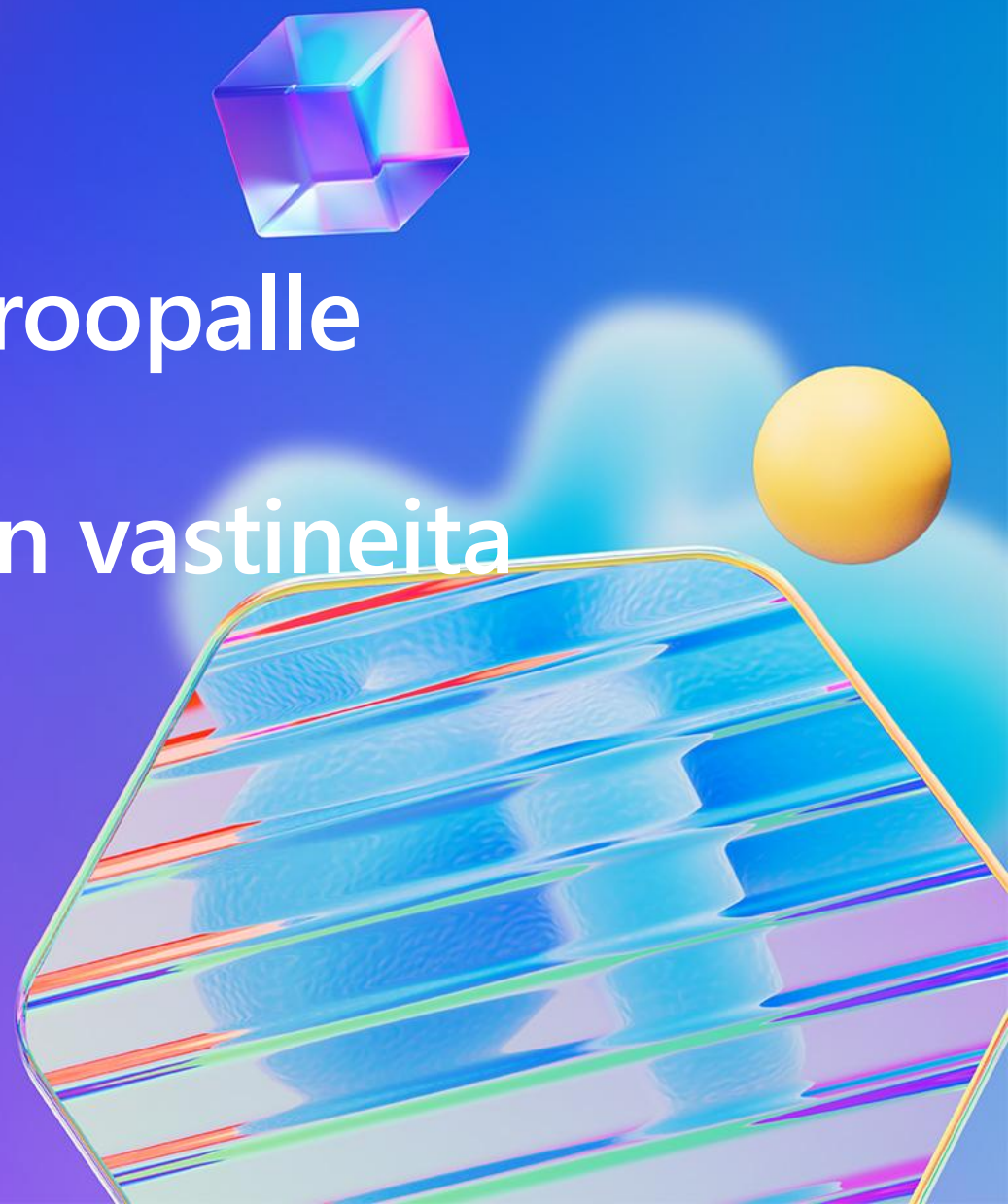
Microsoft

Microsoft Sovereign Cloud ja Microsoft sitoumukset Euroopalle

Juha Karppinen
teknologiajohtaja
Juha.karppinen@microsoft.com

Asioita tänään

- Microsoftin sitoumukset Euroopalle
- Microsoft Sovereign Cloud
- Lehdistön väittämiä ja niiden vastineita

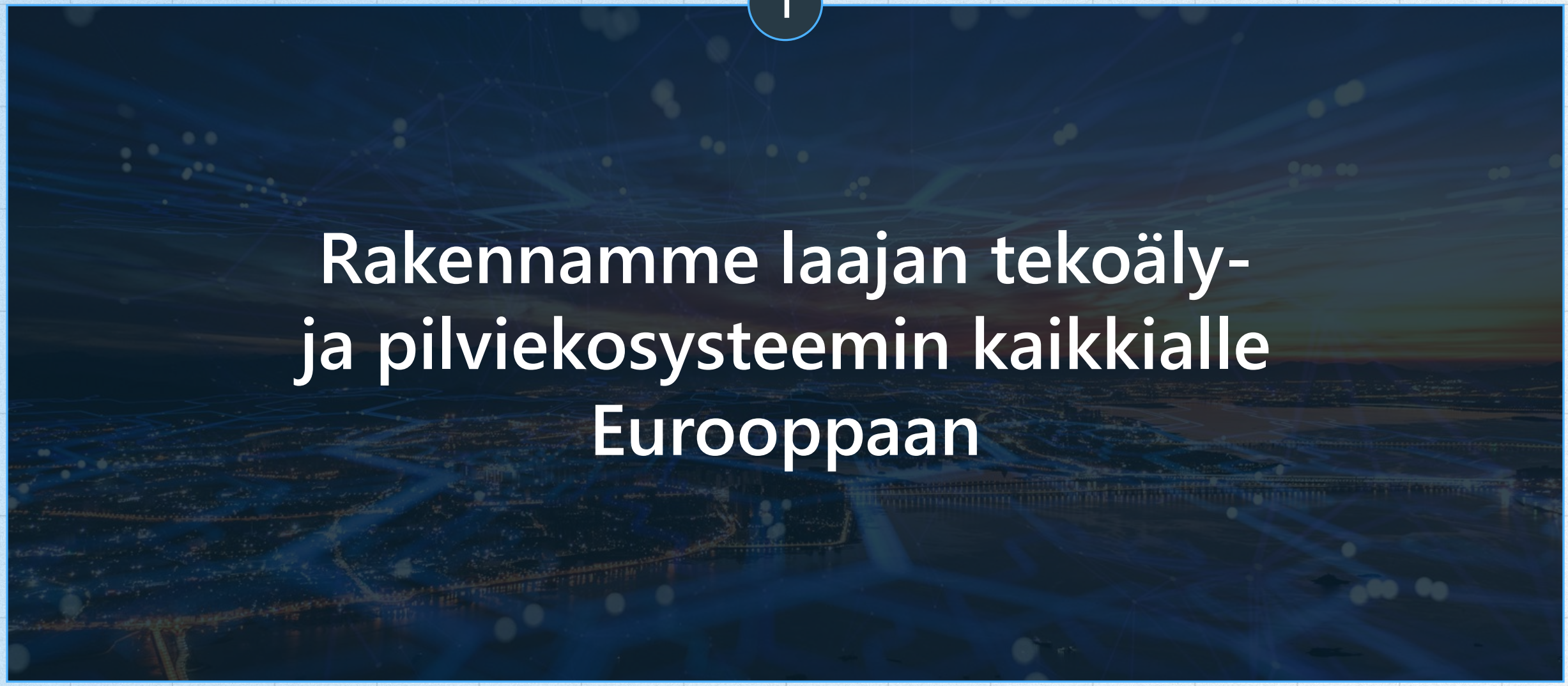


Microsoftin sitoumukset Euroopan digitalisaation kehittämiseen

1. Rakennamme laajan tekoäly- ja pilviekosysteemin kaikkialle Eurooppaan
2. Säilytämme Euroopan digitaalisen resilienssin myös geopoliittisen epävakauden aikana
3. Jatkamme eurooppalaisten tietojen yksityisyyden suojaamista.
4. Autamme aina suojaamaan ja puolustamaan Euroopan kyberturvallisuutta.
5. Autamme vahvistamaan Euroopan taloudellista kilpailukykyä, myös avoimen lähdekoodin osalta.

Microsoftin sitoumukset Euroopan digitalisaation kehittämiseen

1



Rakennamme laajan tekoäly- ja pilviekosysteemin kaikkialle Eurooppaan

Espoon datakeskuksen havainnekuva

Espoon datakeskuksen havainnekuva

Kuva: Olla Architecture

Kuva: Olla Architecture

2

Säilytämme Euroopan digitaalisen resilienssin myös geopoliittisen epävakauden aikana

Microsoftin sitoumukset Euroopan digitalisaation kehittämiseen

2

Säilytämme Euroopan digitaalisen resilienssin myös geopoliittisen epävakauden aikana

Eurooppalaiset pilvipalvelut eurooppalaiselle

Sitoudumme digitaaliseen resilienssiin

Varmistamme palveluiden saatavuuden

Eurooppalaiset datakeskukset ovat EU lakien mukaisia

"Our European data center operations are governed by a newly appointed board of directors composed exclusively of European nationals and employed by Microsoft Ireland Operations Limited, an Irish company that owns all Microsoft datacenter entities in Europe and operates under European law, reinforcing our commitment to local oversight."

Sopimukselliset sitoumukset

Olemme lisänneet tietojenkäsittelysopimukseemme (aka.ms/DPA) liitteen D, jossa kuvaamme sitoumuksemme käyttää kaikkia laillisia keinoja kumotaksemme ja haastaaksemme määräykset, jotka koskevat palveluiden tarjoamisen keskeyttämistä tai lopettamista.

Appendix D – Challenges to Order or Binding Legal Obligation Suspending Online Services

By this Appendix, Microsoft provides the following commitments to National, Federal, and Regional Government Customer entities of the European Union ("EU") Member States, as well as EU accession countries, members of the European Free Trade Association, the United Kingdom, Monaco, the Vatican, and the European Commission ("Protected Government Customer").

1. In the event that Microsoft receives an order or is otherwise subject to a binding legal obligation from any government, agency, commission, or quasi-governmental body requiring Microsoft to suspend or cease the provision, in whole or in part, of Online Services (including, but not limited to, the provision of Microsoft Azure Services, Microsoft Dynamics 365 Services, or Office 365 Services) to the Protected Government Customer – Microsoft, on behalf of itself and its Affiliates, shall:
    a. use available means to secure the voluntary withdrawal, revocation, or rescission of such order; and
    b. use all lawful efforts to challenge the order in the courts of the country whose government issued the order on the basis of any legal deficiencies under the laws of the ordering party or any relevant conflicts with applicable law of the European Union or applicable law of the countries listed above.

    Microsoft will seek permanent and interim injunctive relief if needed to ensure the continuous and uninterrupted provision of the relevant Online Services pending the full and final adjudication of lawful efforts to challenge the order or other binding legal obligation referred to above.
2. Rights granted to Customer under this provision are personal to the Protected Government Customer and may not be assigned.

Kysymys : Microsoft on katkaissut pääsyn Kansainvälisen rikostuomioistuimen (ICC) henkilön osalta Microsoft 365 –palveluihin.

Vastaus:

ICC on ollut ja on edelleen Microsoftin institutionaalinen asiakas, emmekä ole keskeyttäneet palveluja ICC:lle. Olemme ylläpitäneet palvelua, vaikka Yhdysvaltain pakotteet ovat kohdistuneet yksittäisiin henkilöihin. Microsoft tarjoaa teknisen alustan, ja pääsyoikeuksista päättää asiakas. Sopimuksemme velvoittaa Microsoftin haastamaan oikeudessa kaikki ulkopuolelta tulevat määräykset palvelujen keskeyttämiseksi.

ICC on avannut asiaa omilla verkkosivuillaan ja mediassa:

ICC chief prosecutor Karim Khan steps aside until sexual misconduct probe ends

ja https://asp.icc-cpi.int/press-releases/PR-20250518

Microsoft Sovereign Cloud

Kattavat itsenäiset tuottavuus-, tietoturva- ja pilvipalvelu ratkaisujen valmiudet Euroopassa

Public Cloud	Sovereign Public Cloud	Sovereign Private Cloud	Sovereign National Clouds

← Yhtenäinen hallinta- ja kehitysalusta →

← **Palveluiden määrä kasvaa** — **Suvereniteetti kasvaa** →

Sovereign Public Cloud

Saatavilla olevat sovereniteetti kontrollit

Microsoft *Advanced Data Residency for M365* ja *Azure Sovereign Landing Zones* takaavat jo nyt edistyneen suojauksen, tietojen säilytyksen ja eksklusiivinen hallinnan

Digitaaliset sitoumukset Euroopalle – erillisen hallituksen hallinnoima Euroopan toiminta

Tekniset uudistukset

Data Guardian: Eurooppalainen valtuutettu henkilö hyväksyy pääsyn ja valvoo sitä reaaliaikaisesti ja kirjataan lokiin. Asiakas voi myös lisäksi hyödyntää *Customer Lock Box –* toiminnallisuutta (asiakas hyväksyy pääsyn vielä itse)

External Key Management: Salausavaimet ovat tallennettuna asiakkaan rautapohjaisessa HSM-laitteistossa (omassa tai kumppanin) konesalissa. Azure-palvelut pyytävät salausavainta aina tarvittaessa, mutta avain ei koskaan poistu asiakkaan hallusta.

Regulated Environment Management: Määritä ja valvo kaikkia suvereniteetti- ja käytäntörajoituksia yhdessä yhtenäisessä portaalissa.

Sovereign Private Cloud

	Azure Local	Microsoft 365 Local
Kuvaus	**Pilvialusta, joka auttaa varmistamaan sovellusten jatkuvuuden ja tarjoaa Azure-ominaisuuksia paikkoihin, joihin perinteinen pilvi ei sovi**, kuten etäkohteisiin, suojattuihin sisäverkkoihin, jotka tarvitsevat luotettavaa infrastruktuuria.	**Käyttöönottokehys tuottavuus- ja kollaboraatiotyökalujen suorittamiseen** (Exchange Server, SharePoint Server, Skype for Business Server) **turvallisessa** Azure Local **ympäristössä**
Päähyödyt	• **Skaalautuva infrastruktuuri,** kymmenistä ytimistä tuhansiin ytimiin • **Pääsy Azure Arc -yhteensopiviin palveluihin,** mukaan lukien Azuren paikalliset virtuaalikoneet, AKS Arc, ohjelmistopohjaiset verkot, tallennus ja tekoälyn reunatyökuormissa	• **Yhteensopiva Azure-ympäristön kanssa,** mahdollistaa toiminnan hybridi- tai ei julkisessa verkossa olevissa ympäristöissä • **Mahdollisuus hyödyntää** Azure Local'n tarjoamia **julkisen pilven etuja** • **Tuki vuoden 2035 loppuun!!**

- **Joustavuutta ja modulaarisuutta** asiakkaan tarpeisiin räätälöidyille erillisille tai hybriditoiminnoille
- **Täydellinen toiminnallinen autonomia** infrastruktuurin, datan ja palveluiden suhteen
- Yhtenäinen ohjaustaso virtaviivaistaa käyttöönottoa ja elinkaaren hallintaa

Microsoftin sitoumukset Euroopan digitalisaation kehittämiseen

3

Jatkamme eurooppalaisten tietojen yksityisyyden suojaamista

Suojaamme tietojen yksityisyyttä

EU Data Boundary projekti

Turvaamme ja salaamme kaiken asiakasdatan

EU Data Boundary for the Microsoft Cloud

EU Data Boundary -sitoumus koskee EU- ja EFTA-maissa olevia asiakasympäristöjä (tenant). EU Data Boundary tarkoittaa, että asiakaan dataa (määritelty DPA:ssa) ei ainoastaan tallenneta EU:n sisällä vaan **Azure-, Dynamics 365-, Power Platform- ja Microsoft 365** -palvelut myös prosessoivat datan EU:n datakeskuksissa.

Microsoft EU Data Boundary Overview | Microsoft Trust Center

Kysymys : Voiko USA hallitus Cloud Act'iin nojaten saada ja vaatia Microsoftia luovuttamaan asiakkaan dataa?

Vastaus:

Cloud Act jo nimensä perusteella ymmärretään väärin. CLOUD Act (**Clarifying Lawful Overseas Use of Data Act**) on vuonna 2018 Yhdysvalloissa säädetty laki, joka määrittää, milloin ja miten Yhdysvaltain lainvalvontaviranomaiset voivat pyytää teknologia- ja pilvipalveluyrityksiltä dataa, vaikka data sijaitsisi Yhdysvaltojen ulkopuolella.

Se ei luo uusia valvontavaltuuksia, vaan selventää jo olemassa olevia sääntöjä siitä, mihin Yhdysvaltain tuomioistuimen toimivalta ulottuu. Cloud Act vaatii aina tuomioistuimen luvan (etsintäluvan tai määräyksen). Luvan saaminen edellyttää todennäköisiä syitä vakavaan rikokseen – satunnainen tai massaluonteinen pääsy dataan ei ole sallittu. Se Ei salli bulkkidatan keruuta, automaattista pääsyä tai takaovia salaukseen. Microsoft tai muut palveluntarjoajat eivät luovuta salausavaimia.

Cloud Act kunnioittaa muiden maiden lakeja. Laki sisältää ns. comity-mekanismin: palveluntarjoaja voi haastaa pyynnön, jos sen noudattaminen rikkoisi vieraan valtion lakia. Se myös mahdollistaa kahdenväliset valtiosopimukset, joiden avulla poliisi- ja viranomaispyyntöjen käsittely tehostuu.

Suosittelemme tutustumista Cloud Act'iin. Tässä linkkejä ulkopuolisien juristien analyyseihin Cloud Act:sta:

(8) Pilven geopoliittiset ulottuvuudet – oikeudelliset faktat ja fiktio erotettava toisistaan | LinkedIn

Data sovereignty in light of the CLOUD Act: back to the future? - Osler, Hoskin & Harcourt LLP

Kysymys: Voiko Microsoft lukea ja luovuttaa asiakkaan dataa ulkopuolisille tahoille tai esimerkiksi ”vakoilla” eurooppalaisia tarjouskilpailuja Yhdysvaltain kansallisen turvallisuuden nimissä.

Vastaus:

Microsoft käsittelee asiakasdataa tietosuojasopimustamme (www.aka.ms/DPA) mukaisesti, ainoastaan palvelun tuottamiseksi asiakkaalle dokumentoitujen ohjeiden mukaan. Minkäänlainen ”vakoilu” tai luvaton valvonta ei kuulu toimintaamme eikä ole sallittua missään olosuhteissa. Yhdysvaltain hallituksella tai millään muullakaan hallituksella ei ole suoraa pääsyä asiakasdataan.

DPA:n liite C ”Additional Safeguards” liite sisältää lisäsuojauksia, kuten sitoumuksen haastaa tuomioistuimessa kaikki vaatimukset, jotka koskevat EU:n julkishallinnon tai yritysasiakkaiden henkilödataa. Microsoftilla on pitkä kokemus sopimattomien tietopyyntöjen oikeudellisesta haastamisesta.

Microsoft julkaisee kaksi kertaa vuodessa läpinäkyvyysraportit, jotka osoittavat, että tietopyyntöjä EU/EFTAalueen yritysasiakkaiden sisältödataan on äärimmäisen vähän — H2/2024 raportissa **ei ole yhtään** sisällön luovutusta Yhdysvaltain lainvalvonnalle. Julkaisemme raportit osoitteessa https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data#tab-requests-for-enterprise-customer-data

Yhdysvaltain lait eivät mahdollista massavalvontaa tai dataliikenteen laajamittaista keräämistä.

Asiakas voi salata kaikki tallentamansa tiedot (asiakasdata) käyttäen omia salausavaimia ja niihin liittyviä palveluita, kuten Azure Confidential Compute, Azure Key Vault ja Double Key Encryption. Microsoftilla ei ole mahdollisuutta tai keinoa purkaa asiakkaan salausta ja näin ollen lukea selkokielisesti asiakasdataa.

Sopimukselliset sitoumukset

Tietojenkäsittelysopimuksemme liite C, joka liittyy 3. osapuolten tietopyyntöihin. Pyrimme aina haastamaan tietopyynnön:

1. Ohjaamaan kolmannen osapuolen pyytämään tietoja suoraan asiakkaalta.
2. Ilmoittamme asiakkaalle viipymättä, ellei sovellettava laki sitä kiellä.
3. Riitautamme tietojen luovuttamista koskevan määräyksen, jos se on ristiriidassa sovellettavan Euroopan unionin lainsäädännön kanssa.

Appendix C – Additional Safeguards Addendum

By this Additional Safeguards Addendum to the DPA (this "Addendum"), Microsoft provides additional safeguards to Customer for the processing of personal data, within the scope of the GDPR, by Microsoft on behalf of Customer and additional redress to the data subjects to whom that personal data relates.

This Addendum supplements and is made part of, but is not in variation or modification of, the DPA.

1. **Challenges to Orders.** In the event Microsoft receives an order from any third party for compelled disclosure of any personal data processed under this DPA, Microsoft shall:
   a. use every reasonable effort to redirect the third party to request data directly from Customer;
   b. promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and
   c. use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with applicable law of the European Union or applicable Member State law.

If, after the steps described in a. through c. above, Microsoft or any of its affiliates remains compelled to disclose personal data, Microsoft will disclose only the minimum amount of that data necessary to satisfy the order for compelled disclosure.

Kysymys : Microsoft on luovuttanut BitLocker-salausavaimia FBI:lle liittyen Guamin liittovaltion tutkintaa Covid-työttömyysavustusohjelman varojen kavaltamisessa. Pitääkö tämä paikkaansa?

Vastaus:

Kysymys on **kuluttajalaitteista.** Microsoft voi joutua luovuttamaan hallussaan olevia tietoja, mikäli oikeus niin päättää vakavan rikoksen (lapsiporno, huumeet, terrorismi, jne) prosessiin rikoksen tutkintavaiheessa.

BitLocker-palautusavaimet eivät itsessään anna viranomaisille pääsyä kuluttajakäyttäjän laitteelle tallennettuihin tietoihin; **valvontaviranomaisilla on myös oltava fyysisesti hallussaan BitLockerilla salattu laite.**

Vuodesta 2022 lähtien Microsoft on vastannut **38 oikeudelliseen vaatimukseen**, joissa tiedot sisälsivät kuluttajan BitLocker-palautusavaimen. **Kaksikymmentä vaatimuksesta oli lasten hyväksikäyttöä** koskevia tutkimuksia.

Microsoftin sopimusasiakkaiden palautusavainten tallennustila konfiguroidaan erillään kuluttajien palautusavaimista. Microsoft ei ole koskaan toimittanut yritysasiakkaiden palautusavaimia minkään maan viranomaisille.

Kaikkia palveluntarjoajia voidaan vaatia luovuttamaan palveluntarjoajalle pilvessään olevia tietoja. Tämä koskee myös Applea, joka muiden palveluntarjoajien tavoin luovuttaa tietoja, joihin sillä on pääsy pätevän oikeudellisen prosessin yhteydessä, mukaan lukien salatut iCloud-tiedot, kun Applella on pääsy salausavaimiin, kuten Applen verkossa saatavilla olevissa valvontaohjeissa on kuvattu.

Kysymys: Ranskassa Microsoftin lakiasianjohtaja sanoi, että Microsoft ei voi antaa absoluuttista takuuta siitä, etteikö eurooppalaisten julkishallintojen data voisi päätyä Yhdysvaltain viranomaisille, jos nämä esittävät juridisesti pätevän tietopyynnön. Voiko tällainen toteutua.

Vastaus:

Microsoft ei tarjoa millekään hallitukselle suoraa tai rajoittamatonta pääsyä asiakasdataan. Kaikki tietopyynnöt käydään läpi tiukan prosessin mukaisesti sisäisten ja ulkoisten lakitiimien toimesta, jotta varmistetaan, että ne ovat laillisesti päteviä ja pakollisia, noudattavat myös kohdemaan sovellettavaa lainsäädäntöä ja ovat tarkasti rajattuja tiettyihin tilitunnisteisiin.

Ohjaamme lainvalvontaviranomaisen, myös Suomen rikospoliisin, pyytämään tiedot suoraan asiakkaalta, ja ilmoitamme asiakkaalle pyynnöstä sekä toimitamme kopion siitä, ellei laki ja oikeuden tutkintapäätös nimenomaisesti kiellä ilmoittamista. **Kielto voidaan tehdä siinä tapauksessa, että ko. organisaatiota epäillään rikoksesta tai heillä olisi mahdollisuus tuhota pyydettyjä tietoja. Voiko Julkishallinnon organisaatiota epäillä tällaisesta rikoksesta? Emme voi Microsoftina antaa absoluuttista takuuta.**

Olemme ilmoittaneet, että ei ole olemassa yhtään tapausta, jossa olisimme luovuttaneet Yhdysvaltain viranomaisille **Microsoftin ylläpitämään eurooppalaisen julkisen sektorin dataa CLOUD Act’in tai muuhun USA:n lakiin perustuen.**

Microsoftin sitoumukset Euroopan digitalisaation kehittämiseen

4

Autamme suojaamaan ja puolustamaan Euroopan kyberturvallisuutta

- Eurooppalainen CISO
- Tietoturvayhteistyön syventäminen Euroopassa
- Quantum Safe – ohjelma turvaamaan tulevaisuus

Microsoftin sitoumukset Euroopan digitalisaation kehittämiseen

https://blogs.microsoft.com/on-the-issues/2025/06/04/microsoft-launches-new-european-security-program/

Väite: Eurooppalaisia vaihtoehtoja on ja Suomen tulisi ottaa ne heti käyttöön.

Vastaus:

Kyberuhat ja geopoliittiset riskit kasvavat. Microsoft tarjoaa tietoturvan osana pilvipalvelua ja Microsoftin vuosittaiset investoinnit pelkästään tietoturvan kehittämiseen ovat yli 4Mrd USD. Lisäksi Microsoft tarjoaa EU-henkilöstön operoimia, EU:n lainsäädäntöä noudattavia pilvipalveluita ja investoi miljardeja paikalliseen infrastruktuuriin.

Eurooppalaisia pilviratkaisuja tarvitaan, mutta niiden rakentaminen vaatii aikaa ja suuria investointeja. Resilienssiä ei voida heikentää tavoiteltaessa täydellistä omavaraisuutta. Teknisesti korvaavia ratkaisuja on, mutta kokonaisvaihtokustannuksiin vaikuttavat mm. integraatiot, identiteetinhallinta, tietoturvatelemetria, ekosysteemin kypsyys ja sovellusten yhteensopivuus.

Ukrainan sota osoitti, että suurimmat ja kriittisimmät palvelut selviävät vain hyperskaalainfrastruktuurissa, joka kestää massiivisia hyökkäyksiä ja kuormapiikkejä.

Lisäksi on hyvä huomata, että nykyinen salausteknologia tullaan purkamaan kvanttilaskennan keinoin 5–10 vuoden sisällä. Myös tähän uhkaan on varauduttava ja Microsoftin pilvipalvelu on tältä osin asiakkaille luotettava ja kustannustehokas varautumiskeino.

Microsoft Quantum Safe Program

Integroidaan post-quantum-kryptografia (PQC) kaikkiin palveluihin: Azure, Entra ID ja Microsoft 365

Kiitos