Microsoft

Privacy:

Azure gives customers ownership and control of their data

Trusted Cloud:
Microsoft Azure Security, Privacy, Compliance, Resiliency, and Protected IP

Author
Debra Shinder

Microsoft understands that when you use Azure, you are entrusting us with your most valuable asset—your data. You trust that its privacy will be protected and that it will be used only in a way that is consistent with your expectations.

For many organizations, keeping your data private is no longer merely desirable–it's mandatory. Government and industry regulations require that you protect the privacy of certain types of data. Breaches that expose personal information can have serious consequences.

The Microsoft approach to privacy is grounded in its commitment to give you control over the collection, use, and distribution of your customer data. Knowledge is the key to controlling your data, and with Azure:

- You know how Microsoft manages your data. Microsoft uses your customer data only to provide the services agreed upon and does not mine it for marketing or advertising. If you leave the service, Microsoft takes the necessary steps to ensure the continued ownership of your data.
- You know where your data is located. Customers who want to maintain their data in a specific geographic location can rely on the expanding network of Azure datacenters around the world. Microsoft also complies with international data protection laws regarding transfers of customer data across borders.
- You know who can access your data and on what terms. Microsoft takes strong measures to protect your data from inappropriate access, including restrictions that limit access for Microsoft personnel and subcontractors. However, you can access your own customer data at any time and for any reason.
- You know how Microsoft responds to government and law enforcement requests to access your customer data. Microsoft will not disclose customer data hosted in the Microsoft Cloud to a government or law enforcement except as you direct or where required by law.

How Microsoft manages your data

With Azure, you are the owner of your customer data and you retain all right, title and interest in the data. You can access your own customer data at any time and for any reason without assistance from Microsoft.

Microsoft does not share customer data for advertising. Your data is your business. Microsoft does not share business customer data with Microsoft advertiser-supported services, or mine it for marketing or advertising. Microsoft uses your Azure customer data only to provide the service and for purposes compatible with providing the service, including day-to-day operations and troubleshooting.

When Microsoft deletes your data

If you end your Azure subscription, Microsoft will retain your customer data for a period of time as specified in the Online Services Terms so you can extract the data. After the specified retention period ends, Microsoft will delete the customer data and personal data unless Microsoft is permitted or required by applicable law to retain such data or is authorized to do so in the agreement.

If you leave the Azure service or your subscription expires, Microsoft is governed by strict standards and follows specific processes that adhere to the contractual agreement for:

- Removing customer data from cloud systems under its control within specified time frames.
- Overwriting storage resources before reuse.
- Physical destruction of decommissioned hardware.

Learn more about how Microsoft handles data upon service termination.
Download Data Protection in Azure and see "Data Deletion" on page 21.

Where your data is located

As a customer of Azure services, you know where your data is stored. Azure offers an ever-expanding network of datacenters across the globe.

- Most Azure services permit you to specify the region where your customer data will be stored.
- Microsoft does not control or limit the locations from which you or your users may access, copy, or move customer data. Customers and their end users may move, copy, or access their customer data from any location globally.
- Microsoft may replicate customer data to other regions for data resiliency, but will not replicate or move customer data outside the geographic region.
- Microsoft complies with international data protection laws for transfers of customer data across borders.
- Microsoft will not transfer to any third party (not even for storage purposes) data that you provide to Microsoft through the use of Azure services that are covered under the Microsoft Online Services Terms.

Find Azure datacenter locations and get information about data storage for both regional and global services.

Learn more: Where your data is located

Who can access your data and on what terms

Microsoft takes strong measures to help protect your customer data from inappropriate access or use by unauthorized persons. In addition to the physical and technological protections discussed in the "Security" section of this paper, this includes restricting access by Microsoft personnel and subcontractors, and carefully defining requirements for responding to government requests for customer data.

You can access your customer data at all times. You can retrieve a copy of Azure customer data at any time and for any reason without the need to notify Microsoft or ask for assistance. At all times during the term of your Azure subscription, you can access, extract, and delete your customer data stored in Azure. You can also take your customer data with you if you end your subscription.

How Microsoft limits access to customer data. The operational processes that govern access to customer data in Microsoft business cloud services are protected by technical and organizational measures that include strong authentication and access controls, both physical and logical.

- Access to physical datacenter facilities is guarded by outer and inner perimeters with increasing security at each level.
  Learn more about how Azure secures its datacenters.
- Virtual access to customer data is restricted based on business need by role-based access control, multifactor authentication, minimizing standing access to production data, and other controls.
  Learn more about how Azure controls access to your data.
- To ensure control over encrypted data, you have the option to generate and manage your own encryption keys, determine who is authorized to use them, and revoke Microsoft copies of your encryption keys.
  Learn more about how Azure protects your data.

Azure is a multitenant service. This means your data, deployments, and virtual machines may be stored on the same physical hardware as that of other customers. Microsoft uses logical isolation to segregate storage and processing for each customer to help ensure that your customer data is not combined with anyone else's.

Microsoft limits access to your customer data by its personnel. Microsoft has automated a majority of its service operations so that only a small set requires human interaction.

Microsoft defines Customer Data as "all data, including all text, sound, video or image files, and software that are provided to Microsoft by, or on behalf of, the customer through the use of the online service." For example, this includes data that you upload for storage or processing and applications that you run in Azure.

Microsoft's approach to privacy is grounded in its commitment to give you control over the collection, use, and distribution of your Customer Data.

- Microsoft engineers do not have default access to cloud customer data. Instead, they are granted access under management oversight only when necessary.
- Microsoft personnel will use customer data only for purposes compatible with providing the contracted services. These may include troubleshooting aimed at preventing, detecting, or repairing problems affecting the operation of Azure, and the improvement of features such as protecting against threats, like malware.

Microsoft limits access to your customer data by subcontractors whom it hires to provide limited services on its behalf.

- Subcontractors can access and use customer data only to deliver the services they were hired to provide.
- The Microsoft Online Services Subcontractor List discloses the names of subcontractors who have access to customer data and provides advance notice of new subcontractors.

Learn more: Who can access your data and on what terms

Microsoft notifies you in case of a security breach

If Microsoft becomes aware of a breach of security that results in unauthorized access or disclosure of your customer data, Microsoft will:

- Promptly notify you of the security incident.
- Investigate the security incident and provide you with detailed information about it.
- Take reasonable steps to mitigate the effects and to minimize any resulting damage.

How Microsoft responds to government requests for customer data

Microsoft imposes carefully defined requirements on government and law enforcement requests for customer data. Such requests for customer data must comply with applicable laws. When governments or law enforcement agencies make a lawful request for customer data, Microsoft is committed to transparency and limits what it discloses.

- Microsoft will not disclose customer data hosted in Azure to a government or law enforcement except as you direct or where required by law. Microsoft does not give any third party, including law enforcement and government entities, direct or unfettered access to customer data.
- Microsoft always attempts to redirect third-party requests to you.
- If Microsoft is compelled by law to disclose customer data, you will be promptly notified and provided with a copy of the request, unless Microsoft is legally prohibited from doing so. Microsoft takes care to provide only the data specified in the legal order.
- Microsoft has taken steps to ensure that there are no "back doors" for use in government surveillance, and Microsoft does not provide any government with encryption keys or the ability to break the encryption that protects customer data.

Microsoft demonstrates its commitment to transparency by publishing semi-annual reports regarding requests for customer data made by law enforcement agencies. The Law Enforcement Requests Report site provides you with information about such requests made for customer data.

Learn more: Get detailed Microsoft data privacy standards.

Microsoft sets and adheres to stringent privacy standards

Microsoft is transparent about the specific policies, operational practices, and technologies that help ensure the privacy of your data in Microsoft business cloud services.

Microsoft builds privacy protections into Azure

Privacy is built into the Azure infrastructure, governed by Microsoft privacy policies and the Microsoft Privacy Standard, the cornerstone of the Microsoft privacy program. This authoritative document delineates the general privacy requirements for developing and deploying all Microsoft products and services, including Azure.

Standards and processes that support these principles include the Microsoft Online Services Privacy Statement (which details Microsoft's core data protection policies and practices) and the Microsoft Security Development Lifecycle (which integrates privacy requirements in the software development process).

Microsoft contractual commitments back its privacy best practices
Microsoft backs these privacy protections with strong contractual commitments to safeguard customer data, including:

ISO/IEC 27018. Microsoft was the first major cloud provider to adopt the first international code of practice for cloud privacy. An independent audit has verified that Azure is aligned with the ISO/IEC 27018 code of practice.

EU Model Clauses. EU data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA). Microsoft EU Standard Contractual Clauses provide specific contractual guarantees around transfers of personal data for covered services, which Europe's privacy regulators have determined meet EU standards for international transfers of data.

EU-U.S. Privacy Shield. Microsoft is certified to the EU-U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the EU to the United States. Microsoft also abides by Swiss data protection law regarding the processing of personal data from the EEA and Switzerland.

FERPA. The Family Educational Rights and Privacy Act (FERPA) is a US federal law that protects the privacy of student educational records. Microsoft agrees to the use and disclosure restrictions imposed by FERPA on Azure.

HIPAA. The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI). Azure and Azure Government offer customers a HIPAA Business Associate Agreement (BAA).

HITRUST. The Health Information Trust (HITRUST) Alliance created and maintains the Common Security Framework (CSF) to help healthcare organizations and cloud providers demonstrate their security and compliance.

LOPD (Spain). Microsoft was the first hyperscale cloud service provider to receive an authorization from the Spanish Data Protection Agency for its compliance with the high standards governing international data transfer under Spanish Organic Law 15/1999 (Ley Orgánica 15/1999 de Protección de Datos, or LOPD). Microsoft is also the first hyperscale cloud service provider to obtain a third-party audit certification for its online services' compliance with the security measures set forth in Title VIII of Royal Decree 1720/2007.

My Number Act (Japan). The "My Number" system created by Japan's legislature establishes a personal identification number assigned to every resident, foreign and domestic. Microsoft does not have standing access to My Number data stored in Azure; however, Microsoft contractually commits that Azure has implemented technical and organizational security safeguards to help customers protect individuals' privacy.

PDPA (Argentina). In a data transfer agreement, Microsoft makes a contractual commitment that Azure, Dynamics 365, Intune, and Office 365 in-scope services have implemented the applicable technical and organizational security measures stated in Regulation 11/2006 of the Argentine Data Protection Act, and also makes important commitments regarding notifications, auditing of our facilities, and use of subcontractors.

Privacy is built into the Azure infrastructure, governed by Microsoft privacy policies and the Microsoft Privacy Standard, the cornerstone of the Microsoft privacy program.

PIPEDA, PIPA, and BC FIPPA (Canada). The Personal Information Protection and Electronic Documents Act (PIPEDA), Alberta Personal Information Protection Act (PIPA), and British Columbia Freedom of Information and Protection of Privacy Act (BC FIPPA) are Canadian privacy laws that require organizations to take reasonable steps to safeguard information in their custody or control. Microsoft contractually commits that Azure and Intune in-scope services have implemented security safeguards to help protect the privacy of individuals, based on established industry standards.

EU General Data Protection Regulation (GDPR). The European Union's GDPR became enforceable on May 25, 2018. The GDPR sets a new bar globally for privacy rights, security, and compliance. It imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the EU, or that collect and analyze the personal data of everyone residing in the EU, whether or not they are citizens. The GDPR applies to such organizations no matter where they are located.

Microsoft has developed the following materials to help you prepare for compliance with the GDPR:

- Overview of the GDPR serves as an introduction to GDPR and its key concepts.
- How Azure Can Help Organizations Become Compliant with the EU GDPR. This white paper, written for decision makers, privacy officers, and security and compliance personnel, helps organizations identify and catalog personal data in Azure systems, build more secure environments, and simplify management of GDPR compliance.

  Learn more: visit the Microsoft GDPR home page.

Privacy tools

Microsoft simplifies your privacy burden with tools to help you automate privacy. Built-in controls, configuration management tools, and data subject request tools accelerate your compliance and save you money.

Azure Information Protection

You can add classification and protection information for persistent protection that stays with your data regardless of where it's stored or with whom it's shared. Azure Information Protection lets you configure policies to classify, label, and protect data based on its sensitivity. Classification is fully automatic, driven by users, or based on recommendation.

You can choose how your encryption keys are managed, and you can track activities on shared data and revoke access if necessary. Data classification and protection controls are integrated into Microsoft Office and common applications.

Azure Policy

You can define and enforce policies that help your cloud environment become compliant with internal policies as well as external regulations using Azure Policy. You can build custom policies with flexibility or apply built-in policies from Microsoft to govern your Azure resources.

Azure Data Subject Request (DSR) Portal

The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a Data Subject Request or DSR.

The Azure Data Subject Request (DSR) portal enables you to fulfill GDPR requests and shows you how to use Microsoft products, services, and administrative tools to find and act on personal data that reside in the Microsoft cloud to respond to DSRs.

Compliance Manager
Compliance Manager is a workflow-based risk assessment tool that enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft Professional Services and Microsoft cloud services, such as Microsoft Azure.

Compliance Manager provides you with a dashboard view of standards and regulations and assessments that contain Microsoft's control implementation details and test results and customer control implementation guidance and tracking. It provides a compliance score to help you track your progress and prioritize the auditing controls that will help reduce your organization's exposure to risk.

Learn more about Compliance Manager.


Microsoft