### 

### F-Securen lausunto kansallisen big data-strategian luonnokseEN.

Big data luo merkittäviä mahdollisuuksia olemassa oleville liiketoiminoille ja synnyttää kilpailuetua, innovoi uusia palveluita, tehostaa liiketoimintaa ja auttaa tekemään parempia päätöksiä sekä luo pohjan täysin uudentyyppisille yrityksille. On hyvä, että alue on kansallisesti tunnistettu ja siihen panostetaan. Erityisesti big datan osaajista on kova kansainvälinen kysyntä ja Suomen on syytä varmistaa alueeseen liittyvä koulutus ja osaajien saatavauus.

F-Securella on merkittävä kansainvälinen rooli ihmisten tietoturvan ja yksilönsuojan turvaamisessa, joten luonnollisesti korostamme jatkosuunnittelussa yksilönsuoja-asioiden erityistä huomioimista teknisten ja liiketoimintamahdollisuuksien rinnalla.

Suomen perustuslain takaama yksityisyyden suoja ja lainsäädännölliset perusteet tekevät Suomesta sekä houkuttelevan paikan ulkomaisten globaalien palveluntarjoajien investoinneille, että luo vankan pohjan paikallisille palvelutarjoajille ja tietoturvayrityksille. Luonnoksessa on hyvin tunnistettu haasteellisia alueita, kuten yksilönsuojan mahdollinen heikentyminen useita tietolähteitä yhdistelemällä, mutta alue on syytä ottaa erityisen tarkastelun kohteeksi. Vaikka kerätystä datasta olisi pyritty poistamaan yksilöiviä tietoja tai siinä on käytetty pseudoanonyymejä tunnisteita, on selkeä riski, että tietoja yhdistämällä yksittäisen henkilön identiteetti tulee tunnistettavaksi.

Suomen maine tietoturvallisena, puolueettomana maana, jolla on vahva yksityisyyden suoja, on kansainvälinen kilpailuetu. Nykyinen toimintaympäristö mahdollistaa paikallisten yritysten erottautumisen kansainvälisistä kilpailijoistaan ja olisi hyvä, että sama kehitys jatkuisi ja henkilöihin kohdistuvan big datan hyödyntämisessä Suomi olisi myös yksilönsuojan osalta kärkimaa. Suomella on mahdollisuus toimia edelläkävijämaana, jossa on läpinäkyvyys sille mitä tietoa ihmisitä kerätään, kuka omistaa datan sekä taata yksilöille mahdollisuus vaikuttaa siihen, miten tietoa heistä kerätään ja miten sitä hyödynnetään. Tätä osaamista voimme hyödyntää kansainvälisesti.

Big datalla on myös kaksi puolta. Parempien palveluiden ja päätösten lisäksi, teknologia mahdollistaa myös henkilöiden massaseurannan. Avoin data soveltuu useille osa-alueille, mutta on syytä huomioida millainen pääsy ja tietoturva on sellaisilla tietosisällöillä, jota voi hyödyntää ihmisten massaseurantaan. Yhdysvalloissa on tällä hetkellä pohdinnassa, miten seurannalle saataisiin läpinäkyvyyttä ja luoda uudelleen uskoa yksilönsuojan ja yritysten liikesalaisuuksien turvaamiselle, kun Snowdenin paljastukset veivät uskottavuutta ja aiheuttivat menetyksiä paikallisille yrityksille.

Vaikka pyrkimyksenä olisi kerätä tietoa anonyymisti, niin EU:n yksilönsuojan perusteet suostumuksen saamiselle on hyvä huomioida ihmisiin liittyvän aineiston keräämisessä ja säilyttämisessä.

Tietojen valikoiva poistaminen on usein huomattavasti kalliimpaa, kuin tietojen jatkuva säilyttäminen, joten tiedonkeruuvaiheeseen on syytä kiinnittää huomioita.

Tarkempia alueita, jota strategiassa jatkotyöstössä olisi syytä huomioida:

* Mitä menettelytapoja tulisi luoda, että yksilöillä on näkyvyys siihen mitä tietoja heistä kerätään
* Tarjotaanko yksilöille (ja yrityksille) valinnanvapautta datan keräykseen osallistumisessa
* Millaiseen dataan on syytä säädellä pääsyä ja miten se voidaan toteuttaa
* Miten yksilöihin kohdistuvan tietolähteiden yhdistelyä pitäisi säädellä big-data analyysissä
* Miten yksilö voi vaikuttaa, jos väärän datan tai huonojen algoritmien takia päädytään vääriin johtopäätöksiin, esim. syrjinnän tai väärien hinnoitteluperusteiden korjaamiseksi
* Miten huolehditaan, että tietoa ei uudelleen jalosteta ja/tai myydä vääriin tarkoituksiin
* Jos henkilökohtaista informaatiota päätyy kantoihin, miten pitkään dataa säilytetään
* Määritellä toimintamallit tiedonkeräämiselle. Tietoa ei tulisi kerätä salassa, vaan toiminalle pitää olla näkyvyys ja hyväksyntä, eteenkin yksilöihin kohdistuvissa asioissa.
* Määritellä milloin yksilö ja milloin organisaatio omistaa datan

Luonnoksessa on tunnistettu myös Internet of Things (IoT) yhtenä merkittävänä alueena datan synnyttäjänä. Tässä yhteydessä mainitaan tarve laajakaistaisimmille verkoille ja yhteyksille. Vaikkakin alue on vain esimerkinomaisesti mainittu raportissa, niin tuomme kumminkin esille, että tarve saattaa olla enemmänkin energiatehokkaille radioverkoille, joiden hinnoittelumalli sopii kustannustehokkaasti pienten ja satunnaisten datamäärien siirtämiseen. Useissa IoT:n Big Datan sovelluskohteissa, isot tietomassat syntyvät pienten tietomäärien yhdistelmänä. Laajakaistaisuuden tarve on enemmän runkoverkkojen ja palveluiden kuin itse tietolähteen puolla. Tärkeää olisi varmistaa verkkojen saatavuus, jotka mahdollistavat paristokäyttöisten laitteiden pitkän käyttöajan ja kustannusrakenteen, joka sopii pienten tietomäärien keräämisen yksittäisistä kohteista.

F-Secure hyödyntää big dataa useissa sovellusalueissa. Tärkeimpänä alueena tietoturvapalveluiden tuottaminen uusien uhkien tunnistamisessa ja lisäksi perinteisemmät alueet kuten markkinoinnin tehostaminen, tuotteiden laadun parantaminen ja päätöksenteon tuki. Lähtökohtaisesti täysin avoimia siitä, mitä tietoa keräämme, miten käytämme sitä ja miten tarjoamme mahdollisuuden jättäytyä pois tiedon keräämisessä. Pystymme tarvittaessa tarjoamaan hankkeelle esimerkkejä omista toimintamalleistamme. Teknologioiden osalta olemme enemmän big datan hyödyntäjä kuin kehittäjä.

Luonnos on mielestämme hyvä ja siinä tunnistetaan oikeat alueet, mutta toivomme, että jatkotyössä huomioidaan tässä lausunnossa mainitut asiat riittävällä painoarvolla.

F-Secure Oyj:n puolesta

Pirkka Palomäki  
Chief Strategy Officer