Microsoft

Data Residency, Data Sovereignty, and Compliance in the Microsoft Cloud

Contents

Authors: **David Burt and Carol Brown**

Executive summary

Organizations of all sizes are moving to take advantage of the many benefits offered by cloud computing—increased scalability and security, the availability of new technologies, and cost savings. But as they move to the cloud, organizations want to maintain the same level of control over their IT resources as they have in their datacenters. They want their data to be stored and processed in secure facilities, protected from access by criminals, other cloud tenants, government agencies—even the cloud vendors themselves. And they want their data stored as locally as possible, or even on their own premises yet connected to the cloud. In addition to their own needs, organizations are subject to compliance with a growing number of legal and other requirements by governments and industry associations.

Microsoft has decades of experience helping customers keep their data secure, private, and under their control, while also enabling them to comply with regulations and standards relevant to their unique business. The large and ever-expanding network of datacenters comprising the Microsoft Cloud can offer data residency in more places in the world than any other cloud provider. A strong set of policies and technologies offers customers robust options for protecting and controlling their data. The Microsoft Cloud complies with over 100 national, regional, and industry-specific requirements—the most in the industry—providing a foundation for customer compliance. While most customers can meet all their needs relying on the public Microsoft Cloud, those customers who have exceptional needs can take advantage of a range of options that provide enhanced data residency and data sovereignty.

The large and ever-expanding network of datacenters comprising the Microsoft Cloud can offer data residency in more places in the world than any other cloud provider. A strong set of policies and technologies offers customers robust options for protecting and controlling their data.

This paper is written to guide organizations looking to adopt or expand their use of cloud computing services. It offers a detailed look at the data residency, data sovereignty, and compliance aspects of the three main Microsoft cloud services: Microsoft Azure, Microsoft Dynamics 365 and Power Platform, and Microsoft 365. The paper is divided into five main sections:

Understanding data residency, data sovereignty, and compliance gives an overview of each of these core concepts, including an overview of regulatory and technical issues.

Microsoft Cloud infrastructure describes the geographic options for storing data for each of the three main services in the Microsoft Cloud and those of specialized clouds.

Data residency in the Microsoft Cloud gives an overview of data residency options for each of the three main Microsoft cloud services and for hybrid and multicloud services.

Data sovereignty in the Microsoft Cloud discusses how Microsoft manages, protects, and restricts access to customer data, including Microsoft legal policies for government and law enforcement requests for data. Here is an overview of relevant tools for protecting customer data including encryption, key management, and data governance.

Compliance in the Microsoft Cloud provides a summary of the over 100 compliance offerings supported by Microsoft, along with the tools Microsoft offers to help organizations manage their own compliance requirements.

I. Understanding data residency, data sovereignty, and compliance

The three concepts addressed in this paper—data residency, data sovereignty, and compliance—have broad meanings and are sometimes used inconsistently. It's important, therefore, to define them for the purposes of cloud computing and explain how they relate to one another.

Data residency

Data residency is the requirement that data must be stored within a specific geographic boundary, such as within a national boundary. Data residency can be a requirement of a local, national, or regional law or regulation; a nongovernmental requirement such as an industry standard and a certification of compliance; or the contractual terms of a business agreement. Notably, some regulations addressing the transfer of data do not require data residency if adequate protective measures are taken.

Data residency requirements usually apply to all customer data, but in some cases can apply only to specific types of data, such as personal data, health data, or financial data.

Microsoft offers data residency for many services in over 35 countries, more than any other cloud provider, and continues to expand to more countries. This gives Microsoft Cloud customers ever-increasing choices for storing and processing data locally. Data residency options are discussed in Section III.

Data sovereignty

Data sovereignty refers to the concept that data is under the control of the customer and governed by local law. There are two main facets to data sovereignty: enforcement of the customer's control through security and data governance, and the requirement that their data is bound by the laws of the country where the organization is located.

Customers can achieve data sovereignty through administrative policies and technical controls that govern who can access data, how it is used and stored, and how long the customer can retain it. Sovereignty policies can be enforced through such measures as encryption, key management, access controls, and data governance.

The data an organization collects, stores, and processes is bound by the laws and general best practices of the jurisdictional location of that organization. While data residency ensures that data stays in a specified geographical location, data sovereignty makes sure that data adheres to the regulations of the country where the organization is located.

Section IV of this paper discusses in detail the Microsoft policies for managing data that support data sovereignty, including a section on law enforcement access to data. It also outlines the technical measures that both Microsoft and customers can use to secure and govern their data.

Compliance

Compliance refers to the ability of an organization to satisfy industry, national, or global compliance standards and regulations. When referencing cloud computing, compliance usually refers to a specific law, best practice, or standard that governs an information technology (IT) system. Most IT standards and regulations specify controls that govern policies, access, operations, data residency and sovereignty, and the like. Examples include the widely used ISO/IEC 27001 standard for information security management and ISO/IEC 27701, which specifies requirements for a privacy information management system.

The Microsoft Cloud complies with over 100 national, regional, and industry-specific requirements, and Microsoft offers tools to help customers manage their own compliance requirements.

Compliance can be demonstrated through formal certifications and third-party audits as well as by contractual commitments, self-assessments, and customer guidance documents. All these can be used to show that an organization or a cloud service, such as the Microsoft Cloud, meet benchmark IT security, privacy, and data management requirements. They can also serve as a record of the measures that have been implemented to mitigate potential risks.

Certifications and independent audit reports offer formal assurance of an IT system's adherence to a set of requirements. Well-known certifications include the Federal Risk and Authorization Management Program (FedRAMP); Health Information Trust Alliance (HITRUST) Common Security Framework (CSF); the ISO/IEC series of standards; and Payment Card Industry (PCI) Data Security Standards (DSS). Widely acknowledged audit reports include those of Service Organization Controls (SOC) and ISO/IEC 27701. Customers can often obtain a copy of the certificate showing that an IT service complies with the standard and the related audit report.

Most other assurance of compliance relies on attestations or statements by the vendor or IT system owner that an IT system meets a requirement. Common attestations of compliance include those required by the Health Insurance Portability and Accountability Act (HIPAA) and Cloud Security Alliance (CSA) STAR, as well as Standard Contractual Clauses. While attestations are not independently audited and certified, they still provide valuable assurance that required controls have been met.

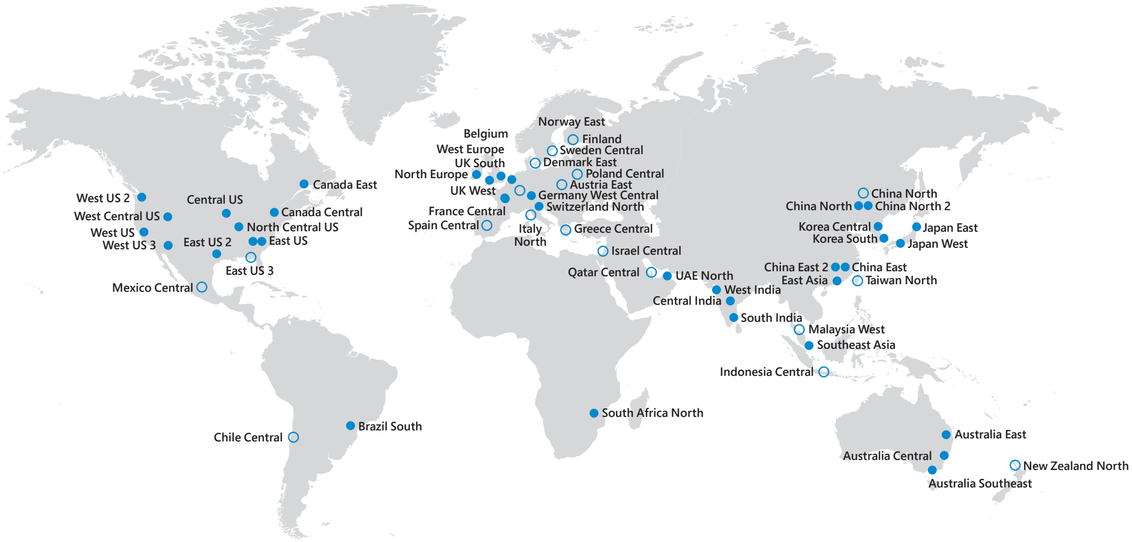
Section V of this paper describes how the Microsoft Cloud complies with over 100 national, regional, and industry-specific requirements, and the tools Microsoft offers to help customers manage their own compliance requirements.

II. Microsoft Cloud infrastructure

The Microsoft Cloud global infrastructure is made up of two key components—physical infrastructure and virtual network components. The physical component comprises over 200 physical datacenters (each datacenter houses a set of networked computer servers) organized into regions and geographies, which are then linked by one of the largest interconnected networks on the planet.

200+ Datacenters | **60+** Datacenter regions | **35+** Countries with data

● Available region
○ Announced region



The Microsoft Cloud global infrastructure

With the connectivity of the global Microsoft network, every datacenter provides low latency, scalability, and the latest advancements in cloud infrastructure.

Microsoft Cloud services infrastructure

Cloud computing is usually divided into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The Microsoft Cloud offers customers all three: Azure is the Microsoft IaaS and PaaS enterprise offering; Dynamics 365 and Power Platform and Microsoft 365 are the Microsoft SaaS enterprise offerings.

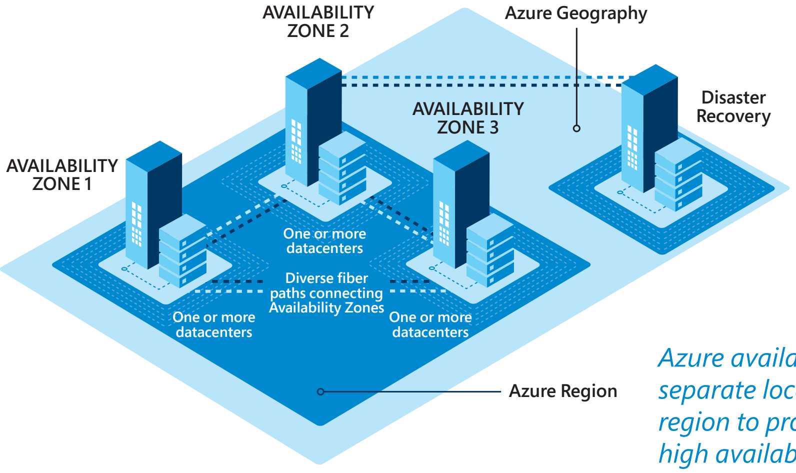
Azure infrastructure (IaaS and PaaS)

Azure global infrastructure is organized into regions, geographies, and availability zones.

An Azure region is a set of datacenters deployed within a country or geographic area and connected through a dedicated regional network, which provides low latency. With more regions around the world than any other cloud provider, Azure gives customers the flexibility to deploy applications where needed. For example, customers can choose to deploy their virtual machines (VMs) into the Brazil South region, which will create VMs in the physical location of Brazil South datacenters.

Azure regions are organized into geographies (or geos). An **Azure geography** is a discrete market, typically containing at least one or more regions, that preserves data residency and compliance boundaries. A geo can be a country or a set of countries. For example, Central India and South India regions are in the India geography, while North Europe and West Europe regions are in the Europe geography. Geographies enable customers with specific data residency and compliance needs to keep their data and applications within a geographic boundary for services that are available in the region they select.

Azure availability zones are physically separate locations within an Azure region that offer high availability to protect applications and data from datacenter failures. A region can have several availability zones—for example, the US West 2 region consists of three availability zones. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking infrastructure. Availability zones are designed so that if one zone is affected, regional services and high availability are supported by the remaining two zones. If an outage occurs within the primary region, there may be failover to another region, but it will not be outside the specified geography unless the customer has configured this in advance.



Azure availability zones are physically separate locations within an Azure region to provide resilience and high availability.

> Get the big picture and the details in Azure:

- Enabling Data Residency and Data Protection in Microsoft Azure Regions.
- Azure geographies and regions
- Azure global infrastructure

Dynamics 365 and Power Platform infrastructure (SaaS)

The global network of Dynamics 365 and Power Platform datacenters offers global and local options for data location.

Global

Global cloud services can be accessed by anyone, anywhere for these geographic locales:

- United States
- Europe
- Asia Pacific

Local

Local cloud physical datacenters reside inside the following geographic locales, and adhere to specific local security requirements:

- Australia
- Brazil
- Canada
- France
- Germany
- India
- Japan
- Norway
- Singapore
- South Africa
- South Korea
- Switzerland
- United Arab Emirates
- United Kingdom

The **global cloud** gives customers access to hyperscale, globally connected cloud services that are deployed from Microsoft datacenters in the United States, Europe, and the Asia Pacific region.

A **local cloud** addresses local data residency requirements by enabling customers within a country to keep their customer data in that country.

> Learn more: Dynamics 365 and Power Platform availability

Microsoft 365 infrastructure (SaaS)

The Microsoft 365 infrastructure is organized into global geographies and certain geographic areas (each, a Geo).

Global geographies offer certain services that are distributed globally, such as Azure Active Directory, Content Delivery Network, and Azure Front Door. They are divided into three geographic areas: Europe, Middle East, and Africa; Asia Pacific; and the Americas.

Geos refer to one or more datacenters contained within the corresponding physical geography. They are located in Australia, Brazil, Canada, European Union, France, Germany, India, Japan, North America, Norway, South Africa, South Korea, Sweden, Switzerland, United Arab Emirates, United Kingdom, and United States.

> Look for information about global geographies and Geos in Where your Microsoft 365 customer data is stored.

The Microsoft public cloud is a secure place for sensitive data and critical services, and will meet the security, privacy, and compliance needs of most customers.

Specialized cloud infrastructure

The Microsoft public cloud is a secure place for sensitive data and critical services, and will meet the security, privacy, and compliance needs of most customers. However, some customers have special requirements for the location and operation of datacenters that go beyond what is available in the Microsoft public cloud. For these customers, Microsoft has several specialized offerings that include hybrid and multicloud infrastructure and the Microsoft Cloud for Sovereignty.

Hybrid and multicloud infrastructure

Hybrid cloud computing refers to a computing environment that combines cloud and on-premises infrastructure, allowing data and applications to be shared between them. Hybrid computing gives customers the benefits of cloud computing while offering interoperability with their on-premises environments. Organizations choose a hybrid cloud approach for many reasons that can include meeting regulatory requirements for data residency or sovereignty. For example, an organization may require that certain data never leaves on-premises datacenters, which a hybrid environment can achieve while using some cloud resources.

Multicloud computing refers to the use of cloud computing services from more than one cloud provider. It can include on-premises resources as well, in which case it would also be a form of hybrid computing. A multicloud strategy gives customers flexibility in managing their data. It enables them to choose services from different cloud providers best suited for a specific task or to take advantage of services offered in a specific location.

Azure offers a variety of hybrid cloud and multicloud options. Customers can extend many Azure services and capabilities to their environment of choice—from the datacenter to edge locations and remote offices—using Azure Arc and Azure Stack. Azure Arc enables customers to extend Azure management and security to any infrastructure; Azure Stack provides the option to deploy hybrid and edge infrastructure along with Azure services and capabilities.

> Learn more: Hybrid and multicloud solutions

EU Data Boundary for the Microsoft Cloud

Microsoft is currently building the **EU Data Boundary for the Microsoft Cloud** for commercial and public sector customers in the EU, which will go beyond current data residency commitments in the EU. This commitment will apply across the main Microsoft cloud services—Azure, Dynamics 365 and Power Platform, and Microsoft 365.

The EU Data Boundary applies to countries in the EU and the European Free Trade Area, and is supported by a significant expansion of datacenters in Europe. Microsoft has opened or announced datacenters in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Netherlands, Norway, Poland, Spain, Sweden, and Switzerland.

Microsoft Cloud for Sovereignty

Microsoft Cloud for Sovereignty (MCFS) is built on Azure public cloud regions, providing public sector customers a solution to build, move, and operate their data and workloads in the cloud while meeting their legal, security and policy requirements and accelerating their digital transformation journey and cloud adoption. Public sector customers can harness the full power of the cloud along with security, and greater transparency, auditability and control over their data sovereignty.

Microsoft Cloud for Sovereignty will leverage engineering innovation to create a customized environment in Azure designed to meet compliance needs. It will also provide processes that give assurances of operational transparency, and invest in technical architectures that build on Microsoft Cloud services for security, encryption, confidential computing, and hybrid cloud management.

III. Data residency in the Microsoft Cloud

As stated earlier, data residency is the requirement that data be stored in a geographic location, such as within a national boundary, and remain in that location. Section II provided an overview of how the Microsoft Cloud infrastructure is organized and the geographic options available for storing data. This section addresses data residency options in the Microsoft Cloud, both in the main services and in specialized clouds.

Understanding data residency in the Microsoft Cloud

The Microsoft Cloud offers hundreds of unique services. For example, Azure offers Azure DevOps, Azure Cosmos DB, and Azure Backup; Dynamics 365 offers Dynamics 365 Sales and Dynamics 365 Finance; Power Platform offers Power Apps and Power BI; and Microsoft 365 offers Exchange Online and SharePoint.

For most services in the Microsoft Cloud, customers have options for selecting a location or moving the location where data will be stored. However, the process for choosing a location varies among the three main cloud services and can also depend on service availability and data type.

For most services in the Microsoft Cloud, customers have options for selecting a location or moving the location where data will be stored.

For example, some services, such as Content Delivery Network, are global in nature, meaning they require that data be stored or processed outside the selected geographic location. Other services may only be available in select geographies. Still other services can store and process data locally but may transfer data out of the selected geography for additional data processing. No matter where customer data is stored, however, Microsoft does not control or limit the locations from which customers or their end users may access customer data.

> Learn more: Where your data is located

Data residency for Microsoft Cloud services

Each service offers customers transparency regarding choices of the geographic location where their data will be stored, along with some exceptions for certain services.

Data residency for Azure services

Most Azure services enable customers to specify the region where customer data will be stored and processed. (Notable exceptions are discussed in “Data residency exceptions for the Microsoft Cloud” (page 11). Microsoft may replicate data to other regions within the same geography for data resiliency, but Microsoft will not store or process customer data outside the selected geography, with certain exceptions.

> Learn more about data residency in Azure :

- For an in-depth look, see **Enabling Data Residency and Data Protection in Azure Regions**.
- For a complete list of services and the regions where they are available, see **Products available by region**.
- For the full list of Azure geographies, including which regions map to which geography, see **Find the Azure geography that meets your needs**.

Data residency for Dynamics 365 and Power Platform services

Most Dynamics 365 and Power Platform services store customer data in the geography associated with the customer's first subscription. For data durability, Microsoft replicates Dynamics 365 and Power Platform customer data within the borders of the selected geography, with some exceptions.

For customers who want to store their data in a different local geography than the one assigned, Microsoft is in the process of accommodating migrations to other geographies. Customers who meet certain business requirements and request a move can use the **Geo Migration** feature to move their environments from one geography to another.

> Learn more:

- Get a list of services and where customer data is stored along with any exceptions by downloading **Availability, data location, language, and localization**.
- Get details on the **Geographic availability for Dynamics 365 and Power Platform services**.

Data residency for Microsoft 365 services

Most Microsoft 365 services store core customer data in a Geo based on the billing address at the time the customer signed up. Customers can identify the designated Geo where a subset of their customer data is stored at rest in **tables available online** that list countries and datacenters worldwide.

Microsoft continues to open new datacenters for business services and to add datacenters in existing regions. Eligible Microsoft 365 customers may request migration for their entire core customer data at rest to a different Geo than the one assigned when they signed up. Core customer data refers to a subset of customer data that includes Exchange Online mailbox content (email body, calendar entries, and the content of email attachments); SharePoint Online site content and the files stored within that site; and files uploaded to OneDrive for Business.

> Learn more about data residency in Microsoft 365:

- For the data location of various services, see the tables in **Datacenter Locations**.
- For data locations specific to services offered in the EU, see **Data locations for the European Union**.

Data residency exceptions for the Microsoft Cloud

Microsoft will not store customer data outside the customer-specified geography without the customer's permission except for certain services, examples of which are provided below.

- **Preview, beta, or other prerelease services** typically store customer data in the United States but may store it in Microsoft datacenters around the world.
- **Content Delivery Network (CDN)** provides a global caching service and stores customer data at edge locations around the world.

- **Azure Active Directory (AAD)** deployments:
  - In the United States, store AAD data solely in the United States.
  - In Europe, store most of the identity data within European datacenters. AAD data in Europe that may be transferred to the United States includes data related to functions such as multifactor authentication and AAD Business to Business (B2B).
  - For all other locations, Microsoft may store AAD data in our datacenters around the world.

  > Get the details in Azure Active Directory - Where is your data located?
- **Services that provide global routing functions** and do not themselves process or store customer data. These services include Traffic Manager, which provides load balancing between different regions, and Azure DNS, which provides domain name services that route to different regions. They may store or process customer data in any Microsoft datacenter.

Data residency exceptions for each service

- Data residency in Azure
- Download Dynamics 365 and Power Platform: Availability, data location, language, and localization.
- Microsoft 365 data locations

Data residency for hybrid and multicloud services

Microsoft hybrid and multicloud services usually involve infrastructure in multiple locations, so how they manage data residency is an important consideration.

Microsoft hybrid and multicloud services usually involve infrastructure in multiple locations, so how they manage data residency is an important consideration.

Azure Arc-enabled servers let customers manage Windows and Linux physical servers, containers, and virtual machines (VMs) hosted outside of Azure on their corporate network or using another cloud provider. This enables customers to run several cloud services on their on-premises infrastructure. Customer data is stored and processed on the customer's infrastructure and is only copied to the cloud if explicitly configured by the customer. Customers using Arc-enabled servers can specify the region where their data is stored.

> Learn more: Data residency with Azure Arc

Azure Stack Edge acts as a cloud storage gateway and enables data transfers to Azure while retaining local access to files. Stack Edge services store and process customer data in Azure regions. By default, data is stored in regional pairs in all the geographies where the service is available. Customers have the option to restrict data to a single region.

> Learn more: Data residency and resiliency for Azure Stack Edge

Azure Stack Hyperconverged Infrastructure (HCI) is a cluster of servers that hosts VMs in a hybrid environment, combining on-premises infrastructure with Azure cloud services. Customer data, including the names, metadata, configuration, and contents of on-premises VMs are never sent to the cloud unless the customer enables certain services, such as Azure Backup or Azure Site Recovery. Any replication of data is controlled by the customer.

> Learn more: Azure Stack HCI data collection

Azure Stack Hub is an on-premises hardware offering. If a customer deploys Stack Hub disconnected from global Azure and from the internet, none of the data stored on the device is sent to Microsoft. If a customer decides to connect a Stack Hub appliance to global Azure or to the internet, the customer is responsible for validating whether Azure or other online services used with the appliance address any data residency concerns.

> Learn more: Azure Stack Hub overview

IV. Addressing data sovereignty in the Microsoft Cloud

Data sovereignty, as noted in Section I (page 4), refers to the concept that data is under the customer's control and governed by local law. This section discusses the built-in policies and practices Microsoft implements to give customers control over their data. It first defines how Microsoft manages, protects, and restricts access to customer data. It then describes the tools and technologies that Microsoft offers customers to assert control over their data, including encryption, key management, and data governance services.

How Microsoft manages customer data

With the Microsoft Cloud, customers own their customer data and retain all rights, title, and interest in and to customer data. Customers can access, modify, or delete their customer data at any time.

Microsoft does not share customer data with advertiser-supported services or for similar commercial purposes, process it for user profiling, or mine it for any purposes such as marketing research or advertising. Microsoft only processes data in accordance with the policies and procedures agreed to.

Microsoft does not share customer data with advertiser-supported services or for similar commercial purposes, process it for user profiling, or mine it for any purposes such as marketing research or advertising.

Microsoft guarantees all this through the contractual commitments made in standard contracts for commercial and public sector customers. The terms that control how customers can use a service are explicitly defined in the **Microsoft Product Terms** and the **Microsoft Products and Services Data Protection Addendum**, both of which are available in 34 languages. Additional amendments cover restricted industries, including financial services, and are available to customers where applicable. An archive contains older versions for reference.

How Microsoft keeps customer data separate

One of the primary benefits of cloud computing is the savings that are achieved through a common infrastructure shared among many customers simultaneously; this concept of shared infrastructure is called multitenancy. Microsoft cloud services are multitenant services, which means that multiple customer deployments are stored on the same physical hardware.

To segregate each customer’s data from the data of others, the Microsoft Cloud uses logical isolation. To do this, the Azure platform uses a virtualized environment, whereby workloads from different tenants run in isolation on shared physical servers. The primary goals of isolation are preventing leakage of, or unauthorized access to, customer data across tenants, and preventing the actions of one tenant from adversely affecting the service of another.

> Learn how the Microsoft Cloud implements logical isolation in each service:

- Isolation in the Azure public cloud and Azure guidance for secure isolation
- Microsoft 365 isolation controls

How Microsoft deletes and retains customer data

When a customer leaves a Microsoft Cloud service or their subscription expires, Microsoft abides by its contractual commitment in the Product Terms. Microsoft follows specific processes for removing customer data from Microsoft cloud systems within specified time frames and for physically destroying decommissioned hardware.

Data deletion and retention. Microsoft follows strict policies for deleting and retaining data. In the Data Protection Addendum, Microsoft contractually commits to specific processes that include deleting customer data from systems under Microsoft control.

After an account is canceled or a subscription lapses, Microsoft will store the customer's data in a limited-function account for 90 days (the retention period). This will enable customers to extract their data or renew their subscription. After this 90-day retention period, Microsoft will disable the account and delete the customer data, including any cached or backup copies. If a customer has not actively deleted the customer data but the subscription has expired, Microsoft will retain the data for at most 180 days.

Data disk destruction. If a disk drive used for storage suffers a hardware failure or reaches its end of life, Microsoft securely erases or destroys it. The data on the drive is completely overwritten to ensure the data cannot be recovered by any means. When such devices are decommissioned, they are shredded and destroyed in line with NIST SP 800-88 R1 **Guidelines for Media Sanitization**. Microsoft retains and reviews records of the destruction as part of its audit and compliance process to verify adherence to its policies.

How Microsoft protects customer data

Microsoft takes a defense-in-depth approach to protecting customer data in the Microsoft Cloud with layers of security. Microsoft datacenters employ rigorous operational controls and processes to prevent unauthorized physical access to its datacenters.

Microsoft takes a defense-in-depth approach to protecting customer data in the Microsoft Cloud with layers of security. Microsoft datacenters employ rigorous operational controls and processes to prevent unauthorized physical access to its datacenters. These include video monitoring 365 days a year, trained security personnel and processes, as well as smart card and biometric access controls.

In the design and operation of the Microsoft Cloud, security is a priority at every step, including code development that follows the Security Development Lifecycle (SDL). This company-wide, mandatory process is based on a rigorous set of security controls that govern operations, as well as robust incident response strategies. Operational Security Assurance (OSA) is an exacting set of practices that make Microsoft cloud services more resilient to attack. It does so by decreasing the amount of time needed to prevent, detect, and respond to real and potential internet-based security threats.

To secure its network boundary, Microsoft employs multiple strategies, including automated detection and prevention of network-based attacks, specialized firewall devices, and Exchange Online Protection (EOP) for protection against spam and malware. To secure network traffic, Microsoft uses additional firewalls at boundary points to help detect, prevent, and mitigate network attacks. Distributed denial-of-service (DDoS) protection at every Azure datacenter helps protect against even the largest of DDoS attacks.

To detect and respond to threats to the Microsoft Cloud, Microsoft engages in continuous security monitoring of its systems. Microsoft uses cloud-based technologies to automatically apply countermeasures, and provides engineers with tools to apply approved mitigation actions quickly across the environment.

For a final layer of protection against unauthorized access to our customers' data, the Microsoft Cloud encrypts all data at rest and in transit with strong, secure encryption protocols. And because encryption is only as secure as the keys used to unlock encrypted data, Microsoft offers two main options for customers to manage their encryption keys: Microsoft-managed keys (also called platform-managed or service-managed) or customer-managed keys. (For more information on key management see page 20.)

> Learn more: **Risk Assessment Guide for the Microsoft Cloud**

How Microsoft restricts access to customer data

Microsoft takes powerful steps to protect customer data from unauthorized access beginning with physical and technological protections. There are also access restrictions for Microsoft personnel and subcontractors and stringent requirements for responding to government requests for customer data.

How Microsoft limits its access to customer data

Microsoft Cloud services are provided through datacenters worldwide, each highly automated, with few operations requiring a human touch or any access to customer content. Microsoft staff supports these services and datacenters using automated tools and highly secure remote access. In fact, access to customer data by Microsoft operations and support personnel is denied by default.

However, when a Microsoft engineer does need access, it is restricted by role-based access controls, multifactor authentication, no default access to customer data, and other controls. All access to customer data is strictly logged, and both Microsoft and third parties perform regular audits to attest that any access is appropriate. To verify the effectiveness of these security controls, Microsoft cloud services undergo a System and Organization Controls (SOC) audit by an AICPA-accredited auditor twice a year. The auditor's attestation report explains the circumstances when access to customer data can occur and how.

> Learn more: SOC Audit Reports. (Microsoft Cloud customers and trial customers have access to these reports.)

Before a Microsoft engineer will be able to gain access, Customer Lockbox will send a request to the customer asking for permission. Only if the customer approves the request will access be granted.

Customer control of Microsoft access: Microsoft Purview Customer Lockbox

Customers concerned about those rare circumstances where Microsoft access to customer data is required can choose to deploy Customer Lockbox. This service, available with certain Azure services and Microsoft 365 subscriptions, will provide an interface for customers to review and then approve or reject Microsoft requests to access customer data for service operations. The most common scenarios involve a customer opening a troubleshooting ticket with a support engineer or a Microsoft-initiated maintenance or troubleshooting operation on underlying software, either of which requires access to customer resources that could include customer data.

Before the Microsoft engineer will be able to gain access, Customer Lockbox will send a request to the customer asking for permission. Only if the customer approves the request will access be granted. Microsoft engineers have eight hours to fix any issues, after which access is automatically revoked.

> Learn more: Microsoft Purview Customer Lockbox

How Microsoft manages access by subprocessors

When Microsoft hires a subcontractor to perform work that may require access to customer data, the subcontractor is considered a subprocessor. Microsoft publicly discloses them in the Microsoft Cloud Services Subprocessors List, which identifies authorized subprocessors who have been audited against a set of stringent security and privacy requirements. (Microsoft Cloud customers and trial customers have access to this list.)

Subprocessors may access both customer data and personal data only to deliver support of the online services that Microsoft has hired them to provide. They are prohibited from using customer data and personal data for any other purpose, and are required to maintain its confidentiality. They are also contractually obligated to meet strict privacy requirements that are equivalent to or stronger than the contractual commitments Microsoft makes to its customers. These are in the Data Protection Addendum and Standard Contractual Clauses (also known as EU Model Clauses).

When engaging new subprocessors, Microsoft provides notice to customers at least six months in advance of giving them access to customers' data. Notice includes updating the Subprocessors List and giving the customer a mechanism to be notified of that update. If Microsoft engages a new subprocessor for a new online service, Microsoft will notify the customer before making that service available to them. If a customer does not accept a new subprocessor, they can terminate their subscription without penalty with a written notice.

> Learn more about subprocessors and data privacy in **How does Microsoft handle your data in the cloud?**

How Microsoft addresses government requests for customer data

Microsoft will challenge every government request for commercial and public sector customer data—from any government—where there is a lawful basis for doing so.

Microsoft has taken a firm public stand on protecting customer data from inappropriate government access. Through clearly defined and well-established response policies and processes, strong contractual commitments, and if need be, the courts, Microsoft defends the data of our customers.

Based on the belief that customers have control over their data, Microsoft will not disclose data to a government except as customers direct or where required by law. Microsoft is principled and transparent about how it responds to requests for data. Microsoft does not give any government direct or unfettered access to customer data, and scrutinizes all government demands to ensure they are legally valid and appropriate.

Microsoft believes that all government requests for data should be directed to the customer. If Microsoft receives a demand for a customer's data, it will direct the requesting party to seek the data directly from the customer. If compelled to disclose or give access to any customer's data, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.

Defending Your Data

Microsoft contractual commitments to commercial and public sector customers include **Defending Your Data**, which extends its obligations to protect customer data from inappropriate government access.

- Microsoft will challenge every government request for commercial and public sector customer data—from any government—where there is a lawful basis for doing so. Microsoft has a proven track record of successfully using the courts to challenge government demands that are inconsistent with the rule of law.
- Microsoft stands behind the strength of its GDPR compliance and other data protection safeguards, but will add reassurance against liability for commercial and public sector customers. Microsoft will provide monetary compensation to these customer's users if it discloses their data in response to a government request in violation of the GDPR. This commitment exceeds the recommendations of the European Data Protection Board. It shows that Microsoft is confident about its protection of public sector and enterprise customers' data and not exposing it to inappropriate disclosure.

Compliance with the CLOUD Act

The Clarifying Lawful Overseas Use of Data Act of 2018—better known as the CLOUD Act—was initiated to balance the privacy rights of users around the world with the need of US law enforcement to access data stored outside the United States.

The CLOUD Act is not a mechanism for greater government surveillance; it is a mechanism for assisting in specific criminal investigations. It aims to ensure that customer data is ultimately protected by the laws of each customer's home country while continuing to facilitate lawful access to evidence for legitimate criminal investigations. The law does not change any of the legal and privacy protections that previously applied to law enforcement requests for data, which continue to apply. US law enforcement must still obtain a warrant demonstrating probable cause of a crime from an independent court before seeking the contents of communications.

Microsoft compliance with the CLOUD Act includes continuing to carefully evaluate every law enforcement request and exercise our rights to protect our customers; direct US authorities to seek data directly from the consumer; and defend in court the rights of our customers if they have been violated by the US government.

> Learn more: **Compliance in the Cloud: Demystifying the Legal Landscape**

Reports on law enforcement requests

In support of its commitment to transparency, Microsoft publishes the number of official law enforcement requests worldwide for customer data in the **Law Enforcement Requests Report**. This 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 US national security.

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

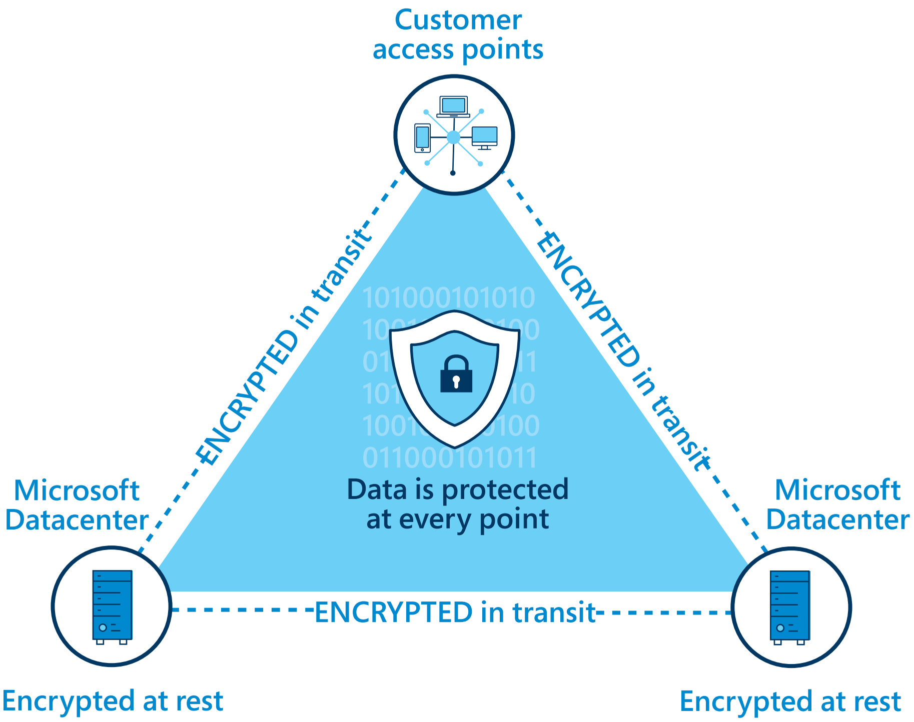
Tools and technologies to protect customer data

Microsoft offers many ways for customers to manage and control the security of their data. These include the means to encrypt data at rest and in transit, options for encrypting data in use, and tools to manage encryption keys.

Microsoft uses multiple encryption methods across the Microsoft Cloud to help protect against unauthorized access to customers' data. Microsoft helps ensure that all Microsoft-managed encryption keys are properly secured, and gives customers a robust set of tools to protect their data.

Encryption

Encryption is fundamental to providing a secure path for data to travel through the Microsoft Cloud infrastructure, and to protecting the confidentiality of data that is stored and processed there. Microsoft policies require the use of strong, secure encryption protocols to protect against unauthorized access to customers' data. Proper key management is also an essential element of encryption best practices, and Microsoft helps ensure that all Microsoft-managed encryption keys are properly secured.



How data is encrypted across the Microsoft Cloud

Validation and enforcement of our encryption policies are independently verified by multiple third-party auditors, and reports of those audits are available on the Service Trust Portal. (Microsoft Cloud customers and trial customers have access to these reports.)

Microsoft also offers many ways for customers to manage and control the security of their data. These include the means to encrypt data at rest and data in transit, options for encrypting data in use, and tools to manage encryption keys.

> Learn more: Encryption in the Microsoft Cloud

Encrypting data at rest

Microsoft policy requires that all customer content stored in Microsoft online services—that is, data at rest—be protected by one or more forms of encryption. Microsoft servers encrypt at the volume level the disk drives containing customer data. This encryption protects customer content if there are lapses in other processes or controls—for example, an attacker gaining physical access to disks containing customer content.

Encryption of data at rest may also be required for compliance with industry and government regulations like HIPAA, PCI DSS, and FedRAMP, which mandate encryption.

In addition, the hardware that implements cryptography must meet stringent requirements. The US Federal Information Processing Standard (FIPS) Publication 140-2 is designed specifically for validating modules that implement cryptography. Microsoft certifies that the cryptographic modules and ciphers used to protect the confidentiality, integrity, and availability of data in the Microsoft Cloud meet the FIPS 140-2 standard.

> Get more information on:

- Encryption at rest in Microsoft cloud services
- The Microsoft approach to FIPS 140-2 validation

Encrypting data at rest in Microsoft Cloud services

Azure. All customer data written in the Microsoft Cloud, including Azure Storage and Azure SQL Server, is encrypted using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant.

> Learn more: Azure data encryption at rest

Dynamics 365 and Power Platform. To perform real-time encryption of data when it is written to disk, Dynamics 365 and Power Platform use Microsoft SQL Server Transparent Data Encryption (TDE), which uses FIPS 140-2 compliant encryption.

> Learn more: Encryption in Microsoft Dynamics 365

Microsoft 365. Microsoft 365 customer data at rest can include files uploaded to a SharePoint Online site or OneDrive for Business, documents uploaded in a Skype for Business meeting, and Exchange Online email messages and attachments stored in mailbox folders.

Every Microsoft storage solution provides one or more industry-standard AES 256-bit data encryption technologies, including BitLocker, Azure Storage Service Encryption, and Microsoft 365 Service Encryption. All of these technologies are FIPS 140-2 compliant.

> Learn more: Encryption in Microsoft 365

Encrypting data in transit

Protecting data as it travels online is essential to any data protection strategy. Organizations that fail to do this are more susceptible to man-in-the-middle attacks, eavesdropping on customer data while it moves over a network, and session hijacking. Data is considered to be in transit when a user’s device communicates with a Microsoft server, a Microsoft server communicates with another Microsoft server, or a Microsoft server communicates with a non-Microsoft server.

To protect data in transit, Microsoft cloud services use industry-standard secure transport protocols, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec). TLS 1.2 effectively establishes a security-enhanced browser-to-server connection to help ensure data confidentiality and integrity between desktops and datacenters. IPsec is used to encrypt connections between virtual private networks (VPNs).

> Learn more: Encryption for data-in-transit

Encrypting data in transit in Microsoft Cloud services

Azure. Data can be secured in transit between an application and Azure by using client-side encryption, TLS 1.2, or Server Message Block (SMB) 3.0. Customers can enable encryption for traffic between their virtual machines and their users.

> Learn more: Encryption of data in transit in Azure

Dynamics 365 and Power Platform. Connections established between customers and Microsoft datacenters are encrypted and all public endpoints are secured using TLS 1.2.

> Learn more: Encryption in Microsoft Dynamics 365

Microsoft 365. Examples of data in transit include mail messages that are in the process of being delivered, conversations taking place in an online meeting, or files being replicated between datacenters.

Microsoft 365 encrypts data in transit using several strong encryption protocols and technologies, as well as FIPS-compliant algorithms for encryption key exchanges. They include TLS for files in transit between users; Microsoft Purview Message Encryption for email in transit between recipients; TLS 1.2 and mTLS to encrypt chats, messages, and files in transit between recipients using Microsoft Teams; and Secure RTP (SRTP) to encrypt media traffic.

> Learn more: Encryption in Microsoft 365

Encrypting data in use

Azure can encrypt customer data for certain Azure services while it is being processed. Azure Confidential Computing is an innovative technology that offers sovereign protection for confidential virtual machines and confidential containers. This unique offering enables encryption inside hardware-based enclaves with Secure Key Release in the Trusted Execution Environment, to ensure that data is encrypted while in use (as well as at rest and in transit.) This helps protect customer data from numerous security risks, including unauthorized access. Customers can benefit from this capability without having to change their application, ensuring that their data is encrypted at all times. Additionally, confidential compute capabilities extend into purpose-built platform services such as Azure SQL Always Encrypted with secure enclaves and Azure Confidential Ledger.

> Learn more: What is confidential computing?

Key management

Encryption is only as secure as the keys used to unlock encrypted data, so proper key management is an essential element of encryption best practice. Microsoft Cloud customers have two main options for encryption key management: Microsoft-managed keys (also called platform-managed or service-managed) or customer-managed keys.

- Microsoft-managed keys are encryption keys that are generated, stored, and managed entirely by Microsoft. Customers do not interact with Microsoft-managed keys.
- Customer-managed keys can be read, created, updated, deleted, as well as administered and stored by the customer in a customer-owned key vault or hardware security module (HSM), a separate physical device dedicated to encryption functions.

The storage location of the encryption keys and access control to those keys is central to an encryption-at-rest model. The keys need to be tightly secured but manageable by specified users and available to specific services. Microsoft recommends **Azure Key Vault**, a FIPS 140-2 Level 1 validated multitenant solution, for storing and managing keys in Microsoft cloud services. Azure Key Vault supports the customer's creation of keys and the import of customer keys for use in customer-managed encryption key scenarios.

> Learn more about **Encryption and key management**.

While every Microsoft Cloud service relies on Azure Key Vault, each service offers other options:

- **Key management in Azure**
- **Manage the encryption keys for Dynamics 365 and Power Platform**
- **Microsoft 365 service encryption with Microsoft Purview Customer Key**

Tools for implementing data governance

Data governance is about implementing policies that ensure that the data is discoverable, accurately defined and classified, and can be protected. Because data residency, data sovereignty, and compliance requirements often involve identifying and enforcing controls on specific types of data, a data governance regime is essential to achieving these goals. The Microsoft Purview family of services offers a set of technical solutions to address each of these areas.

> Learn more:

- For a thorough discussion of data governance, read **A Guide to Data Governance: Building a roadmap for trusted data**.
- Get an overview of **Microsoft Purview**.

Because data residency, data sovereignty, and compliance requirements often involve identifying and enforcing controls on specific types of data, a data governance regime is essential to achieving these goals.

Data discovery and classification

The first step in data governance—before applying policies to manage data—is discovering the data an organization holds. After discovering the data, the organization can classify it, labeling it based on categories such as sensitivity level or retention period.

For example, an organization might classify as sensitive any record that contains a number matching the xxxx-xxxx-xxxx pattern of a credit card number, or set a retention period for any record that is marked "payroll." These classifications would be the basis for enforcing governance policies, such as restricting access to data labeled as sensitive or retaining financial data for a required time period.

- **Microsoft Purview Data Map** provides the foundation for discovering data in the organization. It can scan data in sources that the customer has registered with the Microsoft Purview Data Map, including software-as-a-service (SaaS) applications, and data stored in hybrid, on-premises, and multicloud environments. Scanning captures technical metadata details and classifies the data.
- **Microsoft Purview Information Protection** can discover sensitive data using built-in sensitive information types (for example, credit card numbers or named entities) or custom functions (such as regular expressions or exact data match). It can then automatically classify, label, and protect (encrypt) data throughout its lifecycle.

Information rights management

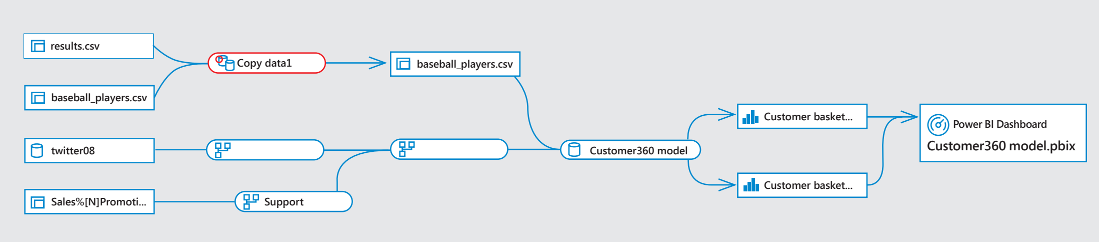
Information rights management enforces data governance by applying policy to data that has been classified, such as for sensitivity or retention, or it can use heuristics to protect data in real time, such as with Data Loss Prevention (DLP).

- Microsoft Purview Information Protection can enforce data governance policies based on an applied label. Customers can use the labels to limit access to specific users or groups or to data in specific geographies, mandate encryption, or set mandatory retention or deletion periods for data.
- Microsoft Purview Data Loss Prevention can enforce data governance policies by detecting sensitive content within files using deep content analysis, and applying protective policies. For example, it could scan for documents marked "confidential," and block them from being shared.
- Microsoft Purview Data Lifecycle Management can enforce data deletion and retention policies, and help meet recordkeeping requirements such as disposition approval, event-based retention triggers, and immutability of files.

Data lineage

Data lineage involves the origin, change, and movement of data over time. It is a process for conceptualizing, preserving, and visualizing the entire lifecycle of data, from creation to any transformations and transfers. Tracing data lineage has a number of important uses for organizations, including for both data residency and compliance. For example, an organization might need to track the geographic movement of data across national borders, or the sources of new data added to existing data, to ensure that only compliant data sources are being used.

Customers can use the Microsoft Purview Data Catalog to extract the lineage of data. Microsoft Purview then creates a visual representation to show data moving from source to destination including ways the data was transformed.



Data Catalog creates a visual representation of data moving from source to destination.

> Learn more: Data lineage in Microsoft Purview

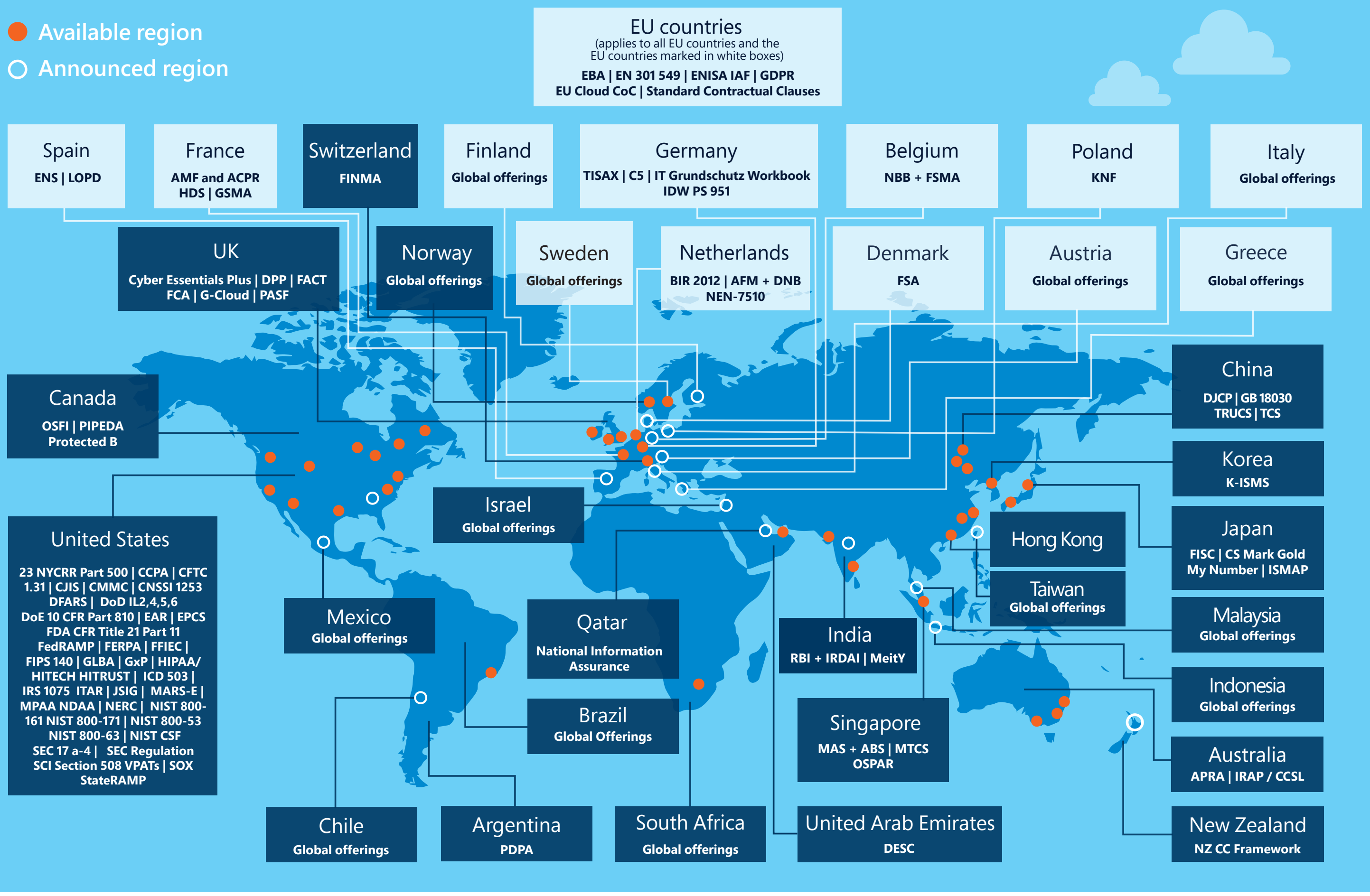
V. Compliance in the Microsoft Cloud

The Microsoft Cloud has more than 100 compliance certifications, audit reports, attestations, and other offerings to demonstrate compliance with national, regional, and industry-specific requirements. They include those that apply globally as well as more than 40 region- and country-specific offerings—from Argentina and China to the United Arab Emirates and the United Kingdom. They also encompass over 40 offerings for such key industries as finance, healthcare, and manufacturing.

Each compliance offering covers a defined set of Microsoft Cloud services, which are Illustrated in the map below by the countries and regions where the offerings apply. The global standards at the top of the graphic apply worldwide. (Click the graphic to see it at full size).

The following compliance standards apply globally

CIS Benchmark | CSA-STAR attestation | CSA-STAR certification | CSA-STAR self-assessment | ISO 20000-1:2011 | ISO 22301 | ISO 27001 ISO 27017 | ISO 27018 | ISO 27701 | ISO 9001 | PCI DSS | SOC 1,2,3 | WCAG | CDSA | CI 3DSS | Shared Assessments | TruSight



● Available region
○ Announced region

EU countries
(applies to all EU countries and the EU countries marked in white boxes)
EBA | EN 301 549 | ENISA IAF | GDPR
EU Cloud CoC | Standard Contractual Clauses

Spain
ENS | LOPD

France
AMF and ACPR
HDS | GSMA

Switzerland
FINMA

Finland
Global offerings

Germany
TISAX | C5 | IT Grundschutz Workbook
IDW PS 951

Belgium
NBB + FSMA

Poland
KNF

Italy
Global offerings

UK
Cyber Essentials Plus | DPP | FACT
FCA | G-Cloud | PASF

Norway
Global offerings

Sweden
Global offerings

Netherlands
BIR 2012 | AFM + DNB
NEN-7510

Denmark
FSA

Austria
Global offerings

Greece
Global offerings

Canada
OSFI | PIPEDA
Protected B

China
DJCP | GB 18030
TRUCS | TCS

Korea
K-ISMS

United States
23 NYCRR Part 500 | CCPA | CFTC 1.31 | CJIS | CMMC | CNSSI 1253
DFARS | DoD IL2,4,5,6
DoE 10 CFR Part 810 | EAR | EPCS
FDA CFR Title 21 Part 11
FedRAMP | FERPA | FFIEC |
FIPS 140 | GLBA | GxP | HIPAA/ HITECH HITRUST | ICD 503 |
IRS 1075 ITAR | JSIG | MARS-E |
MPAA NDAA | NERC | NIST 800-161 NIST 800-171 | NIST 800-53
NIST 800-63 | NIST CSF
SEC 17 a-4 | SEC Regulation SCI Section 508 VPATs | SOX
StateRAMP

Israel
Global offerings

Hong Kong

Japan
FISC | CS Mark Gold
My Number | ISMAP

Taiwan
Global offerings

Mexico
Global offerings

Qatar
National Information Assurance

India
RBI + IRDAI | MeitY

Malaysia
Global offerings

Indonesia
Global offerings

Brazil
Global Offerings

Singapore
MAS + ABS | MTCS
OSPAR

Australia
APRA | IRAP / CCSL

Chile
Global offerings

Argentina
PDPA

South Africa
Global offerings

United Arab Emirates
DESC

New Zealand
NZ CC Framework

It's important to note that simply purchasing an IT product with a compliance certification does not necessarily make its deployment in the Microsoft Cloud automatically compliant as well. For example, a customer may build an ecommerce application on Azure that they want to comply with PCI DSS. While they will inherit foundations of compliance from Azure that make certification easier, the ecommerce application itself will need to undergo a PCI DSS audit to ensure that it is fully compliant.

Compliance with global standards

The Microsoft Cloud has more than 100 compliance certifications, audit reports, attestations, and other offerings to demonstrate compliance with national, regional, and industry-specific requirements.

Global compliance offerings are accepted by countries around the world across many industries and markets, and are among the most widely used in the IT industry. The Microsoft Cloud includes compliance with these broadly accepted standards most of which are certified by an independent auditor:

- **International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards**. The Microsoft Cloud complies with more than half a dozen ISO/IEC standards for security and privacy. These include **ISO/IEC 27001**, which formally specifies an information security management system, **ISO/IEC 27017**, the code of practice for information security controls, and **ISO/IEC 27701** which specifies requirements for a privacy information management system.
- **Center for Internet Security (CIS) Benchmarks** offer a set of configuration baselines and best practices for securely configuring a system.
- **System and Organization Controls (SOC)**, created by the American Institute of Certified Public Accountants (AICPA), provide for internal control reports (**SOC 1**, **2**, and **3**). They are intended to help the customers of service organizations assess and address the risk associated with an outsourced service.

> For a complete list of Microsoft compliance with global requirements, see the **Global** lists in **Azure, Dynamics, and Microsoft 365 compliance offerings**.

Compliance with regional requirements

Microsoft cloud services comply with certifications, laws, and standards specific to over 20 countries from Argentina to the United States and regions that include Europe. The Microsoft Cloud includes compliance with such regional standards as:

- **Federal Risk and Authorization Management Program (FedRAMP)** is a US government program that prescribes a standardized approach for assessing, monitoring, and authorizing cloud computing products and services. All US executive federal agencies are required to validate the security of their cloud services against FedRAMP standards.
- **Federal Information Processing Standard (FIPS) 140-2** is a US government standard that defines minimum security requirements for cryptographic modules in IT products.
- **General Data Protection Regulation (GDPR)** is an EU regulation that accords rights to EU residents to manage personal data that an organization collects. It applies to organizations that offer goods and services to them, or that collect and analyze data for EU residents no matter where the organization is located.

> For a complete list of Microsoft compliance with regional requirements, see the **Regional** lists in **Azure, Dynamics, and Microsoft 365 compliance offerings**.

Compliance with industry requirements

The Microsoft Cloud offers a rich portfolio of compliance with standards and regulations that address various industry requirements such as those in financial services, healthcare and life sciences, media and entertainment, energy, manufacturing, and education. The Microsoft Cloud complies with such industry standards as:

- HITRUST provides a standardized framework and an assessment and certification process against which cloud service providers and healthcare organizations can measure their compliance with HIPAA and HITECH laws.
- PCI DSS is a global information security standard designed to prevent fraud through increased control of credit card data. Organizations of all sizes must follow the PCI DSS if they accept payment from the five major credit card brands.

> For a complete list of Microsoft compliance with industry requirements, see the **Industry** lists in Azure, Dynamics, and Microsoft 365 compliance offerings.

Microsoft tools for customer compliance

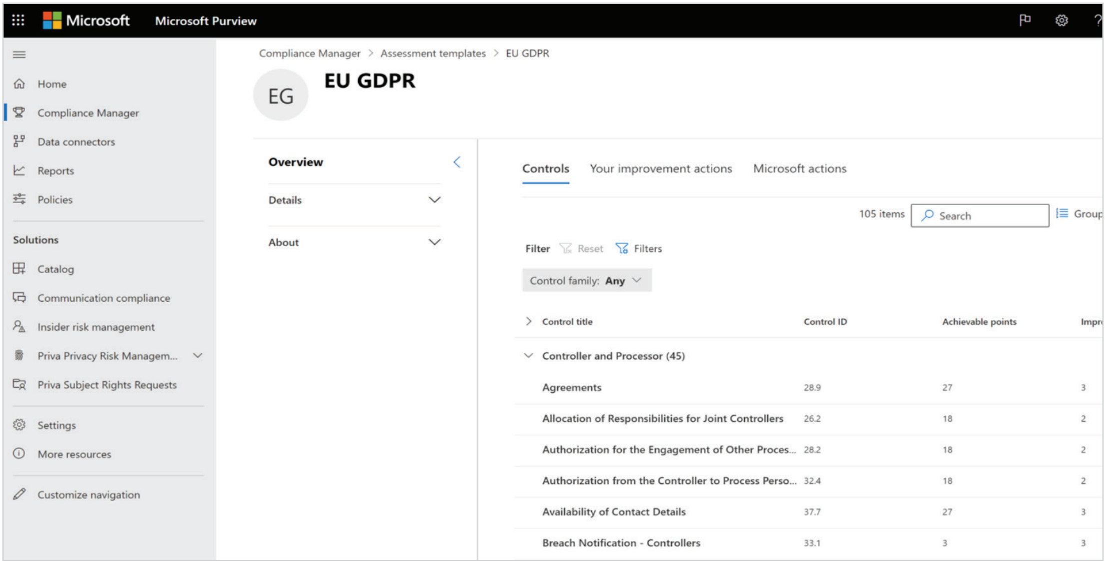
Microsoft helps customers meet their own compliance obligations with an extensive repository of resources that include tools, documentation, and guidance.

Microsoft Purview Compliance Manager

Microsoft Purview Compliance Manager can help Microsoft Cloud customers simplify compliance using templates that contain control mappings of common standards including the EU GDPR, ISO/IEC 27001:2013, and NIST 800-53 Revs. 4 and 5.

Compliance Manager automatically tracks Microsoft-managed controls, and allows the customer to track their own compliance with those controls for which they are responsible. The customer can then use the template to keep track and serve as evidence of their overall compliance, and create a compliance score to help them understand and measure their compliance posture.

> Learn about assessment templates in Compliance Manager.



EU GDPR

Control title	Control ID	Achievable points	Impr
Controller and Processor (45)			
Agreements	28.9	27	3
Allocation of Responsibilities for Joint Controllers	26.2	18	2
Authorization for the Engagement of Other Proces...	28.2	18	2
Authorization from the Controller to Process Perso...	32.4	18	2
Availability of Contact Details	37.7	27	3
Breach Notification - Controllers	33.1	3	3

This Compliance Manager template maps controls required for compliance with the GDPR

Azure Blueprints

The **Azure Blueprints** service offers templates that will configure a customer's Azure environment to adhere to a set of standards or requirements.

Microsoft provides built-in blueprints to help achieve common compliance certification scenarios. For example, the **ISO 27001 Shared Services blueprint** maps and enforces a core set of policies from key portions of ISO 27001 requirements, such as enforcing audit logging and requiring encryption in any Azure environment. Blueprints can also be used to enforce data residency by specifying allowed locations.

Blueprints can be deployed to multiple Azure subscriptions and managed from a central location. Customers can customize the built-in blueprints or create their own blueprints.

> Learn more: **Overview of Azure Blueprints**

Access to audit reports and certificates

In the **New and Archived Audit Reports** on the Service Trust Portal, Microsoft offers access to certificates of compliance, audit reports, bridge letters, and other materials for a number of audited standards. These include such standards as ISO/IEC 27001, SOC, FedRAMP, and HITRUST. The reports confirm compliance of Microsoft Cloud services with these standards and regulatory requirements. They can help information security, compliance, risk management, and privacy professionals with their own compliance and risk assessments, along with documentation of that compliance.

Customers who have active paid or trial subscriptions with Azure, Dynamics 365 and Power Platform, or Microsoft 365 can access the reports directly. New customers and those who are evaluating Microsoft online services can access them with any Microsoft or Office 365 account.

Azure customers or trial customers can also access audit reports and certificates for services in the **Azure Portal**.

Microsoft