Microsoft

Microsoftin pilvipalvelujen tietosuoja – asiakirjojen ja datan tietosuoja pilvessä

Juha Karppinen
Teknologiajohtaja,
National Technology Officer
Juha.karppinen@microsoft.com

Agenda

- Microsoftin pilven tietosuoja ja vaatimustenmukaisuus
- Lisäsuojausmekanismit
- EU Data Boundery
- Julkistus uudesta datakeskusalueesta Suomessa

Microsoft

Microsoftin pilven tietosuoja ja vaatimustenmukaisuus

Uudet vakiosopimuslausekkeet ja tietosuojaneuvoston suositukset

Euroopan komissio hyväksyi 4.6.2021 uudet **vakiolausekkeet,** jotka tulevat korvaamaan nykyiset vakiolausekkeet ja sisältävät uusia tiedon suojaamiseen liittyviä kohtia.

- **Uudet vakiosopimuslausekkeet tulee olla uusien sopimusten osalta käytössä 27.9.2021 mennessä**
- **Vanhoja vakiosopimuslausekkeita voidaan vielä käyttää 27.12.2022 saakka**

Euroopan tietosuojaneuvosto (European Data Protection Board, ”EDPB”) julkisti 21.6.2021 lopulliset omat **suosituksensa** tietosuojaa täydentävistä lisätoimista. Nämä suositukset täydentävät uusia vakiolausekkeita ja niiden tarkoituksena on auttaa yrityksiä toteuttamaan asianmukaisia täydentäviä suojatoimia tarvittaessa. Suositukset annettiin, koska yleinen tietosuoja-asetus ja EU-tuomioistuin eivät kumpikaan määrittele mitä mahdollisesti tarvittavat täydentävät suojatoimet ovat. Suosituksissa kuvaillaan esimerkkien kera prosessi sen arvioimiseksi tarvitaanko suojatoimia ja mitkä suojatoimet olisivat sopivia.

- Tiedonsiirtojen kartoitus
- Arviointi, huomioitava siirron tapauskohtaiset olosuhteet, kyseessä olevan kolmannen maan lainsäädäntö, käytössä oleva siirtoperuste.
- Tietojen viejät ovat vastuussa konkreettisen arvioinnin tekemisestä. Arviointi on myös dokumentoitava huolellisesti.
- Jos käytettyyn siirtoperusteeseen sisältyvät suojatoimet eivät ole sellaisenaan riittäviä, niitä voidaan tietyissä tilanteissa täydentää teknisillä, organisatorisilla tai sopimuspohjaisilla suojatoimilla.

Yksityisensuoja

Varmistamme, että tietosi ovat yksityisiä ja ovat sinun hallinnassasi. Microsoftilla ei ole oletusarvoisesti pääsyä sinun tietoihin.

Asiakas kontrolloi tietojansa

Asiakas päättää, missä tiedot fyysisesti sijaitsevat

Microsoft suojaa tiedot levylla ja siirettäessä verkossa

Microsoft puolustaa tietojasi

Microsoftin uusi tietosuojaliite

- Microsoft on **15.9.2021 julkistanut** uuden pilvipalveluiden **tietosuojaliitteen DPA:n (**Data Processing Addendum). DPA:ssa Microsoft sitoutuu noudattamaan viimeisempiä EU:n tietosuoja-asetuksen ehtoja mahdollisissa GDPR:n alaisien henkilötietojen siirrossa Euroopan talousalueen ulkopuolelle.

- Uudet vakiosopimuslausekkeet sisältävät uusia tiedon suojaamiseen liittyviä menetelmiä

- Microsoft on ottanut käyttöön vakiosopimuslausekkeet ja ne on allekirjoitettu Microsoft Ireland Operations Limited (MIOL), Microsoftin EU-pohjaisena prosessoijana, ja Microsoft Corporation, EU:n ulkopuolisena prosessoijan, välillä.

- Uusi sopimus on **Service Trust -portaalissa** ja se koskee sekä tuotteitamme että ammatillisia palveluitamme (Professional Services). Kun Microsoft allekirjoittaa P2P SCC: t sekä tietojen tuojana että viejänä, Microsoft ottaa lisää vastuuta EU:n velvoitteiden noudattamiseen.

Microsoftin tuotteiden ja palveluiden tietojenkäsittelusopimus

Volyymikäyttöoikeus

Microsoft Products and Services Tietojenkäsittelysopimus

Päivitetty viimeksi 15 syyskuuta 2021

Sisällysluettelo

[Linkki DPA:n]

EU ja USA julkistivat aiesopimuksen 25.3.2022

European Commission - Press release

European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework

Brussels, 25 March 2022

The European Commission and the United States announce that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in the *Schrems II* decision of July 2020.

The new Framework marks an unprecedented commitment on the U.S. side to implement reforms that will strengthen the privacy and civil liberties protections applicable to U.S. signals intelligence activities. Under the Trans-Atlantic Data Privacy Framework, the United States is to put in place new safeguards to ensure that signals surveillance activities are necessary and proportionate in the pursuit of defined national security objectives, establish a two-level independent redress mechanism with binding authority to direct remedial measures, and enhance rigorous and layered oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities.

The Trans-Atlantic Data Privacy Framework reflects more than a year of detailed negotiations between the U.S. and E.U. led by Secretary of Commerce Gina Raimondo and Commissioner for Justice Didier Reynders. It will provide a durable basis for trans-Atlantic data flows, which are critical to protecting citizens' rights and enabling trans-Atlantic commerce in all sectors of the economy, including for small and medium enterprises. By advancing cross-border data flows, the new framework will promote an inclusive digital economy in which all people can participate and in which companies of all sizes from all of our countries can thrive.

The announcement is another demonstration of the strength of the U.S.-EU relationship, in that we continue to deepen our partnership as a community of democracies to ensure both security and respect for privacy and to enable economic opportunities for our companies and citizens. The new Framework will facilitate further U.S.-EU cooperation, including through the Trade and Technology Council and through multilateral fora, such as the Organisation for Economic Cooperation and Development, on digital policies.

The teams of the U.S. Government and the European Commission will now continue their cooperation with a view to translate this arrangement into legal documents that will need to be adopted on both sides to put in place this new Trans-Atlantic Data Privacy Framework. For that purpose, these U.S. commitments will be included in an Executive Order that will form the basis of the Commission's assessment in its future adequacy decision.

Läpinäkyvyys

Kerromme avoimesti prosesseistamme sekä heidän tietojemme käytöstä ja suojauksesta

Näytämme maantieteellisen sijainnin, missä asiakasdata sijaitsee

Julkaisemme viranomaisten tietopyyntöjen lukumäärät

Tarjoamme näkyvyyden miten asiakasdataa käsitellään, miten suojaamme sen ja miten asiakas voi kontrolloida dataansa.

Teemme yhteistyötä kansallisten kyberturvallisuusyksiköiden kanssa ympäri maailmaa tarjotaksemme heille näkyvyyden alustaan, lähdekoodiin ja prosesseihin

Microsoft ei luovuta tietoja viranomaisille

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.

Asiat joihin voisimme vedota oikeudessa:

- Asiakkaan sopimus on Microsoft Ireland Limitted -kanssa
- Eurooppalainen asiakas -> Microsoftin täytyy noudattaa myös asiakkaan maan lakeja
- Data sijaitsee EU-alueella

Katso myös EU-mallisopimuslausekkeet lauseke 15

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

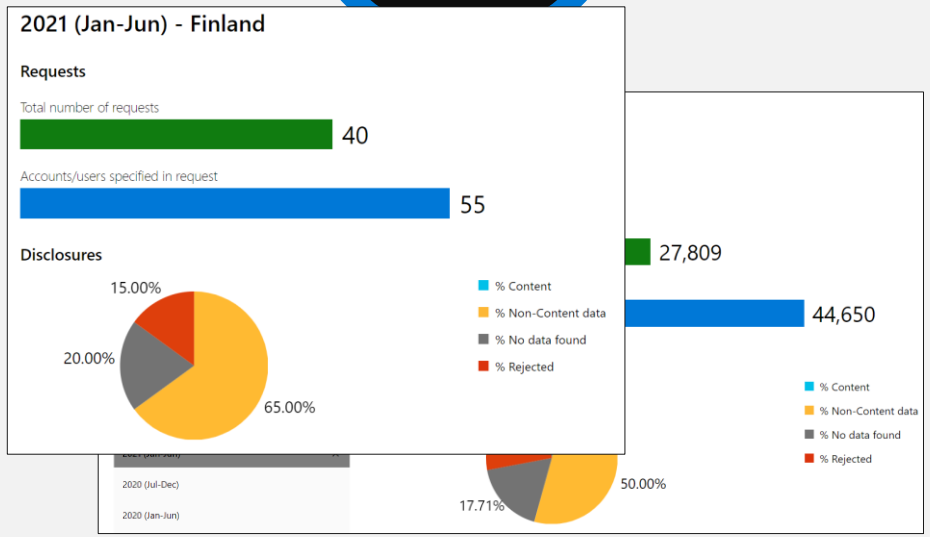
The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to

Viranomaisten tietopyynnöt

Sitoudumme sopimuksellisesti siihen, että emme tarjoa viranomaiselle suoraa pääsyä asiakastietoihin. Jos viranomaiset haluavat päästä tietoihin, sen täytyy tapahtua asianmukaisesti lakeja noudattaen.

1. Uudelleen ohjaus asiakkaalle
2. Lain voimainen pyyntö
3. Ilmoitus



"The Law Enforcement Request Report" julkaistaan puolivuosittain, jossa kerrotaan pyyntöjen yksityiskohdat https://aka.ms/MSLERR

- 01-06/2021: 27 809 pyyntöä, joista 121 pyyntöä valvontaviranomaisilta ympäri maailmaa koski yli 50 henkilön organisaatioita
- 70 tapauksessa nämä pyynnöt hylättiin, 51 tapauksessa jotain tietoa luovutettiin
- Näistä oli 2 pyyntöä US viranomaisilta muiden maiden organisaatoihin

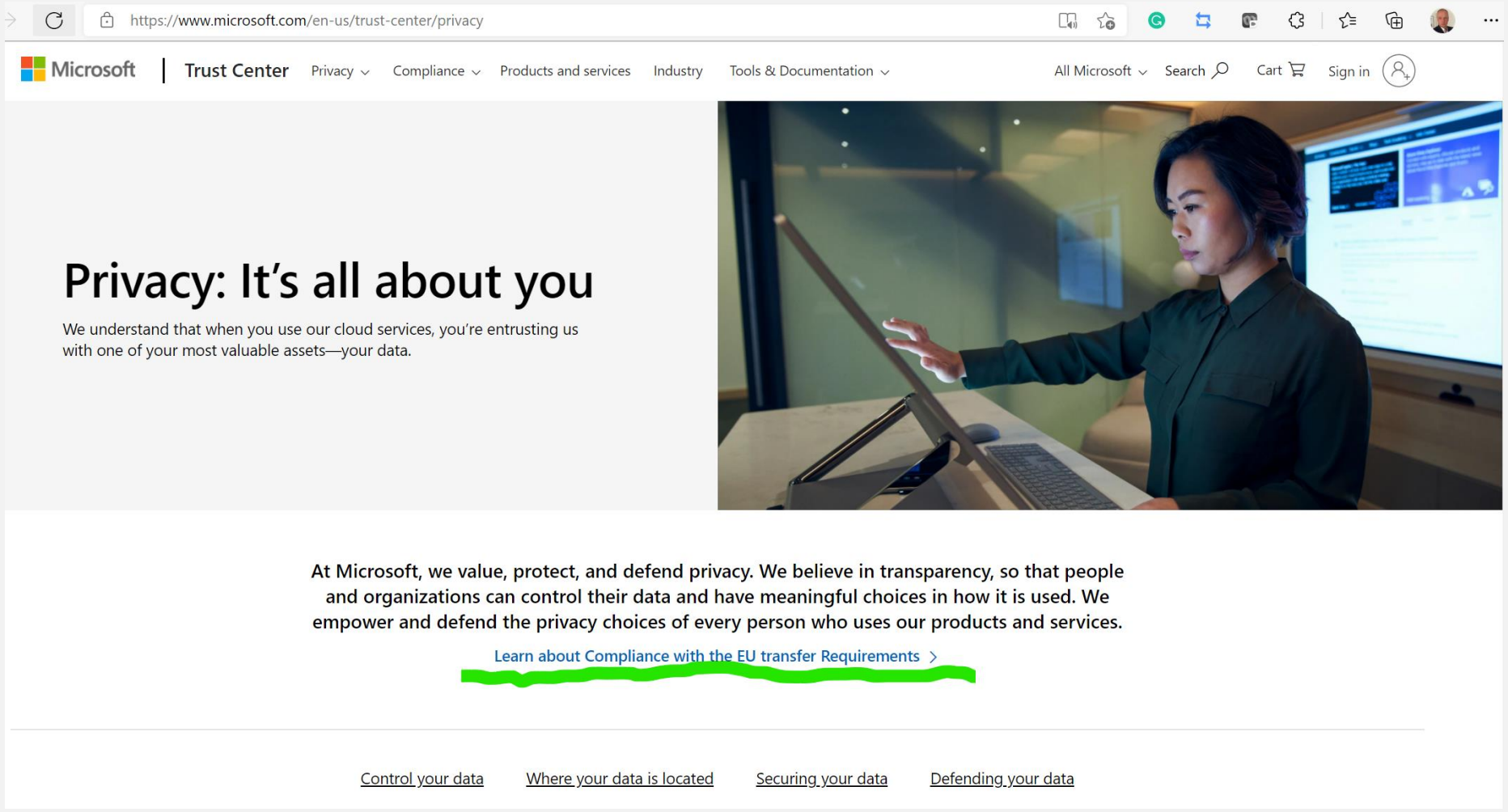
Data Transfer white paper

"Microsoft does **not** provide, and **has never provided**, EU public sector customer's personal data to any government."

"Moreover, outside of the United States, Microsoft does not provide, and has never provided, **EU enterprise customer's** personal to a jurisdiction that was not the same as that in which the **enterprise was located** in respond to government demands for data."

Data Transfer white paper

Nyt saatavissa TrustCenter:stä



Microsoft

Tekniset lisäsuojausmekanismit

Tietoturva

Autamme sinua suojaamaan tietosi

Kehitämme ja ylläpidämme markkinoiden kattavinta tietoturvasympäristöä
Investoimme 20 miljardia $ neljän vuoden aikana kyberturvallisuuteen

Yli 3500 tietoturva-ammattilaista turvaamaan palvelinkeskuksia ja estämään hyökkäyksiä signaalitietokantaa hyödyntäen

2.5 miljardia päivittäistä pilvipalveluiden havaintoa esti lähes 6 miljardia uhkaa asiakkailla vuonna 2020.

Yli 30 miljardia sähköpostin haittaohjelmaa torjuttiin 2020.

Kehitämme ja tarjoamme asiakkaille innovatiivisia lisäturvakontrolleja tietoturvan takaamiseksi.

Tietoturva – datan salaaminen

1. Asiakkaan data käyttäjän ja palveluiden välillä (in transit)

Suojaa käyttäjää viestinnän sieppaukselta ja auttaa varmistamaan tapahtuman eheyden

2. Asiakkaan data datakeskusten välillä (in transit)

Suojaa asiakastietojen joukkokuuntelulta

3. Asiakkaan data tallennettuna (at rest)

Suojaa fyysisen tallennuksen

4. Asiakkaan data muistissa

Suojaa tietoja koneiden muistiin ladattaessa

5. Päästä päähän salaus käyttäjien välillä

Suojaa tietojen kuuntelulta käyttäjien välillä

Microsoft kontrolloima salaus:
https://aka.ms/msazureencryption
https://aka.ms/o365contentencryption

Asiakkaiden kontrolloima salaus:
https://aka.ms/msazureprotection
https://aka.ms/mscloudCMkryptering

Double Key Encryption:
https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption?view=o365-worldwide

Azure– datan salausmekanismit

Azure palveluiden tuki eri avainhallintavaihtoehdoille- https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-models#supporting-services

There are three scenarios for server-side encryption:

Server-side encryption using Service-Managed keys

- Azure Resource Providers perform the encryption and decryption operations
- Microsoft manages the keys
- Full cloud functionality

Server-side encryption using customer-managed keys in Azure Key Vault

- Azure Resource Providers perform the encryption and decryption operations
- Customer controls keys via Azure Key Vault
- Full cloud functionality

Server-side encryption using customer-managed keys on customer-controlled hardware

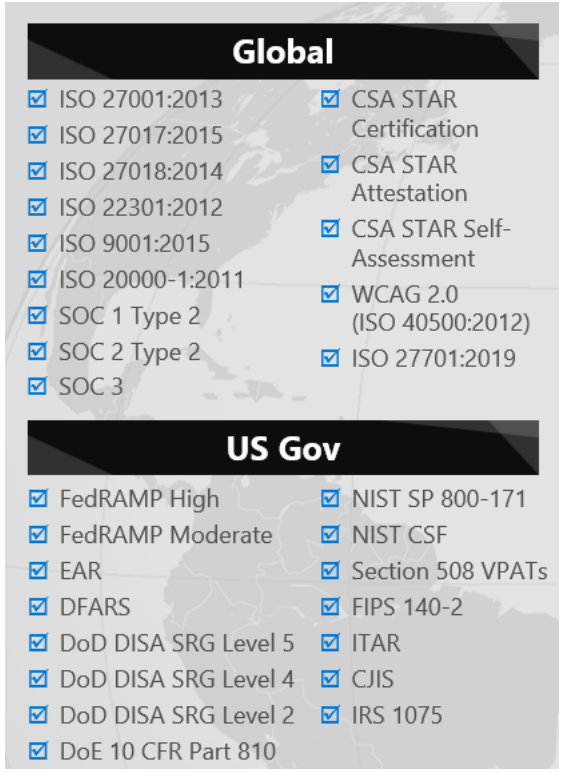
- Azure Resource Providers perform the encryption and decryption operations
- Customer controls keys on customer-controlled hardware
- Full cloud functionality

Supporting services

The Azure services that support each encryption model:

Product, Feature, or Service	Server-Side Using Service-Managed Key	Server-Side Using Customer-Managed Key
AI and Machine Learning		
Azure Cognitive Search	Yes	Yes
Azure Cognitive Services	Yes	Yes
Azure Machine Learning	Yes	Yes
Azure Machine Learning Studio (classic)	Yes	Preview, RSA 2048-bit
Content Moderator	Yes	Yes
Face	Yes	Yes
Language Understanding	Yes	Yes
Personalizer	Yes	Yes
QnA Maker	Yes	Yes
Speech Services	Yes	Yes
Translator Text	Yes	Yes
Power BI	Yes	Yes, RSA 4096-bit

Microsoft pilvipalveluiden sertifioinnit & auditoinnit



Microsoft pilvipalvelut auditoidaan säännöllisesti
- Sertifikaatista riippuen 3 tai vähintää 6kk välein
- Auditoinnit suorittaa ulkopuolinen sertifioitu auditointiorganisaatio (Deloitte, KPMG & Schellman)

Key Vault

Key Vault is a service that allows customers to store and manage passwords and cryptographic keys in a secure manner within the Azure environment. Keys are protected via the use of Thales nShield Hardware Security Modules (HSMs), which are FIPS 140-2 Level 2 compliant under CMVP certificates 2643 and 2121. Customers manage and use the Key Vault service using the Key Vault REST API.

Salausavainten käyttöä voidaan lokittaa ja seurata mihin käytetään [Azure Key Vault logging | Microsoft Docs]

Microsoft

Datan sijainti ja siihen pääsy EU:n ulkopuolelta

Asiakkaille saatavilla olevat tuotekohtaiset “Data Location Maps” -sivustot

We provide information about Microsoft's data location policies and strategies adopted by each Online Service in the Trust Center: Microsoft Privacy - Where is Your Data Located with links to sites with details on data residency and transfer

Azure DevOps Services
Microsoft 365
Microsoft Azure
Microsoft Azure Active Directory
Microsoft Cloud App Security
Microsoft Defender for Endpoint
Microsoft Defender for Identity Personal Data Policy
Microsoft Dynamics 365 for Customer Service
Microsoft Dynamics 365 for Field Service
Microsoft Dynamics 365 for Finance and Operations
Microsoft Intune
Microsoft Power BI
Microsoft Professional Services
Microsoft Threat Protection

Microsoft Azure - pääsy dataan EU ulkopuolelta

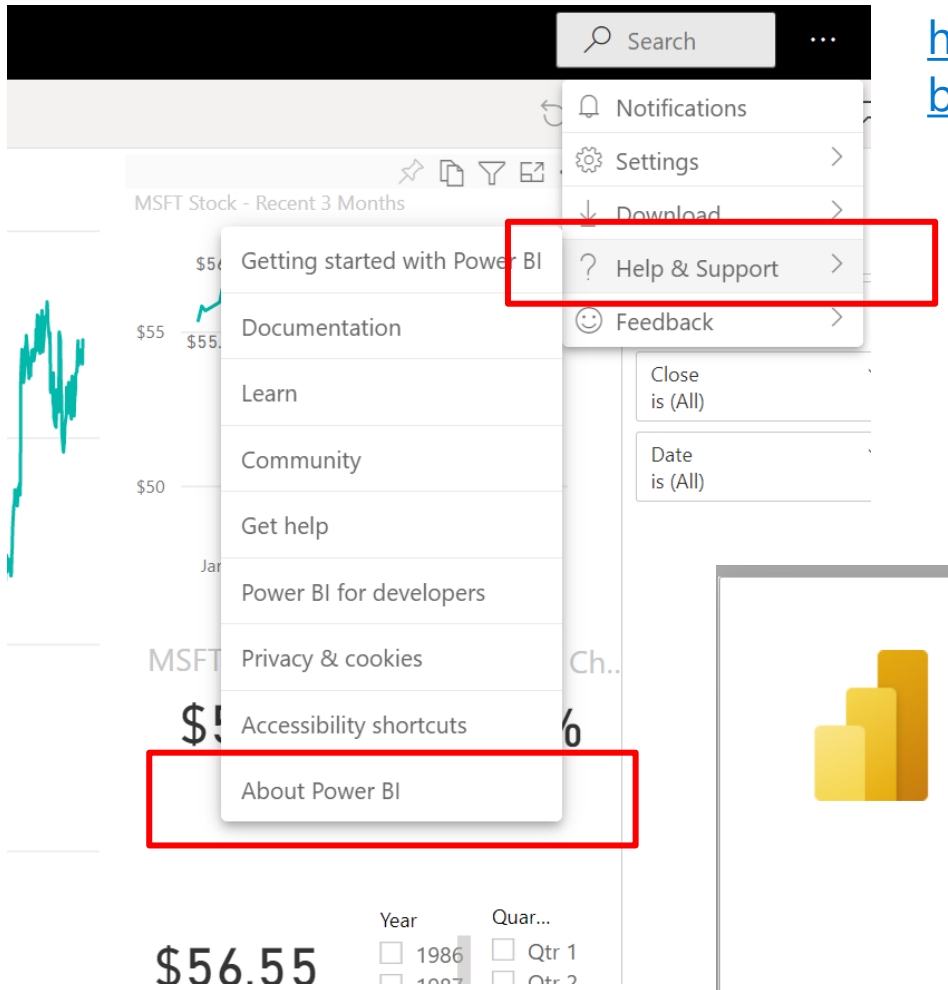
https://azure.microsoft.com/en-us/global-infrastructure/data-residency/#overview

- Microsoft ei tallenna tai käsittele asiakastietoja asiakkaan määrittämän Geon ulkopuolella jos asiakas ei ole itse niin määritellyt tai ratkaisua käytetään EU/ETA –ulkopuolelta
- Asiakas itse päättää, kopioidaanko dataa kahden maantieteellisen alueen välillä tietojen redundanssia tai muita toiminnallisia tarkoituksia varten. Esimerkiksi georedundantti tallennus replikoi Blob-, File-, Queue- ja Table-tiedot kahden alueen välillä samalla Geolla parantaakseen tietojen kestävyyttä palvelinkeskuksen suuren katastrofin sattuessa.

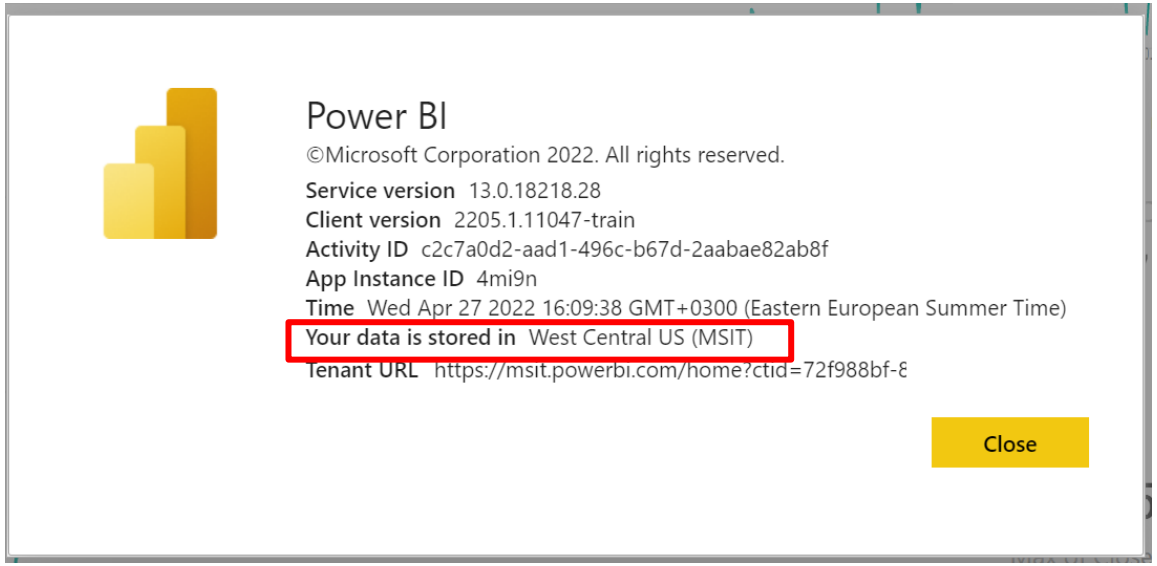
The following services may store or process certain data outside the specified Geo:

- Azure Cloud Services, which backs up web and worker-role software deployment packages to the United States regardless of the deployment region.
- Language Understanding, which may store active learning data in the United States, Europe, or Australia based on the authoring regions which the customer uses. Learn more >
- Azure Machine Learning, may store freeform texts of asset names that the customer provides (such as names for workspaces, names for resource groups, names for experiments, names of files, and names of images) and experiment execution parameters aka experiment metadata in the United States for debugging purposes.
- Azure Databricks, which stores identity data, and certain table names and object path information in the United States.
- Azure Sentine
- Azure Serial Console, which stores all customer data at rest in the Geo selected by customer, but when used through the Azure Portal may process console commands and responses outside of the Geo for the sole purpose of providing the Console experience inside the Portal.
- Azure Purview, which st ain table names, file paths, and object path information in the United States.
- Preview, beta, or other prerelease services, which typically store customer data in the United States but may store it globally.

Microsoft Power BI – datan sijainti



https://docs.microsoft.com/en-us/power-bi/admin/service-admin-where-is-my-tenant-located



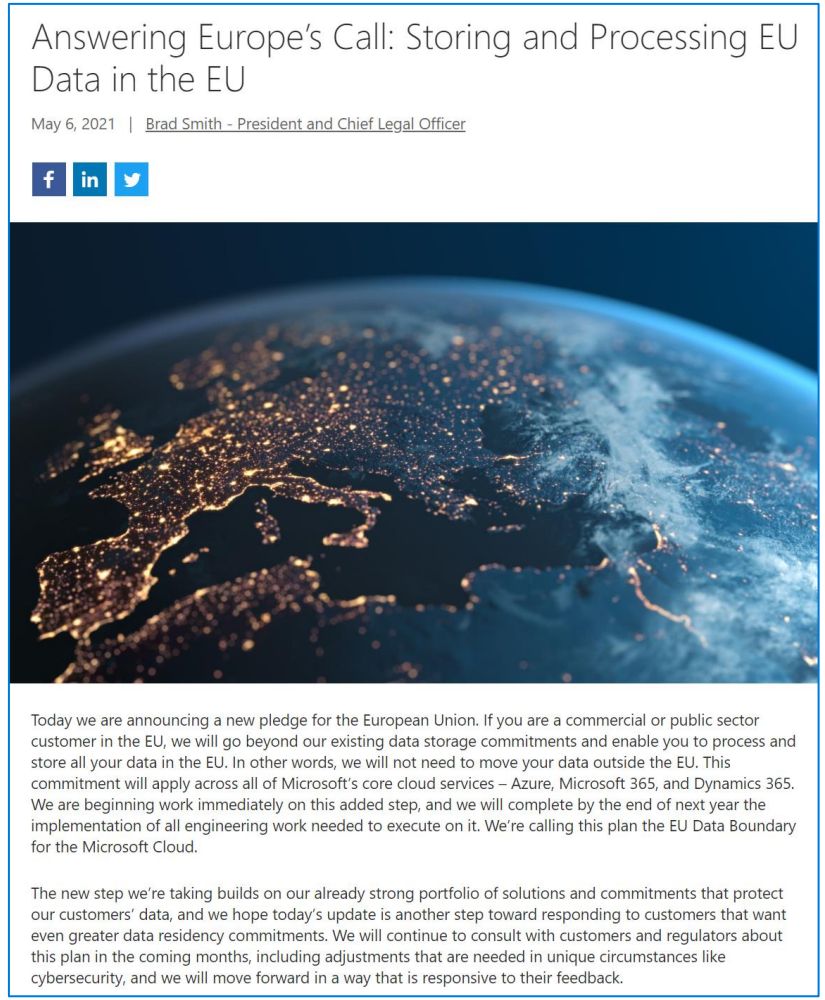
Lupaus uudeksi datan EU-sisärajaksi

Tietojen tallennus ja käsittely:

- *Microsoft tallentaa ja käsittelee EU-alueen asiakkaiden **henkilötietoja** vain EU:n sisällä, mukaan lukien **diagnostiikkatiedot, palveluiden tuottamat tiedot ja tiedot, joita Microsoft käyttää teknisen tuen toimittamiseen***
  - *Kyberturvallisuuteen liittyvät havaintotiedot poikkeus*
- *Tämä sitoumus **koskee kaikkia kolmea pilvipalveluamme - Azurea, Microsoft 365** (mukaan lukien Teams ja OneDrive for Business) ja **Dynamics 365** (mukaan lukien PowerPlatform), sekä niihin liittyviä asiakkaiden tukitoimintoja.*

Asiakaspalvelut ja tuki:

- *Historiallisesti olemme käyttäneet ns. "seuraa aurinkoa" -mallia tukihenkilöstön palvellessa asiakkaita eri aikavyöhykkeiltä.*
- *Jatkossa asiakkaat voivat valita ja käyttää **tukihenkilöstöä, jotka työskentelevät vain EU maissa** tai joiden osalta Euroopan komissio on tehnyt päätöksen riittävästä tietosuojan tasosta.*
- *Poikkeuksena on vakavat ongelmatilanteet, joissa on pakko ottaa tuotekehitysorganisaatiota mukaan ongelman selvittämiseen.*



Answering Europe's Call: Storing and Processing EU Data in the EU

May 6, 2021 | Brad Smith - President and Chief Legal Officer

Today we are announcing a new pledge for the European Union. If you are a commercial or public sector customer in the EU, we will go beyond our existing data storage commitments and enable you to process and store all your data in the EU. In other words, we will not need to move your data outside the EU. This commitment will apply across all of Microsoft's core cloud services – Azure, Microsoft 365, and Dynamics 365. We are beginning work immediately on this added step, and we will complete by the end of next year the implementation of all engineering work needed to execute on it. We're calling this plan the EU Data Boundary for the Microsoft Cloud.

The new step we're taking builds on our already strong portfolio of solutions and commitments that protect our customers' data, and we hope today's update is another step toward responding to customers that want even greater data residency commitments. We will continue to consult with customers and regulators about this plan in the coming months, including adjustments that are needed in unique circumstances like cybersecurity, and we will move forward in a way that is responsive to their feedback.

EU Data Boundary for the Microsoft Cloud

[Answering Europe's Call: Storing and Processing EU Data in the EU - EU Policy Blog (microsoft.com)]

[https://blogs.microsoft.com/eupolicy/2021/12/16/eu-data-boundary-for-the-microsoft-cloud-a-progress-report/]

Findata : Toisiolain muiden palvelutarjoajien tietoturvallinen käyttöympäristö

Uusi versio julkaistu - vaihtoehtoisesti ympäristöt voivat olla pilvipalveluissa

Tietoturvavaatimuksissa on viitattu seuraaviin säännöksiin ja kriteeristöihin:

- Toisiolaki eli laki sosiaali- ja terveystietojen toissijaisesta käytöstä, 552/2019
- KATAKRI 2015 - Tietoturvallisuuden auditointityökalu viranomaisille
    - Suojaustasoja tai turvallisuusluokkia ei huomioida arvioinnissa vaan sovellettavat KATAKRI-vaatimukset ovat ilmoitettu arvioitavan kohteen vaatimusten yhteydessä.
- PiTuKri versio 1.1. maaliskuu 2020 - Pilvipalveluiden turvallisuuden arviointikriteeristö
    - Arviointilaitoksella on mahdollisuus perustaa arviointi PiTuKrin vaatimuksiin KATAKRI:n sijaan kohdissa, joissa se arvioitavan kohteen osalta on tarkoituksenmukaista.

https://www.mediuutiset.fi/kumppanisisallot/microsoft/huippumoderni-tietoturvasertifioitu-tutkimusymparisto-mahdollistaa-entista-laajemman-terveystutkimuksen/

Huippumoderni tietoturvasertifioitu tutkimusympäristö mahdollistaa entistä laajemman terveystutkimuksen

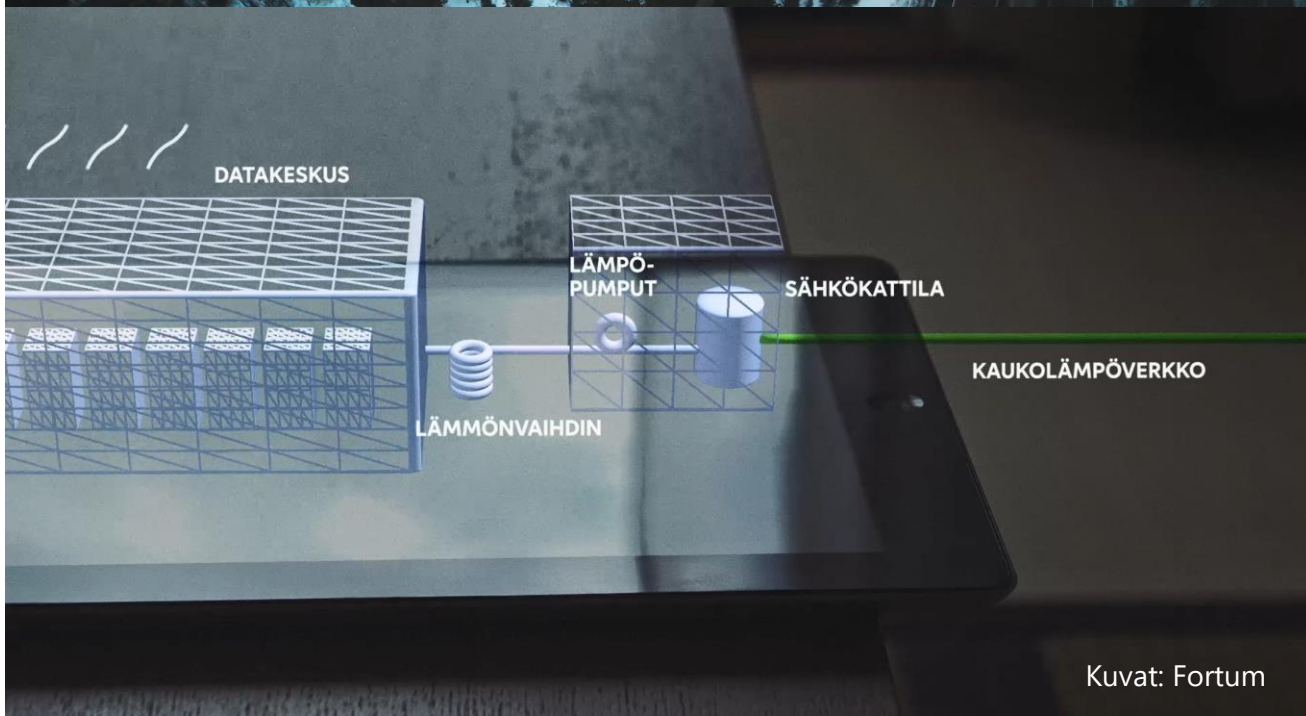
Microsoft

Kestävää digitalisaatiota vauhdittamassa

Datakeskus julkistus

Datakeskukset on suunniteltu toimimaan **sataprosenttisesti päästöttömällä energialla** ja yhteistyömme kautta energiayhtiö Fortum tulee kierrättämään datakeskusten palvelimien jäähdytyksestä syntyvän hukkalämmön **kaukolämmöksi Espoossa, Kauniaisissa ja Kirkkonummella.**

Valmistuessaan datakeskukset vähentävät Suomen vuotuisia hiilidioksidipäästöjä **400 000** tonnilla.



Kuvat: Fortum

Datakeskusalue (Cloud Region) koostuu useista **datakeskuksista**, jotka tulevat sijaitsemaan läntisellä Uudellamaalla.

Kussakin datakeskuksessa on **useita erillisiä konesaleja**.

Kestävän digitalisaation hyödyt

Vihreään energiaan siirtyminen Suomessa vauhdittuu.

Datakeskukset hyödyntävät 100% päästötöntä energiaa.

Hukkalämpö kattaa 40% Espoon, Kauniaisten ja Kirkkonummen noin 250 000 kaukolämmön käyttäjän lämmöntarpeesta.

Suomen vuotuiset hiilidioksidipäästöt vähenevät arviolta noin 400 000 tonnilla.

"Kaikki voittavat päätöksessä investoida datakeskukseen, joka myös tuottaa lämpöä kaupungeillemme ja koteihimme. Se nopeuttaa Suomen digitaalista kasvua ja samalla puhdistaa energiajärjestelmäämme. Toivon, että tämä yhteistyö näyttää mallia muille maille ja kaupungeille, jotka etsivät keinoja yhdistää siirtymän ilmastoneutraaliuteen ja digitaalisen kilpailukyvyn," sanoo **pääministeri Sanna Marin.**

Microsoft ja Fortum yhteistyöhön – Microsoft rakentaa Suomeen datakeskusalueen, joka tuottaa päästötöntä kaukolämpöä Fortumin asiakkaille pääkaupunkiseudulla – Uutishuone

Lisätietoja

Lehdistötiedotteet

- Globaali lehdistötiedote
- Suomenkielinen lehdistötiedote

Asiakkaiden sitaatit

- Microsoftin asiakkaat ja kumppanit tukevat uutta datakeskushanketta – Uutishuone

Sivusto paikallisille yhteisöille

- Datakeskusalue Suomi | Microsoft in your community

Virtuaalinen lehdistötilaisuus

- Katso tallenne täällä

Kiitos!!

Juha.Karppinen@microsoft.com
050 379 9637
Juha Karppinen | LinkedIn

Microsoft

Microsoftin kestävän kehityksen ohjelma

Oppeja Microsoftin kestävän kehityksen matkalta

Pivipalveluihin siirtyminen
vähentää hiilidioksiidipäästöjä

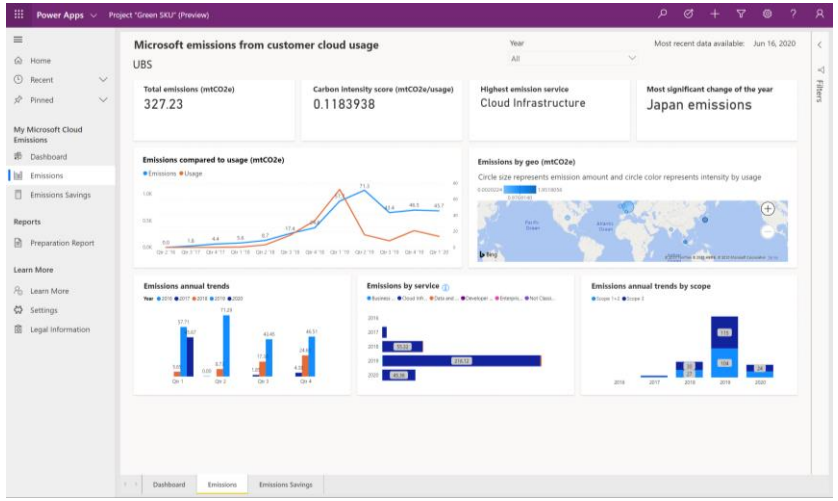
Microsoftin sisäisellä “Hiilimaksulla”
rahoitetaan innovaatioita
ja se ohjaa organisaatiotamme oikeaan toimintaan

Älykkäät rakennukset auttoivat vähentämään energiankulutusta jopa 20%

Älykäs veden käytön seuranta
vähentää veden kulutusta

Lopetaan muovin käyttö kaikessa pakkaamisessa

Ymmärrä päästösi verattuna Microsoftin pilvipalveluihin – Emission Impact Dashboard



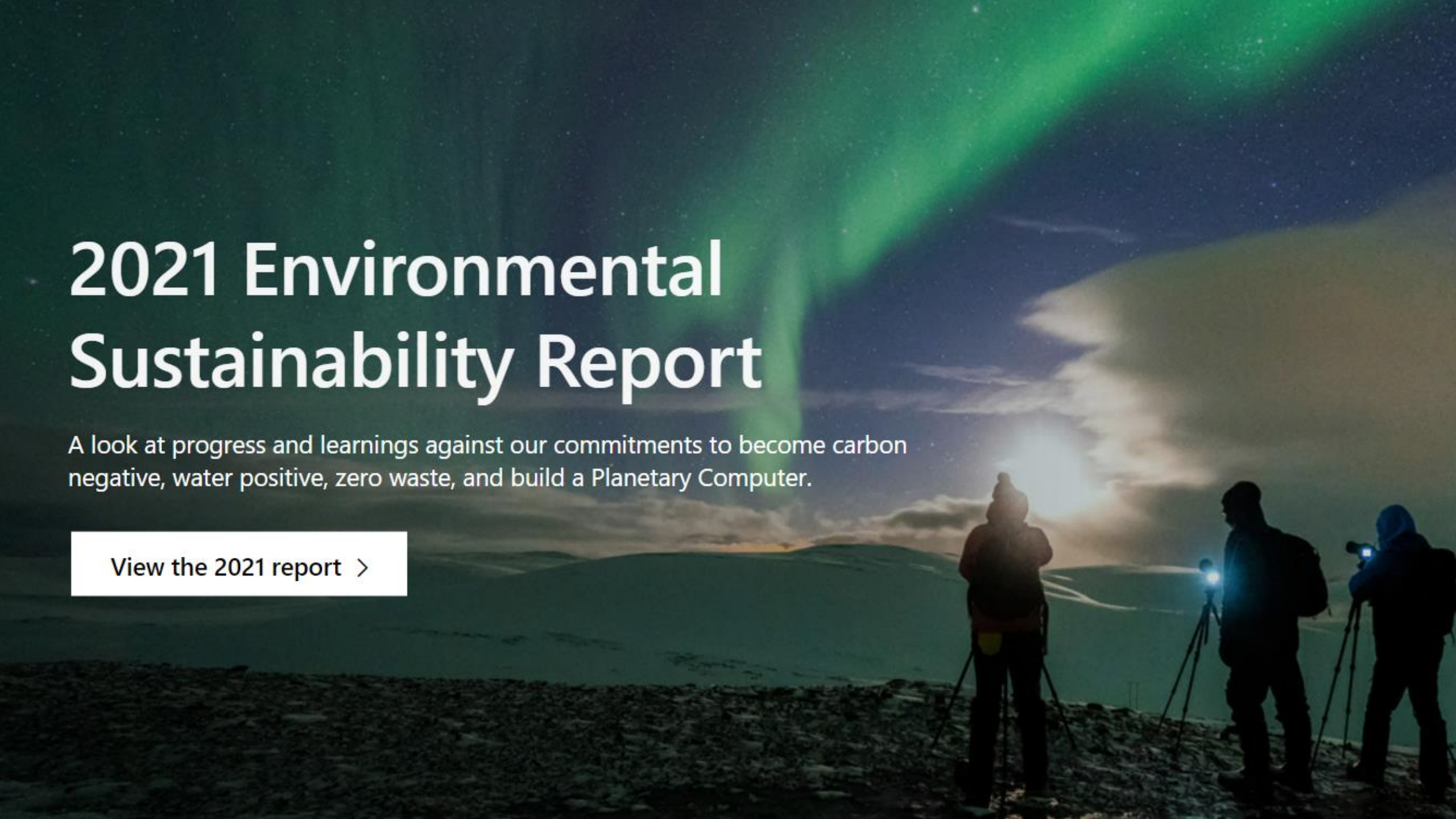
[Microsoft Sustainability Calculator >]

Visualize greenhouse gas emissions associated with your Dynamics 365 and Azure cloud usage

Learn the root cause of emissions changes

Measure impact on your carbon footprint

Calculate how to further reduce emissions


2021 Environmental Sustainability Report
A look at progress and learnings against our commitments to become carbon negative, water positive, zero waste, and build a Planetary Computer.
View the 2021 report >

Pilvi, johon voit luottaa

Asiakkaan luottamus ei ole itsestäänselvyys

Olemme sitoutuneet suojaamaan asiakkaidemme tiedot.

Noudatamme standardeja, lakeja ja asetuksia.

Rakennamme luottamusta toimimalla yhteistyössä toimialojen ja regulaattorien kanssa.

"Käyttäjät arvostavat vain teknologiaa, johon he voivat luottaa."

– Satya Nadella