Addressing sovereignty requirements with Microsoft Azure
Purpose

This document highlights Microsoft Azure’s investments in cloud capabilities that help customers meet their compliance, data residency, and data sovereignty objectives. While we acknowledge that requirements differ greatly between customers, industries, and geographies, the investments we’ve made in compliance, cloud governance, and hybrid capabilities provide flexibility to meet a diverse range of needs.

Introduction

Today’s digital landscape challenges organizations to keep up with the pace of innovation and evolution of threats. The cloud has become indispensable for organizations around the world when it comes to meeting these challenges because of its ever-growing set of capabilities that meet security, operational, privacy, compliance, and sovereignty requirements. As a result, regulated industries and public sector organizations are adopting the cloud to run business-critical applications.

Alongside this adoption, there’s an increased discussion among policy influencers, regulators, and industry bodies regarding the nature of “digital sovereignty” in hyperscale cloud environments that require global investments to deliver the capabilities customers rely on. For many customers, “digital sovereignty” concerns aren’t binary and addressing them isn’t a simple checkbox exercise. However, Microsoft has helped many customers adopt a risk-based approach based on data classification and the criticality of applications, enabling differentiated use of the public cloud, hybrid cloud, and private cloud to meet the sovereignty requirements appropriate for different types of data. Microsoft also helps improve regulatory requirements to be objective and risk-based and allow for innovation. The following considerations are key in that risk-based approach:

Security: What measures are in place to guard against external and internal threats?

Data sovereignty: Does the customer have control over their data, and which jurisdictions can make lawful requests for customer data?¹

Availability/Resiliency: Can the customer continue to operate in the case of catastrophic events (for example, the loss of a datacenter or a major network disruption)?

Operational independence: Can the customer continue to operate independently of the technology supplier?

Confidentiality: How sensitive is the data and what (additional) measures are needed to protect it?

Governance: Which capabilities are available to govern security, privacy, and compliance?

In many countries these considerations make their way into regulations and local compliance frameworks. Microsoft is working to address the unique needs of nations with a comprehensive and trusted set of cloud offerings to meet the spectrum of data residency and sovereignty requirements.

¹ Microsoft defines “customer data” as all data that a customer provides to Microsoft or is provided on the customer’s behalf through use of Microsoft enterprise online services (refer to How Microsoft categorizes customer data for online services).
Helping customers meet their compliance requirements

Meeting compliance obligations in a dynamic regulatory environment is complex. To comply with regulatory requirements, cloud service providers and their customers have a shared responsibility to ensure that each party does their part. The responsibilities vary depending on whether data and applications are hosted on Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS), or in an on-premises environment (as discussed further in Shared responsibility in the cloud).

Microsoft compliance offerings

The Microsoft Cloud has achieved more than 100 compliance certifications to comply with national, regional, and industry-specific requirements governing the collection and use of data. For most customers and data classifications, these certifications are sufficient for regulatory compliance or provide the compliance foundation that customers can build on to meet their compliance requirements. Microsoft offers tools to help customers manage their compliance requirements.

Data residency

Data residency is a common compliance requirement. To help customers meet this requirement, Microsoft has cloud regions in 35 countries, more than any other cloud provider, and continues to expand to more countries. Most Azure services are deployed regionally and enable the customer to specify the region into which the service will be deployed and, therefore, control where the customer data will be stored. Where your data is located provides details on where specific Azure services store and process data. Customers need to determine their applicable data residency requirements and whether these can be met in existing Microsoft regions, especially when workloads need to be deployed across multiple regions to protect against catastrophic events. European Union (EU) countries can often use datacenter regions within the EU for additional resilience or if the required services aren't available in their country. The EU Data Boundary for Microsoft Cloud commitments show we will continue to meet and exceed the requirements of EU data protection laws.

Data governance and compliance management

Maintaining control over data and achieving regulatory compliance go hand in hand and Microsoft provides services and guidance to enable both:

- **Microsoft Trust Center** provides information about the compliance offerings of the Microsoft Cloud and includes certifications and audit reports.

- **Microsoft Compliance Manager** helps customers manage their organization’s compliance requirements, from taking inventory of data protection risks to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

- **Azure Policy** and **Azure Blueprints** enable customers to ensure applications can only be deployed if they’re compliant with applicable policies. Azure also provides several predefined blueprints that meet specific regulatory requirements, such as ISO 27001 and PCI-DSS, and the Azure Security Benchmark Foundation blueprint sample that can be used as a foundation to create new ones.

- **Microsoft Purview** is a unified data governance service that helps manage and govern on-premises, multi-cloud, and SaaS data. Create a holistic, up-to-date map of the data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage.

- The **Cloud Adoption Framework** provides prescriptive guidance and ready-to-use architectures, leveraging Azure Policy.
Using Azure capabilities to safely work with sensitive data

Azure offers multiple ways for customers to customize the degree of protection for cloud workloads on top of the secure foundation the cloud platform provides, such as network controls and endpoint protection, identity controls, security information event management (SIEM) and security orchestration automated response (SOAR), and encryption.

**Encryption.** Encryption is a fundamental component that helps ensure confidentiality of cloud workloads. Microsoft provides customers with several offerings and best practices to manage and control the security of customer data using encryption at rest and in transit. In addition to Microsoft-controlled encryption keys, customers have the option to use customer-managed keys, customer-provided keys, or to perform client-side encryption with customer keys.

**Azure Confidential Computing.** Today, data is encrypted at rest in storage and in transit across the network, but not while in use in memory. Confidential computing protects data in use by performing computation in a hardware-based Trusted Execution Environment (TEE), which only allows access to unencrypted data when it’s inside a secure enclave. Even if someone gains access to the compute environment, they’re prevented from reading the unencrypted data within the secure enclave. This enhances security and minimizes the role of cloud operators in the trust chain. With confidential computing, customers can now have verifiable assurance that their data is under their control, with a key that they can manage, from the time it’s created until it’s destroyed. Some of the services that support confidential computing today are platform enablement capabilities, such as virtual machines and containers, and PaaS/SaaS services, such as databases, container orchestration, and key management. Microsoft’s vision is to enable many more services to support confidential computing.

**Cloud platform security controls and processes**

Cybercrime, whether nation-state sponsored or permitted, is a threat to national security. Cybercriminals target and attack all sectors of critical infrastructure, including healthcare and public health, IT, financial services, and energy sectors. Ransomware attacks are increasingly successful, crippling governments and businesses, and the profits from these attacks are soaring. The Microsoft Digital Defense Report discusses the threat of cybercrime in more detail. These threats are growing in size and complexity, and the hyperscale cloud is a key component to protect against them. The Cyber Defense Operations Center is where all parts of Microsoft’s security apparatus come together to protect, detect, and respond. Here, security experts from across the company monitor the trillions of daily signals to protect Microsoft cloud infrastructure, services, and customers from evolving threats. The benefit of this protection extends to customer infrastructure leveraging hybrid cloud capabilities and services, such as Azure Sentinel.

CDOC operations are just one of the many layers of security. Microsoft uses a Zero Trust approach to design infrastructure and services to be secure by design. This starts with physical security and infrastructure security, which, among others, controls who can gain access to physical infrastructure. Platform integrity and security builds on this and ensures compute hosts haven’t been compromised. Services deployed on top of the platform use various isolation techniques to isolate customers so they can’t compromise the underlying platform and can’t access other customers’ data (refer to Isolation in the Azure Public Cloud).
Microsoft takes strong measures to help protect customer data from inappropriate access or use by unauthorized persons. In addition to the physical and technological protections, there are access restrictions for Microsoft personnel and subcontractors, as well as thorough requirements for responding to government requests for customer data.

Only in rare cases does a Microsoft engineer need access to customer data to resolve a customer issue. Nearly all service operations performed by Microsoft are fully automated, and human involvement is highly controlled and abstracted away from customer data. Access to customer data by Microsoft operations and support personnel is denied by default. Access to the platform is granted through a just-in-time approval process. Access is scoped to the role and activity that needs to be performed. For many services the customer can be part of that approval process through Customer Lockbox. All access to customer data is strictly logged, and both Microsoft and third parties perform regular audits.

With Azure, customers own their own data. They can access their data at any time and for any reason without assistance from Microsoft. Moreover, Microsoft doesn’t use or share customer data for advertising. When customers end their subscription, Microsoft then deletes their customer data within specified time frames.

**Subcontractors and subprocessors.** Microsoft may hire third parties to provide certain limited or ancillary services on our behalf, known as subprocessors. Microsoft is responsible for our subprocessors’ compliance with Microsoft’s obligations in the product terms. Subprocessors’ access to customer data is restricted to the delivery of the services Microsoft has retained them to provide. Subprocessors are prohibited from accessing customer data for any other purpose. For further details and a list of subprocessors, please refer to [Who can access your data and on what terms](#) on the [Microsoft Trust Center](#).

Microsoft has taken a firm public stand on protecting customer data from unlawful government access and, where necessary, has advanced its position through the courts. Microsoft will continue to go to court to defend the local rights of our customers. We routinely deny or challenge orders when we believe they are not legal. Microsoft will also continue to push for new international agreements that strengthen the rights of our customers.

Microsoft doesn’t provide any government (including law enforcement or other government entities) direct or unfettered access to customer data. In case Microsoft receives a government or law enforcement request for customer data, Microsoft first validates the warrant and attempts to redirect the third party to obtain the requested data from the customer. For valid requests that Microsoft isn’t able to redirect to the customer, Microsoft will comprehensively examine this request for disclosure from a legal point of view. Microsoft discloses customer data only when legally compelled to do so, and always makes sure to provide only the customer data specified in the legal order.

Microsoft is committed to transparency and provides the [Law Enforcement Requests Report](#), which brings together in one place the reports that Microsoft issues regularly on requests for customer data made by law enforcement. The [US National Security Orders Reports](#) provides this information for requests related to US national security. The aggregate data in these reports show that most law enforcement requests are targeted to individuals and that Microsoft very rarely is required to provide data stored in overseas datacenters for enterprise customers to US law enforcement. Microsoft doesn’t provide, and has never provided, EU public sector customers’ personal data to any government. For more details on data transfers and on what Microsoft is legally allowed to report, refer to [Compliance with EU transfer requirements for personal data in the Microsoft Cloud](#).
The CLOUD Act. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) doesn’t reduce the protections previously described. The CLOUD Act amends US law to make it clear that law enforcement may compel US-based service providers to disclose data that’s in their “possession, custody, or control,” regardless of where the data is located. This law, however, doesn’t change any of the legal and privacy protections that previously applied to law enforcement requests for data—and those protections continue to apply. Microsoft adheres to the same principles and customer commitments related to government demands for customer data.

Hybrid and on-premises solutions for restricted environments

Customers with more stringent compliance requirements and those who need more control over physical infrastructure, hardware, data flow, or personnel beyond those already previously detailed may be able to leverage hybrid and private cloud solutions. While hybrid solutions are connected to functionality in the cloud, customers can control whether data shared with the cloud environment includes customer data or is limited to monitoring and management data.

- **Azure Arc** enables customers to manage their on-premises infrastructure from the cloud through a single pane of glass and run several cloud services on their on-premises infrastructure. Customer data is stored and processed on the customer infrastructure; this data is only copied to the cloud if explicitly configured by the customer. Arc-enabled services send metadata to the cloud for billing, management, and diagnostics. When disconnected from the cloud, workloads using these services continue to operate, but configuration changes may not be possible depending on the cloud service. This mode enables operational independence if it is required for a limited time in certain scenarios.

- **Azure Stack HCI** is a hyperconverged infrastructure (HCI) cluster solution that can be deployed on-premises to host virtualized Windows and Linux workloads (virtual machines and containers) managed locally or from the cloud. Azure Stack HCI sends metadata to the cloud for billing, management, and diagnostics. [Azure Stack HCI data collection](#) details which data is collected. Azure Stack HCI can run disconnected from the cloud for up to 30 days, supporting periodically disconnected or low-quality networks.

- **Azure Stack Edge** (ASE) is a portfolio of devices delivered by Microsoft as Hardware as a Service (HaaS) solutions that provide small-scale edge compute capabilities, with data replication and synchronization to the Azure cloud. ASE enables customers to run virtual machines, containers, IoT Edge, and machine learning models on a managed rack-mounted or portable device. Customer data is stored and processed on the device and is only copied to the cloud if configured by the customer. Machine learning models can pre-process data before it’s sent to the cloud to mitigate any compliance issues. When connected, ASE may send metadata to the cloud for billing, management, and diagnostics, but the device can operate disconnected for an extended time. While ASE isn’t suited for large-scale deployments, the offline capabilities could be used to keep critical applications available.

- **Azure Stack Hub** is a private cloud solution that enables customers to run a subset of Azure services in their own datacenter. Azure Stack Hub is capable of running completely disconnected for environments that need tight control over which data leaves the environment. With Azure Stack Hub, the customer manages and operates the environment, providing them with complete end-to-end control.

The hybrid and private clouds are important parts of Microsoft strategy and Microsoft continues to invest in hybrid and private offerings to meet the requirements of customers that can’t use the public cloud.
Further reading

- Azure security documentation
- Enabling data residency and data protection in Microsoft Azure regions
- Security in the Microsoft Cloud Adoption Framework for Azure
- Microsoft 365 guidance for security and compliance
- Compliance with EU transfer requirements for personal data in the Microsoft Cloud
- Microsoft products and services data protection addendum
- New steps to defend your data

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2022 Microsoft Corporation. All rights reserved.

Azure, Microsoft, Windows, and other product names are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.