Microsoft

Protecting Data Privacy Using Microsoft Azure

June 2020

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 Affordability 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 five-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 the protection of 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:

- Customer control over the collection, use, and distribution of customer data, facilitated by user-friendly tools and technologies
- Transparency about the specific policies, operational practices, and technologies that help ensure the privacy of your data to enable informed decisions
- Industry-leading security to protect data in transit, in process, and at rest
- Strong compliance rooted in respect for privacy laws and customer rights

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, which describes not only a way of building products, but also a model for operating services and structuring internal governance practices. This comprehensive approach extends to all the people, processes, and technologies that help to maintain and enhance privacy protections for Microsoft customers. We then put our commitments in writing in the Microsoft Privacy Statement where we detail Microsoft data protection policies and practices in clear, straightforward language.

» For more information, see Privacy at Microsoft.

> "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"

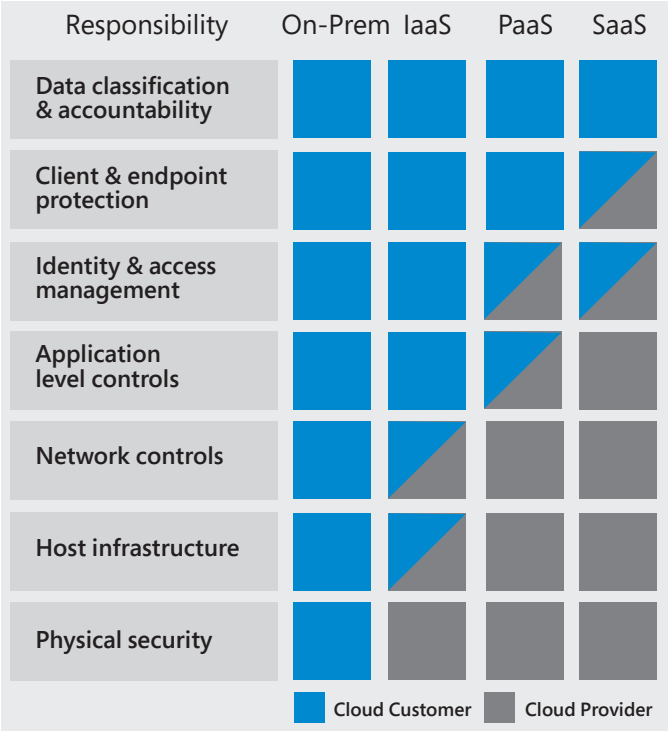
Privacy starts with data security

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.



How the responsibility for data security is shared

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.

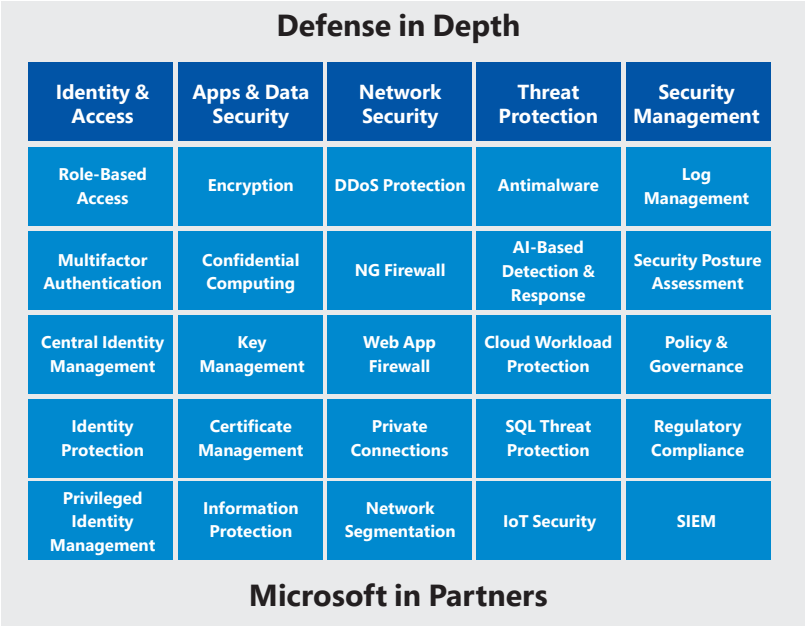
Microsoft is responsible for:	Your organization is responsible for:
Building services and features that can be used in compliance with applicable data protection and privacy regulations and standards.	Configuring the online services you use and training your workers to use those services in a way that 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.



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.

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.

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

- **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.

"Data governance refers to an overarching strategy that encompasses the policies, processes (including technologies), and people involved in managing and protecting 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.
- **Manage consent and notification**. It's important in privacy compliance to be able to document an individual's consent to collect personal data.
- **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 its processing in a timely manner in response to data subject requests. (In the GDPR, individuals are known as *data subjects*.)

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

Some Azure services can be used to identify, classify, and label personal data that resides in email and documents using embedded labels and permissions. This functionality can help you stay in control of how such data is accessed, used, and distributed even when it's shared with other people. These services include:

- **Azure Information Protection** (AIP) can help you classify documents and email by applying labels. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations. When you do this, the classification is identifiable regardless of where the data is stored or with whom it's shared. Metadata is added to files and email headers in clear text, which ensures that other services, such as data loss prevention solutions, can identify the classification and take appropriate action.

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

- **Azure Data Factory and HDInsight** can also help you classify data and label it for privacy compliance, to protect trade secrets, and so on.
- **Azure Data Catalog** can help with the management of metadata and enable you to discover the data sources you need, understand what you find, and then use that data.

» For more information, see What is Azure Data Catalog?

- **Azure Search, Azure Active Directory, Azure SQL Database, Power Query in Excel**, and **Query Explorer** can be used to search for and locate data, including personal data.

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 is allowed to 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 one of the most crucial aspects of 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 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 individuals (or 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.

"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."

How Azure can help you document your compliance

Microsoft offers the ability to access, delete, and export your customer data through the Azure Portal and also directly through pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services.

The **Azure Activity Log** can be used to document actions in Azure, such as who initiated an operation, when it occurred, and what the status of the operation was. You can use the Activity Log to determine the what, who, and when for any write operations (PUT, POST, DELETE) made for the resources in an Azure subscription, and be informed of the status of the operations and other relevant properties.

» 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.

Furthermore, traditional privacy controls may not suffice when new techniques for analyzing structured and unstructured information can discover and extrapolate relationships that reveal individuals' identity even when names and other obvious personal data have been removed.

The rapidly growing Internet of Things (IoT) has brought revolutionary new opportunities for increasing operational performance and increasing productivity. In August 2019, Gartner predicted that 5.8 billion enterprise and automotive IoT endpoints will be in use in 2020. More and more devices of all kinds are connecting to the global network every day, and many of them automatically collect, through sensors, various types of data that are transmitted over the internet. This device-specific data can present privacy issues.

Closely tied to the general growth of IoT is the boom in artificial intelligence (AI) devices. Using specialized machine learning, AI is also capable of reversing the anonymization of personal data, tracking people's movements, and predicting their behavior by profiling their personalities based on past patterns. This creates concerns regarding the privacy of the information that these devices collect.

Privacy 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 person residing in the EU at the time their personal data is being processed. 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. Complying with the GDPR has forced many companies to make significant changes to their IT infrastructures.

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 with regard to 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."

However, there are a number of federal laws that govern data privacy in certain business sectors, such as healthcare (Health Insurance Portability and Affordability 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.

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

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.
- TruSight, which is a risk-assessment utility created by leading US banks. It simplifies assessments by executing best-practice, standardized evaluations, enabling financial institutions to gain greater visibility into potential risks and manage third-party relationships more efficiently and effectively.
- 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.

Additional measures for protecting personal data in Azure

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 of your data in the cloud, including any data sets that contain personal data, as defined under the GDPR.

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 manage data subject consent and notification as well as respond to data subject requests.

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

Manage consent and notification

To comply with certain privacy regulations, such as the GDPR, you may need to obtain and document the consent of data subjects to collect or use their personal data as well as document the distribution of required privacy notices.

How Azure helps you document consent and notification

- The Azure infrastructure can host customized privacy notices to help meet GDPR notification requirements.
- **Azure Active Directory** can be used to request and obtain consent to use data.
- **Azure SQL Database** can be used to document data subjects who have granted their affirmative consent.

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

Respond to data subject requests

An important aspect of complying with the GDPR and similar privacy regulations involves responding to formal requests of data subjects. These include providing them copies of their personal data, correcting inaccurate data or rectifying incomplete data, and in some cases restricting the processing of their data or erasing it.

A data controller's response to these requests can take several forms, depending on the request and the nature of the data. To respond properly, you may need to:

- Find the relevant personal data.
- Assess the data and determine which data to provide to the subject.
- Decide on the format in which you will provide the data—copy of document, redacted version, screenshot, and so on.
- Rectify inaccurate, incomplete, or unlawful data (as specified by the data subject) by editing or removing it from specific documents.
- Restrict the processing of personal data.
- Delete personal data, possibly by deleting the data associated with a data subject.
- Export personal data in a standard electronic format for the user to transmit to another data controller.
- Access, delete, or export system-generated logs associated with a user.

How Azure can help you respond to data subject requests

You can use the **Azure Data Subject Requests for the GDPR** portal to help you find a data subject's personal data that resides in Azure. This online service is available through the Azure portal on Microsoft public and sovereign clouds, as well as through pre-existing APIs and UIs across the breadth of our online services.

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

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

- **Azure Search, Azure Active Directory, Azure SQL Explorer,** and **Query Explorer** can help you identify and rectify inaccurate or incomplete personal data.
- **Azure Active Directory, Azure SQL Database**, and **Query Explorer** can be used to erase personal data.
- **Azure File Service REST API** can be used 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** can all be used to export personal data in a common, structured format.
- **AAD Privileged Identity Management** can be used to restrict the processing of personal data by limiting access.

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

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 robust white papers may offer supporting background.

- 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