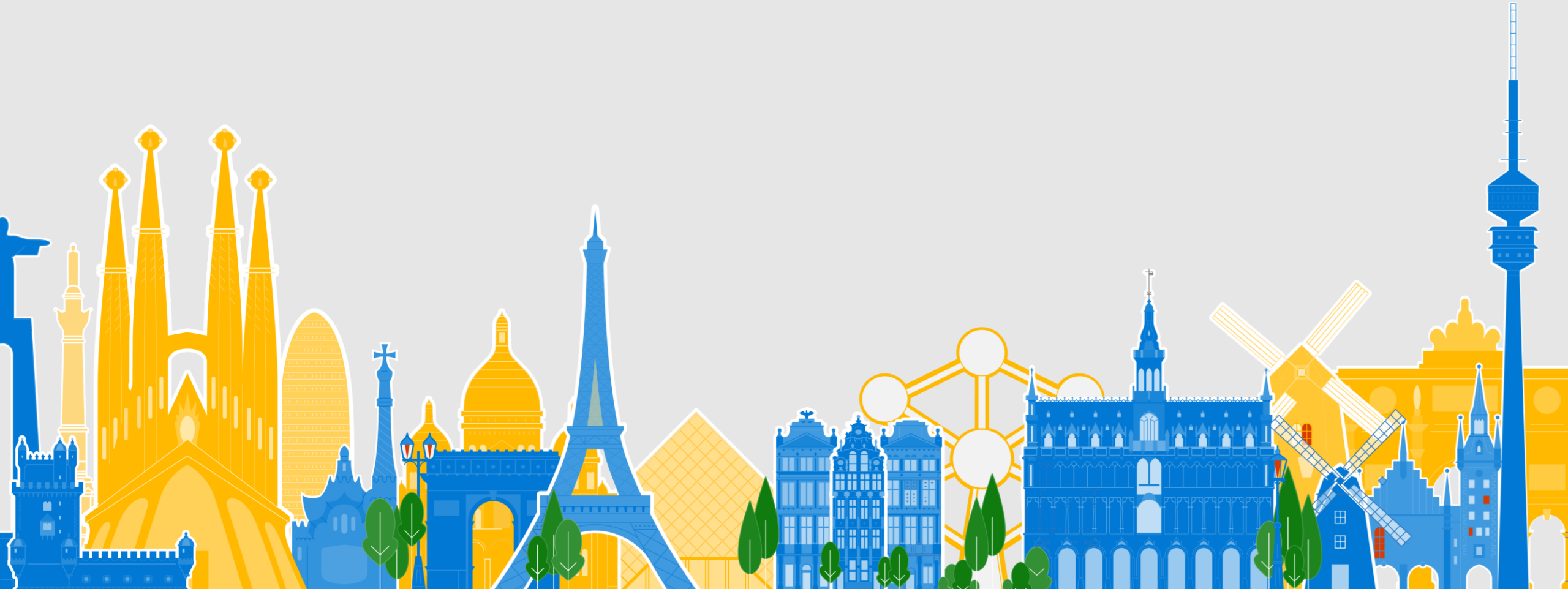
Microsoft

EU Data Boundary for the Microsoft Cloud



Agenda

- Overview of the regulatory landscape
- EU Data Boundary Implementation:
  - Commitments
  - Customer Service and Support
  - Security
- Summary
- Next steps

Regulatory background

The Court of Justice for the European Union (CJEU) decision known as **"*Schrems II*"** invalidated the EU-US Privacy Shield but confirmed the continued validity of Standard Contractual Clauses (SCCs).

SCCs are a legal transfer mechanism for personal data leaving the EEA, provided there are sufficient additional safeguards in place.

Public-sector customers can continue to use all Microsoft services in compliance with EU data protection laws.

The Microsoft EU Data Boundary is the next step in Microsoft's commitment to support the "A Europe fit for the digital age" initiative, which aims to empower people with a new generation of technologies

Helping address these challenges

Microsoft is taking action to address these evolving challenges and to ensure that our customers have what they need to meet regulatory obligations.

Implementation of new Standard Contractual Clauses (SCCs)

Simplified, consolidated Data Protection Addendum

Documented data flows/transfers

Encryption, pseudonymization, data minimization, access restrictions

Defending Your Data contractual commitments

Compliant Today

Today, our services continue to operate in lawful compliance with European laws and regulations

The EU Data Boundary for the Microsoft Cloud

Microsoft's EU Data Boundary for the Microsoft Cloud will set an even higher standard for our EU customers.

For all commercial and public-sector customers located in our new EU Data Boundary, Microsoft will store and compute customers' personal data in the EU Data Boundary **by the end of 2022.**

This **extends our current commitments** around storage and processing in the EU, as we will store and process most customer data, support data, and other personal data in the EU.

This program applies to Microsoft's Commercial Cloud Services:
Azure, Microsoft 365, Dynamics 365 and Power Platform.

We are accelerating our **technical and operational investments** necessary to fulfill this commitment and are building plans that are responsive to feedback from customers and regulators.

EU Data Boundary Implementation

Investments Microsoft is making for the EU Data Boundary by the end of 2022.

Data resides in EU

Redesigning enterprise offerings to store and compute customer data, support data, and personal data in the EU

Support in EU

Redesigning support tools Microsoft currently uses to store personal data in the EU. Offering support from within the EU and increasing our staffing in the region

Increasing transparency around security

As we continue to ensure security – an important part of data protection – we are increasing transparency around how data is used and reiterating purpose limitation

Secure remote access

Implementing virtual desktop infrastructure (VDI) to protect remote access to EU customers' personal data when necessary, and thereby preventing the physical transfer of data

Datacenter expansion in EU

Expanding the number of EU datacenters and increasing capacity in existing EU datacenters to accommodate increased processing and storage in the EU

Reduced sub processors

Limiting number of sub processors that can access EU customers' personal data

Data resides in the EU

Scope of EU Data Boundary

How the EU Data Boundary will apply:

M365, D365, POWER PLATFORM: Tenants located in the EU or EEA will be included in the EU Data Boundary.

Azure: Inclusion in the EU Data Boundary will be based on customer's selection of deployment region, tenant location, or opt-in.

When services running in the EU Data Boundary are used from within the boundary:

Customer Data:

- Services will store and compute customer data within the boundary.

Pseudonymized service generated and diagnostic data logs:

- Personal data in service generated logs associated with services running within the boundary will be stored and computed within the boundary. In cases where Microsoft collects diagnostic data associated with M365, D365, or Power Platform client software, any personal data will also be stored in the boundary if customers use the latest client versions available as of December 2022 and onward.

Microsoft may need to transfer data outside of the EU for some services, such as those that are global in nature, and for uses like security. These transfers will be clearly documented for customers.

When services running in the EU Data Boundary are used from outside the boundary:

If a customer interacts with services from outside the boundary or sends data outside of the boundary themselves, this may result in Microsoft processing customer data and other personal data outside of the boundary.

To provide critical Support functionality, Virtual Desktop Infrastructure minimizes data transfer

Customer service and support

To enable customer support and developer operations, Microsoft personnel will access support data and data logs from other locations to provide customer support and business continuity.

Virtual Desktop Infrastructure (VDI) will limit the data that is transferred to transitory screen images for troubleshooting complex support issues and developer operations. To meet customer requirements for support:

- Microsoft will, in all cases, **ensure that no support data is physically transferred outside Europe**. We will use **VDI as a supplementary measure** for support outside of Europe.
- Microsoft will continue to **increase our staffing in Europe** in support of the EU Data Boundary offering
- Microsoft will **provide an option for customers** to have all their support requests handled in Europe for initial resolution

Supplementary measures

Virtual Desktop Infrastructure (VDI)

Supplementary measure

VDI greatly reduces bulk data transfer risks, a key concern raised by the *Schrems II* judgment, with no standing access to the production environment

What is VDI?

- VDI is a highly secure workstation within the EU data boundary that avoids the physical egress of data from the EU data boundary
- Data in transit is encrypted and reduced to transitory screen shots, resulting in no storage of data outside the boundary
- Impedes against a user's ability to cut, copy, paste, or download the material viewed on screen; view sessions are timebound

When VDI is used to keep EU data in EU:

Support data: In cases where the EU support team cannot resolve a customer issue in a timely manner (see prior slide)

Pseudonymized personal data in logs: When Microsoft personnel require access to personal data within logs to secure or improve Microsoft services

Customer data: In rare cases where the service is down or in need of repair that cannot be fixed through automated tooling and authorized Microsoft personnel requires access to customer data

To provide critical security functionality, some data will need to leave the EU

Security data for cybersecurity protection

- Exceptional protection from cybersecurity attacks requires collection of certain data
- Use of data for cybersecurity protection is consistent with GDPR
- We limit data transfers to only what is required and implement additional protections

Our contractual commitment

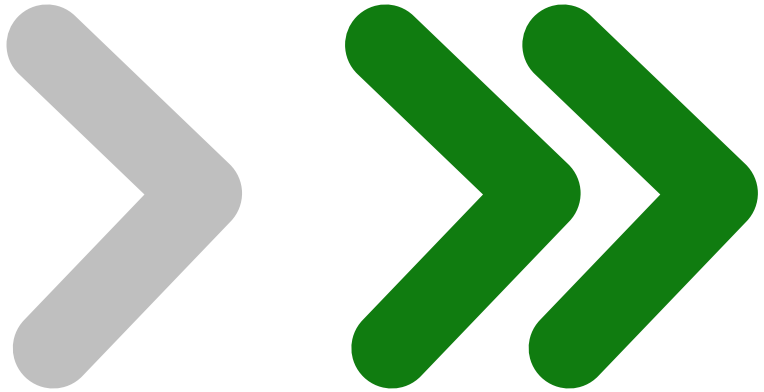
We do not process Customer Data, Professional Services Data, or Personal Data for user profiling, advertising or similar commercial purposes or any purpose other than to provide the products and services and for the business operations listed in our DPA. For security data, that means we process the data only as needed for critical cybersecurity functions in response to clear and compelling security needs and only for that purpose.

Supplementary measures

Why we may move EU security data to the US

What kind of data might be exported to the US

- File metadata, such as file name, file path, file hashes, running on individual devices
- Service audit log data, such as security-related configuration changes, user account login metadata, SharePoint URLs accessed
- Processes and command line commands executed on individual devices



Why we might export it

- To protect against sophisticated modern security threats, we rely on our advanced analytics capabilities, including artificial intelligence, to analyze aggregate activity logs to detect, respond, and remediate these attacks.
- Adversaries attack entities around the world without regard for geographic boundaries, so our response needs to be global.
- The hyperscale cloud enables diverse, ongoing analysis of security-related data without prior knowledge of a specific attack.

Core security data handling principles

Transparency

of security data collected

Isolation

of security data – only used for security purposes

Limit

security data to critical cybersecurity functions and only use it for that purpose

Summary

A.

Today our services operate in compliance with European laws.

B.

Microsoft is making additional investments for the EU Data Boundary

C.

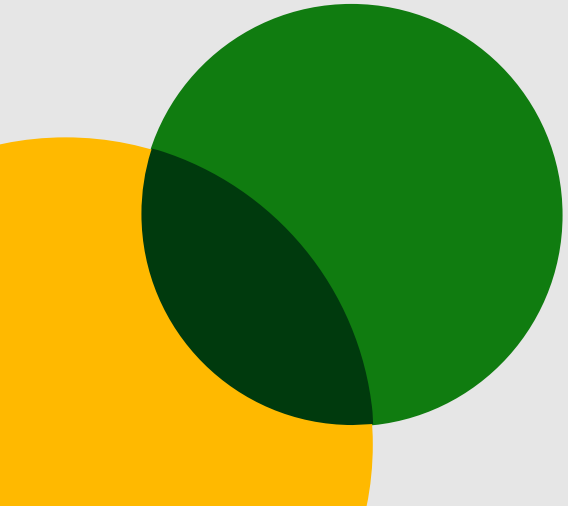
We will continue to offer world-class security and support services and will leverage Virtual Desktop Infrastructure technology to do so.

D.

We transfer data that is needed for critical cybersecurity functions in response to clear and compelling security needs and only use it for that purpose.

E.

Microsoft is on track to implement the boundary by the end of 2022.




Microsoft