Learning Path Compliance and Privacy

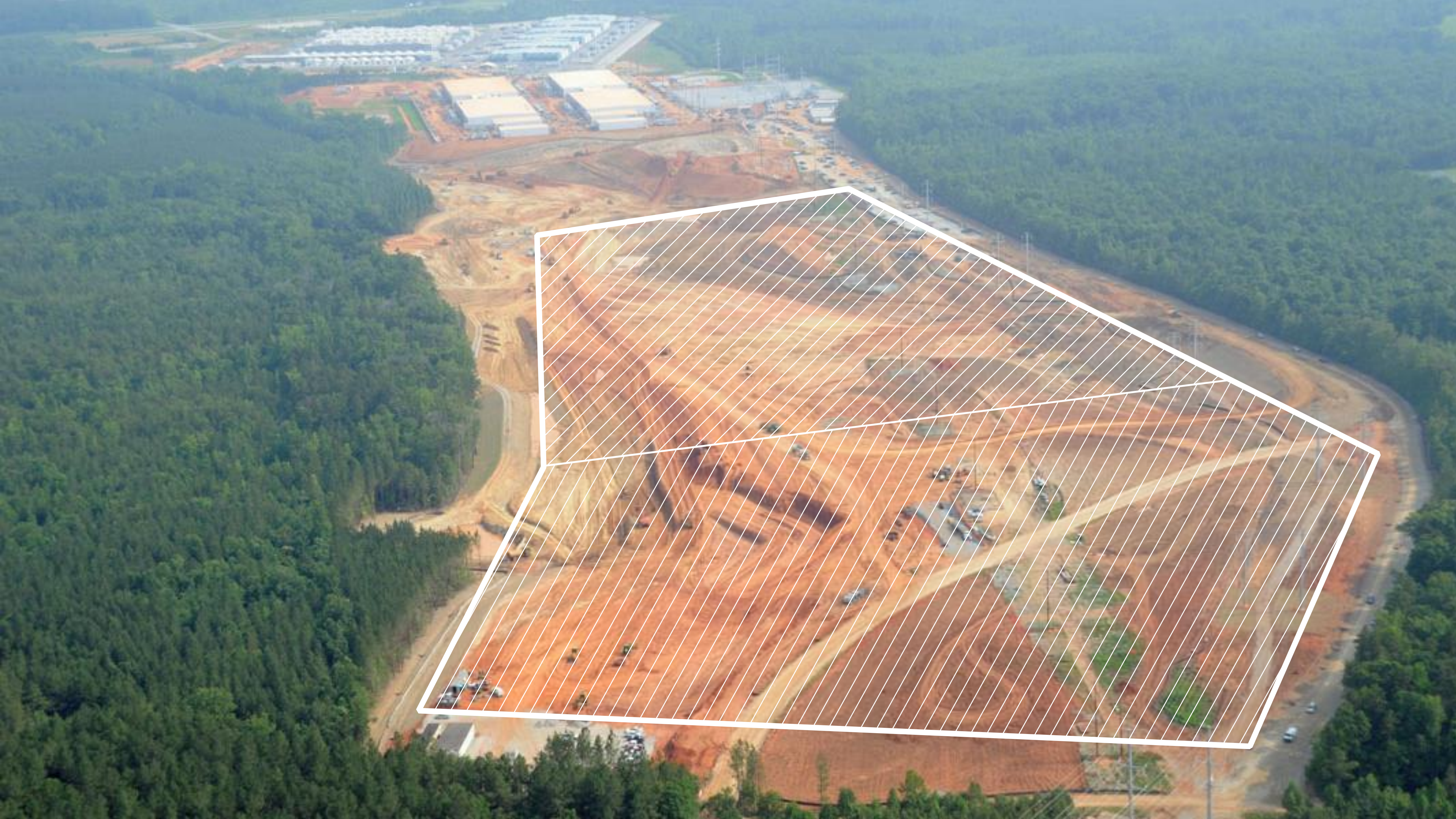
Addressing Compliance and Privacy - Fundamentals

Daniel von Büren; Technical Specialist Security & Compliance
29.10.2021

Agenda

- Hyperscale Cloud
- Microsoft Datacenter
- Data Protection – Contracts

Hyperscale Cloud



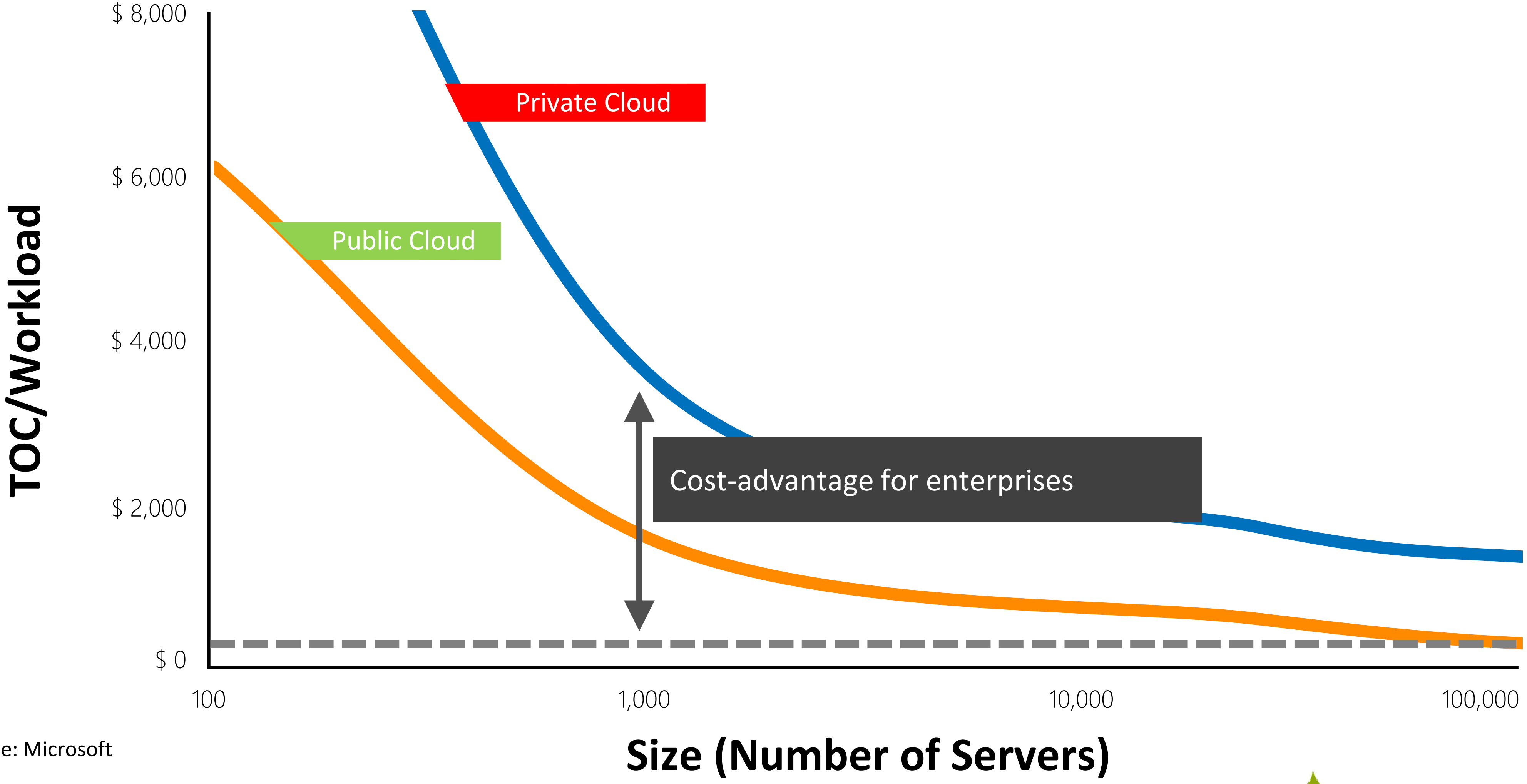
Hyperscale Cloud

Evolving services to hyper-scale requires a radical restructuring of technology, processes, and people

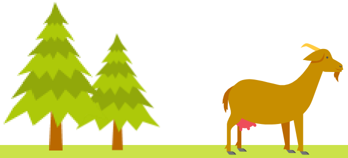
	Enterprise IT		Hyper-Scale
Seats	10,000	→	1,000,000,000
Talent	Custodians	→	Designers
Data Quality	Directional	→	Foundational
Data Access	Pull	→	Push
Assessment	Physical	→	Statistical
Supply Chain	Process	→	Strategic
Budget	Fixed Cost	→	Rates
Architecture	Siloed	→	Integrated
Application integration	Loose	→	Tight
Infrastructure	Overhead	→	Enabler
Reach	Regional	→	Global

	Enterprise IT		Hyper-Scale
Hardware	Custom	→	Commodity
Deployment	Manual	→	Automated
Availability	Infrastructure	→	Service
Operability	MTBF	→	MTTR
Reliability	Hardware	→	Software
Security	Audit	→	Intrinsic
Network downtime	Impacting	→	Irrelevant
Network availability	99.999%	→	99.9%
Design	Primary/Backup	→	Active/Active
Deployment time	Weeks	→	Minutes
System admin	UI	→	API

Economies of Scale



Source: Microsoft

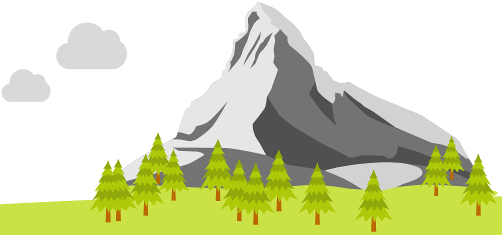


Hyperscale Cloud

If it is

a standardized service,
with **a standardized contract**
and **multitenant**

then – and only then - **it is a Hyperscale cloud**.



Microsoft Datacenter

Facts & Figures

Trusted Cloud Principles

A set of foundational beliefs that guide the way we do business in the cloud

Security

Strong security protects data and safeguards from hackers and unauthorized access by using state-of-the-industry technology, processes, and certifications.

Privacy & Control

Customers control their data, as well as permissions. They can always access their data, take it with them when they terminate an agreement, and delete it upon request.

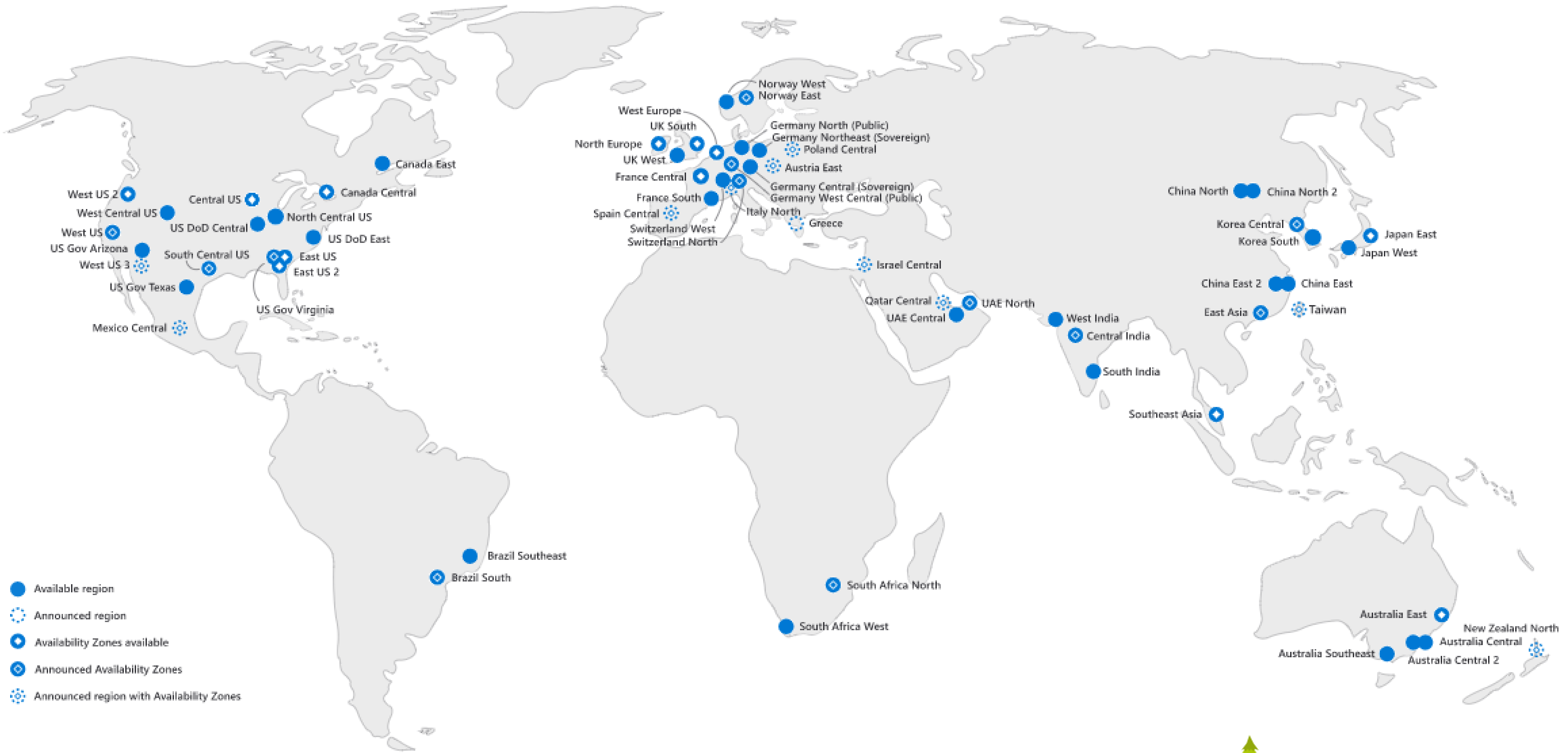
Compliance

Customers can store and manage their data in compliance with their obligations, applicable laws, regulations, and key international standards.

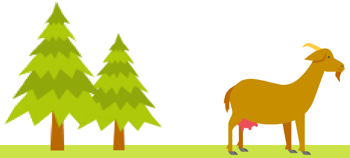
Transparency

Customers know what is happening with their data. Microsoft explains in clear, plain language how the cloud provider uses, manages, and secures data.

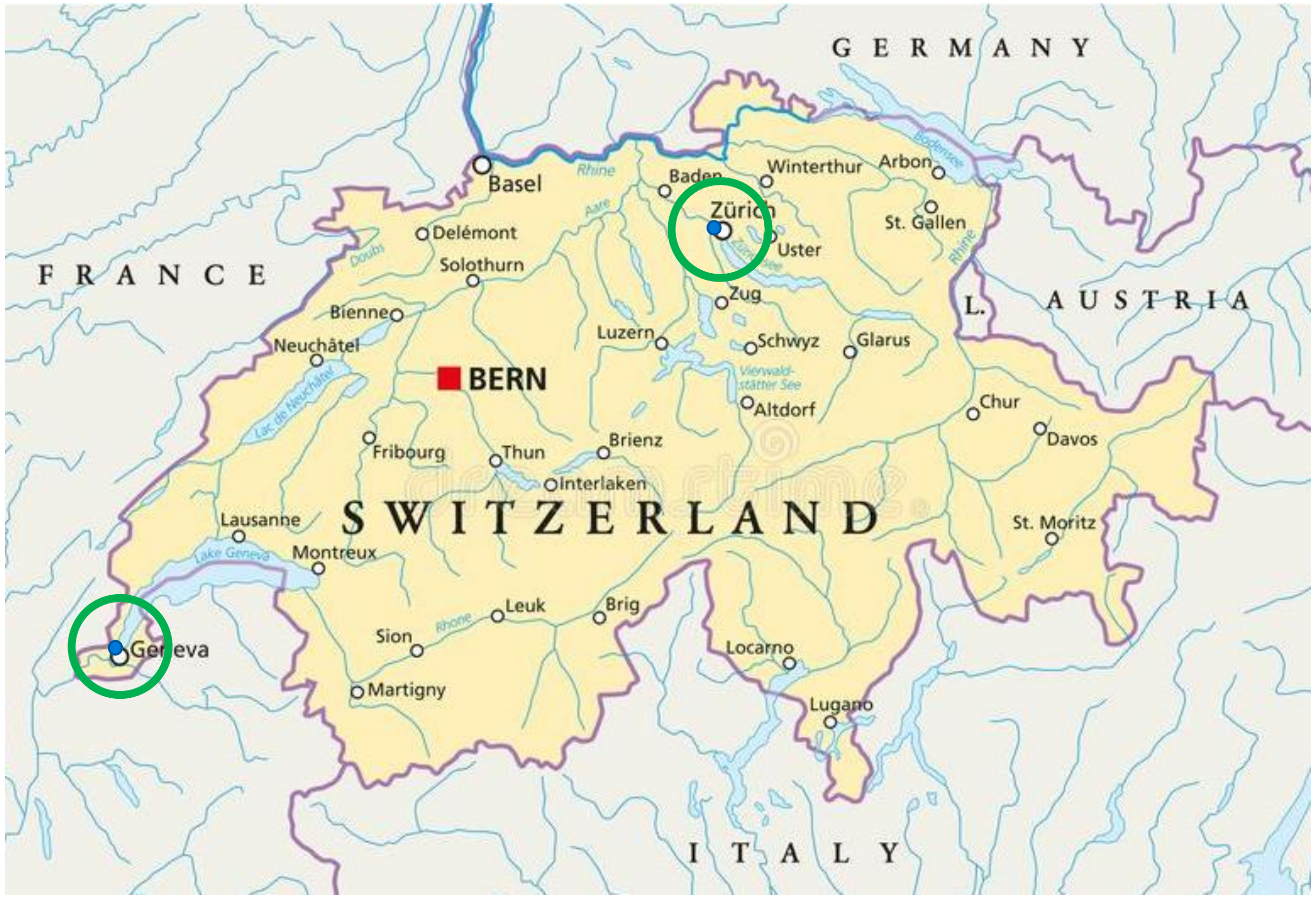
Azure Regions



Source: https://infrastructuremap.microsoft.com/explore



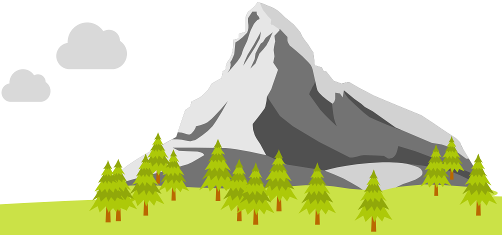
Microsoft Cloud in Switzerland



Compliance

Data Residency

Performance



Data Locations

Office 365

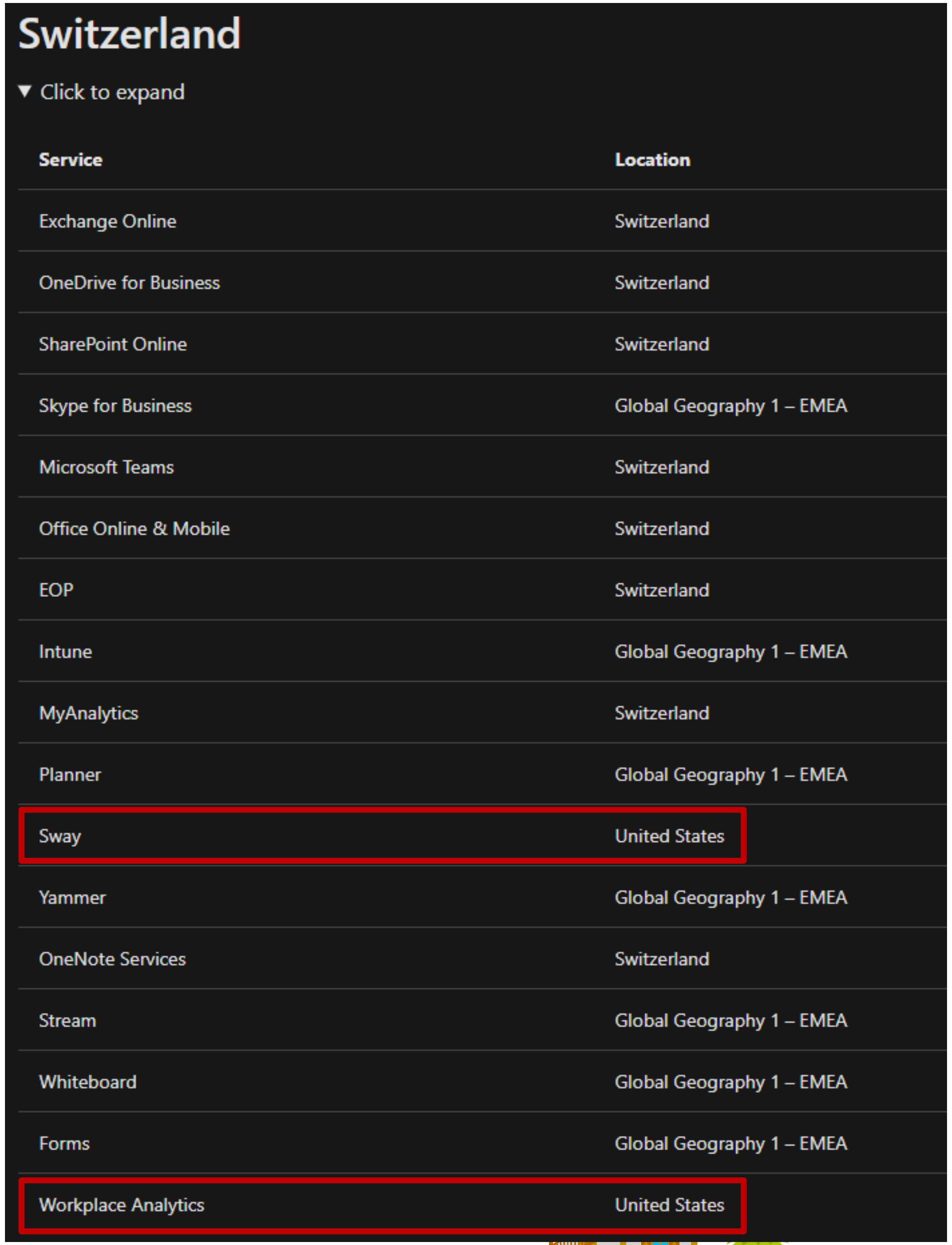
- Location of O365 tenant defines location of O365 online services
- Not all services are available in Switzerland!
- Multi-Geo to meet data residency requirements

Sources: Microsoft O365 Data Locations
Microsoft 365 Multi-Geo

Azure

- Location defined by service
- Multiple locations are possible (e.g. CH for critical data; US for non-critical data)
- Not all services are available everywhere!
- Some Services are Non-Regional!

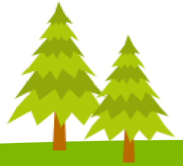
Sources: Azure Products by Region



Switzerland

▼ Click to expand

Service	Location
Exchange Online	Switzerland
OneDrive for Business	Switzerland
SharePoint Online	Switzerland
Skype for Business	Global Geography 1 – EMEA
Microsoft Teams	Switzerland
Office Online & Mobile	Switzerland
EOP	Switzerland
Intune	Global Geography 1 – EMEA
MyAnalytics	Switzerland
Planner	Global Geography 1 – EMEA
Sway	United States
Yammer	Global Geography 1 – EMEA
OneNote Services	Switzerland
Stream	Global Geography 1 – EMEA
Whiteboard	Global Geography 1 – EMEA
Forms	Global Geography 1 – EMEA
Workplace Analytics	United States



Spotlight

- Who has access to data? How can I determine if and how the data is accessed? / Can you explain the data flows…

  Approach:

  - Identify the services you need
  - Clarify if data in those services are critical (e.g. personal data)
  - Focus on the critical services to identify which data goes where
  - → in most situations, this would help to answer the critical questions, without "boil the ocean"

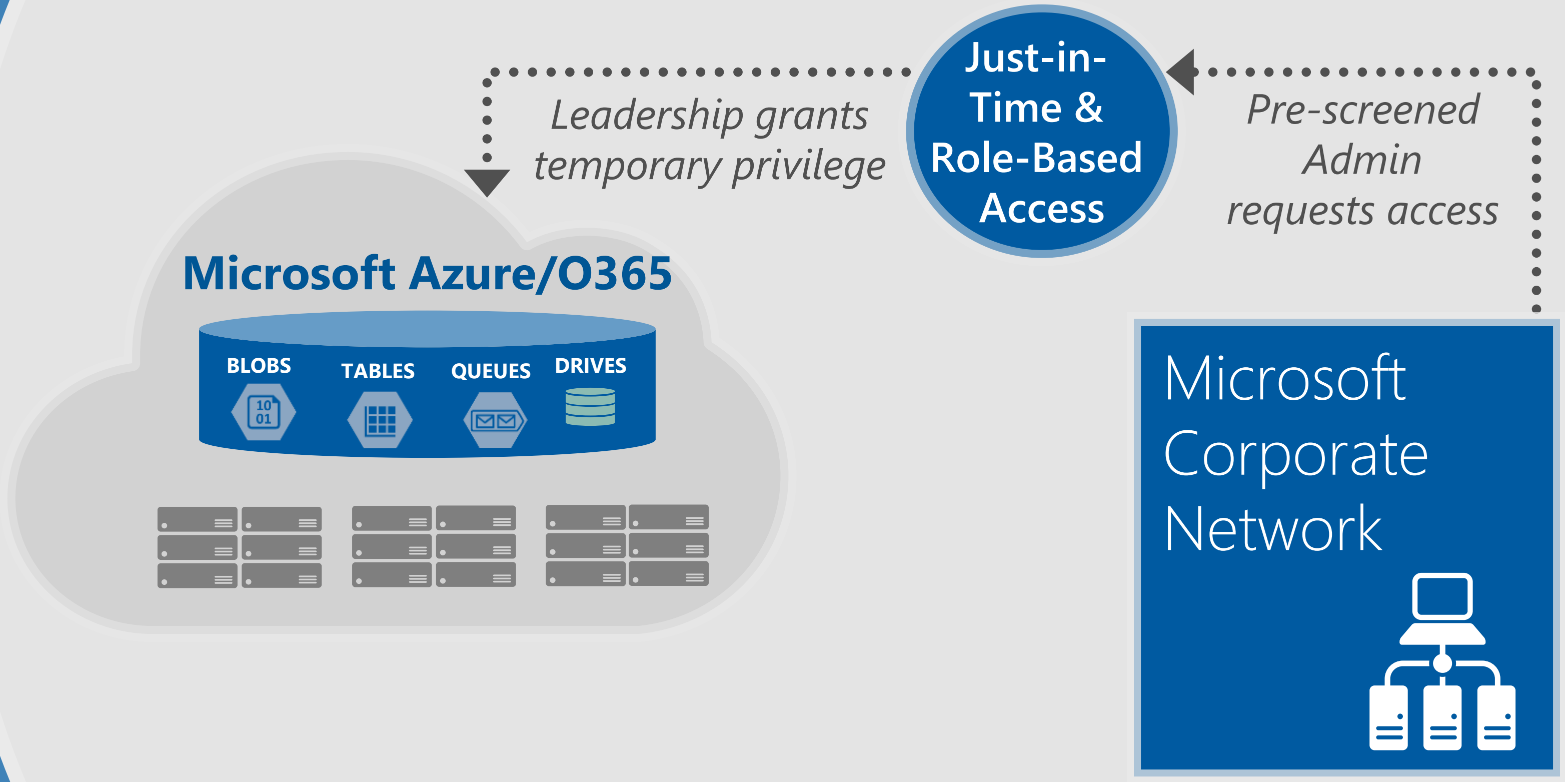
Microsoft Employees Access Management

No standing access to the customer data

Grants least privilege required to complete task

Multi-factor authentication required for all administration

Access requests are audited, logged, and reviewed



Leadership grants temporary privilege

Just-in-Time & Role-Based Access

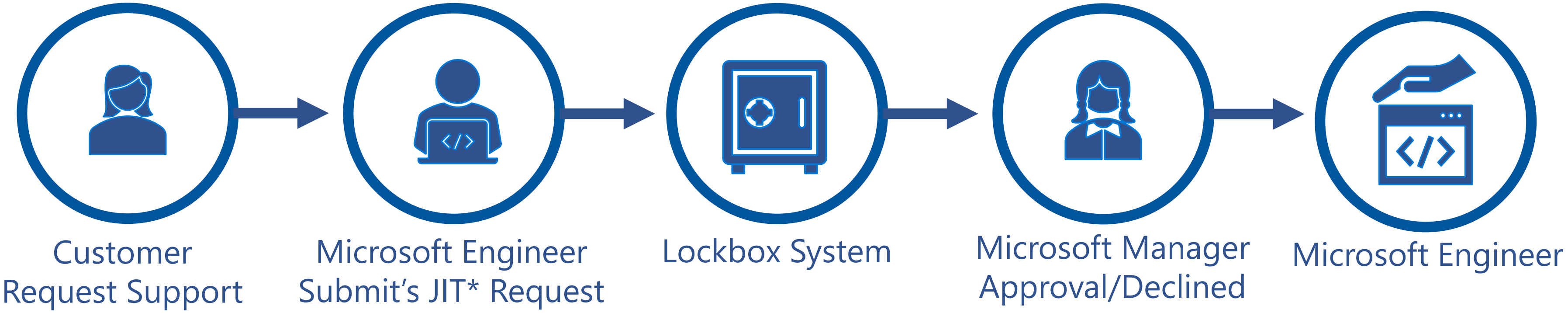
Pre-screened Admin requests access

Microsoft Azure/O365

Microsoft Corporate Network

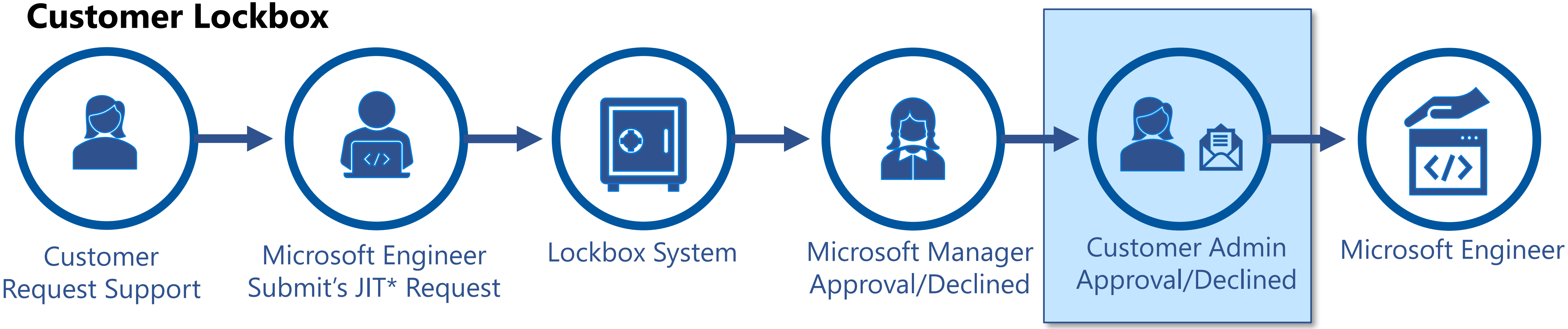
Access Management – Lockbox Process

Standard Lockbox



Customer Request Support → Microsoft Engineer Submit’s JIT* Request → Lockbox System → Microsoft Manager Approval/Declined → Microsoft Engineer

Customer Lockbox



Customer Request Support → Microsoft Engineer Submit’s JIT* Request → Lockbox System → Microsoft Manager Approval/Declined → Customer Admin Approval/Declined → Microsoft Engineer

*JIT – Just-in-Time

Compliance Framework

Regulation

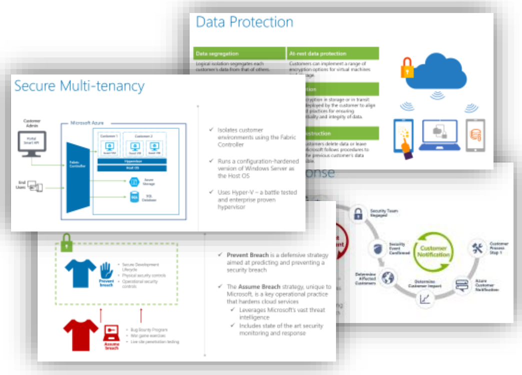
Product Terms

General and specific regulations about all relevant topics (e.g. data handling, security,…) between customer and Microsoft.

Implementation

Technical and Organizational Measures (TOM)

TrustCenter and DOCS provides all details:



Control-framework

Ensure successful implementation of TOM’s

40+ global, industry or regional certifycations:

ISO
ISO 27001 Certified
NIST
AICPA SOC
PCI Security Standards Council
cloud security alliance CSA
enisa
European Commission
HIPAA
GOV.UK

Reporting

Audit reporting

Regularly independent audits per service.
Audit reports would be published on TrustCenter to all customers including all details (full transparency).

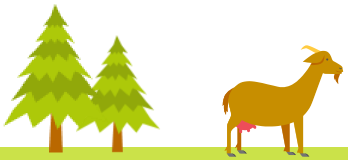
Data Protection - Contracts

How Microsoft supports Data Protection within Contracts

Data Protection in Product Terms

- All data protection topics are handled in the Data Protection Addendum (DPA), which is an integrated part of the Product Terms
- The Product Terms includes general and specific terms about the online services
- The Product Terms (and the DPA) may change on a monthly basis! For customers, the signed contract keeps valid over the whole contract period.
  Customers can adapt the most current contract by requesting an addendum via their licensing partner.
- Topics included in the DPA:
  - Scope
  - Nature of Data Processing; Ownership
  - Disclosure of Processed Data
  - Processing of Personal Data; GDPR
  - Data Security
  - Security Incident Notification
  - Data Transfers and Location
  - Data Retention and Deletion
  - Processor Confidentiality Commitment
  - Notice and Controls on use of Subprocessors
  - Educational Institutions
  - CJIS Customer Agreement
  - HIPAA Business Associate
  - California Consumer Privacy Act (CCPA)
  - Biometric Data
  - Supplemental Professional Services
  - How to Contact Microsoft
  - Appendix A – Security Measures
  - Appendix B – Data Subjects and Categories of Personal Data
  - Appendix C – Additional Safeguards Addendum.

Source: https://aka.ms/dpa



- How is the data deleted after I left the service?
  - DPA – “Data Retention and Deletion”
  - After expiration or termination of a subscription, data remains stored in the online service in a limit function account for 90 days. During this time customer can export his data. After the 90-day retention time, Microsoft will disable Customer’s account and will delete customer data and personal data within an additional 90 days.

- Exit planning
  - Document “Exit Planning for Microsoft Cloud Services.pdf” is available on Service Trust Portal

Spotlight

- Right to audit
  - DPA – "Auditing Compliance"
  - Microsoft will audit his services by independent regulator on a regular basis and publishes the audit reports
  - If those reports are not enough, Microsoft is open to answer specific questions
  - If this still not fulfills the needs of the customer, he may be able to engage an auditor to audit the service
- How are subcontractors selected
  - DPA – "Notice and Controls on use of Subprocessors"
  - Announcing changes 6 month (customer data) / 30 days (personal data, but not customer data) in advance
  - Customer can terminate any subscription without penalties when he would not agree
  - List of subcontractors is published on the Service Trust Portal

Spotlight

- What happens if there is a security incident
  - DPA – “Security Incident Notification”
  - Microsoft promptly notify customer about the security incident
  - Microsoft will investigate the security incident and provide customer with detailed information
  - Microsoft will take reasonable steps to mitigate any damage resulting from the security incident
  - Notification would be done via service portal and/or via email
- What are the Service Level Agreements (SLA)
  - Document wit the SLA’s for Microsoft online services can be downloaded on https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services

Cloud Act

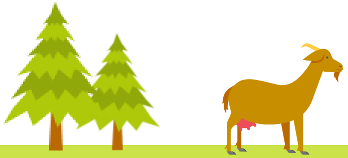
There is a lot of noise and misunderstanding about the Cloud Act…

Cloud Act – what is it:

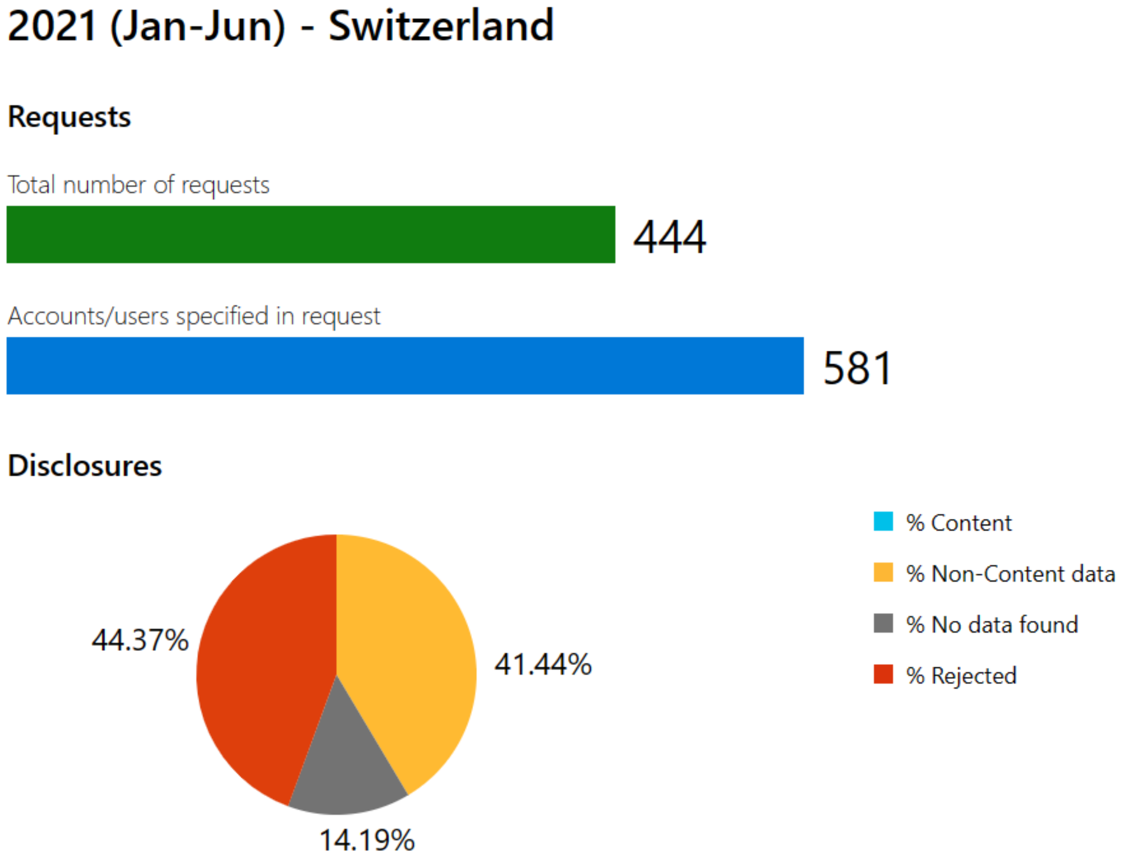
- It’s a regulation how the government of the US can access data abroad, handled by an American company
- But…
  - There is the need of a lawsuit supported by a US court
  - It must be clear what kind of data, from whom and when
  - There is no embargo to inform the customer about the request – and yes, we will do that immediately
  - Disclose data
    - We need to disclose data when it’s about a US citizen
    - We do not have to disclose data when it conflict with the local data protection law

Don’t get me wrong – the Cloud Act must be considered in a risk assessment, but in most cases the probability would be very low.

Source: US CLOUD Act: Why it should not prevent cloud projects – VISCHER
Bericht zum US CLOUD Act (admin.ch)



How Microsoft handles Law Enforcement Requests

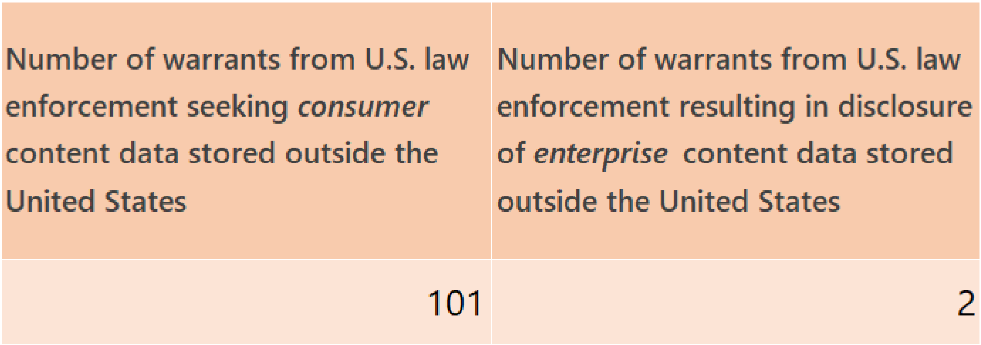


2021 (Jan-Jun) - Switzerland

Requests

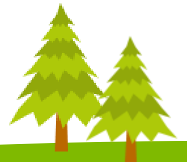
Disclosures

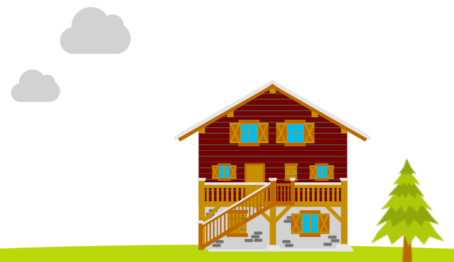
All law enforcement request for Switzerland
(incl. consumer & enterprise customers)



Number of warrants from U.S. law enforcement seeking *consumer* content data stored outside the United States	Number of warrants from U.S. law enforcement resulting in disclosure of *enterprise* content data stored outside the United States
101	2

Globally law enforcement requests based on Cloud Act





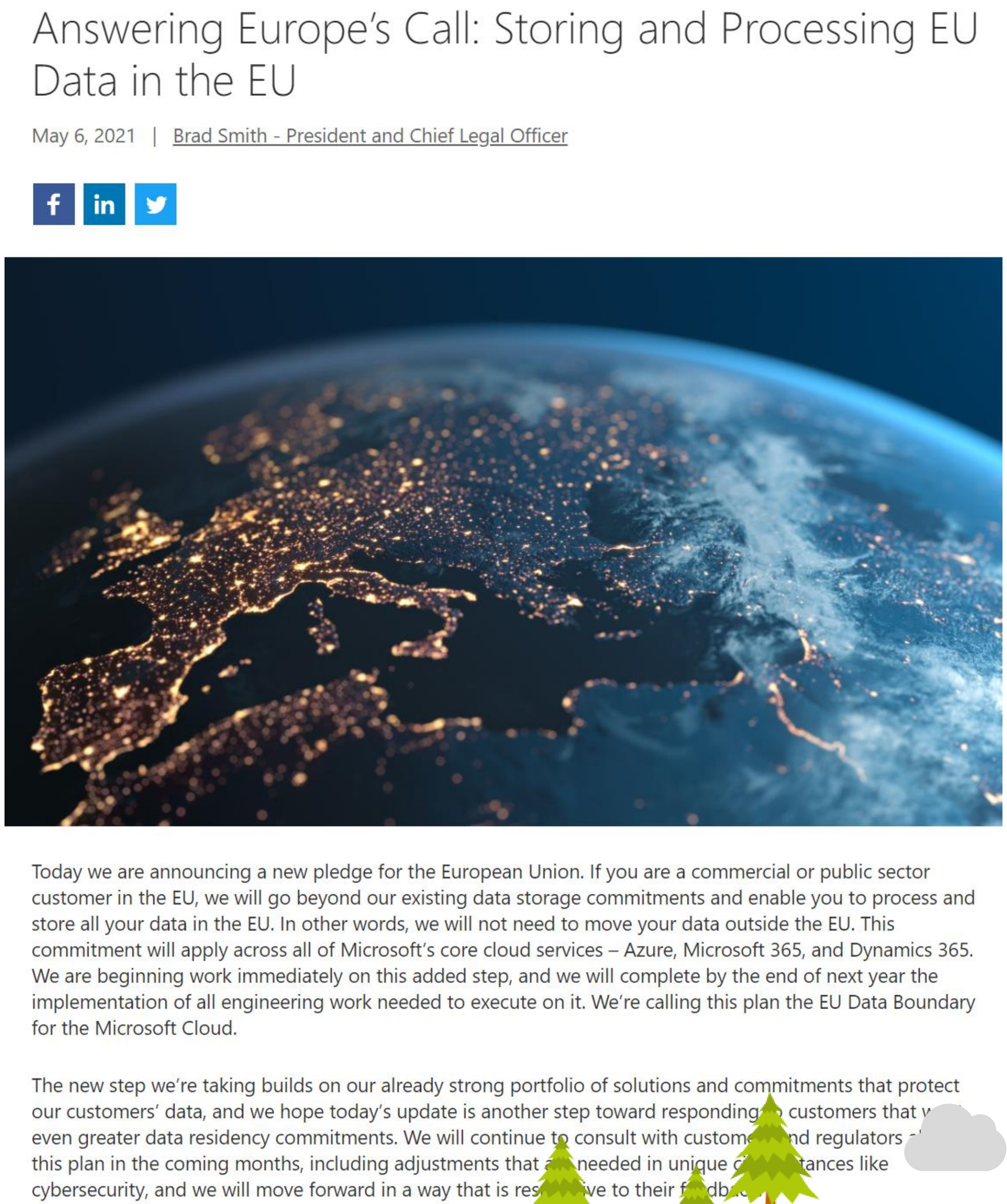
Source: Law Enforcement Request Report | Microsoft CSR

EU Data Boundary

Data storage and processing:

- *For all commercial and public-sector customers located in our new EU Data Boundary, Microsoft will store and process the customers' personal data in the EU Data Boundary by the end of 2022, including diagnostic data, service-generated data and the data Microsoft uses to provide technical support*
- *This strengthens and extends our current commitments around data in transit and at rest*
- *This commitment will apply to each of our three main cloud services – Azure, Microsoft 365 (including Teams and OneDrive for Business) and Dynamics 365 (including Power Platform), as well as associated customer support operations*
- *There may be a small number of instances where a particular additional feature still requires the transfer of data outside the EU Data Boundary. We will provide customers choices over whether to enable those features*

https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/



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.

Microsoft