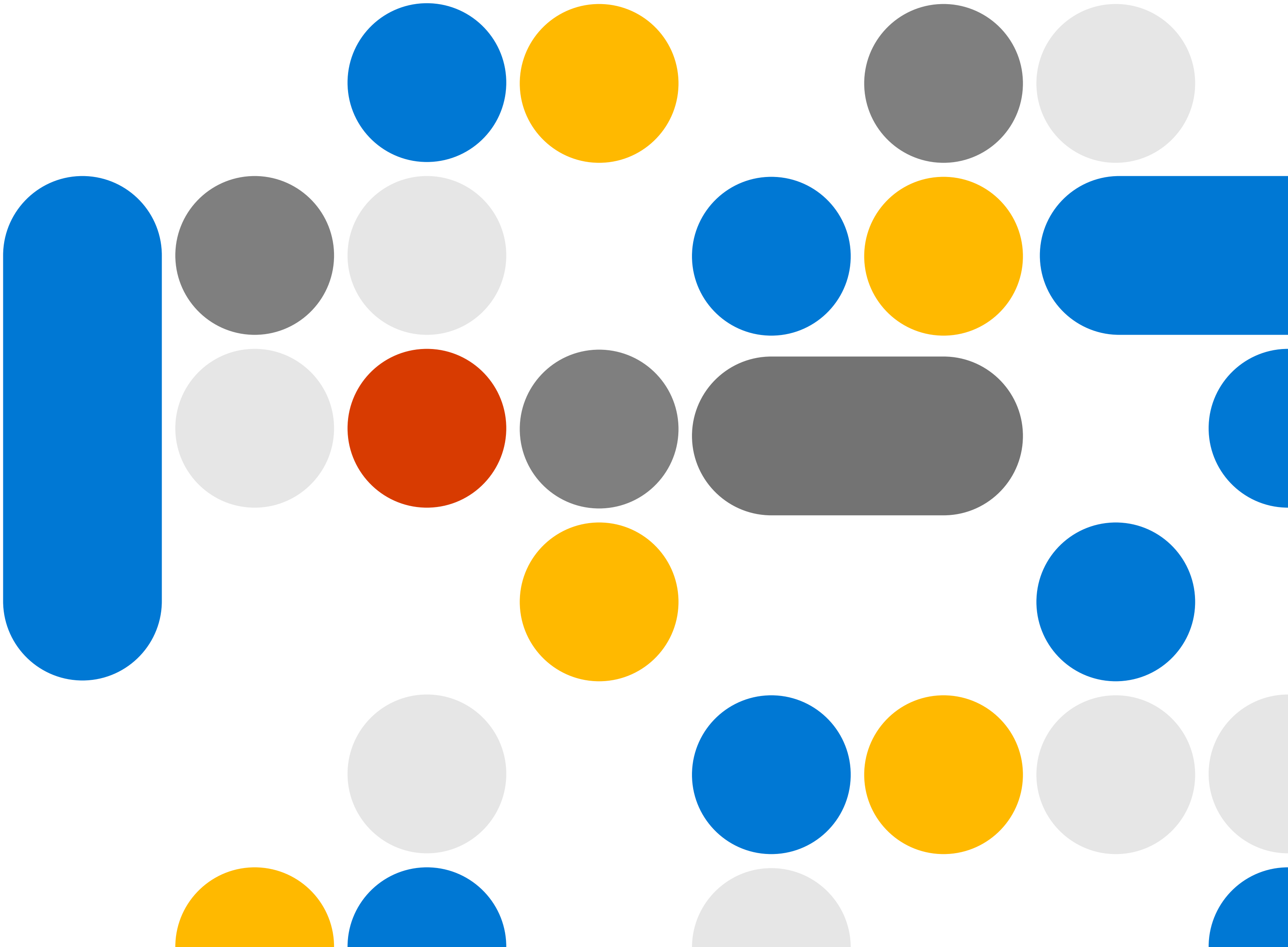
Microsoft

Understanding the Microsoft EU Data Boundary Roadmap: Background, Recap, and Updates

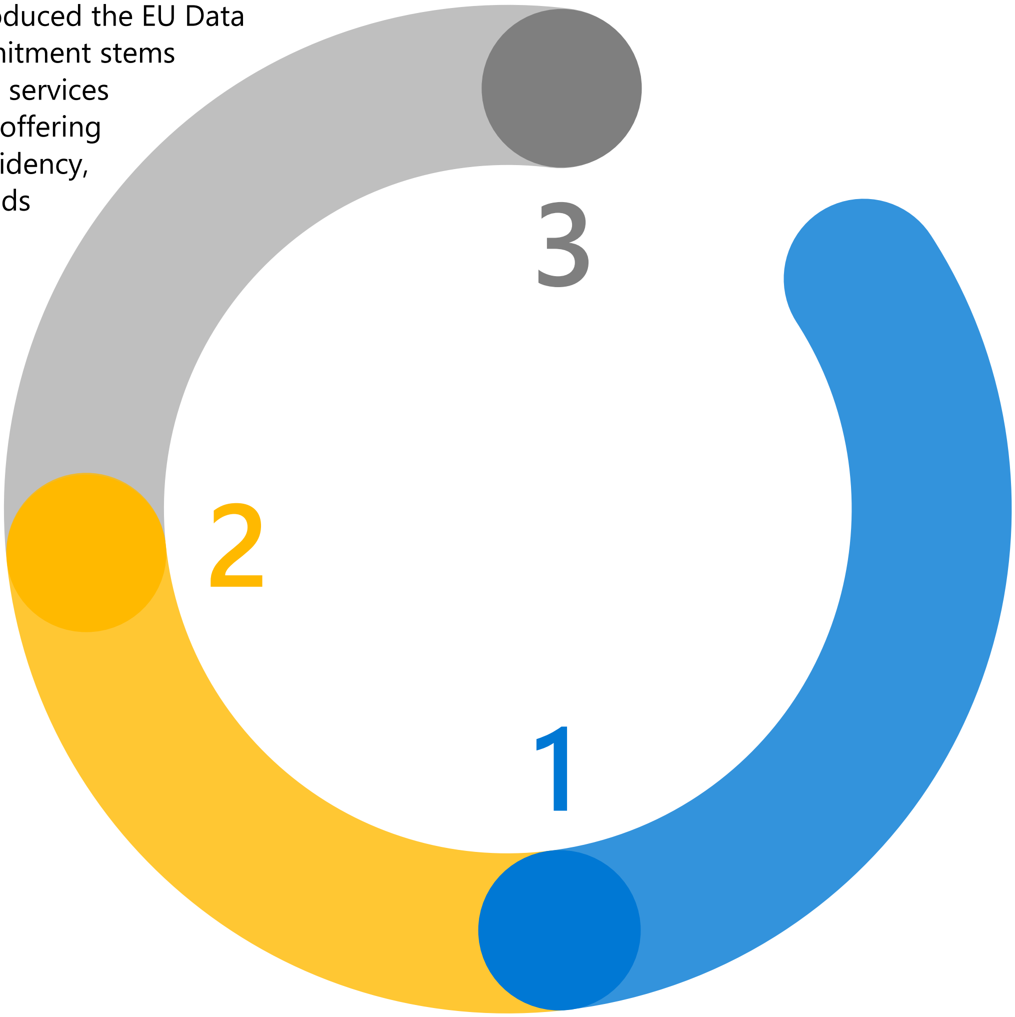
Updated December 2023



Background: The EU Data Boundary Initiative

In a digital age driven by data, security remains at the forefront of concerns, especially for a region as diverse and interconnected as Europe.

Acknowledging the unique needs of the European Union (EU) and the European Free Trade Association (EFTA) nations, Microsoft introduced the EU Data Boundary initiative. This commitment stems from a vision to provide cloud services that respect European values, offering enhanced data protection, residency, and control. The initiative stands as a beacon of Microsoft's commitment to reducing data flows out of Europe and increasing transparency for its commercial and public sector customers.



Phase 1

Customer data and documentation

Kicking off on January 1st, 2023, Wave 1 of the EU Data Boundary initiative focused on customer data. Microsoft committed that customer data associated with Microsoft 365, Dynamics 365, Power Platform, and the majority of Azure services is stored and processed within the EU and EFTA regions. Phase 1 documentation provides sections about temporarily excluded transfer, with explicit commitments and detailed documentation for these exceptions. This wave not only built upon previous local storage commitments but also reduced data outflows from these European regions. To ensure clarity, Microsoft unveiled the

EU Data Boundary Trust Center Page

This hub offers comprehensive documentation detailing the initiative's commitments, data flows, and any limited transfers of customer data outside the region required for maintaining service security, functionality, and reliability. As an added layer of transparency, these documents are available in various languages, continually updated as the initiative progresses.

Phase 2

Pseudonymized Personal Data

The second phase of Microsoft's EU Data Boundary (EUDB) initiative extends its scope beyond customer data to encompass pseudonymized personal data. This category of data, produced during service operations, is now also retained within the European Union (EU) and European Free Trade Association (EFTA) regions under the revised guidelines.

Pseudonymized personal data refers to data where the identity of the individual is not apparent without additional information. By keeping this data within the EU and EFTA territories, Microsoft aims to enhance data protection and privacy for its customers.

As with Wave 1, and customer data, transparency remains a key focus in this phase as well. With Wave 2, Microsoft provides detailed updated documentation to help customers understand data transfers, including any limited transfers necessary for maintaining service excellence and limited transfers for security purposes. This updated documentation includes information about data flows and guidance for understanding scoping and increased levels of data transparency.

Wave 2 represents a significant step forward in Microsoft's commitment to data privacy and protection in the EU and EFTA regions.

EU Data Boundary and Global Cybersecurity Operations

Microsoft’s commitment to exceptional cybersecurity necessitates the transfer of specific personal and customer data outside the EU Data Boundary. This strategic move is imperative to counteract the sophisticated, globally coordinated attacks orchestrated by malicious actors.

Global Intelligence for Robust Defense

Our security services leverage cross-border threat data analysis to provide top-tier, automated defenses and rapid responses, directly enhancing customer protection and safeguarding resources. This global insight informs our alerts and updates, ensuring enterprises are promptly notified of potential breaches or attacks.

Prioritizing Security and Privacy

Data transferred out of the EU is accessible to authorized security personnel, dedicated to enhancing customer protection and bolstering Microsoft’s infrastructure. We employ stringent protection measures including encryption, access controls, and pseudonymization where applicable, all while adhering to our contractual commitments.

Phase 2 cont.

Leveraging Advanced Analytics

Our security posture is fortified through advanced analytics and artificial intelligence, enabling real-time, precise threat detection and reducing false positives. This centralized approach ensures efficiency, consistency, and a superior user experience across our services.

24/7 Security Operations

Microsoft's security operations, rooted in our threat intelligence capabilities, provide relentless, around-the-clock monitoring and response to global threats. Our Azure data centers, located in strategic global hubs, serve as the command centers for these operations, ensuring data integrity, security, and privacy.

Minimizing Privacy Impact for customers

We limit ongoing data transfers to essential service-generated logs and configuration information, aiming for early threat detection. Personal data (and in rare cases, customer data) transferred is carefully protected, aligning with our Microsoft Products and Services Data Protection Addendum and other contractual commitments.

Security Threat Intelligence

Our threat intelligence services play a crucial role in identifying and blocking malicious attempts against customer environments, delivering timely threat intelligence and enabling organizations to bolster their defenses.

Phase 3

Enhancing Technical Support Data

Working toward completion by mid-2024, the third wave targets the elevation of processing and storage capabilities for data received during technical support interactions. When customers request Microsoft technical support, it is important that we are able to promptly engage the right skilled expertise. By mid-2024, we are working to ensure that data provided to us when receiving technical support for Microsoft 365, Power Platform, Dynamics 365 and Azure services is stored within the EU Data Boundary. As we move to store and process support data within the EU Data Boundary, there will be situations where remote access to in-boundary systems or data may be required to provide customer support and to maintain, secure, and operate the services. Required remote access will be completed using secure remote workstations to control data egress from the EU Data Boundary and minimize both the duration and size of any temporary transfers required to complete support functions. In parallel, Microsoft continues to invest in staffing within the EU region and is exploring how to offer an enhanced support option for customers who prefer to have their initial support response handled by support engineers physically located within the EU.

In Summary

Through the EU Data Boundary initiative, Microsoft is at the forefront of integrating comprehensive data protection with cutting-edge technology, delivering unparalleled cloud services that align seamlessly with European values and regulatory standards. As we venture forward, Microsoft's expansive European footprint and investments underline a promise to uphold and enhance Europe's digital future. Together, we embark on a journey where data protection, transparency, and technological prowess coalesce seamlessly.

Microsoft

Understanding the Microsoft EU Data Boundary Roadmap: Background, Recap, and Updates

December 2023