Tietojärjestelmätyön asiantuntija • Sytyke ry:n jäsenlehti Nro 3/2017

Sytyke

REGULAATIOT - digitalisaation suojatiet

BLOCKCHAIN
Sytyke syysseminaari marraskuussa

TIVIA Tieto- ja viestintätekniikan ammattilaiset ry

TIVIA tiedottaa

Vuosi on ollut perinteiseen TIVIA-yhteisön tyyliin sopien, erityisen tapahtumarikas. Seminaareja ja toimintaa on järjestetty jäsenille, viestintää on tehostettu ja pyritty aktiivisesti saamaan uusia jäseniä. Olemme tehneet tänä vuonna alueellisia toimenpiteitä entistä ponnekkaammin. Näistä esimerkkeinä mainittakoon toteutettu Seinäjoella järjestetty seminaari sekä Joensuussa toteutettu tapahtuma yhdessä TIVIAn ja Kauppakamarin kanssa.

Toiminnanjohtaja Mika Helenius on ollut aktiivisesti mukana tuomassa sisältöä tapahtumaan, paikallisyhdistys on nostettu markkinointiviestinnässä keskiöön ja yhteistyötoimija on tuonut oman vahvan panoksensa tilaisuuden järjestämiseksi. Alueen yrityksiä on informoitu jakamalla omalla kansiliitteellä varustettu TIVIA News ennakkoon postitse. Paikan päällä on tehty aktiivista jäsenhankintaa samalla, kun on luotu mahdollisuudet verkostoitua ja kehittää osaamista.

Hyvä esimerkki yhteistyön tiivistämisestä on 2037 - tiekartta tulevaisuuteen -seminaariristeily 5. - 7.10., jossa mukana on yhdistyksistämme Tietoturva. Myös opiskelijat on huomioitu erityisesti risteilypaketin hinnoittelussa. Erityisen tärkeänä pidämme juuri opiskelijoiden osallistamisen toimintaamme tiiviimmin. Opinnäytetyö-kilpailu sekä erilaiset muut palkitsemistilaisuudet kannattaa nostaa paremmin ja useammin esille. Yhteistyön kehittämisestä yritysten, yhdistysten sekä opiskelijoiden osalta on kaikkien etu.

TIVIA on mukana monessa tapahtumassa loppuvuonna. Toivomme aina saavamme tapahtumaan mukaan yhdistyksen, jolloin näkyvyys monipuolistuu kaikkien tahojen osalta. Sytyke on kanssamme syksyllä mm. Mindtrek´ssa Tampereella, Tivi Software & Robotics & A OKI´ssa Helsingissä sekä Talent IT´ssä Espoossa. KAOS on mukana Tivi Enterprise Architecturen -seminaarissa Helsingissä. Ja tietysti me olemme mukana seminaariristeilyllä!

Toimikunnat toivottavat kaikki toiminnan kehittämisestä kiinnostuneet edelleen tervetulleiksi mukaan. Toimikunnan muodostaa jäsenemme. Tavoitteena on saada paras mahdollinen osaaminen mukaan kehittämään TIVIA-yhteisö toimintaa. Toimikuntia ovat:

- jäsenpalvelutoimikunta
- tapahtumatoimikunta
- tietoyhteiskuntatoimikunta
- viestintätoimikunta

Mikäli olet kiinnostunut tulemaan mukaan, lisätietoa saa ja ilmoittautua voi osoitteessa tivia@tivia.fi. Toimikunnat kokoontuvat pääsääntöisesti Adobe Connectin kautta, jolloin siirtymisiä ei paikasta toiseen juuri tule.

Koulutusten osalta olemme tehneet karsintaa niiden osalta, jotka eivät ole olleet jäsentemme mielestä riittävän kiinnostavia. Tällä hetkellä tietosuoja-aihealueena kiinnostaa ja myy. Lisäksi CSM-koulutukset ovat olleet suosittuja. Uutuutena tarjoamme Koneoppista. Tulemme kehittämään tarjoomaa syksyn aikana.

Henkilöuutisia: Tiina Riutta on palannut äitiyslomalta. Toimin osin rinnakkain Tiinan kanssa loppuvuoden osalta. Omalta osaltani kiitän lämpimästi jo tässä vaiheessa Teitä yhteistyöstä.

Me TIVIAssa otamme mielellämme vastaan uusia ideoita toiminnan kehittämiseksi sekä yhteistyön parantamiseksi. Toivomme myös kirjoituksia, artikkeleita ja blogeja nettisivuillemme, joita mieluusti jaamme myös sosiaalisessa mediassa yleisöllemme.

Yhdessä olemme enemmän!

Nina From
markkinointi- ja koulutuspäällikkö
TIVIA

Julkaisija
Systeemityöyhdistys Sytyke ry
Tieto– ja Viestintätekniikan ammattilaiset TIVIA ry
Lars Sonckin kaari 12
02600 Espoo
Vaihde: 020 741 9898

Päätoimittaja
Timo Piiparinen (vt)
paatoimittaja[at]sytyke.org

Taitto
Visionomi

Toimituskunta 3/2017
Mitro Kivinen
Satu Kullström
Paula Miinalainen
Minna Oksanen
Timo Piiparinen

Tilaukset 2017
Sytyke-lehti sisältyy Sytyke ry:n jäsenmaksuun
Vuositilaus 36 €
Irtonumerot 10 €

Vuoden 2017 numerot
1. Tulevaisuuden tekijät
2. Kestävä kehitys
3. Regulaatiot
4. Laivaseminaarin satoa

Painos
Painos 1700 kpl
Painopaikka: K-S Paino
ISSN 2,323-8275 (painettu)
ISSN 2323-8283 (verkkojulkaisu)
5. vuosikerta

Ilmoitukset ja ilmoitushinnat
paatoimittaja[at]sytyke.org

Pääkirjoitus

Regulaatiot - digitalisaation suojatiet

Regulaatiot mielletään liiketoiminnassa usein pakkopullaksi, joka on pakko tehdä prioriteetilla 1 - käynnissä olevien strategisten hankkeiden kustannuksella. Itse olen tutustunut regulaatioihin jo 90-luvulla, kun viranomaisraportointia (Basel 1) ensimmäistä kertaa tehtiin pankeille: noin 200 raporttia, jotka oli pakko tehdä kuukausittain. Jossain vaiheessa kuitenkin huomasimme, että samalla kun kerätään tiedot ulkoisia viranomaisia varten, samaa tietoa voidaan käyttää liiketoimintojen omiin tarpeisiin. Tämä antoi vinkin siitä, että regulaatiohankkeista voi saada jotain hyötyäkin. 2000-luvulla regulaatioiden määrä on kasvanut yhä kiihtyvällä vauhdilla, ja liiketoiminnan on mukauduttava tähän ja löydettävä regulaatioista lisäapua strategiseen kehitykseensä.

Suurin osa regulaatioista liittyy aina tiettyyn liiketoiminta-alueeseen. EU:n tietosuoja-asetus GDPR on kuitenkin toista maata: sen vaikutus näkyy kaikessa, missä käsitellään henkilötietoa. Tietosuoja-asetuksen päätavoite on varmistaa yksilön oikeudet digimaailmassa. Tietosuojasta ja muistakin regulaatioista voidaankin sanoa, että ne ovat digitalisaation suojateitä. Näitä kannattaa visualisoida vaikkapa seuraavasti: kuinka turvallista suojatietä on ylittää, minne ne rakennetaan tai kuinka leveitä suojateitä tarvitaan? Voidaan hahmottaa myös regulaatioiden toimintamalleja. Jos niitä noudatetaan, saadaan turvallisia suojateitä.

Tietosuoja-asetuksen innoittamina kokosimme tämän regulaatioteemanumeron, jossa suurin osa artikkeleista liittyy tietosuoja-asetukseen. Pyrimme saamaan tästä tietopaketin, jolla valotetaan asetusta eri näkökulmista unohtamatta systeemityöammattilaisen arkea.

Turvallista matkaa digitalisaatioon!

Lehtitoimikunnan puolesta
Minna Oksanen

Sisältö

EU GDPR
– EU:n yleinen tietosuoja-asetus prosessina?

”EU GDPR eli yleinen tietosuoja-asetus ja sen vaatimuksia ei pystytä ratkaisemaan kaupallisella tuotteella, vaan yrityksen on mietittävä kokonaisuutta ja toimittava lainsäädännön ja asetuksien mukaisesti. Regulaation vaatimuksiin ei voi vastata yksittäisellä asialla, tuotteella tai jäämällä odottamaan valmiita ratkaisuja – niitä ei tule olemaan. Miettimällä asioita prosessien kautta, voit valmistautua vaatimuksiin askelittain”

Sanomalan uutisten otsikot huutavat EU tietopyyntöjä ja käsittelypyyntöjä – mistä oikein on kyse? Mitkä käsittelyajat nyt voisivat olla ongelmallisia? Aloitetaan ensin taustalta eli miten EU:n GDPR eli EU:n yleinen tietosuoja-asetus koskee myös minua yksilönä?

Miksi prosessit liittyvät tietosuoja -asetukseen ja tietopyyntöihin yhtenä keskeisenä asiana?

Lähestymällä EU GDPR:ää oikeuksien ja vaatimuksien kautta, olennaisessa osassa tiedonhallinnan ja -kä-sittelyn vaatimuksissa ovat henkilön:

- oikeus nähdä omat tietonsa ja mahdollisuus niiden korjaamiseen,
- oikeus tulla unohdetuksi sekä
- oikeus tietojen siirrettävyyteen sähköisesti luettavassa muodossa.

EU:n yleinen tietosuoja-asetus asettaa vaatimuksia ja velvoitteita, johon tietojen tallentajien sekä käsittelijöiden on vastattava määräajoissa. Rekisterinpitäjällä on velvollisuus vastata tietopyyntöön ”ilman aiheetonta viivytystä” ja viimeistään kuukauden kuluessa.

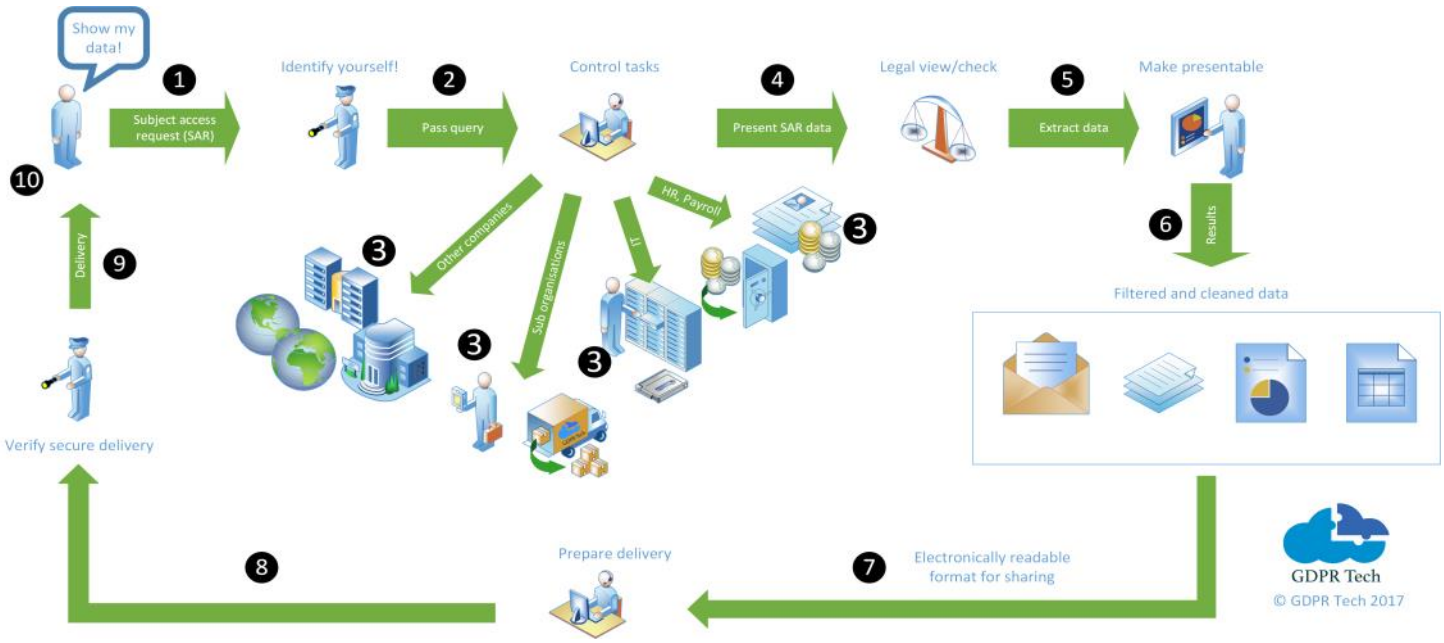
Käytännössä kyselyn pitäisi käynnistää prosessi, joka on suunniteltu, testattu ja toimivaksi todettu - tiedon tallentajalla/käsittelijällä on toteennäyttötaakka eli taakka todistaa, miten, mistä ja millä tavalla.

Henkilön/yksilön tietopyynnössä yrityksen pitää miettiä:

1. Miten tarjotaan henkilölle pääsy omiin tietoihin – onko helpompi tarjota esimerkiksi nettilomaketta, jonka kautta käynnistyy laskuri sisäisesti palvelutasoon.
2. Miten pyynnön tekijän henkilöllisyys varmennetaan, jolla vältetään tietojen antaminen väärälle henkilölle aiheuttamatta samalla uutta tietorikkoumusta.
3. Hyväksytyn tunnistamisen jälkeen prosessi jakaantuu tietopyyntöihin yrityksen sisällä sekä yhteistyökumppaneille.
4. Tietojen arviointi ja luokittelu – mitä voidaan antaa, mikä on yhtiön sisäistä, mikä on henkilön omaa.
5. Miten tiedot rajataan, jos esimerkiksi aineistossa on useita henkilöitä koskevia tietoja, on muut tiedot rajattava luotettavalla tavalla.
6. Miten aineisto kerätään sähköisesti luettavaan muotoon
7. Valmistella toimitus, varmistetaan ettei aineistossa ole ylimääräistä ja samalla huolehditaan lainsäädännön mukaisuudesta myös itse selvitykselle (pääsynhallinta, säilytys…).
8. Luotettava tiedon jakamistapa tietopyynnön tekijälle. Tavallinen sähköposti on kuin postikortti – kuka tahansa ylläpitäjä pystyy lukemaan postia myös viestiketjun varrelta. Salattu sähköposti tai muuten luotettava tiedonjakotapa ja esimerkiksi kertakäyttöisten salasanojen käyttö tiedonjakopalvelussa on suositeltavaa (vai onko suositus)
9. Toimitetaan aineisto tietopyynnön tekijälle.

Kaikki nämä vaiheet ovat EU GDPR:n mukaan suoritettava jäljitettävällä tavalla, jolloin voidaan todentaa mitä missäkin vaiheessa on tehty.

Oletko valmis – EU GDPR:n kovennettu voimaantulo on toukokuussa 2018. Oletko testannut, että pystyt vastaamaan tietopyyntöihin? Olennaista on huomata, että jos pystyt, huomaat samalla, että sisäiset prosessit ovat parantuneet ja tieto onkin löydettävissä helposti.



Juha Sallinen
Juha toimii GDPR Tech yhtiössä konsulttina ja kouluttajana. Työtehtävissä hän ollut pienestä koulutusyhtiöstä suuriin monikansallisiin jätteihin. Tehtävät niin arkkitehtinä kuin myyntitehtävissä antavat laajan kokonaisnäkymän EU GDPR:ään. Hieman yli 20 vuotta tietotekniikkaa takana ja vielä monta edessä.

Sanomalan Uutiset

N:o 190 Perjantai, 13 heinäkuuta 2018 20M € tai 4%

TED:n postipalvelimet ylikuormitettu!

Massiivisen henkilötietovuotoskandaalin kohteena olevan operaattorin huolet jatkuvat.

Viime viikolla negatiivista julkisuutta saaneen TED:n sähköpostipalvelimet ovat olleet ylikuormitettuja asiakkaiden tietopyyntökyselyjen johdosta, kertoo nimetön tietolähteemme.“Emme uskoneet, että näin voisi käydä - tietopyyntöjen tulva on yllättänyt meidät täysin”, kommentoi TED:n viestintävastaava S. Signaali.

TED:n asiakkaat, jotka ovat lukeneet lehdistä viime viikon massiivisesta tietovuodosta, ovat sankoin joukoin lähettäneet omien henkilötietojensa tietopyyntöjä. Lehteemme tulleiden tietojen mukaan TED:llä ei oltu varauduttu tähän ja pyyntöjä käsitellään **käsityönä**. “Lisäksi postilaatikkomme tursuaa tietopyyntöjä ihan **perinteisistä kirjeposteista**”, Signaali jatkaa ihmeissään.

Tietojärjestelmätoimittaja:“Meillähän ei ole mitään vastuuta tästä”

“Eihän meillä TED:n toimittajana ja tietojen tallentajana voi olla mitään vastuuta tästä” - arvioi tietojärjestelmätoimittajan TCZ:n Intian toimipisteestä johtaja Madhavan Madhavan.

Sanomalan Uutiset sai kuitenkin ulkopuoliselta konsulttitalolta PCW:ltä tiedon, että GDPR:n vaikutuksesta myös EU:n ulko-puolinen toimija, joka käsittelee EU-maiden kansalaisten henkilötietoja, on vastuussa.

“Voiko tilanne vielä pahentua?”

Konsulttiyhtiö PCW:n GDPR-asiantuntija B.Wisser kommentoi tapahtunutta lehdellemme näin:

“TED:n osalta tilanne näyttää ajautuvan katastrofiin. Vaikka teimme kaikkemme jo vuonna 2017 ohjeistuksen osalta, niin silti lähetettiin henkilötietoja tavallisen sähköpostin välityksellä. Saati että henkilöitä, joille tietoja läheteltiin olisi tunnistettu”, huokaa Wisser.

Käsittelyajat kriisissä - Lakiosasto avautuu ja pahoittelee

Tausta: TED pyysi uusia työtekijöitä lähettämään sähköpostilla tunnistetiedot, kuten ajokortin skannattuna, varmentamaan henkilöllisyytensä.

“Tiedämme kyllä, että henkilön on saatava häneen liittyvät tiedot nähtäville kuukauden sisällä tai ilman aiheetonta viivytystä”, kommentoi asianajaja L. Rinne.

“Olemme jo kauan toivoneet työkaluja tiedonhallintaan, mutta budjetti ei ole koskaan riittänyt”, kertoo Rinne.

TED:n henkilöosasto on lisäksi pulassa henkilöön liittyvien skannattujen kuvatiedostojen kanssa, kertoo nimetön tietolähteemme.

Sanomalan faktaboksi

B. Wisserin kootut palat EU:n tietosuoja-asetuksesta. Nämä kohdat tulee huomioida henkilötietojen käsittelyssä:

- Lainmukaisuus, avoimuus
- Nimenomainen ja laillinen tarkoitus
- Asianmukaisuus ja minimointi
- Täsmällisyys
- Säilytyksen rajoittaminen
- Turvallinen ja ehyt käyttö, luottamuksellisuus
- Tilivelvollisuus

GDPR Tech

Samat säännöt kaikille

EU:n tietosuoja-asetus takaa samat säännöt kaikille EU:n alueella toimiville yrityksille ja organisaatioille, jotka käsittelevät henkilötietoja. Kussakin maassa on ollut omia säännöksiä, joiden noudattaminen ylirajojen tapahtuvassa liiketoiminnassa on ollut raskasta. Jo EU:ssa toimivien yritysten tiedottamiskustannukset 28:lle eri viranomaiselle ovat olleet vanhassa järjestelmässä 130 miljoonaa euroa vuodessa. Samat säännöt kaikille helpottaa liiketoimintaa ja on myös reilumpaa sekä vauhdittaa yritystoimintaa. On arvioitu, että tämän yhden lain tuomat hyödyt ovat n. 2,3 miljardia euroa.

Tutkimuksen mukaan vain 15 prosenttia ihmisistä tuntee hallitsevansa antamiaan tietoja verkossa. EU:n tietosuoja-asetus varmistaa ihmisten oikeutta omiin tietoihinsa. Omia tietojaan ihmisten tulee saada tarkastaa, korjata, siirtää ja tulla unohdetuksi. Näin henkilötietojen käsittelystä tulee läpinäkyvää ja myös luetettavaa. Epäluottamus tietosuojaa kohtaan on ollut merkittävä digitaalitalouden kasvun este. Luotettava ja läpinäkyvä käsittely mahdollistaa uutta uudenlaista liiketoimintaa. Tästä on esimerkkinä Suomen hallituksen kärkihankkeisiin kuuluva eKuitti, josta enemmän tässä lehdessä toisaalla.

Ketä tämä tarkkaan ottaen koskee?

Asetusta sovelletaan koko EU:n alueella kaikkiin orga-

Paula Miinalainen
Paula on pitkän linjan ICT-ammattilainen. Hänellä on vuosikymmenten aikana kertynyt ammattitaito järjestelmien rakentamisesta erityisesti taloushallinnon ja vakuutustenhoidon alueella. Paulasta on tärkeää se, että nyt yhdenmukaistetaan EU:n direktiivien määräämänä vastaavia järjestelmiä EU:n alueella.

Suojele henkilötietoja - suojele organisaatiotasi

nisaatioihin, jotka käsittelevät EU-kansalaisten henkilötietoja oman toimintansa vuoksi tai käsittelevät niitä toisen organisaation puolesta. Henkilötietoja ovat: nimi, osoite, sijaintipaikka, verkontunnistetiedot, tulot, kulttuurillinen profiili.

Jokaisen organisaation tehtävänä on suojella niiden ihmisten oikeuksia, jotka luovuttavat organisaatiolle tietojaan. Tämän varmistamiseksi on määrätty joukko sääntöjä, joita on pakko noudattaa. Noudattamatta jättäminen on sanktioitu. Sanktio voi olla: varoitus, huomautus, tietojenkäsittelyn keskeyttäminen tai sakko. Sakko voi olla jopa 20 miljoonaa euroa tai 4 % vuosittaisesta liikevaihdosta. Organisaation on nimettävä tietosuojavastaava, jos käsitellään henkilötietoja laajamittaisesti tai käsitellään arkaluontoisiksi luokiteltuja tietoja. On myös suositeltavaa, että yrityksen vastuuvakuutuksiin lisätään tietosuojan vakuutus.

Merkittävä muutos aikaisempaan on se, että organisaatiolla on ”todistustaakka”. Organisaation on pystyttävä kirjallisesti todistamaan, miten asetuksen määräyksiä on organisaatiossa noudatettu. Asetus antaa jonkin verran kansallista liikkumavaraa. Se aiheuttaa lukuisia muutoksia Suomen lainsäädäntöön. Muutokset ovat parhaillaan lausuntokierroksella oikeusministeriössä.

Uutena asiana tietosuoja-asetuksessa on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta tietosuojaviranomaiselle 72 tunnin kuluessa loukkauksen ilmitulosta. Myös rekisteröidylle henkilölle on ilmoitettava viivytyksettä, jos loukkaus todennäköisesti aiheuttaa hänelle haittaa. Tämä on tärkeä uudistus. On tosi tärkeää saada tietää jos esim. luottokorttitiedot ovat vuotaneet vääriin käsiin.

EU:n tietosuoja-asetus GDPR, General Data Protection Regulation, tuli voimaan 24.5.2016 ja siirtymäaika päättyy 25.5.2018

Veli-Matti Heiskanen
Kirjoittaja on toiminut 1990 –luvun puolesta välin lähtien ICT –alan organisaatioiden johtoryhmien jäsenenä. Nykyään Veli-Matti edistää robotiikan leviämistä ja käyttöönottoa Suomessa, valmentaa organisaatioiden myyntiorganisaatioita tekemään arvopohjaista myyntiä ja edesauttaa organisaatioita EU:n tietosuoja -asetusten velvoitteiden täyttämisessä.

Tietotilinpäätös helpottamaan EU:n tietosuoja-asetukseen valmistautumista

Europarlamentin kansalaisvapauksien valiokunnan hyväksymä tietosuoja-asetus ja tietosuojadirektiivi astui voimaan 24.5.2016. Siirtymäaikaa asetuksen noudattamiselle annettiin kaksi vuotta, joten uusia tietosuojasääntöjä aletaan soveltaa 25.5.2018, myös Suomessa.

Vahinkovakuutusyhtiö If:n elokuussa 2017 julkaisemasta kyselytutkimuksesta ilmenee, että lähes kaksi kolmesta pk-yrityksestä arvioi tietävänsä vähintään pääpiirteissään, mitä vaatimuksia sääntely tuo omalle yritykselle. Epäilen kyllä, että tuloksessa korostuu enemmän ymmärrys siitä, että tiedetään milloin tietosuoja -asetus astuu voimaan, ja että otsikkotasolla ymmärretään, mitä asioita ne tulevat koskettamaan. Huolestuttavaa tuon kyselyn tuloksissa oli, että joka seitsemäs vastaaja myönsi, ettei lainkaan tiedä asetuksen merkitystä.

Lähtökohtana uudella asetuksella on suojella kuluttajaa ja harmonisoida jäsenmaiden kansallinen lainsäädäntö sekä luoda yhteiset standardit pitkälle tulevaisuuteen. Asetus korvaa nykyisen EU –direktiivin sekä myös Suomen nykyisen henkilötietolain, ja edellyttää myös henkilötietolain muuttamista suurelta osin.

Mitä muutokset koskettavat?

EU:n yleinen tietosuoja-asetus on pakottavaa lainsäädäntöä ja tulee edellyttämään organisaatioilta perinteisten rekisteriselosteiden, tietoturvan ja tietosuojan lisäksi uusia prosesseja ja jopa aivan uudenlaista työnkuvaa. Eli merkittäviä muutoksia voi olla tiedossa monissa organisaatioissa.

Usein EU:n tietosuoja-asetus ymmärretään vain rekisteriselosteiden tarkennuksena, mutta se on paljon laajempi ja vaativampi velvoite. Vaatimuslistalla ovat myös erilaiset prosessikuvaukset sekä tietojärjestelmiin, tietovarantoihin ja näiden välisiin tietovirtoihin liittyvä dokumentaatio. Nämä kaikki liittyvät kiinteästi tilintekovelvollisuuteen, jossa määritetään, että organisaatiot ovat velvoitettuja osoittamaan ja todistamaan aktiivisesti noudattavansa lakia – asianmukaisesti ja rekisteröidyn henkilön kannalta läpinäkyvästi, ja että tietosuojasäännökset huomioidaan yhteisön tai yrityksen toiminnan suunnittelussa ja toteutuksessa.

Tietotilinpäätös on käytännössä yksi raportoinnin muoto yrityksille ja yhteisöille.

Kaikkien prosessien ja toimenpiteiden tulee olla dokumentoituja. Ja kun tarkastellaan kuvattujen dokumentoitavien toimenpiteiden listaa (mm. tietosuojapolitiikka, tietoarkkitehtuuri- ja tietovirtakuvaukset, koulutusmateriaalit, sertifioinnit, tietotilinpäätösraportointi, roolit, vastuut, työohjeet jne), on helppo todeta, että mistään pienestä asiasta ei ole kyse. Mitä enemmän organisaation liiketoiminta perustuu henkilötietojen keräämiseen ja hyödyntämiseen, ja mitä enemmän niitä koskevia prosesseja on olemassa, sitä suurempi työ uuden tietosuoja-asetuksen velvoitteiden täyttäminen on.

EU:n tietosuoja-asetuksessa on määritelty asiakirja, joka jokaisen rekisterinpitäjän on laadittava, ja pidettävä jokaisen saatavilla. Siitä tulee ilmetä mm. henkilötietojen kä-

sittelyn tarkoitus, mihin tietoja säännönmukaisesti luovutetaan ja kuvaus rekisterin suojauksen periaatteista. Ja kun henkilötietoja ei enää tarvita, ne tulee hävittää järjestelmästä, ellei niiden jatkokäsittelylle ole laillista perustetta. Iso muutos on pystyä perustellusti todentamaan, miksi henkilötietoja ylipäänsä kerätään, mihin niitä käytetään ja miten sekä kuinka pitkään niitä säilytetään.

Henkilötietojen käsittelyn piirteitä uudessa asetuksessa

Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi tiedoiksi. Henkilötietoja ovat esimerkiksi nimi, valokuva, IP-osoite, henkilötunnus, nimi + työnantajan nimi, henkilö jäljitettynä sijaintiin esim. matkapuhelimen avulla ja joissakin tapauksissa myös puhelinnumero.

Henkilö voi vaatia, että hänen henkilötietonsa poistetaan ja ettei niitä käsitellä sen jälkeen, kun henkilötietoja ei enää tarvita niihin tarkoituksiin, joihin ne alun perin kerättiin, ellei käsittelylle ole laillista perustetta. Henkilötiedot saa pyynnöstä huolimatta säilyttää muun muassa silloin, jos se on tarpeen lakisääteisen velvoitteen noudattamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Luonnollisella henkilöllä on myös oikeus saada omat tiedot käyttöönsä yleisesti käytettävässä tiedonsiirtomuodossa milloin tahansa pyydettäessä. Nämä velvoitteet todennäköisesti edellyttävät muutoksia niin toimintatapoihin kuin tietojärjestelmiinkin.

Jo nyt tunnistettuja riskejä olemassa olevissa prosesseissa on ollut mm. liian henkilötiedon kerääminen (suhteessa käyttötarkoitukseen), vanhojen tai virheellisten tai epärelevanttien tietojen käsittely, henkilötietojen käsitteleminen lainvastaisiin tai käsittelyn tarkoituksen vastaisiin tarkoituksiin sekä tyypillisesti useissa organisaatioissa se, että tietoihin pääsee käsiksi liian suuri joukko organisaation työntekijöitä. Uuden asetuksen mukaan käsittelijöiden piiriä tulee rajoittaa, ja myös tietojärjestelmien oikeuksia rajoittamalla varmistaa, että vain asianmukaisilla henkilöillä on pääsy henkilötietoihin.

Mitä on tietotilinpäätös?

Tietotilinpäätös on käytännössä yksi raportoinnin muoto yrityksille ja yhteisöille. EU:n tietosuoja-asetukseen valmistauduttaessa tietotilinpäätös on erinomainen työkalu. Se on myös oivallinen työkalu henkilötiedon haltuunottoon, sekä auttaa myös osoitusvelvollisuuden toteuttamisessa. Tietotilinpäätöksessä on kyse organisaation osien ja ihmisten osaamisen yhdistämisestä ja kuvaamisesta tavalla, jota kaikki voivat hyödyntää. On kuitenkin korostetusti muistutettava, että tietosuojan toteuttaminen on jatkuva prosessi, ja että tietotilinpäätös on nimensä mukaisesti tietotilinpäätöshetken tilanne. Yksi hyvä tapa voisi olla sitoa tietotilinpäätös organisaation vuosikelloon, niin että ajantasainen tietotilinpäätös voidaan kätevästi liittää taloudellisen tilinpäätöksen ”liitteeksi”.

Kun tarkastellaan tietotilinpäätökseen sisältyviä kokonaisuuksia, huomataan, että asianmukaisesti toteutettuna se vaatii paljon työtä, joko organisaation sisäistä työtä, asiaan perehtyneiden konsulttien osaamista tai näiden yhdistelmää. Joka tapauksessa siihen on varattava paljon aikaa, koska jokainen organisaation henkilötietoja käsittelevä prosessi on kuvattava, tarkasteltava ja dokumentoitava erikseen.

Tietotilinpäätökseen laajuuteen vaikuttavia asiakokonaisuuksia ovat mm. liiketoiminnan luonne, koko ja sen vaikutukset tietosuojalle, verkkopalveluihin liittyvät prosessit ja dokumentit, tietosuojan alaista tietoa käsittelevät prosessit ja järjestelmät, tietosuojaan liittyvät ohjeistukset ja dokumentaatio sekä henkilötietojen käsittelyyn liittyvien sopimusten katselmointi.

Lopputuloksena tietotilinpäätöksessä syntyy analysoidut dokumentit ja ohjeistukset, analysoidut henkilötietoja käsittelevät prosessit ja niihin liittyvät tietojärjestelmät, tietovarannot ja tietovirrat, kehityssuunnitelma ja suunnittelun etenemisen varmistavat auditoinnit. Varsinkin, jos tietotilinpäätös tehdään kokonaan organisaation omin voimin, on auditoinnin osoittaminen ulkopuolisen toteuttamana suositeltavaa. Yksi tietotilinpäätöksen eduista on myös se, että jo sen ensimmäistä versiota voidaan hyödyntää osoitusvelvollisuuden täyttämisen todentamiseen.

Kenellä on vastuu tietosuoja-asetuksen velvollisuuksien täyttämisestä?

Vaikka EU:n tietosuoja-asetuksen noudattamista aletaan vaatia vasta 25.5.2018 alkaen, on hyvä ymmärtää, että kyseessä on prosessi, ei projekti.

Vastaus otsikon kysymykseen on yksinkertainen. Vastuu on organisaation johdolla. Jotta asetusta aletaan varmasti noudattaa sen määrittelemässä laajuudessa, on sen noudattamatta jättämisestä määritelty merkittävät sanktiot. Asetuksessa määritellään myös, että organisaatioissa on nimettävä asiasta vastaava henkilö. On myös tärkeää, että määritellään tietoturvaan liittyvät roolit ja vastuut yleisesti. Yksi henkilö ei voi olla koko organisaation tietoturva ja tietosuoja, eli yrityksissä tulisi olla oma määritelty tietoturvaorganisaationsa. Koulutukset aiheesta koko henkilöstölle tulisi pitää jatkuvasti ajan tasalla, jotta kaikki voisivat ja osaisivat toimia astuksen vaatimusten ja yrityksen määrittelemän toimintatavan mukaisesti.

Vaikka tietosuoja-asetuksen noudattamista aletaan vaatia vasta 25.5.2018 alkaen, on hyvä ymmärtää, että kyseessä on prosessi, ei projekti. Ja jos teidän organisaatiossanne ei ole vielä aloitettu ensimmäisen kierroksen projektia asioiden kuntoon saattamiseksi ja dokumentoimiseksi (esim. tietotilinpäätös), nyt alkaa olla viimeiset hetken hihojen käärimiseksi.

Jyrki J. J. Kasvi
Kirjoittaja on kansanedustaja, toimivapaalla Tieto-yhteiskunnan kehittämiskeskus TIEKEstä.

Data on valtaa

Data kertoo meistä käytännössä kaiken. Siksi niin monet haluavat kerätä ja käyttää sitä. Onko yksityisyys jo menetetty, vai turvaavatko tietosuoja-asetus ja tiedustelulait meidän henkilötietomme?

Vuonna 2013 joku saattoi huomata pienen tiedeuutisen, jossa kerrottiin Cambridgen yliopiston tutkijoiden havainneen, että Facebookin "tykkäysten" perusteella voi päätellä muun muassa ihmisen luonteen, uskonnon, etnisen taustan, poliittiset mielipiteet, seksuaaliset mieltymykset, älykkyyden jne. Itse asiassa tutkijoiden kehittämä algoritmi pystyi arvioimaan ihmisten luonteenpiirteitä paremmin kuin heidän puolisonsa.

Sittemmin kyseiset tutkijat rekrytoitiin yritykseen nimeltä Cambridge Analytica, joka auttaa eri maiden poliitikkoja kohdentamaan äänestäjille henkilökohtaisesti räätälöityä viestintää. Neuroottiselle aseksuaalille katoliselle konservatiiville kannattaa kohdentaa erilaisia mainoksia ja uutislinkkejä kuin masentuneelle biseksuaalille agnostikko-liberaalille, etenkin jos toisen halutaan jäävän vaalipäivänä kotiin ja toisen äänestävän.

Cambridge Analytican tunnetuimpia asiakkaita ovat olleet Donald Trump ja Iso-Britannian Brexit-äänestyksen Leave-kampanja. Pelkästään Leave-kampanjaan osallistuneet järjestöt maksoivat lehtitietojen mukaan Cambridge Analytican kanadalaiselle AggregateIQ-tytäryhtiölle some-viestintänsä kohdentamisesta lähes viisi miljoonaa euroa. Rahojen käyttöä ei ole voitu arvioida, koska Iso-Britannian vaalilait eivät ulotu Kanadaan.

Euroopan Unionin vastaus

Cambridge Analytica on hyvä esimerkki siitä, mitä kaikkea meistä kerätyillä tiedolla voidaan tehdä, on sitten kyse hakukonehistoriasta, sosiaalisesta mediasta, sijaintidatasta tai ostoskäyttäytymisestä. Kaikki henkilötiedot ovat arvokkaita, etenkin yhdistettyinä. Moni haluaisikin rajoittaa radikaalisti omien henkilötietojensa keräämistä, mutta samalla monet heidän käyttämänsä digitaaliset palvelut lakkaisivat toimimasta.

Lainsäätäjät ovat heränneet henkilötietojen keräämisen ja hyödyntämisen kysymyksiin jälkijunassa. Esimerkiksi Saksan liittokansleri Angela Merkel on vaatinut, että nettipalveluiden taustalla olevien algoritmien tulisi olla läpinäkyviä, jotta ihmiset voisivat arvioida, miten esimerkiksi hakukoneet ja sosiaalinen media vaikuttavat meidän mielipiteisiimme ja käytökseemme.

Euroopan Unionin vastaus henkilötietojen hallinnan kysymyksiin on yleinen tietosuoja-asetus, GDPR, jonka tavoitteena on parantaa eurooppalaisten tietosuojaa suhteessa meistä tietoja kerääviin yrityksiin ja viranomaisiin. Asetuksen ehkä radikaalein muutos on periaatteellinen; Enää ei riitä, että henkilörekisterin pitäjä noudattaa tietosuojalakia, sen on pystyttävä myös osoittamaan se.

Tietosuoja-asetusta ei pysty kiertämään siirtämällä pilvipalvelimet EU:n ulkopuolelle, vaan organisaation toimipaikka EU:n alueella ratkaisee. Asetusta voidaan tietyissä tilanteissa soveltaa jopa kokonaan EU:n ulkopuolella toimiviin organisaatioihin, kun ne käsittelevät eurooppalaisten henkilötietoja.

GDPR tuo eurooppalaisille uusia oikeuksia, esimerkiksi oikeuden tarkistaa omat tietonsa ja saada tieto myös siitä, miten omia tietoja on käsitelty. Lisäksi ihmisille on ilmoitettava heidän tietojaan koskevista tietoturvaloukkauksista.

Henkilötietojen kaupallisen ja poliittisen hyödyntämisen kannalta tärkein on GDPR:n vaatimus, ettei henkilötietoja saa käyttää muihin tarkoituksiin kuin siihen, jota varten ne on kerätty. Tätä yritetään todennäköisesti kiertää listaamalla verkkopalveluiden käyttöehtoihin käyttötarkoituksia mahdollisimman laveasti. Vain ani harvat kun lukevat käyttämiensä palveluiden käyttöehdot alusta loppuun. Vasta tuleva eurooppalainen oikeuskäytäntö näyttää, kuinka sitovia verkkopalveluiden käyttöehdot käytännössä ovat.

Tiedustelulaki

Perinteisemmän uhkakuvan yksityisyydelle muodostavat kansalliset turvallisuusviranomaiset. Suomi on Euroopan ainoa maa, jonka turvallisuusviranomaisilla ei ole varsinaisia tiedusteluvaltuuksia. Niiden asemesta Suojelupoliisi ja sotilastiedustelu ovat käyttäneet pakkokainolain sallimia tiedonhankintakeinoja, jotka edellyttävät sekä vakavaa rikosta että epäiltyä henkilöä.

Suomeen on kolmen vuoden ajan valmisteltu noin 1000-sivuista tiedustelulakipakettia, josta käyty keskustelu on keskittynyt tietoliikennetiedusteluun, joka on kuitenkin vain pieni osa laajasta kokonaisuudesta. Esitetyt tiedustelulait kattavat sekä sotilas- että siviilitiedustelun sekä kotimaassa että ulkomailla.

Jos valmistellut tiedustelulait hyväksytään esitetyssä muodossa, Suomen sotilas- ja siviiliturvallisuusviranomaiset saisivat toimivaltuudet paitsi tietoliikennetiedusteluun myös esimerkiksi henkilö- ja tietojärjestelmätiedusteluun, jos tuomioistuin arvioi, että "vakava uhka kansalliselle turvallisuudelle" sitä vaatii. Tällainen uhka voisi olla esimerkiksi suomalaisiin ulkomailta kohdistuva tiedusteluoperaatio, jonka torjuntaan perinteiset pakkokeinot eivät riitä.

Tiedustelulakien merkitystä alleviivaa se, että ne edellyttäisivät perustuslain muutosta. Lisäksi tiedusteluoperaatioita valvomaan ollaan perustamassa tiedusteluvaltuutetun virkaa ja eduskuntaan tiedusteluvalvontavaliokuntaa. Koska Suomi on tiedustelulakeja säätäessään muista maista jäljessä, voimme ottaa opiksi muiden maiden virheistä. Historia on opettanut tiedustelutoiminnan vaativan riippumatonta luvitusta ja valvontaa.

Tiedustelulakien valmistelu on vielä kesken, ja esimerkiksi tietoliikennetiedustelun rajoista keskustellaan edelleen. Toivottavasti myös muista tiedustelulakien yksityiskohdista muistetaan keskustella. Muuten monelle tulee ikävänä yllätyksenä, kun ensimmäinen suomalainen tiedusteluhenkilö palautetaan Suomeen ei-toivottuna henkilönä, tai kun suomalainen urkintaohjelma löytyy naapurimaan ministeriön tietokoneista.

Paula Miinalainen
Paula on pitkän linjan ICT-ammattilainen. Hänellä on vuosikymmenten aikana kertynyt ammattitaito järjestelmien rakentamisesta erityisesti taloushallinnon ja vakuutustenhoidon alueella. Paulasta on tärkeää se, että nyt yhdenmukaistetaan EU:n direktiivien määräämänä vastaavia järjestelmiä EU:n alueella.

eKuitti

"Taloushallinto saadaan takaisin Suomeen. Taloushallinto ei ole enää halpatyötä," Finanssiala ry:n kehityspäällikkö Pirjo Ilola

"eKuitti vähentää merkittävästi kirjanpitäjän työtä. Kirjanpitäjästä tulee ylemmän tason talousneuvoja, joka neuvoo miten saadaan aikaan parempaa liiketoimintaa. Miten palvelut saadaan laadukkaammiksi ja kustannustehokkaiksi. Kuittien rivikohtainen ja rakenteellinen standardoitu muoto mahdollistaa tarkan automaattisen toiminnan ohjauksen ja seurannan. Ja merkittävää on, että taloushallinto saadaan takaisin Suomeen. Taloushallinto ei ole enää halpatyötä, joka voidaan ulkoistaa ulkomaille", sanoo Finanssiala ry:n kehityspäällikkö Pirjo Ilola.

"Rakenteinen muoto antaa mahdollisuuden kerätä alv-tiedot eKuiteista. Matkalaskujen käsittely voidaan automatisoida niin, että kalenterista saadaan tiedot siitä mihin matkakulut kohdistuvat. Näin kaikki kulut tulevat heti mukaan kirjanpitoon eikä tule vuoden lopussa kiire kerätä kulukuitteja laatikoiden pohjilta. Rakenteinen eKuitti antaa mahdollisuuden kehittää uusia palveluja kuten linkki tuottajan sivuille, käyttöohjeeseen, kaloritaulukkoon, hiilijalanjälkeen, suklaapoliisiin, terveyssovellukseen jne.", luettelee Pirjo Ilola hyötyjä.

Mikä eKuitti?

Liikenne- ja viestintäministeriö on teettänyt selvityksen ”Ostajan oikeudet kuittidataan. Reunaehtoja, toteutusvaihtoehtoja ja suosituksia”. Se julkaistiin maaliskuussa 2017. Sen voi lukea valtioneuvoston sivuilta https://julkaisut.valtioneuvosto.fi. (Kirjoita avautuvan sivun hakukenttään sana kuittidataa.) Se on osa Suomen hallituksen ”Digitaalisen liiketoiminnan kasvuympäristön rakentaminen –hanketta”. Selvityksessä on seikkaperäisesti käyty läpi EU:n henkilötietosuoja-asetuksen asettamat vaatimukset ja rajoitukset ja niiden noudattamisen merkitys. Kuittien käsittelyssä on arvioitu saavutettavan 5-7 euron säästö per kuitti tai lasku. Valtiohallinnossa voidaan säästää noin 30 henkilötyövuotta eli 2 miljoonaa euroa vuodessa, jos kaikki ostokuittien tiedot saadaan välittymään automaattisesti matka- ja kulunhallinta-järjestelmiin sekä laskujen kierrätys- ja arkisto järjestelmiin. Suomessa tehtiin Suomen pankin tilastojen mukaan vuonna 2015 1,4 miljardia korttimaksua. Tässä luvussa on kaikki korttiostot yritysten tekemät kuin myös kuluttajien. On arvioitu että kuittien tallennuskustannuksissa voidaan säästää yritystasolla noin 800 miljoonaa euroa vuodessa. Suomessa tehtiin noin 7,2 miljoonaa verkkokauppaostoa, jotka ovat enimmäkseen kuluttajaostoja. Myös tästä syntyy säästöjä. Suomessa nostettiin käteistä noin 18,0 miljardia euroa. Myös käteiskaupan kuittien käsittelystä syntyy säästöä.

Elokuussa 2017 ilmestyi Finanssiala ry:n selvitys ”Korttioston kuittitietojen välitys Finvoice-verkkolaskuna”. Pohjana on Finanssialan Finvoice-standardi, jonka käyttäjiä ovat kauppiaat, korttiyhtiöt, yritykset ja tilitoimistot. Lisätietoja on sivustolla www.finvoice.info.

Aluksi Myyjä valitsevat käyttämänsä kuittivaraston ja sopii kuittien välittämisestä. Ostaja sopii myös valitsemansa kuittivaraston kanssa eKuittien vastaanottamisesta ja siihen tarvittavasta eOsoitteesta. Ostohetkellä Myyjä saa tiedot maksun ja tiedon ostajan eOsoitteesta. Kuitti välittyy edelleen ostajan kuittivarastoon ja myyjän taloushallintoon. Ostaja voi välittää eKuitin rakenteisessa muodossa omaan taloushallinnon järjestelmään. eKuitin pohjana on verkkolasku. Koska yrityksillä on jo verkkolasku käytössä, niin ei tarvitse investoida kuittia varten.

Pirjo Ilola

- Toimii kehityspäällikkönä Finanssiala ry, erityisesti Finvoice verkkolaskun asiantuntijana
- Edustaa Suomea Euroopan verkkolaskuryhmässä European Multi-Stakeholder Forum on e-invoicing
- Mukana CENin Teknisessä komiteassa TC 434 Electronic Invoicing, jossa tehtiin direktiivin mukainen verkkolaskun semanttinen malli
- Pankkien edustajana verkkolaskufoorumin ohjausryhmässä ja European Payment Council (EPC):n Standards Task Force ryhmässä, jossa laaditaan SEPA maksujen soveltamisohjeet
- Finanssialan edustajana European E-Invoicing Service Providers Association ja SFS:n Finanssialan seurantaryhmässä

EU:n direktiivi sähköisestä laskutuksesta tulee voimaan 27.11.2018

Direktiivi tarkoittaa, että vuoden kuluttua koko EU:n alueella julkishallinto käsittelee ainoastaan semantiikaltaan saman sisältöisiä sähköisiä laskuja. Laskut ovat myös muodoltaan ja syntaksin sekä tiedonsiirron osalta yhteen toimivia. Julkisia hankintoja tekevät hankintayksiköt ovat velvollisia vastaanottamaan ja käsittelemään direktiivissä mainittujen standardien mukaisia sähköisiä laskuja.

”Kun tiedot ovat laskuissa oikeissa kentissä, niin vastaanotetut laskut saadaan suoraan automaattiseen käsittelyyn. Saadaan tarkempi toiminnan ohjaus ja sopimusten seuranta. Jos yritys on sopinut, että ostetaan tietystä firmasta, niin voidaan valvoa, että näin tapahtuu. Jos ei ole, niin tutkitaan, missä vika. Arjen ohjaus ja seuranta automatisoituu, tarkentuu ja on reaaliaikaista.” sanoo Finanssiala ry:n kehityspäällikkö Pirjo Ilola.

Suomessa julkishallinto on käyttänyt pankkien kehittämää Finvoice-kuvausta tai Tiedon TeappsXML kuvausta (JHS155). Nyt jo 90 % valtiolle tulevista laskuista on verkkolaskuja. Verkkolaskun ja sähköisen laskun ero on määritelty Valtiokonttorin verkkolaskusivustolla seuraavasti:

”Verkkolasku laaditaan, siirretään ja vastaanotetaan rakenteisessa sähköisessä muodossa, joka mahdollistaa sen automaattisen konekielisen käsittelyn vastaanottajalla. Verkkolasku välitetään aina verkossa. Verkkolasku ja sähköinen lasku eivät ole sama asia. Sähköinen lasku voi olla ostolaskujen käsittelyjärjestelmään skannattu lasku tai sähköpostilla välitetty pdf-lasku. Valtio ei vastaanota eikä lähetä sähköpostilla välitettävää laskua.”

Valtiokonttorin verkkolaskuista saat tarkempaa tietoa verkkosivustolta www.valtiokonttori.fi. Kirjoita sivun kohtaan ”Hae sivustolta” sana Verkkolaskutus.

Finassiala ry on tehnyt tutkimuksen paperittoman kirjanpidon vaikutuksesta hiilijalanjälkeen. Tutkimus ”Selvitys taloushallinnon automatisoinnin ilmastovaikutuksista” on luettavissa kokonaisuudessaan Finanssiala ry:n verkkosivustolta www.finanssiala.fi (sivun alalaidasta polku Materiaalipankki, tutkimukset).

EU:n direktiivin mukaista ohjeistusta julkishallinnolle ovat kehittämässä yhdessä Finanssialan ja Tiedon kanssa Kunnan Taitoa oy, Kuntaliitto ja Valtion talous- ja henkilöstöhallinnon palvelukeskus (Palkeet). Syyskuussa Finvoice 3.0 julkaistiin luonnoksena ja kommentointiaikaa on lokakuulle. Tarkoitus on saada valmiiksi julkishallinnon soveltamisohje syksyn aikana. Tavoite on, että julkishallinnon ohje toimisi myös yritysten ohjenuorana laskun tietosisällön niissä vaatimuksissa, joihin he mukauttavat omia järjestelmiään. Tällöin ohjelmistotalojen on helpompi tehdä verkkolaskutoteutuksia, kun vastaanottajat eivät vaadi samaa tietoa eri tietokenttään kuin yhteisesti on sovittu. Ja tämä koko EU:n alueella!

Standardointi on perusta sille, että voi rakentaa kilpailukykyä

Standardointi on maratonia, se ei ole pikajuoksua!

Kysyn millaista on tehdä standardointityötä isossa mittakaavassa koko EU alueena. Olen kokenut useasti yhden yhtiön tai konsernin osalta että yhteisten käsitteiden luominen ei olekaan mikään itsestäänselvyys.

Pirjo Ilola kertoo tuntojaan: ”Standardointi on perusta sille, että voi rakentaa kilpailukykyä. Jos ei kommunikoi niin, ei voi rakentaa uutta. Perusdata pitää kulkea yhteisesti sovitulla standardilla. Standardointi on maratonia, se ei ole pikajuoksua. Se on hidasta, vaikeaa, joudutaan tekemään kompromisseja ja luopumaan. - Yhteistyö on myös synergiaa. Opitaan toisilta ja työ tuottaa myös tulosta.

Kerro Eurooppa yhteistyöstä?

”Arki on erilainen eri maissa. Esimerkiksi meille tuttu hyvityslasku on käsitteenä joissakin maissa aivan tuntematon. Lasku lähetään takaisin ja pyydetään uusi lasku.”

Pirjo Ilola teki eurooppalaiseen standardointiin osallistuvien suomalaisten tahojen kanssa yhteistyötä. Yhdessä määriteltiin etukäteen Suomen tavoitteet standardille. Määrittelivät, mitkä ovat pakolliset asiat ja mistä voidaan neuvotella. ”Tämä on Suomen edunvalvontaa. Kun kotiläksyt on hyvin tehty ja on kokouksissa paikanpäällä ja ottaa kantaa niin tuloksia syntyy. Uskottavuus syntyy kun tekee yhteistyötä koko ajan. Se on työlästä ja rankkaa. Mutta Suomen salaisuus on ahkera osallistuminen. Niin saa omat asiat läpi. Aito kiinnostus palkitaan.”

Pekka Salomaa
Pekka on asiakkuuksien hallinnan ja asiakaskokemuksen parantamisen konsultti. Hän työskentelee suuressa regulaatiohankkeessa toiminnallisena konsulttina. Aiemmin Pekka on työskennellyt monissa vaativissa muutos- ja digitalisointiprojekteissa mm. Tiedossa ja DHL:ssä. Pekka uskoo, että ihmisen tulee olla isäntä ja teknologian renki.
www.linkedin.com/in/pekkasalomaa

EU:n henkilötietosuoja-asetus – liiketoiminnan toivelahja

Tämän kirjoituksen otsikko saattaa tuntua ensi lukemalla hieman oudolta, onhan vuosien varrella totuttu siihen, että kaikenlaiset sääntelyt, varsinkin EU- tasoiset lähinnä aiheuttavat ylimääräisiä kustannuksia ja hankaluuksia yrityksien liiketoiminnalle.

Onhan toki aiemminkin usein mainittu, että lähestymällä sääntelyn tuomia muutostarpeita oikein voidaan muutoksesta saada paljonkin hyötyä. Jostain syystä kuitenkin lopputulos usein on kallistunut yrityksen kannalta negatiiviseksi tai korkeintaan nykytilan säilyttäväksi.

Nyt EU:sta on siis tuotu yritysten ja organisaatioiden työstettäväksi asetus luonnollisten henkilöiden tietojen suojelemiseksi. Vuoden 2018 toukokuusta alkaen henkilötietoja käsittelevien organisaatioiden on hallittava henkilötietoja tehokkaasti, systemaattisesti, asiakaskeskeisesti ja pystyttävä tarvittaessa todistamaan viranomaiselle, että toiminta on asetuksen mukaista. Mielestäni tämä tuo yrityksille lähes ainutlaatuisen mahdollisuuden saada runsaasti liiketoiminnallista hyötyä tekemällä muutoksia, jotka ovat – asetuksen velvoittamana – aidosti asiakkaan näkökulmasta hyödyllisiä.

Tämä GDPR –asetus (General Data Protection Regulation) perustuu ajatukselle, että henkilötiedot ovat henkilön itsensä määräämisvallassa eikä niiden tahojen, jotka hänestä tietoa ovat keränneet. Henkilön oikeudet tietoihinsa kasvavat ja samalla tietojen kerääjien velvollisuudet lisääntyvät. Henkilöllä on oikeus – tietyin rajoituksin – tietojensa tarkistamiseen, korjaamiseen, siirtämiseen ja käytön rajoittamiseen. Yritysten on kaikessa henkilötietojen käsittelyssään toteutettava näitä oikeuksia. Lisäksi mm. henkilötietojen ajantasaisuudelle sekä niitä koskevalle tietoturvalle on asetettu nykyistä tiukempia vaatimuksia. Muutoksena nykytilanteeseen on myös osoitusvelvollisuus siirtymässä henkilöltä yritykselle.

On selvää, että tämä asetus koskee yrityksien toimintaa ehkä kokonaisvaltaisemmin kuin mikään muu ennen sitä. Tästä päästään otsikon väittämään. Nyt yritysten on pakko miettiä monien asioiden tekemistä uudella tavalla ja myös toteutettava uudistukset. Monet näistä uudistuksista ovat asioita, joita joka tapauksessa olisi tullut tehtävälistalle yritysten miettiessä menestymisen edellytyksiä muuttuvassa, yhä enemmän asiakaskeskeisessä kilpailuympäristössä.

Vaikka asiakaskeskeisyydestä, asiakaskokemuksen kehittämisestä tms. on puhuttu jo pitkään ja monet yritykset kertovat toimivansa asiakaskeskeisesti, ei tarvitse tehdä kovin syvälle menevää analysointia huomatakseen, että toiminnan kehittämislähtökohdat ovat suureksi osaksi sisäisiä. Muutoksia perustellaan asiakkaista lähteväksi, mutta toteutuksia nähdessään huomaa helposti, että asiakkaiden näkökulma on varsinkin IT-toteutuksissa jäänyt sivuosaan.

Tässä vaiheessa moni lukija varmaan on noussut takajaloilleen ja todennut, että ”kyllä meidän yrityksessä on oikeasti tehty asiakaslähtöisiä IT-ratkaisuja. Mitä tämä kaveri oikein luulee?” Varmasti monessa organisaatiossa näin onkin, mutta väitän, että sisäänpäin kääntyneitä, tekniseen toteutukseen ja sisäiseen valvontaan nojautuvia IT-ratkaisuja on vielä aivan liian paljon.

Myös EU on jo aikaa sitten huomannut tämän. Siellä on todettu, että digitalisoituvassa maailmassa kuluttajien luottamus siihen, että heistä kerättyä tietoa käytetään heidän hyväksymällään tavalla, on aivan liian alhainen. Henkilötiedon hallintaa ajatellaan yksilön perusoikeutena.

Tietosuoja-asetuksen tarkoituksena on toimia eräänlaisena digitalisaation suojatienä kuluttajille. Yksilön tulee voida luottaa suojatietä ylittäessään siihen, että se on tehty häntä varten, ei sen suunnittelijoita tai fyysisiä toteuttajia tai viranomaisia ajatellen. Tärkeintä ei ole se, monenko sentin etäisyydellä valkeat raidat ovat toisistaan tai paljonko täsmälleen on matkaa lähimpään risteykseen. Suojatien tulee olla turvallinen, sen on oltava luontevien kulkureittien varrella ja sen pitää kaikin tavoin helpottaa tien ylittämistä, oli ylittäjä sitten vanha tai nuori, vammainen tai terve.

Tällaista henkilötietojen suoja-

tietä todella tarvitaan. Media uutisoi lähes päivittäin tietoturvarikkomuksista. USA:ssa tuli juuri ilmi tämän vuoden aikana tapahtunut, yli 140 miljoonan ihmisen (!) henkilötietojen varastaminen. Virossa aloitetaan varotoimet tietomurtojen varalta, ja saattaa olla, että syksyn paikallisvaalien sähköinen äänestys joudutaan perumaan (HS 10.9.2017).

Palta eli Palvelualojen työnantajat tekee vuosittain tutkimusta digitalisaatiosta. Tämänvuotisen tutkimuksen tulokset tukevat esittämääni ajatusta asiakaskeskeisyyden puutteista digitaalisissa ratkaisuissa. Tutkimuksessa haastateltiin yli tuhatta Suomessa toimivan yrityksen päättäjää. Kysyttäessä yrityksen päämotiivia toteuttaa digitaalisia ratkaisuja, asiakaskeskeisyys oli vasta kolmannella sijalla. Sen nimesi tärkeimmäksi vain 10 prosenttia vastaajista. Lisäksi 42 prosenttia ei osannut vastata tähän kysymykseen mitään.

Seuraavassa käsittelen muutaman esimerkin avulla, miksi tämä tietosuoja-asetus todellakin voi olla kuin taivaan lahja monille yrityksille. Tietosuoja-asetus mielestäni ohjaa organisaatioita kohti näitä tavoitteita asettaessaan asiakkaan näkökulman ylimmäksi.

- IT:n ja liiketoiminnan yhteistyön tiivistäminen ja tehostaminen
- oikeasti asiakaskeskeisten ja -ystävällisten ratkaisujen tuottaminen
- uusien, tehostettujen toimintatapojen kehittäminen
- organisaation joustavuuden lisääminen paremman kilpailukyvyn luomiseksi

IT:n ja liiketoiminnan yhteistyön tiivistäminen ja tehostaminen on ollut aiheena pinnalla jo monta vuotta. Liiketoiminta on ottanut yhä enemmän vastuuta omista IT-hankinnoistaan, jättäen IT-osastolle lähinnä teknisen tukiroolin. IT-johto on kipuillut uuden roolin löytämisessä, eikä liiketoiminnan osaaminen aina ole riittänyt kokonaisvaltaisesti optimaalisten ratkaisujen valintaan. Teknisesti toimivien, mutta liiketoiminnan tarpeiden sekä asiakkaiden kannalta puutteellisista ratkaisuista on joskus menty toiseen äärilaitaan: tuotetaan ratkaisuja, jotka kyllä tukevat liiketoiminnan siiloa, mutta aiheuttavat paljon hankaluuksia sopiessaan huonosti yrityksen kokonaisprosesseihin. Lisäksi yritykset ovat kustannussäästöjä ja joustavuutta hakiessaan voimakkaasti ulkoistaneet IT-osaamistaan, kasvattaen näin riippuvuutta IT- toimittajista ja muista ulkoisista osaajista. On huomattu, että ulkoistuskolikollakin on kaksi puolta. Pilvestä tulevien pakettisovellusten räätälöinti tehokkaasti yrityksen toimintaa tukemaan ei läheskään aina ole tuottanut toivottuja tuloksia. Yrityksessä oleva järjestelmien osaamisvaje näkyy mm. silloin, kun pitäisi tukea kehitettyjä uusia tuotteita tai palveluja parhaalla mahdollisella tavalla.

Jotta tietosuoja-asetuksen vaatimuksiin (tietosuoja oltava yrityksen toimintaan sisäänrakennettuna ja oletusarvoisena) pystytään vastaamaan, on yrityksen toimintaa nyt välttämätöntä ajatella (liike) toiminnallisten tai IT- siilojen sijaan horisontaalisesti, asiakkaan end-to-end- prosessia tukien.

Kaikessa suunnittelussa on oltava lähtökohtana katsoa toimintaa asiakkaan näkökulmasta, muokaten sisäisiä prosesseja ja niitä tukevia IT-kyvykkyyksiä. Kun IT:n ja liiketoiminnan sekä kaiken muun yrityksessä tapahtuvan asiakkaan tietoja koskevan toiminnan yhteensovittaminen tehdään oikein, lopputulos väistämättä yhdistää asiakaskeskeisyyden ja liiketoiminnallisen hyödyn.

Mitä tarkoittaa **'oikeasti asiakaskeskeinen ja –ystävällinen'**? Eikö jokainen organisaatio jo toimi asiakaskeskeisesti? Onhan tämä aihe ollut pinnalla jo pitkään, itse asiassa useita vuosikymmeniä. Itse väitän, että monessa organisaatiossa ei välttämättä ole täysin ymmärretty, saati sitten omaksuttu aitoa asiakkaan ensisijalle asettamista toimintaa, palveluita ja ICT-ratkaisuja suunniteltaessa.

Tähän on tietenkin monia syitä, eikä tämän kirjoituksen tarkoitus ole niitä sen syvemmin pohdiskella.

Sen sijaan nykytilannetta voidaan mielestäni aivan liian usein kuvata mm. seuraavasti:

- tehdään asiakastutkimuksia, mut-

ta johtopäätökset toiminnan kehittämiseksi lähtevät sisäisistä – usein IT-teknisistä lähtökohdista. IT-arkkitehtuuri ei tue asiakaskeskeisyyttä.
- painotetaan keinoja ja määritellään tavoitteet sisäisesti. Asiakkaan tavoitteiden saavuttaminen jää taka-alalle
- osaoptimoidaan IT-kehitys. Tuotetaan pistemäisiä ratkaisuja hieman ad hoc-perusteisesti.

Oletko sinä, hyvä lukija, joskus vastannut asiakaskyselyyn nimelläsi tai muilla yhteystiedoillasi ja vastattuasi saanut jossain vaiheessa tietoa siitä, millaisia erityisesti sinua hyödyttäviä kehitystoimenpiteitä vastauksesi ovat auttaneet kysyjäorganisaatiota toteuttamaan? Niinpä niin, en minäkään. Siksi en enää nykyään vastaa mihinkään kyselyihin. Pelkkä lause ’keräämme tietoa toimintamme kehittämiseksi’ ei sano minulle yhtään mitään. Mitä minä tuosta kehittämisestä konkreettisesti hyödyn?

Tietosuoja-asetus ohjaa väistämättä henkilötietoa keräämiä organisaatioita asiakaslähtöisyyteen mm. määrittelemällä, että kaikella kerättävälle tiedolle on oltava etukäteen määritelty, selkeästi asiakkaalle ilmoitettu käyttötarkoitus sekä asettamalla henkilötietojen käytölle ja siitä viestinnälle läpinäkyvyysvaatimuksia. Jatkossa ei tule olemaan mahdollista kerätä tietoa periaatteella ’kerätään nyt, mietitään myöhemmin mitä sillä tehdään’. Asetuksen vaatimukset myös ohjaavat kohti systemaattista henkilötiedon hallintaa, mukaan lukien tiedon omistajuus, joka nykyisin melko usein on määritelty lähinnä teknisestä näkökulmasta. Nyt tietoa on alettava hallita niin, että se tuottaa asiakkaan näkökulmasta mielekkäitä selkeitä ja hyödyllisiä kokonaisratkaisuja.

IT-kehitys usein heijastaa melko suoraan liiketoiminnan siiloutumista joko toiminnoittain tai liiketoiminta-alueittain. Eräs tuttuni työskentelee suuressa suomalaisessa yrityksessä myynnin liiketoiminta-alueella. Kyseisessä yrityksessä on teknisesti hyvälaatuiset IT-sovellukset käytössä. Ongelmana käyttäjien kannalta onkin juuri tuo monikkomuoto: käyttäjillä on aivan liian monta sovellusta, mihin heidän tulee tuottaa tietoa. Koska heidän tuottamansa data on jaettu pistemäisesti eri osa-alueisiin perustuen yrityksen IT-arkkitehtuuriin, on lähinnä sattumaa mikäli tuotettu data muodostaa asiakkaan kannalta mielekkään ja hänen tavoitteitaan tukevan kokonaisuuden.

Asetuksen tuoma näkökulma pakottaa yritykset ajattelemaan asiakasmatkoja kokonaisuutena ja ottamaan henkilötietojen käsittely kokonaisuutena mukaan toimintaansa ’by default and by design’ eli oletusarvoisesti ja sisäänrakennetusti. Asiakasnäkökulma on siis oltava ennakkoehtona kaikelle IT-tekemiselle, joka jollakin tavalla tukee liiketoimintaa. Tulevaa ja meneillään olevaa IT-kehittämistä on arvioitava siten, että tietosuojan vaatimuksien toteuttaminen on priorisoitu ja toteutettu, ja tätä kyvykkyyttä on jatkuvasti ylläpidettävä ja kehitettävä.

Toiminnan kehittämistä on arvioitava jatkossa ensisijaisesti sen perusteella, mitä lisäarvoa muutoksilla saadaan asiakkaalle luotua. Aivan niin, onhan näin jo tehty vaikka kuinka pitkään. Melko pitkän ja monelta toimialalta olevan kokemukseni sekä lukuisten lukemieni tutkimustulosten ja artikkelien perusteella rohkenen väittää, että käytännössä ollaan vielä monessa organisaatiossa melko kaukana tästä. Siksi asetusten vaatimusten täyttäminen tulee väistämättä tarkoittamaan uusien toimintatapojen, prosessien ja roolien muodostamista. Näitä muutoksia on puolestaan digitaalisesti tuettava, joten IT:tä ohjataan systemaattisesti kohti aitoa asiakaskeskeisyyttä.

Viimeinen esimerkkini siitä, miksi tietosuoja-asetus tosiaan on liiketoiminnalle toivelahja, sisältää eräänlaisen kaksiteräisen miekan: mikäli **organisaation joustavuutta ja asiakaslähtöistä rakennetta** rohkeasti ja päättäväisesti kehitetään niin, että tehdyt muutokset paitsi mahdollistavat tietosuoja-asetuksen mukaisen toiminnan – josta muuten on tiedon kerääjällä osoitusvelvollisuus – luodaan myös aivan uusia mahdollisuuksia parantaa yrityksen asemaa kilpailussa. Jos asetuksenmukaisuuteen tähtäävää projektia taas ajatellaan yhtenä täytettävänä regulaatiovaatimuksena, joka tuo lisätyötä ja –kustannuksia, näyttää yrityksen tie jatkossa kovin synkältä.

Jo monen vuoden ajan on nostettu pinnalle ajatus, että yritysten tulisi organisoitua niin, että ne joustavasti pystyvät muodostamaan virtuaalisia – tai jopa virallisen organisaatiorakenteen mukaisia – tiimejä, joiden pääasiallinen tehtävä on jatkuvasti parantaa tärkeimpiä asiakasmatkoja. Parantaminen tapahtuu tekemällä asioinnista ja ostamisesta asiakkaille helppoa, nopeaa ja tyydytystä antavaa sekä ylittämällä heidän odotuksensa kerta toisensa jälkeen.

Tällaisten muutosten teossa kaksi tärkeää asiaa ovat mittaaminen sekä IT:n oikein suunniteltu tuki.

Mittaamisen tulee heijastaa paitsi yrityksen, myös sen asiakkaiden tavoitteiden saavuttamista. Sisäisen ohjauksen ja raportoinnin ohella on aidosti mitattava asiakaskokemuksen parantamiseen liittyviä määrällisiä ja ennen kaikkea laadullisia asioita. On pystyttävä katsomaan aidosti asioita ulkoa päin.

IT:n tuen liiketoiminnalle on mahdollistettava asiakassuhteiden hoitamisen laadullinen parantaminen.

Tuettavat prosessit kulkevat end-to-end asiakkaan, ei niinkään yrityksen näkökulmasta.

Tämä asettaa IT:lle uudenlaisia haasteita, mutta samanaikaisesti tuo valtavasti uutta potentiaalia osoittaa arvo liiketoiminnalle aivan uudella tavalla ja tasolla.

EU:n tietosuoja-asetuksen (GDPR) keskeiset määritelmät (artikla 4)

Tietosuoja-asetuksen henkilötiedon määritelmä on vanhan henkilötietolain määritelmää yksityiskohtaisempi ja asetuksen määritelmään sisältyy esimerkkejä henkilötiedoksi määriteltävistä tiedoista.

Asetuksen mukaan:

- **Henkilötiedolla** tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tavanomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

  Henkilötieto voi määritelmän mukaan olla esimerkiksi paikkatieto, joka kertoo jotakin tietystä henkilöstä; kuva, joka yhdistettynä esimerkiksi osoitetietoihin kertoo jotakin tietystä henkilöstä tai tämän elinolosuhteista; tai IP-osoite, jos tämä voidaan liittää tiettyyn käyttäjään; tai käyttäjätunnus.

- **Henkilötiedon käsittelyllä** tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietojen kokoelmiin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, esimerkiksi tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

- **Henkilörekisteri** on mikä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein. Tietomassa voi olla keskitetty, hajautettu tai jaettu eri perustein. Esimerkiksi jäsenrekisteri ja käyttäjärekisteri ovat henkilörekistereitä.

- **Rekisterinpitäjä** on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

- **Henkilötietojen käsittelijä** on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Lähde: Suomen Kuntaliiton yleiskirje 29.5.2017 sivu 2
www.kuntaliitto.fi/yleiskirjeet/2017/yleinen-tietosuoja-asetus

Muita linkkejä
EU komission ohje ”Tietosuoja Paremmat säännöt pienten yritysten kannalta”
www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/tiedotteet/z0PdCBWW7/Data_protection_infographic_FI-LR.pdf

Oikeusministeriön ohje
www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Minna Oksanen
Minna on tiedon hallinnan asiantuntija, jolla on kokemusta regulaatioihin liittyvistä hankkeista erityisesti finanssisektorilla. Viimeisen vuoden hän on osallistunut laajaan tietosuojahankkeeseen tiedon hallinnan näkökulmasta. Hänen vahvuuksiaan on myös ymmärrys liiketoimintatiedon mallintamisesta ja hyödyntämisestä.

Kaiken takana on tieto

Haluan omistaa tämän artikkelin edesmenneelle veljelleni Villelle, joka oli yksi Suomen johtavista tietosuoja-asiantuntijoista ja sai myös minut kiinnostumaan aiheesta tarkemmin. Koska en ole juristi vaan informaatioalan ammattilainen, oma näkökulmani aiheeseen on tietolähtöinen ja siihen on voimakkaasti vaikuttanut iso tietosuojahanke, jossa olen ollut mukana viimeisen vuoden ajan.

Ymmärtääksemme tietosuojan asettamia vaatimuksia tiedon hallinnalle, pitää tuntea tietosuoja-asetuksen perusperiaatteet: mitä tietoa organisaatiossa on, mikä tästä on henkilötietoa ja mitkä ovat sen käsittelyperusteet. Oikein tulkittuna ja toteutettuna tietosuoja-asetus voi tuoda liiketoiminnallista kilpailuetua, kun yrityksen tietopääomaa hyödynnetään asiakkaan palvelun parantamiseksi esimerkiksi hänen suostumuksellaan.

Ensi vuoden toukokuussa voimaan astuva EU:n tietosuoja-asetus tuo suuria muutoksia henkilötietojen käsittelyyn. Asetuksessa henkilötieto nähdään kuuluvan loogiseen rekisteriin. Yksi looginen rekisteri voi sisältää yhden tai useamman tietojärjestelmän, jonne tiedot on fyysisesti tallennettu. Toinen mahdollisuus on, että yksi tietojärjestelmä pitää sisällään usean eri rekisterin tietoja. Esimerkiksi samassa asiakasjärjestelmässä voi olla usean organisaatio-osan tietoja.

On huomattava, että tietosuoja-asetus ei kohdistu vain ulkoisiin asiakkaisiin, vaan sen piirissä ovat kaikki liiketoiminnassa mukana olevat eri henkilöosapuolet henkilökunnan tiedot mukaan lukien. Osapuolen käsitteeseen liittyen on tärkeää ymmärtää osapuolen elinkaari sekä prosessi- että tietonäkökulmasta. Esimerkiksi kun henkilö perustetaan asiakasjärjestelmään, hänestä tulee asiakasosapuoli, ja järjestelmästä on tällöin pystyttävä tunnistamaan, mitkä tiedot henkilö antaa itse ja mitkä haetaan muita kanavia pitkin. Asetuksen mukaan henkilöllä on oikeus omiin tietoihinsa, jopa niin, että tiedot voidaan siirtää toiselle palveluntarjoajalle.

Jokaisesta rekisteristä tulee tehdä rekisteri-/tietosuojaseloste, jossa kuvataan, mitä henkilötietoa rekisterissä voi olla ja millä tavoin tätä tietoa voidaan käsitellä. Asetuksessa ei tähän oteta suoraan kantaa, vaan kunkin organisaation on tämä tulkittava omista toimintaprosesseistaan, esimerkiksi hyödyntämällä liiketoiminnan käsite- tai tietomallia.

Henkilötiedon käsite on laaja. Siihen kuuluvat toisaalta perustiedot kuten nimi, osoite ja puhelinnumero, mutta myös kaikki henkilöön liittyvä toiminnallinen tieto sekä sellainen

tieto, josta henkilön voi tunnistaa joko suoraan tai yhdistämällä useita tietoja toisiinsa. Tästä päästään siihen johtopäätökseen, että erityisesti tieto-orientoituneessa organisaatiossa lähes kaikki tieto on henkilötietoa. Asetuksen mukaan rekisteröidyllä eli henkilöllä on oikeus tehdä omista tiedoistaan rekisterikohtaisia tietopyyntöjä. Tällöin henkilölle on toimitettava lähes kaikki häneen liittyvä tieto, pois lukien esimerkiksi liikesalaisuuksiin ja rikosepäilyihin liittyvät tiedot.

Myös vapaamuotoiset kommenttikentät kuuluvat henkilötietoihin, joten tästä voi seurata tarve ohjeistaa, mitä tietoa työntekijät organisaation sisällä kirjoittavat näihin kenttiin. Erityisen tarkkana on oltava arkaluonteisen tai muuten liiketoiminnassa salassa pidettävän tiedon kohdalla. Asetuksen artiklassa 9 mainitaan erityiset henkilötietoryhmät, jotka tarkoittavat henkilöön kohdistuvia arkaluonteisia tietoja. Näitä ovat mm. terveyteen, uskontoon, rotuun ja seksuaaliseen suuntautumiseen liittyvät tiedot sekä myös tieto ammattiliittoon kuulumisesta.

Tietosuoja-asetus ei siis pelkästään ohjaa tietojen käyttämistä, vaan myös vahvistaa, että toimitaan oikein muiden liiketoimintaa ohjaavien lakien puitteissa. Esimerkiksi jos henkilö haluaa poistaa tietojaan (“oikeus tulla unohdetuksi”), voivat muut liiketoiminnan säilytysaikavaateet estää tämän. Pisimmillään säilytysaika voi eräiden vakuutuslajien osalta olla jopa 100 vuotta, kun taas potentiaalisen asiakkaan tietoja saa säilyttää esimerkiksi vain puoli vuotta. Myös erityisesti riskienhallinnalla on omia velvoitteita asiakkaiden tietojen säilytykseen.

Asetuksessa käytetään termiä tietojen käsittelyperuste, jolla varmistetaan henkilötietojen oikea käyttötarkoitus eri liiketoimintaprosesseissa. Jotta käyttötarkoitukset voidaan ymmärtää, pitää myös selvittää, miten tieto liikkuu organisaatiossa: missä järjestelmissä se tuotetaan ja, ennen kaikkea, mitkä liiketoiminnan prosessit sitä käyttävät. Esimerkiksi kun asiakas käyttää oikeuttaan oikaista tietojaan, pitää tietojen korjaus viedä läpi koko prosessin. Tärkeää on siis ymmärtää asiakasprosessi kokonaisuutena.

Kun siirrytään yleisistä periaatteista yksittäisen henkilötietoelementin kuvaamiseen, on tietosuojan näkökulmasta tunnistettava useita eri ulottuvuuksia. Perinteisten kuvauksen ja muodon lisäksi merkittävässä roolissa ovat ainakin tiedon elinkaari sekä miten tietoa syntyy, hallitaan ja poistetaan. Tässä ulottuvuudessa voidaan huomioida myös henkilön osapuolirooli ja siihen liittyvät elinkaaren vaiheet: mikä on tiedon lähde, antaako rekisteröity tiedon itse vai saadaanko se esimerkiksi virallisesta lähteestä ja kauanko tietoa kuuluu säilyttää. Toinen ulottuvuus on tiedon käyttövaltuus eli kuka tietoa saa nähdä ja mahdollisesti myös muuttaa. Lisäksi on selvitettävä, onko tieto arkaluonteista. Näiden lisäksi tietoelementtejä voidaan myös luokitella liiketoiminnan muiden tarpeiden mukaan.

Miten tiedonhallinta ja tietosuoja liittyvät toisiinsa? Onko tiedonhallinnan tavoitteena yrityksen tietopääoman tuntemus, tietojen oikeellinen käyttö, tiedon oikeellisuus vai tiedon laadun parantaminen? Nämä kaikkihan kuuluvat myös tietosuoja-asetuksen tavoitteisiin. Ainoa ero, jonka itse löydän, on se, että tietosuojan kohteena on henkilötieto ja tiedonhallinnassa laajasti koko liiketoimintatieto. Siksi voidaan sanoa, että tiedonhallinnan roolin on oltava vahva myös tietosuoja-asetuksen tulkinnassa.

Perustellusti voidaan siis sanoa, että hyvä tiedonhallinta on tietosuojan ja muidenkin regulaatioiden onnistumisen edellytys. Näin varmistetaan myös, että asiakkaiden ja muidenkin rekisteröityjen saama asiakaskokemus saadaan onnistumaan ja he voivat luottaa omien tietojensa osalta suojattuun toimintamalliin. He voivat siis astella luottavaisesti digitalisaation suojateitä pitkin.

Kimmo Rousku
Kimmo on toiminut sivutoimisena tietokirjailijana ja luennoitsijana vuodesta 1985 alkaen. Päätoimenaan hän kehittää digitaalista turvallisuutta julkiseen hallintoon VAHTI-pääsihteerinä valtiovarainministeriössä. Yllä mainitut mielipiteet eivät edusta hänen työnantajansa kantaa, vaan ne ovat hänen henkilökohtaisia mielipiteitään. Palaute: kimmo[at]ict-tuki.fi

Miksi tulevaisuus pelottaa minua?

Kummasta pidät enemmän: historiasta vai tulevaisuudesta? Vai oletko nykytilanteeseen keskittyvä realisti? Vanha viisaus on, että pitää tuntea historiaa ymmärtääkseen nykyaikaa ja osatakseen ennustaa tulevaisuutta. Mutta päteekö se alati kehittyvän ICT-teknologian tarjoamien palveluiden ja turvallisuuden osalta? Mielestäni ei.

Historia voi vääristää ja luoda mielikuvia

Mielestäni vaarana on, että ICT-teknologian historiallisiin ratkaisuihin tukeutuminen luo liian samankaltaisia ratkaisuja ja palveluita, joilla ”ICT-esi-isämme” ratkoivat oman aikansa ongelmia, joilla ei kuitenkaan ole enää suurta merkitystä. Pitäisikin ennemmin katsoa tulevaisuuteen avoimin mielin vapaasti laatikon ulkopuolelle innovoiden, jotta pystyisimme luomaan niitä kuuluisia killer-appeja. On siis tartuttava hetkeen ja tilaisuuteen. Ja tämä koskee ennen kaikkea kaikkia turvallisuutta edistäviä innovaatioita.

Tulevaisuus pelottaa!

Seison yleensä kahdella jalalla - toinen uppoaa teknologiasuohon ja toinen turvallisuusmaailman hetteikköön. Katsoessani ympärillä vallitsevaa teknologiaa, jota voi kutsua myös kybertoimintaympäristöksi, ja arvioidessani sen uhkia, voin hyvin helposti todeta, että tällä kehityksellä olemme alle kymmenessä vuodessa todella *suurissa* ongelmissa. Miten niin? Saamme nykyisin yhä useammin lukea merkittävistä tieto- tai kyberturvallisuutta koskevista poikkeamista, jotka ovat aiheuttaneet merkittävää vahinkoa organisaatioille ja niiden asiakkaille joko taloudellisesti tai muussa mielessä, esimerkiksi maineen tai luottamuksen menettämisenä, pahimmillaan ihmishenkien menetyksenä. Vuonna 2016 tietomurtojen määrä kasvoi 40%, ja vuosi 2017 näyttää yhä synkemmältä (linkki 1). Entäpä jos tämä kehitys jatkuu kiihtyvänä?

Kybermyrskyt tulevat yltämään myös Muumilaaksoon

Edelliset esimerkit ovat lähes kaikki Yhdysvalloista tai siellä toimivista yrityksistä. Mutta myös Suomessa on koettu ongelmia, ennen kaikkea lunnashaittaohjelmien (ransomware) sekä osin palvelunestohyökkäysten muodossa. Jos joku vielä kuvittelee, että meille Muumilaaksoon eivät kybermaailman myrskyt yllä, tämä harhaluulo kannattaa nopeasti karistaa harteilta.

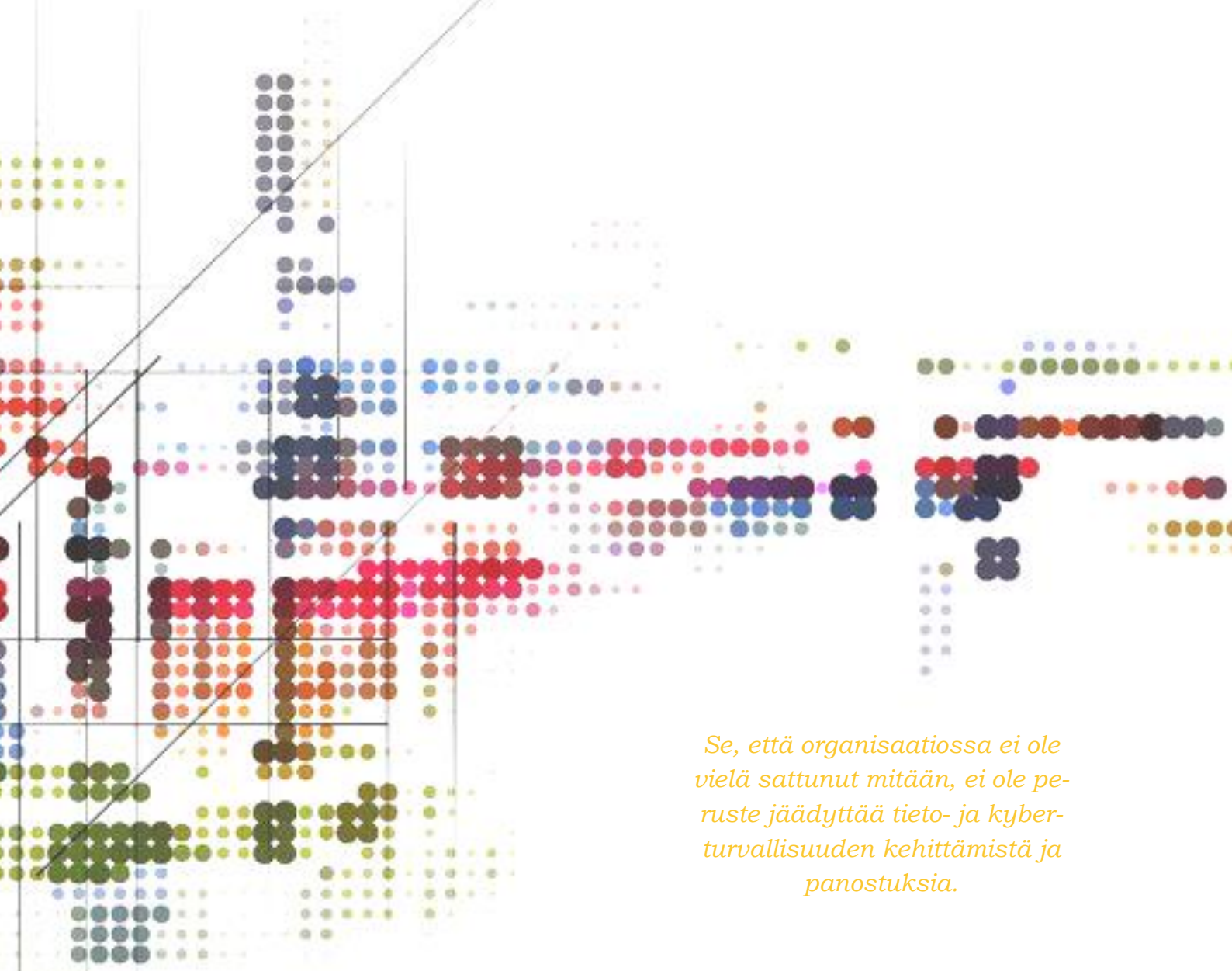
Suomi pärjää globaalisti hienosti tieto- (linkki 2) ja kyberturvallisuuden (linkki 3) erilaisissa mittareissa. Valitettavasti tämä saattaa luoda illuusion siitä, että meillä menee hyvin, koska eihän meillä tapahdu – julkisuuteen päätyviä - tietomurtoja.

Presidentti Trumpin toteamus Suomen erinomaisuudesta (linkki 4) kyberturvallisuudessa kannattaa ottaa kohteliaisuutena. Olemme kärkijoukoissa, mutta emme ole edelläkävijöitä.

Jokaisen organisaation tulee tunnistaa oman toiminnan osalta digitaalisen liiketoiminnan kriittisyys ja sen mukaisesti priorisoida tämän kokonaisuuden turvallisuuteen liittyviä panostuksia. Se, että organisaatiossa ei ole vielä sattunut mitään, ei ole peruste jäädyttää tieto- ja kyberturvallisuuden kehittämistä ja panostuksia. Koska rikolliset keksivät koko ajan yhä edistyksellisempiä keinoja, organisaatiosi pitää myös jatkaa näiden asioiden kehittämistä.

Tietoverkko- ja kyberrikollisuus –tuotteistettu palvelukokonaisuus

Tietoverkko- ja kyberrikollisten me-



Se, että organisaatiossa ei ole vielä sattunut mitään, ei ole peruste jäädyttää tieto- ja kyberturvallisuuden kehittämistä ja panostuksia.

nestys pohjautuu mahdollisuuteen hyödyntää ja kohdistaa toiminta perinteisestä kivijalkarikollisuudesta eli analogiajan ja manuaalisesta rikollisuudesta digitalisoiduksi, automatisoiduksi hyvin johdetun liiketoiminnan kaltaiseksi toiminnaksi. Rikolliset ovat erittäin tehokkaasti toteuttaneet omat alamaailmansa palvelut.

Jos me olemme ulkoistaneet palvelumme SaaS- ja pilvipalveluiden avulla, rikolliset ovat tehneet saman esimerkiksi CaaS – crime as a service palveluilla. Tietoverkkorikollisuus on tehty hyvin helppokäyttöiseksi, jolloin näiden palveluiden käyttäjälle saattaa jopa tulla tunne, että eihän tässä ole mistään rikollisesta kyse.

Tarvitsemme turvallisuuden digitalisaatiota

Onko tämä nyt sitä kuuluisaa turvallisuudella pelottelua? Kyllä, pitää paikkansa, mutta ennen kaikkea turvallisuuden kehittäminen tulee nähdä digitaalisten palveluiden mahdollistajana. Jos emme kykenisi esimerkiksi rajaamaan käyttöoikeuksia, salaamaan tietoliikennettä, keräämään lokeja, tunnistamaan käyttäjiä, huolehtimaan tietoturvapäivityksistä, kahdentamaan tai muuten parantamaan kriittisten palveluiden korkeakäyttöisyyttä – joutuisimme palaamaan MTK:n aikakaudelle – siis manuaaliseen tietojenkäsittelyyn.

Se, mihin meidän täytyy seuraavaksi kyetä, on näiden (tieto) turvatoimintojen digitalisaatio. On haettava uusia, osin disruptiivisia keinoja uusia toiminnan turvaksi laadittuja kontrolleja ja muita teknisiä ratkaisuja. Tässä automatisaatiolla, ohjelmistorobotiikalla ja keinoälyllä tulee olemaan valtava merkitys, ja tässä, jos missä, on suomalaisella ohjelmistoteollisuudella ehdottomasti näytön paikka. Kun tähän yhdistetään esimerkiksi IoT-laitteiden ja verkkojen turvaamisessa piilevät miljardit eurot, mahdollisuuksia on sekä kehittää omaa turvallisuutta että luoda uusia palveluita.

Milloin meille tulevat oikeat turvarobotit? On totta, että kaupassa päivystävät ja kiertelevät söpöt lampaalta näyttävät turvarobotit eivät kuulosta katu-uskottavalta (vrt. Schäfer), mutta tuon pörröisen robotin sisällä voi piillä kaiken näkevä, haistava ja tunnistava keinoäly, jota rikolliset eivät huijaa ☺.

Linkit

1. www.identityforce.com/blog/2017-data-breaches
2. www.microsoft.com/en-us/security/Intelligence-report
3. www.itu.int/pub/D-STR-GCI.01-2017
4. www.tivi.fi/Kaikki_uutiset/trump-ylisti-suomen-kyberturvaosaamista-pitaisiko-innostua-ikavia-uutisia-suomi-ei-ole-maailmanlaajuinen-edellakavija-6673178

Petteri Järvinen
Petteri on seurannut IT-tekniikkaa 1980-luvun alusta lähtien. Hän on kouluttanut yrityksiä tietoturva-aiheista ja kirjoittanut 30 IT-kirjaa.

Tietosuoja edellyttää tietoturvaa

Käsitteet tietoturva ja tietosuoja menevät arkikielessä helposti sekaisin, eivätkä IT-ammattilaisetkaan aina tee eroa niiden välillä. Jatkossa termit kietoutuvat toisiinsa entistä vahvemmin.

Tietoturvalla pyritään varmistamaan tietojen saatavuus, eheys ja luottamuksellisuus. Tiedot voivat olla mitä tahansa dataa: mittaustuloksia, autojen rekisterinumeroita, rahansiirtoja tai vaikka kaupan kuukausiraporttia varten kerättyjä myyntilukuja.

Henkilötiedoksi data muuttuu, jos se voidaan yhdistää luonnolliseen henkilöön. Tiedot ihmisen liikkumisesta, rahankäytöstä tai terveydestä ovat ilmiselvästi henkilötietoja. Tietosuoja pyrkii varmistamaan, ettei tietoja käytetä ilman aihetta eikä henkilön oikeutta yksityisyyteen loukata.

Jotta asia ei olisi liian yksinkertainen, GDPR (General Data Protection Regulation) laskee henkilötiedoiksi kaikki ne merkinnät, jotka voidaan epäsuorasti yhdistää henkilöihin. Tällöin esimerkiksi yrityksen sisäverkon lokitiedot tulevat lain velvoitteiden piiriin.

Vahinkoja ei enää ole

Toukokuussa 2018 päättyvän siirtymäkauden jälkeen vanha henkilötietolaki korvautuu uudella, aiempaa tiukemmalla versiolla. Periaatteet ovat ennallaan, joten hyvää rekisterinpitotapaa noudattanut yritys selviää muutoksista vähemmällä kuin se, joka on tähän asti elänyt harmaalla alueella tai jättänyt lain tyystin noudattamatta.

Yksi keskeisimmistä muutoksista on se, että uuden lain myötä yrityksellä on lainmukainen velvollisuus suunnitella ja dokumentoida henkilötietojen käyttöön liittyvät järjestelmät ja prosessit, sekä kouluttaa työntekijät. Mahdollisen tarkastuksen tullessa yrityksen on pystyttävä itse osoittamaan, että henkilötietojen käsittely on huolellista ja tietoturvasta on huolehdittu.

Suomessakin on ollut tapauksia, joissa verkkopalveluihin on murtauduttu ja sen jälkeen käyttäjien tietoja levitetty nettiin. Yleensä kyse on ollut salasanoista ja käyttäjätunnuksista, mutta joissain tapauksissa mukana on ollut myös osoitteita ja jopa henkilötunnuksia. Näitä tietoja on käytetty vielä vuosia myöhemmin identiteettivarkauksiin ja tilauspetoksiin.

Jatkossa yritys ei voi enää vedota siihen, että sattui vahinko. Onnistunut tietomurto on merkki siitä, ettei asioista ole huolehdittu lain edellyttämällä tavalla. Siitä voi seurata yritykselle taloudellisia sanktioita tai rekisterinpitäjä voi joutua asiasta henkilökohtaiseen rikosvastuuseen.

”Hupsista” ei jatkossa ole mikään selitys tapahtuneelle.

Lisäksi uusi laki tuo mukanaan ilmoitusvelvollisuuden. Yrityksen on tiedotettava tapahtuneesta tietosuojaviranomaisille sekä henkilöille, joiden tietoja on vuotanut. Ilmoitus on tehtävä viipymättä, eikä yritys voi enää piilotella asiaa.

Jatkossa yritys ei voi enää vedota siihen, että sattui vahinko.

Tällainen läpinäkyvyys parantaa asiakkaiden luottamusta sähköisiin palveluihin, mutta yrityksille se ei jätä vaihtoehtoja: tietoturva on pantava aidosti kuntoon.

Tietoturva ei koske yksinomaan henkilötietojärjestelmiä vaan kaikkea muutakin koneellista tiedonkäsittelyä. Sähköpostin liitteestä verkkoon livahtava haittaohjelma voi varastaa henkilötietoja tai kiristysohjelman tapauksessa estää niiden käytön.

Päivittämätön sovellus tai verkkopalvelin voi avata hakkerille pääsyn tietokantoihin tai mahdollistaa websivujen sotkemisen. Henkilökunnan uteliaisuudesta johtuva rekisteritietojen selaus on sekin tietoturvaongelma, koska se paljastaa luottamuksellista tietoa. Ongelmat voidaan välttää koulutuksella sekä riittävällä lokitietojen seurannalla.

Tietoturva ei ole rakettitiedettä

Media uutisoi kehittyneistä ATP-hyökkäyksistä (ATP=Advanced Persistent Threat), valtiollisista vakoiluohjelmista ja kehittyneistä hakkeriiskuista. Niitä vastaan on vaikea suojautua. Sen sijaan jokaisen organisaation on hoidettava helpot asiat kuntoon. Tietoturva ei ole rakettitiedettä eikä edes tekniikkaa. Pikemminkin kyse on toimintojen ohjeistamisesta, prosessien suunnittelusta ja käyttäjien motivoinnista.

GDPR aiheuttaa tarpeen inventoida ja tarkistaa kaikki yrityksen tietojärjestelmät.

Jos tietoturva nähdään vain työnantajan asiana, tietoturvaohjeita ei jakseta noudattaa. Ne nähdään vain hidasteina, jotka estävät tehokasta työntekoa, etätyötä ja tietojen siirtämistä organisaatioiden välillä.

Onneksi meillä jokaisella on lukuisia älylaitteita ja olemme riippuvaisia lukemattomista verkkopalveluista. Tietoturvan toteuttaminen ei ole yksin työnantajan etu vaan myös jokaisen henkilökohtainen asia.

Uhkakuvat muuttuvat ajan myötä ja kokemus on osoittanut, että tutuistakin asioista pitää muistuttaa työntekijöitä säännöllisesti. Siksi esimerkkien avulla tapahtuva koulutus ja myönteisen kehityksen palkitseminen ovat parhaita keinoja tietoturvan kohentamiseen.

Mitä sitten jokaisen pitää osata? Esimerkiksi salasanat. Tärkeintä on, että salasanat ovat riittävän vahvoja ja jokaiseen palveluun käytetään eri salasanaa. Vanha ohje salasanan säännöllisestä proaktiivisesta vaihtamisesta on nykymaailmassa turha. Salasanojen turha vaihtaminen tuottaa enemmän haittaa kuin hyötyä.

Mobiililaitteet ovat mainettaan turvallisempia. En ole löytänyt Suomesta vielä yhtään aitoa älypuhelimeen tarttunutta virusta. Turhia varoituksia ja pelottelevaa mainontaa on nähty sitäkin enemmän. Mutta mobiililaitteissa on omat riskinsä, kuten laitteen varastaminen tai olan yli tapahtuva pin-koodin urkinta.

USB-tekniikka on melkoinen murheenkryyni. USB-tikuilla voidaan ujuttaa järjestelmiin kehittyneitä haittaohjelmia, jotka pystyvät ylittämään jopa ns. air-gapin eli varastamaan tietoa koneista, joita ei ole kytketty verkkoon. Varovaisuus kaikkien USB-laitteiden käytössä on oleellisen tärkeää.

Tunnuksia verkkopankkiin ja sisäverkon palveluihin kalastellaan säännöllisesti. Mitään linkkiä ei saa klikata suoraan sähköpostista, vaan palveluihin pitää mennä aina selaimen kirjanmerkkien kautta tai kirjoittamalla osoite näppäimistöltä omin käsin.

Tietoturvaan liittyy myös tiedon elinkaaren hallinta. Säilyvyyden varmistamiseksi tiedoista pitäisi aina olla ajantasainen kopio pilvipalvelussa tai USB-tikulla, jotta levyn rikkoutuminen tai kiristyshaittaohjelma ei pääsisi tuhoamaan niitä.

Uuden lain nojalla henkilöllä on oikeus tulla unohdetuksi ts. oikeus vaatia tietojensa poistamista järjestelmästä. Tällöin poiston on oltava riittävän turvallinen, jottei tietoja jää vahingossa roikkumaan järjestelmän muihin osiin, eikä niitä palauteta vahingossa.

GDPR aiheuttaa tarpeen inventoida ja tarkistaa kaikki yrityksen tietojärjestelmät. Samalla on hyvä tarkistaa niihin liittyvät tietoturvatekijät. Jos tietoturva ei ole kunnossa, tietosuojakaan ei voi toteutua.

Ja se voi pahimmillaan tuottaa paitsi ison mainevahingon myös johtaa rikostutkintaan.

Testaus säädellyillä aloilla

On paljon teollisuuden aloja, joita säätelee liiketoiminnan sääntöjen lisäksi jokin viranomaisen säädös tai alan oma standardi. Näillä aloilla täytyy tehdä kaiken muun testauksen lisäksi yleensä pakollisia testejä. Parhaimmillaan testaaja pystyy yhdistelemään itselleen optimaalisen testaustavan ja tuottamaan samalla säädösten sanelemat testaustulosdokumentit. Aina näin ei kuitenkaan ole, vaan joskus täytyy tehdä testejä periaatteessa moninkertaisesti. Tälläkin on kuitenkin tarkoituksensa, sillä moninkertainen testaus on yksi turvallisuuskriittisten alojen redundanssin luomisen keinoista – tehdään kriittiseen asiaan kaksi järjestelmää / toimintatapaa ja saadaan sitä kautta lisävarmuutta turvalliseen toimintaan.

Kyseessä on virallisesti termi nimeltä Yhdenmukaisuuden testaus [FiSTB][1], englanniksi Compliance testing, mutta joskus kuulee myös Finglish-termiä regulaatioiden testaus. Mitä sitten on yhdenmukaisuus eli Compliance [ISTQB][2]?

Yhdenmukaisuudella tarkoitetaan siis säädösten tms. mukaisuutta. Yleisin sovellutus yhdenmukaisuuden testauksesta on yksi hyväksymistestauksen muodoista eli ”Sopimuksiin ja sääntöihin perustuva hyväksymistestaus” [FiSTB]. Kuten asian positiointikin jo ilmaisee, niin ajatellaan, että ohjelmistokehitysprojekti tekee hyvän järjestelmän ja testaa sen hyvin ja sitten lopuksi hyväksymistestauksen aikana tarkistetaan, ovatko yhdenmukaisuuskriteerit täyttyneet.

Yhdenmukaisuus on käytännössä aina joidenkin dokumenttiin kirjattujen vaatimusten todentamista, eli sillä ei vielä taata toimiiko järjestelmä todella kaikissa tilanteissa. Vaikka tällainen testaus on pitkälle todentamista (verification), kutsuvat standardit usein näitä pakollisia testejä kuitenkin kelpuutukseksi (validation). On toki semantiikkaa, mikä on oikeasti kelpuutusta, ja mukana on lisäksi paljon hyväntahtoista ajattelua, että kaiken kelpuutuksen saisi kirjattua paperille. Kuitenkin säädöksen tai standardin vaatimuksiin, tai joskus niistä johdettuihin standardisettiin testejä, on pyritty kuvaamaan olennaisimmat asiat, jotka pitää toimia. Käymällä nämä läpi saadaan hyvä perusvarmuus, että järjestelmä toimii vaatimusten mukaisella tavalla. Hyvänä esimerkkinä tällaisesta ovat tietoliikennealan standardit, jotka velvoittavat verkkovalmistajia ajamaan läpi vakiosetin TTCN-testejä [ETSI][3]

Näiden pakollisten testien lisäksi pitää tehdä normaalien hyvien testitapaussuunnittelutekniikoiden avulla hyvää kattavaa testausta. Joidenkin alojen standardit ohjaavatkin tähän suuntaan ja itse asiassa velvoittavat käyttämään tiettyjä testitapaussuunnittelutekniikoita, jotta saavutetaan hyviä kattavuuksia. Esim. ISO-61508 standardi määrittää Safety Integrity Leveleille (SIL:eille) eri tasoisia koodikattavuustekniikan käyttövaatimuksia. Kriittisimmälle tasolle (4) jopa vakavasti suositellaan moniehtokattavuutta (MC/DC Condition coverage) [Bullseye][4] Tuo standardi on yleisesti elektroniikka-alan käytössä. Ilmailualan DO-178B standardi käyttää vastaavaa luokitusta.

Mielenkiintoinen esimerkki on terveydenhuoltoalan laitteiden tarve täyttää amerikkalaisen FDA:n vaatimukset [FDA][5]. Nuo vaatimukset kohdistuvat kaikkiin testausvaiheisiin (sekä kehittäjä että testaaja), mutta myös kaikkiin ohjelmistokehityksen vaiheisiin. Tämä standardi on yksi parhaita esimerkkejä tarpeesta tuottaa tietynlaisia raportteja (esim. Loppuraportti) ja tehdä testausta tietyssä järjestyksessä (esim. sekä kehittäjän että testaajan toimesta). Monet terveydenhuollon alan toimijat ovat näistä testauksen rakenteellisista vaatimuksista huolimatta menestyksekkäästi siirtyneet ketteriin toimintatapoihin, mutta läpäistäkseen FDA:n vaatimukset heidän täytyy lisäksi tuottaa määrämuotoinen dokumentaatio suunnitelluista testeistä, testien tuloksista ja vikaraporteista jäljitettävyyksineen. Käyttämällä sopivia testauksenhallinnan työkaluja tämä onnistuu.

Uusimpia viimeaikaisia esimerkkejä jonkin säädöksen mukaisuudesta on paljon tietojärjestelmien kehittäjiä ja tilaajia puhututtanut uusi eurooppalainen tietosuojalainsäädäntö[EUGDPR][6]. Olemmeko GDPR:n mukaisia? Pitkälti tämä liittyy tietojärjestelmien pitämien rekisterien kykyyn hallita itseään. Koska GDPR esittelee joukon oikeuksia yksilölle[7].

- saada tieto omien tietojen vuodosta
- saada pääsy omiin tietoihin
- saada tiedot pois rekisteristä
- saada tiedot mukaansa
- rajoittaa tietojen antaminen vain niille, jotka niitä tarvitsevat
- saada vastuuhenkilö tietojen säilöntään.

GDPR toteutuu, jos tietojärjestelmä pystyy hoitamaan näitä asioita. Usein GDPR-implementaatio tarkoittaakin jonkin aineistonhallintaohjelmiston käyttöönottoa. Testaus taas lähtee liikkeelle näiden mainittujen skenaarioiden testauksesta, tarkastelleen koko ajan, mitä tapahtuu tietokannassa, kun jokin operaatio on tehty. GDPR on myös hyvä esimerkki säädöksestä, jossa hyvin suuri osa säädösten mukaisuuden työtä on tietojärjestelmän määrittelyä ja ohjelmointia, ei niinkään testausta. Näin tietysti tavallaan on tilanne kaikkien säädösten kohdalla, mutta monet säädökset jättävät vapauksia siihen, millä lailla tietojärjestelmä on toteutettu, kunhan sitten lopuksi voidaan testauksella todentaa, että ollaan säädösten mukaisia. GDPR taas ei toteudu testausta päälle liimaamalla, vaan tietojärjestelmään pitää esim. rakentaa kyky paikallistaa mikä tahansa tieto teratavuista käyttäjädataa ja sitten kyky poistaa tuo tieto kokonaan. Muuten vaatimus saada käyttäjän tiedot pois rekisteristä ei toteudu.

Summa summarum, eri aloilla on erilaisia säädöksiä ja niiden mukaisuutta voi ja täytyy sekä testata että toteuttaa jo määrittelyssä ja toteutuksessa. Paras yhtälö on, kun testauksen kattavuus ja säädösten vaatimukset saadaan yhdistettyä samaan tehokkaaseen testaajan ajankäyttöön.

Lähteet

1. http://www.fistb.fi/sites/fistb/files/liitteet/istqb_sanasto_2015-04-30%202.3%20ENG-FI.pdf
2. http://glossary.istqb.org/search/compliance
3. http://www.ttcn-3.org/index.php/downloads/standards/conformance-test-suites
4. http://www.bullseye.com/minimum.html
5. https://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm085281.htm
6. http://www.eugdpr.org/
7. http://www.eugdpr.org/key-changes.html

Kari Kakkonen
Kari on tuotantotalouden DI Aalto-yliopistosta. Hän työskentelee Knowitilla Suomessa Lead Consultant ja Director, Quality and Competences -rooleissa. Kari on International Software Testing Qualifications Board (ISTQB):n johtoryhmän varainhoitaja ja Finnish Software Testing Board (FiSTB):n puheenjohtaja. Hän on TestausOSYn ohjausryhmässä. Kari on valittu 100 tietotekniikkavaikuttajan joukkoon ja hän on yksi Agile Testing Foundations -kirjan kirjoittajista.

Laki tulee - mitäs nyt?

Tässä lehdessä käsitellään montaa ajankohtaista ja jo voimaankin tullutta uutta lakia. Jotkin lait vaikuttavat merkittävästi yrityksiin ja vaativat niiltä mittaviakin tietojärjestelmäinvestointeja. Osa organisaatioista on tottuneempi ottamaan huomioon lakien muuttumista kuin toiset. Tässä artikkelissa esitän yhden mallin siitä, miten yritys voi aloittaa lain vaikutusten analysoinnin. Tätä vaikutusanalyysiä on hyvä käyttää lakihankkeen projektisuunnitelman pohjana ja vaatimusanalyysin lähtökohtana.

Laki ei tule yhtäkkiä. Sitä valmistellaan pitkään ja sen vaikutuksista yrityksille keskustellaan lehdistössä, niin asia-artikkeleissa kuin yleisönosastollakin. Kun huomataan, että nyt olisi tulossa itseä koskeva laki, pitää nimetä lain seurantaan ja valmisteluun oma vastuuhenkilö. Hänen tehtävänään on selvittää lain ennustetut aikataulut ja tulevan lain vaikutusten laajuus yrityksen näkökulmasta. Mitä lähempänä lain voimaantulo on, sitä enemmän asiassa on työtä.

Eduskunnan sivuilta löytyy lista kaikista valmistelussa olevista laeista. Eduskunnan sivut kertovat varsin seikkaperäisesti lain valmistelusta. Sivuilta löytyy myös linkki Finlex -sivustolle, jossa on listattuna kaikki tekeillä olevat lakiasiat. Kukin valmistelussa oleva laki esitellään perusteluineen. Näiden lukemisesta on hyvä aloittaa.

Lakiteksti kannattaa kopioida ja tallettaa joko dokumenttiin firman Sharepointtiin, tai vaikka Confluenceen. Joka tapauksessa sellaisessa muodossa ja sellaiseen paikkaan, että kaikki pääsevät lukemaan sitä ja että siihen on helppo palata ja viitata jatkossa. Lisäksi lakiteksti todennäköisesti muuttuu valmistelun edetessä ja nämä muutokset pitää ottaa huomioon ja päivittää tallennettua tekstiä muutosten mukana. Myös valmistelu ja lain perustelut kannattaa ottaa talteen.

Seuraava vaihe onkin lakiin tutustuminen ja sen vaikutusten arviointi. Ensimmäiseksi on syytä lukea lain perustelut ja itse lakiteksti kerran läpi, jotta kokonaisuus hahmottuu. Seuraavaksi on hyödyllistä lukea laki luku luvulta, pykälä pykälältä, momentti momentilta ja kohta kohdalta samalla dokumentoiden asian herättämät ajatukset.

Lain kommentointi on kätevää tehdä tätä varten luotuun taulukkoon. Siinä on sarakkeina lain kohta, eli viittaus itse asiaan, mahdollisesti lakiteksti, joka on herättänyt ajatuksen tai kysymyksen, itse ajatus / kysymys, mihin tietojärjestelmään tai toimintoon asia vaikutta, kuka asiasta tietää, asian prioriteetti ja muut mahdolliset huomiot. Taulukkoon voi lisätä sarakkeita sitä mukaa, kun tarpeita tulee lisää. Taulukko pitää tallettaa sellaiseen paikkaan, että kaikki pääsevät sitä kommentoimaan ja lisäämään huomioita. Näitä ei pidä lähetellä sähköpostissa, vaan sähköpostiin laitetaan linkki, joka osoittaa talletuspaikkaan. Sähköpostissa käsittely aiheuttaa vaikeasti hallittavan versio-ongelman.

Lakia lukiessa kunkin pykälän kohdalla pitää miettiä, mitä tämä asia vaikuttaa omaan toimintaan. Jos juuri kyseinen kohta ei vaikuta, sen voi ohittaa. Esimerkiksi määrittelyosassa on kerrottu, keitä laki koskee ja tästä luvusta vain itseä koskevat kohdat huomioidaan. Muut kannattaa suosiolla jättää huomioimatta, sillä itseäkin koskevia huomioita tulee helposti kymmeniä, jopa satoja. Lakiteksti on monipolvista ja tarkkaa. Niinpä samassa pykälässä voi olla useita eri asioita. Eri momenteilla mainitaan erilaisia vaikutuksia ja niissä voi olla listauksia. Siksi huomiot kannattaa kirjata momenteittain ja jopa yksi kohta kerrallaan.

Alkuvaiheessa on hyvä kirjata vain yksi huomio yhdelle taulukon riville. Voi vaikuttaa siltä, että rivejä tulee tällä lailla erittäin paljon. Kuitenkin jokainen huomio on syytä käsitellä erikseen. Lisäksi laissa käsitellään samaa asiaa eri kohdissa, esittelyosassa, asialuvussa ja sanktioissa. Kukin huomion kirjoittaminen omalle rivilleen mahdollistaa asioiden yhdistelemisen myöhemmin.

Etukäteen kerätyt lakitekstiin ja valmisteluun perustuvat huomiot mahdollistavat tehokkaan analyysityön. Analyysiin pitää kiinnittää

Mitro Kivinen
Mitro on kokenut systeemityön johtaja.

monenlaisia henkilöitä omasta organisaatiosta. Hyviä ehdokkaita ovat kokonaisarkkitehti, kehitys- ja järjestelmäpäälliköt, tietohallinnon asiantuntijat, liiketoiminnan asiantuntijat, tietysti organisaation omat lakimiehet ja yksiköiden johtajat. Samalla kun näiltä kaikilta kysytään kommentteja, heitä sitoutetaan tulevaan lain vaatimaan muutokseen. Laki muuttaa todennäköisesti sekä toimintaa, että tietojärjestelmiä ja muutos vaatii toteutuakseen koulutusta ja viestintää. Tämähän on ihan tavallista systeemityötä!

Kultakin sidosryhmää pitää ohjeistaa niin, että miettivät kunkin itseään koskevan huomion kohdalla seuraavia kysymyksiä:

- *Kuinka tämä lain kohta toteutuu tällä hetkellä?*
- *Mikä muuttuu?*
- *Kuinka muutos pitäisi toteuttaa?*
- *Kenen kanssa muutoksesta pitää keskustella?*
- *Mihin kaikkialle organisaatiossa muutos vaikuttaa?*
- *Kuinka iso työ muutoksessa on?*

Kun analysoidaan sitä mihin kaikkialle muutos vaikuttaa, pitää ottaa huomioon prosessit, ohjeet, käytännöt, tietojärjestelmät, kerättävä data ja organisaation yleinen kyvykkyys.

Sanktiopykäliin pitää kiinnittää erityistä huomiota. Mahdolliset lain noudattamatta jättämisestä koituvat sanktiot asettavat hintalapun projektin vaihtoehtoiskustannukselle. Toisin sanoen, minkä suuruisen riskin organisaatio ottaa, jos se ei täytä tulevan lain vaatimuksia, eli ei ole niin sanotusti compliant. Tässä kohdassa pitää miettiä myös, millä tavalla organisaatio todistaa noudattavansa lakia. Näitä todistamisen asioita ovat erilaiset lokit, audit trail -polut, raportit ja muut lain noudattamisesta todistavat artefaktit. Lakimiehiä tarvitaan ottamaan kantaa siihen, mikä on riittävä taso asioiden todistamiselle.

Lain vaatima muutos voi olla suurilta osin organisaation toimintaa koskeva, mutta siihen helposti liittyy tietojärjestelmien uudelleen sovittaminen tai jopa uusien tietojärjestelmien hankinta. Tarvittavan muutoksen analysointi tähtää siihen, että organisaatio tietää mitä sen pitää saavuttaa ollakseen valmis, kun uusi laki astuu voimaan. Analyysin pohjalta tehdään hanke- tai projektisuunnitelma, budjetti ja aikatauluarvio.

Käytännössä uusi lakiteksti syntyy lopullisessa muodossaan vasta juuri ennen voimaantuloa. Reagointiaika voi jäädä lyhyeksi. Siksi lain valmistelua, siitä käytävää julkista keskustelua sekä erilaisten valiokuntien työskentelyä pitää seurata aktiivisesti. Lain valmisteluvaiheessa kannattaa yrittää vaikuttaa lakitekstiin käytettävissä olevia kanavia pitkin. Lain valmistelijoilla itsellään on vain harvoin käytännön kokemusta siitä, millaisia muutoksia lain noudattamiseksi yrityksissä pitää tehdä. Toisaalta, lain valmistelijat ja säätäjät eivät ole systeemityön ammattilaisia. Ilman hyvää omaa valmistelua, ei lain säätämiseen voi vaikuttaa. Siksi hyvä pohja -analyysi on välttämätöntä jo aikaisesta vaiheesta lähtien.

Heidi Kakko
Kirjoittaja toimii BI-alueen palveluja tarjoavassa Aureolis Oy:ssa BI-konsulttina ja on ollut mukana erilaisissa finanssialan hankkeissa lähes kymmenen vuotta. Erityisesti erilaiset regulaatiohankkeet ovat tulleet hänelle vuosien mittaan tutuksi.

Regulaatiohankkeet työllistävät finanssilaitoksia

Regulaatiot eli sääntelyt työllistävät suurta joukkoa asiantuntijoita niin Suomessa kuin muuallakin maailmassa. Ne ovat olleet jo pitkään merkittävä osa erilaisten finanssilaitosten sovelluskehityksen työnkuvaa ja ovat sitä jatkossakin, koska sääntelyiden määrä ei ole vähenemässä.

Regulaatiohankkeita riittää

Euroopan unionin regulaatiohankkeet hallitsevat vahvasti finanssialaa, ja ne koskevat tavalla tai toisella jokaista olemassa olevaa finanssialan laitosta, niin pankkeja, vakuutusyhtiöitä kuin sijoituspalveluita tuottavia yrityksiäkin. Jokaisessa finanssialan yrityksessä ne hallitsevat suurta osaa vähintäänkin BI-sovelluskehi-tyksestä. Regulaatiohankkeet ovat viranomaisvaatimuksena pakollisia tehtäviä, joten niiden toteuttaminen ei ole harkinnanvaraista. Resurssit niiden tekemiseen on siis löydyttävä.

Otetaan esimerkkinä Solvenssi II ja Basel (I, II, III ja kohta myös IV). Solvenssi II -laskenta on henki-, vahinko- sekä jälleenvakuutustoiminnan vakavaraisuutta säätelevä hanke, jota ohjaavat EU-direktiivit Solvency II ja Omnibus II, joita on valmisteltu vuodesta 2009 lähtien. Alun perin Solvenssi II:n piti astua voimaan jo vuonna 2012, mutta kokonaisuudessaan se saatettiin voimaan vasta vuonna 2016.

Basel puolestaan on rahoituslaitosten vakavaraisuutta säätelevä hanke, jonka juuret johtavat jo vuoteen 1930. Tuolloin Belgian, Iso-Britannian, Italian, Ranskan ja Saksan keskuspankit sekä ryhmä joitakin yksityisiä pankkeja Japanista ja Yhdysvalloista perustivat Kansainvälisen järjestelypankin. Sen alkuperäinen tarkoitus oli varmistaa Saksan maksukyky ensimmäisen maailmansodan sotakorvausten maksujen takkuillessa. Järjestelypankin alaisuuteen perustettiin Baselin komitea vuonna 1974 reaktiona joukkoon pankkien tekemiä konkursseja. Vuodesta 1988 alkaen eri maissa toisistaan eronneet säännökset yhdenmukaistettiin ja kansainvälisesti toimivien pankkien oman pääoman suuruudelle asetettiin vähimmäisvaatimukset. Nämä säädökset tunnetaan nimellä Basel I, ja ne ovat koko vakavaraisuussääntelyn perusta. Basel II julkistettiin vuonna 2004, se astui voimaan vuonna 2007 ja on voimassa toistaiseksi. Siihen on kirjattu muun muassa pätevät oman pääoman vähimmäisvaatimukset. Sen perimmäinen idea on luottoriskin oikeassa mittaamisessa. Tällä hetkellä voimassa on myös Basel II:ta täydentävä Basel III, mutta uutta täydentävää Basel IV -sääntelyä ollaan jo kovaa vauhtia valmistelemassa. Baselia ohjaavat Euroopan unionin säätämä luottolaitosdirektiivi CRD IV sekä vakavaraisuusasetus CRR.

Näiden kahden suuren hankkeen lisäksi on vielä joukko muita enemmän ja vähemmän suuria hankkeita, kuten tietosuojauudistus, erilaiset sijoittamiseen liittyvät hankkeet (esimerkiksi MiFID ja MiFIR), vakuutusten tarjoamiseen liittyvä direktiivi (IDD), vakuutusmuotoiset sijoitustuotteet (PRIIPS), johdannaisten sääntely (EMIR), rahoitusinstrumentteihin liittyvä säädös (IFRS9) sekä monia, monia muita. Näistä esimerkiksi tietosuoja on tällä hetkellä keskustelun kohteena monessa henkilötietoja käsittelevässä yrityksessä, eikä vähiten juuri finanssialalla, jossa lähes kaikki käsiteltävä data koskee tavalla tai toisella henkilötietoja.

Basel puolestaan on rahoituslaitosten vakavaraisuutta säätelevä hanke, jonka juuret johtavat jo vuoteen 1930.

Jos on paljon erilaisia säädöksiä, direktiivejä sekä asetuksia, niin on paljon myös viranomaisia ja valvojia, jotka pitävät huolen siitä, että säädöksiä, direktiivejä ja asetuksia ja niiden mukanaan tuomia lakeja noudatetaan. Kansallisella tasolla Suomessa finanssialaa valvovat muun muassa Finanssivalvonta ja Suomen Pankki (Suomen keskuspankki). Myös muilla Euroopan mailla on omat finanssivalvojansa sekä keskuspankkinsa. Kansainvälisellä tasolla valvojia onkin sitten jo enemmän kuin kourallinen. Näitä ovat muun muassa Euroopan Keskuspankki, Euroopan järjestelmäriskikomitea (ESRB), Euroopan Komissio, Euroopan Parlamentti. Lisäksi jokaiselle osa-alueelle on oma valvojansa: Euroopan arvopaperimarkkinaviranomainen (ESMA), Euroopan pankkiviranomainen (EBA) sekä Euroopan vakuutus- ja lisäeläkeviranomainen (EIOPA). Ja puhumattakaan vielä sitten Amerikan finanssivalvonnasta, joka sekin ulottuu osittain Eurooppaan asti.

Töitä riittää

Tie direktiivistä, asetuksesta tai säädöksestä valmiiksi toteutukseksi on pitkä. Esimerkiksi Solvenssi II:n ja Baselin direktiivit, asetukset sekä erilaiset säädökset liitteineen ja tulkintoineen sisältävät tuhansia sivuja tekstiä ja taulukoita. Näiden tul-

Nykyaikainen riskilaskenta perustuu vahvaan tilastomatematiikkaan

kinta ei aina ole niin yksiselitteistä, ja työssä kaivataankin sekä vakuuttamisen ja pankkitoimialan ammattilaisten, lakimiesten että matemaatikkojen ja analyytikkojen osaamista. Laajat ja vuosia kestäneet hankkeet ovatkin työllistäneet niin liiketoiminnan määrittelijöitä kuin teknisiä toteuttajia jo vuosia ja työllistävät varmasti jatkossakin, siitä pitää huolen sääntelyyn tasaista tahtia julkaistavat muutokset sekä laajennukset. Merkittäviä kustannuksia aiheutuu laite- ja lisenssihankinnoista sekä järjestelmien kehittämisestä. Regulaatiohankkeet ovatkin erittäin resursseja sitovia, aikaa vieviä sekä suoraan sanoen kalliita – kustannukset näkyvät pakostakin myös kuluttajien kukkaroissa esimerkiksi erilaisina palvelumaksuina.

Regulaatiohankkeiden läpivienti on vaatinut ja vaatii edelleen parhaat tekijät niin liiketoimintamäärittelijöiden kuin järjestelmätoteuttajienkin osalta. Sekä Solvenssi II:ssa että Baselissa tehdään matemaattisesti erittäin vaativaa laskentaa sekä hyödynnetään tilastollisia menetelmiä, joten monenlaisia osaajia tarvitaan. Pitkän linjan järjestelmäasiantuntijoillekin löytyy yhä edelleen ratkottavaa sovellusarkkitehtuurista, ajojen optimoinnista ja lopputulosten mallintamisesta parhaiten hyödynnettävään muotoon. Melko usein hankkeista puhutaan raportointihankkeina, mikä on sikäli harhaanjohtavaa, että nykyaikainen finanssisektorin tilastomatematiikkaan ja malleihin perustuva riskilaskenta on hankkeiden ydin ja vie käytännössä valtaosan resursseista.

Säädöksiä varten rakennetut pakolliset järjestelmät eivät täytä pelkästään välittömiä viranomaisvaatimuksia, vaan ne tuottavat myös arvokasta tietoa finanssialan yritysten riskienhallinnan ja toiminnanohjauksen käyttöön. Esimerkiksi Baselia varten rakennetut järjestelmät tukevat toisaalta järkevää lainan myöntämisprosessia, toisaalta riskilaskentojen tuloksia voidaan hyödyntää myös esimerkiksi sijoitustoiminnan tukena.

Risut ja ruusut

Erilaiset säädökset tuovat tullessaan paljon hyvää ja vähän huonoakin. Tärkein tavoite on luonnollisestikin, että mahdollisesti edes yksi pankkikriisi jää kokematta. Ehdottoman hyvää on myös valvonnan mukanaan tuoma yhdenvertaisuus asiakkaiden välille. Kun sääntely vaatii, että lainan hakijat pisteytetään hyväksytyn prosessin ja laskentatavan mukaisesti, lainoja myönnetään valittujen parametrien pohjalta, siinä missä lainanantoprosessi saattoi aikaisemmin perustua aikaisemmin vähemmän rationaalisiin syihin.

Miinuspuolelle on laskettava se, että uudet säännökset tuovat myös paljon kustannuksia pankeille, vakuutusyhtiöille ja muille finanssialan yrityksille. Lisäksi ne sitovat henkilöresursseja, jotka voisivat tehdä muunkinlaista liiketoiminnan kehitystyötä, kuten uusien palveluiden kehittämistä.

Kuluttajan on kuitenkin hyvä huomioida se merkittävä seikka, että vaikka kustannusten kasvun myötä myös asiakasmaksut kasvavat, niin esimerkiksi aiemmin mainittu tietosuojauudistus työllistää muun muassa pankkeja ja vakuutusyhtiöitä pääosin yksittäisen kuluttajan edun vuoksi. Eli summa summarum ei niin huonoa, ettei jotakin hyvääkin.

Regulaatiohankkeiden läpivienti on vaatinut ja vaatii edelleen parhaat tekijät niin liiketoimintamäärittelijöiden kuin järjestelmätoteuttajienkin osalta.

Lineaarinen regulaattori

Lineaarisen jänniteregulaattorin toiminta perustuu säädettävään jännitehäviöön ennen piirin syöttöä (lähde: Wikipedia). Siinäpä se. Kuten lukija saattaa jo huomata, kolumnisti on taas sen ongelman edessä, että miltä kulmalta lähtisi tätä niin antoisaa aihetta pöyhimään.

Myöntää täytyy, että yhdessä välilehdessä on Samuli Edelmanin 'Karavaanari' –kappaleen sanat, jotenkin on jäänyt korvan perukoille soimaan tuo 'RegulaatiO, reguLAATIO, on kaikkien kaveri'. En kuitenkaan ryhtynyt sanoituksen soveltamiseen, koska joku ohjelmistotalon kerhobändi sen olisi kuitenkin ottanut repertuaariinsa, mennyt lataamaan sen spotifyhin ja mihin minä ne sanoituksesta tulleet rahat laittaisin? Pankkitilillä raha happanee ja osakkeet kohta romahtavat, olisin joutunut vielä tuhlaamaan ne.

Toisessa välilehdessä on – aiheeseen liittyen – tiedon haku avainsanoilla 'inkvisition hyödyt'. Mielenkiintoista muuten, että noilla sanoilla ei oikein mitään hyötyjä näytä löytyvän. Täytyyhän nyt siinäkin asiassa olla jotain hyödyllistä. Natsi-Saksallakin oli sentään ne autobahnit ja volkkari.

Regulaatiomaailmassa eläminen on kyllä toisaalta helppoa. Ei tarvitse miettiä, että miksi jotain asiaa pitää tehdä. Siinä on sellainen pieni lapsuusregression vivahdus. Se pitää tehdä, koska se on pakko. Ja sitten se siis tehdään. Prioriteettikin on aika selvillä ja ennen kaikkea aikataulu. Nyt on esimerkiksi monta päivämäärää, joiden jälkeen tiedetään tulevan maailmanloppu, vedenpaisumus ja lopuksi vielä heinäsirkat.

PSD2 räjäyttää pankit (pun intended) tulevan tammikuun 13 päivä, IFRS 9, PRIIPS, MiFID ja MiFIR puolitoista viikkoa aikaisemmin, GDPR sitten halvaannuttaa lopun tietoa käsittelevän maailman toukokuussa. Nuo ensinnä mainitut keskittyivät finanssimaailmaan, tokihan regulaatioita on niin energiateollisuudessa kuin maataloudessakin. GDPR eli tietosuoja-asetus koskee mukavasti vähän kaikkia aloja, kaikkia sellaisia, joissa käsitellään henkilötietoja.

Raskasta ja hankalaa asiaa, koska aika monella yrityksellä on asiakkaita, jopa yksityishenkilöitä ja heidän tietojaan on tietenkin tarpeellista säilyttää. Asetuksen voimaantulon hankaluutta voitaisiin kyllä helpohkosti lieventää: tietosuoja-asetus – ja muutkin pakolliset – pitäisi saattaa voimaan niin, että ne velvoittavat vain voimaantulosta eteenpäin tehtäviä asioita. Onhan se nyt nimittäin kumma, että voin ajaa 50-luvulla rakennetulla autolla ilman turvavöitä, koska auton rakennusvaiheessa turvavöitä ei oltu edes keksitty, mutta jos nyt jossain on olemassa joku kymmenen vuotta sitten tehty asiakasdatan tietokanta kirgistanialaisella palvelimella, niin siitähän nyt sitten kamala hässäkkä on saatava aikaan. Tosin täytyy myöntää, että en muista, että onko GDPR:ssä juuri nimenomaan mitään mainittu vanhoista kirgistanialaisista palvelimista.

Meille siis annetaan jostain epämääräiseltä korkealta taholta joskus hieman sekavia säännöstöjä noudatettaviksi ja näiden säännöstöjen noudattaminen aiheuttaa mittavasti muutoksia nykykäytäntöihin ja sitä kautta lisätöitä, joiden tekeminen on pois liiketoiminnan kehittämisestä. Jotkut ehkä parantavat maailmaa ja monet on jopa tarkoitettu suojelemaan meitä, ihan tavallisia pulliaisia. Tämä kannattaakin kaikkien niiden ruuansulatus kippuralla stressaavien regulaatiohankkeiden parissa työskentelevien muistaa, tämä on sinun omaksi parhaaksesi. Kiität vielä joskus, kun ymmärrät tämän aherruksen tarkoituksen. Ja taas regressiovärähdys kulki lävitseni.

Eräs miettimisen arvoinen aspekti tässä tietosuoja-asetuksessa on salaliittoteoria. Voisiko olla, että koska joka tapauksessa EU on temppeliherrojen masinoima suunnitelma vallan anastamiseksi, niin yhdessä vapaamuurareiden kanssa on nyt ajateltu saattaa henkilötiedot redundanssia välttäen kolmanteen normaalimuotoon, jotta kaikki olisi sitten helppo luovuttaa mystisissä uhrimenoissa vastateurastetun karitsanveren mukana paholaiselle. En itse olisi tästä kovin huolissani, luotan, että Illuminatin jäsenet pelastaisivat meidät tästä tilanteesta ja kaaoksen kautta syntyisi sitten se toivottu Uusi Maailmanjärjestys. Se sellainen, jossa on kehitetty regulaatio-ohjelmistorobotit, jotka tekevät viranomaislähtöiset muutokset koodiin ja antaisivat propellipäiden pelata WoT... siis suunnitella mahtavia yleishyödyllisiä sovelluksia, joilla poistetaan sodat ja nälänhätä maailmasta.

Joka tapauksessa, regulaatiohankkeiden työllistävää vaikutusta ei mitenkään voida kieltää. Olkaamme siis kiitollisia siitä. Hmm. Herra Hitlerhän rakennutti ne moottoritiet juuri sen takia, että saataisiin kansa kotinurkista nurisemasta töihin ahertamaan...

Sytyttääkö? - Liity jäseneksi

Systeemityöyhdistys Sytyke ry on Tieto- ja viestintätekniikan ammattilaiset TIVIA ry:n suurin valtakunnallinen teemayhdistys, joka jo vuodesta 1979 lähtien on kehittänyt tietojärjestelmäalan ammatillista osaamista. Sytyke yhdistää suomalaiset tietojärjestelmätyön ammattilaiset liiketoiminnasta teknisiin asiantuntijoihin. Käsittelemme alan ajankohtaisia teemoja, keskustelemme ja opimme yhdessä – hypetystä tervejärkisesti. Sytykkeen osaamisyhteisöissä samoista teemoista kiinnostuneet verkostoituvat asiantuntijatapahtumissa.

Lisätietoja: www.sytyke.org
Hallituksen sähköpostilista: info[at]sytyke.org

Jäseniksi voivat liittyä kaikki tietojärjestelmäalasta kiinnostuneet henkilöt ja organisaatiot. Systeemityöyhdistys Sytykkeen jäseneksi liitytään Tieto- ja viestintätekniikan ammattilaiset TIVIA ry:n verkkosivustolla valitsemalla jäsenyhdistykseksi Systeemityöyhdistys Sytyke. Liittymislomake osoitteessa: www.tivia.fi/liity
Henkilöjäsenmaksu vuonna 2017 ilman lehteä on 64€ vuodessa, nuorelle opiskelijalle 20€ vuodessa. Jos ennestään olet jo TIVIA ry:n jonkin toisen yhdistyksen jäsen, niin Sytykkeen lisäjäsenyys maksaa vain 15€ vuodessa.

Lisätietoja: www.tivia.fi, www.sytyke.org ja jasenasiat[at]tivia.fi

Hallitus 2017

Timo Piiparinen
puheenjohtaja
Jyväskylän kaupunki
puheenjohtaja[at]sytyke.org
timo.piiparinen[at]sytyke.org

Veli-Matti Heiskanen
varapuheenjohtaja
Nordicrobots
veli-matti.heiskanen[at]sytyke.org

Ville Availa
Ambientia
ville.availa[at]sytyke.org

Matias Miettinen
Tampereen AMK
matias.miettinen[at]sytyke.org

Minna Oksanen
Talent Base
minna.oksanen[at]sytyke.org

Janne Ollenberg
Samlink
janne.ollenberg[at]sytyke.org

Lea Pitkänen
KREAM Helsinki
lea.pitkanen[at]sytyke.org

Eija Mether
varajäsen
Telia Company
eija.mether[at]sytyke.org

Heikki Naski
varajäsen
Edita Publishing
heikki.naski[at]sytyke.org

Liittokokousedustajat 2017

Mitro Kivinen
mitro.kivinen[at]iki.fi

Lauri Laitinen
lauri.laitinen[at]nokia.com

Minna Oksanen
minna.oksanen[at]sytyke.org

Sytyke

Syysseminaari marraskuussa

- Blockchain
- Syyskokous

Seuraa ilmoittelua:
www.sytyke.org

Seuraavassa numerossa:
Laivaseminaarin satoa