ilmoituksessa, joka koskee myös muita asioita, suostumuksen antamista koskeva pyyntö on esitettävä selvästi erillään muista asioista helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Mikään tätä asetusta rikkova osa sellaisesta ilmoituksesta ei ole sitova.
3. Rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa. Suostumuksen peruuttaminen ei vaikuta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen. Ennen suostumuksen antamista rekisteröidylle on ilmoitettava tästä. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin sen antaminen.
4. Arvioitaessa suostumuksen vapaaehtoisuutta on otettava mahdollisimman kattavasti huomioon muun muassa se, onko palvelun tarjoamisen tai muun sopimuksen täytäntöönpanon ehdoksi asetettu suostumus sellaisten henkilötietojen käsittelyyn, jotka eivät ole tarpeen kyseisen sopimuksen täytäntöönpanoa varten.”

Nostamme esiin eräitä oleellisuuksia:

Yksiselitteinen. Yksilön suostumus henkilötietojensa käsittelyyn on osoitettava yksiselitteisesti. Suostumusta kerättäessä ei saa olla epäselvyyttä siitä, onko yksilö suostunut henkilötietojensa käsittelyyn vai ei. Käsittelijän tai rekisterinpitäjän on osoitettava suostumuksen olemassaolo.

Lausuma tai selkeästi suostumusta ilmaiseva toimi. Suostumuksen pitää olla selkeä yksilön suostumusta ilmaiseva tahdonilmaisu. Suostumusta ei voi antaa hiljenemällä tai jättämällä jotain tekemättä. Kontekstuaalinen implikatuuri ei täytä suostumuksen ehtoja: suostumusta ei voi päätellä pelkästään asiayhteydestä. Suostumus on annettava nimenomaisesti ja varta vasten.

Vapaaehtoinen. Yksilöllä pitää olla todellinen valinnan mahdollisuus. Yksilöä ei saa johtaa harhaan, pakottaa tai rangaista suostumuksen antamatta jättämisestä. Sopimuksen ehtona ei saa olla sellaisten henkilötietojen tallentaminen, jotka eivät ole tarpeellisia sopimuksen täytäntöönpanemiseksi. Suostumus ei ole vapaaehtoinen, jos rekisteröidyn ja käsittelijän välillä on selkeä epäsuhta (esimerkiksi yksilö – julkinen virasto tai työntekijä–työnantaja). Suostumus ei ole vapaaehtoisesti annettu, jos ei ole mahdollisuutta antaa erillistä suostumusta eri käsittelytarkoituksille.

Yksilöity. Suostumus pitää antaa erillään muista käsiteltävistä asioista. Suostumuksen pitää kat-

taa kaikki käsittelytoimet, joilla on sama tarkoitus. Muihin tarkoituksiin tarvitaan erilliset suostumukset. Suostumuksen antaminen ei anna rekisteröijälle vapaita käsiä käyttää henkilötietoja. Suostumusta ei voi antaa osana muiden ehtojen hyväksymistä.

Tietoinen. Yksilön pitää tietää rekisterinpitäjän henkilöllisyys ja käsittelyn tarkoitukset. Yksilölle pitää kertoa mahdollisuudesta perua suostumus. Asetuksen 12–14 artikloissa on lista tiedoista, jotka on annettava yksilölle, jotta tämä voi varmistua henkilötietojen reilusta ja läpinäkyvästä käsittelystä. Käsittelyä koskevat tiedot on esitettävä tiiviissä, läpinäkyvässä, helposti ymmärrettävässä ja saatavissa olevassa muodossa.

Suostumuksen antamisen jälkeen yksilöllä on oikeuksia. Suostumuksen voi perua ja kerätyt tiedot on mahdollista nähdä. Peruminen on oltava yhtä helppoa kuin suostumuksen antaminen. Henkilötietoja ei saa säilyttää ikuisesti, vaan vain sen aikaa kuin se on tarpeen alkuperäisen tarkoituksen toteuttamiseksi. Rekisterinpitäjän on kerrottava yksilölle, miten kauan henkilötietoja säilytetään tai miten säilytysaika määräytyy. Merkittäviä kansallisesti säädettyjä henkilötietojen käsittelyä määritteleviä lakeja on sosiaali- ja terveydenhuollossa sekä rikosasioissa, ja ne on otettava huomioon asetuksen lisäksi.

Sosiaali- ja terveydenhuollon asiakkaiden ja potilaiden henkilötietojen käsittelyssä GDPR:ää sovelletaan osin, mutta sitä täydennetään kansallisella lainsäädännöllä. Lista laeista, asetuksista ja ohjeista on sisäministeriön (2019) verkkosivuilla. Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018) määrittelee henkilötietojen käsittelyä rikosasioissa.

Asetuksen selostusaineistoja on moninaisia ja niiden laatu vaihtelee suuresti. Jokaisella on oma näkökulmansa asetukseen. Yksilöiden kohdalla kyse on itsemääräämisoikeudesta. Yritysten intresseissä on käyttää henkilötietoja asiakkaan palvelemiseen, oman liiketoiminnan kehittämiseen ja markkinointiin. Monen verkkoyrityksen kauppatavaraa ovat käyttäjistään kerätyt tiedot. Julkisyhteisöt keräävät tietoja omien palveluidensa tuottamiseen. Niiden vastuulla on myös säädöksen tehokas valvonta. Moniulotteisessa konfliktikentässä on mahdotonta maksimoida samanaikaisesti kaikkien intressejä.

Tiettävästi Suomessa ei ole aiemmin testattu järjestelmällisesti GDPR:n käytännön toimivuutta. Toimittaja Anni Lassila (2019) tosin testasi oikeutta saada hänestä kerätyt tiedot.

Testi

Testaamme seuraavat hypoteesit:

H1: Toimijoiden tietosuojakäytännöt ovat asetuksen mukaisia, eli ne noudattavat asetuksen määräyksiä.

H2: Suostumus henkilötietojen käsittelyyn annetaan nimenomaisesti, eli se täyttää asetuksessa määritellyt suostumuksen kriteerit.

H3: Suostumuksen peruuttaminen on yhtä vaivatonta kuin sen antaminen, eli suostumuksen perumisen jälkeen henkilötietojen poisto tai muut toimenpiteet tapahtuvat yksilön kannalta yhtä vaivattomasti kuin suostumuksen antaminen.

H4: Toimijoiden tietosuojakäytännöt ovat yhdenmukaisia yritysten ja virastojen kesken, eli ne toimivat samalla GDPR:n määräämällä tavalla.

Sovellamme toimintatutkimuksen tekniikoita. Pääasiallinen aineistonkeruumetodimme on toimintatutkimuksessa laajasti käytetty havainnointi. Valitsimme kohteet julkiselta ja yksityiseltä sektorilta. Tärkeä kriteeri oli koko, koska asetus on tiukempi yli 250 työntekijän yritykselle. Suuren yrityksen tai viraston ja yksilön välillä on suurin ero käytettävissä olevien resurssien ja vallan suhteen. Suurilla toimijoilla on enemmän voimavaroja saattaa tietosuojakäytäntönsä lainmukaisiksi kuin pienillä. Jokaisella kohteella on verkkosivuillaan GDPR:n mukainen tietosuojaseloste sekä tietosuojavastaavan yhteystiedot.

Kävimme seuraavissa kohteissa: DNA, Elisa, Instrumentarium, Mehiläinen, Osuuspankki, Specsavers, Telia, Terveystalo, Turun kaupunginkirjasto, Turun seudun joukkoliikenne ja Ylioppilaiden terveydenhoitosäätiö. Kaikki toimipisteet sijaitsivat Turussa. Sähköisesti otimme yhteyttä näihin kohteisiin: Apple, Facebook, Google, Sanoma Oyj, Traficom, Veikkaus, VR ja YLE.

Toteutimme testin tammi-maaliskuussa 2019 käymällä yrityksessä tai virastossa tai ottamalla yhteyttä sähköisesti verkkosivujen kautta tai sähköpostilla. Käyntejä oli 11 ja sähköisiä yhteydenottoja kahdeksan. Käyntien kesto oli noin puoli tuntia.

Yrityksiin menimme mahdollisena tulevana asiakkaana tai henkilötietojen käsittelystä kiinnostuneena nykyisenä tai entisenä asiakkaana. Virastoihin menimme henkilötietojen käsittelystä kiinnostuneena kansalaisena. Tapaamistilanteet eivät olleet tarkkaan strukturoituja, koska tutkimme

tavallista vuorovaikutusta asiakkaan ja työntekijän välillä.

Suostumuspeliä testasimme käytännössä esittäytymällä neljässä kohteessa uudeksi asiakkaaksi ja havainnoimalla käsittelijän ja yksilön vuorovaikutusta. Seitsemässä kohteessa kävimme nykyisenä asiakkaana. Kysyimme, onko suostumus annettu, ja jos on, niin miten, milloin ja mihin tarkoitukseen.

Suostumuksen havainnoinnin lisäksi kysyimme yleisesti tietosuojasta ja henkilötietojen käsittelystä. Yleisimpiä kysymyksiä olivat: mitä henkilötietoja käsitellään, mitä tarkoitusta varten niitä käsitellään, ketkä henkilötietoja voivat käsitellä, miten luvaton käsittely estetään, miten kauan tietoja säilytetään ja luovutetaanko niitä kolmansille osapuolille? Tarkoituksena oli osaltaan arvioida, miten asetuksessa mainitut henkilötietojen käsittelyä koskevat periaatteet toteutuvat. Havainnot kirjattiin heti tapaamisen päätyttyä.

Sähköinen yhteydenotto toteutettiin 27. helmikuuta 2019 sähköpostilla tai verkkosivulla olevalla lomakkeella ja kahdella muistutuskierroksella. Tietosuojaselosteissa toistuu oikeutettu etu perusteena henkilötietojen käsittelylle. Se mainitaan asetuksessa kuudennen artiklan f-kohdassa sekä johdanto-osan kappaleissa 47–49. Oikeutettu etu voi tulla kyseeseen asiakassuhteessa. Yksilön perus- ja vapausoikeudet voivat syrjäyttää oikeutetun edun. Yksilöllä on oikeus ottaa yhteyttä tietosuojavastaavaan henkilötietojensa käsittelyyn ja oikeuksiinsa liittyen GDPR:n 38. artiklan 4. kohdan perusteella.

Kaikkiin kohteisiin lähetettiin seuraavat kysymykset:

1. Mitä te tarkoitatte oikeutetulla edulla?
2. Milloin oikeutettu etu on perusteena henkilötietojen käsittelylle?
3. Miten arvioitte, onko käsittely lainmukaista oikeutetun edun perusteella?
4. Milloin yksilön vapaus- ja perusoikeudet estävät oikeutetun edun perusteella tehtävän käsittelyn?
5. Kuka käsittelee henkilötietoja?
6. Miten käsittelyä valvotaan?
7. Miten luvaton käsittely estetään?
8. Mitä vaikutuksia henkilötietojen käsittelyn rajoittamisella on?
9. Miten arvioitte tietojen säilytysajan?
10. Miten säilytysaika ilmoitetaan asiakkaalle?
11. Miten säilytysajan voi ennakoida?
12. Miten henkilötiedot pseydonymisoidaan?
13. Voiko asiakas varmistua pseydonymisoinnin onnistumisesta?
14. Mitä henkilötietoja käsitellään suostumuksen perusteella?
15. Miten osoitatte suostumuksen?
16. Ovatko GDPR:n vaatimukset mielestänne selkeitä?
17. Ovatko GDPR:n vaatimukset mielestänne suoraviivaista implementoida?

Pyysimme kohteita vastaamaan kahden viikon kuluessa eli 13. maaliskuuta 2019 mennessä.

Tulokset

Selvityksemme osoittaa, että GDPR ei toimi. Kontaktoimamme toimijat eivät ole perillä asetuksen määräyksistä. Asettamamme hypoteesit saivat vähän tai eivät ollenkaan tukea empiirisestä aineistosta. Organisaatioissa voi olla tahoja, joilla on kuvaamamme parempi tietämys, mutta tämä ei riitä, jos asiakasrajapinnassa epäonnistutaan.

Havaitsimme puutteita läpinäkyvyydessä, käyttötarkoitussidonnaisuudessa, tietojen minimoinnissa ja säilytyksen rajoittamisessa. Henkilöllä ei ole todellisia mahdollisuuksia varmistua tietojensa lainmukaisesta käsittelystä. Henkilötietoja talletettiin kohteissa enemmän kuin niitä tarvittiin ja niiden käyttötarkoituksista tai säilytysajoista ei osattu tai haluttu kertoa.

Kaikissa kohteissa kerrottiin, että henkilötietoja saa käsitellä vain työntekijä työhönsä liittyen, mutta teknisesti useammalla henkilöllä on pääsy niihin. Kysyttäessä toimenpiteistä, joilla luvatonta käsittelyä estetään, monet tietävät jonkinlaisen lokin olemassaolosta, mutta ei sen tarkasta toiminnasta. Vaihtelua on siinä, jääkö lokiin merkintä pelkästä katselemisesta vai vain muokkaamisesta. Kolmessa kohteessa työntekijä kertoi, että rekisteriä ei voi selata vapaasti ilman yksilöivää tietoa.

Useissa kohteissa asiakasta kehotettiin tutustumaan toimijan tietosuojaselosteeseen. Työntekijät eivät itse osaa selostaa tietojen prosessointia ja kansalaisen valintamahdollisuuksia. Tietosuojan merkitystä vähätellään. Yleisiä selityksiä oli, että on helpompiakin tapoja saada henkilötietoja kuin kyseisen toimijan rekistereistä. Toinen yleinen selitys oli, että nykymaailmassa ei ole mahdollista hallita henkilötietojaan.

Sähköiseen yhteydenottoomme reagoi määräajassa puolet eli neljä kahdeksasta kohteesta. Nopein vastaus tuli kolmessa työpäivässä (Traficom).

Kolme muuta vastausta tulivat viikossa (Apple ja Sanoma Oyj) tai kahdessa (Yle). Veikkaus vastasi kahden muistutusviestin jälkeen. Muut kohteet eivät vastanneet. Applen tietosuojavastaava vastasi englanniksi suomenkielisten verkkosivujen kautta lähetettyyn suomenkieliseen viestiimme. Vastauksessa kehotettiin asiakasta tutustumaan yhtiön tietosuojaselosteeseen. Traficomin, Sanoma Oyj:n, Veikkauksen ja Ylen vastauksissa lainattiin sopivia kohtia toimijoiden tietosuojaselosteista tai linkitettiin niihin.

Sähköisiin tiedusteluihimme saamamme reaktiot ovat jokseenkin hyödyttömiä. Toimijoiden käytännöt eivät tutkimiemme käytäntöjen osalta noudata asetuksen määräyksiä. H1 ei siten saa aineistostamme tukea.

Suostumuksesta ei olla perillä yrityksissä ja virastoissa. Yhdessä kohteessa suostumus pääteltiin asiayhteydestä, eikä asiakkaan suostumusta tietojen tallentamiseen pyydetty ollenkaan. Vapaan valinnan mahdollisuus ei täyttynyt kohteissa, joissa suostumusta pyydettiin, mutta ilman sen antamista ei voinut saada palvelua. Aina ei ole selvää, käsitelläänkö henkilötietoja suostumuksen perusteella. Se hämärtää rajaa suostumuksen nojalla käsiteltävien tietojen ja muiden välillä. Kohteissa, joissa oltiin jo asiakkaita, suostumus katsottiin annetuksi asiakkuuden yhteydessä. Kohteissa ei kerrota, miten pitkään suostumus on voimassa ja miten pitkään tietoja säilytetään perumisen jälkeen.

Asetuksessa määritellyt suostumuksen kriteerit eivät täyty. Yksilöt antavat suostumuksensa tietämättä mitä se tarkoittaa. Suostumusta tyypillisesti ei sen enempää varsinaisesti kysytä kuin varsinaisesti anneta. Suostumuksen antaminen on rituaali vailla sisältöä. H2 ei siten saa aineistostamme tukea.

Suostumuksen peruuttamisen voidaan katsoa olevan yhtä vaivatonta kuin sen antaminen, jos se ei vaadi yksilöltä suostumuksen antamisesta poikkeavia toimia. Suostumuksen peruminen ei onnistu yhtä helposti kuin sen antaminen. Suostumuksen antaminen oli tietojen luettelemista ääneen tai työntekijä kirjasi tiedot henkilöllisyystodistuksesta. Suostumus annettiin joko suullisesti tai allekirjoittamalla suostumusta ilmaiseva paperi. Suostumuksen peruminen ei ollut yhtä vaivatonta, koska se vaati yksilöltä lomakkeiden täyttämistä ja omaa aktiivisuutta. Peruminen ei johda heti mihinkään konkreettisiin toimiin. Asiakkaan ilmaistessa halunsa perua suostumus käsittelijät eivät tiedä, miten toimia.

Sekaannusta aiheutti myös ero suostumuksen perumisen ja tietojen poiston välillä. Yleisesti ottaen suostumisen perumisen vaivattomuus riippuu siitä, mihin tietoja on käytetty. Suostumuksen peruminen suoramarkkinointiin onnistuu helpommin kuin kaikkia tietoja koskevan suostumuksen peruminen.

Suostumuksen peruminen ei ole yhtä vaivatonta kuin sen antaminen. Perumisen vaivattomuus vaihtelee sen mukaan, mitä tietoja suostumuksen perusteella oli käsitelty tai mihin tarkoitukseen tietoja käsiteltiin. H3 ei siten saa aineistostamme tukea.

Käytännöt eroavat eri toimijoiden välillä. Eroja oli suostumuksen antamisessa ja perumisessa, luvattoman käsittelyn estämisessä ja valvomisessa, käsittelijöiden osaamisessa ja tietämyksessä asetuksen määräyksistä, kerättyjen tietojen määrässä ja käsittelytarkoituksissa ja vastauksissa sähköisiin yhteydenottoihimme.

Tietosuojakäytännöt eivät ole yhdenmukaisia virastoissa ja yrityksissä eikä niiden kesken. H4 ei siten saa aineistostamme tukea.

Hypoteesimme H1–H4 eivät saaneet aineistosta tukea: toimijoiden tietosuojakäytännöt eivät ole asetuksen mukaisia, suostumusta henkilötietojen käsittelyyn ei anneta nimenomaisesti, suostumuksen peruuttaminen ei ole yhtä vaivatonta kuin sen antaminen ja toimijoiden tietosuojakäytännöt eivät ole yhdenmukaisia.

Tietojen käsittelyssä ei ole tapahtunut oleellista parannusta asetusta edeltävään tilanteeseen. Havaittavin muutos on verkkosivujen päivitetty tietosuojaseloste, mutta organisaatioiden asiakasrajapinnassa muutoksia ei ole omaksuttu. Asetuksen toimeenpano on kesken toimipisteissä.

Päätelmät

Tietosuoja ja siihen liittyvä sääntely on tarpeen. Henkilötiedot ovat kauppatavaraa, niiden merkitys ei ole vähenemässä ja niitä kerätään enenevissä määrin. Emme pysty luotettavasti hahmottamaan tulevia henkilötietojen käyttötarkoituksia tai -tapoja. Osa niistä voi olla yksilön kannalta kielteisiä.

Kaikilla relevanteilla toimijoilla on kosolti parannettavaa tietosuojan turvaamiseksi. Lähes kolme vuotta asetuksen antamisesta sen voimaantuloon ei riittänyt määräysten implementoimiseen.

Yksilöiden pitää olla tietoisia oikeuksistaan ja vaatia, että tietosuoja-asetusta noudatetaan. Hyväuskoisuutta ja välinpitämättömyyttä on liikaa. Ei pidä olettaa, että GDPR:n myötä henkilötietojen käsittely on laillista.

Arviomme on, että GDPR ei ole lunastanut kansalaisten ja median odotuksia. Testimme osoittaa, että suostumuksella ei käytännössä ole ratkaisevaa tai todellista merkitystä. Suostumus on suureksi osaksi illuusio, eikä se näyttele oleellista osaa koko prosessissa.

Tallettajien pitää opiskella asetusta, kouluttaa henkilöstö nykyistä oleellisesti paremmin ja valvoa, että sääntöjä noudatetaan. Kohteissa ei omin sanoin osattu selostaa henkilötietojen prosessointia ja kansalaisen valintamahdollisuuksia. Yksilöä kehotettiin itse lukemaan asetusta ja perehtymään aihepiiriin. Pelkkä näyteikkunan eli tietosuojaselosteen päivittäminen ei riitä, vaan käytäntöjen pitää myös olla lainmukaisia.

Tietojärjestelmien pitää olla sellaiset, että luvaton käsittely ei ole työntekijän luotettavuuden varassa. Toimintakulttuuri on liian välinpitämätöntä ja yksilön oikeuksista piittaamatonta. Työntekijöillä pitää olla kannustimia tietosuojasta huolehtimiseen.

Valvontaviranomaiset ovat suurilta osin laiminlyöneet velvollisuutensa. Viranomaisten pitää valvoa käytännössä valvontaiskuin. Asetuksessa mainittuja sertifiointimekanismeja ja tietosuojamerkkejä ja -sinettejä on käytettävä. Viranomaisten pitää puuttua tulkintaeroihin tarkentamalla määräyksiä ja soveltamiskäytäntöjä, jotta laittomat ja lainmukaiset käytännöt tulevat selviksi.

Poliitikkojen pitää arvioida, onko tarvetta lisäsääntelylle, paneutua asiaan paremmin ja teettää vaikuttavuusanalyysejä. On myös vakavasti pohdittava vaihtoehtoisia toimintatapoja. Millä muilla keinoilla kuin suostumuksella henkilötietoja voisi hallita?

Median pitää kiinnittää enemmän huomiota asiaan. Suomalaisten julkisten virastojen tietosuojatoilailuista uutisoidaan, mutta yrityksistä samanlaisia uutisia ei ole juuri julkaistu.

Asetuksen julkilausuttuna tavoitteena on lisätä kansalaisten luottamusta henkilötietojen turvalliseen käsittelyyn ja tietosuojaan. Tätä tavoitetta nykykäytännöt eivät edistä.

Asetus ei ole onnistunut, koska se mahdollistaa monia tulkintoja, edellyttää henkilöiltä kohtuuttoman paljon taustatietoja ja käsittelijöiltä ja rekisterinpitäjiltä enemmän ammattitaitoa kuin heillä nyt on. Useat perusteet henkilötietojen käsittelylle ja kansallisesti säädettävät kohdat tekevät epäselväksi, mitä lakia tai asetusta kussakin tilanteessa kuuluu soveltaa.

GDPR:n 97. artiklan mukaan Euroopan komission on arvioitava ja uudelleentarkasteltava asetusta vuonna 2020. Osoitimme jo paljon parantamisen varaa.

Suostumuksen antamisen ehtoja ja niiden toteutumista olisi syytä tutkia systemaattisesti suuremmalla aineistolla. Ainesta laajempaan tutkimukseen on runsaasti.

KIRJALLISUUS

Euroopan komissio (2017) Final results of the European Data Market study measuring the size and trends of the EU data economy. https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy (luettu 19.3.2019)

Lassila, Anni (2019) Tietopyyntö paljastaa, mitä tietoja yritys kerää. Helsingin Sanomat, 12.3.2019, 28–29.

Sisäministeriö (2019) Lainsäädäntö ohjaa asiakas- ja potilastietojen hallintaa. https://stm.fi/asiakastietojen-potilastietojen-salassapito (luettu 19.3.2019)

Tietosuojavaltuutetun toimisto (2019) Tietosuojavaltuutetun toimistolle on ilmoitettu jo 2700 henkilötietojen tietoturvaloukkausta. Tiedote. https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuojavaltuutetun-toimistolle-on-ilmoitettu-jo-2700-henkilotietojen-tietoturvaloukkausta (luettu 19.3.2019)