Microsoftin Online-palveluiden ehdot

Microsoftin vastine Pekka Kiviniemen (KallioLaw) 22.8.2018 VAHTI Työpaja #14:ssa esittämille kommenteille ja väitteille

Asianajaja Pekka Kiviniemi on esittänyt VAHTI Työpajassa #14 omia tulkintojaan Microsoftin ehdoista ja toimintatavoista. Kiviniemen yksipuoliset kommentit on julkaistu valtiovarainministeriön VAHTI-yhteishankkeiden materiaalit -sivustolla. Tässä vastineessa pyrimme oikaisemaan Kiviniemen kommenteissa ja väitteissä esiintyneitä epäselvyyksiä ja väärinkäsityksiä.

Microsoftin Online Services Terms eli Online-palveluiden ehdot löytyvät osoitteesta http://www.microsoftvolumelicensing.com/.

Useat Kiviniemen kommenteista koskevat EU:n yleistä tietosuoja-asetusta (”tietosuoja-asetus”). Microsoft on täysin sitoutunut siihen, että pilvipalvelumme täyttävät kaikki tietosuoja-asetuksen vaatimukset ja tämä ilmenee myös sopimusehdoistamme.

Online-palveluiden ehdoissa sitoudumme siihen, että Microsoft noudattaa Euroopan talousalueen tietosuojalainsäädännön vaatimuksia, jotka liittyvät Euroopan talousalueelta peräisin olevien henkilötietojen käsittelyyn. Tietosuoja-asetuksen 28(1) artikla edellyttää rekisterinpitäjän ja käsittelijän välistä sopimusta, jonka on katettava kyseisessä artiklassa listatut asiat. Tämän vaatimuksen täyttämiseksi Microsoftin Online-palveluiden ehdot sisältävät ”Tietosuoja-asetukseen liittyvät ehdot” (Online-palveluiden ehtojen liite 4). Yksityiskohtaisempaa tietoa siitä miten Microsoft käsittelee Asiakastietoa ja henkilötietoa on myös muualla Online-palveluiden ehdoissa, erityisesti osiossa ”Tietosuojaehdot” (”Data Protection Terms”).

Vastauksia Kiviniemen Online-palveluiden ehtoihin esittämiin kommentteihin

A1: Muiden kuin Microsoftin tuote (”Non-Microsoft Product”) tarkoittaa Online-palveluiden ehtojen määritelmän mukaan kolmannen osapuolen ohjelmistoa, tietoja, palvelua, verkkosivustoa tai tuotetta, *jota Microsoft ei ole sisällyttänyt Online-palveluunsa*. Tällaisiin tuotteisiin tyypillisestis soveltuvat erilliset, kyseisten kolmansien osapuolten ehdot.

A5-A6: Tietosuoja-asetus on suoraan sovellettavaa lainsäädäntöä eli sitä sovelletaan sellaisenaan myös Suomessa. Tuleva kansallinen tietosuojalaki voi tietyiltä osin täydentää sitä, mutta se ei voi olla tietosuoja-asetuksen vastaista.

On tärkeää huomata, että soveltuvat lait riippuvat myös siitä, mitä tietoja Online-palveluissa käsitellään (esim. onko Asiakastieto jonkun erityissääntelyn alaista). Vain Asiakas itse pystyy arvioimaan soveltuuko tietty palvelu Asiakkaan tiedoille ja käyttötapauksille. Microsoftilla ei ole näkyvyyttä Online-palveluissa käsiteltävien Asiakkaan tietojen sisältöön tai arvoon. Microsoft ei myöskään hallitse tai valvo mitä komponentteja Asiakas tuo Online-palveluun tai miten Asiakas määrittelee tekniset asetukset.

Microsoft soveltaa uusinta tekniikkaa käyttävää tietoturvaa ja tarjoaa avoimesti tietoa siitä miten Online-palveluita tuotetaan, jotta Asiakkaat voivat määritellä oikeat tavat ja asetukset, joiden mukaisesti Asiakas

käyttää palveluita siten, että pystyy noudattamaan soveltuvia lakeja myös siirryttyään käyttämään pilvipalveluita. Viimekädessä on kuitenkin Asiakkaan velvollisuus valita Online-palveluiden asetukset ja käyttötarkoitukset ja käsitellä tietojaan niiden tärkeyden ja arkaluonteisuuden vaatimalla tavalla.

A8: Tässä sopimuskohdassa mainitut käytännöt ovat sellaisia tekoja, jotka voisivat aiheuttaa haittaa tai vahinkoa Microsoftille, palveluille, asiakkaillemme tai kolmansille osapuolille. Tämä lista kielletyistä käytännöistä on toimialalle tyypillinen. Microsoftin on pystyttävä puuttumaan tällaisiin väärinkäytöksiin suojellakseen kaikkia Microsoftin asiakkaita. Microsoft myös sitoutuu tässä siihen, että mahdolliseen Online-palveluiden keskeyttämiseen ryhdytään vain siinä laajuudessa, kuin on kohtuullisesti välttämätöntä. Välttämättömyys riippuu käsillä olevasta tapauksesta ja rikkomuksen aiheuttamasta riskistä. Jos riski on siedettävällä tasolla, Microsoft pyrkii aina ensin ilmoittamaan ennen palvelun keskeyttämistä.

Microsoft käyttää ja käsittelee Asiakastietoja ainoastaan voidakseen tarjota Asiakkaille Online-palveluita ja vain ehdoissa määritetyin tavoin. Asiakastietoihin pääsy on tarkkaan rajattua (ks. erityisesti Online-palveluiden ehtojen kohta ”Tietoturva”). Kiviniemen väite Microsoftin Asiakastietoon kohdistamasta valvonnasta on väärä.

Lisätietoja:

Microsoft Trust Center: Who can access your data and on what terms

A10-A11: Kuten edellä on mainittu, Asiakkaiden, jonka toimialalla sovelletaan erityislainsäädäntöä, tulee itse arvioida soveltuvatko Microsoftin Online-palvelut heidän erityistarpeisiinsa. Microsoft sitoutuu tarjoamaan palvelut tietyllä tavalla.

Koska Microsoft ei voi yleisesti tietää sisältävätkö Asiakkaan tiedot henkilötietoa vai ei, Microsoft suhtautuu kaikkeen Asiakastietoon kuin se olisi henkilötietoa. Asiakkailla on myös itsellään vastuu noudattaa tietosuoja-asetuksen Asiakkaille asettamia vaatimuksia ja Asiakkailla on myös itsellään vastuu omista toimistaan tietojensa hallinnoimiseksi.

A13: Ks. alla kommentti A38-A39.

A14–A15: Microsoft ei anna pääsyä mihinkään Asiakastietoihin minkään maan lainvalvontaviranomaisille tai muillekaan kolmansille osapuolille, ellei laki siihen velvoita. Kaikissa tapauksissa noudatamme seuraavia toimintatapoja, jotka soveltuvat riippumatta siitä tuleeko vaatimus lainvalvontaviranomaiselta vai yksityiseltä osapuolelta viranomaisteitse:

- Microsoft kehottaa viranomaista pyytämään Asiakastietoja suoraan Asiakkaalta.
- Arvioimme tarkkaan vastaanottamamme vaatimukset ja varmistamme niiden laillisuuden. Puutteelliset vaatimukset hylätään ja luovutettava tieto rajoitetaan vain täysin välttämättömään ja vaatimuksessa hyvin yksilöityyn. Esimerkiksi Yhdysvaltain viranomaisilta tulevan vaatimuksen on oltava esitetty oikean laillisen menettelyn mukaisesti, sen on perustuttava vahvaan rikosepäilyyn (”probable cause”) ja sen on oltava toimivaltaisen tuomioistuimen vahvistama. Euroopassa sijaitsevia tietoja koskee eurooppalainen lainsäädäntö, mukaan lukien tietosuoja-asetus. Microsoft on menestyksekkäästi onnistunut haastamaan ristiriitaisia vaatimuksia oikeudessa ja teemme niin jatkossakin.

- Jos Microsoftin on lain velvoittamana pakko antaa pääsy Asiakastietoihin viranomaiselle, Microsoft ilmoittaa asiasta viipymättä Asiakkaalle ja toimittaa Asiakkaalle kopion luovutusvaatimuksesta, jollei tätä ole laissa kielletty.
- Microsoft ei anna millekään kolmannelle osapuolelle (a) suoraa, epäsuoraa, rajoittamatonta tai valvomatonta pääsyä Asiakastietoihin, (b) Asiakastietojen salaamiseen käytettyjä alustan salausavaimia tai (c) minkäänlaista käyttöoikeutta Asiakastietoihin.

Ollaksemme mahdollisimman avoimia, julkaisemme sivustollamme maakohtaiset tilastot lainvalvontaviranomaisten tekemistä asiakastietoja koskevista tietopyynnöistä ja siitä miten niihin on vastattu (”Law Enforcement Requests Report”). Valtaosa tietopyynnöistä koskee kuluttaja-asiakkaita. Vuonna 2017 Microsoft vastaanotti Yhdysvaltain viranomaisilta 163 tietopyyntöä koskien Yhdysvaltojen ulkopuolella sijaitsevaa tietoa. Yksikään niistä ei koskenut Enterprise-asiakkaiden tietoja (yritysasiakas, jolla on vähintään 50 käyttäjää).

Lisätietoja:

Microsoft Trust Center: Responding to government and law enforcement requests to access customer data

Periaatteemme ja usein kysytyt kysymykset (FAQ).

A17–A18: Microsoft käsittelee henkilötietoja ainoastaan Asiakkaan dokumentoitujen ohjeiden mukaisesti. Online-palveluiden ehdoissa todetaan, että nämä ohjeet muodostuvat Asiakkaan volyymikäyttöoikeussopimuksessa (mukaan lukien Online-palveluiden ehdot) sovitusta sekä siitä, miten Asiakas käyttää tuotteiden ominaisuuksia ja konfiguroi ne. Asiakas voi muuttaa ohjeita konfiguroimalla tuotteita ja muuttamalla niiden toimintoja. Microsoftin ei ole mahdollista vastaanottaa sellaisia ohjeita, jotka ovat ristiriidassa Online-palveluiden toiminnallisuuksien kanssa, sillä pilvipalveluita ei ole mahdollista muokata asiakaskohtaisesti enempää, kuin mitä asiakas itse voi tehdä. Kiviniemen esittämä väite siitä, että Microsoft pystyisi lisämaksua vastaan vastaanottamaan muita asiakaskohtaisia ohjeita tai määräyksiä, on väärä.

A19-A20: Tietosuoja-asetus on suoraan sovellettavaa lainsäädäntöä eli sitä sovelletaan sellaisenaan myös Suomessa. Tässä sopimuskohdassa olevat määritelmät eivät ole tapauskohtaisia. Henkilötietoja käsitellään tämän sopimuksen alla aina samaa tiettyä tarkoitusta varten, joka on Online-palveluiden toimittaminen Asiakkaan volyymikäyttöoikeussopimuksen mukaisesti. Käsiteltävät henkilötiedot ja rekisteröidyt ovat myös määritelty kaikille asiakkaille samalla tavoin.

A23–A25: Microsoftin ja Asiakkaan välisessä suhteessa Asiakkaan tiedot kuuluvat Asiakkaalle. Microsoft ei toimiessaan henkilötietojen käsittelijänä tai apukäsittelijänä vastaa itsenäisesti rekisteröityjen pyyntöihin, sillä Asiakkaan tulee itse päättää tiedoistaan ja vastata rekisteröityjen pyyntöihin. Microsoft ei myöskään mene Asiakkaan tietoihin, eikä voi tietää mille lailliselle perusteelle Asiakkaan henkilötietojen käsittely perustuu. Microsoft ei siksi pystyisi arvioimaan tarvittavia toimenpiteitä. Microsoft ohjaa rekisteröidyt tekemään pyynnöt rekisterinpitäjälle. Jos Microsoft vastaanottaa tietopyynnön rekisteröidyltä ja pystyy varmistumaan siitä, kuka rekisterinpitäjä on (minkä asiakkaan käyttäjä rekisteröity on), Microsoft ilmoittaa pyynnöstä Asiakkaan järjestelmänvalvojalle.

A26-A27: Kiviniemen väite on virheellinen. Online-palveluiden ehtojen liitteenä 4 olevissa tietosuoja-asetukseen liittyvissä ehdoissa Microsoft sitoutuu nimenomaisesti tietosuoja-asetuksen mukaisiin tietosuojavaatimuksiin. Lisäksi tietosuoja-asetuksen Artikla 32 soveltuu myös suoraan henkilötietojen käsittelijöihin. Sen lisäksi, että tämä Online-palveluiden ehtojen jakso sisältää sitoumuksen noudattaa asianmukaisia tietosuojatoimenpiteitä (suhteessa kaikkiin Asiakastietoihin), se myös sisältää tarkkaa tietoa siitä, millaisia tietoturvatoimenpiteitä Microsoft noudattaa, jotta Asiakkaat voivat arvioida niitä omia vaatimuksiaan vastaan.

A28-A30: Kuten muutkin pilvipalveluiden tarjoajat toimialalla, Microsoft tuottaa Online-palveluita jaetun vastuun mallin kautta. Sekä Microsoftin että Asiakkaan on otettava vastuu lakien noudattamisesta.

Soveltuvat lait riippuvat myös siitä, mitä tietoja Online-palveluissa käsitellään (esim. onko tieto henkilötietoa, erityissääntelyn tai valvonnan piiriin kuuluvaa tietoa tms.). Vain Asiakas itse pystyy arvioimaan soveltuuko tietty palvelu Asiakkaan tiedoille ja käyttötapauksille. Microsoftilla ei ole näkyvyyttä Online-palveluissa käsiteltävien Asiakkaan tietojen sisältöön tai arvoon. Microsoft ei myöskään hallitse tai valvo mitä komponentteja Asiakas tuo Online-palveluun tai mitä asetuksia Asiakas määrittelee.

Microsoft soveltaa uusinta tekniikkaa käyttävää tietoturvaa ja tarjoaa avoimesti tietoa siitä miten Online-paveluita tuotetaan, jotta Asiakkaat voivat määritellä oikeat tavat ja asetukset, joiden mukaisesti Asiakas käyttää Online-palveluita siten, että pystyy noudattamaan soveltuvia lakeja myös siirryttyään käyttämään pilvipalveluita. Viimekädessä on kuitenkin Asiakkaan velvollisuus valita Online-palveluiden asetukset ja käyttötarkoitukset ja käsitellä tietojaan niiden tärkeyden ja arkaluonteisuuden vaatimalla tavalla.

Koska Microsoft ei tiedä minkälaisia tietoja Asiakas vie palveluun, Microsoft ei voi päättää minkälaiset tietoturvatoimet ovat ”asianmukaiset”. Tästä syystä Microsoft tarjoaa avoimesti tietoa noudattamistamme tiukoista turvallisuustoimista, järjestelmistä ja prosesseista, jotka Microsoftilla on käytössä, jotta Asiakkaamme voivat tehdä informoituja päätöksiä perustuen siihen mitä vain Asiakkaat itse tietävät omista tiedoistaan.

A31: Microsoft ei voi sallia yksittäisten Asiakkaiden tekemiä tarkastuksia Online-palveluiden tuotantoon tai datakeskuksiin, koska tällainen toiminta vaarantaisi Microsoftin kyvyn tarjota korkean tason tietoturvaa ja tietosuojaa kaikille Asiakkaille. Yksittäisten Asiakkaiden tekemiä tarkastuksia ei olisi myöskään mitenkään käytännössä mahdollista toteuttaa isossa mittakaavassa. Microsoft tarjoaa laajasti yksityiskohtaista tietoa auditoinneista. Kuten näissä ehdoissa on kuvailtu, Microsoft noudattaa monia standardeja, kuten ISO 27001, 27002 ja ISO 27018 ja julkaisee niihin liittyvät tarkastusraportit. Auditoinnit toteuttaa asiantuntevat itsenäiset kolmannen osapuolen tietoturvatarkastajat ja auditointiraportit julkaistaan Asiakkaille Service Trust Portalissa (https://servicetrust.microsoft.com/). Toimintatapa vastaa toimialan käytäntöä ja Tietosuojatyöryhmä Working Party 29:n hyväksymää tapaa suorittaa tarkastukset johtuen niistä epäkäytännöllisyyksistä ja turvallisuusriskeistä, jotka liittyisivät yksittäisten auditointien sallimiseen multi-tenant -ympäristöissä.

A32: Väite on virheellinen.

A33-A37: Tämä ehtojen turvallisuusongelmailmoituksia (”Security Incident Notification”) koskeva jakso ei koske pelkästään henkilötietoihin vaan kaikkiin Asiakastietoihin kohdistuvia tietoturvapoikkeamia. Myös käytetty termi on ehdoissa vanhempi ja laajempi kuin tietosuoja-asetuksen termi ”Henkilötietoloukkaus”.

Microsoft sitoutuu tässä niihin toimenpiteisiin, mitkä Asiakas tarvitsee ja minkä perusteella Asiakkaat voivat täyttää tietosuoja-asetuksen mukaiset velvoitteensa. Toisin kuin Kiviniemi on väittänyt, Microsoftin ehdoissa ei kavenneta henkilötietojen käsittelijän toimintavelvollisuuksia. Tietosuoja-asetuksen mukaan henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa. On kuitenkin rekisterinpitäjän velvollisuus ilmoittaa siitä tarvittaessa valvontaviranomaiselle ja rekisteröidyille. Tämä vastuunjako tulee suoraan tietosuoja-asetuksen 33 artiklasta.

A38-A39: Voidakseen tarjota hyperskaalan pilvipalveluita, Microsoftilla on oltava resursseja, mukaan lukien alihankkijoita, ympäri maailmaa. Nämä resurssit pystyvät esimerkiksi ratkomaan tietynlaisia teknisiä ongelmia. Microsoftin Trustcenter-sivustolla on lista kaikista niistä henkilötietojen apukäsittelijöistä *sijainteineen*, joilla on pääsy Asiakastietoihin ja henkilötietoihin. Jos Asiakas ei hyväksy uutta apukäsittelijää, Asiakas voi irtisanoa kyseisen Online-palveluiden tilauksen ilman seuraamuksia.

Microsoft ei millään lailla kontrolloi tai rajoita sitä, miten Asiakkaat tai heidän loppukäyttäjänsä voivat siirtää Asiakkaan tietoja. Asiakas ja Asiakkaan käyttäjät voivat käyttää palvelua mistä päin maailmaa tahansa ja näin siirtää tietoja kolmansiin maihin tietosuojalainsäädännön tarkoittamassa merkityksessä.

Henkilötietojen siirto kolmansiin maihin Microsoftin palveluissa perustuu Microsoftin EU:n ja Yhdysvaltain Privacy Shield Framework -sopimuksen mukaiseen sertifiointiin sekä ”Online-ydinpalveluiden” osalta Microsoftin tarjoamiin Euroopan komission 5.2.2010 tekemän päätöksen mukaisiin mallisopimuslausekkeisiin (EU Direktiivi 95/46/EY 26 artiklan 2 kohta, Online -palveluiden ehtojen liite 3) (”EU-mallisopimuslausekkeet”). Euroopan Unionin ja Yhdysvaltojen välinen Privacy Shield -sopimus turvaa EU-kansalaisen perusoikeudet siirrettäessä henkilötietoja Yhdysvaltoihin ja luo periaatteet yrityksille, jotka siirtävät henkilötietoja EU:n ja Yhdysvaltojen välillä. Microsoft myös takaa Online-palveluiden ehdoissa, että henkilötietojen siirtoon kolmanteen maahan tai kansainväliselle organisaatiolle sovelletaan tietosuoja-asetuksen artiklassa 46 kuvattuja asianmukaisia suojatoimia ja että tällaiset siirrot ja suojatoimet dokumentoidaan tietosuoja-asetuksen 30(2) artiklan mukaisesti.

Alihankkijat voivat käsitellä tietoja vain niiden palveluiden toimittamiseksi, joita varten Microsoft on ne palkannut, eivätkä ne saa käyttää tietoja muihin tarjoituksiin. Useat alihankkijoista tarjoavat Microsoftille työntekijöitä, jotka työskentelevät yhdessä Microsoftin työntekijöiden kanssa palveluiden tuottamiseksi. Tietoja käsitellään silloin Microsoftin tiloissa ja järjestelmissä. Alihankkijat ovat sitoutuneet sopimuksellisesti vähintään yhtä tiukkoihin salassapitoa ja yksityisyydensuojaa koskeviin vaatimuksiin kuin mitä Microsoftin ja asiakkaan välillä on sovittu. Alihankkijoiden pitää myös täyttää kaikki tietosuoja-asetuksen asettamat vaatimukset. Asiakastietoja käsittelevien apukäsittelijöiden on myös sitouduttava EU:n mallisopimuslausekkeisiin niiltä osin, kuin Microsoft käyttää niitä tietojen siirtämisen perusteena.

Ks. lisäksi Online-palveluiden ehtojen kohta ”Asiakastietojen tallennuspaikka” (”Location of Customer Data at Rest”), mikä sisältää Asiakastietojen tallennuspaikkaa koskevia sitoumuksia.

Lisätietoja:

Microsoft Trust Center: Where your data is located

Microsoft Trust Center: Who can access your data and on what terms (ks. erityisesti “We limit access by subprocessors” ja “Lists of subcontractors”)

A43: Asiakkaiden tiedot ovat Asiakkaiden tietoja, eikä Microsoft voi erotella onko Asiakastiedoissa henkilötietoja vai ei. Asiakkaat voivat koska tahansa poistaa Asiakastiedot tai niissä olevat henkilötiedot - vaikka vain yhtä henkilöä koskevat tiedot.

A44: Tämä ehtojen jakso koskee sitä kuinka kauan Asiakas voi hakea tietoja palvelusta vielä tilauksen päätyttyä, jos Asiakas ei ole poistanut tietoja. Asiakas voi koska tahansa poistaa Asiakastiedot tai osia niistä (esim. henkilötietoja) jo ennen palvelun päättymistä.

Lisätietoja:

Microsoft Trust Center: Data Management at Microsoft (ks. “What happens to your data if you leave the service”)

A48: Kiviniemen väite siitä, ettei Microsoft muokkaa tietoturvatoimenpiteitä tilanteen eläessä, on virheellinen. Useiden käytäntöjen kohdalla vaatimukset on myös sidottu ”alan standardiin”, mikä jo sinällään vaatii kehittymistä ajan myötä.

A50: Bing-hakupalveluihin (”Bing Search Services”) ei sovellu Online-palveluiden ehtojen liite 4 (Tietosuoja-asetukseen liittyvät ehdot), sillä niiden käyttöön sovelletaan osoitteessa https://go.microsoft.com/fwlink/?LinkId=521839 sijaitsevaa Microsoftin Tietosuojalauseketta. Tämä johtuu siitä, että Online-palveluiden ehtojen liite koskee Microsoftin suorittamaa henkilötietojen käsittelyä Asiakkaan puolesta. Bing-hakupalveluiden osalta Microsoft ei toimi henkilötietojen käsittelijänä Asiakkaan puolesta vaan siltä osin kuin palvelun tarjoamisen yhteydessä tulee käsiteltäväksi henkilötietoja, Microsoft käsittelee niitä rekisterinpitäjänä.

A52: Kiviniemen väite, jonka mukaan kaikkiin Microsoftin sopimuksiin soveltuu Yhdysvaltain lainsäädäntö, on virheellinen. Microsoftin ja Asiakkaan välisiin sopimuksiin soveltuva lainsäädäntö ja riidanratkaisumekanismi on määritelty Microsoftin ja Asiakkaan välisessä volyymikäyttöoikeussopimuksessa.