Microsoft

Protecting data privacy using Microsoft Azure

June 2021

Contents

Introduction

The amount of data being created, shared, and stored today is growing exponentially. With data at its heart, the pursuit of digitization—often referred to as digital transformation—is profoundly altering business. Companies are leveraging data to improve the customer experience, generate new business, boost employee productivity, and increase the efficiency of organizational processes. The data they manage includes what they upload for storage or processing, data generated by applications hosted in the cloud, records created as part of normal business processes, the personal data of customers, as well as trade secrets, processes, and other proprietary enterprise information.

As that volume of data has grown, government and industry regulations to keep data secure and private are proliferating. Many regulations revolve around protecting the privacy of personal data in particular. The EU General Data Protection Regulation (GDPR), the US federal Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA), individual US states' privacy laws such as those recently enacted by California, and many others lay out strict rules for keeping individuals' personal data private.

With requirements that are complex and constantly evolving, meeting compliance obligations in this dynamic regulatory environment can be challenging. Microsoft Azure, designed from the ground up to protect data, includes many tools and features that can help you navigate this ever-changing landscape.

This paper discusses the Azure tools and services that your organization can use and the steps you can take to protect your data, focusing on two specific types of data of concern to Azure customers:

- Customer data: all data, including text, sound, video, or image files and software, that a customer provides to Microsoft or that is provided on their behalf through their use of Microsoft online services, excluding Microsoft Professional Services.
- Personal data (a subset of customer data): any information that relates to an identified or identifiable natural person. It ranges from very basic information such as a name and email address to much more personal information that can include physical characteristics, economic status, or mental health. It can also include automatically collected device-specific information that may be tied or linkable to a person's account and such data as IP addresses, search queries, and location.

In this paper, we start with the relationship between privacy and security, and outline the responsibility that Microsoft and our customers share for data security. We then suggest a four-step approach to data governance for protecting both customer and personal data. We follow it with an overview of data privacy regulations and measures you can take using Azure to address specific regulatory requirements for protecting personal data.

"Microsoft Azure, designed from the ground up to protect data, includes many tools and features that can help you navigate this ever-changing landscape."

The Microsoft commitment to privacy

Microsoft has a long history of dedication to data privacy and protection that has evolved over many decades of being entrusted with our customers' data. This trust and experience has shaped the company's time-tested approach to applying the highest standards of privacy protection, based on the following principles.

You control your data

With Azure, you are the owner of the data that you provide for storing and hosting in Azure services. We do not share your data with advertiser-supported services, nor do we mine it for any purposes like marketing research or advertising.

We process your data only with your agreement, and when we have your agreement, we use your data to provide only the services you have chosen. These agreements apply equally to subcontractors (or, subprocessors) that Microsoft authorizes and hires to perform work that may require access to your data. They can perform only the functions that Microsoft has hired them to provide, and they are bound by the same contractual privacy commitments that Microsoft makes to you.

If you leave the Azure service or your subscription expires, Microsoft follows strict standards for removing customer data from its systems.

You choose where your data is located

When you use Azure, you choose where your data is located. Through our large and ever-expanding network of datacenters around the globe, Azure enables you to choose from more than 60 regions linked by one of the largest interconnected networks on the planet, including more than 150 datacenters.

However, no matter where your data is stored, Microsoft does not control or limit the locations from which you or your end users may access, copy, or move customer data. Most Azure services enable you to specify the region where your customer data will be stored and processed.

Azure offers tools to help you control the location of your data—for example, you can use Azure Policy or Azure Blueprint to restrict access to selected regions for your subscription.

"When Microsoft envisions a new product or service, privacy and data protection principles are considered at each phase of development. This is part of our Privacy by Design philosophy."

Azure secures your data at rest and in transit

With state-of-the-art encryption, Azure protects your data both at rest and in transit. Azure secures your data using various encryption methods, protocols, and algorithms, including double encryption.

- For **data at rest**, all data written to the Azure storage platform is encrypted through 256-bit AES encryption and is FIPS 140-2 compliant. Proper encryption key management is essential. By default, Microsoft-managed keys protect your data, and Azure Key Vault helps ensure that they are properly secured. Azure key management also includes server-side encryption that uses service-managed keys, customer-managed keys in Azure Key Vault, or customer-managed keys on customer-controlled hardware. With client-side encryption, you can manage and store keys on premises or in another secure location.
- For **data in transit**—data moving between user devices and Microsoft datacenters or within and between the datacenters themselves—Microsoft adheres to IEEE 802.1AE MAC Security Standards and uses and enables your use of industry-standard encrypted transport protocols, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec).

Microsoft defends your data

Through clearly defined and well-established response policies and processes, strong contractual commitments, and if need be, the courts, Microsoft defends your data. We believe that all government requests for your data should be directed to you. We do not give any government direct or unfettered access to customer data. Microsoft is principled and transparent about how we respond to requests for data.

Because we believe that you have control over your own data, we will not disclose data to a government except as you direct or where required by law. Microsoft scrutinizes all government demands to ensure they are legally valid and appropriate.

If Microsoft receives a demand for a customer's data, we 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.

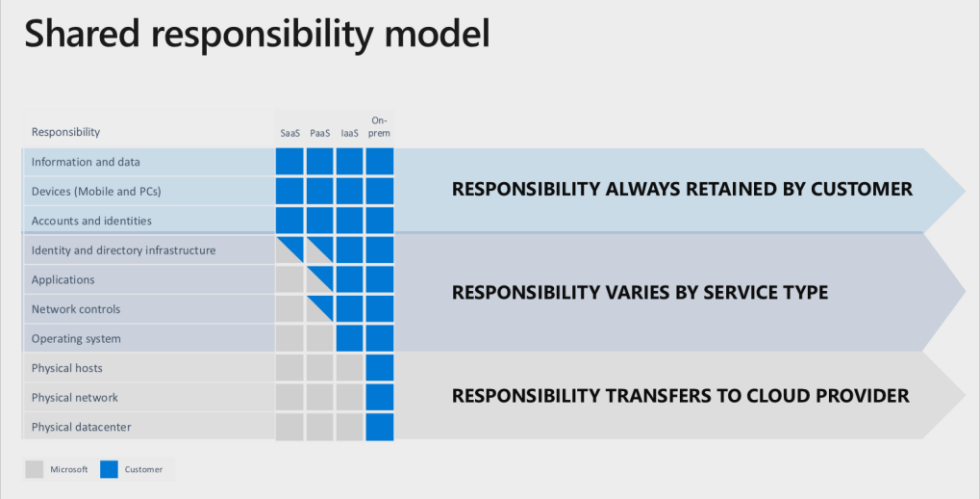
Privacy starts with data security

The focus of this paper is on protecting your data and its privacy, but without security there can be no privacy. To understand the difference between the two, think of protecting privacy as the objective and security—in the context of compliance—as the means by which you can attain that desired result.

Your organization may have moved to the cloud for more cost-effective, easily accessible, and secure IT operations. Putting your data in the cloud has many advantages but when you partner with a cloud services provider like Microsoft, you want to know that they take data security and compliance as seriously as you do.

Data security as a shared responsibility

When the data you collect and store resides in the cloud, the security of that data becomes a responsibility that you share with Microsoft. While you are still responsible for some aspects of security, Microsoft becomes responsible for others, depending on the applicable cloud computing model as illustrated below.



The table below illustrates this division of responsibility when it comes to protecting the data you generate, collect, process, and store in the Azure cloud.

Microsoft is responsible for:	Your organization is responsible for:
Building services and features that can be used in compliance with applicable data protection and privacy regulations and standards.	**Configuring the online services you use and training your workers to use those services in a way that maintains compliance requirements for your industry and location.**
Creating strong operational controls to protect customer data in the cloud.	**Using and configuring the online services in a way that limits unintended data sharing and access.**
Demonstrating its commitment to data protection by obtaining certifications, sharing attestation reports, and signing agreements.	**Verifying that Microsoft audit reports, certifications, and other evidence meet your organizational data protection expectations.**

» For more information, see Shared Responsibilities for Cloud Computing

> "When the data you collect and store resides in the cloud, the security of that data is a responsibility that you share with Microsoft."

Azure responsibility for data security

Azure enables a multilayered security strategy that includes identity and access controls, application and data security, network security, threat protection, and security management. This defense-in-depth approach to security in Azure provides built-in security controls and tools to help you protect all your data, including any personal data.

Defense in Depth

Identity and Access	Apps and Data Security	Network Security	Threat Protection	Security Management
Role-Based Access	Encryption	DDoS Protection	Antimalware	Log Management
Multifactor Authentication	Confidential Computing	NG Firewall	AI-Based Detection and Response	Security Posture Assessment
Central Identity Management	Key Management	Web App Firewall	Cloud Workload Protection	Policy and Governance
Identity Protection	Certificate Management	Private Connections	SQL Threat Protection	Regulatory Compliance
Privileged Identity Management	Information Protection	Network Segmentation	IoT Security	SIEM

Microsoft Partners

All these Azure tools and controls play a role in giving you control over and protecting the privacy of your data.

In the shared responsibility model, Microsoft handles the security of the physical datacenter, physical network, and physical host machines, and protects Azure datacenters with access controls, perimeter security, surveillance cameras, biometric authentication, metal detectors, and more. The customized hardware inside datacenters has integrated security controls and is protected by ISO-compliant safeguards such as locked server cages and racks, smartcard readers, monitoring around the clock by security staff, and other mechanisms.

> "This defense-in-depth approach to security in Azure provides built-in security controls and tools to help you protect all your data."

Customer responsibility for data security

Your data is your business: Microsoft does not know what kind of data customers choose to store in Azure. The data you store in the Azure cloud—your customer data—belongs to you, and your organization owns it and controls its collection, use, and distribution.

When your organization collects, stores, or processes the personal data of customers, employees, or other individuals, you incur obligations to protect the privacy of that information whether it resides in your on-premises network or in the cloud. You are also responsible for complying with the laws, industry regulations, contractual obligations, public expectations, or other requirements that may apply to your business.

To take on this data protection responsibility, you could explore a comprehensive data protection framework, which often incorporates these elements:

- **Identification of personal data:** Trace and identify all types of data (including personal data).
- **Data classification:** Assign data to categories based on sensitivity levels so the appropriate controls can be implemented.
- **Data governance practices and processes:** Define policies, roles, and responsibilities for the access, management, and use of data.
- **Data protection measures:** Use appropriate technical and organizational measures that incorporate data privacy and protection principles to integrate the necessary security safeguards into the collection, storage, processing, and management of data.
- **Data breach response plan:** Create a response strategy and train employees to apply corrective actions.
- **Data management practices specific to compliance requirements** of the GDPR, CCPA, and other comprehensive privacy laws. Establish policies and practices to enable you to handle the requests of individuals to rectify inaccurate or incomplete personal information, restrict processing of personal data, and completely erase personal data when appropriate.
- **Documentation:** Keep proper records to show adherence to the regulations.

In addition, your organization is responsible for the security of the guest operating systems running on your virtual machines, as well as your applications, user accounts and identity, access and network controls, and the security of your client endpoints.

Azure provides mechanisms that you can use to help protect the data that you generate, collect, process, and store in the cloud.

Data governance and guidelines for protecting customer data

Data governance refers to an overarching strategy that encompasses the policies, processes (including technologies), and people involved in managing and protecting data. An effective data governance plan forms the foundation of an organization's approach to protecting data and its privacy, and is also key to compliance with national, regional, and industry-specific requirements governing the collection and use of data. Supported by effective technology, it is a driving force to help document the basis for lawful processing, and define policies, roles, and responsibilities for the access, management, security, and use of personal data.

An effective data governance program enforces how and where data is stored and sent, who has access to it and at what level, and what actions can be performed on the data, by whom, when, using what methods, and under what circumstances. It should be designed to protect the data and prevent any unauthorized access or exposure, and also contain a response plan that can be put in place quickly if an incident occurs. Consult your data privacy attorney as you develop and implement your data governance strategy.

Azure offers tools and services that can help you implement these aspects of your organization's data governance program:

- **Identify and classify customer data more quickly and accurately:** Effectively protecting customer data involves a step-by-step process that begins with identifying your data in all the different locations where it resides, and classifying it in appropriate categories, as determined by your organization; for example, you may need to distinguish between personal data and sensitive personal data.
- **Establish and apply policies to govern use of and access to your customer data:** This includes restricting permissions only to those users who need access to perform their jobs, and granting that access for the shortest time and with the least privileges possible.
- **Protect the integrity and confidentiality of customer data** using information protection and data security technologies. You may need to apply security controls, automated when possible, that will enforce the policies and protect your data from both internal and external unauthorized access and accidental exposure.
- **Document compliance:** You must also be able to produce and retain required documentation and maintain auditable records to prove your compliance with privacy policies.
- **Respond to data subject requests:** To fully comply with the requirements of such privacy laws as the GDPR, you must be able to find and provide copies of personal data or make modifications to it or the processing of it in a timely manner in response to data subject requests. (In the GDPR, individuals are known as data subjects.)

"Data governance refers to an overarching strategy that encompasses the policies, processes (including technologies), and people involved in managing and protecting data."

- **Respond to data breaches.** Azure responds to data breaches following a five-stage process: detection, assessment, diagnosis, stabilization, and closure. Microsoft will notify customers of any personal data breach (except for those cases where personal data is confirmed to be unintelligible).

In the following sections, we'll look a little more closely at the Azure tools and technologies that can be used to help you accomplish each of these.

Identify and classify customer data

Digital data can be created or captured in many different forms, and these many different types come with varying levels of sensitivity. For the purposes of complying with privacy regulations, it's important to understand the following categories:

- **Customer data** is all data, including text, sound, video, or image files and software, that you provide to Microsoft or that is provided on your behalf through your use of Microsoft online services, excluding Microsoft Professional Services. For example, it includes data that you upload for storage or processing, personal data, applications that you upload for distribution through a Microsoft enterprise cloud service, and proprietary enterprise information.
- **Personal data,** a subset of customer data, is any information that relates to an identified or identifiable natural person. Individuals are considered to be identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier, or other factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
- **Sensitive personal data,** specifically called out in the GDPR, is defined as "special categories of personal data." It includes data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

It's important to classify data properly so you can apply appropriate security controls. Therefore, a common first step in meeting data privacy obligations is to locate, identify, and classify all personal data that your organization stores and manages.

» For more information, see how Microsoft categorizes data

"It's important to classify data properly so you can apply appropriate security controls."

How Azure can help you identify and classify customer data

Azure Purview is a unified data governance service that can help you manage data across on-premises, multicloud, and software-as-a-service (SaaS) sources. With automated data discovery, data classification, and end-to-end data lineage, it can help you catalog, understand, and classify your data, all in one unified environment.

Azure Purview comprises three services—Data Map, Data Catalog, and data insights—with Purview Data Map as the foundation for discovering data and unifying the Purview Data Catalog and Purview data insights experience.

- **Purview Data Map** can be used to create a unified map of your data across hybrid sources that is kept up to date through an automated scanning and classification system. It helps you classify data through built-in and custom classifiers and Microsoft Information Protection sensitivity labels, and helps label sensitive data consistently across SQL Server, Azure, Microsoft 365, and Microsoft Power BI.
- **Purview Data Catalog** enables discovery of your data. You can search for data using technical or business terms, easily understand data by browsing associated technical, business, semantic, and operational metadata, identify the sensitivity level of data, and know where your data came from with interactive data lineage visualization.
- **Purview data insights** affords an overview of your data, which offers an in-depth understanding of what data is actively scanned, where sensitive data is, and how it moves.

» For more information, see What is Azure Purview?

Manage use of and access to customer data

You should control who can access customer data (and documents) and under what conditions, as well as monitor that access and grant only the amount of access that users need to perform their jobs, revoking it when it's no longer needed.

How Azure can help you manage use of and access to customer data

- **Azure Role-Based Access Control (RBAC)** can be used to limit use of specific data, for example, to read-only. It can also enforce separation of duties, enabling you to define fine-grained permissions to grant only the amount of access that users need to perform their jobs.

» For more information, see What is role-based access control (RBAC) for Azure resources?

- **Azure Active Directory Privileged Identity Management** can be used to minimize the number of people who have access to customer data, and can also help you discover, restrict, and monitor privileged identities and their access to resources. You can also use this service to enforce on-demand, just-in-time administrative access when needed.

  » For more information, see What is Azure AD Privileged Identity Management?

- **Azure Information Protection (AIP)** can help you control both who can access a document or email message, and further control whether that document can be edited, is restricted to read-only, or can be printed or forwarded. It uses Azure Rights Management to help ensure that your data remains protected no matter where it's stored or with whom it's shared. Rights Management is integrated with other Microsoft cloud services and applications, such as Office 365 and Azure Active Directory. It can also be used with your own line-of-business applications and information protection solutions from software vendors, both on premises and in the cloud.

  » For more information, see What is Azure Information Protection?

Protect customer data through security controls

Securing data is crucial to protecting privacy, and your organization is responsible for protecting your data as well as protecting the security of your applications, user accounts and identity, access and network controls, and the security of your client endpoints.

How Azure can help you secure customer data

Encryption of data is an important element of protecting it in case of a breach. Azure supports various encryption models, including server-side encryption that uses service-managed keys, and customer-managed keys in Key Vault or on customer-controlled hardware. Azure includes data protection capabilities through built-in services, components, and configurations that you can select to apply encryption to internal data and traffic including data at rest, data in transit, and data in process.

- **Azure Key Vault** can be used to segregate role functionality in the management of keys and data.

  » For more information, see Azure Key Vault basic concepts.

- **Azure Storage Service Encryption, Azure Disk Encryption, and Transparent Data Encryption for Azure SQL Database** can all be used to protect data by securing it using strong cryptographic technologies.

  » For more information, see Azure Encryption Overview.

In addition, Azure offers these tools to help you keep your organization's data secure:

> "Azure supports various encryption models, including server-side encryption that uses service-managed keys, and customer-managed keys in Key Vault or on customer-controlled hardware."

- **Azure Security Center** can be used to implement unified security management and advanced threat protection. Integration with Azure Policy can also help you apply security policies across hybrid cloud workloads to enable encryption, limit organizational exposure to threats, and respond to attacks.

  » For more information, see What is Azure Security Center?

- **Azure Information Protection** uses Azure Rights Management to help protect documents and email, using encryption, identity, and authorization policies to control who can access each document and what each person is allowed to do with it.

  » For more information, see What is Azure Information Protection?

Document the protection of customer data

You may be responsible not only for complying with the legal and regulatory requirements applicable to your organization, but also for demonstrating compliance if you're audited. (Such documentation has the added benefit of enabling you to respond more quickly and easily to the requests of data subjects in response to the GDPR.)

Documentation can include logs, records, reports, or observations that demonstrate compliance with the regulatory requirements applicable to your organization; because these requirements vary, consult your attorney for specific guidance.

» For more information, see Overview of Azure platform logs.

Protecting the privacy of personal data

The advent of big data and sophisticated data analytics methods have increased concerns about data privacy. Vast quantities of data are gathered, analyzed, and stored across huge content stores in virtualized environments for ease of search and retrieval and the ability to serve as a global resource. Some of this is personal data of varying degrees of sensitivity. Enterprise standards and best practices governing the handling and security of big data are still in the process of evolving. New and better means for protecting and securing any data sets that might contain personal data is essential to maintain compliance with privacy regulations.

Privacy laws and regulations overview

The easy global exchange of information over the internet has made it increasingly difficult for individuals to safeguard, access, and control their personal data. Likewise, it's harder for organizations to protect the privacy of the individuals whose data they collect, process, and store in the course of doing business.

Gathering and contextualizing data and drawing insights from it helps businesses make better strategic decisions and better serve their customers. Companies collect personal data from many sources, both directly and indirectly, including from website interaction, public records, social media, and tracking purchases. This can include names, addresses, government ID numbers, credit card and banking information, medical and healthcare records, as well as any identifiers that are or can be linked to an identifiable individual.

However, when the personal data that your organization collects falls under one or more of the many government and industry regulations that set forth compliance requirements, proper data handling is no longer merely good customer relations—it becomes a serious obligation. The rapid increase in the types and amount of personal data stored in digital format, the growing threat of data breaches, and heightened awareness on the part of the public regarding the consequences of exposure of personal data have led to the demand for more and stricter laws governing how organizations use, share, and store such data.

Privacy laws are not new. Federal statutes recognizing privacy as a fundamental right first came to the forefront in the 1970s. Since that time, new technologies have changed the privacy landscape dramatically. Today privacy regulations exist at the state, federal, and regional levels as well as those that are industry specific.

EU General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR), which went into effect in May 2018, is a far-reaching regulation that is intended to protect the privacy of the personal data of any EU resident. Its mandates include enhanced personal privacy rights and an increased duty to protect personal data. It applies to all companies operating in the EU, no matter where they are based.

The GDPR gives individuals (referred to in the regulation as data subjects) the right to manage their personal data that has been collected, processed, or stored by an agency or organization (known as the data controller, or just controller). Personal data is any data that that is linked or can be linked to an identified or identifiable natural person.

The GDPR spells out specific rights of data subjects regarding their personal data. A formal request by a data subject to a controller to take an action on personal data is called a data subject request. These include the right to obtain copies of personal data, request corrections to it, in certain cases restrict the processing of it or delete it or receive it in an electronic format so it can be moved to another controller.

» Microsoft makes contractual commitments with regard to the GDPR in the Microsoft Online Services Terms and extends these GDPR commitments to all volume licensing customers.

US data privacy laws

The United States has not enacted a broad federal law similar to the GDPR. The Federal Privacy Act of 1974 only protects information collected by government agencies, not by private entities, although the US Federal Trade Commission can bring action against companies that fail to comply with their published privacy policies as "deceptive practices."

> "Proper data handling is no longer merely good customer relations—it becomes a serious obligation."

However, there are a number of federal laws that govern data privacy in certain business sectors, such as healthcare (Health Insurance Portability and Accountability Act, or HIPAA), financial services (Gramm-Leach-Bliley Act), and education (Family Educational Rights and Privacy Act, or FERPA). The United States also has federal laws that pertain to certain types of data or the data of certain classes of people, such as children (Children's Online Privacy Protection Act, or COPPA).

In addition, many US states have also either enacted or proposed laws protecting the privacy of personal information. The California Consumer Privacy Act (CCPA) is currently the most comprehensive of these. The CCPA defines personal data as any information relating to an identified or identifiable person (referred to in the law as a *consumer*). There is no distinction between a person's private, public, or work roles; the CCPA also protects family and household data. Businesses regulated by the CCPA will have a number of obligations to those consumers that include responding to their right, conferred by the CCPA, to request (similar to the GDPR) to receive a copy of, delete, and restrict the processing of their personal data.

Private industry regulations

Not all privacy regulations are imposed by governmental bodies; there are a number of industry-specific standards that reference privacy, including:

- The **Payment Card Industry Data Security Standard (PCI DSS)**, which was developed by a private sector council formed by major credit card companies. The council functions as a governing entity and compliance with its standards is mandatory for merchants and other organizations that collect, process, store, or transmit the personal information of credit card holders. Although PCI DSS compliance is not mandated by any federal statute, some states have incorporated it into their own laws.
- The **Health Information Trust Alliance (HITRUST)**, which is governed by representatives from the healthcare industry. HITRUST created and maintains the Common Security Framework, which provides a benchmark—a standardized compliance framework, assessment, and certification process—against which cloud service providers and covered health entities can be certified for compliance.

» See the comprehensive portfolio of Azure compliance offerings that can help you comply with a wide range of national, regional, and industry-specific privacy requirements governing the collection and use of data.

Protect personal data in compliance with data privacy laws

Microsoft is committed to data privacy compliance across its cloud services and has designed the Azure platform with industry-leading security controls, compliance tools, and privacy practices to safeguard all your data in the cloud, including any data sets that contain personal data.

"The Azure platform with industry-leading security controls, compliance tools, and privacy practices to safeguard all of your data in the cloud."

In addition to the guidelines laid out in the data governance section of this paper, Azure can help you implement specific components of your organization's efforts to respond to data subject requests and data breaches.

» To learn more about Microsoft policies and practices for protecting personal data, see the Online Services Data Protection Addendum (DPA).

Respond to data subject requests

An important aspect of complying with the GDPR, the CCPA, and similar privacy regulations often involves responding to the formal requests of data subjects and consumers to take action on their personal data. These formal requests are known as data subject requests (DSRs) and include the right to obtain copies of personal data, restrict the processing of it, delete it, or receive it in an electronic format. The GDPR also protects the right of a data subject to correct inaccurate data or rectify incomplete data.

The GDPR distinguishes between a *data controller* and a *data processor*. The controller, such as your organization, controls the purposes and means of processing data; the processor, such as Microsoft, processes personal data on behalf of the controller. When a data controller receives a DSR, they must provide a timely, GDPR-consistent response to it.

How Azure can help you respond to data subject requests

Microsoft suggests a process for responding to DSRs and offers services and administrative tools to help data controllers find, access, and act on personal data in response.

The process Microsoft follows covers these six phases:

- **Discover:** A DSR begins with discovery. Use Microsoft search and discovery tools to find customer data that may be the subject of a DSR. Once potentially responsive documents are collected, you can perform one or more of the DSR actions listed below. Alternatively, you may determine that the request doesn't meet your organization's guidelines for responding to DSRs.
- **Access:** Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that can be available to the data subject.
- **Rectify:** Make changes or implement other requested actions on the personal data, where applicable.
- **Restrict:** Restrict the processing of personal data, either by removing licenses for various Azure services or turning off the desired services where possible. You can also remove data from the Microsoft cloud and retain it on premises or at another location.
- **Delete:** Permanently remove personal data that resided in the Microsoft cloud.
- **Export/Receive:** Provide an electronic copy (in a machine-readable format) of personal data to the data subject.

» For more information, see Azure Data Subject Requests for the GDPR and CCPA.

"An important aspect of complying with the GDPR and similar privacy regulations involves responding to the formal requests of data subjects."

Azure provides the following services to help you respond to and address data subject requests in a timely manner. You can use:

- The **Azure Data Subject Requests for the GDPR** portal to help find a data subject's personal data that resides in Azure. This service is available through the Azure portal on Microsoft public and sovereign clouds, as well as through pre-existing APIs across our online services.
- **Azure Purview** to find, identify, and classify customer data with automated data discovery, sensitive data classification, and end-to-end data lineage.
- **Azure Active Directory, Azure SQL Database, and Query Explorer** to limit authorized access to personal data and erase it.
- **Azure File Service REST API** to delete Azure File Storage or Azure Table Storage data.
- **Azure Active Directory, Azure SQL Database, the Cosmos DB Migration Tool, and the Azure Storage REST API** to export personal data in a common, structured format.
- **AAD Privileged Identity Management** to restrict the processing of personal data by allowing you to limit, manage, and monitor access.

Respond to data breaches

Under GDPR terms, a personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed."

Microsoft takes extensive security measures within Azure to protect against data breaches. Microsoft will notify customers of any personal data breach, except for those cases where personal data is confirmed to be unintelligible—for example, encrypted data where the integrity of the keys is confirmed. These measures include both physical and logical security controls, as well as automated security processes, comprehensive information security and privacy policies, and security and privacy training for all personnel. Security is built into Azure from the ground up, starting with the Security Development Lifecycle, and Microsoft has a dedicated global incident response service that works to mitigate the effects of attacks against Azure.

Due to the nature of cloud computing, where multiple customers share infrastructure, not all data breaches occurring in a customer cloud environment involve Microsoft online services. Microsoft employs a shared responsibility model to define security and operational accountabilities. Both the cloud services provider and the customer are accountable for portions of cloud security. If a breach occurs in online services, Microsoft will investigate; if the breach occurs in the customer's realm of responsibility, the customer is required to respond.

How Azure responds to data breaches

Azure responds to data breaches following a five-stage process: detection, assessment, diagnosis, stabilization, and closure.

1. **Detect:** First indication of a potential incident.
2. **Assess:** The on-call incident response team member assesses the impact and severity of the event. Based on evidence, the assessment may or may not result in further escalation to the security response team.
3. **Diagnose:** Security response experts conduct technical or forensic investigation, and identify containment, mitigation, and workaround strategies.
    - Microsoft assigns appropriate priority and severity levels to an incident by determining the functional impact, recoverability, and information impact. Both the priority and severity may change over the course of the investigation, based on new findings and conclusions. Security events involving imminent or confirmed risk to customer data are treated as high severity and worked on around the clock to resolution.
    - If the security team believes customer data may have been breached, they initiate the Customer Incident Notification process. Microsoft provides impacted customers with an accurate, actionable, and timely notice, and notifies regulatory authorities as required.
    - Microsoft delivers customer notices no more than 72 hours from the time the breach was declared, except in the following circumstances:
        - Microsoft believes a notification increases risk to other customers. For example, the act of notifying may tip off an adversary causing an inability to remediate.
        - Other unusual or extreme circumstances vetted by Microsoft's legal department and the executive incident manager.
        - The 72-hour timeline may leave some incident details available. These are provided to customers and regulatory authorities as the investigation proceeds.
4. **Stabilize and recover:** The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps, such as quarantine, may occur immediately. The team may plan for longer term mitigations after the immediate risk has passed.
5. **Close and post-mortem:** The incident response team creates a post-mortem that reviews the details of the incident, with the intention to revise policies, procedures, and processes to prevent a recurrence.

Resources

As you work to ensure that your organization is properly protecting the customer and personal data that it collects, processes, and stores, these additional comprehensive webpages and white papers can offer supporting background information:

- Azure compliance documentation
- Azure governance documentation
- Azure data security and encryption best practices
- Achieving Compliant Data Residency and Security with Azure
- Security, Privacy, and Compliance in Microsoft Azure