## Q: What is included as part of the EU Data Boundary for Microsoft services as of January 1, 2023?

**A:** On **January 1, 2023**, Microsoft launched **Phase 1** of the **EU Data Boundary** initiative. This phase focused on increasing the **local storage and processing** of **Customer Data** within the **European Union (EU)** and **European Free Trade Association (EFTA)** regions. Core services like **Azure**, **Microsoft 365**, **Dynamics 365**, and **Power Platform** were part of this rollout, ensuring that **Customer Data** generated from these services remained primarily within Europe.

However, **limited continuing transfers** of **Customer Data** may still occur to ensure that customers benefit from the full scope of **hyperscale cloud computing**. This includes instances where maintaining performance or security requires minimal data transfers outside the EU. Microsoft has documented these transfers in its **Data Protection Addendum (DPA)** and **Product Terms**, ensuring **transparency** for all customers. The full list of services and specific transfer scenarios can be found on the [EU Data Boundary Trust Center](link).

## Q: Is Microsoft Copilot chat covered by the EU Data Boundary, and if so, how is the service's data stored and processed within the EU/EFTA region?

**A: Microsoft Copilot** chat is subject to EU Data Boundary commitments. That means any Customer Data and personal data generated through Copilot chat is stored and processed in Microsoft datacenters located within the EU/EFTA, subject to the same limited-transfer exceptions (for example, threat intelligence or security operations) that apply to other EU Data Boundary Services.

**Additionally:**

- **System-generated logs** from Copilot chat that may contain personal data are pseudonymized wherever possible.
- **Configuration requirements** are similar to other EU Data Boundary Services in Microsoft 365. If your Microsoft 365 tenant is provisioned in an EU/EFTA region (and you have not enabled Multi-Geo capabilities), then Copilot chat follows the same data residency commitments described in the Microsoft Product Terms.
- **Limited outbound transfers** may occur for maintenance, security, or technical support reasons, but those transfers are governed by strict contractual commitments, encryption, and access controls, all of which are detailed in the EU Data Boundary Trust Center.

By adhering to these measures, Copilot chat provides data residency and processing assurances that align with the EU Data Boundary, helping you meet local compliance and regulatory obligations while still benefiting from AI-driven productivity.

**Microsoft**

# Empowering Europe: Microsoft's EU Data Boundary Initiative FAQs

## Q: Why is the EU Data Boundary necessary if I am already using Microsoft Online Services in compliance with EU regulations?

**A:** While **Microsoft Online Services** already comply with **EU regulations**, including **GDPR**, the **EU Data Boundary** introduces a more robust, **localized approach** to data residency, ensuring that **Customer Data** remains within the EU/EFTA regions. By limiting **cross-border data transfers**, the EU Data Boundary makes it easier for customers to comply with **local laws** that may demand more stringent data protection standards.

The initiative also simplifies the process of conducting **Transfer Impact Assessments (TIAs)**, reducing the number of potential transfer scenarios that need to be assessed. Additionally, Microsoft's enhanced **transparency documentation** allows customers to understand exactly how and why data transfers occur, streamlining compliance and minimizing administrative efforts.

For more information, you can explore the [Microsoft EU Data Boundary Trust Center](#).

## Q: How can I configure Microsoft services to use the EU Data Boundary?

**A:** Each of Microsoft's core cloud services—**Azure**, **Microsoft 365**, **Dynamics 365**, and **Power Platform**—has specific **technical configurations** to align with the **EU Data Boundary**. To use the **EU Data Boundary** version of these services, customers must follow the service-specific configuration requirements outlined in the **Product Terms** and supporting documentation. To store **Professional Services Data** in the **EU Data Boundary** for **Azure**, customers must configure Azure Resource Manager to the **EU Data Boundary** as described in the [EU Data Boundary Transparency Documentation](#).

These resources provide clear, detailed instructions on how to set up services within the **EU/EFTA** regions, ensuring that  personal data remains fully compliant with **local residency** requirements. You can find all relevant documentation and configuration guides in the [EU Data Boundary Trust Center](#).

## Q: Will there be any loss of functionality within the EU Data Boundary compared to standard cloud services?

**A:** No. The **EU Data Boundary** does not reduce or change the functionality of Microsoft's cloud services. Whether operating within or outside of the **EU Data Boundary**, customers will receive the same high-quality, **secure** services with all the features and performance they expect from **Microsoft 365**, **Azure**, **Dynamics 365**, and **Power Platform**.

The **EU Data Boundary** is a data residency enhancement, ensuring that customer data is stored and processed within the **EU/EFTA** regions without sacrificing functionality, performance, or **cloud scalability**.

# Empowering Europe: Microsoft's EU Data Boundary Initiative FAQs

## Q: Does using the EU Data Boundary version of services come with additional costs?

**A:** No, Microsoft does not charge any **additional fees** for the use of **EU Data Boundary** services. Customers can use services that comply with **EU data residency requirements** without any price increases, ensuring **cost efficiency** while benefiting from enhanced **data protection** and **compliance**.

For further details about service pricing and terms, refer to the [Microsoft Pricing Overview](#).

## Q: Where can I find documentation on the ongoing transfers of data outside the EU?

**A:** Microsoft is committed to **transparency** regarding any ongoing **data transfers** that occur outside the EU as part of the **EU Data Boundary**. Customers can access detailed **data flow documentation** on the **EU Data Boundary Trust Center**. This includes information on the scenarios in which **limited data transfers** may still be necessary, along with comprehensive descriptions of how such transfers are managed to ensure **security** and **compliance**.

All relevant documentation is available [here](#).

## Q: What is the relationship between the EU Data Boundary, Microsoft Cloud for Sovereignty, and Advanced Data Residency?

**A:** These solutions address different aspects of **data protection** and **regulatory compliance**:

- **EU Data Boundary**: Focuses on ensuring that **Customer Data** remains within the EU/EFTA regions for key services, reducing **cross-border transfers** and providing **localized compliance**.
- **Microsoft Cloud for Sovereignty**: Designed for **public sector customers**, this solution enables greater control over **data governance** and **compliance** processes, while still leveraging the full power of Microsoft's cloud offerings.
- **Advanced Data Residency**: Offers more **granular control** over the location of **Microsoft 365** data, ensuring that customer data at rest is stored within specific geographies, including the EU.

For more details on the **Microsoft Cloud for Sovereignty**, visit [this page](#).

**Empowering Europe: Microsoft's EU Data Boundary Initiative FAQs**

## Q: What advancements were introduced in Phase 2 of the EU Data Boundary?

**A: Phase 2**, which launched in **January 2024**, extended Microsoft's efforts beyond **Customer Data** to include **pseudonymized personal data**. This data, which has been altered to remove direct identifiers, is now processed and stored within the **EU/EFTA** regions.

By keeping **pseudonymized data** in-region, Microsoft continues to uphold its commitment to **data sovereignty** while further reducing the number of data transfers outside the EU. **Phase 2** also enhanced the **EU Data Boundary Trust Center**, adding more documentation on how **pseudonymized data** is managed and ensuring that customers have greater **transparency** into how this data is handled.

For more information on **pseudonymized data** and **Phase 2**, check out the [EU Data Boundary Phase 2 Overview](#).

## Q: How does Phase 3 of the EU Data Boundary address Professional Services Data?

**A: Phase 3**, launched in **February 2025**, focuses on the **storage** of **Professional Services Data**. When customers in the EU or EFTA regions request **technical support** for services such as **Microsoft 365**, **Dynamics 365**, **Azure**, or **Power Platform**, the Professional Services Data they provide as part of the support process is now stored entirely within the **EU/EFTA** regions.

As with previous Phases, transparency is a central focus of Phase 3. Microsoft's transparency documentation on the EU Data Boundary Trust Center has been updated to include commitments for the storage of Professional Services Data and information about limited transfers of this data outside of the EU Data Boundary.

For more details on **Phase 3** of the **EU Data Boundary**, visit the [EU Data Boundary Trust Center](#).

## Q: How does Microsoft handle security data that may be transferred outside the EU?

**A:** While the **EU Data Boundary** keeps the majority of **personal data** within the EU/EFTA, certain limited data transfers may be necessary for **global security operations**. This data is used to enhance **threat detection**, **investigation**, **remediation,** and **prevention** across all regions.

To protect this data, Microsoft uses protections such as **encryption**, **pseudonymization**, and **strict access controls**, ensuring that only authorized security personnel access it. The **global threat intelligence** gained from these transfers is crucial for detecting and mitigating **cyberattacks**.

Learn more about when Microsoft **transfers** data for security purposes [here](#).

## Q: How does cross-boundary data analysis comply with data protection regulations?

**A:** Microsoft's **cross-boundary data analysis** complies fully with **GDPR** (Article 32) and the **EU Charter of Fundamental Rights** (Article 6). When limited data transfers occur outside the EU for **security** or **threat detection**, they are carried out with strict **pseudonymization**, **encryption**, and **access controls** to ensure compliance with EU regulations.

For more details, see the [Microsoft GDPR Resource Center](#).

## Q: Can customers opt out of having their data transferred outside the EU for security analysis?

**A:** No, customers cannot opt out of **limited and necessary data transfers** for **global cybersecurity** purposes. These transfers are crucial for maintaining a robust, **global security posture** that protects against **sophisticated cyberattacks**. However, Microsoft employs stringent **security controls** and **contractual commitments** to ensure that customer data is always handled with the highest level of **protection** and **transparency**.

## Q: What are the next steps for the EU Data Boundary after Phase 3?

**A:** With **Phase 3** now complete, Microsoft will continue to assess customer needs and **regulatory developments**. Future enhancements may include **additional controls** and **capabilities** to ensure ongoing compliance with evolving regulations. The **EU Data Boundary Trust Center** will remain the central resource for updates, ensuring that customers are informed about any changes or new features introduced post-Phase 3.

This updated FAQ aligns with the completion of **Phase 3** of the **EU Data Boundary** initiative and provides comprehensive answers to key questions.

For more information, please visit the [Microsoft EU Data Boundary Trust Center](#).