Liite: GDPR:n vaikutukset automaatioympäristöihin

Jussi Leppälä, Data Privacy Officer, Valmet

Automaatiojärjestelmien ensisijainen tarkoitus on harvoin henkilötietojen käsittely. Silti on tärkeää tunnistaa tilanteet, joissa tietosuojalait tulevat sovellettaviksi. Suomalaisille ja yleisemmin eurooppalaisille toimijoille EU:n yleinen tietosuoja-asetus, GDPR, on tärkein henkilötietojen säätelyä koskeva laki. Käyttäjähallinta on ilmeinen alue, jossa henkilötietoja käsitellään myös automaatiojärjestelmissä. Laitemittaustiedot voivat niin ikään olla henkilötietoja, jos ne pystytään yhdistämään henkilöön esim. aikaleiman ja paikkatiedon avulla.

Milloin Yleinen tietosuoja-asetus tulee sovellettavaksi

Yleisen tietosuoja-asetuksen kannalta oleellisin kysymys on, tuleeko asetus sovellettavaksi tarkastellussa järjestelmässä lainkaan. Erittäin usein vastaus on kyllä. Useimmilla organisaatiolla on hyvä valmius toteuttaa tähän liittyvät vaatimukset, koska ne altistuvat samoille vaatimuksille joka tapauksessa muissa käsittelytoimissaan. Lähes jokainen yritys käsittelee vähintään omien työntekijöidensä ja asiakkaidensa henkilötietoja.

KÄSITELLÄÄNKÖ HENKILÖTIETOJA?

Henkilötietoja ovat kaikki tiedot, jotka liittyvät elävään ihmiseen. Tietojen ei kuitenkaan tarvitse olla suoraan yhdistettävissä. Useimmissa tilanteissa päätelaitteen IP-osoite on henkilötieto, koska se voidaan yhdistää päätelaitteen haltijaan muiden tietojen avulla. On hyvä huomata, että amerikkalaisessa kirjallisuudessa usein nähtyä termiä PII, Personally Identifiable Information, käytetään tyypillisesti suppeammassa merkityksessä. PII:n tulee sisältää nimi tai joku muu suoraan identifioiva tunniste: on siten mahdollista löytää esimerkkejä tiedoista, jotka eivät ole PII-tietoja mutta ovat henkilötietoja. Yleinen tietosuoja-asetus mainitsee erikseen verkkotunnisteet henkilötiedon määritelmän yhteydessä.

ONKO HENKILÖTIETOJEN KÄSITTELY SELLLAISTA, ETTÄ YLEINEN TIETOSUOJA-ASETUS TULEE SOVELLETTAVAKSI

Jos käsittely tapahtuu EU:n alueella olevan rekisterinpitäjän tai käsittelijän EU:n alueella olevan toimipaikan yhteydessä, yleinen tietosuoja-asetus tulee sovellettavaksi. Jos käsittely liittyy EU:n alueella oleviin henkilöihin, käsittely on yleensä asetuksen piirissä, vaikka yrityksellä ei olisikaan toimipaikkaa EU:n alueella. On kuitenkin mahdollista, että maailmanlaajuisen yrityksen EU:n ulkopuolella olevien tytäryhtiöiden suorittama käsittely ei ole asetuksen piirissä, vaikka yrityksen pääkonttori olisikin EU:n alueella. Tästä huolimatta voi olla helpompaa ja tarkoituksenmukaisempaa soveltaa samoja käsittelyperiaatteita maailmanlaajuisesti kuin ryhtyä paikalliseen räätälöintiin.

Roolit henkilötietojen käsittelyssä

REKISTERINPITÄJÄ, KÄSITTELIJÄ JA REKISTERÖITY

Yleinen tietosuoja-asetus määrittelee ihmisille erilaisia oikeuksia, kun heitä koskevia tietoja käsitellään. Toisaalta asetus määrittelee velvollisuuksia tiedon käsittelijöille. Koska nämä velvollisuudet ovat erilaisia eri tietosuojarooleissa, on tärkeää selvittää, missä roolissa kulloinkin toimitaan. Rekisterinpitäjä on ensisijaisessa vastuussa rekisteröidyn oikeuksien toteuttamisesta.

Rekisterinpitäjä on taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Itse käsittelyn voi silti tehdä joku muu. Näin ollen esim. työnantaja on rekisterinpitäjä työntekijöiden henkilötietojen käsittelyssä, vaikka käyttäisikin siihen ulkoisen toimittajan pilvipalvelua. Toimittaja toimii tällöin henkilötietojen käsittelijänä. Jos työnantaja on ostanut käyttämänsä ohjelmiston toimittajalta ja käyttää ohjelmistoa itse hallinnoimillaan palvelimilla, ohjelmiston toimittajalla ei luultavasti ole mitään yleisen tietosuoja-asetuksen määrittelemää roolia. Joskus kaksi tahoa määrittelee yhdessä henkilötietojen käsittelyn tarkoitukset ja keinot. Tällöin puhutaan yhteisrekisterinpitäjistä. Monet toimijat haluavat välttää tällaista asetelmaa mm. siihen liittyvien vastuiden määrittelyn vaikeuden takia.

Automaatiojärjestelmän toimittajalla ei joissain tilanteissa ole mitään yleisen tietosuoja-asetuksen tarkoittamaa roolia. On mahdollista, että toimitetun järjestelmän henkilötietojen rekisterinpitäjänä toimii asiakas. Asiakas voi lisäksi käyttää apunaan henkilötietojen käsittelijöitä. Jos järjestelmän toimittaja operoi tai ylläpitää järjestelmää asiakkaan puolesta, voi toimittaja toimia puolestaan yhtenä tai ainoana käsittelijänä.

Vaikka automaatiojärjestelmän toimittaja toimisi puhtaasti vain ohjelmiston toimittajana eikä siten rekisterinpitäjänä tai käsittelijänä, on toimittajan syytä varmistaa, että järjestelmä tukee ja mahdollistaa rekisterinpitäjälle lainmukaisen toiminnan ja esim. rekisteröityjen oikeuksien helpon toteuttamisen. Siten tietosuoja tulee ottaa huomioon jo järjestelmän suunnitteluvaiheessa.

Henkilötietojen käsittelijä määritellään toimijaksi, joka käsittelee tietoja rekisterinpitäjän puolesta ja lukuun. Käsittelijä voi toimia ainoastaan rekisterinpitäjän ohjeiden mukaan eikä saa käsitellä henkilötietoja omiin tarkoituksiinsa. Rekisterinpitäjän ja käsittelijän suhdetta säädellään näiden välisellä sopimuksella, jonka sisällölle yleinen tietosuoja-asetus asettaa lukuisia vaatimuksia.

Tietosuojaviranomaiset

Tietosuojan toteutumista valvoo kussakin EU:n jäsenvaltiossa valvontaviranomainen, joka on Suomessa tietosuojavaltuutettu. Useassa Euroopan maassa toimivan rekisterinpitäjän päätoimipaikan valvontaviranomaisella on valta toimia rekisterinpitäjän ns. johtavana valvontaviranomaisena. Parhaimmillaan tämä yksinkertaistaa rekisterinpitäjän kommunikointia viranomaisten kanssa: rekisterinpitäjä voi asioida oman johtavan valvontaviranomaisensa kanssa, vaikka rekisteröity jossain muussa maassa olisikin tätä koskevassa asiassa ottanut yhteyttä paikalliseen viranomaiseen.

TIETOSUOJAVIRANOMAISEN VALTUUDET

Yleinen tietosuoja-asetus antaa tietosuojaviranomaisille laajat tutkintavaltuudet ja merkittävät korjaavat toimivaltuudet. Voimakkaimpiin korjaavin toimivaltuuksiin kuuluvat mm. oikeus määrätä käsittelykielto ja oikeus määrätä hallinnollinen sakko. Sakot voivat suurimmillaan olla 20 M€ tai 4% yrityksen edellisen tilikauden maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi näistä luvuista on suurempi.

Rekisterinpitäjän velvoitteet

Yleinen tietosuoja-asetus määrittelee rekisterinpitäjälle useita velvollisuuksia. Ehkä tärkein muutos, jonka yleinen tietosuoja-asetus toi, on osoitusvelvollisuus: ei riitä, että rekisterinpitäjä noudattaa käsittelyssään tietosuojaperiaatteita, vaan rekisterinpitäjän on myös pystyttävä osoittamaan, että niitä noudatetaan ja on noudatettu. Tehdyistä sakkopäätöksistä ilmenee, että osoitusvelvollisuuden edellyttämää dokumentaatiota myös vaaditaan.

SELOSTE KÄSITTELYTOIMISTA

Rekisterinpitäjän ja käsittelijän tulee pitää yllä selostetta käsittelytoimistaan. Nämä selosteet tulee tarpeen tullen voida näyttää valvontaviranomaiselle. Vaikka selosteiden sisällössä on paljon samoja tietoja, jotka pitää ilmoittaa rekisteröidyille heidän tietojensa käsittelystä, ovat kyseessä kuitenkin kaksi eri asiaa ja usein kaksi eri dokumenttia: selosteet liittyvät osoitusvelvollisuuteen ja informointi rekisteröidyn oikeuksiin.

TIETOSUOJAA KOSKEVIEN TIETOTURVALOUKKAUSTEN KÄSITTELY

Yleinen tietosuoja-asetus määrittelee kolme eri velvollisuutta rekisterinpitäjälle tietosuojaa koskeviin tietoturvaloukkauksiin liittyen: 1. Rekisterinpitäjän tulee dokumentoida kaikki henkilötietojen tietoturvaloukkaukset. 2. Jos tietoturvaloukkauksesta aiheutuu ihmisille riski, niin rekisterinpitäjän pitää ilmoittaa loukkauksesta valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa. 3. Kun tietoturvaloukkaus aiheuttaa korkean riskin ihmisille, tietoturvaloukkauksesta tulee lisäksi ilmoittaa rekisteröidyille.

Rekisterinpitäjän tietoturvaloukkauskirjanpitoon voi tulla paljon tapahtumia. On syytä huolellisesti dokumentoida kunkin tietoturvaloukkauksen yhteydessä tehty riskiarvio, jonka perusteella on päätetty, raportoidaanko tietoturvaloukkaus viranomaisille ja rekisteröidyille. Päätös tulee jälkikäteen pystyä perustelemaan. Useassa Euroopan maassa toimivan rekisterinpitäjän tulee lisäksi päättää, tehdäänkö ilmoitus pelkästään johtavalle tietosuojaviranomaiselle vai annetaanko tieto myös muille tietosuojaviranomaisille, joiden piirissä olevia rekisteröityjä loukkaus koskee.

Monelle rekisterinpitäjälle 72 tunnin aikarajaa voi olla haasteellinen, etenkin jos tietoturvaloukkaus tapahtuu juhlapyhien aikaan.

KÄSITTELYPERIAATTEET

Yleinen tietosuoja-asetus sisältää joissain kohdin varsin yksityiskohtaisiakin ohjeita. Laajemmin tarkasteltuna se on kuitenkin varsin yleinen, nojaa periaatteisiin ja antaa rekisterinpitäjälle paljon harkintavaltaa ja -vastuuta. Rekisterinpitäjän pitää noudattaa käsittelyperiaatteita, jotka listataan asetuksen 5 artiklassa ja pystyä myös osoittamaan noudattavansa niitä. Käsittelyperiaatteisin kuuluvat mm. käsittelyn läpinäkyvyys, tietojen minimointi ja käyttötarkoitussidonnaisuus, täsmällisyys, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus.

KÄSITTELYN OIKEUSPERUSTEET

Rekisterinpitäjän pitää määrittää kullekin käsittelytoimenpiteelle sen oikeusperuste ja kertoa se rekisteröidyille. Asetus listaa kuusi mahdollista oikeusperustetta: 1. suostumus, 2. tarpeellisuus sopimuksen täytäntöönpanemiseksi, 3. tarpeellisuus rekisterinpitäjän lakisääteisen velvollisuuden noudattamiseksi, 4. tarpeellisuus henkilön elintärkeiden etujen suojaamiseksi, 5. tarpeellisuus yleistä etua varten tai julkisen vallan käyttämiseksi sekä 6. tarpeellisuus rekisterinpitäjän oikeutettujen etujen toteuttamiseksi. Suostumus on luultavasti näistä tunnetuin mutta se ei ole ensisijaisessa asemassa muihin nähden. Teollisuusympäristössä suostumus itse asiassa harvoin tulee kysymykseen, koska suostumuksen tulee olla aidosti vapaaehtoinen ollakseen pätevä. Eurooppalaiset tietosuojaviranomaiset usein katsovat, että työsuhteen yhteydessä annettu suostumus ei voi olla vapaaehtoinen työnantajan ja työntekijän välisen voimaepätasapainon vuoksi: työntekijän katsotaan

olevan haavoittuvassa asemassa työnantajaan nähden. Tämän takia rekisterinpitäjän oikeutetut edut lienee tyypillisin käsittelyn oikeusperuste teollisuusympäristöissä.

TASAPAINOTESTI

Kun käsittelyn oikeusperusteena käytetään rekisterinpitäjän oikeutettuja etuja, tulee näitä etuja punnita rekisteröidyn etuja sekä perusoikeuksia ja -vapauksia vasten. Käsittely ei ole mahdollista, jos jälkimmäiset syrjäyttävät rekisterinpitäjän edut. Yleinen tietosuoja-asetus ei määrittele tämän intressipunninnan muotoa ja dokumentointia kovin yksityiskohtaisesti, mutta valvontaviranomaiset ovat julkaisseet asiasta omia ohjeitaan ja suosituksiaan. Teollisten järjestelmien käyttäjähallinnan ja mittaustietojen osalta tulee harkittavaksi, kuinka yksityiskohtaisen työntekijöiden valvonnan kyseiset tiedot mahdollistavat ja onko tietojen kerääminen ja käyttö oikeasuhtaista. Tässä on syytä olla erityisen tarkkana, jos käsitellään ns. erityisiä henkilötietoryhmiä, kuten biometrisiä tietoja yksilön tunnistamista varten. Työntekijöiden velvoittamista sormenjälkitunnistuksen käyttöön kulunvalvonnan ja työajan seurannan tarkoituksiin on joissain tilanteissa pidetty kohtuuttomana. Erityisten henkilötietoryhmien käsittelyn tulee lisäksi täyttää joku 9 artiklan erityisehdoista.

SISÄÄNRAKENNETTU JA OLETUSARVOINEN TIETOSUOJA

Yleinen tietosuoja-asetus edellyttää, että henkilötietojen käsittelyperiaatteet otetaan huomioon jo käsittelyä suunniteltaessa ja ne toteutetaan itse käsittelyyn. Tässä yhteydessä mainitaan erityisesti tietojen minimointi ja tarvittavat suojatoimet. Esimerkkinä suojatoimista on mm. henkilötietojen pseudonymisointi, jossa henkilötietoja käsitellään siten, että niitä ei enää voi yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Näitä lisätietoja tulee säilyttää erillään ja teknisin ja organisatorisin toimenpitein varmistaa, että yhdistämistä ei tapahdu.

VAIKUTUSTENARVIOINTI JA ENNAKKOKUULEMINEN

Kun suunniteltu käsittely todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksien ja vapauksien kannalta, yleinen tietosuoja-asetus edellyttää, että rekisterinpitäjä toteuttaa arvioinnin käsittelyn vaikutuksista henkilötietojen suojalle. Jos mahdollisten riskiä pienentävien toimenpiteiden jälkeenkin korkea riski on edelleen olemassa, rekisterinpitäjän tulee kuulla valvontaviranomaista ennen käsittelyn aloittamista. Jo ennen asetuksen voimaantuloa monilla kansainvälisillä yrityksillä oli käytäntö vaikutustenarvioinneista vastaavissa tilanteissa. Näitä arviointeja kutsuttiin usein englanninkielisellä nimellä Privacy Impact Assessment, PIA. Jotkut yritykset ylläpitävät edelleen kahta arviointikäytäntöä: asetuksen tarkoittamia arviointeja (Data Protection Impact Assesment, DPIA) ja vapaaehtoisia arviointeja, jotka voivat olla hyvinkin samanlaisia (PIA). Ennen uuden käsittelytoimen aloittamista, yrityksen on hyvä dokumentoida alustava riskiarvio käsittelyn vaikutuksista ja päätös siitä, pitääkö yritys asetuksen tarkoittamaa vaikutustenarviointia lakivelvoitteenaan.

Vaikutustenarvioinnin voi tehdä yritys itse mutta ei ole epätavallista, että rekisterinpitäjä turvautuu ulkoiseen apuun vaikutustenarvioinnin tekemiseksi ja dokumentoimiseksi. Tyypillisesti yrityksen oman henkilökunnan asiantuntemusta tarvitaan ulkoisenkin tahon tekemän vaikutustenarvioinnin tueksi.

Käsittelysopimukset

Rekisterinpitäjän ja käsittelijän suhde määritetään sopimuksella, jossa tulee vahvistaa mm. käsittelyn kohde ja kesto, käsittelyn alaisten henkilötietojen tyyppi ja rekisteröityjen ryhmät, käsittelijän mahdollinen oikeus käyttää muita käsittelijöitä apunaan sekä käsittelijän sitoumus auttaa rekisterinpitäjää tämän lakisääteisten velvollisuuksien noudattamisessa. Sopimuksen tekemättä jättäminen voi altistaa molemmat osapuolet sanktioille. Sekä rekisterinpitäjillä että käsittelijöillä on usein omat valmiit ehdotuksensa tällaiseksi sopimukseksi. Joskus ei käytetä suoraan kumpaakaan ehdotusta, vaan neuvotellaan erikseen molemmille osapuolille sopiva kompromissi. Kohdat, jotka johtavat erillisiin keskusteluihin liittyvät usein vastuisiin ja korvausvelvollisuuteen tietosuojaa koskevien tietoturvaloukkausten yhteydessä, kustannusten jakoon, jos rekisteröidyn oikeuksien toteuttaminen vaatii käsittelijän apua, rekisterinpitäjän oikeuteen auditoida käsittelijä, apukäsittelijöiden käyttämiseen, henkilötietojen siirtoon kolmansiin maihin ja käsittelijältä mahdollisesti vaadittaviin tietoturvasertifikaatteihin tai -raportteihin.

Rekisterinpitäjän ja käsittelijän välinen sopimus on tunnetuin yleisen tietosuoja-asetuksen edellyttämistä sopimuksista. Asetus edellyttää lisäksi, että yhteisrekisterinpitäjät määrittelevät keskinäisellä järjestelyllä vastuunjakonsa asetuksen velvoitteiden osalta. Henkilötietojen vaihto yritysten välisissä järjestelyissä voi myös olla kahden itsenäisen rekisterinpitäjän välistä vaihtoa. Tällöin yritykset voivat sopimuksellisesti varmistaa, että vastaanottavan osapuolen käsittelytarkoitukset ja -keinot ovat sopusoinnussa luovuttavan yrityksen tavoitteiden ja arvojen kanssa.

Tietojen siirto kolmansiin maihin

Yleinen tietosuoja-asetus mahdollistaa henkilötietojen siirron Euroopan talousalueen sisällä varsin vapaasti. Tämä tuntuu luonnolliselta, koska asetus on EU:n alueella suoraan sovellettavaa lainsäädäntöä ja siten henkilötietojen suoja on näissä maissa samanlaisella tasolla. Jos henkilötietoja halutaan siirtää kolmansiin maihin, asetus edellyttää, että henkilötietojen suojan tasoa ei vaaranneta. Siirto voi perustua kolmeen asiaan: Euroopan komission päätökseen kohdemaan tai -organisaation riittävästä tietosuojan tasosta, asianmukaisiin suojatoimiin tai erityistilanteita koskeviin poikkeuksiin. Helpoin tapaus on, jos kohdemaa on komission listalla riittävän tietosuojan tason maista. Lista on kuitenkin aika lyhyt. Yhdysvaltalaisille yrityksille oli lisäksi käytössä ns. Privacy Shield -järjestely, jossa riittävän tietosuojan taso katsottiin saavutettavaksi itsesertifiointimenettelyn kautta. EU-tuomioistuin kuitenkin julisti Privacy Shield -järjestelyn mitättömäksi 16.7.2020. Luultavasti yleisin tapa mahdollistaa siirrot kolmansiin maihin on tukeutua asianmukaisiin suojatoimiin ja niistä yleisimmin

komission hyväksymiin mallisopimuksiin. Niidenkin käyttö voi edellyttää oikeudellisia, teknisiä tai organisatorisia lisäjärjestelyjä tapauskohtaisesti. Edellä mainittu EU-tuomioistuimen päätös nosti vaatimustasoa myös mallisopimusten käytössä ja monet toimijat ovat olleet epävarmoja siitä, mitkä lisätoimet ovat riittäviä. Komission uusien mallisopimusten ja Euroopan tietosuojaneuvoston ohjeiden toivotaan selventävän asiaa, mutta asia tulee edelleen vaatimaan tarkkuutta. Hyvä asianmukainen suojatoimi, joka mahdollistaa kansainväliset siirrot monikansallisen yrityksen sisällä ovat valvontaviranomaisen vahvistamat yritystä koskevat sitovat säännöt. Toistaiseksi vahvistusmenettely on ollut varsin vaativa ja kestänyt eri vaiheineen ennemminkin muutaman vuoden kuin kuukausia eikä yrityksiä, jotka tähän perusteeseen voivat nojautua, ole kovin paljon. Kolmantena siirtoperusteluokkana ovat erityistilanteita koskevat poikkeukset. Tällaisia poikkeuksia voivat olla esim. elintärkeiden etujen suojaaminen, jos rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumustaan. Vaikka nimenomainen suostumus on yksi poikkeuksista, tulisi säännönmukaisten siirtojen perustua johonkin muuhun kuin poikkeuksiin: päätökseen riittävän tietosuojan tasosta tai asianmukaisiin suojatoimiin.

Rekisteröityjen oikeudet

Yleinen tietosuoja-asetus vahvisti rekisteröityjen oikeuksia. Niihin liittyvä keskustelu asetuksen voimaantulon yhteydessä teki myös ihmiset aikaisempaa tietoisemmiksi henkilötietojen käsittelystä, käsittelyyn liittyvistä riskeistä ja omista oikeuksistaan. Rekisteröidyn oikeuksia ovat oikeus saada tietää henkilötietojen käsittelystä, oikeus saada pääsy tietoihin ja saada kopio tiedoista, oikeus tietojen oikaisemiseen, oikeus tietojen poistamiseen, oikeus käsittelyn rajoittamiseen, oikeus vastustaa käsittelyä, kun käsittely perustuu rekisterinpitäjän oikeutettuihin etuihin sekä oikeus siirtää tiedot järjestelmästä toiseen. Nämä oikeudet eivät tyypillisesti ole absoluuttisia: esim. oikeus tietojen poistamiseen toimii suoraviivaisimmillaan, jos käsittelyn oikeusperuste on suostumus. Jos käsittelylle on joku muu pätevä oikeusperuste, käsittely voi usein jatkua, vaikka rekisteröity pyytäisikin tietojen poistamista. Rekisterinpitäjän pitää joka tapauksessa varautua siihen, että rekisteröidyt haluavat toteuttaa oikeuksiaan. Jos mahdollista, voi olla hyvä toteuttaa osa oikeuksista itsepalveluna, jolloin vältytään kalliilta erityistarkasteluilta ja käsityöltä. Jotkut sosiaalisen median palvelut esim. tarjoavat rekisteröidylle kopion omista tiedoistaan tällaisen itsepalvelun kautta. Teollisuusympäristössä ei itsepalvelumahdollisuutta ehkä ole ainakaan vanhempiin järjestelmiin teknisesti toteutettu, mutta rekisterinpitäjän on hyvä valmistautua rekisteröityjen tietopyyntöihin luomalla asiasta käytännöt ja ohjeet, jotka varmistavat, että pyyntöihin vastataan oikeasisältöisesti määräajassa. Vastaus on syytä toimittaa ripeästi, asetuksen mukaan ”ilman aiheetonta viivytystä ja joka tapauksessa kuukauden kuluessa”. Jos pyynnön esittäjää ei voida luotettavasti tunnistaa, pyyntöä ei välttämättä voida toteuttaa. Usein on tarkoituksenmukaista käyttää samaa tunnistautumista kuin tietoja kerättäessä.

Viestinnän luottamuksellisuus

Sähköisen viestinnän luottamuksellisuudesta ei säädetä Euroopassa suoraan yleisessä tietosuoja-asetuksessa, vaan sähköisen viestinnän tietosuojadirektiivissä 2002/58/EY, sen täydennyksessä 2009/136/EC ja niiden kansallisissa implementaatioissa. Suomessa tästä säädetään sähköisen viestinnän tietosuojalaissa. Direktiivin 2002/58/EY suunnitellun seuraajan, ns. ePrivacy-asetuksen ehdotusluonnos mainitsee erikseen, että sitä tulee soveltaa myös esineiden internetiin ja laitteiden väliseen viestintään. Tällä voi olla merkitystä automaatiojärjestelmien välitystietojen ja viestien sisältöjen käsittelyssä.

Tietosuojaohjelman organisointi, tietosuojavastaava

Yleisen tietosuoja-asetuksen tultua voimaan useimmissa yrityksissä on otettu käyttöön organisaatiolle sopiva tietosuojan johtamisjärjestelmä. Automaatiojärjestelmiin liittyvät tietosuojakysymykset tulevat luontevasti osaksi jo olemassa olevaa johtamisjärjestelmää. Tietosuojan johtamisjärjestelmän voi organisoida monella tavalla mutta tyypillisesti se sisältää raportointimekanismit ja -metriikat, hallintamallin, tietoisuuden kasvattamisen ja koulutuksen sekä tietosuojaa koskevat ohjeet ja käytännöt.

Yleinen tietosuoja-asetus määrittelee myös tietosuojavastaavan roolin. Joissain tilanteissa tietosuojavastaavan nimittämisestä tulee lakisääteinen velvollisuus rekisterinpitäjälle. Rekisteripitäjän on tällöin julkistettava tietosuojavastaavan yhteystiedot ja ilmoitettava ne valvontaviranomaiselle. Tietosuojavastaavan ei välttämättä tarvitse kuulua rekisterinpitäjän henkilöstöön, vaan tietosuojavastaavana voi toimia myös palvelusopimuksen perusteella. Tietosuojavastaavan tehtäviin kuuluvat mm. neuvonta, asetuksen noudattamisen seuranta ja yhteistyö valvontaviranomaisen kanssa. On tapauksia, joissa tietosuojaviranomainen on määrännyt sakkoja rekisterinpitäjälle, joka ei ole nimittänyt tietosuojavastaavaa, vaikka asetus olisi sitä edellyttänyt.

Tietosuojalakeja maailmalla

Yleistä tietosuoja-asetusta on sen voimaan tultua pidetty ehkä maailman vaikutusvaltaisimpana tietosuojalakina. Se ei kuitenkaan ole ainoa laatuaan, vaan yli sadassa maailman valtiossa on jonkinlainen tietosuojalaki. Viime vuosina monia lakeja on uusittu ja niitä valvovien viranomaisten toimintaedellytyksiä on parannettu. Jotkut uusista laeista ovat saaneet vahvoja vaikutteita EU:n yleisestä tietosuoja-asetuksesta. Tällaisia ovat mm. Thaimaan ja Brasilian uudet tietosuojalait, joita molempia alettiin rajoitetusti soveltaa vuoden 2020 aikana. Automaatiojärjestelmien kannalta

mielenkiintoisia ovat lisäksi ainakin maat, joissa on velvollisuus ilmoittaa henkilötietoja koskevasta tietoturvaloukkauksesta viranomaiselle. Tällaisia maita ovat mm. Kanada, Australia, Turkki, ja Uusi-Seelanti. Joissakin maissa kuten Japanissa tällainen ilmoitus on toistaiseksi vain suositus.

Yrityksen, joka toimii monen valtion alueella, täytyy löytää sopivat keinot lainmukaiseen henkilötietojen käsittelyyn kaikilla alueilla. Useimmat tietosuojalait pohjautuvat onneksi samoihin periaatteisiin. On siksi varsin yleistä, että valitaan joku laki tietosuojaohjelman pohjaksi ja täydennetään vaatimuksia sitä mukaa, kun niitä tunnistetaan muilla toiminta-alueilla. Usein on kustannustehokkainta soveltaa vain yksiä käsittelyperiaatteita koko toiminta-alueella.

Lyhenne- ja selitysluettelo

- DPIA = Data Protection Impact Assessment
- GDPR = General Data Protection Regulation
- PIA = Privacy Impact Assessment
- PII = Personally Identifiable Information

Viitteet

[Yleinen tietosuoja-asetus] = EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus), 27.4.2016, https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[ePrivacy-asetus] = Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus), 10.1.2017, https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:52017PC0010

[Tietosuojaneuvoston ohje suostumuksesta] = Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1 Adopted on 4 May 2020, European Data Protection Board, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Tämä on liite kirjaan:

Automaation tietoturva – Kriittisen tuotannon turvaaminen

(ISBN: 978-952-5183-58-0, ISSN 1455-6502, SAS julkaisusarja nro 51, © Suomen Automaatioseura ry, www.automaatioseura.fi/AutomaationTietoturva)