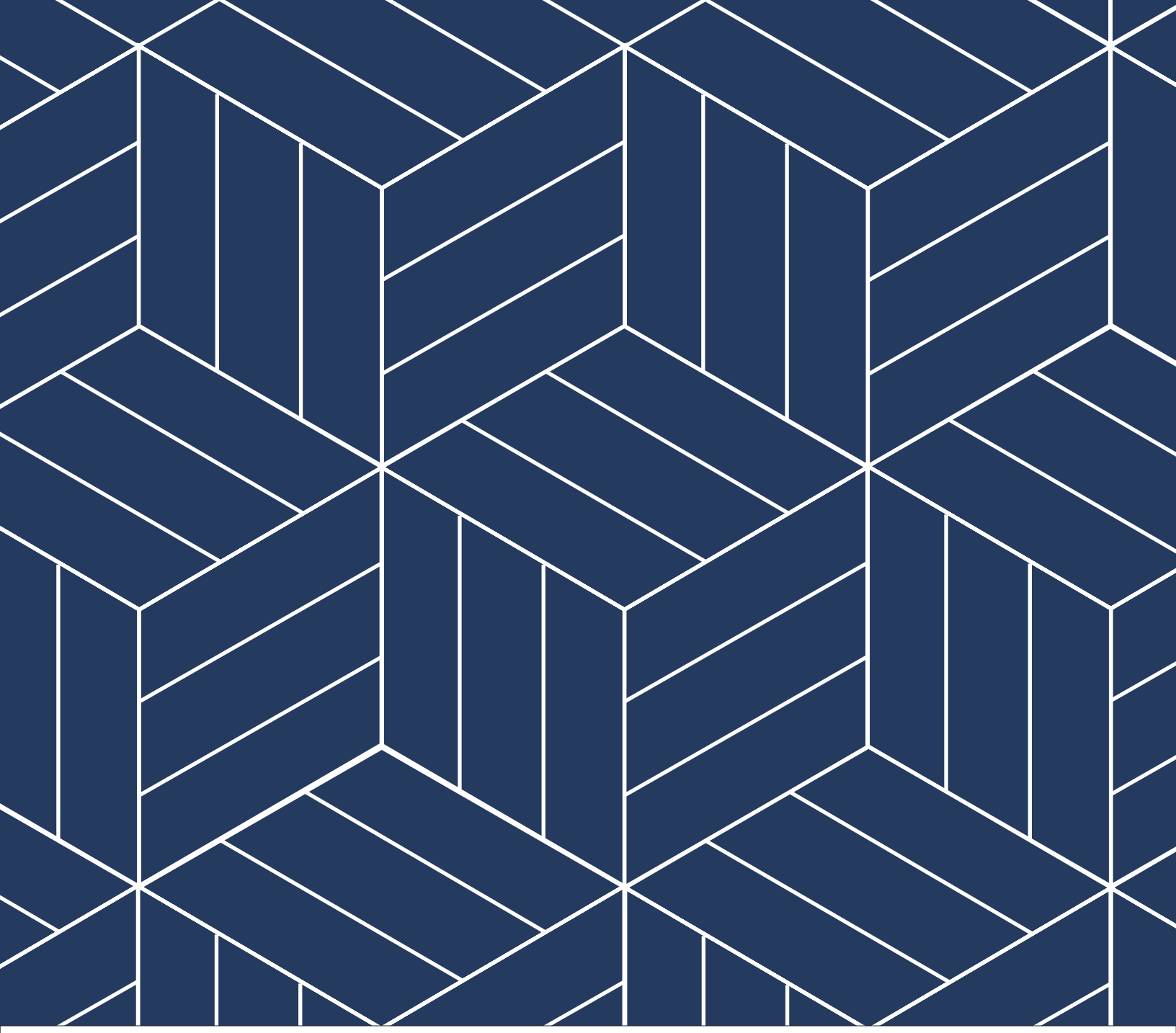


# Achieving Compliant Data Residency and Security with Azure

Microsoft

# Authors

Markus Feichtner
Debra Shinder
Christoph Siegert

# Contributors

Darren Brust
David Burt
Justin Denk
Roger Halbherr
Marc Holitscher
Shont Miller
Glenn Pittaway
Seth Varty
Stevan Vidich

# Contents

# Introduction

Security and compliance–basic elements of the trusted cloud–are top priorities for organizations today. This paper is designed to help customers ensure that their data is handled in a manner that meets their data protection, regulatory, and sovereignty requirements on the global cloud architecture of Microsoft Azure.

Transparency and control are also essential to establishing and maintaining trust in cloud technology. Microsoft recognizes that restricted and regulated industries require additional details for their risk management and to ensure compliance at all times. Microsoft provides an industry-leading security and compliance portfolio.

Security is built into the Azure platform, beginning with the development process, which is conducted in accordance with the Security Development Lifecycle (SDL), and includes technologies, controls and tools that address data management and governance, Active Directory identity and access controls, network and infrastructure security technologies and tools, threat protection, and encryption to protect data in transit and at rest.

Microsoft also provides customers with choices to select and limit the types and locations of data storage on Azure. With the innovation of the security and compliance frameworks, customers in regulated industries can successfully run mission-critical workloads in the cloud and leverage all the advantages of the Microsoft hyperscale cloud. This simple approach can assist customers in meeting the data protection requirements of government regulations or company policies by helping them to:

- Understand data protection obligations.
- Understand the services and controls that Azure provides to help its customers meet those obligations.
- Understand the evidence that customers need to assert compliance.

The paper is structured into these three sections, with each diving deeper into the security and technologies that help Microsoft customers to meet data protection requirements. The final section discusses specific requirements to which industries and organizations in selected European markets are subject.

# I. Understand data protection obligations

The process of achieving compliant data residency and security begins with knowing the obligations and the types and locations of the data which require protection. First, conduct an analysis to determine which legal and contractual requirements apply to the workloads. These may vary based on the location of the organization, the jurisdiction where the files are stored and processed, and the applicable business sector. Components of understanding data obligations include data classification, data location, and the respective responsibilities for data protection under the shared responsibility model.

## Data classification with Microsoft Azure

Data comes in many different types with varying levels of sensitivity. This whitepaper focuses primarily on **customer data**, which Microsoft defines as all data, including text, sound, video or image file, and software, that a customer provides to Microsoft or that is provided on the customer's behalf through its use of Microsoft enterprise online services (in the context of this paper, Microsoft Azure). For example, customer data includes content that the customer uploads in Azure Storage or SQL Database, as well as applications and other virtual machine content the customer uploads to execute in Azure Virtual Machines. Microsoft does not distinguish between the types of content that customers upload into the service and classifies all such content as customer data subject to the same high level of protection.

**Personal data** is any information that relates to an identified or identifiable natural person. Personal data provided by a Microsoft customer through its use of the service, such as the names and contact information of the customer's end users, would also be customer data. Personal data can also include certain pseudonymous data that is not customer data, such as the user ID that a Microsoft service assigns to each user; such personal data is considered pseudonymous because it, alone, cannot identify the individual.

This whitepaper focuses on the handling of customer data (including any personal data therein) because it is the most sensitive category for any customer. Microsoft also classifies and implements policies to protect other categories of data as follows:

- **Administrator data** is the information about customer administrators that is supplied during signup, purchase, or administration of Microsoft services, such as administrator names, phone numbers, and email addresses. It also includes aggregated usage information and data associated with the administrator account, such as the controls that are selected. Microsoft uses administrator data to provide services, complete transactions, service the account, and detect and prevent fraud.

- **Object metadata** is information provided by the customer or on the customer's behalf that is used to identify or configure Online Service resources, such as software, systems, or containers, but does not include their content or user identities (both of which would be customer data, as described above). Examples of object metadata include the names and technical settings of Azure Storage accounts, Virtual Machines, SQL Databases and their tables, column headings, and forms. Customers should not include personal data or other sensitive information in object metadata because object metadata may be shared across global Microsoft systems to facilitate operations and troubleshooting.

- **Payment data** is the information customers provide when making online purchases with Microsoft. It may include a credit card number and security code, name and billing address, and other financial data. Microsoft uses payment data to complete transactions, as well as to detect and prevent fraud.

- **Support and consulting data** means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by or on behalf of a customer (or that the customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain Professional Services or Support. This may include information collected over phone, chat, e-mail, or web form. It may include descriptions of problems, files transferred to Microsoft to resolve support issues, automated troubleshooters, or information obtained by accessing customer systems remotely with customer permission. It does not include administrator data or payment data.

## Data location

Data location is another important aspect to consider in the selection of a cloud service. Microsoft Azure offers services in over 50 regions and is provided from over 100 datacenters around the globe. To select the appropriate data location for specific workloads, consider the following:

- Technical considerations
- Regulatory considerations

### Technical considerations

High latency (the delay between a client request and a cloud service provider's response) impacts the usability of real-time applications. Due to the unmatched global footprint of Microsoft datacenters all over the world, customers can choose locations that enable them to reach their customers wherever they are, thus reducing latency while providing a better customer experience.

Customers should determine the appropriate Azure Region for their workloads based on the location of their users or customer base. If they are targeting a global user base, Azure offers multiple services that ease the global deployment and operations of cloud workloads, reduce latency, and increase application performance. These include:

- Azure Content Delivery Network (Azure CDN) is a global distribution platform for delivering high-bandwidth content near customers at the edge. CDN is used to deliver both static and dynamic content. Benefits include better performance and improved customer experience through reduction of latency.
- Azure Cosmos DB supports true global applications. Cosmos DB is a fully managed, globally distributed, multimodel database that is built to provide low latency and elastic scalability coupled with enterprise-grade performance and security.

Details of Microsoft data residency commitments are provided in the data residency section below.

### Regulatory considerations

Thanks to the harmonized European General Data Protection Regulation (GDPR) and the Digital Single Market (DSM) policy, which enables the free flow of data in the European Union, customers from the European Union are not restricted to keeping data only in the country of origin. Beginning with directive 95/46/EC of the European Parliament and of the European Council, followed by the GDPR, the European institutions seek to harmonize the protection of the fundamental rights and freedoms of individuals in respect to processing activities and to ensure the free flow of personal data between member states.

The European Commission is actively shaping the Digital Single Market, influencing national and international sector regulation to allow free flow of data in this market. This provides customers with choices regarding where they want to deploy their data to ensure a high level of protection for personal data.

In addition to regulatory mandates, data residency requirements may result from internal customer policies or contractual requirements by clients of Microsoft customers. In this case, customers may choose the appropriate Azure region and limit the storage of customer data to this region.

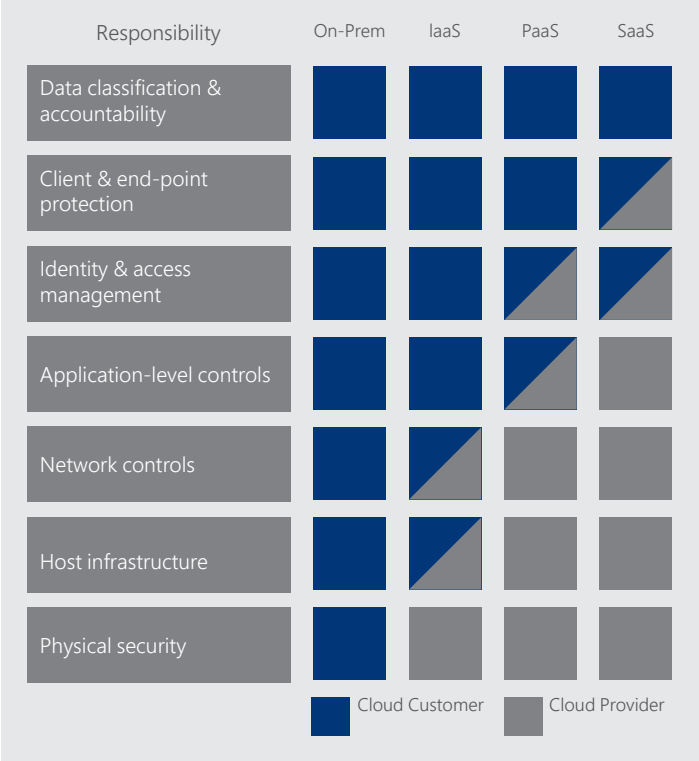
There are also additional requirements for protected data, which are classified by government entities. Microsoft Azure can meet these requirements in several markets.

## Shared responsibility

Shared responsibility in the public cloud comes with hosting resources on a public cloud service provider's infrastructure. Responsibility for each aspect of security depends on which cloud service model is used (IaaS/PaaS/SaaS). With IaaS, the cloud service provider is responsible for the core infrastructure security, which includes storage, networking, and compute at the underlying base operating level (the physical level).

As customers move from IaaS to PaaS and then to SaaS, the customer becomes responsible for less and the cloud service provider is responsible for more.

The figure below describes how shared responsibility works across the cloud service models.




For more detailed information, see the shared responsibility whitepaper.

**Microsoft Azure offers a set of protective measures, controls, and best practices that enhance the overall security of your application.**

# II. Understand the services that Azure provides to help customers meet obligations

One of the most important aspects of cloud security is the development of compliant and secure applications and workloads. Microsoft Azure can help organizations meet the requirements of regulatory mandates and internal policies through the many security measures that are built into its services. Azure offers a set of protective measures, controls, and best practices as discussed in the following subsections.

For security best practices, see the document titled Security Best Practices for Azure Solutions.

## Azure Secure Score

The Secure Score function in Azure Security Center is a security analytics tool that provides customers with visibility into their organizations' security posture and helps assess system security. Secure Score considers the severity and the impact of the recommendation, and based on that information, it assigns a numerical value to show customers how acting on the recommendation can improve the security posture of the customer's cloud solutions.

When a recommendation is remediated, the recommendation score updates and the overall Secure Score is also updated. The overall Secure Score is an accumulation of all recommendation scores.

The main goals of the Secure Score are to provide the following capabilities to the customer's organization:

- Visualization of client's security posture
- Fast triage and suggestions to provide meaningful action to help increase the security posture
- Measurement of the workload security over time

## Data management and data governance services and tools

Data management and data governance are key to a successful business operation in today's data-driven world. The flood of data creates an urgent requirement and responsibility for all organizations to leverage valuable opportunities and protect and secure sensitive data.

Microsoft provides tools to support organizations in evaluating, directing, and monitoring the handling and use of data within the organizations in alignment with ISO/IEC 38505. By using these tools, companies can gain visibility into data that is stored in the platform and can more effectively manage the data.

Microsoft recommends the following four-step process to discover, manage, protect, and document data in public clouds:

1. **Discover: Identify which data types exist and where they reside**
   To support clients' data classification efforts, Microsoft offers the Azure Information Protection (AIP) service. Azure Information Protection is a cloud-based solution that helps organizations classify, label, and protect their documents and emails. This protection can be achieved automatically by administrators who define rules and conditions, manually by users, or through a combination of the two whereby users are provided with recommendations.

Classification is identifiable at all times, regardless of where the data is stored or with whom it's shared. The labels include visual markings such as a headers, footers, or watermarks. Metadata is added to files and email headers in clear text. The clear text ensures that other services, such as data loss prevention solutions, can identify the classification and take appropriate actions.

2. **Manage:** **Govern how data is used and accessed**
   Data protection is achieved via Azure Rights Management (Azure RMS). This is the technology used by AIP and it is integrated with other Microsoft cloud services and applications, such as Office 365 and Azure Active Directory. This protection technology uses encryption, identity, and authorization policies to protect data across multiple devices. Protection that is applied through Azure RMS stays with the documents and emails, independently of their location—inside or outside the customer's organization, networks, file servers, and applications.

   AIP and RMS keep customers in control of their data, even when it's shared with other people. AIP and RMS are globally available services that are built into the Azure platform. Customers can also use Azure RMS with their own line-of-business applications and information protection solutions from software vendors, whether these applications and solutions are on-premises or in the cloud.

3. **Protect:** **Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches**
   As part of an efficient data management strategy, customers can select the appropriate technical and operational measures to safeguard their data in the cloud. Microsoft provides guidelines to help their customers match requirements for regulated data types. These documents are available for download in the Service Trust Platform (STP) portal. The STP is a companion feature to the Microsoft Trust Center, and it allows Microsoft customers to:

   - Access audit reports across Microsoft cloud services on a single page.
   - Access compliance guides that help customers understand how they can use Microsoft cloud service features to manage compliance with various regulations.
   - Access trust documents to help in understanding how Microsoft cloud services help protect data.

Customers who have active paid or trial subscriptions with Azure accounts can access the STP directly. New customers and those who are evaluating Microsoft online services can access the STP by signing up for a product trial.

**Guidance and whitepaper focus areas include the following:**

| Vertical | Region | Offering | Available | Enables deployment of workloads |
|---|---|---|---|---|
| Public sector | Germany | Microsoft Azure will pursue a C5 assessment for its new German datacenters, supporting regulated industries to deploy their compliant workloads in the cloud. The C5 attestation will simplify the deployment of unclassified workloads by German public sector customers to the cloud. | Microsoft Trust Center | Azure Cloud datacenters in Germany |
| Public sector | United Kingdom | The Crown Commercial Service renewed the Microsoft cloud services classification to Government Cloud v6. UK government agencies and partners can use in-scope services to store and process UK government data classified as OFFICIAL, which includes the vast majority of government data. | Microsoft Trust Center | Azure Cloud datacenters in the UK |
| Automotive industry | Europe | Microsoft achieved TISAX certification for selected Azure datacenters, including data classified as AL3 (at least level 2) for selected Azure data centers. | ENX Portal | Selected Azure public clouds |
| FSI customers | Selected markets | Whitepapers on finance and insurance regulation. | Microsoft Trust Center | All Azure public clouds |
| Public sector | Australia | Microsoft is the first global public cloud provider to be awarded certification for protected data in Australia. | Microsoft Trust Center | Azure Cloud datacenters in Australia |
| Merchants | All regions | Microsoft completes an annual PCI-DSS assessment using an approved Qualified Security Assessor. | Microsoft Trust Center | Cardholder data can be stored and processed on the Azure platform. |
| Healthcare | All regions | Microsoft Azure received certification to HITRUST CSF, which allows the deployment of HITRUST solutions to the cloud. Also, Azure was the first major cloud provider that achieved the certification Hébergeur de données santé (HDS), allowing its customers to store health data in its data centers in France. | Microsoft Trust Center | Selected Azure public clouds |

A listing of Microsoft certifications and compliance offerings can be found in the Trust Center.

**4. Report:** **Keep required documentation and manage data requests and breach notifications**

The Azure portal provides tenant admins with a simple, powerful tool to quickly fulfill the Data Subject Requests that are central to compliance with the GDPR. Customers can search for relevant data via service-specific discovery tools, which can be accessed via API or the Azure portal. This makes it easy for customers to delete or maintain the data that is relevant for these requests. Details are described in the respective services' reference documentation, which provides instructions for applicable CRUD (create, read, update, delete) operations.

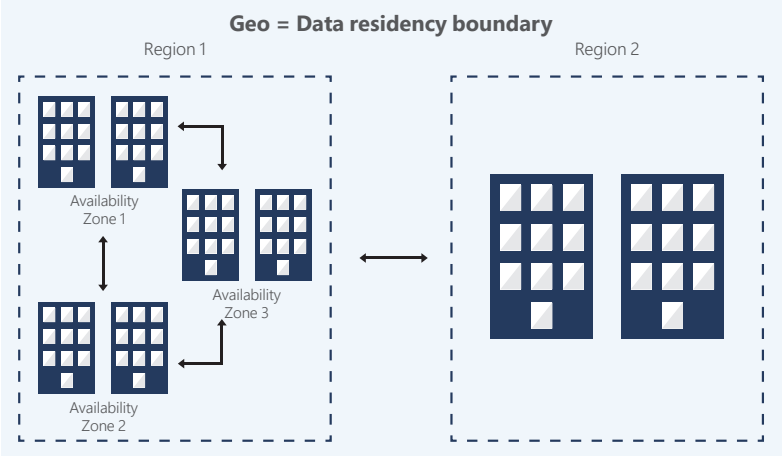
## Customer data residency

Each Azure region is paired with another region (except Brazil) within the same geography; together they make a regional pair or "geo." A geo can be a country or a set of countries (see the Azure datacenter map here). Across each geo, Azure will serialize platform updates (planned maintenance) so that only one geo will be updated at a time. In addition, in the event of an outage affecting multiple regions, at least one region in each geo will be prioritized for recovery. This provides resiliency and business continuity.

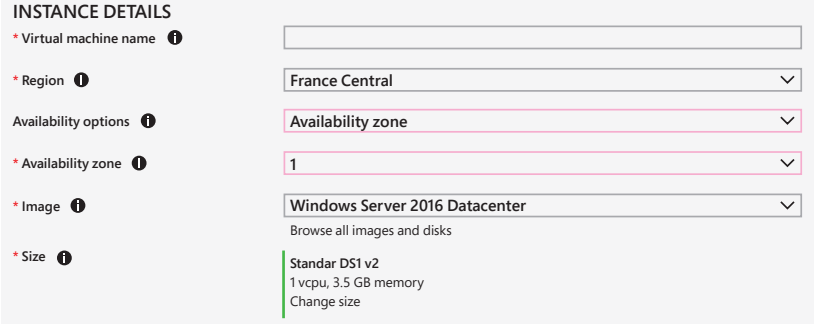
Most Azure services are deployed regionally and enable customers to specify the region into which the service will be deployed, and thus control where the customer data will be stored. Examples of such Azure services include virtual machines, storage, and SQL Database. For a complete list, see Services by Region. For these services, customers preselect the region in which the service will be deployed. The service may replicate customer data stored in that service to other regions in that geo for data resiliency, but Microsoft will not replicate or move customer data outside the geo.

Customers and their end users may still move, copy, or access customer data from any location globally. The Microsoft Trust center outlines where customer data is stored and notes some limited exceptions to this rule on the Azure datacenter map website. For example, if a customer deploys Azure SQL Database or Storage in Germany West Central (announced), the customer data may be replicated to Germany North (announced) for disaster recovery purposes, but will remain stored inside Germany.

Some Azure services (non-regional services) do not enable the customer to specify the region where the service will be deployed because they rely on a global architecture. These non-regional services may store customer data in any Microsoft datacenters unless specified otherwise. Examples include Azure Active Directory, Azure Content Delivery Networks, or services that provide global routing functions and do not themselves process or store customer data, such as Traffic Manager. Information about non-regional services is provided on the Azure datacenter map website and a complete list of non-regional services can be found at Services by Region.




**For regional services, location can be defined by the region variable in the Azure portal or via Azure Resource Manager (ARM) script. As detailed above, customer data will be stored at rest only in the geo for that region.**




**Most Azure services are deployed regionally and enable the customer to specify the region into which the service will be deployed, and thus control where the customer data will be stored.**

### Use Azure Policy to control data residence

Microsoft provides Azure Policy to implement governance over cloud infrastructure and data, including but not limited to which services can be deployed, resource monitoring requirements, or regions in which resources can be deployed. Once policies are established, not only will new resources that are deployed be checked against the policies, but all resources will be periodically scanned to help ensure ongoing compliance.

Policies are composed of conditions or rules that describe when a policy is to be enforced and an effect or action to be executed if the conditions are satisfied. In addition to enabling the ability to create custom policies, Azure Policy offers several built-in policies that are available by default, including the Allowed Locations policy that is used to restrict the locations an organization can specify when deploying resources. Additional information on Azure Policy can be found in the Overview of Azure Policy.

## Tenant separation

The Azure platform uses a virtualized environment, whereby workloads from different tenants run in isolation on shared physical servers, to keep customers' data secure in the multitenant environment. User instances operate as standalone virtual machines that do not have access to a physical host server, and this isolation is enforced by using physical processor privilege levels.

Hypervisors are designed to be as small as possible and undergo rigorous security reviews to prevent a workload from being able to detect other workloads. Each workload sees a virtual storage device containing only the files associated with its own data. Moreover, the hypervisor has complete control to start, stop, and pause workloads. It also controls the physical network cards, so it can filter all the network packets based on the workload identity and tenant. The physical storage media contents are tagged with the tenant owner and associated virtual machine.

In addition, tenants can control their network connectivity between servers and the Internet, and they can create separate virtual networks for different purposes such as production, development, and testing. The hosting provider's fabric controller coordinates with hypervisors hosting workloads for each tenant to make sure only workloads on the same virtual networks of a tenant can see each other's traffic or have connectivity to the Internet.

More information can be found in the document titled Isolation in the Azure Public Cloud.

## Identity Management

Azure Active Directory (Azure AD) the multitenant, cloud-based directory and identity management service from Microsoft. For specific information about where customers' identity data is stored, use the Where is your data located? tool in the Microsoft Trust Center.

**Further information can be found here:**

- Microsoft Trust Center
- Microsoft Trust Center: where your data is located
- Identity data storage for European customers in Azure Active Directory
- Azure Active Directory Data Security Considerations Whitepaper

## Azure encryption

Encryption is a fundamental component that helps ensure confidentiality of cloud workloads. Microsoft Azure provides customers with several offerings to manage and control the security of customer data, including the means to encrypt all of the following:

- Data at rest
- Data in transit
- Data during processing

Microsoft uses multiple encryption methods, protocols, and algorithms across its products and services to help provide a secure path for data to travel through the Azure infrastructure, and to help protect the confidentiality of data that is stored within the infrastructure. Microsoft uses some of the strongest, most secure encryption protocols in the industry to provide protection against unauthorized access to its customers' data. Further information can be found here: Azure encryption overview.

Proper key management is an essential element in encryption best practices, and Azure Key Vault helps ensure that encryption keys are properly secured. With Azure Key Vault and Bring Your Own Key (BYOK), customers have full control over the key management process. Azure Key Vault and BYOK are discussed in more detail later.

**Customer data is automatically encrypted when it's written to Azure Storage by using Storage Service Encryption.**

### Encryption of data at rest

Microsoft Azure provides multiple methods to protect customers' storage instances. Best practice is to use Role-Based Access Control (RBAC) and Azure Active Directory to manage access to customer data.

Further information about RBAC and access management for cloud resources can be found in the document titled What is role-based access control (RBAC)?

Customer data at rest is automatically encrypted when it's written to Azure Storage by using Storage Service Encryption. With this feature, the Azure storage platform automatically encrypts data before persisting it to Azure Managed Disks, Azure Blob, Queue, or Table storage, or Azure Files, and decrypts the data before retrieval. The handling of encryption, encryption at rest, decryption, and key management in Storage Service Encryption is transparent to users. All data written to the Azure storage platform is encrypted through 256-bit AES encryption, which is one of the strongest block ciphers available. Customers can configure encryption keys to be managed by Microsoft or do it themselves, according to their preference.

Further information regarding Storage Service Encryption can be found in the document titled Azure Storage Service Encryption for data at rest.

Customers can configure operating system (OS) and data disks used by Azure virtual machines (VMs) to be encrypted using Azure Disk Encryption. Microsoft Azure offers multiple options to encrypt OS and data discs for Windows Server and Linux instances. Azure Disk Encryption encrypts Windows and Linux infrastructure as a service (IaaS) virtual machine disks by using the BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the operating system disk and the data disk. BitLocker also encrypts Shielded VMs in Windows Server 2016, to ensure that fabric administrators can't access the information inside the virtual machine. The Shielded VMs solution includes the new Host Guardian Service feature, which is used for virtualization host attestation and encryption key release.

Further information regarding encrypting Windows and Linux VM disks can be found in the document titled Azure Disk Encryption for IaaS VMs.

Additional encryption technologies for specific storage types are available, including the following:

- Transparent Data Encryption (TDE) encrypts data at rest when it's stored in an Azure SQL Database and Azure SQL Data Warehouse.
- Always Encrypted supports the ability to encrypt data within client applications prior to storing it in Azure SQL Database.
- Azure Cosmos DB is encrypted by default, using secure key storage systems, encrypted networks, and cryptographic APIs. The encryption keys are managed by Microsoft and rotated per its internal guidelines.
- Azure Data Lake Storage (ADLS) is protected by transparent encryption of data at rest similar to what is provided with Azure SQL Database. Azure Data Lake Store is on by default and performs key management by default, but there is an option to self-manage the keys if desired.

Customers can grant delegated access to the data objects in Azure Storage by using Shared Access Signatures (SASs). A SAS provides granular control over the type of access granted to clients, such as specific permissions and allowed IP range. Further information about SAS can be found in the document titled Using shared access signatures (SAS).

Azure storage analytics can track the authentication method that someone is using when they access Storage. Storage Analytics metrics are enabled by default for new storage accounts. Logging can be enabled, and both metrics and logging can be configured in the Azure portal.

Further information about how to enable and use this tool can be found in the document titled Storage Analytics.

## Encryption of data in transit

Microsoft enables and encourages Azure customers to encrypt customer data in transit to Microsoft datacenters through the Transport Layer Security (TLS), which uses a combination of asymmetric (TLS handshake) and symmetric (shared secret) cryptography to encrypt communications as they travel over the network. In support of the Microsoft promise to provide best-in-class encryption to customers, Microsoft will discontinue support for the less secure Transport Layer Security (TLS) versions 1.0 and 1.1, in favor of TLS version 1.2.

Microsoft also uses the Internet Protocol Security (IPsec), an industry-standard set of protocols, to provide authentication, integrity, and confidentiality of data at the IP packet level as the data is transferred across the network.

Investment by Microsoft in research and development has brought about a breakthrough in encryption of data in transit. Every Azure server contains Azure SmartNICs, which are based on the Field Programmable Gate Array (FPGA) technology. These FPGAs are programmable hardware modules, which significantly speed up the processing of data, including encryption of data in transit. This enables high performance for all workloads along with low latency. Microsoft publishes the hardware design under an open source license, allowing the community and its customers to benefit from this innovation.

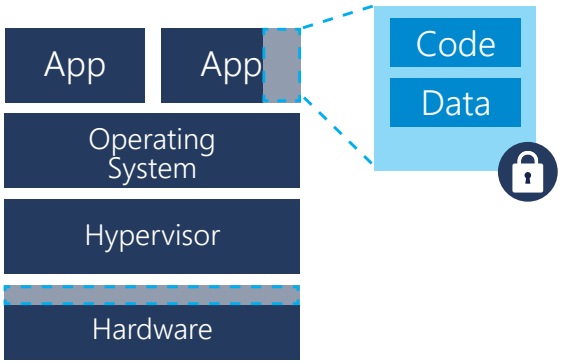
Further information on Microsoft's hardware innovation for the cloud can be found here.

## Encryption during processing of data–Confidential computing

Azure confidential computing is a new offering which provides an additional security level for customer data while it is in use. It helps protect customer data at runtime, creating a trusted environment for high-security requirements. Confidential computing helps ensure that when data needs to be "in the clear"(unencrypted) for efficient processing, the data is protected inside a Trusted Execution Environment (TEE), also known as an enclave. An example is shown in the figure below.

Confidential computing brings TEEs such as Intel SGX and Virtualization Based Security (VBS), previously known as Virtual Secure mode, to the cloud. TEEs help to ensure that no one on the outside can view the data or the operations inside the TEE, even with a debugger. This also helps to ensure that only authorized code is permitted to access data. If the code is altered or tampered with, the operations are denied and the environment is disabled. If implemented correctly, the TEE enforces these protections against viewing and modification, including access by Microsoft personnel, during the time the data is being processed.

The figure below illustrates how the TEE protects the data and code during processing.




Further information about Azure encryption technologies and options can be found here:

- Azure Encryption Overview
- Azure Data Encryption-at-Rest
- Azure Data Security and Encryption Best Practices
- Azure Cosmos DB Encryption
- Storage Service Encryption using customer-managed keys in Azure Key Vault
- Azure Storage Security Guide
- Azure Confidential Computing

## Azure Key Vault with Bring Your Own Key (BYOK)

Azure Key Vault, mentioned above, is a cloud-hosted service that provides centralized storage and management of cryptographic keys and other secrets that are used in customers' cloud applications. This Azure service enables customers to safeguard cryptographic keys, certificates, and application passwords, and helps protect secrets from accidental leakage.

Azure Key Vault uses specialized hardware security modules (HSMs) for maximum protection and is designed in a way that allows customers to maintain control of keys and data. Usage of customers' stored keys can be monitored and audited in different ways, including Azure logging and the import of these logs into Azure HDInsight. Customers can also incorporate this information into their existing security information and event management (SIEM) systems. This supports Microsoft customers in performing additional analysis, such as threat detection.

Azure Key Vault allows segregation of secrets in multiple vaults. This helps reduce the chances of accidental loss of security information by centralizing the storage of application secrets. Azure Key Vault can handle requests and renewals of TLS certificates. It also provides features that enable robust certificate lifecycle management.

Note that Azure Key Vault is designed to support application keys and secrets and it is not intended to be a store for user passwords. Access to a key vault is controlled through two separate interfaces: the management plane and the data plane. The management plane and data plane access controls work independently. Customers should use dedicated role definitions in Azure Active Directory to manage role-based access. This approach implements an effective segregation of duties.

Azure Key Vault also provides a bring-your-own-key capability. Customers can generate the keys on-premises using an offline workstation equipped with a Thales HSM and then transmit the keys securely to the Azure HSMs in the cloud. The Thales software used for the key submission ensures that the keys are bound to this environment and can never be extracted out of the HSMs. Customers who require additional functions such as enterprise key management processes or hybrid cloud setups can use the CipherTrust Cloud Key Manager from Thales.

Further information about how to use Azure Key Vault to protect secrets, certificates, and keys can be found here:

- Integrate Azure Key Vault logs into HDInsights
- Bring your own Key–Azure Key Vault

## Solutions for telemetry data

Telemetry refers to automated collection of data and can take on many forms. For cloud services where customer data is stored and processed in the cloud, telemetry consists of application and server logs that are required to maintain modern applications and platforms. These logs provide customers with the information they need to operate and troubleshoot their workloads and provide Microsoft with the information needed to operate, troubleshoot, and improve the platform.

Microsoft utilizes telemetry data for clearly defined usage scenarios, in line with GDPR requirements and aligned to the best practices described in ISO/IEC 19944. Service health is an important aspect of telemetry analysis. Microsoft collects schematized telemetry data to diagnose and perform root-cause analysis on incidents for the platform. Services utilize this data to trigger self-healing processes, and this reduces the amount of manual human intervention required. As an example, when the load on a specific component increases, the platform assigns more resources to cope with the demand.

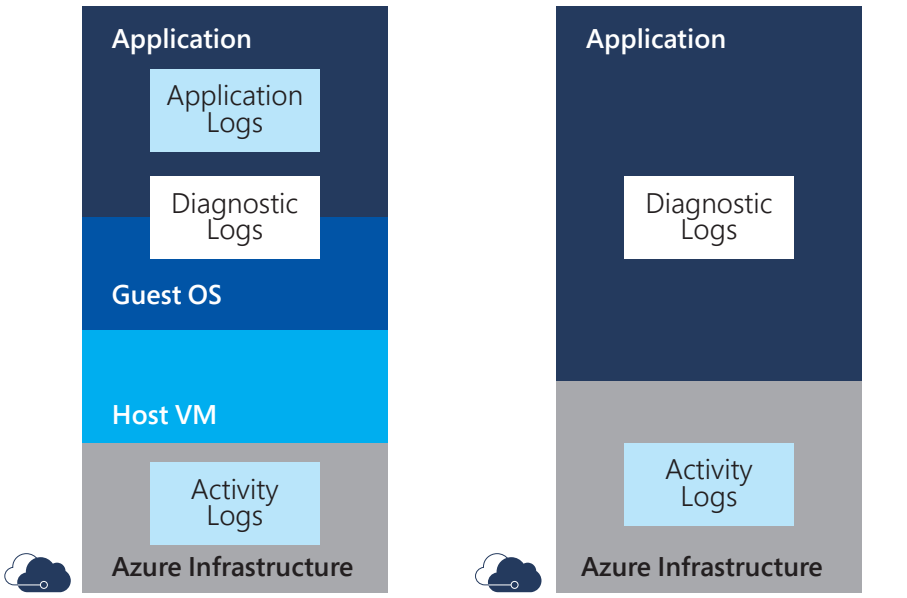
Microsoft has integrated anonymized telemetry into the Azure DevOps tools, providing engineers with valuable information to reduce error in the code. To enable pay per use, telemetry data is used for billing purposes and is sent to central billing tools.

Customers can use Microsoft Azure tools to manage the health of their workloads. This generates telemetry information. For example, telemetry data is collected by the following services:

- **Azure Monitor** This service provides a 360-degree view of applications, infrastructure, and the network with advanced analytics, dashboards, and visualization maps. Azure Monitor provides customers with a centralized hub that helps to identify network glitches, CPU spikes, memory leaks in code, and other issues before they impact the customer's workload.

- **Application Insights** Application Insights is an extensible Application Performance Management (APM) service for web developers on multiple platforms. It can monitor web applications during runtime. It will automatically detect performance anomalies and it includes powerful analytics tools to help diagnose issues and understand what users actually do with the app. Application Insights helps to continuously improve performance and usability by sending telemetry from the customer's web applications to the Azure portal. It works for apps on a wide variety of platforms, including .NET, Node.js, and J2EE, hosted on-premises or in the cloud. Collectors are designed to provide a schematized output of data, limit the transmission of personal data as much as possible, and transmit the data securely. The user must define a data retention policy. Customers can also utilize this data to build high-availability workloads, which can detect an incident based on the telemetry information and perform automated predefined actions to mitigate the incident.

The figure below illustrates the coverage of the log solutions.




**Transparency and customer control**
Azure provides transparency and control functions for some of the most common types of telemetry scenarios using Windows Server and Linux virtual machines.

**Windows Server VM on Azure: telemetry insights**
Windows Server images on Azure are set up similarly to off-the-shelf products. Customer administrators can adapt the telemetry configuration from on-premises to cloud instances.

Customers can control the diagnostic data they share with Microsoft with easy-to-use management tools provided by Microsoft. For example, Windows Security Baselines can be used to efficiently configure Windows 10 and Windows Server settings for best security practices.

Further information on how to use security baselines can be found in the document titled Windows security baselines.

Some customers may want to minimize connections from their Windows systems to Microsoft services. The Windows Restricted Traffic Limited Functionality Baseline can be used to restrict such connections from Windows Server to Microsoft.

The Windows Restricted Traffic Limited Baseline (.zip file) can be downloaded at https://go.microsoft.com/fwlink/?linkid=828887.

Further information about the Windows Restricted Traffic Limited Functionality Baseline can be found in the document titled Manage connections from Windows operating system components to Microsoft services.

Windows Server diagnostic data settings can be configured using familiar management tools, such as Group Policy, MDM, Windows Provisioning, or Registry. Setting the Windows Server diagnostic data levels through a management policy overrides any device-level settings.

Microsoft has also provided a PowerShell cmdlet that enables customers to delete existing Windows diagnostic data that was transferred to Microsoft from the current device. The script can be launched manually via the command line or implemented as an automated script for Windows Server 2016/2019 Virtual Machines.

Further information about how to manage Windows Diagnostic Data can be found here:

- WindowsDiagnosticData Documentation
- Powershell WindowsDiagnosticData is available for download here.

**Linux VM on Azure: telemetry insights**
For customers who run Linux virtual machines on Azure, Microsoft provides the Linux agent (WALinuxagent) as open source software to their clients. It is available at GitHub. Microsoft provides full transparency so administrators will know which data are sent from Linux to the Azure platform. This information can be correlated and used for further analysis, to monitor important system metrics and to perform data-based decisions. Additionally, customers can implement log analytics to analyze application-level logs.

**Nearly all service operations performed by Microsoft are fully automated and human involvement is highly controlled and abstracted away from customer data.**

## DevOps access and Lockbox

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.

The design principles defined for the development of Azure services require a schematized telemetry setup. In Azure, the most important use case for telemetry is its use as a sensor for the automated operation of the cloud. Based on the telemetry information and desired state configuration, remediation activities are triggered via automation, thus reducing the additional risk caused by manual human intervention.

Azure undergoes a Service Organization Control (SOC) audit by an American Institute of Certified Public Accountants (AICPA) accredited auditor every three months to verify the effectiveness of its security controls in audit scope. The SOC 2 Type 2 attestation report published by an accredited auditor explains the circumstances under which access to customer data can happen, and how. See the latest report titled Azure and Azure Government SOC 2 Type II Report for more information. By far, the most common scenario involves a customer opening a troubleshooting ticket with Azure Support and requesting access to customer resources that could potentially include customer data.
For the majority of support scenarios, access to customer data is not needed.

Access to customer data is restricted, based on business need, by role-based access controls, multifactor authentication, minimization of standing access to production data, and other controls. Access to the platform of DevOps personnel is requested via the Just-in-Time (JIT) access tool. All access to customer data is strictly logged, and both Microsoft and third parties perform regular audits (as well as sample audits) to attest that any access is appropriate.

### Customer Lockbox for Microsoft Azure

To further safeguard customer data, Microsoft has introduced the Customer Lockbox for Microsoft Azure. Customer Lockbox is a new service that provides customers with the capability to control how a Microsoft engineer can access the customers' content stored in an Azure service in those rare instances when it's necessary. As part of the support work flow, a Microsoft engineer may require elevated access to customer content. Customer Lockbox puts the customer in charge of that decision by enabling the customer to review and approve or deny such elevated requests.

Customer Lockbox is an extension of the Just-in-Time (JIT) work flow and also comes with full audit logging enabled. Customers can access the logs related to Customer Lockbox via the Azure portal and integrate them into their SIEM systems.

Further information on Customer Lockbox for Azure can be found here.

Note again that for the majority of support scenarios, access to customer data is not needed and the work flow should not require Customer Lockbox.

### Implementation of policies

Microsoft has created a set of internal policies and technical controls that govern data handling. These controls and policies are designed to conform with International Organization for Standardization ISO27018, the standard of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. For example, for application code, any output written to the log files goes through data scrubbers that remove customer data before the data is sent to central systems. These measures minimize the risk of customer data being replicated to analysis or operations repositories.

## Solutions for hybrid and on-premise environments

Microsoft delivers multiple solutions to enable intelligent edge solutions. This allows customers to benefit from cloud services while retaining data on their premises and addresses requirements whereby data must not leave the environment, even for technical concerns or policy requirements.

### Microsoft Azure Stack

Microsoft Azure Stack is an extension of Azure; it brings the agility and innovation of cloud computing to customers' on-premises environments and enables the only hybrid cloud that allows the building and deployment of hybrid applications anywhere. Organizations can build modern applications across hybrid cloud environments, balancing the right amount of flexibility and control.

Developers can build applications using a consistent set of Azure services and DevOps processes and tools, then collaborate with operations to deploy to the location that best meets the business, technical, and regulatory requirements. Developers can speed up new cloud application development by building on application components from the Azure Marketplace, including open source-tools and technologies.

Azure Stack offers a rich set of tools and automation that enables Microsoft customers to manage workloads on-premises similarly to their cloud workloads. Customers are in full control of customer data and can set up hybrid scenarios so classified workloads on-premises can interact securely with workloads in the cloud. Security considerations and compliance regulations are important drivers for organizations that choose to control their infrastructures using private/hybrid clouds while using IaaS and PaaS technologies to modernize their applications. Azure Stack was designed for these scenarios, and security and compliance are areas of major investment for Azure Stack.

The whitepaper Azure Stack: An extension of Azure provides more about this.

Further information about security and compliance controls in Azure stack can be found in the document titled Azure Stack infrastructure security posture.

## Data Box Edge and gateway

Microsoft has announced hardware devices and virtual machines for on-premises deployment that provide integration features for hybrid workloads. The Azure Data Box Edge is a storage solution that can pre-process AI (artificial intelligence) workloads on-premises. It is a physical appliance that resides on the customer's premises. It accelerates secure data transfer because only a subset of information needs to be sent to the Azure Cloud. This gives the customer control over the data flow and data sovereignty. The device creates a centrally managed and secure connection to the cloud. Key management can be fully performed by the customer.

The Azure Data Box Edge documentation provides further information.

# III. Understand the assurance or evidence that customers need to assert compliance

Complying with regulatory and policy requirements isn't enough; organizations must also be able to prove that they are in compliance. Microsoft can help customers do this, through its compliance offerings and tools such as Compliance Manager, as well as security assurance measures and commitments defined in the Online Services Terms (OST). In addition, Azure Security and Compliance Blueprints help customers deploy solutions in scenarios that have compliance requirements.

## Compliance offerings

Microsoft Azure possesses an industry-leading compliance portfolio. This helps customers meet their compliance commitments. Azure compliance offerings are grouped into four categories: globally applicable, US government, industry specific, and region/country specific. Compliance offerings are based on various types of assurances, including formal certifications, attestations, validations, authorizations, and assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents produced by Microsoft.

Learn more about the extensive Microsoft Azure compliance offerings in the whitepaper titled Overview of Microsoft Azure compliance.

The online database in the Microsoft Trust Center provides a list of Microsoft's compliance offerings.

### Compliance Manager

Compliance Manager enables customers to manage their organizations' compliance activities from one centralized place. It's a cross-Microsoft-Cloud solution that helps organizations understand and manage the complex compliance landscape. Organizations can use it to perform ongoing risk assessments and receive actionable insights that help to improve data protection capabilities and simplify processes with the built-in collaboration and audit-ready reporting tools.

Compliance Manager provides three key capabilities:

- **Control mapping** – GDPR, ISO 27001, and ISO 27018.
- **Facilitate collaboration** – Assign, track, and record compliance-related activities for more efficient collaboration across teams.
- **Assessments and audits** – Conduct pre-audits to prepare for external audits.

To help organizations assess Microsoft Cloud under the shared responsibility model, Compliance Manager provides a dashboard view of assessments that clearly shows the implementation progress of controls that fall under the responsibility of Microsoft and those that are the customer's responsibility. The compliance actions provided by Compliance Manager are recommendations; it's up to the customer to evaluate and validate the effectiveness of these recommended customer controls as they relate to the organization's regulatory environment. Implementing the recommendations does not guarantee compliance.

Learn more about how to use Compliance Manager to help meet data protection and regulatory requirements when using Microsoft cloud services.

**Compliance Manager enables customers to manage their organizations' compliance activities from one centralized place.**

## Protected data

Microsoft Azure provides protection that meets the requirements of many different local regulatory entities around the world. For example, Microsoft has undergone an IRAP (Information Security Registered Assessors Program) assessment. This certification provides assurance to Australian public sector customers in government and their partners that Microsoft has appropriate and effective security controls in place for the processing, storage, and transmission of sensitive and official information that holds Dissemination Limiting Markings (DLMs) or is classified at the Protected level. This includes the majority of government, healthcare, and education data in Australia.

Learn more about IRAP assessments.

**Microsoft believes data privacy is a fundamental right, and that the GDPR is an important step forward for clarifying and enabling individual privacy rights.**

## Data privacy compliance and the GDPR

Microsoft is committed to complying with local privacy laws and protecting the privacy of its users. The Azure compliance portfolio includes conformity to cloud privacy practices such as ISO/IEC 27018. That commitment includes ensuring that Microsoft products and services comply with laws that are applicable to cloud providers, such as the GDPR.

Microsoft will comply with all laws and regulations applicable to its provision of its Online Services, including security breach notification laws. However, Microsoft is not responsible for compliance with any laws or regulations applicable to the customer or the customer's industry that are not generally applicable to information technology service providers. Microsoft does not determine whether customer data includes information subject to any specific law or regulation.

Microsoft believes data privacy is a fundamental right, and that the GDPR is an important step forward for clarifying and enabling individual privacy rights. Also, Microsoft recognizes that the GDPR required significant changes by organizations all over the world with regards to the discovery, management, protection, and reporting of personal data that is collected, processed, and stored within an organization.

Microsoft contractually commits to meet GDPR requirements not only in the European Union but in all public cloud regions. Microsoft also contributes actively to upcoming privacy standards, such as the ISO/IEC 27522.

# Security assurance

Microsoft helps provide security assurance to customers through the Security Development Lifecycle (SDL) and by conducting regular penetration testing of Azure, along with other practices designed to improve security in the cloud environment.

## Security Development Lifecycle (SDL)

The Microsoft SDL was established as a mandatory policy in 2004 and was designed to be an integral part of the software development process at Microsoft. The development, implementation, and constant improvement of the SDL represents a strategic investment by Microsoft in the security effort.

The SDL signified an evolution in the way software is designed, developed, and tested and it has now matured into a well-defined methodology. The Microsoft commitment to a more secure and trustworthy computing ecosystem has also inspired the creation of a wealth of guidance papers, tools, and training resources that are available to the public.

Learn more about the Security Development Lifecycle.

### Penetration tests

Microsoft continuously conducts penetration tests of the Azure platform. To optimize the penetration testing approach, Microsoft utilizes the red team/blue team approach. The red team focuses its efforts on attacking the internal Azure infrastructure, while governed by rules of engagement. The blue team is the defense team, which focuses on real world response; its members are tasked with finding and preventing attacks. In addition to this internal penetration testing work, Azure also undergoes annual penetration testing by an external, independent entity.

Learn more about penetration testing in the video titled Red vs. Blue–Internal security penetration testing of Microsoft Azure.

Customers can perform penetration testing themselves or via a third party, as well. To do so, they must comply with the terms stated in the Microsoft Cloud Unified Penetration Testing Rules of Engagement. Download the Penetration Testing Rules of Engagement.

## Commitments defined in the Online Services Terms

When customers subscribe to an Online Service through a Microsoft Volume Licensing program, the terms that control how they can use the service are defined in the Volume Licensing Online Services Terms (OST) document and program agreement. Due to the frequency with which Microsoft adds new services, the OST is updated monthly. Additional amendments exist to cover restricted industries, including financial services. The OST is available in 35 language versions. An accessible archive contains older versions for reference.

Learn more about the OST on the Licensing Terms webpage.

The Online Services Terms cover important aspects of cloud usage by Microsoft customers, including the following:

- **Data privacy commitments:** Microsoft has implemented operational processes to meet the exacting requirements of the GDPR. Microsoft also offers customers EU Model Clauses, referred to in the Online Services Terms as Standard Contractual Clauses, that make specific guarantees around transfers of personal data for in-scope Microsoft Azure services.
- **Technical and organizational measures:** Microsoft describes and documents technical and organizational measures in the Online Services Terms. Those measures are set forth in the Microsoft Security Policy, which is available for download in the Trust Center. These comply with the requirements for Information Security Management Systems (ISMS) set forth in ISO27001, ISO 27002, and ISO 27018. Additional descriptions of the technical and organizational measures can be found in the Microsoft Azure SOC 2 Type 2 assessment report, which is available in the Trust Center.
- **Service level agreements (SLA):** The detailed service level terms for Microsoft Azure can be found on the Service Level Agreements page of the Azure website.

## Security and Compliance blueprints

Microsoft Azure provides a series of security and compliance blueprints, which support customers in highly regulated markets to build compliant, cloud architectures. The blueprints also include best practices and patterns for various compliance controls, enabling Microsoft customers to utilize the newest technologies and state-of-the-art security for their workloads.

These blueprints provide detailed deployment instructions, including guidelines on automation, architecture diagrams, and documentation. They also provide threat models, which support the risk management process and point to potential risks when customers perform modifications.

The Azure Security and Compliance blueprints can be accessed via the "Compliance" section of the Azure Security Documentation web site.

## How Microsoft handles government requests

Microsoft has taken a firm public stand on protecting customer data from inappropriate government access, and where necessary, it has advanced its position through the courts. Microsoft will continue to push for new international agreements that add to their customers' rights.

**Microsoft has taken a firm public stand on protecting customer data from inappropriate government access, and where necessary, it has advanced its position through the courts. Microsoft will continue to push for new international agreements that add to our customers' rights**

When Microsoft receives a government or law enforcement request for customer data, Microsoft attempts to redirect the third party to obtain the requested data from the customer and may provide the customer's basic contact information to facilitate this. Microsoft will promptly notify the customer of any third-party request and give the customer a copy where permitted. For valid requests that Microsoft is not able to redirect to the customer, 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 site, which brings together in one place the reports that Microsoft issues regularly on requests for customer data made by law enforcement, as well as government requests related to U.S. national security.

The aggregate data Microsoft has published shows clearly that only a tiny percentage—a small fraction of one percent—of Microsoft customers have ever been subject to a government request related to criminal law or national security. For enterprise customers, that number drops further to a mere handful.

# IV. Applying the framework to selected European markets

The general security and compliance framework discussed in this paper can be more specifically applied to various geographic markets. The following sections discuss applicability to the German and French markets.

## France

Microsoft Azure operates two datacenter regions in France, providing its customers a platform to run their workloads in close proximity to their clients in France.

### Data privacy

Thanks to the efforts Microsoft has invested in GDPR compliance, personal data as defined by the French Data Protection Act (FDPA and the amendment FDPA2) and regulated by the CNIL (Commission Nationale de l'Informatique et des Libertés) can be stored in all Azure public cloud datacenters. Customers must assess in advance the compliance of a particular data location, depending on their data classification. The shared responsibility section in this whitepaper provides additional help in determining the appropriate technical and organizational measures that are required to protect personal data.

### Finance industry regulation

Microsoft offers a checklist, that provides customers regulated by the Autorité des Marchés Financiers (AMF) and Autorité de Contrôle Prudentiel et de Résolution (ACPR) with guidance to meet regulatory requirements for the finance and insurance industries.

Download the checklist from the Service Trust Portal.

### Hébergeur des données de santé (Health Data Hosting)

Microsoft achieved the certification Hébergeur des données de santé on the 31st of October 2018 for the Azure datacenter in France, becoming the first cloud provider with this offering. Cloud services help to modernize the French IT systems in the health sector and improve the service for patients. Organizations from the life science and healthcare sectors can utilize Azure core services to process health data in their workloads.

### TISAX (Trusted Information Security Assessment Exchange)

The European automotive industry created the TISAX (Trusted Information Security Assessment Exchange) standard to establish a common assessment framework for all suppliers. An independent auditor completed the TISAX assessment for specific Microsoft datacenters at Level 2 (AL2). An AL2 assessment is required for data with a high need for protection, such as data classified as confidential. The TISAX audit report can be obtained by members on the ENX (European Network Exchange) portal.

**Compliance mapping for Azure regions in France**

| Sector | ISO 27001<br>Validation that security controls and ISMS is in place | ISO 27018<br>Protection of PII | Financial Checklist | SOC 2 Type II<br>Independent AICPA SOC controls assessment | TISAX<br>Enables classified workloads for the automotive industry |
|---|---|---|---|---|---|
| Public Sector | ✓ | ✓ | | ✓ | |
| Finance Insurance | ✓ | ✓ | ✓ | ✓ | |
| Automotive | ✓ | ✓ | | ✓ | ✓ |
| Healthcare | ✓ | ✓ | | ✓ | |

## Germany (new regions)

Microsoft Azure provides solutions to help clients meet their compliance requirements. This section covers information specific to the German market as Microsoft prepares to launch its new public Germany regions in 2019, which will benefit from the feature-rich security solutions and controls of the global Azure public cloud.

### IT-Security Act

All Microsoft Azure datacenters on German soil will be in scope as critical infrastructure, as defined by the German IT-Security law (IT Sicherheitsgesetz). Independent third-party audits will be used to pursue compliance with this regulation for Microsoft Azure services deployed in Germany.

### C5 Compliance Attestation

The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) established the Cloud Computing Compliance Controls Catalogue (C5), which describes the baseline for cloud security in regulated markets, especially the public sector, finance, and insurance industries. Microsoft Azure will pursue a C5 assessment for its German datacenters, to support regulated industries in deploying their compliant workloads in the cloud. The C5 attestation will simplify the deployment of unclassified workloads by German public sector customers in the cloud.

### IT Grundschutz

In Germany, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) provides the IT-Grundschutz methodology, which consists of an ISO- 27001-compatible ISMS (BSI Standards 200-1, 200-2) and a dedicated risk analysis method (BSI Standard 200-3).

Microsoft will pursue creating together with a partner, a workbook to help Microsoft Azure customers who wish to use Azure services to implement the IT-Grundschutz methodology within the scope of their existing or planned ISO 27001 certification based on IT-Grundschutz.

### Data privacy

Thanks to the efforts Microsoft has invested in GDPR compliance, personal data as defined by the Federal Data Privacy Law (BDSG-new) can be stored in all Azure public cloud datacenters. Customers must assess in advance the compliance of a particular data location, depending on their data classification. The shared responsibility section in this whitepaper provides additional help in determining the appropriate technical and organizational measures that are required to protect personal data.

### TISAX (Trusted Information Security Assessment Exchange)

The European automotive industry created the TISAX (Trusted Information Security Assessment Exchange) standard to establish a common assessment framework for all suppliers. Microsoft will pursue TISAX certification for Azure Germany. The TISAX audit report for European regions can be obtained by members on the ENX (European Network Exchange) portal.

**Compliance mapping for Azure regions in Germany**

| Sector | IT-Security Act | BSI C5<br>Attestation for BSI C5 requirements | ISO 27001<br>Validation that security controls and ISMS are in place | ISO 27018<br>Protection of PII | Grundschutz Workbook<br>Supports our clients to map the existing security controls of Azure to their Grundschutz ISMS | SOC 2 Type II<br>Independent AICPA SOC controls assessment | TISAX<br>Enables classified workloads for the automotive industry |
|---|---|---|---|---|---|---|---|
| Public Sector | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Finance Insurance | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Automotive | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| Healthcare | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |

# Conclusion

This whitepaper provides insights on key security offerings of the Azure platform and is designed to help customers in restricted industries understand how to achieve compliant workloads in the public Azure cloud, including in the new Germany regions, France, and other public Azure regions.

Microsoft continuously adds features and documentation to assist customers in addressing their compliance needs and to provide transparency regarding Microsoft practices and processes. This documentation will be updated as new features become available.


Microsoft